accenture

2020 CYBER THREATSCAPE REPORT

Executive Summary

Accenture Security

CONTENTS

2020 OBSERVATIONS

In the past year, security strategies and practices have been tested like no other. Rapidly accelerated digital transformations, opportunistic phishing campaigns, discontinuity of information security operations and financial constraints are creating the perfect storm in a COVID-19-disrupted world. CISOs who understand these challenges and can pivot their security approach can help their organizations to emerge stronger.

Accenture Cyber Threat Intelligence (Accenture CTI) has been creating relevant, timely and actionable threat intelligence for more than 20 years. Now, following the acquisitions of Context[1] in March 2020 and Seattle-based Security of Things company, Deja vu Security[2] in June 2019, Accenture Security has gained an additional 20 years' intelligence reporting and deep expertise in the techniques, tools and methods for securing connected devices and Internet of Things (IoT) networks. The cyber threat intelligence team, referred to in this report as Accenture CTI, provides T security and business operations with actionable and relevant decision support.

Since our last report in 2019[3], our cyber threat intelligence and incident response teams have investigated numerous cases of suspected cyber espionage and financially-motivated targeting. During these investigations, threat intelligence analysts and incident responders have gained first-hand visibility of the tactics, techniques and procedures (TTPs) employed by some of the most sophisticated cyber adversaries.

Our track record of experience serves us well as we unravel the changes in cybersecurity threats in the last 12 months[4]. Early in 2020, due to the COVID-19 pandemic, most businesses across the globe found they needed to shift quickly to remote work—some did so according to a plan, others reacted but not according to their plan, and still more did not even have a plan. Remote work has challenged enterprise security monitoring in numerous ways from the platforms used for communication to the devices people are using and networks on which they transmit data. We have seen an increase in social engineering opportunities as cyberespionage and cybercriminal groups attempt to take advantage of vulnerable employees unfamiliar with managing their technology environments. The worldwide, economic and business disruptions have put tremendous financial challenges on businesses. Those pressures inevitably flow down to information security operations to maintain or increase coverage under ever-tighter budgetary constraints.

[1] Accenture Acquires Context Information Security, a UK-Based Cybersecurity Consultancy, March 06, 2020. https://newsroom.accenture.com/news/accenture-acquires-context-information-security-a-uk-based-cybersecurity-consultancy.htm

[2] Accenture Acquires Deja vu Security, Seattle-Based 'Security of Things' Company, June 17, 2020. https://newsroom.accenture.com/news/accenture-acquires-deja-vu-security-seattle-based-security-of-things-company.htm

[3] 2019 Cyber Threatscape Report, Accenture, 2019. https://www.accenture.com/gb-en/insights/security/cyber-threatscape-report

[4] Research was conducted between June 2019 and June 2020.

Sophisticated threat actors are employing new TTPs to help achieve their long-standing objectives of regime survival, economic acceleration, military superiority, information operations and cyber espionage. As we detail later in this report, our threat intelligence analysts have seen adversaries develop new implants for use against Outlook Web Access (OWA) and Exchange environments, and more sophisticated command and control methods that attempt to disrupt detection efforts through internal proxy mechanisms.

Criminals will still work to monetize access to data or networks, perhaps more frequently than before as the economy continues to be vulnerable. As we have seen this year, supply chain compromise and off-the-shelf tools could feature heavily, as could ongoing evidence of custom tools designed to evade defenses.

Ransomware has increased in popularity among bad actors, as data theft increases the pressures on victims. With game-changing ransomware attacks, such as the Maze threat[5], the name-and-shame technique has gained momentum that calls into question the cost versus disruption debate.

In such a climate, and with organizations attempting to stabilize their current operations, CISOs should put the right controls in place to create a safe and secure environment. Accenture has identified **four elements of adaptive security** that can help: a secure mindset, secure network access, secure work environments and secure collaboration. CISOs should engage with business leaders to plan, prepare and practice for greater cybersecurity resilience, backed by the right resources and investments. Accenture believes a multi-dimensional crisis management strategy, with many work streams and teams that collaborate closely, often on a daily basis, is the way to help achieve cybersecurity resilience—and can help to protect enterprises from harm.

Read on to take a deeper dive into the five frontline trends identified in 2020. These insights can enhance the work of security teams and put security technology investments, security processes and the business strategy on a firm footing to help achieve the desired level of cyber resilience.

[5] Abrams, Lawrence. "Allied Universal Breached by Maze Ransomware, Stolen Data Leaked," Bleeping Computer, November 21, 2019. https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/

FIVE FRONTLINE TRENDS

The 2019 Cyber Threatscape report noted that strong investment in cybersecurity was not lacking. But despite these investments, good threat intelligence was a priority to tackle the relentless pressure from cybercriminals and nation-states and the gaps in the cyber defense posture of suppliers, partners and acquisitions.

Now, the **2020 Cyber Threatscape report** reveals five factors that are influencing the cyberthreat landscape:

01 COVID-19 ACCELERATES THE NEED FOR ADAPTIVE SECURITY

There is no quick fix to the issues presented by the global pandemic. Even as society and business manage the health and humanitarian aspects, organizations need to deal with the economic and operational fallout, which is creating financial and budget challenges for companies' information security operations in the mid- to long-term. The pandemic has opened the door to opportunistic threats, creating social engineering opportunities such as new phishing campaigns. It has also put unprecedented pressure on organizations as they struggle with business continuity, travel restrictions and remote working. As data continues to be seen as a high value, sought after commodity, security leaders should consider embracing adaptive security[6]—putting the right controls and monitoring in place to help create a safe and secure working environment for their enterprise.

[6] Emerge stronger with adaptive security, Accenture, June 2020. https://www.accenture.com/gb-en/insights/security/coronavirus-adaptive-security

02 NEW, SOPHISTICATED TTPS TARGET BUSINESS CONTINUITY

Established platforms are observed to be under siege as sophisticated cyberthreat actors have aggressively targeted systems supporting Microsoft Exchange[7] and OWA, such as Client Access Servers (CAS). Such compromises are a breeding ground for malicious activities. Web-facing, data-intense systems and services that typically communicate externally can make it easier for adversaries to hide their traffic in the background noise, while authentication services could open up a credential harvesting opportunity for cybercriminals. Attacks against such platforms are not always pretty—they can range from crude, to simple, to sophisticated, especially as threat actors are evolving their techniques to exploit such vulnerabilities all the time. Recent campaigns against government entities have involved newly-designed malware families configured with internally-routable command and control infrastructure, likely also designed for evasion. These kinds of innovation can challenge network defenders. State-aligned operators could continue—in most cases—to need to emphasize stealth and persistence to meet their intelligence-gathering goals. Such capabilities and detection evasion approaches underline the importance of identifying and tracking priority adversaries and then threat hunting against the specific behaviors employed by the priority adversaries.

[7] Accenture CTI internal research

03 MASKED OR NOISY CYBERATTACKS COMPLICATE DETECTION

Cyberthreat actors routinely chain together off-the-shelf tools with living-off-the-land techniques—a phrase describing the creative abuse of readily available tools—complicating detection and attribution. Since off-the-shelf tools offer the benefits of deniability, continued effectiveness and ease of use, their accelerated use is likely to continue for the foreseeable future. Spear phishing has stepped up a gear, too. Recognized threat groups have targeted government organizations and corporations, leading to the theft of information. These activities have occurred in Europe, North America and Latin America, and there has been significant activity directed towards emerging economies and India. And threat actors—increasingly, organized cybercriminal groups—continue to try to compromise their victims' supply chains. Managed service providers and software vendors are being targeted but the direct connectivity between peer organizations working on joint projects is also being exploited. Continuous and bespoke threat intelligence tailored for the specific organizational profile is a priority—from strategic to tactical and technical—as is an intelligence-led security approach that focuses on the most important mitigations for identified adversaries. Organizations should ensure they understand the commonly used tools and techniques, especially those involving malicious use of native systems and penetration test tools, and validate they can be detected in their environment.

04 RANSOMWARE FEEDS NEW PROFITABLE, SCALABLE BUSINESS MODELS

Alongside finding new ways to infect businesses with ransomware, threat actors are finding new ways to influence victims to pay. In November 2019, a new, game-changing strain of ransomware known as Maze infected a large security staffing company, stole company data, and notified the media—eventually publicly releasing 700MB of data when the ransom was not paid[8]. This "name and shame" approach adds pressure on victims to pay up, even though law enforcement and the cybersecurity industry have always advised against paying ransoms. Only threat actors are profiting—ransomware recovery responders, Coveware, noted that in the first quarter of 2020 an average ransom payment rose to US$178,254 up 60 percent from the same period the year before[9]. The situation could become far worse. As threat actor profits increase, they can innovate and invest in more advanced ransomware, and take advantage of the greater vulnerabilities of remote working. Accenture expects threat actors employing these tactics to continue to evolve and proliferate for the remainder of 2020 and beyond.

[8] Abrams, Lawrence. "Allied Universal Breached by Maze Ransomware, Stolen Data Leaked," Bleeping Computer, November 21, 2019. https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/

[9] Ransomware Attacks Fracture Between Enterprise and Ransomware-as-a-Service in Q2 as Demands Increase, Coveware, August 3, 2020. https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report

05 CONNECTEDNESS HAS CONSEQUENCES

As more critical systems are exposed and greater connectivity is enabled as a result of powerful technologies and the Internet attackers are finding new ways to exploit them. Increasingly, businesses are using unpatched and untested devices—which pose a much more realistic and accessible target. Cloud and Internet-connected devices are far more widespread. Security leaders are fighting back, using public bug bounty programs and detection frameworks, but Operational Technology (OT) threats still prompt the need for more effective security controls. Security testing can be expensive—and it is difficult to assess the risk posed by each device, with dramatic differences in device security testing between small and large manufacturers. Slowly but surely threats are being identified and remedied. As detailed in this report, this year saw an increase in the number of OT vulnerabilities reported by researchers, which were addressed by vendors with patches. Many of the common classes of vulnerabilities affecting IoT devices have been at least partially solved, and now the challenge is applying this knowledge wherever applicable. Going forward, security leaders should share this knowledge and develop standardized systems that are simple, easy to integrate, and bear close scrutiny.

In this report, Accenture CTI offers leading practices to help tackle these frontline trends and introduce adaptive security measures that can secure mindsets, network access, work environments and collaboration.

Accenture CTI aims to help its clients, partners and community members by providing this information to help them stay ahead of relevant threats to their businesses, industries and geographies.

A FLEXIBLE FUTURE

A year ago, no one could have predicted the impact of the health and humanitarian crisis that has gripped our world during 2020. Nor could we have foreseen how such unprecedented circumstances would open the door to innovative cybercrime. And as cyberattackers prey on the susceptibility of newly remote workers by offering lures and traps that imitate credible sources, Security Operations Centers find they need to tap into tactical, operational and strategic threat intelligence to identify trends and technologies that threaten business continuity.

Organizations can adapt and take steps to a more flexible and secure future if they:

Think "anytime, anywhere"

Secure all users, devices, and network traffic consistently with the same degree of effectiveness, regardless of where they are based. Remember that secure network access and applications are just as fast with security as they are without.

Be transparent

Give users access to what they need when they need it. Make these changes transparent to them—without asking them to "jump through hoops" to do their job effectively.

Inspire calm and confidence

Make security leaders the catalyst for change, using empathy and compassion to deliver a more agile response. Employing adaptive security creates confidence; for instance, organizations can use the cloud or expand access to more remote users.

Where possible, simplify

Consider managed services and automate where it makes sense. For instance, security event response, tool deployment, and rule management, can benefit from limited human intervention.

Build for resilience

As organizations look to emerge stronger, business continuity and crisis management plans must be fit for purpose. Business leaders should expect more frequent crises. They need to transform how they think about security. Is it really cost-effective to do everything in-house? Should they leverage a global player to secure their ecosystem? Engage with business leaders to plan, prepare and practice for greater cybersecurity resilience, backed by the right resources and investments.

By putting such measures in place, organizations can outmaneuver uncertainty, emerge stronger from crises, and gain greater cyber resilience.

ABOUT THE REPORT

The 2020 Cyber Threatscape report presents key findings from research by the Accenture cyber threat intelligence team, with significant contributions from some of our recent acquisitions, including Context and Deja vu Security. It covers cyberthreat trends the Accenture CTI team has observed and analyzed from June 2019 until June 2020. It provides an overview of the trends and how Accenture CTI believes they might evolve and grow throughout the year.

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 cyber threat intelligence from Accenture. 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 2020 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.

CONTACTS

Joshua Ray

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

Josh Ray is Managing Director for Cyber Defense across Accenture Security globally. Josh has more than 20 years of combined commercial, government and military experience in the field of cyber intelligence, 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 United States Navy.

Scott Bachand

Global Intelligence Director & Strategy Lead
scott.bachand@accenture.com

Scott directs product strategy, provides research oversight and manages the operations of Accenture CTI globally. Prior to joining Accenture, Scott served as the Chief Technical Officer of Mission Cyber at Accenture Federal Services. He served in the United States Air Force, where he completed a distinguished career, retiring as the Technical Director of Operations of US Cyber Command (USCYBERCOM).

Jayson Jean

CTI Business Development Lead
jayson.jean@accenture.com

Jayson Jean is Director of Business Operations for Accenture CTI in North America and the Asia Pacific region, with responsibility for business development of the Cyber Threat 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 CTI.

Howard Marshall

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

Howard Marshall is Managing Director for Cyber Threat Intelligence and leads the business globally. Prior to joining, Howard was FBI Deputy Assistant Director of the Cyber Readiness, Outreach, and Intelligence Branch. He holds a Bachelor of Arts degree in Political Science and a Juris Doctorate from the University of Arkansas.

Valentino De Sousa

Europe & Latin America CTI Lead
valentino.de.sousa@accenture.com

Valentino De Sousa leads Accenture CTI in Europe and Latin America. 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.

Simon Warren

Business Development, Accenture Security
simon.warren@accenture.com

Simon leads Business Development for Accenture CTI in Europe and Latin America. Prior to this role, Simon led the Accenture CTI practice in Australia. Before joining Accenture, Simon spent more than 10 years with the military.

Contributors

Patton Adams, Omar Al-Shahery, Joseph Chmiel, Amy Cunliffe, Molly Day, Oliver Fay, Charlie Gardner, Gian Luca Giuliani, Samuel Goddard, Larry Karl, Paul Mansfield, Hannaire Mekaouar, Mei Nelson, Nellie Ohr, and Kathryn Orme.

About Accenture

Accenture is a leading global professional services company, providing a broad range of services in strategy and consulting, interactive, technology and operations, with digital capabilities across all of these services. We combine unmatched experience and specialized capabilities across more than 40 industries—powered by the world's largest network of Advanced Technology and Intelligent Operations centers. With 506,000 people serving clients in more than 120 countries, Accenture brings continuous innovation to help clients improve their performance and create lasting value across their enterprises.

Visit us at **www.accenture.com**

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence.

Follow us @AccentureSecure on Twitter or
visit us at **www.accenture.com/security**

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.

www.accenture.com