accenturesecurity

2019

CYBER THREATSCAPE REPORT

EXECUTIVE SUMMARY

CONTENTS

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 a 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.

EXECUTIVE SUMMARY

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.

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.

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.

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 the full 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.

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.

A SECURITY PIVOT

- **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.

CONTACTS

Joshua Ray
Managing Director, Accenture Security I 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 I 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 I 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.

Valentino De Sousa
Security Senior Principal I 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 impeding 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 I 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 Prattico, 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

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.