

accenture[>]security

2019

CYBER THREATSCAPE REPORT

iDEFENSE 
Part of Accenture Security

CONTENTS

EXECUTIVE SUMMARY	4
WHAT'S INSIDE?	8
FIVE THREAT FACTORS	12
1 COMPROMISING GEOPOLITICS: NEW THREATS EMERGE FROM DISINFORMATION AND TECHNOLOGY EVOLUTION	
Overview	12
Top-line assessment: Key judgments	13
Hacking minds and hearts	13
Disinformation tradecraft	15
Cyber-enabled information operations	18
Social media as the disinformation battlefield	19
Artificial Intelligence, 5G and disinformation	22
Hacktivism masks	24
Challenges of fighting disinformation and other information operations	28
Geopolitical events could engender disruptive and exploitative cyberthreat activity	29
Cyberthreat uses of global events: Opportunism and participation	32
A cost-benefit proposition	33
Use of current events as lures	34
Destructive malware and backdooring: A Damocles sword over critical infrastructure	37
Summary	38
2 CYBERCRIMINALS ADAPT, HUSTLE, DIVERSIFY AND ARE LOOKING MORE LIKE STATES	
Overview	39
Top-line assessment: Key judgments	39
Secure syndicates: A new model for cybercrime operations	40
Regional cybercrime: Exploitation of localized technologies	41
Big game hunting: More targeted attacks	43
Network access for sale	46
Summary	49

3	HYBRID MOTIVES POSE NEW DANGERS IN RANSOMWARE DEFENSE AND RESPONSE	
	Overview	50
	Top-line assessment: Key judgments	50
	Ransomware attacks, vectors and motives	51
	Leading practices for ransomware mitigation	60
	Summary	65
4	IMPROVED ECOSYSTEM HYGIENE IS PUSHING THREATS TO THE SUPPLY CHAIN, TURNING FRIENDS INTO FRENEMIES	
	Overview	66
	Top-line assessment: Key judgments	67
	Background	67
	Politically motivated supply chain compromises continue	68
	The underground market for supply chain compromise	71
	Geopolitics and supply chain frenemies	73
	Proactive defense: Leveraging cyberthreat intelligence to protect supply chains	74
	Integrating CTI with merger and acquisition pursuits	75
	Summary	82
5	LIFE AFTER MELTDOWN: VULNERABILITIES IN COMPUTER CLOUD INFRASTRUCTURE DEMAND COSTLY SOLUTIONS	
	Overview	83
	Top-line assessment: Key judgments	83
	Transient execution side channel attacks	84
	Risk overview	85
	Mitigations	85
	Summary	89
	A SECURITY PIVOT	90
	ABOUT THE REPORT	92
	GLOSSARY	93
	CONTACTS	99

EXECUTIVE SUMMARY

In the face of growing cybercrime, there are few deterrents more effective than hitting attackers where it hurts most—in their own wallets. The more organizations invest in securing their networks and training their staff on how to safely navigate the digital workplace, the harder and more expensive it becomes for threat actors to disrupt or breach networks.

But reducing any return on cybercriminals' own investments or cutting into their profits, is only effective if they maintain the status quo—and many do not. Far from being overwhelmed by hardening environments, threat actors are proving their confidence as chameleons. As threat actors face effective defenses to tried and tested attack vectors, they adapt and switch to try out new tactics, techniques and procedures (TTPs). And this adaptation is proving successful. In particular, we are seeing the emergence of new cybercrime operating models among high-profile threat groups. Relationships are forming among “secure syndicates” that closely collaborate and use the same tools—suggesting a major change in how threat actors work together in the underground economy, which will make attribution even more difficult.

The Accenture Security iDefense Threat Intelligence Services team has observed a distinct and dangerous shift in threat actor TTPs during the past 12 months. Threat actors are pivoting their operations strategically, operationally and tactically—and in doing so they are testing the resilience of organizations who are doing their best to keep up. Let's take a look at these changes in more detail.

From a **strategic** perspective, Accenture iDefense has observed global disinformation continues to battle for “hearts and minds” with threat actors becoming more skilled at exploiting legitimate tools. While disinformation campaigns to influence domestic or foreign political sentiment and sway national elections are likely to continue, the wider potential impact of disinformation on global financial markets is a concern. The financial services industry—and, more specifically, high-frequency trading algorithms, which rely upon fast, text-driven sources of information—are likely to be targeted by large-scale disinformation efforts in the future.

In January 2019, a firm was targeted by an elaborate hoax involving a spoofed letter purporting to be written by the fund group's chief executive officer.¹ The letter claimed the firm was divesting in coal companies in its actively-managed funds and changing voting patterns to take a stronger stance on climate change. The adversaries also created a website that looked like the large investment management corporation's genuine webpage. Several thousand people received the fake letter and large news outlets initially picked up the letter as a legitimate communication. It was eventually revealed that the letter and website were the work of an activist seeking to raise awareness for social issues, such as the environment. The incident emphasized the low barrier to entry for an effective disinformation campaign. These incidents remain dangerous indicators for the future of cyberthreats to financial institutions and financial market infrastructures. A well-orchestrated disinformation campaign may have serious consequences on brand reputation, specific markets, and even market stability. The tools required to implement a successful campaign are well within the capability for ideologically, financially, and politically motivated threat adversaries already targeting the financial sector.

To take full advantage of the world stage, threat actors are paying even closer attention to important global events and are using them as distractions or lures to breach target networks. Accenture iDefense has seen a sharp decline in "true" hacktivism and is instead seeing more state-sponsored hacktivism with goals to disrupt events and influence a wide range of activities in the sponsoring nation's favor. Nation-states are increasingly outsourcing malicious cyberoperations to cybercriminals to increase their capabilities and attain strategic goals—blurring lines between politically and financially motivated cyberthreat activities.

¹ What's the cyber future for Financial Services? April 26, 2019. Accenture. <https://www.accenture.com/us-en/blogs/blogs-cyber-future-financial-services>.

EXECUTIVE SUMMARY

In such a climate, advances in technology such as artificial intelligence and fifth-generation cellular network technology (5G) communications could provide new opportunities for threat actors to achieve their objectives. And as new avenues are being targeted for attacks, cyberdefenders should look more closely at how they monitor their supply chain and business partners in tandem with their own security efforts. Many threat actors are circumnavigating target networks by trying to breach them via the networks of trusted partners, business associates and other third-party networks. As ever, cybercriminals are persistent and inventive—if they can't get in one way, they will keep trying until they find another.

From an **operational** perspective, Accenture iDefense has seen how some attackers are continuing to focus on infecting legitimate software applications with malicious code to try to accomplish supply chain compromises. But they are also making subtle changes to how they work and who is part of their inner circle. After several high-profile law enforcement takedowns, threat actors have started to close doors on the open sharing of malware and exploits and, instead, are sharing within only smaller, trusted syndicates.

The majority of hackers still rely on human error as the main way to breach networks; however, with increased awareness of domain-squatting and phishing, the returns for such attack methods has decreased. Even so, some tried and tested methods are far from being abandoned. Threat actors continue to use “living off the land” tools and non-malicious software, such as Remote Desktop Protocol (RDP) and PowerShell, in malicious ways to attempt to avoid detection.²

From a **tactical** perspective, Accenture iDefense notes that ransomware attacks have risen as one of the key destructive tools used for financial

2 Security Response. “What is Living off the Land?” October 3, 2018. Symantec. <https://medium.com/threat-intel/what-is-living-off-the-land-ca0c2e932931>.

gain, with attackers seeking extortion alongside sabotage and destruction. Many threat actors are reusing existing malware in new ways or using new types of malware to exploit different types of vulnerabilities. Threat actors are continuing to abuse code-signing techniques by using stolen digital certificates to sign their malicious files and malware to avoid detection.

Further technical impact is being experienced as a result of the proliferation of the use of cloud computing. This open and popular environment has prompted security researchers and adversaries to look for risk in the cloud infrastructure, leading to the discovery of multiple side-channel vulnerabilities in modern computer microprocessors (CPUs) over the last two years. Such vulnerabilities pose a high risk to organizations as adversaries help themselves to better access to sophisticated and sensitive data.

In the 2017 and 2018 Threatscape reports, Accenture iDefense stated that organizations need to enhance their threat intelligence capabilities to stay ahead of cyberthreats, rather than just activate their incident response plans when their networks are breached. In 2019, this recommendation has not changed—and is unlikely to change in the foreseeable future.

In the past year, cybercriminals have continued to test the resilience of organizations and governments by layering attacks, updating techniques and establishing new, intricate relationships to better disguise their identities. It is no longer enough to plan for attacks or understand what to expect. To help reduce business risks, organizations need to make a security pivot of their own. By pivoting their approach to security on a regular basis, they can keep up-to-date with the shifting threat landscape, organizations' adversaries and those adversaries' TTPs, and be better placed to achieve cyberresilience.

EXECUTIVE SUMMARY

WHAT'S INSIDE?

The 2018 Cyber Threatscape report noted the clear need for more effective use of actionable threat intelligence. With state-sponsored activities a growing force to be reckoned with, extended supply chain threats, targets against critical infrastructure and a surge in miner malware and more financially motivated advanced persistent threats, CISOs have had their work cut out to budget and act effectively.

Strong investment in cybersecurity has not been lacking. But despite these investments, the relentless creativity of cybercriminals continues to put pressure on organizations to be defense ready. Threat intelligence provides the right information to make better business decisions. But the scope of that intelligence is growing. Businesses could start evaluating their cyberpostures from many different perspectives—the cyberposture of suppliers, partners and acquisition targets are just as important as their own organizations to avoid opening up new security gaps or inviting in threat actors who are dormant or active on third-party networks.

The 2019 Cyber Threatscape report has discovered five factors that are influencing the cyberthreat landscape:

1. Compromising geopolitics: New threats emerge from disinformation and technology evolution

Global businesses may find themselves in the crosshairs as geopolitical tensions persist. As cyberthreat actors take advantage of high-profile global events and seek to influence mass opinion, we can expect these actors to not only sustain current levels of activity but also to take advantage of new capabilities as new technologies enable more-sophisticated threat TTPs. Geopolitical analysis and a strategic-level understanding of the events that motivate cyberthreats to action

can help businesses manage known threats and allocate resources in anticipation of emerging threats.

2. Cybercriminals adapt, hustle, diversify and are looking more like states

Despite high-profile law enforcement actions against criminal communities and syndicates in 2018, the ability of threat actors to remain operational highlights the significant increase in the maturity and resilience of criminal networks in 2019. Our analysis indicates conventional cybercrime and financially-motivated, targeted attacks will continue to pose a significant threat for individual Internet users and businesses. However, criminal operations will likely continue to shift their tactics to reduce risks of detection and disruptions. They could also attempt to maximize the return on effort in several ways such as: shifting away from partnerships to operating within close-knit syndicates; taking advantage of familiarity with the local environment; increasing the precision of targeting by using legitimate documents to identify likely victims before delivering malware; or selling and buying direct access to networks for ransomware delivery rather than carrying out advanced intrusions.

3. Hybrid motives pose new dangers in ransomware defense and response

The ransomware threat will be exacerbated further by the sale of access to corporate networks—through which an attacker can deploy ransomware on a corporate-wide scale—and the potential of ransomware with self-propagating abilities (such as WannaCry) to reemerge could pose a significant threat to businesses, particularly those with time-critical operations.

EXECUTIVE SUMMARY

While the motives behind such an attack may appear to be financial, targeted ransomware attacks may at times serve hybrid motives, whether financial, ideological, or political. Regardless of motive, while the ransomware threat remains, organizations must ensure they take adequate measures to prepare, prevent, detect, respond, and contain a corporation-wide ransomware attack. Considering the possibility that an apparently financially-motivated ransomware attack may in fact serve other purposes, a ransom payment may not guarantee the restoration of company data; therefore, companies should plan for the recovery of operations, even in the event of a disruptive loss of data.

4. Improved ecosystem hygiene is pushing threats to the supply chain, turning friends into frenemies

The global interconnectedness of business, the wider adoption of traditional industry cyberthreat countermeasures and improvements to basic cybersecurity hygiene appear to be pushing cyberthreat actors to seek new avenues to compromise organizations, such as targeting their supply chains—including those for software, hardware and the cloud. Organizations should routinely seek full awareness of their threat profiles and points of supply chain vulnerability. Organizations can try to improve processes that guard against the cybersecurity risks inherent in the landscape of modern global business operations by integrating cyberthreat intelligence into M&As and other strategically important actions, incorporating vendor and factory testing into their processes, and implementing industry-focused regulations and risk assessment standards.

5. Life after meltdown: Vulnerabilities in compute cloud infrastructure demand costly solutions

The discovery of multiple side-channel vulnerabilities in modern CPUs over the last two years could pose a high risk to organizations running their compute infrastructure in the public cloud. Adversaries can use this class of side-channel vulnerabilities to read sensitive data from other hosts on the same physical server. Mitigations are available for most platforms, cloud deployments, and software. However, most of the mitigations come at a cost of reduced performance, leading to a potential increase of compute costs for enterprises. Understanding the threats posed by CPU vulnerabilities is important to design a proper risk mitigation strategy, which can be vastly different for each organization.

In this report, Accenture iDefense offers leading practices to consider for mitigating ransomware, suggestions regarding employee cybersecurity training, evaluations of international events coming up in the next 12 months and outlines which threat actors might use such events for nefarious purposes. Accenture iDefense aims to help its clients, partners and community members by providing this information so that they can stay ahead of threats pertinent to their businesses, industries and geographies.

FIVE THREAT FACTORS

1 **COMPROMISING GEOPOLITICS: NEW THREATS EMERGE FROM DISINFORMATION AND TECHNOLOGY EVOLUTION**

OVERVIEW

Government agencies, research firms and media reports continue to warn of cyberthreats to upcoming elections.³ Election threats remain high, even as defense efforts are also increasing. Meanwhile, many threat actors continue to try taking advantage of and seek to influence many other types of global political and geopolitical events, such as international summits, evolving international tensions and sporting events—like the Olympics.

Phishing lures, destructive malware targeting, and influence operations on a social media battlefield closely follow global, political and international events. As a result, these events provide contextual insight and help to assess the motives, timing and targeting of cyberthreat operations.

3 Suggested reading: “Worldwide Threat Assessment of the US Intelligence Community.” January 29, 2019. DNI. <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf>; “Best Practices for Securing Election Systems.” May 21, 2019. US-CERT. <https://www.us-cert.gov/ncas/tips/ST19-002>; “Progress Made, But Additional Efforts Are Needed to Secure the Election Infrastructure.” February 28, 2019. DHS OIG. <https://www.oig.dhs.gov/sites/default/files/assets/2019-03/OIG-19-24-Feb19.pdf>; “Election Cybersecurity: Challenges and Opportunities.” February 2019. ENISA. <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/election-cybersecurity-challenges-and-opportunities>; “Elections under threat: securing democracy in cyberspace.” February 26, 2019. Microsoft. <https://blogs.microsoft.com/eupolicy/2019/02/26/securing-democracy-in-cyberspace/>; “An update on our work to prevent abuse ahead of the EU elections.” January 29, 2019. Google. <https://www.blog.google/around-the-globe/google-europe/update-our-work-prevent-abuse-ahead-eu-elections/>; “Homeland Security Chief Cites Top Threat to U.S. (It’s Not the Border).” March 18, 2019. *The New York Times*. <https://www.nytimes.com/2019/03/18/us/politics/homeland-security-cyberthreats.html>.

TOP-LINE ASSESSMENT: KEY JUDGMENTS

- Social media remains a battleground for the hearts and minds of worldwide audiences, as it can be used for disinformation and other forms of information operations to try to sway opinion and influence policy.
- So-called “cyber-enabled information operations” (CyIO) that can exploit the openness and speed of communications in cyberspace, sometimes drawing on cyberthreat operations such as hacking, distributed denial-of-service (DDoS) and defacements, are considered a particular threat. Advances in technology, such as artificial intelligence and 5G communications, could provide new opportunities for threat actors to take advantage of and influence global political events.
- We expect upcoming world events to become the setting for information operations and other cyberthreat activity—ranging from espionage to DDoS to destructive attacks. These events include elections, the 2020 Tokyo Summer Olympics, events related to NATO expansion and activities, and key commemorative dates.
- Cyberthreat actors could engage with these geopolitical events in various ways: as opportunists, using them as phishing lures or distractions, and as participants seeking to influence outcomes.

HACKING MINDS AND HEARTS

When Keir Giles, a security researcher in London, received a LinkedIn invitation from one “Katie Jones,” who described herself as an area studies specialist at a Washington DC think tank, he detected something fishy. He called on other researchers to analyze the profile photo of an

FIVE THREAT FACTORS

attractive redhead. They soon concluded that “Katie Jones” did not exist; the photo had been created using generative adversarial networks, or GANs, a form of artificial intelligence. Whoever created it was apparently attempting to gain the trust of Keir Giles, and likely to spy on him.⁴

The case of the illusory “Katie Jones” exemplifies the problem of disinformation being used for political purposes. Malicious actors can exploit the capabilities of cyberspace—the speed and openness of the Internet and other information technologies, as well as legitimate tools, like artificial intelligence, and illegitimate tools, like malware, to pursue their strategic goals. All of these come together in what the US Defense Department and scholars like Dr. Herb Lin of Stanford University call cyber-enabled information operations. Lin notes that, while traditional cyberwarfare “prosecutes conflict through the hacking of computers” cyber-enabled information operations does the same “through the hacking of people’s minds and hearts.”⁵

One area in which such operations have been used—elections—dominates the headlines. Urgent discussions in many countries focus on whether cyberthreat actors can manipulate vote counts and voter registration information. Entities, suspected of being SNAKEMACKEREL threat group actors, unsuccessfully attempted such direct manipulation during the 2014 Ukrainian elections⁶ and succeeded in obtaining access to local United States’ election boards in 2016.⁷

4 Satter, Raphael. “Experts: Spy used AI-generated face to connect with targets.” June 13, 2019. AP News. <https://www.apnews.com/bc2f19097a4c4fffaa00de6770b8a60d>.

5 Lin, Herb. Cyber-Enabled Information Operations Through the Lens of Cyberwar. Cybersecurity and Privacy (CySeP) Technical Program. June 11, 2019, Stockholm, Sweden. <https://cysep.conf.kth.se/agenda.html>.
McCain, John. “NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2019-CONFERENCE REPORT” July, 2018. https://www.acq.osd.mil/dpap/dars/docs/FY19_NDAA_Conf_Bill.pdf.

6 iDefense Security Intelligence Services. “Outcast Russia Eyes 2019.” February 1, 2019. IntelGraph reporting.

7 Mueller, Robert. “Report on the Investigation into Russian Interference in the 2016 Presidential Election.” March 22, 2019. US Department of Justice. <https://www.justice.gov/storage/report.pdf>.

Whether or not such direct manipulation of vote counts is successfully undertaken in the future, broader cyber-enabled information operations may continue to target elections worldwide. Threat actors use them, for example, to discredit candidates, sow doubt in the legitimacy of election results and undermine confidence in political institutions. Simply compromising a candidate's e-mail account to selectively leak compromising information or even just to threaten to leak it could be used to discredit a politician or blackmail them into making friendly policy decisions, for example. However, these operations could go much further than just elections.

DISINFORMATION TRADECRAFT

Disinformation is communication designed to influence perceptions. Tactics can range from outright falsification, to the selection and distortion of facts to tell a misleading story.

Disinformation is one type of "information operations" (IO). The United States military defines IO as actions taken "for the use and management of information to pursue a competitive advantage."⁸ One top social media company defines IO as "actions taken by organized actors (governments or non-state actors) to distort domestic or foreign political sentiment, most frequently to achieve a strategic and/or geopolitical outcome."⁹ In addition to deliberate disinformation, information operations also include propaganda (the spread of information to promote a particular political cause) and misinformation (the spread of inaccurate information without an intent to deceive).¹⁰

8 Theohary, Catherine. "Defense Primer: Information Operations." Updated December 18, 2018. Congressional Research Service. <https://crsreports.congress.gov/product/pdf/IF/IF10771>.

9 Weedon, Jen et al. "Information Operations and Facebook." April 27, 2017. <https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf>.

10 Theohary, Catherine. "Defense Primer: Information Operations." Updated December 18, 2018. Congressional Research Service. <https://crsreports.congress.gov/product/pdf/IF/IF10771>.

FIVE THREAT FACTORS

Those who carry out disinformation and other IO can do so via “white” methods (broadcasting one’s message openly through state media), “grey” methods (placing information in other sympathetic media), and “black” methods (using hackers, trolls, and honeypots).¹¹ They seek to target various audiences. For a non-state actor such as a criminal group or gang, the audiences could include one’s own group members or a rival group, law enforcement, politicians, or the general public. For a state, audiences could include one’s own population; the adversary country’s politicians, bureaucrats or soldiers; various groups within the adversary country’s population; or world opinion as a whole. Aimed at one’s own group or population, information operations could seek to reassure, shape opinion, or scare the population into rallying around a particular purpose. When targeting politicians or decisionmakers, IO could persuade, scare, or lure them into making decisions favorable to the group undertaking the operations. When aimed at an adversary group’s military or general population, IO may erode its desire to resist, win its support, or gain leverage by crafting alternate narratives or sowing divisions.

The term “Advanced Persistent Manipulators,” coined by analyst Clint Watts of the Foreign Policy Research Institute and George Washington University, describes entities—whether activist or extremist groups, national governments, political campaigns, lobbyists, businesses or celebrities—that have the resources to conduct “an extended, sophisticated, multi-platform, multi-media information attack on a specified target,”¹² sometimes combining online influence campaigns with real-world activities such as rallies. They can employ “trolling-as-a-service” firms to aggregate audience data and disseminate targeted and, often inauthentic messaging, sometimes involving altered data.

11 iDefense Security Intelligence Services. “Aggressive Defensiveness: Russian Information Operations against the US Political System.” January 7, 2017. IntelGraph reporting.

12 “Advanced Persistent Manipulators (APM).” June 5, 2019. Alliance for Securing Democracy. <https://securingdemocracy.gmfus.org/wp-content/uploads/2019/02/APM-Clint-1.pdf>.

Disinformation and other IO pursue goals that can be summed up with variant catchy “D-words”: “dismiss an opponent’s claims or allegations, distort events to serve political purposes, distract from one’s own activities, and dismay those who might otherwise oppose one’s goals.”¹³ Another list of D-words to describe the goals “divide, discredit, distract, deny, and demoralize.”¹⁴

Tactics used in information operations can include false news, disinformation, or what Facebook calls “false amplifiers”—“networks of fake accounts aimed at manipulating public opinion.”¹⁵ Examples of the use of these tactics include:

- flooding the media with multiple versions of a story¹⁶ to confuse the audience and make them give up on trying to understand the truth, similar to the “chaff” used in kinetic warfare to misguide enemy radar;
- publicizing scandalous information to discredit a critic or adversary;
- distracting world opinion from negative information, by highlighting or even creating some other crisis or scandal; and

13 Jackson, Dean. “Issue Brief: Distinguishing Disinformation from Propaganda, Misinformation, and “Fake News.” October 17, 2017. National Endowment for Democracy. <https://www.ned.org/issue-brief-distinguishing-disinformation-from-propaganda-misinformation-and-fake-news>.

14 iDefense Security Intelligence Services. “Outcast Russia Eyes 2019.” February 1, 2019. https://intelgraph.idefense.com/#/node/intelligence_alert/view/df6d1797-79c5-42fd-9792-d5abbbe4467e; iDefense Security Intelligence Services. “GRU Unmasking Opens New Phase of CyberCold War.” November 17, 2018. IntelGraph reporting.

15 Weedon, Jen et al. “Information Operations and Facebook.” April 27, 2017. <https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf>.

16 Rid, Thomas. March 29, 2018. Twitter. <https://twitter.com/RidT/status/979420795024871424>.

FIVE THREAT FACTORS

- using inauthentic social media profiles to inflame real-world violence by publicizing rallies of rival groups,¹⁷ and even to influence government policies.¹⁸

CYBER-ENABLED INFORMATION OPERATIONS

CyIO¹⁹ can be defined broadly to include any information operations taking place in cyberspace, including in online media and social media.²⁰ Alternatively, CyIO can be defined more narrowly, to refer to information operations leveraging offensive cyberthreat activity such as breaches and DDoS. As the Congressional Research Service summarizes military uses of CyIO, “Cyberspace operations can be used to achieve strategic information warfare goals; an offensive cyberattack, for example, may be used to create psychological effects in a target population. A foreign country may use cyberattacks to influence decision making and change behaviors,” as in the massive state-attributed attack on a major entertainment company in 2014 in apparent retaliation for a movie criticizing the state’s leader.²¹ CyIO can also weaken a country’s military capabilities by disrupting communications or serving as a deterrent.²²

17 Joyner, Chris. “‘Pro-white’ rally at Stone Mountain collapses amid internal strife.” January 31, 2019. Atlanta Journal-Constitution. <https://www.ajc.com/news/breaking-news/pro-white-rally-stone-mountain-collapses-amid-internal-strife/gvReqHeqcXNqFytV9xm1jK/>.

18 Rezaian, Jason. Why does the U.S. need trolls to make its Iran case? June 11, 2019. The Washington Post. <https://www.washingtonpost.com/opinions/2019/06/11/why-does-us-need-trolls-make-its-iran-case/>.

19 “Summary: Department of Defense CyberStrategy.” September 18, 2018. US Department of Defense. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF; Kerr, Jaclyn and Herbert Lin. “On Cyber-Enabled Information Warfare and Information Operations.” forthcoming, Oxford Handbook of Cybersecurity, 2019. May 2019. Oxford University Press. <https://ssrn.com/abstract=3015680>.

20 “Statement of Chris Inglis before the Senate Armed Services Committee.” April 27, 2017. <https://www.armed-services.senate.gov/hearings/17-04-27-cyber-enabled-information-operations>.

21 “The Interview: A guide to the cyber attack on Hollywood”. 29 December 2014. BBC News. <https://www.bbc.co.uk/news/entertainment-arts-30512032>.

22 Theohary, Catherine. “Defense Primer: Information Operations.” Updated December 18, 2018. Congressional Research Service. <https://crsreports.congress.gov/product/pdf/IF/IF10771>.

State-sponsored cyber-enabled information operations combine cyberthreat activities—such as stealing or altering information or conducting DDoS attacks—with information operations, like the use of disinformation and software bots, in attempts to weaken people, organizations and countries that are hostile to that state. A typical example could include breaching a target’s e-mails, analyzing the stolen content to find unflattering information, possibly distorting or embellishing that information; false hacktivism and creating inauthentic online personas and troll bots to broadcast the negative information and to influence popular opinion against the target.²³

SOCIAL MEDIA AS THE DISINFORMATION BATTLEFIELD

Social media has become an increasingly fraught battlefield for cyberthreat actors and more broadly, information operations. The near omnipresent role of social media in everyday life has positioned online communities as target-rich environments which exist beyond the conventional purview of corporations’ security controls. This has propelled social networks to the frontlines, as high-yield arenas for manipulation.

In recent years, the research center Citizen Lab, has detailed the tradecraft of state-affiliated groups spreading disinformation via social media. One group, given the name “Endless Mayfly,” is suspected of conducting both disinformation and malware campaigns. Endless Mayfly used typo-squatted domains to impersonate global news outlets, “replacing letters with look-alike characters to create visually identical domains.”²⁴ These sites were promoted on social media platforms as part

23 iDefense Security Intelligence Services. “Cultural and Political Flashpoints Could Drive Cyberoperations in Entertainment Industry.” March 14, 2019. IntelGraph reporting.

24 Lim, Gabrielle, et. al. “Burned After Reading: Endless Mayfly’s Ephemeral Disinformation Campaign.” May 14, 2019. The Citizen Lab. <https://citizenlab.ca/2019/05/burned-after-reading-endless-mayflys-ephemeral-disinformation-campaign/#fn1>.

FIVE THREAT FACTORS

of an effort to spread disinformation to journalists. The group leveraged extensive use of ephemerality by intentionally deleting content once it has been sufficiently circulated. Covering one's tracks could provide a level of plausible deniability, something upon which state actors often rely. On at least one occasion, it is believed that Endless Mayfly also hosted malicious mobile applications, impersonating Twitter, on a subdomain of one of their disinformation websites, which mimicked the social media platform. When viewed through the lens of state surveillance, these types of scenarios become increasingly concerning. Some nation-states are likely to continue teasing out their opposition and monitoring their citizens through manipulation of information on social networks, coupled with spyware campaigns.

Case study: Financial market manipulation via social media bots

From an industry perspective, social media coupled with disinformation, can present unique challenges. Financial services, specifically high-frequency trading algorithms which rely upon fast, text-driven sources of information, are likely to be affected by large-scale disinformation. Academic research has already found that social media bots “could have an impact on returns, volatility and trading volume of individual stocks.”²⁵ The research highlights the converse relationship between amplified messaging (negative or positive) and the market, raising important policy concerns for safeguarding financial stability. Maliciously influencing trading in this manner is in some ways an extension of “pump and dump” activity associated with various criminal operations, including the group behind the post-SEC EDGAR breach trades and their larger ecosystem of compatriots.²⁶

25 Fan, Rui, et. al. “Social media bots and stock markets.” Updated November 2018. Swansea University. https://www.researchgate.net/publication/331639758_Social_media_bots_and_stock_markets.

26 Mathews, Lee. “SEC Charges Hackers Who Broke Into EDGAR Database And Traded On Stolen Secrets.” January 15, 2019. <https://www.forbes.com/sites/leemathews/2019/01/15/sec-charges-hackers-who-broke-into-edgar-database-and-traded-on-stolen-secrets/#6aea981e5979>.

Overall, the threat landscape has shifted, opening the door for destructive malware and autonomous tools to be mixed with fake news, equipping organized cybercriminals and nation-states with an arsenal of tactics, techniques and procedures at their disposal. “For financial services, such an attack could upend the stability and trust that sustains the entire system. The combination of the multifaceted and multi-staged campaigns of disinformation, paired with cyberattacks, can be expected to continue in coming years.”²⁷

Case study: Evolving from misinfodemics to disinfodemics in healthcare

The spread of inaccurate information through social media can have serious ramifications in healthcare. “Misinfodemics,” a phrase coined by Harvard researchers, melds misinformation and disease epidemics. The Harvard researchers note that “digital health misinformation is having increasingly catastrophic impacts on physical health.”²⁸ Ebola, for example, has been more easily spread following the dissemination of misleading online information concerning preventative guidance. Where inaccurate messages “go viral,” health workers on the ground are met with mistrust and hostility, making it tough to drive down infection rates. “The spread of the informational viruses interferes with the fight against actual biological viruses.”²⁹ One could also hypothesize a parallel scenario of “disinfodemics,” in which a threat actor deliberately uses disinformation to catalyze epidemics.

27 Accenture Security. “Future cyberthreats: Extreme but plausible threat scenarios in Financial Services.” May 2019. https://www.accenture.com/_acnmedia/PDF-100/Accenture_FS_Threat-Report_Approved.pdf#zoom=50.

28 Gyenes, Nat, et. al. “How Misinfodemics Spread Disease.” August 30, 2018. The Atlantic. <https://www.theatlantic.com/technology/archive/2018/08/how-misinfodemics-spread-disease/568921/>.

29 Igaier, Joachim, et. al. “The communication aspects of the Ebola virus disease outbreak in Western Africa – do we need to counter one, two, or many epidemics?” October 2015. Croatian Medical Journal. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4655935/>.

FIVE THREAT FACTORS

Hypothetically, disinformation intended to degrade public health could be utilized by states to target adversarial nations. Actors are likely to use fabricated media content or falsified personas to discredit legitimate sources of health information and further degrade them through cyberattacks. In a tangential example, the SNAKEMACKEREL threat group targeted international anti-doping agencies in 2018. In an attempt to discredit the anti-doping community, the state-sponsored actors used false online accounts to release stolen, sometimes intentionally doctored, information concerning nearly 250 athletes from almost 30 countries.³⁰

Social media has also been used to spread weaponized lures directly. Amplification of politicized narratives which elevate topics of interest to targeted users sets the stage for the success of these lures, as in the WINTERFLOUNDER example described on page 36. This is one of a number of ways cyberthreat actors can leverage disinformation during their campaigns.

ARTIFICIAL INTELLIGENCE, 5G AND DISINFORMATION

Emerging technologies, such as artificial intelligence (AI), present new avenues of expression for potential geopolitical activity, including disinformation. One menacing use of AI is in the creation of “deepfakes,” which are high-quality forged images or videos that could be used for anything from discrediting or blackmailing a political opponent, rival company or extortion target, to causing worldwide panic with a video of a head of state purportedly claiming to have launched a nuclear weapon. The propagation of synthetic media content, such as deepfakes, is likely to accelerate as fabrication tools become more accessible and widespread. This could spill over into the cyberdomain, where both politically and financially

³⁰ iDefense Security Intelligence Services. “US Indictment Fingers [Redacted] in SNAKEMACKEREL Targeting of Anti-Doping Organizations.” November 12, 2018. IntelGraph reporting.

motivated actors could leverage deepfakes during target reconnaissance on social networks or social engineering campaigns, for example.

In the report “Know Your Threat: AI Is the New Attack Surface,”³¹ Accenture Labs explains this phenomenon and other avenues of adversary opportunity opened up by increasingly complex machine-learning models, especially image content and classification, natural language processing and industrial control systems (ICS). As they focus more on interference with AI modeling, threat actors and groups are likely to deploy adversarial AI, corrupting the ability of machine learning algorithms to interpret system inputs and exercising control over their behavior. To do this, attackers may create adversarial examples to break the model’s performance, using deep learning models known as Generative Adversarial Networks. Researchers have demonstrated proof-of-concept (PoC) attacks against malware detection and optical character recognition. Adversarial AI using deep-learning applications in natural-language processing could enable the manipulation of algorithms that determine sentiment, gather intelligence, or filter for spam and phishing.

Accenture encourages organizations to combine multiple approaches to help ensure robust, secure AI, especially rate limitation, input validation, robust model structuring and adversarial training. Media sources have named various tools to help detect inauthentic videos.^{32,33}

Another watershed technology with the potential to enable massive surveillance and disruption is fifth-generation cellular network technology,

31 “Know Your Threat: AI is the New Attack Surface,” Accenture, 2019. https://www.accenture.com/_acnmedia/Accenture/Redesign-Assets/DotCom/Documents/Global/1/Accenture-Trustworthy-AI-POV-Updated.pdf.

32 “AI and Machine Learning Exploit, Deepfakes, Now Harder to Detect.” PCMAG, May 13, 2019. <https://www.pcmag.com/article/367357/ai-and-machine-learning-exploit-deepfakes-now-harder-to-detect>.

33 “Browser Plug-ins that Spot Fake News Show the Difficulty of Tackling the ‘Information Apocalypse.’” The Verge, August 23, 2018. <https://www.theverge.com/2018/8/23/17383912/fake-news-browser-plugin-ins-ai-information-apocalypse>.

FIVE THREAT FACTORS

or 5G. This technology promises the local processing of data by so-called edge servers and base stations, potentially increasing data speed and efficiency up to a hundredfold over the current cellular data rate; however, this local control means those who control the infrastructure could tamper or spread disinformation to 5G users.³⁴ These issues dovetail into national security concerns, as core multinational disagreements persist around the accountability of 5G infrastructure providers and concerns that the control of equipment and software in 5G infrastructure could enable a small group of companies to conduct information operations against a global population of users. We believe sufficiently advanced AI and Edge systems in control of layer seven application data could dynamically splice deepfakes into streaming content to select users. This technique would likely be used to target VIPs and other decision makers while they consume news media.

HACKTIVISM MASKS

One type of cyber-enabled information operations is hacktivism. Increasingly, Accenture iDefense has found it used by state rather than non-state actors. In some cases it is used to discredit the same organizations that seek to counter disinformation.³⁵ Hacktivism is one of the most visible and colorful areas of the cyberthreat landscape and draws on a wide range of ideological and political inspirations found across the world—hacktivists attempt to advance their political agendas by seeking to damage, degrade or disrupt organizations through interference with or attacks against networked systems.

34 Cybersecurity and Infrastructure Security Agency. "Overview of Risks Introduced by 5G Adoption in the United States." July 31, 2019. https://www.dhs.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf.

35 iDefense Security Intelligence Services. "Account Anonymous Post to CyberGuerrilla the Seventh Disclosure of Internal Documents From the Integrity Initiative." March 28, 2019. IntelGraph reporting.

While conventional, independent hacktivism has been gradually declining in volume and impact since its peak in 2011, intelligence organizations from several countries appear to have sought to direct and support friendly hacktivist actors and exploit false hacktivist personas to carry out information operations. Hacktivists' activity, especially when directed against high-profile targets, tends to generate attention disproportionate to their actual technical impact on the networked systems targeted. Even in the absence of serious technical damage, negative publicity can inflict reputational and financial losses and legal costs, potentially including fines mandated in the European Union by the General Data Protection Regulation (GDPR).³⁶

Accenture iDefense has developed a system for assessing the degree of a hacktivist persona's likely relationship with a government, including factors such as whether the persona's stated ideological goals and activities align with those of a government and whether their aims and targets evolve in response to changing priorities of that government. As an example, some 19 percent of a sample of events covering the 2007 to 2017 period that Accenture iDefense analyzed can be linked to suspected fully state-controlled personas.³⁷

Actors can use false hacktivist personas predominantly to publicize sensitive data obtained from the targeted entity. If the information itself is sufficiently sensitive, hacktivists may "dump" the raw data on a hacktivist messaging site or through social media, but perpetrators may also adjust the data through focused selection or falsification to spin a desired narrative. The attempted manipulation of data leaked from the 2017 campaign of French President François Macron exemplifies the practice of

36 iDefense Security Intelligence Services. "iDefense Explains: How GDPR Could Influence Cyber-criminal Extortion and Data-for-Ransom Attack." May 4, 2018. IntelGraph reporting.

37 iDefense Security Intelligence Services. "State-Sponsored Hacktivism: Attributing CyberInformation Operations Using Hacktivist Personas." May 2, 2018. IntelGraph reporting.

FIVE THREAT FACTORS

adjusting the data to spin a desired narrative.³⁸ Hacktivists often seek to circulate data through social media or mainstream media sites to reach a wider audience.

Case study: The integrity initiative

Between November 5, 2018, and May 7, 2019, the Integrity Initiative³⁹—a UK-based not-for-profit charity describing itself as dedicated to education in good governance—suffered seven information disclosures of information regarding its members, finances, operating goals and recruitment initiatives. An actor using the moniker “Anonymous” posted the leaks to CyberGuerrilla, a leaks website that Russian-speaking hackers use often (see Figure 1).⁴⁰ “Anonymous” constructed a narrative implying that the United Kingdom government used the initiative as an information campaign to undermine Russia by installing pro-Western individuals in prominent positions throughout Europe. Following the disclosures, Russian state media outlets like Sputnik News and RT swiftly circulated the leaks to a wider audience. The SNAKEMACKEREL threat group carried out a similar attack targeting the German Council on Foreign Relations, the Aspen Institute and the German Marshall Fund in late 2018, according to Microsoft research.⁴¹

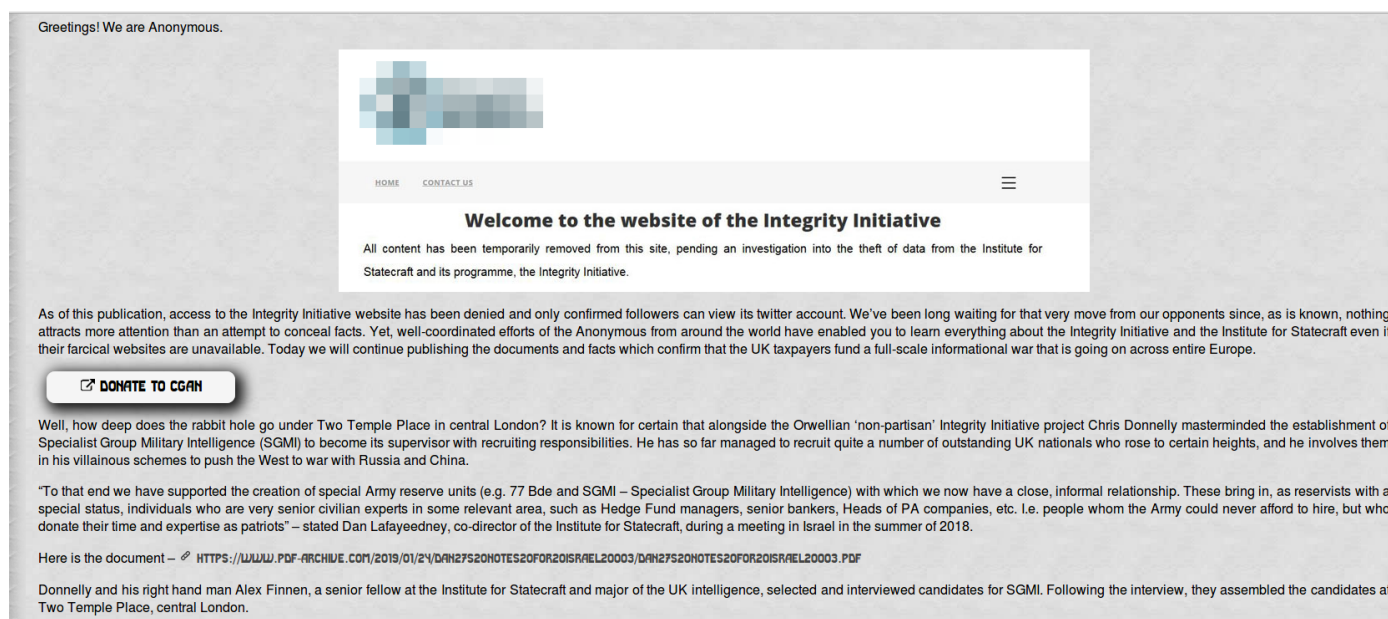
38 iDefense Security Intelligence Services. “Anonymous Yet Familiar: The Use of False Personas by Russian Cyberinformation Operations.” November 27, 2018. IntelGraph reporting.

39 Integrity Initiative. “Statement on Russian media publication of hacked II documents.” November 26, 2018. <https://web.archive.org/web/20181219044330/https://www.integrityinitiative.net/>.

40 iDefense Security Intelligence Services. “Account Anonymous Posts to CyberGuerrilla Fifth Disclosure of Internal Documents from Integrity Initiative.” January 25, 2019. IntelGraph reporting; Anonymous. “The nAbAt a ICC soApbOX ‘Operation Integrity Initiative.’” British informational war against all. Part 5.” January 24, 2019 (Screenshot taken June 5, 2019). CyberGuerrilla. <https://www.cyberguerrilla.org/blog/operation-integrity-initiative-british-informational-war-against-all-part-5/>.

41 Burt, Tom. “New steps to protect Europe from continued cyberthreats.” February 20, 2019. Microsoft. <http://web.archive.org/web/20190220083910/https://blogs.microsoft.com/eupolicy/2019/02/20/accountguard-expands-to-europe/>.

FIGURE 1. Posting by Anonymous on the CyberGuerrilla hacktivist website on January 24, 2019⁴²



Case study: The Yemen CyberArmy

The Yemen CyberArmy (YCA) is the handle of a self-proclaimed Yemeni nationalist hacktivist group that claimed responsibility in 2015 for defacement attacks against Saudi media organizations and a breach of the Saudi Ministry of Foreign Affairs network.⁴³ Accenture iDefense has assessed that the group emerged to retaliate against Saudi Arabia in response to Saudi-led military operations against Shiite Houthi rebels in Yemen. After being quiet for three years, the activist persona allegedly re-emerged in 2019 in a series of defacements of Saudi media and business websites. The defacements included praise for a series of December 2018 Shamoon wiper malware attacks against the energy industry and threats of

42 "The nAbAt an ICC soApboX 'Operation 'Integrity Initiative.'" British informational war against all. Part 5." January 24, 2019 (Screenshot taken June 5, 2019). CyberGuerrilla. <https://www.cyberguerrilla.org/blog/operation-integrity-initiative-british-informational-war-against-all-part-5/>.

43 Dalek, Jakub et al. "Information Controls during Military Operations." October 21, 2015. The Citizen Lab. <https://citizenlab.ca/2015/10/information-controls-military-operations-yemen/>.

FIVE THREAT FACTORS

further disruptive attacks. The exact identity of the re-emerged YCA persona has not been disclosed or otherwise identified.⁴⁴

CHALLENGES OF FIGHTING DISINFORMATION AND OTHER INFORMATION OPERATIONS

Detecting and counteracting the spread of deliberate disinformation can be difficult. In Estonia, a highly digitized country that suffered a massive cyberattack in 2007 and continual disinformation campaigns, volunteer “Baltic elves” monitor the Internet for disinformation, a CyberDefense League of IT specialists shares threat information, and the government has fined or suspended biased media sources.⁴⁵

Attempts to fight disinformation in court are long and expensive, and the perpetrators may never be brought to justice, as in the case of alleged disinformation experts indicted by the team of Special Counsel Robert Mueller.⁴⁶

Finally, threat actors may make deliberate attempts to discredit the very investigators who are uncovering disinformation, as in the case of the Integrity Initiative, described above.

44 iDefense Security Intelligence Services. “Yemen CyberArmy Returns with Defacements Referencing Shamoan Wiper Attacks.” January 9, 2019. IntelGraph reporting.

45 “Countries and Regions: Baltic States.” Accessed June 19, 2019. EU Versus Disinformation. <https://euvsdisinfo.eu/reading-list/countries/> ; Prague Manual. April 30, 2018. <https://www.europeanvalues.net/wp-content/uploads/2018/07/Prague-Manual.pdf>.

46 Jurecic, Quinta. “Where in the World Is Elena Khusyaynova?” October 26, 2018. Lawfare. <https://www.lawfareblog.com/where-world-elena-khusyaynova>.

GEOPOLITICAL EVENTS COULD ENGENDER DISRUPTIVE AND EXPLOITATIVE CYBERTHREAT ACTIVITY

Based on past behavior, cyberthreat activity may accompany the key scheduled and unscheduled events noted in Figure 2 and occurring between mid-2019 and mid-2020.

FIGURE 2. Key events of 2019 and 2020 that may attract cyberthreat activity
(table footnotes continued on page 31.)

Date	Event	Past activity
October 2019	Brexit deadline	Profiting from Brexit panic, SNAKEMACKEREL has delivered malware using Brexit-themed lure documents. Since before the 2016 Brexit referendum, hackers have sought to sow confusion and panic around the Brexit issue. ⁴⁷
July–August 2020	US political conventions	If consistent with past behavior, SNAKEMACKEREL is likely to attempt information theft, disinformation operations and the weaponization of election-related documents. SNAKEMACKEREL, JACKMACKEREL and MUDCARP will almost certainly also attempt cyberespionage against United States political candidates and parties. ⁴⁸

47 Yip, Michael. “Snakemackerel delivers Zekapab malware.” November 29, 2018. Accenture. <https://www.accenture.com/us-en/blogs/blogs-snakemackerel-delivers-zekapab-malware>; iDefense Security Intelligence Services. “Profiting from Panic: Brexit and Potential Russian Threat Activity Affecting Financial Institutions.” March 8, 2019. IntelGraph reporting.

48 iDefense Security Intelligence Services. “Aggressive Defensiveness: Russian Information Operations against the US Political System.” January 7, 2017. IntelGraph reporting; iDefense Security Intelligence Services. “Anonymous Yet Familiar: The Use of False Personas by Russian Cyberinformation Operations.” November 27, 2018. IntelGraph reporting; iDefense Security Intelligence Services. “US Indictment Casts Light on Russian Strategies in 2016 US Election and Future Threats.” July 18, 2018. IntelGraph reporting; iDefense Security Intelligence Services. “Iron Friends: China Hacking Cambodia 2018 Election Entities.” July 19, 2018. IntelGraph reporting.

FIVE THREAT FACTORS

FIGURE 2 Key events of 2019 and 2020 that may attract cyberthreat activity (cont'd.)

Date	Event	Past activity
August 2020	2020 Tokyo Summer Olympics	Threat actors have carried out hacktivism campaigns against the World Anti-Doping Agency (WADA), and the cyberthreat group behind Olympic Destroyer malware conducted significant operations against the 2018 PyeongChang Winter Olympics. ⁴⁹
November 21–22, 2020	G20 Summit meetings	G20 Summit meetings are popular targets for hacktivist campaigns, including those that conduct denial-of-service attacks, and have also attracted the use of regionally specific techniques, such as the exploitation of vulnerabilities in Korean-language Hangeul word processor tools. Threat groups have also used the G20 summit as a lure for phishing campaigns targeting organizations unrelated to the meeting. ⁵⁰
September 15–30, 2020	UN General Assembly 75th Session	The UN is a frequent hacktivist and cyberespionage target, especially when hosting large member events such as General Assembly gatherings. ⁵¹
Unscheduled	Global defense and security conferences	Global military conferences in general are likely to be preferred targets of state-sponsored cyberespionage activity. Accenture iDefense expects SNAKEMACKEREL in particular to target attendees of defense and security conferences in 2020 such as the Underwater Defence & Security Conference, using malicious document attachments and possibly other means. ⁵²
Unscheduled	NATO and EU enlargement plans	In 2017, SNAKEMACKEREL targeted Montenegro government officials prior to Montenegro's accession to NATO. In December 2018, the same group targeted North Macedonian officials during that country's NATO admission. North Macedonia's NATO accession is expected to become official in 2020. ⁵³ Other countries aspiring to join or discussing NATO membership include Bosnia and Herzegovina, Georgia, Ukraine, Sweden and Finland. Countries aspiring to join the European Union include Serbia, Montenegro and Turkey.
Unscheduled	Sanctions declarations	Threat groups such as SNAKEMACKEREL, Syrian Electronic Army and Endless Mayfly have responded to sanctions declarations with campaigns of disinformation and access attempts against selected government targets. ⁵⁴

Occasionally, cyberthreat actors—ranging from hacktivists to state-sponsored actors—conduct operations on significant dates or the anniversaries of significant events. Three key anniversaries occur in the latter part of 2019 that may serve as catalysts for such activity:

- October 1, 1949: Proclamation of the People’s Republic of China (70 years)
- November 4, 1979: Seizure of United States hostages in Iran (40 years)
- November 9, 1989: Fall of the Berlin Wall (30 years)

49 iDefense Security Intelligence Services. “Cyber-threats against 2018 PyeongChang Winter Olympics.” February 7, 2019. IntelGraph reporting; iDefense Security Intelligence Services. “Secure Olympics Tokyo 2020: Is Japan Prepared for the Games?” April 29, 2019. IntelGraph reporting.

50 iDefense Security Intelligence Services. “Technical Analysis of HWP-based Malware Targeting Current Events.” June 21, 2018. IntelGraph reporting; iDefense Security Intelligence Services. “Hacktivist Activity for Sept. 1-8, 2016.” September 9, 2016. IntelGraph reporting; iDefense Security Intelligence Services. “Phishing Attack Targeting Tibetan Organizations uses 2014 G20 Summit to Deliver MNkit and Lurk Malware.” November 13, 2014. IntelGraph reporting.

51 iDefense Security Intelligence Services. “Hacktivist Campaign OpStopTheUN Claims to Carry Out a Series of DDoS Attacks Against United Nations Websites.” September 13, 2018. IntelGraph reporting.

52 iDefense Security Intelligence Services. “SNAKEMACKEREL Campaign Likely Targeting NATO Members, Defense and Military Outlets.” December 21, 2018. IntelGraph reporting.

53 iDefense Security Intelligence Services. “SNAKEMACKEREL Campaign Likely Targeting NATO Members, Defense and Military Outlets.” December 21, 2018. IntelGraph reporting.

54 Lim, Gabrielle, et al. “Burned After Reading Endless Mayfly’s Ephemeral Disinformation Campaign.” May 14, 2019. CitizenLab. <https://citizenlab.ca/2019/05/burned-after-reading-endless-mayflys-ephemeral-disinformation-campaign/>; iDefense Security Intelligence Services. “GRU Unmasking Opens New Phase of CyberCold War.” November 17, 2018. IntelGraph reporting; iDefense Security Intelligence Services. “Cultural and Political Flashpoints Could Drive Cyberoperations in Entertainment Industry.” March 14, 2019. IntelGraph reporting.

FIVE THREAT FACTORS

CYBERTHREAT USES OF GLOBAL EVENTS: OPPORTUNISM AND PARTICIPATION

Every significantly impactful or highly visible event offers an occasion for cyberthreat actors to emerge, seeking to capitalize on the access a target affords or the scale of a potential cybercrime profit. Cyberthreat adversaries may use those events opportunistically, participate in them, or both.

As opportunists, threat actors can take advantage of the impact or visibility of events by using several techniques, such as crafting phishing lures with distracting e-mail subject lines related to recent events, setting up counterfeit websites and misleading e-mail sender domains, and turning poorly defended event websites into watering holes, to name just a few examples. Whether criminally or financially motivated, threat actors may seek to take advantage of legal changes, price swings or international geopolitical maneuvering. They may use dramatic headlines about world events to lure victims into activating malicious documents. Any current event can present an opportunity for exploitation.

As participants, threat actors may seek to influence events themselves. Governments may use cyberthreat activity to pursue strategic goals in various ways: using espionage to steal technology benefiting national industries and military programs or to gain visibility into or leverage over political decision making in a target country; stealing money to fund a regime or movement; conducting cyber-enabled information operations to influence opinion or decision making; and engaging in disruptive or destructive activities designed to weaken or demoralize an adversary and demonstrate a credible threat to deter adversaries from belligerent behavior.

A COST-BENEFIT PROPOSITION

Political analysis helps put cyberthreat capabilities into perspective, as they are one of many tools a state or criminal may rely on to advance their interests. It is understood that states weigh the perceived benefits of computer network exploitation or attack against its risks and costs in comparison to military, diplomatic or economic options while criminal actors operate within legal and political contexts and may demonstrate patriotism or provide expertise and services to government officials to reduce the risk of punishment for their activities. Evaluation of these generally consistent influences can help assess future behavior.

Evaluating political factors, Accenture iDefense assessed⁵⁵ in early April 2019 that although Ukraine had withstood geopolitical cyberthreat activity in the past, a country hostile to Ukraine would likely refrain from blatant attempts to disrupt or alter the results of its 2019 presidential election, as an adversary country could pursue its broader goals in other, less-costly ways. As expected, at the end of April, Ukrainian authorities announced there had been no major cyberattacks against its elections.⁵⁶ Similarly, countries subject to heavy economic sanctions or harsh tariffs from other countries must weigh the potential benefits of retaliation, including via cyberthreat means, against the prospect that retaliation may alienate sympathetic countries.⁵⁷

Drawing on an analysis of possible motivations for conducting disruptive cyberattacks, Accenture iDefense estimated correctly that political

55 iDefense Security Intelligence Services. "In Long Ukrainian Election Season, Russia May Pursue Strategic Goals without Major Cyberthreat Operations." April 5, 2019. IntelGraph reporting.

56 "National Police: No cyberattacks on CEC systems recorded during second round of elections." April 24, 2019. Ukrinform. <https://www.ukrinform.net/rubric-elections/2688206-national-police-no-cyberattacks-on-cec-systems-recorded-during-second-round-of-elections.html>.

57 iDefense Security Intelligence Services. "US-Iran Tensions Mount on JCPOA Withdrawal Anniversary: Cyberespionage Likely; Cyberattack Dependent on Further Escalation." May 8, 2019. IntelGraph reporting.

FIVE THREAT FACTORS

tensions surrounding the 2018 PyeongChang Winter Olympics would motivate cyberthreat actors to disrupt the events, whereas threat actors may have much less incentive to disrupt the World Cup tournament.⁵⁸ As the 2020 Tokyo Summer Olympics approach, international tensions could incentivize a variety of political actors to try disrupting the games. Those actors and incentives should become more apparent as the games draw closer and political events evolve. In addition, the 2020 Olympics and other major international events like the 2019 Rugby World Cup could provide opportunities for ticket fraud and other financially motivated cyberthreat activity that usually accompanies such events.⁵⁹

Political analysis of any sort is not a foolproof predictive tool; however, an understanding of the environments in which cyberthreat actors operate, the pressures and incentives that motivate them, the costs and benefits they may calculate, and the nature of their targeting, can help assess the likelihood and confidence of potential cyberthreat action. As events unfold, the comparison of actual results against predictions can further tune estimated calculations.

USE OF CURRENT EVENTS AS LURES

In 2019, Accenture iDefense analysts observed numerous cyberthreat groups leveraging global and regional current events (including political, military and social) as themes for content in spear phishing lure documents, which according to the MITRE ATT&CK framework are used as an Initial Access tactic to gain a foothold into targeted networks.⁶⁰

58 iDefense Security Intelligence Services. "Campaign Targets E-mail Addresses Associated with 2018 PyeongChang Olympics." January 10, 2018. IntelGraph reporting; iDefense Security Intelligence Services. "Cyber-threats against 2018 PyeongChang Winter Olympics." February 7, 2018. IntelGraph reporting.

59 iDefense Security Intelligence Services. "iDefense Explains: Potential Cyber-threats to 2018 FIFA World Cup." May 31, 2018. IntelGraph reporting.

60 "Initial Access." June 5, 2019. MITRE. <https://attack.mitre.org/tactics/TA0001/>.

The SNAKEMACKEREL (also known as APT28) threat group has consistently used geopolitical, military and global events themes in its spear phishing attacks, many of which have targeted NATO members or affiliates.⁶¹

Figure 3 provides a small list of examples dating back to 2017 that illustrate largely military event types.

FIGURE 3. SNAKEMACKEREL military-theme phishing lures

Date	Lure Document Name (modeled event)	Apparent Target	TTPs
December 2018	"UDS 2019 Current Agenda.doc" (Underwater Defence & Security conference)	Entity likely in Macedonia ⁶²	Dropped Seduploader custom malware implant
March 2018	"Defence & Security 2018 Conference Agenda.docx" (Underwater Defence & Security conference)	Entity likely in Montenegro ⁶³	Used Dealer's Choice, an Adobe Flash exploit platform
November 2018	"Brexit 15.11.2018.docx" ⁶⁴	Entity likely in Czech Republic	Exploited Microsoft Office vulnerability (CVE-2017-0199) to drop Zekapab custom malware implant
October 2017	"Conference_on_Cyber_Conflict.doc" (International Conference on CyberConflict US [CyCon US]) ⁶⁵	Entity likely in Romania	Dropped SedUploader

61 "Reckless campaign of cyberattacks by Russian military intelligence service exposed." October 3, 2018. NCSC. <https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed>.

62 Brady, Matthew and Kimberly Bucholz. "SNAKEMACKEREL Delivers SedUploader Malware." February 13, 2019. Accenture iDefense. <https://www.accenture.com/us-en/blogs/blogs-snakemackerel-delivers-seduploader-malware>.

63 Falcone, Robert. "Sofacy Uses DealersChoice to Target European Government Agency." March 15, 2018. Palo Alto Networks. <https://unit42.paloaltonetworks.com/unit42-sofacy-uses-dealerschoice-target-european-government-agency/>.

64 Yip, Michael. "SNAKEMACKEREL Delivers Zekapab Malware." November 29, 2018. Accenture iDefense. <https://www.accenture.com/us-en/blogs/blogs-snakemackerel-delivers-zekapab-malware>.

65 iDefense Security Intelligence Services. "CyberConflict Conference (CyCon) 2017 CFP Used as Lure for SEDUPLOADER Delivery." October 23, 2017. IntelGraph reporting.

FIVE THREAT FACTORS

Accenture iDefense analysts estimate that SNAKEMACKEREL actors could continue to leverage notable political and military events as themes in future spear phishing lure document content and almost certainly with regard to upcoming military and defense conferences.

The WINTERFLOUNDER cyberthreat group (also known as Gamaredon Group⁶⁶) has also consistently used geopolitical and military themes as lures against entities that may be government and public sector bodies based in Ukraine. Accenture iDefense has found two lure documents attached to spear phishing e-mails that WINTERFLOUNDER actors sent in April 2019; the group used both along with the Pterodo custom backdoor to target unknown entities likely based in Ukraine. One lure bears similarity to other WINTERFLOUNDER phishing activity focused on the Ukraine elections.⁶⁷

66 Reichel, Dominik and Anthony Kasza. "The Gamaredon Group Toolset Evolution." February 27, 2017. Palo Alto Networks. <https://unit42.paloaltonetworks.com/unit-42-title-gamaredon-group-toolset-evolution/>.

67 iDefense Security Intelligence Services. "WINTERFLOUNDER Campaign Lure Pegged to Ukrainian Election Scandal." April 30, 2019. IntelGraph reporting.

FIGURE 4. WINTERFLOUNDER phishing lure describing purportedly intercepted radio communications (original Accenture iDefense analysis from a WINTERFLOUNDER malware sample)⁶⁸

Розвідувальні зведення (частина II) РЕО на сході України станом на 21:00 11 квітня ц.р.		Таємно Прим. № 1
3 аналізу матеріалів радіоперехоплення встановлено:		
Оцінка	Зміст	Підрозділ, що здобув інформацію
Воєнна сфера:		
<i>1 АК та 2 АК</i>		
	07:51:31 24 січня ц.р.	
24 січня ц.р. на територіях т.зв. ЛНР та ДНР продовжується командно-штабне навчання з органами управління та силами Єдиної державної системи попередження, та ліквідації надзвичайних ситуацій (25 січня ц.р – завершення). В рамках навчань відпрацьовувались питання охороні оборонно критичних об'єктів інфраструктури, зокрема електричних підстанцій. На 25 січня ц.р. в ЛУТУТИНЕ в рамках навчань заплановано проведення показових заходів. З 20:00 24 січня ц.р. до 07:00 25 січня ц.р. введено оперативну паузу.	-Алло -Я не знаю, я со вторника на казарме, у нас сейчас учения -Да -Я сейчас на выезде и со вторника на казарму перевели, по объектам покидали, кто там я не знаю, дежурит -Тут х...й поймешь кто где дежурит, тех сменили, тех убрали, ну, такое вводное поступает мы меняемся -Я со вторника, хр...н когда нас опустят, как ушел в 8 утра и все -Да ничего страшного -Добро, все	Ман. гр. “Аквепарк”, “Посейдон”, “Карат”, “Легіон-2”, “Непгун”
	10:15:47 24 січня ц.р.	
	- Учения б...я устроили, я ху...ю. Средилюдей, среди хат. Охраняют они б...я периметр. - Очень стратегически, металлолом б...я. - Я считаю что практика у них не правильная. По периметру там, в серой зоне. - Не надо меня оберегать, в моем дворе с пушкой. - Ну, ладно, это мое мнение.	

DESTRUCTIVE MALWARE AND BACKDOORING: A DAMOCLES SWORD OVER CRITICAL INFRASTRUCTURE

The Ukrainian blackouts of 2015 and 2016 and the devastating Petya.A (NotPetya) attack of June 2017 showed the power of destructive and disruptive malware.⁶⁹ Several countries’ intelligence services reported that cyberthreat actors from adversary countries have pre-positioned backdoors throughout large parts of the global financial, physical and Internet infrastructure, with these backdoors potentially capable of being triggered in a destructive or disruptive attack. A January 2019 assessment

68 iDefense Security Intelligence Services. “WINTERFLOUNDER Campaign Lure Pegged to Ukrainian Election Scandal.” April 30, 2019. IntelGraph reporting.

69 iDefense Security Intelligence Services. “Cyber Threatscape Report.” August, 2017. https://www.accenture.com/t20170930t063734z_w_/cr-en/_acnmedia/pdf-62/accenture-cyber-threat-scape-report-us.pdf.

FIVE THREAT FACTORS

by the United States Office of the Director of National Intelligence (ODNI), for example, named countries it deems capable of using cyberattacks to disrupt United States natural gas pipelines for days or weeks and electrical distribution networks for hours. The capabilities ODNI described do not necessarily need to be used in the foreseeable future. The mere awareness of their existence influences policymakers to carefully consider the use of offensive or even retaliatory cyberattacks. In fact, turning off lights in a large country or causing a dam to fail may cross unclear lines of what actions are acts of war, thus inviting retaliation. But the simple threat that an adversary could unleash these outcomes could have a deterrent effect.⁷⁰

SUMMARY

Accenture iDefense expects global businesses to find themselves in the crosshairs as geopolitical tensions persist. As cyberthreat actors take advantage of high-profile global events and seek to influence mass opinion, the world can expect these actors to not only sustain current levels of activity but also to take advantage of new capabilities as new technologies enable more-sophisticated threat TTPs. Geopolitical analysis and a strategic-level understanding of the events that motivate cyberthreats to action can help businesses manage known threats and allocate resources in anticipation of emerging threats.

70 "DNI COATS OPENING STATEMENT ON THE 2019 WORLDWIDE THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY." January 29, 2019. US Office of the Director of National Intelligence. <https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/1949-dni-coats-opening-statement-on-the-2019-worldwide-threat-assessment-of-the-us-intelligence-community>.

2 CYBERCRIMINALS ADAPT, HUSTLE, DIVERSIFY AND ARE LOOKING MORE LIKE STATES

OVERVIEW

Conventional cybercrime and financially motivated targeted attacks remain highly active, despite several high-profile law enforcement takedowns in 2018;⁷¹ however, Accenture iDefense has observed several significant changes in cybercrime that analysts have broken down into four distinct sections: conventional cybercrime operations, localized cybercrime, targeted attacks and “hack ‘n’ hustle.”

TOP-LINE ASSESSMENT: KEY JUDGMENTS

- Conventional cybercrime operations continued to be active during 2019, with actors sharing document builders and malware for use in crimeware campaigns and targeted intrusions.⁷² But we can observe a new level of resilience and maturity in organized cybercrime as crimeware groups shift their operating model from one of open partnerships on underground forums to one of close-knit syndicates due to high-profile law enforcement actions.

71 Greenberg, Andy. “Feds Take Down A Half-Billion Dollar Cybercrime Forum After 7 Years Online.” February 7, 2018. Wired. <https://www.wired.com/story/infraud-feds-takedown-cybercrime/>; Burgess, Matt. “Inside the takedown of the alleged €1bn cyber bank robber.” April 4, 2018. Wired UK. <https://www.wired.co.uk/article/carbanak-gang-malware-arrest-cybercrime-bank-robbery-statistics>. US Department of Justice. “Two International Cybercriminal Rings Dismantled and Eight Defendants Indicted for Causing Tens of Millions of Dollars in Losses in Digital Advertising Fraud.” November 27, 2018. <https://www.justice.gov/usao-edny/pr/two-international-cybercriminal-rings-dismantled-and-eight-defendants-indicted-causing>.

72 Nir, Sivan. “Threadkit, Formbook Exploit Old Microsoft Vulnerability.” February 6, 2019. Skybox Security. <https://blog.skyboxsecurity.com/formbook-threadkit/>.

FIVE THREAT FACTORS

- Localized underground economies continue to emerge and grow in non-English-speaking countries such as China and Brazil, which tend to target their domestic populations due to familiarity with their own societies, cultures and environments.
- An attack trend known as “big game hunting”, where cybercriminal threat actors and groups conduct targeted intrusions for financial gain, is on the increase. It can include the use of a wide range of bespoke malware and commodity “crimeware” available for download or purchase from underground forums and marketplaces and frequently uses legitimate penetration testing tools.
- Network access can be used to carry out a range of malicious activities, and there has been a marked increase in the sale of remote access to compromised networks on underground forums and marketplaces. The number of incidents where financially motivated threat actors employ commodity malware to conduct intrusions for financial gain is also on the rise.

SECURE SYNDICATES: A NEW MODEL FOR CYBERCRIME OPERATIONS

Crimeware spam campaigns continued to be active in 2018 and 2019, with Emotet, AZORult, Loki Bot, Pony, NanoCore and Nocturnal among the most commonly observed types of crimeware. The most-common type of spam campaign attachments used to deliver malware remain Microsoft Office documents weaponized with malicious macros, closely followed by rich-text format (RTF) documents with embedded object linking and embedding (OLE) objects created to exploit vulnerabilities such as the CVE-2017-11882 vulnerability. Exploit kit activity over the last 12 months came primarily from the Fallout, RIG and GrandSoft exploit kits.⁷³ Attackers have used exploit

⁷³ Segura, Jérôme. “Exploit kits: winter 2019 review.” January 18, 2019. Malwarebytes. <https://blog.malwarebytes.com/threat-analysis/2019/02/exploit-kits-winter-2019-review/>.

kits such as Magnitude, Underminer and GreenFlash Sundown to deliver ransomware primarily to Asian countries.⁷⁴

In addition to the conventional waves of crimeware spam campaigns, Accenture iDefense analysts have observed the shared use of commodity document builders, such as ThreadKit, and script-based malware, such as More_Eggs, among conventional crimeware campaigns and targeted attack groups, such as Cobalt Group, making attribution more difficult and further highlighting the intricate relationships between actors in the underground economy.

Accenture iDefense analysts assess that conventional crimeware campaigns could continue to be active. However, given the recent high-profile takedowns of popular underground communities such as Alphabay,⁷⁵ Hansa⁷⁶ and, more recently, Wall Street,⁷⁷ the operating model of crimeware groups may continue to shift from that of loosely connected affiliates or partnerships toward that of more closely knit syndicates.

REGIONAL CYBERCRIME: EXPLOITATION OF LOCALIZED TECHNOLOGIES

Accenture iDefense analysts observe that cybercrime scenes differ from region to region depending on each region's status of technological development, Internet culture, and social, political, legal and economic environment. This difference has been growing stronger since 2018. As targeting domestically provides the advantage of familiarity with the local

74 Ibid.

75 "AlphaBay Takedown." July 20, 2017. FBI. <https://www.fbi.gov/news/stories/alphabay-takedown>.

76 Sheridan, Kelly. "Dark Web Marketplaces Dissolve Post-AlphaBay, Hansa Takedown." June 5, 2019. Dark Reading. <https://www.darkreading.com/threat-intelligence/dark-web-marketplaces-dissolve-post-alphabay-hansa-takedown/d/d-id/1331971>.

77 Greenberg, Andy. "Feds Dismantled the Dark-Web Drug Trade—but It's Already Rebuilding." May 9, 2019. Wired. <https://www.wired.com/story/dark-web-drug-takedowns-deepdotweb-rebound/>.

FIVE THREAT FACTORS

environment, regional cybercriminals often choose to do so and seek to exploit popular, localized technologies, such as online payment platforms or communication tools, for financial gains.

In emerging economies such as China,⁷⁸ current national economic development strategies highly encourage technology-oriented innovation, leading to a sharp rise in the development, adoption and exportation of advanced technologies such as the Internet of Things (IoT), artificial intelligence (AI), robotics and smart cities, all of which play an important role in driving economic growth, though the legal regulations of such technologies often lag behind.⁷⁹ However, the hasty adoption of emerging but otherwise immature technology, such as the development of cryptocurrency, mobile payments and Fintech, has led to more opportunities for cybercriminals to exploit for financial gain.⁸⁰

Cybercriminals often develop equivalent “black technology”⁸¹ to explore new technologies to obtain illicit profits. For example, in China, digital financial fraud that utilizes Fintech is a growing trend in 2018.⁸² This kind of financial fraud combines big data and AI technologies to analyze stolen personally identifiable information (PII) to target victims with tailored fraud scenarios, which increases attack success rates and the efficiency of fraud activities and lowers the costs of conducting fraudulent acts.⁸³

78 iDefense Security Intelligence Services. “The Other Booming Industry: Characteristics and Global Effect of the Chinese Online Underground Economy.” July 14, 2018. IntelGraph reporting.

79 iDefense Security Intelligence Services. “Cat and Mouse Game: China’s Cryptocurrency Regulations and Cryptocurrency Cybercrime.” December 5, 2018. IntelGraph reporting.

80 Barret, Brian. “Hack Brief: Hackers Stole \$40 Million From Binance Cryptocurrency Exchange.” May 8, 2019. Wired. <https://www.wired.com/story/hack-binance-cryptocurrency-exchange/>.

81 “What is black about ‘black technology’?” (“黑科技”究竟是什么?). May 30, 2018. Xinhua Net. http://www.xinhuanet.com/politics/2018-05/30/c_1122909806.htm.

82 “数字金融反欺诈-洞察与攻略” (“Digital Finance Anti-fraud – Observation and Strategy”). November 2018. Tencent Financial Security & China Academy of Information and Communication Technology (CAICT). <http://www.caict.ac.cn/kxyj/qwfb/bps/201811/P020181127615657923423.pdf>.

83 Ibid.

BIG GAME HUNTING: MORE TARGETED ATTACKS

Accenture iDefense analysts have observed a significant increase in the past two years in cybercriminal threat actors and groups conducting targeted intrusions for financial gain. This attack trend, which is sometimes referred to as “big game hunting,” can include the use of a wide range of bespoke malware and commodity “crimeware” malware available for download or purchase from underground forums and marketplaces, including banking Trojans, information stealers, keyloggers and loaders. Cybercriminal threat actors carrying out targeted intrusions also frequently use legitimate penetration testing tools, such as Metasploit, Cobalt Strike, PowerShell Empire (PSE), Meterpreter and Mimikatz. Accenture iDefense analysts have continued to observe activities from targeted attacks threat groups, with FIN7, Cobalt Group and Contract Crew (also known as Silence) being the most prominent and active such groups.

FIN7

FIN7⁸⁴ is an advanced cybercriminal group that specializes in targeted attacks against organizations in the retail, hospitality and financial services sectors. FIN7 is highly organized and vertically structured, operating under the front of a legitimate penetration testing company named Combi Security. FIN7 typically conducts spear-phishing attacks using malicious document attachments against selected individuals in targeted organizations. Malware delivered in these attacks has included the Carbanak implant and bespoke script-based implants such as HALFBAKED, Bateleur and DNSMessenger. In addition, FIN7 has used a wide range of penetration testing tools such as Meterpreter, Cobalt Strike and Mimikatz for initial access and post-exploitation activities. Other bespoke malware that Accenture iDefense analysts have observed include 7Logger, Vampire

84 iDefense Security Intelligence Services. “FIN7.” January 16, 2019. IntelGraph reporting.

FIVE THREAT FACTORS

Loader and a memory-scraping malware known as Vampire Dumper, all of which were designed to be used on point-of-sale (PoS) infrastructure. The group focuses heavily on carrying out targeted attacks to exfiltrate datasets of value for resale, especially payment card industry (PCI) data.

During the past 12 months, Accenture iDefense analysts have observed that despite the indictments that the United States Department of Justice issued in August 2018, FIN7 continues to be active. Although still active, there have been significant changes in the group's TTPs, including the use of a new script-based backdoor called GUDWIN⁸⁵ (also known as GRIFFON), which resembles a simplified version of the Bateleur backdoor, as well the use of legitimate documents with embedded images from remote sources to identify individuals who are likely to open malicious documents. The changes indicate that the group is trying to reduce its footprint on targeted networks by increasing the precision of its targeting. Based on the telemetry from Accenture iDefense and partners during the past 12 months, Accenture iDefense assesses with moderate confidence that FIN7's primary focus remains on the retail and hospitality sectors.⁸⁶

Cobalt Group

Cobalt Group⁸⁷ is an advanced financially motivated threat group that has been active since as early as mid-2016. Accenture iDefense analysts have observed several of the group's distinctive TTPs, including the preference and ability to create new first-stage malware families and the reuse of specific mail servers in multiple campaigns. The group also exhibits a preference for using Cobalt Strike as a main payload to establish access to compromised machines and entrench on target networks.

85 iDefense Security Intelligence Services. "GUDWIN." September 3, 2018. IntelGraph reporting.

86 iDefense Security Intelligence Services. "Targeted Threats against Financial Services: A Primer." December 7, 2018. IntelGraph reporting.

87 Defense Security Intelligence Services. "Cobalt Group." January 4, 2019. IntelGraph reporting.

Activity during late 2018 and early 2019 has mostly revolved around the CobInt (also known as COOLPANTS) malware family. This group primarily focuses on targeting financial services in the United States, Europe and Commonwealth of Independent States (CIS) countries, including Russia. Cobalt Group displays a strong preference for delivering malware via spear phishing with the use of malicious Office documents that are similar those that FIN7 uses. Accenture iDefense analysts have observed the use of Microsoft Word Intruder and ThreadKit builders to generate malicious documents. As of late 2018 and into 2019, the group is using the Word macro-based download kit referred by Accenture iDefense analysts as Little Pig to download the CobInt backdoor malware, which enables deeper reconnaissance and lateral movement, as the malware has the ability to download other malware components. Despite the arrests of three individuals associated with the group, activity continues into 2019.

Contract Crew

Contract Crew⁸⁸ is a financially motivated threat group that targets financial institutions with a focus on automated teller machines (ATMs) in the CIS region since at least 2016. As of late 2018 and early 2019, Contract Crew has reportedly expanded its targeting beyond Russia and Commonwealth of Independent States (CIS) countries to include European and Middle Eastern countries. Contract Crew exhibits a strong preference for using spear-phishing e-mails to deliver malicious files to intended targets, with those e-mails subsequently dropping first-stage malware on a targeted system. The types of malicious files delivered include JavaScript downloaders, VBScript downloaders disguised as OLE-embedded objects in DOCX documents, documents weaponized with CVE-2015-2545 or CVE-2017-0199 exploits, CHM files embedded in DOC files, RAR or ZIP archives

88 iDefense Security Intelligence Services. "Contract Crew." April 4, 2019. IntelGraph reporting.

FIVE THREAT FACTORS

containing additional nested file types, and Windows Shortcut file (.lnk) downloaders. Exploitation via any of these methods would then trigger the download and execution of the Silence Downloader, which would subsequently download the Silence backdoor's main module. The group also has custom proxy toolsets that can be deployed to enable access to harder-to-reach networks, such as those inside financial institutions. Contract Crew uses multiple stages of execution to include the use of legitimate system utilities to increase obfuscation and dwell time. Activities from Contract Crew have been observed to continue well into 2019.

NETWORK ACCESS FOR SALE

Over the course of the last two to three years, Accenture iDefense has observed a marked increase in the sale of remote access to compromised networks on underground forums and marketplaces, as well as an increase in the number of incidents in which financially motivated threat actors employ commodity malware to conduct intrusions for financial gain. Actors can use network access to carry out an array of malicious activities, including malware distribution, theft of PII, exfiltration of payment card data and more, although how to use a network where an actor has purchased access is ultimately up to that buyer. Since the beginning of 2019, Accenture iDefense has observed several high-profile threat groups engaged in the buying and selling of network access in the underground. Such examples include "Nikolay," a group specializing in the sale of access to numerous corporate networks, and "GandCrab," an enterprise distributing ransomware through an affiliate program it operates.

Nikolay is a threat group that Accenture iDefense observes and monitors that maintains a presence on several Russian- and English-language underground forums, using a number of aliases across these underground forums. Nikolay specializes in selling access to compromised networks

across multiple verticals. Accenture iDefense analysts assess with moderate confidence that Nikolay relies on compromised RDP connections to obtain and sell corporate network access (see Figure 5). Analysis of forum postings suggests Nikolay took a hiatus between December 2018 and March 2019, during which the group indicated that its RDP exploits were “no longer working,” thus rendering the group’s primary tool obsolete. Since returning, the group has updated its sales focus by disclosing the number of machines to which they sell access—something they did not do initially. Accenture iDefense notes that this disclosure was likely made to capitalize on the ongoing trend in which actors conduct ransomware attacks through RDP connections.

FIGURE 5. Advertisement from Nikolay selling RDP access to franchise retail operator (sensitive details redacted)

The screenshot displays a Malicious Event page with the following details:

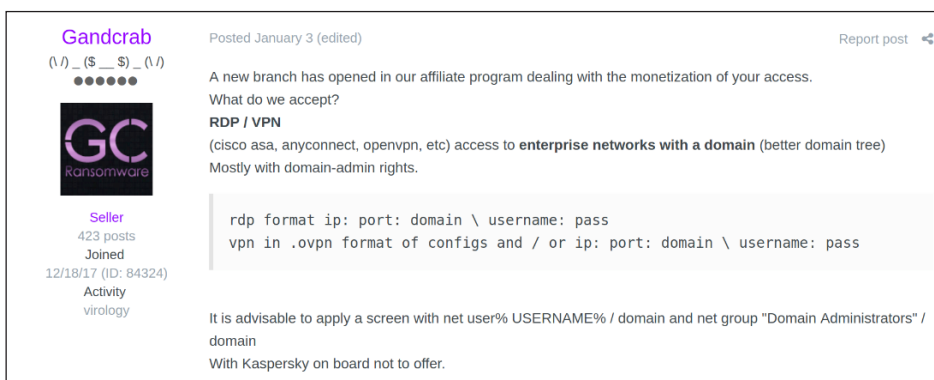
- SEVERITY:** MEDIUM
- THREAT TYPE[S]:** Cyber Crime
- Created On:** Jul 19, 2018 11:30 AM BST by iDefense Staff
- Last Published:** Jul 19, 2018 2:24 PM BST by iDefense Staff
- 80 RELATIONSHIPS**
- Description:** On July 19 2018, an actor using the handle Nikolay posted an advertisement on the Russian-language criminal forum [redacted] for access to the corporate network of a large retail franchise operator, including access to the franchised shops and approximately 20,000 hosts on the network. The actor priced the access at 7,000 USD via escrow and indicated they could be contacted via Jabber at [redacted] or private message on the forum. iDefense analysts assess with moderate confidence that the organization is [redacted] franchise retail operator with locations in the MENA, Eastern Europe and Central Asia regions. Major retail and food services brands franchised by the operator include: [redacted list].
- My Ratings:**
 - Relevance: ☆ ☆ ☆ ☆ ☆
 - Timely: ☆ ☆ ☆ ☆ ☆
 - Useful: ☆ ☆ ☆ ☆ ☆
- Node Graph:** A graph showing relationships between entities: Verticals (2), Target 214 (2), Account Nikolay Adm... (80), and Nikolay (Account) (74).
- July 19 2018 Update:** iDefense analysts have been in communication with the actor via Jabber and assess with high confidence that [redacted] is the victim organization being targeted. The actor claims to have RDP access to the company's internal network with access to 4,400 POS [redacted]

FIVE THREAT FACTORS

Since March 2018, the group using the alias GandCrab on a popular Russian-language underground forum has distributed ransomware of the same name through an affiliate program model advertised on that forum. This model involves the group recruiting partners that are paid to distribute the ransomware through means such as spam, exploit kits and targeted attacks. Upon successful distribution, affiliates will receive 60 percent to 80 percent of all ransom payments, while GandCrab will pocket the remaining 20 percent to 40 percent.⁸⁹

In January 2019, Accenture iDefense observed GandCrab posted a discussion thread in which the group offered to monetize remote access to compromised corporate networks (see Figure 6). The group expressed interest in gaining entry to corporate networks through RDP or VPN software such as Cisco ASA, AnyConnect or OpenVPN. In the event that forum members can provide GandCrab with entry, the group will try to deploy its ransomware onto the victim network and split all proceeds 50–50 with the access providers. In the discussion thread, the group states that it will utilize licensed versions of popular penetration testing tools such as Cobalt Strike and Metasploit Pro to gain network access.

FIGURE 6. Threat group GandCrab offering to monetize access to compromised networks



The screenshot shows a forum post from the user 'Gandcrab'. The post is titled 'A new branch has opened in our affiliate program dealing with the monetization of your access. What do we accept?' and lists 'RDP / VPN' as the service offered. It specifies '(cisco asa, anyconnect, openvpn, etc) access to enterprise networks with a domain (better domain tree) Mostly with domain-admin rights.' The post includes a code block with RDP and VPN connection formats: 'rdp format ip: port: domain \ username: pass' and 'vpn in .ovpn format of configs and / or ip: port: domain \ username: pass'. A note at the bottom states: 'It is advisable to apply a screen with net user% USERNAME% / domain and net group "Domain Administrators" / domain With Kaspersky on board not to offer.'

Gandcrab
(\ /) _ (\$ _ \$) _ (\ /)
●●●●●

Posted January 3 (edited) Report post

A new branch has opened in our affiliate program dealing with the monetization of your access.
What do we accept?
RDP / VPN
(cisco asa, anyconnect, openvpn, etc) access to **enterprise networks with a domain** (better domain tree)
Mostly with domain-admin rights.

```
rdp format ip: port: domain \ username: pass  
vpn in .ovpn format of configs and / or ip: port: domain \ username: pass
```

It is advisable to apply a screen with net user% USERNAME% / domain and net group "Domain Administrators" / domain
With Kaspersky on board not to offer.

⁸⁹ iDefense Security Intelligence Services. "Account GandCrab Advertises GandCrab Ransomware Version 5.0." September 27, 2018. IntelGraph reporting.

The increase in sales of access to compromised networks and growth in targeted intrusions on the part of financially driven threat actors suggests that this market has proven lucrative, which is evidenced by the fact that Nikolay has purportedly sold access to individual networks for tens of thousands of dollars—a belief based on numerous claims from the group on underground websites. Additionally, Accenture iDefense has observed countless other threat actors selling network access for similar monetary amounts. Even if malicious actors with access to valuable corporate assets do not possess the necessary knowledge to monetize access, there are countless opportunities to earn income through either selling access or partnering with others with more advanced skill sets.

SUMMARY

Financially motivated actors remain highly active despite high-profile law enforcement actions against criminal communities and syndicates in 2018. That these actors' abilities to remain operational despite the arrests highlights the significant increase in the maturity and resilience of criminal networks in 2019. Accenture iDefense analysts assess with high confidence that conventional cybercrime and financially motivated targeted attacks will continue to pose a significant threat for individual Internet users and businesses. However, criminal operations will likely continue to shift their tactics to reduce risks of detection and disruptions, as well as to maximize the return on effort, in several ways such as: shifting away from partnerships to operating within close-knit syndicates; taking advantage of familiarity with the local environment; increasing the precision of targeting by using legitimate documents to identify likely victims before delivering malware; or selling and buying direct access to networks to deliver ransomware rather than carrying out advanced intrusions.

FIVE THREAT FACTORS

3 HYBRID MOTIVES POSE NEW DANGERS IN RANSOMWARE DEFENSE AND RESPONSE

OVERVIEW

Ransomware attacks can cause serious disruption to business operations and can be costly, even if the data has been backed up properly and is securely stored offline. The attacks involving the Goga ransomware, for example, have reportedly cost victim organizations at least US\$40 million in the first quarter of 2019.⁹⁰ It is no surprise for Accenture iDefense analysts to observe the continuation of ransomware attacks and the emergence of targeted ransomware attacks. Organizations should ask themselves not only if they are implementing leading practices for security to protect against ransomware attacks, but also if they understand the ways in which their organizations may be targeted.

TOP-LINE ASSESSMENT: KEY JUDGMENTS

- Aside from delivering ransomware via spam campaigns, threat actors appear to be planting ransomware directly on networks by purchasing from underground communities Remote Desktop Protocol (RDP) access to compromised servers obtained through vulnerability exploitation and RDP brute forcing.⁹¹
- Ransomware attacks can significantly affect organizations financially by disrupting business operations, and the fact that the cost to repair or restore systems can be high.

90 Kass, D.H. "LockerGoga Ransomware Victims: Dozens of Industrial, Manufacturing Firms—MSSP Alert." March 26, 2019. MSSP Alert. <https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/lockergoga-victims/>.

91 iDefense Security Intelligence Services. "Overview of Recent Ransomware Activity." March 29, 2019. IntelGraph reporting.

- Some threat actors use ransomware for destructive purposes, in addition to or instead of financial ones.

RANSOMWARE ATTACKS, VECTORS AND MOTIVES

Recent ransomware attacks

- Unknown actors gained access to several organizations and infected networks with Goga (also known as LockerGoga) ransomware during a series of attacks that may have started on January 22, 2019, and continued for months.⁹²
- Lake City, Florida, paid a US\$460,000 ransom in June and received a decryption key, but was still far from recovering all its files nearly a month later.⁹³
- E-mail spam campaigns on Valentine’s Day were used to spread the GandCrab ransomware.⁹⁴
- Accenture iDefense analysts have observed daily spam campaigns spreading Troldesh, ransomware attacks involving Goga, Globelmposter and Cryakl; and extortion attacks using commercial encryption software rather than malware.⁹⁵
- There were reports of a surge in MegaCortex ransomware attacks in May 2019.⁹⁶ Figure 7 shows a MegaCortex ransom note.

92 iDefense Security Intelligence Services. “Overview of Recent Ransomware Activity.” March 29, 2019. IntelGraph reporting.

93 <https://www.cbsnews.com/news/ransomware-attack-lake-city-florida-pay-hackers-ransom-computer-systems-after-riviera-beach/>.

94 Sheridan, Kelly. “Valentine’s Emails Laced with Gandcrab Ransomware.” February 14, 2019. Dark Reading. <https://www.darkreading.com/threat-intelligence/valentines-emails-laced-with-gandcrab-ransomware/d/d-id/1333883>.

95 iDefense Security Intelligence Services. “Overview of Recent Ransomware Activity.” March 29, 2019. IntelGraph reporting.

96 iDefense Security Intelligence Services. “Technical Analysis of MegaCortex.” May 9, 2019.

FIVE THREAT FACTORS

FIGURE 7. MegaCortex ransom note⁹⁷

```
1
2 Your companies cyber defense systems have been weighed, measured and Have been found wanting.
3 The breach is a result of grave neglect of security protocols.
4 All of your computers have been corrupted with MegaCortex malware that has encrypted your files.
5
6 We ensure that the only way to retrieve your data swiftly and securely is with our software.
7 Restoration of your data requires a private key which only we possess.
8 Don't waste your time and money purchasing third party software, without the private key they are useless.
9
10 It is critical that you don't restart or shutdown your computer.
11 This may lead to irreversible damage to your data and you may not be able to turn your computer back on.
12
13 To confirm that our software works email to us 2 files from random computers and C:\lc_vagsi.tsv file ('s)
14 and you will get them decrypted.
15 C:\lc_vagsi.tsv contain encrypted session keys we need in order to be able to decrypt your files.
16
17 The softwares price will include a guarantee that your company will never be inconvenienced by us.
18 You will also receive a consultation on how to improve your companies cyber security .
19 If you want to purchase our software to restore your data contact us at:
20
21 ezequielgramlich6204294@mail.com
22 cammostyn9012404@mail.com
23
24 We can only show you the door. You're the one who has to walk through it.
25
```

Ransomware impact and distribution vectors

Based on the ransomware attacks described in the previous section, Accenture iDefense analysts assess with high confidence that the ransomware families displayed in Figure 8 have been prevalent or active during 2019 and likely continue to be a significant threat in the near future.⁹⁸

IntelGraph reporting.

97 *ibid.*

98 iDefense Security Intelligence Services. "Overview of Recent Ransomware Activity." March 29, 2019. IntelGraph reporting.

FIGURE 8. Ransomware distribution and infection vectors ⁹⁹
 (table footnotes continued next page.)

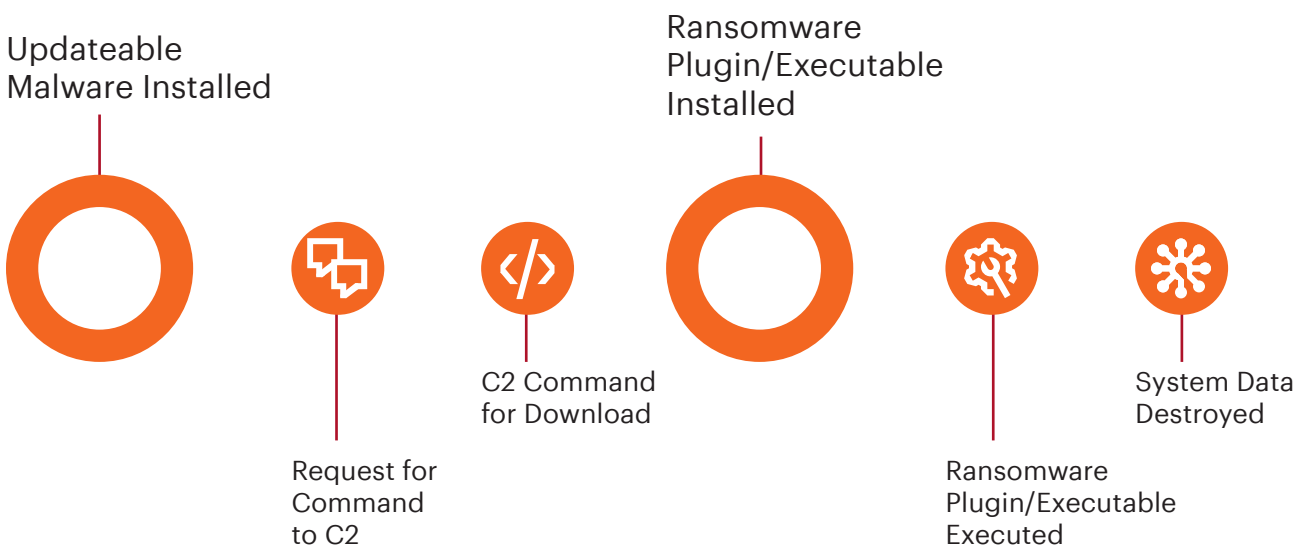
Ransomware	Distribution or Infection Vector	Autospreading Capability	Known Incidents	Distribution Prevalence
Goga	Unknown—suspected RDP or server compromise	None—manually spread through batch files	Companies in the energy, utilities, chemicals and natural resources industries	Low/Targeted (opportunistic)
Ryuk	RDP compromise and downloaded by other malware	None—manually spread through batch files	Jackson County Tribune Publishing	Low/Worldwide (opportunistic)
Troldesh	Spam campaigns	None	Unknown—likely medium-high	High/Worldwide
GandCrab	Spam campaigns using Fallout exploit kit ¹⁰⁰ MSP via plug-in compromise ¹⁰¹	None—unconfirmed EternalBlue SMB exploit	Unknown—likely medium-high	High/Worldwide
GlobelImposter	RDP Spam campaigns	None—lateral movement through scripts, other malware and system tools	Company in products vertical	Medium/Worldwide
Cryakl	Spam campaigns	None	Companies in the products and resources verticals	Medium/Europe, Asia and, Africa
Yatron	Unknown	EternalBlue and DoublePulsar SMB exploits USB, peer-to-peer (P2P), LAN, Rar file, Drive and, mIRC	Unknown	Unknown
MegaCortex¹⁰²	Unknown—suspected RDP or server compromise	None—manual and automated tools to spread malware through a network		Low/Targeted (opportunistic)

⁹⁹ iDefense Security Intelligence Services. “Overview of Recent Ransomware Activity.” March 29, 2019. IntelGraph reporting

FIVE THREAT FACTORS

Accenture iDefense assesses that ransomware attacks may continue to make substantial amounts of money for threat actors. The median demand for ransom that Accenture iDefense analysts observed in 2018 was around US\$10,000 per incident, with the highest demand being US\$8.5 million. The healthcare industry, financial institutions and professional services were targeted the most.¹⁰³ Accenture iDefense also assesses that there may be a trend toward using updatable malware, such as a downloader, remoted administration tool, bot or backdoor, to download a ransomware component on compromised machines, as depicted in Figure 9.

FIGURE 9. Updatable malware and ransomware¹⁰⁴



Source: Accenture

100 Palmer, Danny. "The Fallout exploit kit is back delivering GandCrab ransomware after a brief hiatus." January 18, 2019. ZDnet. <https://www.zdnet.com/article/this-malware-spreading-tool-is-back-with-some-new-tricks/>.

101 Kass, DH. "GandCrab Targets MSPs in Criminal Franchise Scheme." March 12, 2019. MSSP Alert. <https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/gandcrab-targets-msps/>.

102 iDefense Security Intelligence Services. "Technical Analysis of MegaCortex." May 9, 2019. IntelGraph reporting.

103 Staff. "Beazley Breach Briefing – 2019." March 21, 2019. Beazley. https://www.beazley.com/news/2019/beazley_breach_briefing_2019.html.

104 iDefense Security Intelligence Services. "Identifying Malware Families: Ovidiy Stealer, LiteHTTP Bot and AsuraHTTP Ransomware." May 10, 2019. IntelGraph reporting.

The “Best Practices for Ransomware Mitigation” section provides recommendations for mitigating the risks of ransomware.

Motives of ransomware attacks

Accenture iDefense assesses that the following motives for carrying out ransomware attacks exist:

- Hacktivism
- Financial gain
- Destruction posing as ransomware attack
- Geopolitical messaging

Hacktivism

Ransomware may actualize apparent hacktivist campaigns such as the JCry ransomware deployed as part of OpJerusalem (see Figure 10) in which the motive behind the attack is to use the usual ransom note is used to convey an ideological agenda and/or disrupt the business operations of the targeted organizations.

FIGURE 10. Political message from JCry malware observed as part of OpJerusalem



FIVE THREAT FACTORS

Financial gain

In addition to targeting by specific countries, threat actors may search for organizations that have the fiscal resources necessary to pay a large ransom. Threat actors can find opportunistic elements to exploit, such as RDP systems with weak or already-compromised credentials that can serve as access points for a site-wide ransomware campaign.¹⁰⁵ As an example, the Goga ransomware (see Figure 11), which hit numerous companies in the engineering, chemicals, and metals industries, is a targeted threat that may have been deployed via opportunistic means.

FIGURE 11. Goga ransom note¹⁰⁶

```
1 Greetings!
2
3 There was a significant flaw in the security system of your company.
4 You should be thankful that the flaw was exploited by serious people and not some rookies.
5 They would have damaged all of your data by mistake or for fun.
6
7 Your files are encrypted with the strongest military algorithms RSA4096 and AES-256.
8 Without our special decoder it is impossible to restore the data.
9 Attempts to restore your data with third party software as Photorec, RannohDecryptor etc.
10 will lead to irreversible destruction of your data.
11
12 To confirm our honest intentions.
13 Send us 2-3 different random files and you will get them decrypted.
14 It can be from different computers on your network to be sure that our decoder decrypts everything.
15 Sample files we unlock for free (files should not be related to any kind of backups).
16
17 We exclusively have decryption software for your situation
18
19 DO NOT RESET OR SHUTDOWN - files may be damaged.
20 DO NOT RENAME the encrypted files.
21 DO NOT MOVE the encrypted files.
22 This may lead to the impossibility of recovery of the certain files.
23
24 The payment has to be made in Bitcoins.
25 The final price depends on how fast you contact us.
26 As soon as we receive the payment you will get the decryption tool and
27 instructions on how to improve your systems security
28
29 To get information on the price of the decoder contact us at:
30 RomanchukEyla@protonmail.com
31 CouwetIzotofo@o2.pl
32
```

¹⁰⁵ iDefense Security Intelligence Services. "Overview of Recent Ransomware Activity." March 29, 2019. IntelGraph reporting.

¹⁰⁶ Accenture iDefense Threat Intelligence.

In addition to compromising networks themselves, ransomware actors may purchase access to networks that have already been compromised, providing faster access to systems for such threat actors' own attacks. As an example, a threat actor known as "Nikolay" was advertising the sale of compromised networks in early 2019, providing a listing of the number of compromised nodes and stating in the advertisement that these hosts were suitable for ransomware.¹⁰⁷

With the focus on larger and more substantial targets, threat actors can maintain their motive of realizing a higher ROI,¹⁰⁸ which, in turn, attracts actors with more resources and skills to such campaigns. Accenture iDefense assesses that more experienced threat actors typically practice better tradecraft and operational security, which leads to longer-running campaigns that are less subject to law enforcement disruption. Other successful campaign activity may include affiliate programs.

Actor "BulletToothTony" has advertised a Snatch ransomware affiliate program in which the malware is not sold, but affiliates are given a percent of any successfully obtained income.¹⁰⁹ In some cases, as in the case of the JSWORM affiliate program, these shares may be near 70 percent for the affiliate and 30 percent for the non-affiliate organizer who provides the malware, infrastructure and other elements required for a successful ransomware campaign.¹¹⁰ In this way, threat actors can focus on areas of specialization, leading to a higher volume of successful campaign activity.

107 iDefense Security Intelligence Services. "Threat Group "Nikolay" Advertises Access to Multiple Companies for Ransomware Attacks." March 21, 2019. IntelGraph reporting.

108 iDefense Security Intelligence Services. "Overview of Recent Ransomware Activity." March 29, 2019. IntelGraph reporting.

109 iDefense Security Intelligence Services. "Account BulletToothTony Advertises Snatch Ransomware Affiliate Program." March 21, 2019. IntelGraph reporting.

110 iDefense Security Intelligence Services. "Account jsworm Advertises JSWORM Ransomware Affiliate Program." May 6, 2019. IntelGraph reporting.

FIVE THREAT FACTORS

Destruction posing as ransomware attack

Ransomware can also serve hybrid motives, including a mix of financial and/or ideological purposes. Some ransomware appears to have been deployed to destroy information on a target rather than to efficiently make money. Ransomware's ability to destroy data, degrade performance and disrupt services can enable threat actors to cover up evidence of espionage, fraud or other crimes, as Accenture iDefense has shown.¹¹¹

It can also be used to manipulate markets by discrediting major market players, lowering the target company's share price and raising the price of the company's product by cutting off production. The Goga ransomware that paralyzed a Scandinavian aluminum company in March 2019 involved a variant that makes it difficult to pay the ransom,¹¹² suggesting that its real target may have been the victim company's share price. Although this would suggest an ultimately financial motive, the intended immediate effect may be destructive rather than the collection of a ransom payment.

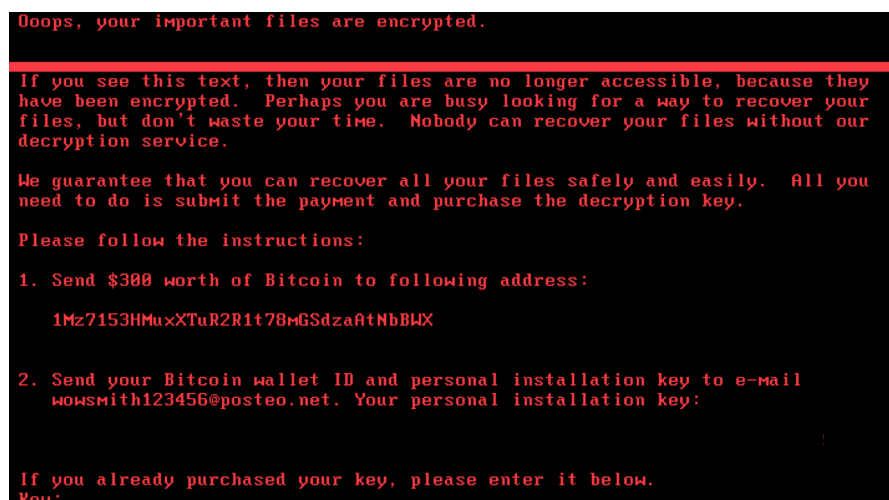
The motives behind a ransomware attack can also be political. The Petya malware outbreak of June 27, 2017, appears to have been a geopolitical attack aimed at paralyzing government and business in Ukraine (see Figure 12).¹¹³ It targeted that country by infecting an update of a software application that is widely used for tax filings and other official functions there, but it also crippled other companies that do business in Ukraine. In the future, politically motivated ransomware attacks that target a country could again be spread by infecting or replacing software that is widely used in a target country, such as tax or other government software unique to that country.

111 iDefense Security Intelligence Services. "iDefense Explains: The Coverup (One Use for Destructive Malware)." July 31, 2018. IntelGraph reporting.

112 Biasini, Nick. "Ransomware or Wiper? LockerGoga Straddles the Line." March 20, 2019. Talos Intelligence. <https://blog.talosintelligence.com/2019/03/lockergoga.html>.

113 Greenberg, Andy. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." August 22, 2018. Wired. <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>

FIGURE 12. Petya ransom message ¹¹⁴



Geopolitical messaging

Even a single ransomware campaign can serve a mix of financial and political purposes. For example, GandCrab, a criminal ransomware group, expressly refrains from targeting people in certain countries. Many cybercriminals refrain from targeting their co-nationals to avoid criminal prosecution and the group's targeting behavior could be motivated by their being located in the same country as their targets. In October 2018, GandCrab also vowed to provide decryption keys to people in war-torn Syria as a humanitarian gesture; however, it declared it would never release keys to victims in other countries, as "we need to continue punitive proceedings against certain countries."¹¹⁵ Accenture iDefense observed that GandCrab's targeting in October included entities in Germany, Switzerland and the Netherlands—countries that had actively investigated and denounced chemical attacks by the Syrian government against civilians.¹¹⁶ Other possible motives for

114 iDefense Security Intelligence Services. "Global Ransomware Outbreak Cripples Major Companies Worldwide." March 1, 2018. IntelGraph reporting.

115 iDefense Security Intelligence Services. "Account GandCrab Burnishes Patriotic Credentials by Showing Sympathy for Syria." November 6, 2018. IntelGraph reporting.

116 *ibid.*

FIVE THREAT FACTORS

the timing of the aforementioned Goga attack on a Scandinavian aluminum manufacturer in March could be political.

LEADING PRACTICES FOR RANSOMWARE MITIGATION

The following mitigations are leading practices:¹¹⁷

- **General ransomware mitigation methods:** In general, to counter ransomware issues, Accenture iDefense recommends maintaining regular backups of system data, preferably via a cloud-based solution. Additional recommendations include the following:
 - Ensure that anti-virus products and endpoint solutions are up-to-date.
 - Maintain regular and robust backups of storage devices, servers and end-users' computer data.
 - In case of infection or detection of malware, immediately disconnect affected systems from the network on which they reside.
 - Re-image infected systems whenever possible and restore users' data from backups.
 - Do not contact an attacker or pay a ransom.
 - Monitor and revoke invalid, abused or compromised certificates from trust stores and certificate authorities at their organizational sites.
 - Possibly consider using obfuscation and deception countermeasures against ransomware that target specific file

117 iDefense Security Intelligence Services. "Overview of Recent Ransomware Activity." March 29, 2019. IntelGraph reporting.

extensions by internally using unique extensions types and associating them with the appropriate application. For instance, configure company devices to open and save .doc files as .dllmox files, which ransomware should ignore as unimportant or as system files. Organizations could use the same technique to also obfuscate other files types.

- **Active Directory mitigation methods:**

- Use Azure ATP, Azure identity protection and Azure AD Conditional Access.¹¹⁸
- Implement the following suggestions for detecting DCShadow:¹¹⁹
 - Monitor and analyze network traffic associated with data replication (such as calls to DrsAddEntry, DrsReplicaAdd and especially GetNCChanges) between domain controllers (DCs), as well as to and from non-DC hosts.
 - Consider monitoring for and alerting on the replication of active directory (AD) objects.
 - Leverage AD directory synchronization (DirSync) to detect changes to the state of the directory using AD replication cookies.
 - Create a baseline and periodically analyze the configuration partition of the AD schema and set up alerting on the creation of nTDSDSA objects.

118 Seres, Debbie. "Cybersecurity threats: How to discover, remediate, and mitigate." August 13, 2018. Microsoft. <https://www.microsoft.com/security/blog/2018/08/13/cybersecurity-threats-how-to-discover-remediate-and-mitigate/>.

119 Staff. "DCShadow." Accessed on March 25, 2018. MITRE. <https://attack.mitre.org/techniques/T1207/>.

FIVE THREAT FACTORS

- Investigate the use of Kerberos Service Principal Name (SPNs), especially those associated with services (beginning with “GC/”) by computers not present in the DC organizational unit (OU).
- **RDP mitigation methods:** Accenture iDefense suggests the following mitigation methods against RDP attacks:¹²⁰
 - Disable the RDP service if it is unnecessary. If necessary, do not leave RDP accessible from the Internet.
 - Remove unnecessary accounts and groups from Remote Desktop Users groups, and enable firewall rules to block RDP traffic between network security zones.
 - Audit the Remote Desktop Users group membership regularly and remove the local administrators’ group from the list of groups allowed to log in through RDP.
 - Limit remote user permissions if remote access is necessary. Use remote desktop gateways and multifactor authentication for remote logins. Make sure a strong password requirement is in place.
 - Change group policy objects (GPOs) to define shorter timeout sessions and maximum amounts of time any single session can be active and set a maximum amount of time that a disconnected session stays active on the RD session host server.
 - Change GPOs to set the maximum amount of time that a disconnected session stays active on the RD session host server.

¹²⁰ Staff. “Remote Desktop Protocol.” Accessed on March 25, 2018. MITRE. <https://attack.mitre.org/techniques/T1076/>.

- Ensure any third-party vendors that require RDP access have security procedures in place and are following them.
- **Suggested vulnerability mitigation methods against Exploit Kits:**
 - Patch vulnerabilities associated with software.
 - Apply software updates as they become available.
 - Use a supported and recent Windows operating system.
 - Ensure that anti-virus products and endpoint solutions are up-to-date.
- **Recommended phishing campaign mitigation methods:**
 - Ensure that anti-virus products and endpoint solutions are up-to-date.
 - Regularly train users to not click links or open attachments in e-mails from unknown or untrusted sources, particularly external sources.
 - Search mail server logs to see if any user within the corporation has received the same or similar e-mails by looking at e-mail subjects, e-mail true senders, e-mail X-mailer headers, e-mail sender IP addresses, file attachment names or hashes.
 - If other users have received malicious e-mails, remove the e-mails from their inboxes before they have opened them to mitigate the risk from those e-mails.
 - If users have opened a malicious e-mail, further investigate the user's asset using available network and system logs to look for indications of the e-mail attachment(s) being executed on the host and network communication associated with any malware family

FIVE THREAT FACTORS

attributed to the e-mail attachments. If there is evidence that a user has executed the associated malware, the affected user should have a corporate malware remediation process applied and immediately have their passwords reset.

- **Server Message Block (SMB) mitigation methods related to EternalBlue:** Accenture iDefense recommends implementing the following mitigation methods related to EternalBlue and ransomware:
 - Apply the Microsoft patch for the MS17-010 SMB vulnerabilities.
 - Disable SMBv1 wherever possible.
 - Do not allow SMB connections directly from the Internet.
 - Follow best practice guidelines related to ransomware infections that computer emergency readiness teams (CERTs) have issued.
 - Quarantine attachments.
 - Segment affected hosts.
 - Prevent the shutdown of victim systems until appropriate staff can triage those systems.
 - Restore hosts to known good states.
 - Ensure that backups are available and work.
 - Use a privilege forest explorer to verify that least-privilege accessibility is in place.
 - Disable the execution of any files that carry the name “perfc.dat” as well as the PSEXEC utility from the Sysinternals Suite.

SUMMARY

The ransomware threat will continue to be a worldwide threat against all industry sectors, but the sale of access to corporate networks (see “Network access for sale” section starting on page 46) through which an attacker can deploy ransomware on a corporate-wide scale could further exacerbate the threat. Ransomware with self-propagating abilities (such as WannaCry) could re-emerge to pose a significant threat to businesses, particularly those with time-critical operations.

While the motives behind such an attack may appear to be financial, targeted ransomware attacks may at times serve hybrid motives, whether financial, ideological, or political. Regardless of motive, the ransomware threat will remain for the foreseeable future; businesses should try to ensure they have taken the adequate measures to prepare, prevent, detect, respond, and contain any corporation-wide ransomware attack. Considering the possibility that an apparently financially-motivated ransomware attack may in fact serve other purposes, a ransom payment may not guarantee the restoration of company data; therefore, companies should plan for the recovery of operations even in the event of a disruptive loss of data.

FIVE THREAT FACTORS

4 IMPROVED ECOSYSTEM HYGIENE IS PUSHING THREATS TO THE SUPPLY CHAIN, TURNING FRIENDS INTO FRENEMIES

OVERVIEW

Supply chain and third-party cyberthreats continue to be prominent risks for corporations and individuals globally. The traditional boundaries of attack surfaces are shifting as suppliers, partners and managed service providers integrate with organizations' business processes and infrastructure. This activity has affected cloud hosting¹²¹ and accounting software providers,¹²² as examples, leading to the disruption of operations for their global, corporate customer base. Cyberthreat actors, especially those who are part of politically motivated groups, appear to be exploiting this interconnectivity during their campaigns. While we observe cybercriminal chatter on underground forums concerning supply chains has been infrequent, extortive attacks in 2018 and 2019 demonstrate the appetite financially motivated groups have for targeting integral third parties most likely to cause significant disruption and damage if they are breached.¹²³

121 Krebs, Brian. "Cloud Hosting Provider DataResolution.net Battling Christmas Eve Ransomware Attack." January 2, 2019. Krebs on Security. <https://krebsonsecurity.com/2019/01/cloud-hosting-provider-dataresolution-net-battling-christmas-eve-ransomware-attack/>.

122 Nicholas, Shaun. Late with your financial paperwork? Here's a handy excuse: Malware smacked your bean-counter cloud offline. May 8, 2019. The Register. https://www.theregister.co.uk/2019/05/08/cch_hit_by_malware/.

123 Accenture Strategy. "Chief supply chain officers: Do you know where your weakest link is?" 2016. https://www.accenture.com/t00010101t000000_w_/it-it/_acnmedia/pdf-27/accenture-strategy-supply-chain-video-transcript.pdf; Cimpanu, Catalin. "Cloud-based virtual desktop provider hit by ransomware." July 22, 2019. ZDNet. <https://www.zdnet.com/article/cloud-based-virtual-desktop-provider-hit-by-ransomware/>.

TOP-LINE ASSESSMENT: KEY JUDGMENTS

- Supply chain and third-party compromises are likely to continue, especially as part of politically motivated campaigns.
- The rapidly changing geopolitical landscape can influence supply chain risks.
- The effect of cyberthreats on supply chain management, third-party risk, and merger and acquisition functions necessitates that organizations employ proactive, intelligence-driven approaches to cyberdefense.

BACKGROUND

Cyberthreat actors have identified supply chains as an effective means to infiltrate victim organizations. Even in industries like aerospace and defense in which most companies have adopted mature security hygiene practices or in which the regulatory landscape has forced such adoption, supply chains still present risks. The breadth of the supply chain threat is larger than information and communications technology and extends beyond network-delivered cyberattacks on information and information systems.

Technical analyses such as MITRE's "Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War"¹²⁴ have also drawn attention to the issue of adversarial targeting of supply chains by stating that most nation-states and advanced criminal groups have a full complement of technologies and resources available to achieve their asymmetric strategies and goals as they relate to cyberespionage and cybercrime. They usually take advantage of the

¹²⁴ Gronager, John, et. al. "Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War." August 2018. MITRE. <https://www.mitre.org/sites/default/files/publications/pr-18-2417-deliver-uncompromised-MITRE-study-8AUG2018.pdf>.

FIVE THREAT FACTORS

inherent vulnerabilities in complex supply chain ecosystems, especially the lack of oversight associated with operational security and siloed threat intelligence sharing. These vulnerabilities could include everything from patch management to employee education and awareness. Accenture iDefense anticipates that this practice will increase as supply chains and third parties remain rich targets for intellectual property theft, initial access, fraud, disruption and other malicious activity.

POLITICALLY MOTIVATED SUPPLY CHAIN COMPROMISES CONTINUE

Supply chains have been seen to become the preferred targets of politically motivated threat groups as they represent the lowest hanging fruit when threat actors consider compromising mature targets. Of the many advantages supply chains as targets offer to an adversary, two of the major benefits include the fact that smaller organizations within a supply chain often have less-robust or even non-existent cybersecurity defenses and, second, the fact that these organizations usually offer a networked connection to their customers via supplier portals, shared networks or trusted relationships between employees. If an adversary can exploit a member of the supply chain, the potential exists to advance from the supplier's network to that of the intended target.

Software supply chain compromise has remained a popular initial access¹²⁵ technique that suspected nation-state adversaries have used in 2019. This is exemplified by Operation ShadowHammer,¹²⁶ disclosed in March 2019, which involved the compromise of update software produced by a Taiwan-based company. Accenture iDefense analysis of the TTPs used in this supply chain compromise incident showed that its modular

¹²⁵ "Initial Access." June 5, 2019. MITRE. <https://attack.mitre.org/tactics/TA0001/>.

¹²⁶ iDefense Security Intelligence Services. "PIGFISH Again?: Analysis of Operation ShadowHammer Supply Chain Incident." March 28, 2019. IntelGraph reporting.

backdoor known as ShadowHammer shared traits with ShadowPad,¹²⁷ the malware family used in a similarly-styled 2017 attack against various software products that South Korean-based NetSarang produced. The Taiwan-based company was one of the targets of another supply chain compromise incident that security research firm Morphisec disclosed in 2017 and that affected a widely-used computer utility tool.¹²⁸ Accenture iDefense attributes each of these incidents with moderate confidence to what it calls the PIGFISH (also known as APT17 and Barium)¹²⁹ threat group, which was also allegedly behind an attack against several East Asian gaming and interactive media companies disclosed in March 2019.¹³⁰ During this incident, threat actors likely stole digital certificates from victim organizations to digitally sign malware used in future intrusion operations, possibly including Operation ShadowHammer. The consistent use of such code-signing¹³¹ techniques to evade network defense controls by signing malicious binaries with legitimate, stolen digital certificates is a major concern, as it erodes the trust and integrity that organizations place in automated update software that third-party vendors provide.

In both the ShadowPad and ShadowHammer incidents, threat actors appear to have set up command-and-control (C2) infrastructure for a period of approximately six months. This may be indicative of the total dwell time during which the threat actors had access to compromised systems. Based on historical observations that Accenture iDefense made as they relate to this threat group, PIGFISH actors appear to be focused

127 iDefense Security Intelligence Services. "Analysis of NetSarang SHADOWPAD Supply-Chain Attack." August 21, 2017. IntelGraph reporting.

128 iDefense Security Intelligence Services. "Who Will Deliver the Next Petya.A? Third-Party Software and Services Could Paralyze Entire Sectors or Countries." July 6, 2018. IntelGraph reporting.

129 "Greenberg, Andy. "A Mysterious Hacker Group is on a Supply Chain Hijacking Spree." May 3, 2019. Wired. <https://www.wired.com/story/barium-supply-chain-hackers/>.

130 iDefense Security Intelligence Services. "PIGFISH Actors Continue Supply Chain Attacks in Southeast Asia." March 12, 2019. IntelGraph reporting.

131 "Code Signing." June 5, 2019. MITRE. <https://attack.mitre.org/techniques/T1116/>.

FIVE THREAT FACTORS

on compromising entire supply chains and their proprietary technologies rather than targeting individual organizations. This focus may reflect an operational cadence whereby this adversary uses each sustained supply chain compromise incident as a jumping point for subsequent opportunities to conduct politically motivated attacks against specific targets to fulfill broad collection requirements.

Another suspected state-sponsored threat group that previously conducted supply chain compromises is BLACK GHOST KNIFEFISH (also known as Dragonfly),¹³² which appears to be active again this year. Accenture iDefense analysts discovered what appears to be a new sample of the custom Heriplor¹³³ backdoor Trojan in April 2019. This threat group gained substantial notoriety in July 2017 when details emerged about sustained targeting of organizations operating in the energy and manufacturing verticals based in North America and Western Europe.¹³⁴ US government officials dubbed this campaign “Palmetto Fusion.”¹³⁵ As Accenture iDefense previously detailed in the Accenture Cyber Threatscape Report 2018,¹³⁶ in 2014 BLACK GHOST KNIFEFISH actors successfully compromised software that three ICS equipment providers located in Central and Western Europe produced.

Based on these observations, Accenture iDefense asserts with moderate confidence that sophisticated cyberactors could continue to use supply chain compromise as an initial access technique, specifically as it relates to infecting legitimate software with malicious code.

132 iDefense Security Intelligence Services. “Black Ghost Knifefish.” July 7, 2017. IntelGraph reporting.

133 iDefense Security Intelligence Services. “Newly Observed Heriplor Sample Linked to BLACK GHOST KNIFEFISH Actors.” May 8, 2019. IntelGraph reporting.

134 iDefense Security Intelligence Services. “Analysis of Energy-Sector Targeting through SMB Techniques.” July 3, 2017. IntelGraph reporting.

135 iDefense Security Intelligence Services. “Analysis of Alert TA18-074A Indicators.” March 16, 2018. IntelGraph reporting.

136 “Cyber Threatscape Report 2018: Midyear Cybersecurity Risk Review.” 2018. Accenture Security. https://www.accenture.com/_acnmedia/PDF-83/Accenture-Cyber-Threatscape-Report-2018.pdf.

THE UNDERGROUND MARKET FOR SUPPLY CHAIN COMPROMISE

To date, Accenture iDefense has observed few illicit products and services affecting supply chain resources on underground forums and marketplaces, which Accenture iDefense assesses is primarily due to an overall lack of technical expertise on the part of financially motivated threat actors. While there is a large supply of purportedly compromised corporate network access points in the underground representing various industries, threat actors selling network access frequently indicate that they are doing so either because they do not know how to monetize access or because the nature of the content on the networks is not of interest to them. Access is frequently sold through auctions, with specified purchasing prices. Despite the large number of auctions, the demand for access to such networks appears to be quite low.

Since the beginning of 2018, Accenture iDefense has observed a small supply of goods relating to the production and maintenance of ATMs that could potentially result in “jackpotting,” which are attacks that force the machines to dispense cash. These goods may also enable threat actors to research vulnerabilities and subsequently create exploits for ATMs; one example appeared in an advertisement posted to an underground marketplace in August 2018. In this case, an actor advertised disk images, schematics and documentation for specific ATM brands.¹³⁷ At the time, the actor offered to sell the materials for 1 bitcoin (BTC) (approximately US\$7,630 as of August 2, 2018). The buyer could potentially use the products to create staging environments for testing purposes and exploit development.

Aside from a small market for products and services relating to ATM manufacturing and maintenance, Accenture iDefense has observed few

¹³⁷ iDefense Security Intelligence Services. “Examining ATT&CK Techniques: Threat Actors’ Use of Supply Chain Compromise.” March 3, 2019. IntelGraph reporting.

FIVE THREAT FACTORS

advertisements of supply chain vulnerabilities on underground forums and marketplaces. Marketing valuable vulnerabilities would likely result in detection by law enforcement and security researchers who would then alert the affected organization(s). As a result, transactions for such vulnerabilities are likely to occur out of view of underground website users and instead on closed communication platforms.

Even though valuable vulnerabilities that may result in a supply chain compromise are not frequently advertised, Accenture iDefense analysts have tracked a notable actor advertising source code for multiple products of an international security solutions provider.¹³⁸ The actor primarily sells code for a platform that offers to help organizations by securely connecting a variety of network types, IoT devices, mobile devices, industrial control networks including sensors, supervisory control and data acquisition (SCADA), and human machine interfaces (HMIs) over public and other untrusted networks and communication channels.¹³⁹ The actor claims to have analyzed the source code and determined the technologies that can be leveraged to exploit the platform, and stated that companies in numerous sectors, including the government and critical infrastructure sectors, use the products. As the technologies are supposedly vulnerable to exploitation, an interested party could easily use the source code to compromise organizations and any system or network built on the advertised platform. Accenture iDefense has seen multiple follow-up responses from the actor on a popular underground website. Initially, the actor sought 13 BTC (approximately US\$95,000 at the time of the posting) for the code dump.¹⁴⁰

138 iDefense Security Intelligence Services. “<Redacted> Cyber-security Company <Redacted> Exposes Critical Infrastructure Sectors in Europe and North America to Risks of Cyber-crime and Espionage.” June 13, 2018. IntelGraph reporting.

139 *ibid.*

140 *ibid.*

The specific cases highlighted above are the rare ones in which financially driven threat actors have advertised products that could result in supply chain compromise with proper exploitation. Accenture iDefense has found that supply chain vulnerabilities advertised on underground forums and marketplaces primarily affect the financial services industry. The supply of such vulnerabilities in the underground exceeds the demand, possibly due to the advanced technical knowledge required to exploit affected systems and monetize access. Threat actors are frequently hesitant to disclose details of supply chain vulnerabilities on readily accessible underground websites to avoid alerting law enforcement or security researchers.

GEOPOLITICS AND SUPPLY CHAIN FRENEMIES

The effect of geopolitical risks on businesses, especially global technology companies, has been severe in 2018 and 2019.¹⁴¹ These organizations are facing ever-more-complex threats to their supply chains, a result of having products and services spread across every corner of the world. Companies, no matter their sizes, should factor in geopolitical risks in business decision making, due partly to the global nature of modern supply chains.

Although organizations may avoid business disruptions by familiarizing themselves with local regulations and complying with local laws in each country where they operate or have business partners, an understanding of the political factors underlying official policies in host and partner countries can also help companies avoid damaging their international relationships. Meanwhile, as cyberthreats vary by country, threat actors may seek advantage in evolving geopolitical contexts, such as trade conflicts and global power shifts, by manipulating an organization's supply

¹⁴¹ Ellyatt, Holly. "The effect of geopolitics on global growth worries me most, WEF president says." January 21, 2019. CNBC. <https://www.cnbc.com/2019/01/21/the-effect-of-geopolitics-on-global-growth-worries-me-most-wef-president-says.html>.

FIVE THREAT FACTORS

of products or services to compromise a networked environment. Actively developing situational awareness and setting up effective warning systems can help businesses assess their threat landscapes, establish protocols and craft response plans to specific conditions ahead of time.

The modern interdependent and interconnected global economy has resulted in a complex supply chain for most businesses but has also created a supply chain “frenemy network” through which businesses must maneuver, as business partners and suppliers can be both trusted and untrusted. For example, a company that is a key provider in the supply chain of one product may compete in another area with the same company to which it is a supplier. Threats could arise from this partner-competitor relationship due to escalating market competition or conflicts resulting from different cultural understandings of business practices. Organizations need to understand suppliers’ cybersecurity practices, such as whether they patch emerging vulnerabilities in a timely manner, as well as new products and innovations that they are developing. Operating wisely with “frenemies” to reduce supply chain risks is an important factor in the success of an international business.

PROACTIVE DEFENSE: LEVERAGING CYBERTHREAT INTELLIGENCE TO PROTECT SUPPLY CHAINS

When trying to proactively and properly combat threats to supply chains, organizations should integrate cyberthreat intelligence (CTI) into their security postures and interweave CTI from external sources with internal data and analysis. This interweaving can provide a full appreciation of the risks associated with leveraging a supply chain and enable enhanced situational awareness for decision makers and operators involved in daily operations and strategic initiatives such as mergers and acquisitions (M&As).

Successfully leveraging actionable CTI is one of the most important countermeasures an organization can employ when attempting to reduce the likelihood of an adversary leveraging its supply chain as an exploit vector. Successfully leveraging actionable CTI can help an organization identify which members of its supply chain represent the highest criticality or risk of compromise and institute the right types of defenses to help reduce this threat, even if that organization lacks the ability to institute critical changes directly on a supplier's network.

When employing CTI to protect a supply chain, an organization should seek to understand the historical threats posed by its unique ecosystem of suppliers. For instance, enumerating the individual threat groups that previously targeted these suppliers could help an organization to better understand the TTPs likely still in use by these particular adversaries. Organizations may also consider surveying the cybersecurity policies of their supply chain providers to evaluate risk. Armed with this data, an organization can deploy defenses to help detect and prevent activity associated with specific tools these threat groups used as they attempted to jump across networks and exploit trusted relationships. This intelligence can be directly passed to members of the supply chain to show them how they may be attacked in the future.

An organization can also gather CTI by monitoring adversaries' actions and communications online; doing so may help give those companies knowledge of upcoming threat actor campaigns that may affect the organizations themselves or their supply-chain vendors.

INTEGRATING CTI WITH MERGER AND ACQUISITION PURSUITS

M&As present unique challenges related to politically motivated cyberthreat campaigns and cybercrime because one of the entities in an M&A could run the risk of inheriting current and future vulnerabilities and

FIVE THREAT FACTORS

risks associated with the other party. If one of the entities is unknowingly a victim of a previous compromise, once merged, the adversary could potentially inherit a new victim as well. There are several critical moments during the M&A process when CTI should be at the forefront of any organization. These moments occur before, during and following any merger or acquisition.

Prior to merger or acquisition

An organization should seek to understand as fully as possible the historical threats posed to the target of a merger or acquisition. As most M&As are initially kept private because of legal and other requirements, this step could prove difficult; however, companies should view it as a priority. The acquiring organization should collect and analyze as much data as possible to determine if threat actors have in the past targeted the organization to be acquired and if the acquiring organization could become a target in the future because of the acquisition. If CTI indicates that threat actors have targeted the acquired organization in the past, the acquiring organization should seek complete situational awareness as to which threat group(s) carried out the attacks, the TTPs those groups leverage, and any harvestable and actionable technical indicators from those attacks to conduct a proper investigation of the acquired organization's network, when the time is right to do so. If CTI indicates that the organization to be acquired has not yet been targeted, the acquiring organization should still determine if the acquired organization falls within the known collection requirements of any threat groups. From a tactical perspective, CTI should identify actual technologies, programs and other forms of intellectual property that compromise these intelligence requirements. By compiling a list of the high-value programs and technologies for each M&A target, the acquiring organization can decide if any of them are known to be of interest to an adversarial threat group.

During and after a merger or acquisition

During and after any M&A activity, CTI should play an integral role in aiding senior-level decision makers as they make current and future business decisions; help network defenders at all levels proactively mitigate future campaigns; and detect any current suspicious activity. For example, CTI should help C-suite executives understand where fresh vulnerabilities exist because of newly acquired high-value programs, technologies, intellectual property or PII that may currently lack proper protection against future cyberthreat targeting.

Technical CTI should provide organizations with high confidence and actionable indicators that cyberdefense operators can use both to alert for suspicious traffic post-merger or acquisition, and to leverage when performing incident response investigations, if the merged networks show signs of compromise. This technical CTI should provide enough context to give merging organizations immediate and complete situational awareness of TTPs and even attribution, if possible.

Cloud security strategy

For many organizations, cloud environments generally provide greater security than local solutions would. However, cyberthreat actors have begun to turn their focus toward cloud environments, seeing them as target-rich. Cloud service provider (CSP) and managed service provider (MSP) compromises have given cyberthreat actors unauthorized access to sensitive information across numerous industries.¹⁴² Companies rely on vendor support to secure cloud storage and release critical vulnerability patches, but still need to implement their own security controls. US Department of Homeland Security (DHS) reporting warned organizations

¹⁴² Stubbs, Jack et. al. "Inside the West's failed fight against China's 'Cloud Hopper' hackers." June 26, 2019. Reuters. <https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/>.

FIVE THREAT FACTORS

in spring 2019 of decreased security postures when using popular cloud-based office applications.¹⁴³ The reporting noted that compromised organizations did not have designated IT cloud security teams and recommended that organizations set up company cloud strategies as a necessary step in reducing corporate vulnerabilities. The recommended company strategies include multi-factor authentication (MFA) to protect against O365 credential theft, disabling of legacy e-mail protocols and configuring of network management password synchronizing.¹⁴⁴

Vendor device testing

Security testing is a crucial part of the technology development and acquisition process. This testing can be especially daunting for large firms as they harmonize a diverse suite of technologies to optimize business operations. Continuous monitoring of cyberthreats to software, firmware and hardware can enable organizations to be proactive and efficient with their allocation of resources to the in-depth vetting of third-party technologies.

A factory acceptance test (FAT), also known as a vendor accepted test (VAT), involves a manufacturer testing devices in simulated environments prior to client deployment and installation.¹⁴⁵ A FAT evaluates a device's compatibility with client specifications, validates the quality of a tested device and ensures seamless integration into a client's operational technology (OT) environment. FATs are usually conducted during the first installation of significant upgrades or when switching to a new vendor but are often overlooked when repurchasing from a trusted vendor,

¹⁴³ Department of Homeland Security Cybersecurity and Infrastructure Security Agency. "Analysis Report (AR19-133A)." May 13, 2019. US-CERT. <https://www.us-cert.gov/ncas/analysis-reports/AR19-133A>.

¹⁴⁴ *ibid*.

¹⁴⁵ Dahl, Johan. "Factory and Site Acceptance Tests (FAT, SAT) For Electrical and Automation Systems in a Power Plant." Accessed on May 13, 2019. Electrical Engineering Portal. <https://electrical-engineering-portal.com/download-center/books-and-guides/power-substations/fat-sat-power-plant>.

which presents an opening for malicious actors. Trusted vendors are just as susceptible to vulnerabilities, and their devices should be tested for firmware misconfigurations or malware. To further confirm device integration into an environment, a site acceptance test (SAT) occurs at the client site after a FAT. For smaller organizations that cannot afford the use of an on-site simulated testing environment, a third-party test lab is suitable for conducting SATs.

Third-party risk assessments and contracts

Case study: How Financial Services are responding to third-party risk

In the financial services industry, authoritative bodies, including the European Supervisory Authorities (ESAs)—the European Banking Authority (EBA), European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA)—are continuing to emphasize third-party cyber risks. The ESAs have proposed a legislative framework to monitor the resilience of critical service providers, and in the interim, firms are encouraged to leverage threat-intelligence-led cyberresilience testing to understand their attack surfaces.¹⁴⁶

Evaluation of “key financial market participants and their critical functions, including (wholesale and retail) banks, broker-dealers, financial market infrastructures, financial market utilities, and other critical third parties, the different threat actors (including their TTPs) targeting these entities, and the common vulnerabilities”¹⁴⁷ is considered a crucial step in evaluating the breadth and depth of threats to the sector. In Europe, this

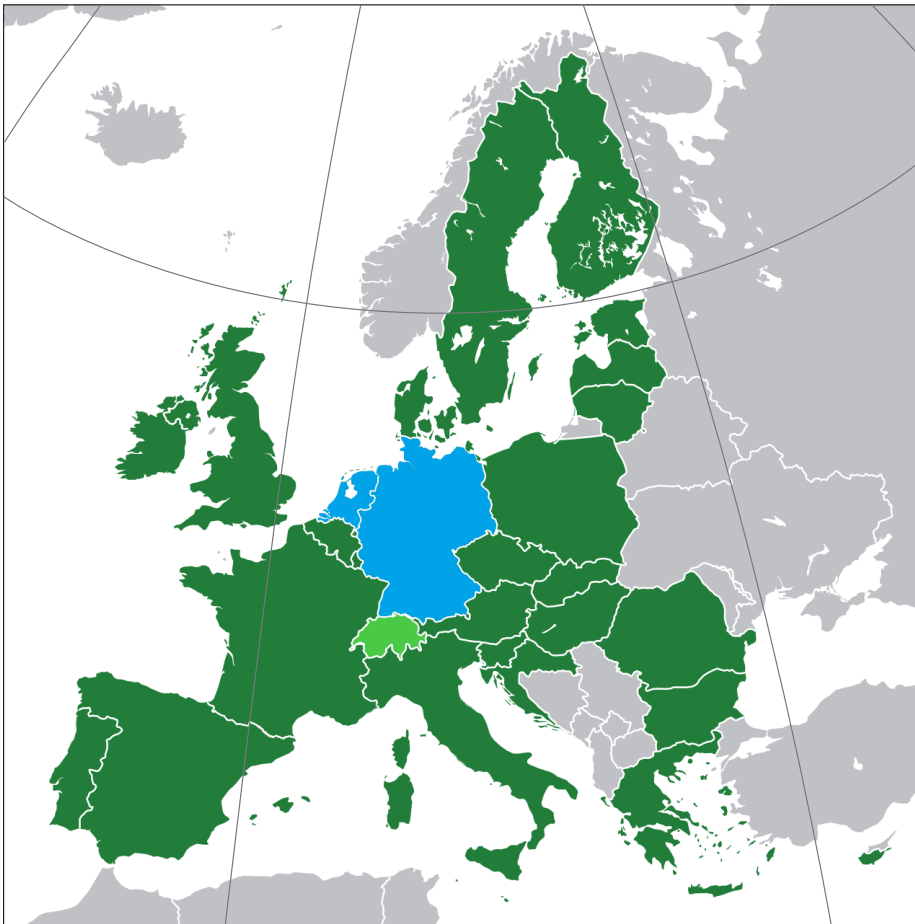
146 “Joint Advice of the European Supervisory Authorities.” April 10, 2019. European Union. <https://eba.europa.eu/documents/10180/2551996/JC+2019+26+%28Joint+ESAs+Advice+on+ICT+legislative+improvements%29.pdf/4d2ad5e2-1570-48bd-819a-7cd9b4e8b157>.

147 “TIBER-EU FRAMEWORK: How to implement the European framework for Threat Intelligence-based Ethical Red Teaming.” May 2018. European Central Bank. https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf.

FIVE THREAT FACTORS

evaluation is done through the TIBER-EU framework that is being adopted via national implementations across various countries (see Figure 13). At the onset of a TIBER assessment, the evaluator produces a targeted threat intelligence report (TTI report) regarding the entity being tested. This report includes coverage of infrastructure that has been outsourced and critical third parties.

FIGURE 13. Eurozone countries (colored), showing the Netherlands and Germany in blue as national implementers of the TIBER-EU framework ¹⁴⁸



148 Solberg J., S. "File:Global European Union.svg." Accessed on June 6, 2019. Wikimedia Commons. https://commons.wikimedia.org/wiki/File:Global_European_Union.svg. Used under Creative Commons Attribution 3.0 Unported license. iDefense modification of this image to illustrate adoption of TIBER-EU and associated frameworks does not suggest endorsement by the licensor.

In 2019, industry-focused guidance from United States regulators has shed light on the risk third parties pose to critical infrastructure sectors, including the oil and gas, and financial services sectors. North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) 013-1, titled “CyberSecurity Supply Chain Risk Management,” requires vendors to notify electric utility customers of known product vulnerabilities.¹⁴⁹ Previously, vendors were not obligated to disclose exploits; as a result, critical devices would remain unpatched. As electric utilities continue to implement standards to ensure grid resiliency and security, other critical infrastructure sectors continue their standards development work. Operational Technology (OT) environments in the oil and gas, and chemicals industries are considered to be particularly vulnerable during this standards development phase.

An alternative for industries lacking finalized standards to help mitigate supply chain and third-party risks is to consider including in their software and hardware vendor agreements a requirement to disclose known vulnerabilities. In addition to government regulations, where they exist, information sharing and strengthened third-party relationships could help to reduce cyberthreat vulnerabilities throughout the supply chain. In addition to contracts, companies may wish to conduct third-party risk assessments. Additionally, the risk of a potential third-party cyberattack should be calculated into companies’ standard risk management process.

149 “NERC CIP 013-1: CyberSecurity Supply Chain Risk Management.” October 18, 2018. North American Electric Reliability Corporation. <https://www.nerc.com/pa/Stand/Reliability Standards/CIP-013-1.pdf>.

FIVE THREAT FACTORS

SUMMARY

The global interconnectedness of business, and the broadening adoption of traditional industry cyberthreat countermeasures and basic cybersecurity hygiene push cyberthreat actors to seek new avenues to compromise targets such as supply chains, including those for software, hardware and cloud. As a component of routine operations, organizations should seek full awareness of their threat profiles and points of supply chain vulnerability.

By integrating cyberthreat intelligence into M&As and other strategically important actions, incorporating vendor and factory testing, and implementing industry-focused regulations and risk assessment standards, organizations can grow mature processes to guard against the cybersecurity risks inherent in the landscape of modern global business operations.

5 LIFE AFTER MELTDOWN: VULNERABILITIES IN COMPUTER CLOUD INFRASTRUCTURE DEMAND COSTLY SOLUTIONS

OVERVIEW

It is estimated that 83 percent of enterprise workloads will move to the cloud by the year 2020.¹⁵⁰ This race to the cloud has prompted security researchers and adversaries to look for vulnerabilities in the cloud infrastructure, leading to the discovery of multiple side-channel vulnerabilities in modern CPUs over the last two years. These sophisticated CPU vulnerabilities, affecting both server and workstation CPUs, pose a high risk to organizations running their compute infrastructure in the public cloud. Adversaries can use this class of side-channel vulnerabilities to read sensitive data from other hosts on the same physical server.

TOP-LINE ASSESSMENT: KEY JUDGMENTS

- Multi-tenant public cloud providers are ideal targets for exploitation of side-channel CPU vulnerabilities, which can be exploited, for example, to read data from other hosts on the same physical server.
- Mitigations are available for most platforms, cloud deployments, and software. However, most of the mitigations come at a cost of reduced performance, leading to increase of compute costs for most enterprises.
- Understanding the threats posed by CPU vulnerabilities is important to design a proper risk mitigation strategy, which can be vastly different for each organization.

¹⁵⁰ Columbus, Louis. "83% Of Enterprise Workloads Will Be In The Cloud By 2020." January 7, 2018. Forbes. <https://www.forbes.com/sites/louiscolombus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020/>.

FIVE THREAT FACTORS

Since January 2018, computer hardware security researchers have disclosed multiple vulnerabilities in microprocessors. The discovery and disclosure of these vulnerabilities, broadly classified as Spectre and Meltdown,¹⁵¹ have broken down the assumptions of hardware security and the threat models associated with computer processor hardware and have brought back microprocessor security research into the foreground.

By November 2018, security researchers had found and disclosed multiple new variants of Meltdown and new attack techniques for Spectre vulnerabilities. In May of 2019, security researchers disclosed four new side-channel information disclosure vulnerabilities which affect Intel processors. These vulnerabilities are popularly referred to as Zombieload, RIDL and Fallout.¹⁵² Due to the amount of interest received, it is likely that additional variants and vulnerabilities are currently being investigated at this time.

TRANSIENT EXECUTION SIDE CHANNEL ATTACKS

Modern microprocessors attempt to increase the number of instructions which can be executed in parallel to boost their performance. One method of increasing the processor's throughput is to execute instructions which are likely to be executed soon, prior to the instruction being requested. To achieve this, processors predict or "speculate" possible "future values." Based on speculation, the processor executes ahead of time and keeps the results of such yet-to-be-executed instructions transiently. If the processor predicts correctly, when the "speculated group of instructions" arrive, the processor already has all the computed results ready, resulting in higher performance. However, if the processor speculated incorrectly, the results are discarded.

151 iDefense Security Intelligence Services. "Meltdown and Spectre Multiple Processor Information Disclosure Vulnerabilities." January 2, 2018. IntelGraph reporting.

152 iDefense Security Intelligence Services. "Intel Information Disclosure Vulnerabilities - Zombieload, RIDL and Fallout." May 15, 2019. IntelGraph reporting.

Security researchers have now found that even though the processor discards the results of incorrectly speculated instructions, there are indirect means (side-channels) of gaining information about the transient results. This information disclosure has resulted in vulnerabilities like Spectre, Meltdown, Foreshadow and other related variants.

Most of the affected hypervisors, operating systems, and hardware vendors have released patches, mitigations, and defenses to tackle the multitude of speculative execution issues that have been brought to light in the past two years.

RISK OVERVIEW

The side-channel vulnerabilities affect most modern microprocessors, servers and workstations alike. However, the largest risk occurs in one major class of services—cloud computing. Typically, public cloud computing services have multiple tenants sharing compute instances on the same physical hardware. In this multi-tenant architecture, each tenant's data is supposed to be completely isolated and secured from the other tenants. A multi-tenant architecture which uses processors that are vulnerable to side-channel attacks can be exploited by a malicious co-tenant to extract information from another tenant's instance.

MITIGATIONS

Cloud deployments

Organizations that want to try and minimize the risks associated with the exploitation of these vulnerabilities should consider using a single-tenant dedicated host cloud environments. Single-tenant environments provide a more isolated hardware environment while enabling the flexibility of a cloud deployment.

FIVE THREAT FACTORS

Popular cloud providers provide the option to use dedicated physical hardware resources, minimizing the risk of cross-container or shared-hardware-host attacks (see Figure 14). It is important for customers to read the fine print of the cloud service, as the implementation may vary between vendors. For example, Amazon Web Service (AWS) offers a dedicated instances option such that each instance runs in a virtual private cloud on hardware that is dedicated to a single customer or account. Although this ensures total physical isolation, the catch is that the dedicated instances may share the same underlying physical hardware with non-dedicated instances deployed from the same account. This is particularly important to consider in the case of a single account running a multi-tier application with components running on both dedicated and non-dedicated instances.

FIGURE 14. Cloud providers with dedicated instances and alternate processors

Cloud provider	Dedicated instance option	Choice of processor
Amazon AWS EC2	Yes	Yes ¹⁵³
Microsoft Azure	Yes	Yes (limited) ¹⁵⁴
Google Cloud	Yes	No
Oracle Cloud	Yes	Yes ¹⁵⁵
IBM Cloud Compute	Yes	No

153 Amazon. "Introducing new Amazon EC2 instances featuring AMD EPYC processors." Accessed July 15, 2019. <https://aws.amazon.com/ec2/amd/>.

154 AMD. "A Great Time to Move to AMD EPYC on Azure." February 11, 2019. <https://community.amd.com/community/amd-business/blog/2019/02/11/a-great-time-to-move-to-amd-epyc-on-azure>.

155 AMD. "AMD and Oracle Collaborate to Provide AMD EPYC™ Processor-Based Offering in the Cloud." October 23, 2018. <https://www.amd.com/en/press-releases/2018-10-23-amd-and-oracle-collaborate-to-provide-amd-epyc-processor-based-offering>.

Finally, organizations that are extremely risk averse can choose to have an on-premises cloud. This vastly reduces the risk and enables the organization to accept some management overhead without sacrificing performance.

Private infrastructure

There are many mitigations available for organizations to remediate the risk on privately maintained infrastructure.¹⁵⁶ The side-channel vulnerabilities have resulted in vendors offering mitigations at various levels of the computing stack—processors, hypervisors, operating systems and software.

Software updates

Most operating system vendors have issued security updates to mitigate these vulnerabilities. However, in most cases, the resulting compute performance has been lower. In some instances, the performance degradation has been reported to be a staggering 30 percent.¹⁵⁷ For example, for the Portsmash¹⁵⁸ vulnerability, the solution is to disable simultaneous multithreading (SMT), which can lead to degraded performance. The most popular software patch is Google's Retpoline,¹⁵⁹ which prevents the processor from speculating on the target of an indirect jump.

156 Microsoft Azure. "Guidance for mitigating speculative execution side-channel vulnerabilities in Azure." June 3, 2019. <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/mitigate-se>.

157 Sloss, Benjamin Treynor. "An update on Sunday's service disruption." June 3, 2019. Google Cloud. <https://cloud.google.com/blog/topics/inside-google-cloud/an-update-on-sundays-service-disruption>.

158 iDefense Security Intelligence Services. "CVE-2018-5407 - Multiple Vendor Microprocessors Design Error Information Disclosure Vulnerability." November 2, 2018. IntelGraph reporting.

159 iDefense Security Intelligence Services. "Meltdown and Spectre Multiple Processor Information Disclosure Vulnerabilities." January 2, 2018. IntelGraph reporting.

FIVE THREAT FACTORS

Compiler vendors have included new compiler flags which add protection against some vulnerabilities, like Spectre.¹⁶⁰ Newer versions of compilers default to these flags. To take advantage of these compiler updates, most software vendors must recompile their applications with updated compilers. This is not always easy, as some sub-components of large applications can still be using older libraries which are not compiled with Spectre mitigations, thereby degrading the overall security posture of the entire application.

New hardware

The simplest mitigation is to replace the hardware with newer hardware which has protections built-in to address these vulnerabilities. Although the cost of replacing hardware prematurely can be expensive, it may be worth the investment to replace server hardware out of cycle. Updating to new hardware does not, however, guarantee future security as new classes of CPU vulnerabilities are found every year.

To counter this, processor vendors provide firmware updates where possible. They also provide microcode updates to operating system vendors, which are shipped as security updates. Microcode updates are applied at boot-time by the operating system, which can help in patching some of the security vulnerabilities on-the-fly. The ideal way to deal with this risk is to apply mitigations at all possible levels of the compute stack—hardware and software.

¹⁶⁰ Phabricator. “[Spectre] Introduce a new pass to do speculative load hardening to mitigate Spectre variant #1 for x86.” March 23, 2018. <https://reviews.llvm.org/D44824>; Phoronix. “Spectre Mitigation Added To GCC 8, Seeking Backport To GCC 7.” January 14, 2018. https://www.phoronix.com/scan.php?page=news_item&px=GCC-8-Spectre-Mitigation-Lands; Microsoft. “Spectre mitigations in MSVC.” January 15, 2018. <https://devblogs.microsoft.com/cppblog/spectre-mitigations-in-msvc/>.

Risk acceptance

The cloud compute architecture has changed the way organizations have assumed risk. In most cases, an organization runs compute instances in a multi-tenant cloud and has best practices in place to minimize risk for cost savings. This approach can work well, especially for smaller organizations, when the compute data is less sensitive.

However, for organizations that prefer to have complete control over the compute resources, some amount of risk acceptance can help realize some of the costs of having an on-premises cloud. With a vastly different threat model, an organization with an on-premises cloud solution can choose to not apply the mitigations which may heavily degrade application performance. A hybrid solution which uses on-premises cloud for sensitive data and the public cloud for non-sensitive data can also be a solution for some organizations.

SUMMARY

No two organizations have the same needs. Performing a careful analysis of business objectives, security and growth strategy is necessary before architecting and managing a cloud solution.



A SECURITY PIVOT

Cybercrime is not a one-time event. Just as one avenue of income has been blocked, cybercriminals will swiftly move on to another, often more sophisticated means of entry. And even tried and tested methods of attack, such as ransomware, can be subject to change, as threat actors apply the principles but interpret the execution in new and different ways.

Today, organizations must not only take on the disruptive forces that are changing their industries with speed, confidence and continuous innovation, but also remember their most important currency—trust. Security is front and center of maintaining that trust, but with new threats constantly emerging, it is being sorely tested.

In summary:

- **Communications targeting global stage may not be all they seem.** Advances in technologies, such as artificial intelligence and 5G communications, along with social media and other fast communications channels, are providing a new, easy gateway to influencing and impacting the geopolitical landscape. Organizations should be vigilant and prepare for the fact that world events are often a target, with phishing lures or distractions taking advantage of and being used to influence outcomes.
- **Cybercriminals are shifting—and so should you.** Conventional cybercrime operations continue to happen, but they are also evolving. Close-knit syndicates are favored alongside localized underground economies, especially in non-English-speaking countries. New TTPs, such as “big game hunting” and hack ‘n’ hustle network access intrusions are on the increase. Established attack methods, such as using commodity malware, emphasize how important it is for organizations to stay one step ahead of the cyberattackers.

- **The mixed motives behind ransomware are making it more destructive.** The consequences of ransomware can be far more than financial—significant disruption to business operations, and a high cost to repair or restore systems, are part of the ransomware experience, not to mention the impact on business brand, culture and trust. There is no guarantee that paying a ransom will restore lost data.
- **This is no time for splendid isolation—your ecosystem needs you.** Threat actors continue to favor creating third-party compromises, especially as part of politically motivated campaigns. The effect of cyberthreats on supply chain management, third-party risk, and merger and acquisition functions means organizations should employ proactive, intelligence-driven approaches to cyberdefense.
- **Beware of opening more than the back door.** The potential for exploitation of side-channel CPU vulnerabilities so that data can be read from other hosts on the same physical server appear to make multi-tenant public cloud services an ideal target. And mitigations come at a cost—reduced performance that leads to an increase of compute costs for most enterprises. Designing a risk mitigation strategy can be vastly different for every organization.

Organizations should tackle cyberresilience with a security pivot mind-set. They should learn not to dwell on the vulnerabilities of the past and be consistent but flexible in their defense. They should look at security with a wide lens, to include the vulnerabilities of partners and third parties in the scope of their cyberstrategies. And they should learn to make a security pivot, adapting their approach to meet the latest demands from a rapidly changing world.



ABOUT THE REPORT

The Cyber Threatscape Report 2019 presents key findings from Accenture iDefense threat intelligence research into significant cyberthreat trends. This report covers cyberthreat trends the Accenture iDefense threat intelligence team has observed and analyzed from January 2019 until July 2019. It provides an overview of the trends and how Accenture iDefense threat intelligence believes they might evolve and grow throughout the year ahead.

This report should serve as a reference and strategic complement to daily intelligence reporting to provide IT security and business operations with actionable and relevant decision support based on Accenture iDefense threat intelligence. It aims to inform IT security teams, business operations teams, and organizations' leadership about emerging cyber trends and threats, to help those groups anticipate key cybersecurity developments for the remainder of the 2019 calendar year (and in some cases beyond), and to provide, where appropriate, solutions to help reduce organizations' risk research using primary and secondary open-source material.

Accenture iDefense threat intelligence has been creating relevant, timely and actionable threat intelligence for 20 years, by collecting threat data, indicators of compromise, geopolitical-based, regional-based, and industry vertical-based intelligence. Our team was built to help provide our clients with actionable and relevant threat intelligence that they use to support decisions that help them enhance their security teams, defend their networks, and bolster their security technology investments, their security processes and their business strategy.

The following table defines malware, threat groups, exploit kits and vulnerabilities listed throughout the report.

GLOSSARY

Name	Type	Description	Page
AZORult	Malware	AZORult is an infostealer malware that gathers user credentials stored in several applications. It also collects information such as Bitcoin wallets, running processes, a list of installed applications, and information about the compromised computer, such as username in use, host name, operating system and other information.	40
Bateleur	Malware	Bateleur is a JavaScript backdoor capable of capturing information about a victim machine and downloading additional modules to perform other functions such as taking screenshots and executing other malware, such as TinyMet.	43
Carbanak	Threat Group	Carbanak (also known as Anunak and Teleport Crew) is a sophisticated and persistent cybercrime group that targets financial institutions, the hospitality industry and credit card data. It has caused damage of up to US\$1 billion from the financial sector since at least 2013, having carried out fraudulent banking transactions and ATM compromises.	43
Cobalt Strike	Tool	Cobalt Strike is a penetration testing tool that features numerous methods to complicate detection. Both legitimate security professionals and threat actors use this tool.	43
CobInt	Malware	CobInt is a multi-stage malware variant likely developed and used by the Cobalt Group. It is commonly delivered via exploit documents (Word files). Upon delivery, it is broken into three stages: an initial downloader, a main component and additional modules.	45
Cryakl	Malware	Cryakl (also known as Simlosap and Fantomas) is a ransomware that has been around since 2014. It is written in Delphi, and the later versions use asymmetric RSA encryption.	51

GLOSSARY

Name	Type	Description	Page
CVE-2015-2545	Vulnerability	The CVE-2015-2545 vulnerability is a memory corruption vulnerability in Microsoft Office that exists due to improper handling of Office files containing embedded graphic images, specifically Encapsulated Postscript (EPS) files. Remote exploitation of this vulnerability could enable an attacker to execute arbitrary code with current user privileges on the targeted host.	45
CVE-2017-0199	Vulnerability	The CVE-2017-0199 vulnerability is a remote code execution vulnerability that exists in the way that Microsoft Office and WordPad parse specially crafted files. An attacker who successfully exploited this vulnerability could take control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.	45
CVE-2017-11882	Vulnerability	The CVE-2017-11882 vulnerability is a buffer overflow vulnerability that allows remote code execution because of an error in the EQNEDT32.EXE component process, which handles OLE objects relating to Microsoft Office's equation editing functionality. Malicious RTF documents often take advantage of the vulnerability by including a specially crafted OLE object that will exploit the vulnerability.	40
Emotet	Malware	The Emotet Trojan is a highly automated and continually developing banking Trojan. Commonly distributed through spam campaigns, Emotet's worm-like capabilities make this Trojan an effective tool for cybercriminals. First-stage malicious documents can use Emotet as a second-stage downloader now that it has transformed from a banking Trojan into more of a downloader.	40
Fallout	Exploit Kit	Fallout is an exploit kit that Accenture iDefense first observed for sale in the underground in September 2018.	40
Goga	Malware	Goga (also known as LockerGoga) is a ransomware that leverages RSA 4096-bit encryption to encrypt files in local drives and mapped network drives.	50

Name	Type	Description	Page
GandCrab	Malware	GandCrab is a ransomware variant known to be distributed through malspam and malicious advertising. Threat actors continue to develop the malware. In recent campaigns, Accenture iDefense has observed GandCrab being distributed in tandem with the Vidar banking Trojan.	46
GandCrab	Threat Group	GandCrab is a threat group that has advertised the sale of the GandCrab ransomware affiliate service on the Russian-language underground forum Exploit.	48
Globelmposter	Malware	Globelmposter is a ransomware that uses its resources section to configure itself. It is considered a copycat of the Globe ransomware.	53
GrandSoft	Exploit Kit	GrandSoft is an exploit kit that has been around in some form since 2012. Threat actors used it in 2018 and 2019 to deliver GandCrab ransomware.	40
Greenflash Sundown	Exploit Kit	Greenflash Sundown is an exploit kit that targets systems in Asian countries. It is a private and extensively modified version of the Sundown exploit kit.	41
GUDWIN	Malware	GUDWIN is a JavaScript backdoor that shows code similarities with Bateleur. Known aliases of GUDWIN include Baby Bateleur and GRIFFON.	44
HALBAKED	Malware	HALBAKED is a VBScript backdoor capable of collecting information about a victim machine and downloading additional malware to perform functions such as taking screenshots.	43
JCry	Malware	JCry is a custom ransomware built by unknown threat actors.	55
JSWORM	Malware	JSWORM is ransomware developed in C++ and advertised on the Russian criminal forum Exploit.	57

GLOSSARY

Name	Type	Description	Page
Little Pig	Malware	Little Pig is a toolkit that generates malicious Microsoft Office macro code used to download additional malware onto a compromised machine when the macro is executed.	45
Loki Bot	Malware	Loki Bot is a resident loader, and password and cryptocurrency wallet stealer. Loki Bot captures passwords from browsers, as well as e-mail, FTP, SSH and poker clients.	40
Magniber	Malware	Magniber is a ransomware delivered primarily by the Magnitude exploit kit.	97
Magnitude	Exploit Kit	Magnitude is an exploit kit that has been around in some form since 2012. Threat actors most often use the kit to deliver the Magniber ransomware to targets in Asian countries.	41
MegaCortex	Malware	MegaCortex is a recent ransomware developed with the C++ programming language. The ransomware consists of two main components: the loader (executable) and MegaCortex's DLL, which is the malware's file encryptor component. MegaCortex uses batch files similar to the ones used in Goga's attacks to stop system services and applications and start the malware.	51
Metasploit	Tool	The Metasploit Framework and Metasploit Pro represent a very popular open-source and commercially supported penetration testing framework that both legitimate security professionals and threat actors use.	43
Microsoft Word Intruder	Malicious Tool	A Microsoft Word Intruder is a toolkit that generates weaponized Microsoft Word documents that download or execute a malware payload.	45
Mimikatz	Tool	Mimikatz is a tool that enables the procurement of credentials to Windows systems.	43
NanoCore	Malware	NanoCore is a remote administration tool written in .NET and used in both cybercrime and cyberespionage campaigns.	40

Name	Type	Description	Page
Nocturnal	Malware	Nocturnal is an information-stealing malware that targets many browsers and system applications. It can be administered through a Web panel.	40
OPJerusalem	Threat Campaign	OpJerusalem is a threat campaign initiated by Palestine sympathetic hacktivist threat actors.	55
Petya	Malware	Petya is a ransomware that overwrites the Master Boot Record to deny victims access to their systems and files. Petya has various aliases, including EternalPetya, NotPetya, ExPetr, Pnyetya, SortaPetya and Petna.	58
Pony	Malware	Pony (also known as Pony Loader and Fareit) is an information stealer, the main functionality of which includes the ability to collect and exfiltrate credentials and other information from an infected host. It also has the ability to act as a downloader that drops other malware.	40
PowerShell Empire	Malicious Tool	PowerShell Empire (PSE) is a PowerShell and Python post-exploitation agent.	43
RDP Brute Force Attack	Attack Type	In a Remote Desktop Protocol (RDP) brute force attack, an attacker gains access to a victim's computer by using brute force techniques which can effectively crack weak passwords. Typically, the attacker scans a list of IP ranges for RDP port 3389 (default RDP port) which are open for connection.	50
RIG	Exploit Kit	RIG is an exploit kit that has been around since 2014; although its level of activity has declined, it is still periodically seen in the wild.	40
Ryuk	Malware	Ryuk is a ransomware variant that surfaced in 2018. Attackers have used the malware in attacks against organizations across multiple industry verticals. Accenture iDefense has observed Ryuk being delivered after an initial Trickbot infection on victim systems. The malware has code overlap with the Hermes ransomware, which the NEEDLEFISH threat group uses.	53

GLOSSARY

Name	Type	Description	Page
Silence	Malware	Silence is a modular backdoor used by Contract Crew (also known as Silence) to proxy malicious traffic into internal network segments and monitor user activities by taking screenshots of computer activities. The Silence Downloader downloads and installs the Silence backdoor.	43
Silence Downloader	Malware	Silence Downloader is a malware family used by the Contract Crew (also known as Silence) threat group to download the Silence malware.	46
Snatch	Malware	Snatch is a ransomware variant used in an affiliate program operated by the threat actor BulletToothTony.	57
Threadkit	Exploit Kit	Threadkit is an Office document exploit builder kit that supports a variety of recently released exploits, including those for the CVE-2018-4878, CVE-2018-0802, CVE 2017-11882, CVE-2017-8759, CVE-2017-8570 and CVE-2017-0199 vulnerabilities.	41
Troldesh	Malware	Troldesh is a ransomware first spotted in early 2015. The ransomware is also known as Encoder.858 or Shade.	51
Underminer	Exploit Kit	Underminer is an exploit kit that targets Asian countries and is known to deliver a bootkit or a cryptocurrency miner malware.	41
Yatron	Malware	Yatron is a full-feature ransomware with the ability to encrypt drives, spread itself, remain persistent and impose time limit restrictions.	53



CONTACTS

Joshua Ray

Managing Director, Accenture Security | joshua.a.ray@accenture.com

Josh Ray is Managing Director for CyberDefense across Accenture Security globally. Josh has 18 years of combined commercial, government and military experience in the field of cyberintelligence, threat operations and information security. He holds a Bachelor of Science degree in information technology from George Mason University, an Executive Certificate in strategy and innovation from MIT Sloan School of Management and served honorably as a member of the US Navy.

Howard Marshall

Associate Director, Accenture Security | howard.marshall@accenture.com

Howard Marshall focuses on intelligence operations for Accenture iDefense. Prior to joining, Howard was FBI Deputy Assistant Director of the CyberReadiness, Outreach, and Intelligence Branch. He holds a Bachelor of Arts degree in Political Science and a Juris Doctorate from the University of Arkansas.

Rob Coderre

Senior Manager, Accenture Security | robert.c.coderre@accenture.com

Rob Coderre specializes in Product Management for the Accenture iDefense Security Intelligence Services. Previous roles include consulting, channel development, sales engineering and product management for emerging technical markets. He holds a Bachelor of Science degree in aerospace engineering from the University of Notre Dame and is an active CISSP and member of ISSA.

CONTACTS

Valentino De Sousa

Security Senior Principal | valentino.de.sousa@accenture.com

Valentino De Sousa leads Accenture iDefense in Europe and Latin America and CyberDefense in the United Kingdom and Ireland. Previous roles include leading different threat intelligence teams responsible for malware analysis, research and development, analysis of adversaries, active campaigns and leading indicators of impending attacks. He holds a Bachelor of Science in business administration from the American University of Rome and a Master of Science in terrorism studies from the University of East London.

Emily Cody

Senior Manager, Accenture Security | emily.a.cody@accenture.com

Emily Cody has 14 years of experience in business development and marketing for FTSE 30 and professional services organizations. Prior to joining Accenture, Emily was a Business Account Lead at PwC and Business Development Lead for France and Germany at BAE Systems.

Jayson Jean

Senior Manager, Accenture Security—iDefense Business
jayson.jean@accenture.com

Jayson Jean is Director of Business Operations for Accenture iDefense in North America and APAC, with responsibility for business development of the CyberThreat Intelligence portfolio. Prior to this role, Jayson has 14 years of experience building the strategic direction and leading product development for Vulnerability Management at Accenture iDefense.

Contributors

Patton Adams, Kiran Bandla, Matthew Brady, Kellie Bryan, Brandon Catalan, Cole Dunn, Rikki George, Roya Gordon, Christopher Kolling, Deapesh Misra, Rohit Mothe, Mei Nelson, Nellie Ohr, Meredith Pratico, Bryan Richardson, Nancy Strutt, Thomas Willkan, Curt Wilson and Michael Yip.

CONTACT US

Josh Ray

Managing Director, Accenture Security
joshua.a.ray@accenture.com

Howard Marshall

Associate Director, Accenture Security
howard.marshall@accenture.com

Rob Coderre

Senior Manager, Accenture Security
robert.c.coderre@accenture.com

Visit us at www.accenture.com



Follow us @AccentureSecure



Connect with us

© 2019 Accenture. All rights reserved. Accenture, the Accenture logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of Accenture and its subsidiaries in the United States and in foreign countries. All trademarks are properties of their respective owners. All materials are intended for the original recipient only. The reproduction and distribution of this material is prohibited without express written permission from Accenture iDefense.

Given the inherent nature of threat intelligence, the content contained in this report is based on information gathered and understood at the time of its creation. The information in this report is general in nature and does not take into account the specific needs of your IT ecosystem and network, which may vary and require unique action. As such, Accenture provides the information and content on an “as-is” basis without representation or warranty and accepts no liability for any action or failure to act taken in response to the information contained or referenced in this report. The reader is responsible for determining whether or not to follow any of the suggestions, recommendations or potential mitigations set out in this report, entirely at their own discretion.

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world’s largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 482,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

ABOUT ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organization’s valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit the Accenture Security blog.