Booz | Allen | Hamilton®

2021 CYBER THREAT TRENDS OUTLOOK

CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER

CONTENTS

The year 2020 has been unlike any we have experienced, and this is true with regard to cyber threats, too. If this year has taught us anything, it is the importance of preparing for known threats. In the span of a few weeks, our economy, education systems, and lifestyles were altered by a scenario that experts had long been warning about. Yet, as we all faced the new realities of the pandemic, the world continued to move forward with advances in technology and markets.

Cyber threats are increasing in both scope and frequency. From ransomware operators refining and polishing their business models, to the rapid adoption of cloud as organizations seek to gain operational efficiencies, attack surfaces are expanding, and threat actors are evolving. In this time of both change and adjustment, the Cyber Threat Trends Outlook explores what is known about key cybersecurity issues that lie ahead.

We open with a scene that is far too easy to imagine playing out in the coming year but that every business leader hopes never to experience. The scene features Dakota Alexander, the fictional CEO of a *Fortune* 500 company, managing the fallout after a front-page breach to her enterprise. She is joined by Arnie Weir, a powerful board member for her organization. Together they are flying to testify to a congressional committee on the recent breach. Though fictitious, this account is all too plausible given the current cyber threat landscape.

FLIGHT

by P.W. SINGER

She drained the incredibly small cup in one sip. As a CEO, she was not used to sitting in the last row in coach, but it was necessary for the sake of appearances. She was on her way to Washington, DC, to brief members of the congressional committee who requested her testimony.

Thinking back, it had been both a needed technical migration and a cost-savings move, all timed around a communications strategy to excite the market right before the third-quarter analyst call. Around the same time that Dakota had revealed on Twitter that the company would be migrating to a cloud-based infrastructure, a system administrator had touted on LinkedIn that he got a new job at the company. All it had taken was a single opened spear phishing email to that new administrator, posing as an invitation to a corporate family barbeque for new IT employees, and the hackers were inside the company's enterprise network.

As Dakota did the media and shareholder circuit over the next weeks, talking about the new post-COVID-19 model of remote work and "doing more with less," the hackers had worked their way through the corporate network, monitoring traffic and moving laterally from one system to another.

The rush to migrate all the systems by the end of the fiscal year had meant a mad dash, with Dakota herself driving the team to the edge of what was possible. There was grumbling about the new CEO making people work weekends, but in the end, they'd made it. And the market loved it.

The logs that the chief information security officer (CISO) later showed her revealed the hackers had achieved a different kind of win on the very same date. During the transition, they'd harvested the cloud credentials.

And then the cyber criminals dropped the hammer. A massive release of data.

The hackers had left a message in Dakota's inbox, sent from inside the network. The public dump had just been a proof case. Unsaid was that it would also keep her company off balance, busy putting out fires while the real operation kicked in.

The hackers messaged that they had the ability to lock down the entire Research and Development team's data with ransomware. Dakota brought the chief financial officer (CFO) into the discussion to help assess the risk; plus, he'd ultimately have to be the one to approve any payments to the criminal organization. The CFO estimated there was well over $120 billion in future revenue at stake. The company could maybe restore and replace the files, but given how deep the hackers were in, they couldn't be 100% sure of that. And, if the company did get the data lake back up, they couldn't be certain that nothing had been corrupted in the weeks the hackers sat in there, the zeros and ones inside tests, records, or product designs unknowingly altered.

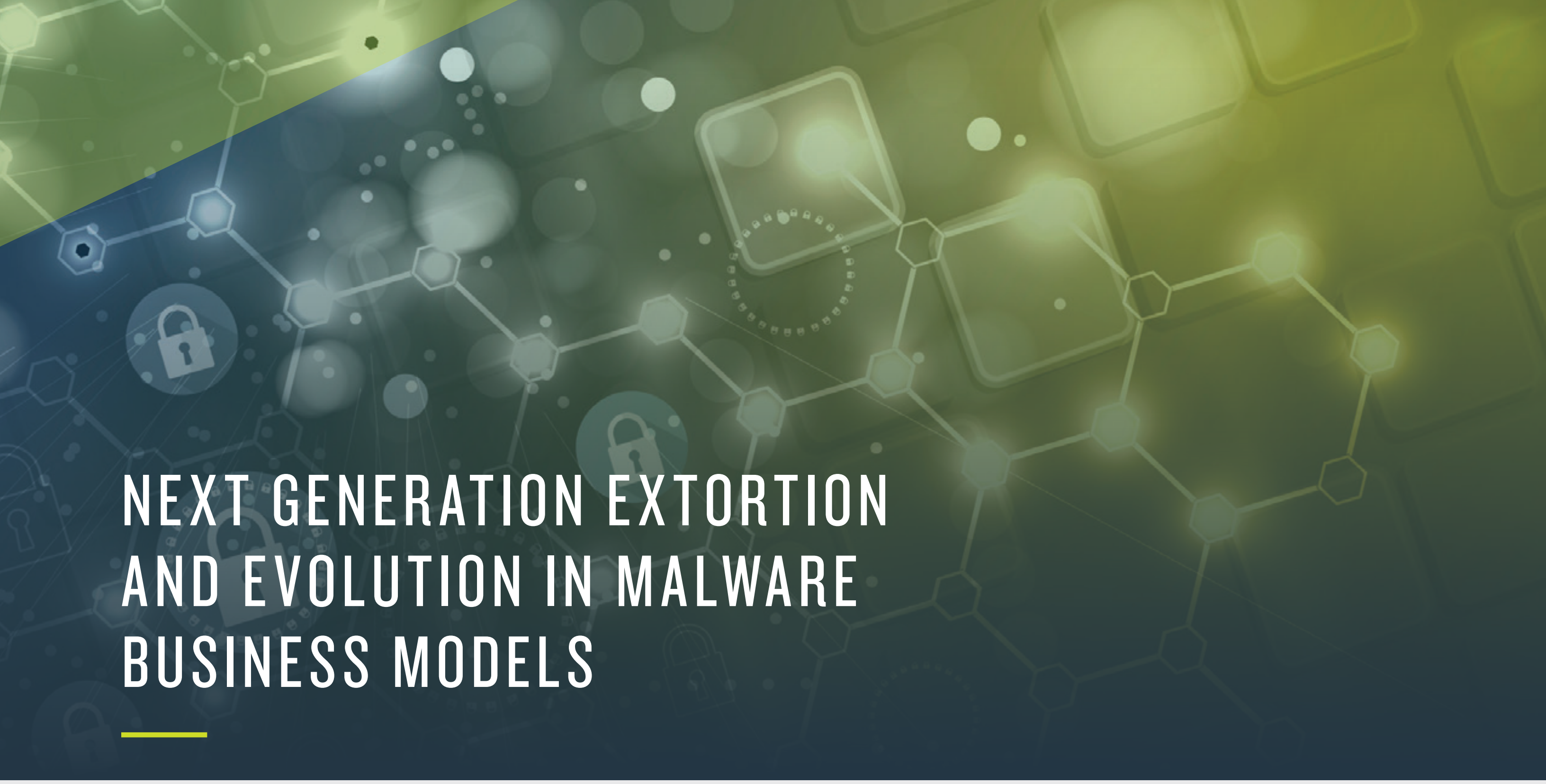
The biggest "what if" took her mind back to business school. The hacking had all played out on new technology, but none of it had really been a technology issue. It was actually all about strategy and employee education. What if she'd made sure the whole organization focused on getting the basics down first, rather than the theater of transformation?

A board member had recently told to her, "You don't have to outrun the bear, only the other guy running from it."

That wasn't true either. She knew that now. It wasn't about keeping a step ahead of some other company, so that some other CEO would be the one to fly coach. When you have something valuable, the bear will just keep running after you.

Her finger tapped the cup's thin rim, thinking over what she'd have to do to keep her job and be the one that actually got to implement these hard-earned lessons. Maybe the crisis management plan would work. Maybe it wouldn't. The next hours would tell.

She looked over her opening statement script one more time. If she was still CEO by tomorrow, she knew there would have to be sweeping changes to her company's security program, with an emphasis on proactive preparedness. Never again would she be caught off guard!



NEXT GENERATION EXTORTION AND EVOLUTION IN MALWARE BUSINESS MODELS

Cybercriminals inspired by the successes of innovative extortion tactics by ransomware operators will double down on their experimentation with ransomware business models and cybercriminal business ventures, further professionalizing and developing this formerly amorphous subset of crime:

Ransomware operators are likely to spend more time in the networks of their targets and attempt to hit multiple organizations simultaneously to drive higher payouts at a faster pace.

Criminal organizations deploying ransomware-as-a-service (RaaS) will adapt their business models to accommodate exceedingly limited engagements with a smaller and more thoroughly vetted customer base.

2020 WAS A REVOLUTIONARY YEAR FOR RANSOMWARE TACTICS

THE TRULY AMBITIOUS CYBERCRIMINAL MAY SPEND THE ADDITIONAL TIME TO COMPROMISE AN ENTIRE NETWORK OF COMPANIES, STRIKE ALL OF THEM AT ONCE, AND DEMAND A SINGLE LARGE RANSOM PAYMENT FROM THE ORIGINATING COMPANY TO PROVIDE THE DECRYPTION KEYS.

Refinement of the Data-Dump Strategy

The tumultuous year of 2020 has seen the popularization of extortionist ransomware tactics, particularly from the Maze and Sodinokibi ransomware operators, in which organizations not only are compromised and their data held for ransom but also are further threatened with data theft and public disclosure. These bad actors have continued to develop their tactics, threatening to send notifications to regulatory bodies and even stock exchanges, detailing the victims they have breached, all in an attempt to force faster and higher payments.

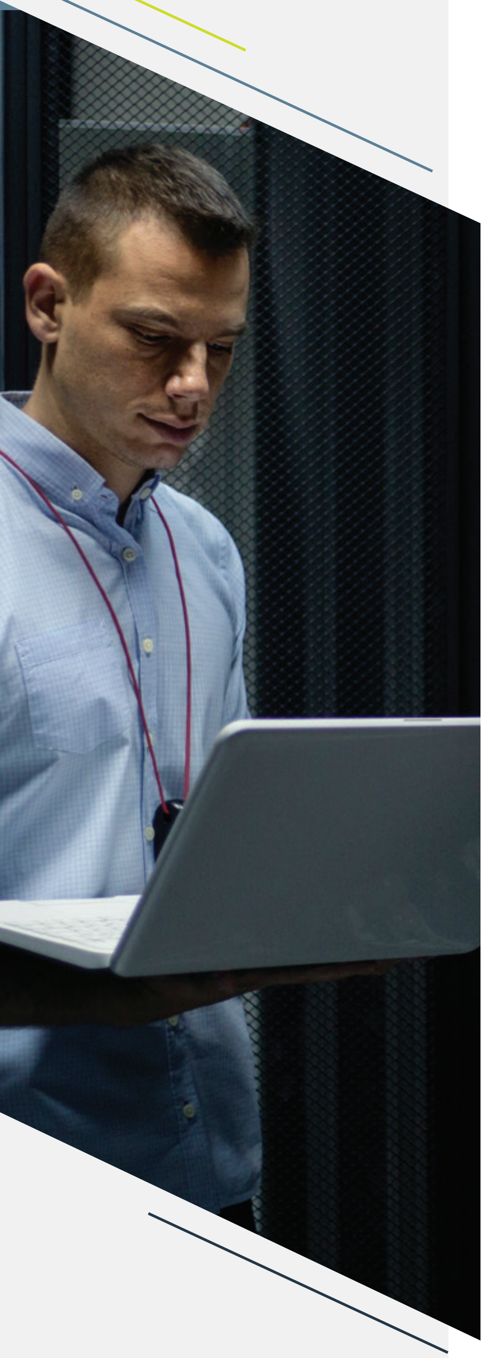
Further refinement of tactics used by ransomware operators is likely to include threats against third-party data, suppliers, customers, and other relational targets. For instance, a manufacturing company may find its proprietary data leaked and may even serve as the springboard for attacks on vendors and partners. The truly ambitious cybercriminal may spend the additional time to compromise an entire network of companies, strike all of them at once, and demand a single large ransom payment from the originating company to provide the decryption keys.

RaaS Model May Evolve to Include New Financing Mechanisms

One ongoing trend that is likely to evolve is the RaaS model. While this model reached a previous apoapsis with the Angler exploit kit and other crimeware-as-a-service offerings between 2014 and 2016, recent years have shown that the model has remained attractive and profitable, if not very publicly visible. Future developments are likely to include custom RaaS operations, in which would-be cybercriminals without the technical expertise can commission malware, tools, or even entire frameworks. These would likely be paid from a portion of the proceeds of such activity, which would nominally constrain this work to solely ransomware engagements, though well-resourced cybercriminals are likely to desire the purchase of tools and malware for their own use via lump-sum payments.

This may lead to the emergence of new financing mechanisms for criminal operations. Cybercriminals have discussed, in open forums, proposals to create a venture capital organization or stock market of sorts, where interested parties can finance the development of malware, tools, and frameworks without ever writing a line of code. The returns on these investments are likely to be handsome, as some recent ransom payments have shown. Recent targeted ransomware payments have averaged between $1 million and $2 million, with some payments exceeding even these generous figures. For cybercriminals without a diverse skill set, or a malicious insider looking for the means to garner a significant payout, these would provide the means and motive, along with a healthy financial payout, to drive the growth of these new models.

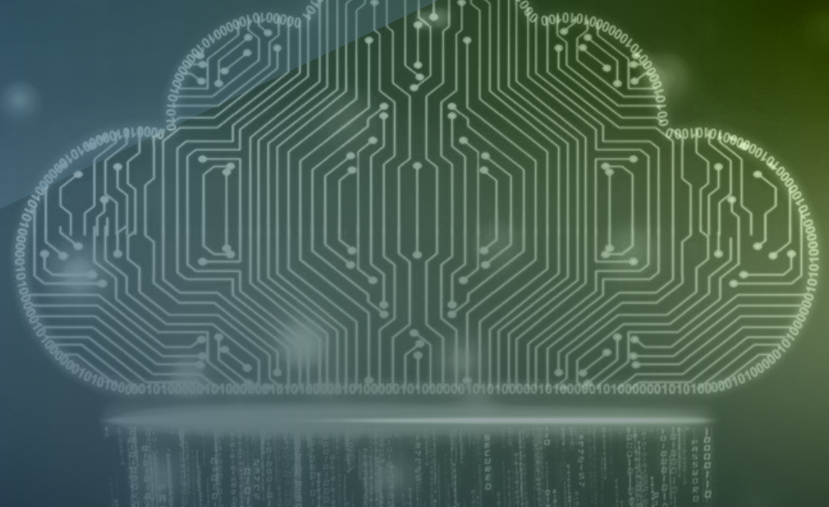
Not all business models are successful, and even carefully researched investments are never guaranteed to deliver a strong return. What is guaranteed to be successful is the malware-as-a-service operator, because the work of those operators has always been in strong demand and has commanded a hefty premium. For the best of the best, from the days of the Angler exploit kit to the Golden Chickens RaaS, the returns are enough to justify further malicious activities. At the very least, Booz Allen expects that cybercriminals and cybercriminal organizations will attempt to innovate and drive the next big thing in malware business models. Undoubtedly at least some of these experiments will yield fruit.



ESSENTIAL MITIGATION STRATEGIES

Organizations should:

- Institute a patching policy that ensures that critical vulnerabilities and the associated patches are identified and deployed monthly
- Implement two-factor authentication (2FA) on all accounts, from admin to user
- Disable PowerShell via group policy object (GPO) on machines where it is not required for day-to-day operations
- Implement an aggressive backup strategy that includes both onsite and offsite backups
- Develop comprehensive ransomware playbooks and runbooks
- Implement scheduled (annually at a minimum) tabletop and wargaming exercises to test these responses
- Establish retainer relationships with an outside incident response firm and outside counsel that will clear a response path
- Establish an internal or external hunt program that will identify suspicious network activity and action alerts
- Conduct a thorough review of the cyber insurance policy to understand what mitigation and remediation activity is covered (some policies have "Betterment" clauses that can assist with mitigation strategies).



BUILDING CASTLES IN THE CLOUD

SUPPLY CHAIN ATTACKS VIA CLOUD-HOSTED DEVELOPMENT ENVIRONMENTS

Booz Allen expects threat actor interest in targeting platform-as-a-service (PaaS) solutions—particularly cloud-based development environments—to rise as a potential vector for conducting supply chain attacks:

Historically, threat actors have targeted shared libraries, software development kits (SDK), and integrated development environments (IDE) as a means to conduct widespread attacks, inserting malicious code into otherwise benign applications.

As cloud-hosted development environments become more popular, these solutions may attract the same illicit activity that other development tools and resources have seen in previous attacks.

A CLOUD THREATS PRIMER

Cloud computing has revolutionized the way organizations of all sizes and across nearly every industry have designed their information technology (IT) infrastructure. Though each allows for cheap and rapid deployment of IT resources, the types of cloud computing solutions vary, and categories include software-as-a-service (SaaS), which provides fully functional applications with no management by the consumer (e.g., webmail or cloud storage apps); PaaS, typically used to develop or deploy customized applications, with the customer managing some software, but not the underlying host and infrastructure; and infrastructure-as-a-service (IaaS), with a service provider managing the underlying physical or virtual infrastructure, and the customer managing everything from the hosted operating system up.

The widespread adoption of cloud computing services has been the source of significant benefits and high-profile missteps and abuses. As organizations have migrated from in-house servers to IaaS hosting, misconfigured access controls have exposed millions of database records,[1] or left the door open for attack by threat actors deploying ransomware or cryptominers.[2] Further, threat actors of all stripes make use of SaaS solutions to help evade detection by hosting malware payloads on cloud-storage[3] service or exfiltrating data from compromised hosts via messages to accounts on widely used webmail.[4]

Booz Allen expects the types of attacks abusing cloud solutions to continue to evolve, possibly including the convergence of several known tactics used in software supply chain attacks to target PaaS solutions used to develop and deploy software applications.

COMPROMISE AT THE SOURCE

Targeting the tools and resources used throughout the software development lifecycle is a well-established tactic used by threat actors for inserting malicious code into otherwise benign applications. These attacks can include inserting code into widely used software libraries, SDKs, or IDEs, which bring together libraries, compilers, and other development tools into a single platform. Several recent examples of attacks against development resources have included a campaign reported by GitHub in late May 2020, in which threat actors had inserted "Octopus Scanner" malware into at least 26 open source Apache NetBeans repositories; NetBeans is an IDE used for Java applications.[5] Similarly, researchers reported a campaign leveraging supply chain attacks to compromise a compilation environment tool used by Chinese developers, which was used as an attack vector to ultimately deliver ransomware.[6]

A VIABLE ATTACK PLATFORM

PaaS solutions have been abused by threat actors to achieve several nefarious objectives. Some of the most recent incidents have used PaaS services to obfuscate command and control (C2) infrastructure or redirect users of a targeted service to malicious infrastructure. In March 2020, researchers reported that the BlackWater malware was observed using Cloudflare

[1] https://www.comparitech.com/blog/information-security/microsoft-customer-service-data-leak/

[2] https://redlock.io/blog/cryptojacking-tesla

[3] https://research.checkpoint.com/2020/guloader-cloudeye/

[4] https://twitter.com/JaromirHorejsi/status/927818231498313730

[5] https://securitylab.github.com/research/octopus-scanner-malware-open-source-supply-chain

[6] https://blog.360totalsecurity.com/en/panther-ransomware-strikes-again/

AS ORGANIZATIONS HAVE MIGRATED FROM IN-HOUSE SERVERS TO IAAS HOSTING, MISCONFIGURED ACCESS CONTROLS HAVE EXPOSED MILLIONS OF DATABASE RECORDS, OR LEFT THE DOOR OPEN FOR ATTACK BY THREAT ACTORS DEPLOYING RANSOMWARE OR CRYPTOMINERS.

Workers—a PaaS product used to speed up web applications by distributing instances across sites on the Cloudflare Edge Network—as intermediate C2 servers, thus obscuring the true origin of the attack and limiting victims' ability to block malicious traffic without potentially disrupting other legitimate services.[7] In addition, in July 2020, a company providing cloud communication platform-as-a-service (CPaaS)—a service used by developers to integrate communications features into their applications—reported that a JavaScript library used by one of their routing engines had been maliciously updated; the library was accessed on a misconfigured cloud storage server, and updated with JavaScript that redirects users to a malicious URL likely used to gather information from and serve malvertising to mobile devices.[8]

Looking forward, Booz Allen notes that cloud-hosted development environments—including cloud-IDE as well as other development tools—may provide point of convergence for known threat actor tactics with a new and increasingly popular technology. Cloud-IDEs provide many of the same features of traditional IDEs, while reducing the burden of managing disparate requirements for various software development projects.[9] As the popularity of cloud-based development tools increases, attacks against these tools—such as modifying resources used by the PaaS service or otherwise compromising the PaaS provider—could allow threat actors a means of reaching a large collection of developers, and even larger number of victims using those developers' applications.

[7] https://www.bleepingcomputer.com/news/security/blackwater-malware-abuses-cloudflare-workers-for-c2communication/

[8] https://www.twilio.com/blog/incident-report-taskrouter-js-sdk-july-2020

[9] https://medium.com/better-programming/my-favorite-cloud-ides-e6afaa94d96b

MITIGATIONS

Security controls that may help end users of potentially compromised applications as well as developers that may incorporate cloud-based development environments into their workflow include the following:

- Organizations can protect against software supply chain attacks by deploying endpoint detection and response (EDR) tools that may detect anomalous or suspicious behavior by applications, including those normally believed to be trustworthy.[10]
- Controls such as application allowlisting can be used limit the applications available in a corporate environment to those developed by trusted vendors that have a specific business use; however, if a trusted vendor is compromised, allowlisting would not necessarily protect against malicious updates to the trusted application.
- Software developers should make extensive use of code signing to secure software components (including configuration files, scripts, and packages) and check digital signatures of imported libraries or updates. Code signing keys should be stored to prevent rogue users of the development environment signing malicious code.
- Developers should secure their development environments by applying strict access controls and ensuring prompt deployment of patches; when using cloud-hosted development tools, organizations may consider a private-cloud deployment model to provide additional control over the environment.

[10] https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/supply-chain-malware

AI, EVASION, AND THEFT

THE NEXT STEPS IN “INTELLIGENT” CYBERCRIME

As artificial intelligence (AI) revolutionizes the services available across nearly all industries, advanced threat actors will prioritize attacks that target machine learning (ML) methods used by organizations.

Developing AI-based tools to build malware that can reliably defeat AI-based security solutions will be a priority for actors seeking to remain undetected.

The underlying data models created using ML algorithms—generated from troves of big data and painstaking tuning by researchers—will be a prime target for intellectual property theft.

BEATING "INTELLIGENT" SECURITY SOLUTIONS

Advances in AI technology have enabled a revolution in new services and capabilities across a wide range of industries, and in cybersecurity, one of the most significant advances has been in malware detection. Startups and tech heavyweights have all thrown their hats into the ring, offering a variety of AI-enabled security services, including AI-enabled intrusion detection systems, network- and host-level anomaly detection, and AI-based network deception systems. Among the most mature of these AI security solutions is the use of ML algorithms in antivirus (AV) engines. For decades, malware developers have sought to stay a step ahead of the static signatures and heuristic analysis techniques used in AV engines by using tactics like polymorphic (i.e., self-modifying) malware, which has led to exponential growth in the samples observed in the wild, including as many as 230,000 new malware samples daily.[1] One of the most powerful tools in detecting this onslaught of previously unobserved malware is the AI-based AV engine.

MALWARE GETS SMART

Booz Allen anticipates that in response to the increasingly sophisticated detection measures, threat actors will turn their sights on AI-enabled tools to aid their malware development process—for instance, incorporating AI-enabled tools to finalize malware payloads before use, similar to the sophisticated encoders, packers, and obfuscators used today. Researchers have demonstrated proof-of-concept (POC) tools that can be used to defeat even the most advanced AV systems.[2] [3] The POCs approached the problem the same way a potential attacker would, by treating the targeted AV system as a "black box" with no information on its functioning beyond the "malicious" or "benign" output, and leveraged an ML system to pass a Windows portable executable (PE) file to an AV engine and iteratively modified it until it was classified as benign, while preserving the PE's malicious functionality. Notably, this automated process is not terribly different from tactics already used by some threat actors, such as iteratively uploading malware samples to public sandboxes and manually modifying them to lower AV detections.[4]

[1] https://purplesec.us/resources/cyber-security-statistics/

[2] https://www.blackhat.com/docs/us-17/thursday/us-17-Anderson-Bot-Vs-Bot-Evading-Machine-Learning-Malware-Detection-wp.pdf

[3] https://arxiv.org/pdf/1702.05983v1.pdf

[4] https://unit42.paloaltonetworks.com/unit42-oilrig-actors-provide-glimpse-development-testing-efforts/

LEAP-FROGGING AI RESEARCH

Another core threat to AI services across a variety of industries is the targeting of the underlying data models for intellectual property theft. The explosion in viable AI services in recent years is due largely to a convergence of several factors, including the availability of advanced, open source ML tools and access to troves of big data and affordable computing power to train AI models. In many ways, the secret ingredient to AI services is not the algorithms but rather the data used to build a trained model capable of reliably producing true positive results. Whether this is scouring medical imaging data to identify cancer or processing network logs to detect anomalous behavior indicative of an intrusion, much of the work by researchers is aggregating data and tuning the model. Once this model is established, efforts by researchers could be for naught if the model is stolen and integrated into a competitor's service. This will likely be a major focus for sophisticated actors seeking to conduct economic espionage and intellectual property theft. This type of activity could take the form of a traditional cyber attack—for example using unauthorized network access to simply copy model data—though researchers have also recently demonstrated POC techniques to use the output of a trained neural network model as input for another model conducting a "mimicking attack," which replicates the functionality of the original model without needing access to the original training data or information on the targeted neural network.[5]

MITIGATIONS

Concerned organizations should consider the following mitigation options:

- To limit the threats of malware payloads specifically designed to defeat AI-enabled AV solutions, organizations should implement a defense-in-depth strategy to disrupt attacks elsewhere in the kill chain; for example, hardening internet-facing infrastructure and training employees can limit the likelihood of successful delivery, and network security tools such as intrusion detection systems can be used to detect command and control traffic.
- Organizations should build and train their AI systems to be robust to adversarial attacks.
- Organizations need to treat AI models as proprietary intellectual property and protect them as they would any proprietary software.
- Organizations actively developing AI services should expect trained models to be a major target for threat actors specializing in economic espionage, apply additional security controls for accessing these assets, and consider using techniques such as digitally watermarking trained models to prove ownership.[6]
- As new techniques for copying or mimicking AI models emerge, developers may need to align specific mitigations to attack techniques; for example, the "mimicking attack" POC referenced above can be mitigated by withholding confidence values from the model output.

[5] https://arxiv.org/pdf/1912.03959.pdf

[6] https://arxiv.org/pdf/1802.02601.pdf

PARCEL AND SHIPPING SERVICES AS CRITICAL INFRASTRUCTURE

Cybercriminals and state-aligned cyber threat actors will likely increasingly target the parcel and shipping sector because the importance of their operations and infrastructure has increased as a consequence of the coronavirus pandemic.

Enterprising cybercriminals may leverage the increased public reliance on the shipping sector to infect shippers and their customers.

The elevated level of shipment notifications may reduce the public's caution regarding delivery notifications, increasing their susceptibility to phishing.

Expanded package delivery could make reshipment scams more viable and less likely to be discovered.

Cybercriminals may take advantage of overstressed operations around holidays or other critical periods to extract ransoms from shippers.

State-aligned adversaries may view the parcel and shipping sector as a particularly valuable social and economic target for possible disruption that falls below a threshold for retaliatory response.

Adversaries can obtain a wide variety of outcomes by targeting this sector, ranging from impacting national morale to interfering with democratic elections.

RISING CYBER RISK TO THE PARCEL AND SHIPPING SERVICES SECTOR

The coronavirus pandemic has made more broadly apparent the critical importance of the parcel and shipping sector to the national well-being. Since the pandemic began in early 2020, consumer spending on America's largest online retailer, Amazon, rose 35 percent from the same period in 2019.[1] This shift in consumer behavior stretches the limits of the capacity of the U.S. parcel and shipping services sectors that will continue over the interim as society reacts to the pandemics' uncertain cycles. Booz Allen believes these trends will continue well into 2021. Cyber threat actors of all kinds will seek to leverage this new reality to enrich themselves and promote their malicious interests.

Cybercriminal Threats

Ubiquitous public and private reliance on the parcel and shipping sector makes it an increasingly valuable target for profit-motivated cybercriminals. Consumers are increasingly accustomed to receiving multiple order status emails, delivery notifications, package receipt notifications, and return labels for just a single item. Phishing schemes involving malicious FedEx, DHL, and UPS delivery updates spiked during the early months of the pandemic.[2] It is clear that phishing attempts represent only the surface of potential threat vectors against the parcel and shipping sector, but cybercriminals will increasingly seek to slip malicious emails and attachments into overwhelmed consumers' inboxes.

- **Targeting Shippers with Ransomware:** In 2021, cybercriminals will likely seek to disrupt parcel and shipping sector operations during critical periods of operation. Ransomware deployed across a shipper's network in the days leading up to a major holiday or during a period of coronavirus-related economic lockdown could have dramatic impact on operations and consequential financial implications for shippers industry-wide.
- **Reshipping Scams:** The parcel and shipping services sector has long been used to launder funds and illicitly obtained goods. Our experts predict reshipment scams will increase as consumer behavior trends toward more home deliveries. Tracking such scams will likely be increasingly difficult, particularly because greater numbers of package deliveries can be used as a form of cover for criminal activities. Cybercriminals will likely be increasingly able to recruit reshipping or other money mules, witting or otherwise, who need extra income during the global coronavirus-induced recession and unemployment.[3]

State-Aligned Threats

Cybercriminals are not unique in their interest in targeting organizations involved in parcel delivery. Booz Allen believes state-aligned threat actors may also prioritize U.S. mail and parcel delivery services to support their strategic goals. U.S. adversaries may take advantage of the elevated importance of the parcel and shipping sector to disrupt critical services, undermine public confidence in U.S. public sector services, or generally demoralize the population.

- **Strategic Disruptions:** The elevated utility of the parcel and shipping services sector, particularly during a global pandemic, could elevate its status as a target for U.S. adversaries

[1] "Insights on Changing Consumer Spending," Facteus Insight Report on Consumer Spending and Transactions (FIRST), Facteus, July 15, 2020, accessed July 22, 2020, https://www.facteus.com/reports/first-report-7-152020/.

[2] Jonathan Greig, "Fake FedEx, DHL, and UPS delivery issues used in COVID-19 phishing scams," TechRepublic, May 1, 2020, accessed July 22, 2020, https://www.techrepublic.com/article/fake-fedex-dhl-and-ups-deliveryissues-used-in-covid-19-phishing-scams/.

[3] Brian Krebs, "How Cybercriminals are Weathering COVID-19," Krebs on Security, April 30, 2020, accessed July 23, 2020, https://krebsonsecurity.com/2020/04/how-cybercriminals-are-weathering-covid-19/.

intent on disrupting American life. Disrupting this sector would be a particularly acute social and economic pain point for U.S. citizens relying heavily on shipping for medicine, food, and other necessities during recurring periods of economic lockdown and social distancing. Targeting this sector could be a viable asymmetric choice for adversaries wishing to cause disruption to industries considered less critical than others like energy or telecommunications.

- **Impacting Critical Services:** Beyond universal, last-mile parcel and mail delivery, the shipping services sector also plays a crucial role in certain critical government functions that adversarial nations could try to disrupt. The coronavirus pandemic has quickly increased the number of states supporting universal vote by mail, greatly expanding a service provided by the shipping sector that is critical to American democracy. The $10 billion in damages caused by the NotPetya wiper attack launched by Russian military intelligence in 2017 demonstrates just how destructive and disruptive a foreign adversary can be to an organization with global operations.[4]

MITIGATIONS

Concerned organizations should:

- Increase the level of network monitoring around periods of increased public reliance on the parcel and shipping services sector, such as holidays and other critical periods such as elections or natural disasters.
- Pay close attention to the strategic and geopolitical environment, with the understanding that the parcel and shipping services sector is a viable target for asymmetric cyber attack. Prioritize activities based on this evolving risk profile.
- Launch public relations campaigns to educate the public on the type of communications they can expect as clients.
- Train employees to be vigilant when receiving and opening emails from organizations in the parcel and shipping services sector and know how to identify/report a potential phishing email.
- Review your overall cybersecurity controls for network and authentication layer segmentation to ensure that crown-jewel assets have additional protections if an incident were to occur.

[4] Andy Greenburg, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History,” Wired, August 22, 2018, accessed July 24, 2020, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-codecrashed-the-world/.

MANDATED CONTACT TRACING APPS MAY OPEN DOORS FOR LARGE-SCALE CYBER ATTACKS

The COVID-19 tracing app ecosystem and surrounding social circumstances create appealing opportunities for diverse threat actors, including state-aligned, for-profit, and trolls.

Many contact tracing apps were developed with minimal regard for privacy and security, sometimes resulting in insecure apps and centralized databases of population-wide personally identifiable information (PII).

Adversaries may attempt to surveil users, install data stealing and surveillance backdoors, steal large PII databases, create fake outbreaks, and blackmail and harass users.

Risks of these threats will likely be highest in countries with high adoption rates, which are typically undemocratic countries that mandate installation under threat of steep civil and criminal penalties.

COVID-19 CONTACT TRACING APPS HAVE APPEARED WORLDWIDE. IN AT LEAST 47 COUNTRIES, GOVERNMENTS HAVE SPONSORED THE DEVELOPMENT OF SUCH MOBILE APPLICATIONS TO ALERT PEOPLE WHO HAVE BEEN IN CLOSE CONTACT WITH AN INFECTED PERSON SO THAT THEY CAN PROACTIVELY TEST FOR THE VIRUS AND ISOLATE.

NOVEL CORONAVIRUS SPURS NOVEL TRACKING SOLUTIONS

COVID-19 contact tracing apps have appeared worldwide. In at least 47 countries, governments have sponsored the development of such mobile applications to alert people who have been in close contact with an infected person so that they can proactively test for the virus and isolate.[1] Epidemiologists estimate that community transmission could be halted if 56%–60% of a population were to use these apps[2] and it would slow measurably with at least 15% adoption.[3] For context, in the United States, those app adoption rates have been similarly achieved only by YouTube, Facebook, and Gmail.[4] To this end, 29 countries have mandated adoption; otherwise, residents may face fines, jailtime, or loss of employment.[5] [6]

Security and privacy were often not prioritized. South Korean officials, for example, have stated that they "could not afford a time-consuming security check on the app that would delay its deployment."[7] As a result, some apps have reportedly been vulnerable to exposure of users' names, current locations, and infection status, as well as the manipulation of users' location and interaction data.[8] [9] Several countries have adopted centralized data collections for all users, planning to keep sometimes permanent records of users' historic location and infection status.

These technical and situational circumstances create opportunities for adversaries to advance diverse agendas.

- **Internal security groups** could require visitors, such as business travelers, to install these applications, exposing them to remote tracking. These apps could be backdoored to collect data held on mobile devices, such as account credentials and sensitive personal, business, and financial data, as well as intercept two-factor authentication at the device level.
- **Espionage and counterintelligence groups** could steal centrally collected personal and location data to enhance other large-scale data sets. This scenario might mirror the trend of Chinese state-linked actors stealing databases from government insurance providers,[10] travel companies,[11] and credit agencies.[12]
- **Criminals** could distribute fake tracking apps through official and unofficial channels to capture monetizable personal and financial information. They could also engage in novel forms of blackmail, changing users' infection status to positive under threat of becoming a social pariah unless a fee is paid.

[1] https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/

[2] https://www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percentdownload/

[3] https://www.dw.com/en/loved-or-loathed-how-germanys-coronavirus-tracking-app-is-faring/a-53959165

[4] https://www.statista.com/statistics/281605/reach-of-leading-us-smartphone-apps/

[5] https://www.aljazeera.com/news/2020/05/qatar-covid-19-app-mandatory-experts-question-efficiency200524201502130.html

[6] https://www.technologyreview.com/2020/05/07/1001360/india-aarogya-setu-covid-app-mandatory/

[7] https://www.nytimes.com/2020/07/21/technology/korea-coronavirus-app-security.html

[8] https://www.nytimes.com/2020/07/21/technology/korea-coronavirus-app-security.html

[9] https://www.amnesty.org/en/latest/news/2020/05/qatar-covid19-contact-tracing-app-security-flaw/

[10] https://www.nytimes.com/2019/05/09/technology/anthem-hack-indicted-breach.html

[11] https://www.reuters.com/article/easyjet-cyber-china/chinese-hackers-seen-behind-cyberattack-on-easyjetsources-idUSL8N2D14MA

[12] https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020

- **Cyberwarfare groups** could distribute destructive updates to users. Updates for applications with country-limited userbases have been prime targets in international conflicts. For example, the Russian military used Ukrainian tax software in 2017 and North Korean actors used South Korean filesharing software in 2009 to distribute wiper and distributed denial of service (DDoS) botnet malware.
- **Disinformation groups** could target the apps in efforts to create fake outbreaks by modifying communities' health status en masse.
- **Trolls** could harass specific individuals by changing their infection status.

The risk of many of these threats will be highest in countries where adoption is widespread. Countries that have legally mandated installation will likely have higher adoption rates than in countries with voluntary adoption rates, a line generally demarcated by undemocratic and democratic countries. As of July 2020, Qatar, for example, has achieved a world-leading 91.8% adoption rate through its installation mandate;[13] whereas, voluntary-install countries like France and Germany[14] have had less than 15% adoption, observing shrinking installation bases when infections declined.[15]

MITIGATIONS

Much of the burden for securing contact tracing apps will fall on the companies contracted to develop and deploy them—a process that should include security testing of the app, and use of robust authentication and access controls for communications with back-end databases. However, organizations concerned with potential risks to mobile devices in their environment—including those related to mandated contact tracing apps—should consider:

- Exploring the use of mobile device management (MDM) platforms that can centralize control and enable remote management of data security, configuration, software deployment, and other administrative functions
- Exploring the use of application containerization solutions that may be used to isolate enterprise applications or data on employees' personal devices
- Applying general security best practices to enterprise mobile devices, including ensuring devices have strict access controls and data encryption, and that users are trained to recognize potential threats.

[13] https://qz.com/1880457/global-contact-tracing-app-downloads-lag-behind-effective-levels/

[14] https://www.vice.com/en_us/article/akzne5/europeans-arent-really-using-covid-19-contact-tracing-apps

[15] https://www.swissinfo.ch/eng/swiss-support-wanes-for-masks-and-covid-tracing-app/45829502

CYBERCRIMINALS WILL LIKELY CAPITALIZE ON RAPID U.S. TELEHEALTH ADOPTION

The massive shift to a remote delivery model brought on by the COVID-19 pandemic—including the rapid expansion of U.S. telehealth services—will change the way cybercriminals target health data:

The response to the COVID-19 pandemic has led to massive adoption of telehealth services in 2020, and the use of telehealth services is unlikely to contract after the pandemic clears.

Mass adoption of this technology will lead to new cybercrime focus, with an emphasis on stealing patient data to enable fraud, target health data in ransomware attacks, trick patients in social engineering schemes, and target remote patient monitoring (RPM) devices.

Telehealth security is a patient safety issue, with potentially catastrophic risks for data vulnerabilities, service disruptions, and device failures.

EXPANDING ACCESS MAY LEAD TO EXPANDING ATTACKS

The COVID-19 outbreak is quickly remaking the face of healthcare delivery as providers and patients turn to telehealth.[1] According to the Health Resource Services Administration, telehealth uses electronic information and telecommunications technologies to remotely provide clinical healthcare, patient and professional health- related education, and public health and health administration services; some of the core technologies used in these services may include videoconferencing, store-and-forward imaging, and streaming media and are typically accessible via the internet, including wired and wireless communications. Telemedicine typically includes clinical care, such as treatment of chronic conditions, medication management, and specialist consultations, and can be consider a subset within broader telehealth services. Notably, telemedicine and telehealth share similar technology, infrastructure, and weaknesses to illicit cyber activity.[2]

TELEHEALTH SERVICES INCREASE UNDER HEALTH EMERGENCY

In March 2020, Medicare and Medicaid experienced substantial policy transitions to provide access to telehealth services to 60 million Americans in response to the pandemic.[3] New legislation and federal regulation changes allowed government providers to further expand remote health services.[4] Prior to the public health emergency, in a given week, 13,000 Medicare recipients used fee-for-service (FSS) telehealth, but by the last week of April that number increased to 1.7 million recipients.[5] Large U.S. technology firms are moving into the telemedicine field, pushing platforms that integrate once disparate databases used for billing, scheduling, patient data, and that facilitate patient-provider collaboration. Firms like GE Health, Google, and Microsoft are launching cloud-based systems for medical device management and telehealth delivery with Health Insurance Portability and Accountability Act (HIPAA) certification.[6]

[1] https://www.msn.com/en-au/news/australia/are-all-doctors-offering-telehealth-during-the-coronaviruspandemic-and-do-you-have-to-use-it/ar-BB11St78

[2] https://www.healthit.gov/faq/what-telehealth-how-telehealth-different-telemedicine

[3] https://www.nbc4i.com/news/washington-dc/president-trump-expands-telehealth-service-coverage-formedicare-recipients/

[4] https://medcitynews.com/2020/03/cms-shares-specifics-on-sweeping-medicare-telehealth-expansion/

[5] https://www.healthaffairs.org/do/10.1377/hblog20200715.454789/full/

[6] https://www.bralin.com/cloud-platform-security-showdown-g-suite-vs-office-365

LARGE U.S. TECHNOLOGY FIRMS ARE MOVING INTO THE TELEMEDICINE FIELD, PUSHING PLATFORMS THAT INTEGRATE ONCE DISPARATE DATABASES USED FOR BILLING, SCHEDULING, PATIENT DATA, AND THAT FACILITATE PATIENT-PROVIDER COLLABORATION.

These companies and delivery systems will also face distinct challenges. MTS Intel assesses that the use of telehealth more widely will result primarily in cybercriminal activity targeting these systems or devices for monetary benefit. As home-deployed medical devices assume the risks of other internet-of-things (IoT) devices but transmit essential data used in medical diagnoses, they may pose the most significant risk for patients:

- **Billing Fraud:** Attackers typically conduct billing fraud over the phone using stolen information to demand payment for physician-ordered medical devices or fake medical debt collection.[7] Alternatively, they pair stolen patient numbers with falsified provider data to submit fraudulent claims with insurers.[8]
- **Ransomware:** Ransomware operators prey on hospitals and medical providers,[9] hoping encrypted patient data motivates payment. As patients receive care remotely, telemedicine data will also be a significant target for attackers looking to capitalize on the value of critical data stored on managed service providers (MSP) and local cloud instances.
- **Phishing and Credential Theft:** Phishing and credential theft are already top risks to enterprise systems. Attackers will use established techniques to attack G Suite, Microsoft, or other enterprise- grade systems. Attackers may subject patients and providers to medical-themed phishing campaigns or redirect to spoofed websites for credential theft.[10]
- **RPM/Home Telehealth Solutions:** Traditionally, providers deploy patient monitoring systems in a medical facility, but RPM systems are deployed in a patient's home. Providers use device data to treat acute conditions and chronic illness, but these devices must maintain confidentiality, integrity, and availability of patient data and ensure patient safety.[11]

[7] https://www.ag.state.mn.us/Consumer/Publications/VoicePhishing.asp

[8] https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackersthan-your-credit-card-idUSKCN0HJ21I20140924

[9] https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/

[10] https://www.healthcareitnews.com/news/microsoft-cloud-healthcare-touts-telehealth-remote-teamcollaboration

[11] https://www.nccoe.nist.gov/projects/use-cases/health-it/telehealth

MITIGATIONS

Concerned organizations should consider the following mitigation options:

- **Telehealth Strategy and Architecture:** The pervasive need for innovative telehealth solutions to provide continuity of care during the pandemic is giving rise to rapid technology implementations that lack clinical and technical integration. As we adjust to the post-COVID reality, healthcare systems should develop or refine an enterprise telehealth strategy with cybersecurity considerations built into every layer of the telehealth ecosystem, from the infrastructure to the supply chain, software, endpoint provisioning, and clinician and patient education.
- **Third-Party Vendor Security:** Healthcare is a highly regulated industry, and there are multiple standards in place to protect patients and healthcare systems (e.g., HIPAA, SOC 2, HITRUST, Federal Information Processing Standard [FIPS] 140-2). However, the rapid acceleration of the telehealth industry has introduced new vendors with less experience navigating complex healthcare security regulations. Organizations including the National Consortium of Telehealth Resource Centers and the American Medical Association provide checklists with security and privacy considerations for reviewing telehealth vendors. In addition to relying on regulatory compliance, firms need to evaluate the vendors' security controls, intrusion systems, and policies on accidental disclosure of data or unauthorized access to ensure they are equivalent or exceed the providers' benchmarks.[12]
- **User Authentication:** Patient data is of particular value to attackers for its use in billing fraud. High- profile patients and public figures using this service may also be subjected to additional scrutiny or blackmail if their data is leaked or made available to scammers. Firms should implement robust user authentication measures to ensure patient IDs and personally identifiable information (PII) stay secure.
- **Device Security:** Administrators should consider implementing remote management for devices such as tablets or mobile phones used by providers with access to telehealth data. Similarly, providers may also require patients to use specific apps with embedded security controls on their PCs or mobile devices to further secure provider-patient sessions.
- **Telehealth Peripherals:** RPM solutions are essentially IoT systems used for medical purposes but share similar risks to cyber threats.[13] Like other vulnerable IoT devices, RPM devices should use unique passwords and take authorized firmware updates. Patients will require clear instructions on how to configure and install the devices on their home network to ensure only encrypted data is sent to providers.[14]

The healthcare industry is at a critical inflection point, as connected care has the potential to transform the clinician and patient experience. However, the rapid expansion of telehealth services creates new risks for patient safety and enterprise security. Including the right information technology (IT) and information security representatives in the planning process and building in end-to-end cybersecurity measures are essential to take advantage of the current telehealth momentum while mitigating potential threats.

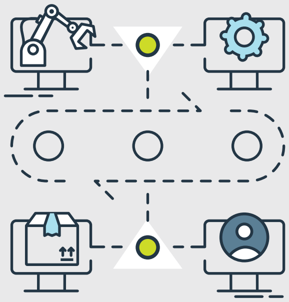
[12] https://www.healthcareitnews.com/news/potential-security-crisis-presented-rapid-telehealth-rollouts

[13] https://www.nccoe.nist.gov/projects/use-cases/health-it/telehealth

[14] https://www.darkreading.com/iot/medical-devices-on-the-iot-put-lives-at-risk/a/did/1337448?_mc=bib&itc=bib

5G TO EXPAND THE ATTACK SURFACE FOR INDUSTRIAL IOT

The marriage of 5G networks and industrial control systems/operational technology (ICS/OT) will result in a compounded attack surface and expose underlying flaws in how industrial internet-of-things (IIOT) networks operate.



Current ICS/OT environments rely on network segmentation to mitigate cyber risks.

Organizations need to reconsider the structure of IIOT network setups, and vendors need to present secure, actionable solutions to organizations using their ICS/OT products.

The introduction of 5G technology may reduce the layers of abstraction between network segments and introduce new devices.

5G TO CHANGE OPERATIONAL TECHNOLOGY ENVIRONMENTS

Many disparate industries anticipate the arrival and wider availability of 5G networks for the enhancements 5G offers to a variety of environments, including the wireless integration of IIOT systems. The ICS and OT environments stand to benefit the most from this revolutionary technology—despite their legacy of outdated operating systems and vulnerabilities discovered decades after implementation.

High-profile vulnerabilities have emerged just as ICS and OT device security is beginning to become a priority for organizations. Transitioning these networks to 5G will present an entirely different attack surface to these environments that are often less protected than enterprise endpoints because network abstraction provides a perceived degree of protection.

5G to Centralize Communications in ICS Environments

In most cases, the migration to 5G will maintain a similar level of network segmentation; however, the new technologies will likely centralize network operations and data collection to a layer-agnostic hub or edge network.[1] This means the hub can be used to enrich communications from lower level components—including the physical and controller levels, which are completely abstracted from the internet-facing network layers in existing wired environments. The enrichments—as well as access—offered by centralizing OT communications through an internet-facing device are likely to appeal to attackers and offer more disruptive and destructive attacks through direct access to physical operations.

> THE ENRICHMENTS—AS WELL AS ACCESS—OFFERED BY CENTRALIZING OT COMMUNICATIONS THROUGH AN INTERNET-FACING DEVICE ARE LIKELY TO APPEAL TO ATTACKERS AND OFFER MORE DISRUPTIVE AND DESTRUCTIVE ATTACKS THROUGH DIRECT ACCESS TO PHYSICAL OPERATIONS.

5G's Viability as a Wireless Solution for ICS Environments May Expose Security Issues with Legacy Protocols

Many ICS/OT devices use the Modbus protocol. Modbus was standardized in 1979 with few changes since— including several implicit limitations that degrade the security of the protocol and make it a questionable choice for internet-facing technologies: communications are sent in clear text with no encryption, and there is no authentication or data integrity checking.[2] Efforts to integrate Modbus into other wireless technologies, such as Global System for Mobile (GSM) Communications, 3G, 4G, WiFi, and Bluetooth, were generally unsuccessful because of excess latency. Excess latency effectively prohibits real-time operation, which is a requirement across varying industries and implementations. 5G is the first emerging wireless technology that removes this latency barrier, enabling latency-sensitive operations like Modbus communications.

One of the key benefits of 5G technology is network slicing, which allows internet service providers (ISP) to divide the network based on the needs of each device. There were three primary 5G network slices envisioned as described below, but network slices can be tailored to meet any specific use case (e.g., enhanced security):

- **Enhanced Mobile Broadband (eMBB):** Higher bandwidth
- **Ultra-Reliable Low-Latency Communication (uRLLC):** Low-latency
- **Massive Internet-of-Things (mIoT):** Integration of billions of IoT devices

[1] https://www.automationworld.com/factory/iiot/article/21132891/is-the-purdue-model-still-relevant

[2] https://www.cyberbit.com/blog/ot-security/scada-modbus-protocol-vulnerabilities/

For industrial 5G setups, organizations can use commercially available 5G networks, or build stand-alone systems intended to support the OT environment and integrate industrial languages like Modbus. The biggest threat posed to 5G IIOT networks comes from commercial implementations where the network will be mixed with the mIoT network slice; this network slice hosts devices known to suffer from poor security, such as printers and cameras, significantly increasing the likelihood that connected devices will be compromised and used to conduct malicious activity. For implementations using an archaic and insecure protocol like Modbus, an attacker can simply send a command to a device without the recipient validating the nature of the request. The consequences of such attacks will be more costly than traditional cyber attacks, given the real-world nature of ICS/IIOT environments and the role these connected systems play. Further, these emerging technologies present an ever-evolving threat landscape that cannot yet be profiled; vulnerabilities will inevitably be discovered as the technology becomes ubiquitous.

MITIGATIONS

Organizations should expect and prepare for 5G/IIOT attacks and vulnerabilities:

- **Harden underlying structures:** Ensure that systems are as up to date as is feasible for their respective technology. Consider upgrading devices that are unsupported by manufacturers if there is a newer version that comes with support and security updates.
- **Strategize 5G network architecture:** There are many factors involved in migrating IIOT to 5G networks. Do you plan to implement a private 5G network or a managed commercial solution, and what implications come with that choice? Be involved in network architecture discussions and consider possible impacts stemming from centralizing network layer management.
- **Talk Security Strategy with IIOT vendors:** Be direct and request details about how a technology holds up in these new environments. Consider inquiring about communications protocols and if there are more secure options than legacy protocols.
- **Address "tech debt" in advance:** Ensure your organization addresses known security flaws or outdated technologies before deploying 5G in IIOT environments.
- **Plan security strategy:** Consider how your security detection stack will identify and alert on attacks in IIOT environments.

5G TO INCREASE SECURITY PRESSURE ON MOBILE HOTSPOTS

5G availability will change the way people access the internet, drive more widespread adoption of mobile hotspots for internet access, and increase attacker incentives to find and exploit vulnerabilities in these devices.

The availability and quality of 5G cellular networks will drive increased use of mobile hotspots to access the internet.

Interest in targeting vulnerabilities in such devices will increase as users rely on mobile hotspots for their primary internet connection at home and in densely populated areas.[1] [2]

[1] https://www.qualcomm.com/media/documents/files/deploying-5g-nr-mmwave-for-indoor-outdoor.pdf

[2] https://www.qualcomm.com/media/documents/files/5g-nr-mmwave-deployment-strategy-presentation.pdf

MOBILE HOTSPOTS, CELLULAR MODEMS, AND THEIR SHORTCOMINGS

The promises of 5G to offer faster, more reliable cellular internet connections[3] and the opportunity to connect more types of devices to the internet via a cellular network introduce the possibility of greater incentive for attackers to target devices connected to cellular networks. Of particular concern are mobile hotspots and stand-alone cellular modems.

5G Modems and Hotspots Expected to Replace Existing Internet Connections

Cellular modems are the devices used to connect directly to a cellular network and establish an internet connection. Mobile hotspots contain a cellular modem and a Wi-Fi router that allow devices to connect to the Wi-Fi network and access the internet. They usually offer user interface and configuration via a web portal.

Evolutions of mobile hotspots could replace cable or fiber modems in households or even office buildings.[4] Moreover, based on what the public knows about the few 5G smartphones and mobile hotspots already on the market, we believe that future 5G products will function similarly to their 4G predecessors.

Poor Security in Mobile Hotspots Likely to Continue as They Proliferate

Unfortunately, existing stand-alone cellular modems and mobile hotspots are notorious for including minimal security and abundant, easily exploitable vulnerabilities.[5] [6] Most of the researched vulnerabilities relate to the mobile hotspot's user-facing web portal and the potential for an attacker to use a system compromised through social engineering or other means to seize control of the mobile hotspot without the user's knowledge.[7] Other vulnerabilities relate to the modem and the potential for rogue cellular infrastructure to help attackers control the modem.[8]

An impactful vulnerability could allow affected devices to be enlisted in a Mirai-style botnet, generate revenue via ad fraud or premium services, compromise the internet traffic of the connected devices, or even simply cause the device to permanently stop functioning.

RECOMMENDATIONS

Whether attackers will be incentivized to discover and exploit such a vulnerability depends on multiple trends in the 5G market, outlined below. Organizations should monitor these trends and adapt to changes they effect in the security environment.

Adoption

First, the more devices connect to 5G networks, the larger the pool of potential victims. Practical details of 5G connections like speed, reliability, coverage, hardware cost, and data cost will affect adoption. Organizations can monitor the market for vulnerabilities and exploits in 5G mobile hotspots and factor this information into decisions to allow or require employees to use 5G to access the internet.

Diversity

A larger number of hardware and especially software families for 5G modems will limit the impact of vulnerabilities. If, as the 5G market matures, one chipmaker or software developer for 5G modems comes to dominate,[9]

[3] https://www.digitaltrends.com/mobile/5g-vs-4g/

[4] https://www.5gamericas.org/wp-content/uploads/2019/07/5G_Americas_White_Paper_on_5G_IOT_FINAL_7.16.pdf

[5] https://www.pentestpartners.com/security-blog/reverse-engineering-4g-hotspots-for-fun-bugs-and-netfinancial-loss/

[6] https://www.cnet.com/news/that-4g-hotspot-could-be-a-hotbed-for-hackers/

[7] https://www.blackhat.com/docs/us-14/materials/us-14-Lindh-Attacking-Mobile-Broadband-Modems-Like-ACriminal-Would-WP.pdf

[8] https://www.pentestpartners.com/security-blog/breaking-bad-firmware-encryption-case-study-on-thenetgear-nighthawk-m1/

[9] https://www.businesswire.com/news/home/20200415005447/en/Strategy-Analytics-2019-CellularBaseband-Market-Share

a vulnerability in that hardware or software will affect a much larger share of devices.[10] On the other hand, if the market remains relatively segmented among different suppliers, the pool of potential victims for such a vulnerability and the potential payoff for discovering one will remain lower. When conducting security audits on 5G equipment, organizations should factor in the value of a diverse set of technologies, to limit the potential impact of vulnerabilities. Using products from well-known vendors rather than a new market entrant should be considered until the new products have been tested.

Developers

Finally, the security posture of chipmakers, stack developers, operating system suppliers, original equipment manufacturers, carriers, and other contributors to 5G products will strongly affect the resiliency of those products. Hardened software, easy or automatic patching, and long support lifecycles would help this class of products rise to modern information security challenges. Organizations should already be assessing these criteria when auditing new partners and equipment. These practices will continue to be important with 5G technologies.

MITIGATIONS

Concerned organizations should prepare for attacks on 5G mobile hotspots by:

- Monitoring the above trends to gauge how likely attackers are to target 5G devices and the potential impact of a major vulnerability discovery
- Ensuring 5G adoption and acquisition processes include robust security audits and full supply chain investigations, to inform security-driven decisions
- Prescribing that cellular products and systems connected to them follow the same security policies as other networked systems, including the use of intrusion detect systems, established patching processes, and careful management of employee access and privileges
- Continuing to leverage security best practices for devices connecting to corporate resources through the 5G hot spots such as virtual private networks (VPN), providing an extra layer of protection

AN IMPACTFUL VULNERABILITY COULD ALLOW AFFECTED DEVICES TO BE ENLISTED IN A MIRAI-STYLE BOTNET, GENERATE REVENUE VIA AD FRAUD OR PREMIUM SERVICES, COMPROMISE THE INTERNET TRAFFIC OF THE CONNECTED DEVICES, OR EVEN SIMPLY CAUSE THE DEVICE TO PERMANENTLY STOP FUNCTIONING.

[10] https://pdfs.semanticscholar.org/5a3d/449416fe93ed374b4095ca574fd1a8c49df8.pdf

IN CLOSING

We have seen unprecedented challenges for global enterprises, including myriad new cyber threat tactics and business models. At Booz Allen, our proven approach is founded on decades of experience providing advanced cyber defense solutions to the most sophisticated global enterprises and government agencies. We were cyber experts long before most service providers in the market today existed and strongly believe cybersecurity is a business imperative.

We recommend that organizations combine a top-down and bottom-up approach to building a culture that is constantly aware of security threats. This starts at the board level, but it is crucial that the practitioners of your organization adopt this culture to truly remain resilient. However, organizations do not operate in a vacuum; they need to have a cohesive security strategy with third-party vendors and suppliers, as well as cloud security providers to truly create a blanket of security upstream and downstream of their operations.

For 2021, we offer three core tenets that can help act as a north star for staying secure:

1. **Don't become distracted**—continue to invest in strong foundations and hygiene to defend against these evolving cyber threats.
2. **Be proactive to be resilient**—from securing research and development data to understanding supply chain and third-party risk management, it is imperative to understand potential adversaries, your organization, and how to respond to a cyber crisis.
3. **Have an incident response retainer in place**—not all retainers are created equal, so choose a partner that understands the nuances of breach recovery and have your organization actively practice its response. With more than 106 years of experience in management consulting and over 5,000 in-house security practitioners, we understand there is no substitute for being prepared.

And remember the lesson from our earlier narrative flight—if you have something of value, the bear will always come after you. Be prepared.

To stay connected on the latest threat trends year round

boozallen.com/cybertrends

About Booz Allen

For more than 100 years, military, government, and business leaders have turned to Booz Allen Hamilton to solve their most complex problems. As a consulting firm with experts in analytics, digital, engineering, and cyber, we help organizations transform. We are a key partner on some of the most innovative programs for governments worldwide and trusted by their most sensitive agencies. We work shoulder to shoulder with clients, using a mission-first approach to choose the right strategy and technology to help them realize their vision. With global headquarters in McLean, Virginia and offices worldwide, our firm employs nearly 27,200 people and had revenue of $7.5 billion for the 12 months ending March 31, 2020. To learn more, visit BoozAllen.com. (NYSE: BAH)

Copyright © 2020, Booz Allen Hamilton.

Any conclusion or recommendation by Booz Allen as contained in this report should not be viewed as any guarantee or opinion of any future events or future outcomes. Booz Allen undertakes no obligation to update any conclusions or recommendations to reflect anticipated or unanticipated events or circumstances in this report. Booz Allen does not guarantee that this report has identified all cyber threats, or that a security incident or security breach will not occur. Booz Allen takes no responsibility and is not liable for reliance by anyone on the information contained in this report, and any reliance is at the sole risk and discretion of the recipient of this report.