Booz | Allen | Hamilton®

2019 CYBER THREAT OUTLOOK

Eight ways threat actors will make waves in 2019

CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER

Technological change and investment continue at a breakneck pace—yet cyber threats keep up. Tried and true methods—phishing, denial of service, credential compromise—remain successful in many attacks, but new ones emerge routinely. The move to cloud is but one example: failure to add multi-factor authentication nearly confirms a compromise.

After producing thousands of intelligence reports for clients in 2018, our team combed the trends and threat landscapes to formulate some novel ideas that help teams prepare over the next year. We look at the world through many lenses—from our tactical, technical experience to our big-picture geopolitical understanding—to anticipate the black swans, the game changers, and the "next big thing." Our report captures what we see awaiting cyber defenders in 2019 and offers some ideas on what to do about it.

A few notable trends we covered in last year's report.

We noted that certain countries would try to **bust sanctions with cryptocurrencies, by developing alternative currencies and robbing exchanges.** Iran,[1] Russia,[2] and Venezuela announced plans to develop cryptocurrencies with the objective of subverting mounting U.S. sanctions. In 2018, North Korean hackers allegedly stole more than USD 500 million from breached exchanges.[3]

We believed that **an adversary would cripple a large city or state government** with targeted ransomware, presaging the Sam Sam group—with alleged connections to Iran—targeting the Atlanta city government in March.[4]

We thought that **adversaries would compromise small software developers to infect twice-removed members of the supply chain**, such as the criminals who breached a font provider to distribute cryptomining malware that became bundled in several widely used PDF editors.[5]

We believed that **U.S. voting infrastructure's security would not improve.** Assessments of U.S. election security in 2018 were often scathing.[6]

This 2019 Cyber Threat Outlook report again attempts to peer over the horizon and assess emerging and notable threat trends. Here's a snapshot of what we've spotted:

States may use their burgeoning **information warfare capabilities to influence consumers and harm companies**, just as they already target voters and foment civil strife.

State-linked groups could find new uses for **Internet-of-Things (IoT) botnets**, such as Tor-like communication infrastructure.

Adversaries might develop novel attack vectors that **exploit the growing pervasiveness of non-WiFi wireless protocols**, especially among IoT devices.

Adware networks, a long-standing security nuisance, could be leveraged for more harmful targeted attacks.

Increased adversary emphasis on misattribution will likely result in more examples of confident attribution by the private sector later being disproved, further undermining public confidence in attribution.

Government-backed adversaries may increasingly **penetrate the industrial control systems (ICS) of water utilities** to conduct reconnaissance and generate fear and uncertainty, mirroring their historical focus on frequent intrusions and rare disruptions at energy firms.

Booz Allen believes that in 2019, states will increasingly use their growing information-warfare capabilities to target the private sector. Just as state cyber actors have tried to manipulate voters, they may increasingly try to manipulate consumers, people who "vote with their wallets."

States have already harassed companies with politically and economically motived information warfare.

SONY

In 2014, North Korea retaliated against Sony's planned release of a film mocking Kim Jong Un by leaking unreleased movies, salary data, and embarrassing emails from the studio.

KEURIG

In 2017, Russian trolls reportedly amplified a minor far-right-wing protest of coffee maker brand Keurig, urging consumers to smash their devices.[7]

ANTONOV

In 2018, unidentified hackers defaced the website of Antonov, an aeronautics firm symbolic[8] of Ukraine's growing economic independence from Russia. The hackers published a fake "open letter" from the company decrying the Ukrainian government's lack of support, possibly to mar government-industry relations.[9]

COMPANIES IN THE CROSSHAIRS OF INFORMATION WARFARE

In recent years, many governments have learned how to manipulate their opponents' opinions and decisions with cyber activity, sometimes called "information warfare." This activity encompasses a wide range of tactics, from orchestrating targeted breaches followed by data leaks to employing troll armies to push disinformation. So far, states have mainly used these capabilities for political and military purposes, like nudging voters and enflaming cultural conflict. Booz Allen believes that, in 2019, states will increasingly use their growing information-warfare methods applied to economic conflict and will likely aim to generate investor, regulatory, consumer, or political backlash against targeted sectors and companies by fabricating or inflaming public relations and legal controversies.

The private sector has long been in the crosshairs of state-sponsored cyber operations. Often, these attacks further national economic initiatives. They steal information, such as intellectual property and corporate bidding strategies, to help an adversary's domestic industry. In some cases, larger political conflicts manifest as cyber attacks that publicly harm symbolic and strategically important companies. For many years, state-sponsored disruptive and destructive attacks have targeted these entities—for example distributed denial of service (DDoS) campaigns against the U.S. financial sector retaliating against U.S. sanctions. Information warfare offers states yet another toolbox of tactics to advance these same economic and political agendas.

Information-warfare methods applied to economic conflict will likely attempt to inflame or generate public relations and legal controversies to harm targeted sectors and companies with investor, regulatory, consumer, or political backlash. State-backed hackers could leak companies' controversial internal communications or expose employee misbehavior that companies had hoped to handle privately. Adversaries may try to breach companies, their executives, corporate or employee social media accounts, and news media websites to spread fake or embellished news stories. Legions of secretly state-managed social media accounts ("troll armies") can stoke consumer backlash by amplifying minor controversies and disseminating fabricated stories at scale.

The 2019 geopolitical environment abounds with reasons for states to use their tested information warfare techniques in new arenas. One independent think tank determined in 2017 that at least 30 governments sponsor social media armies to target critics and spread propaganda, a capabilities that could readily be directed towards the private sector.[10]

For Booz Allen, Iranian targeting of U.S. firms is top of mind in 2019.

The United States increasingly pressures Iran to renegotiate the so-called "Nuclear Deal," levying sanctions on Iran and demanding that other countries cut Iran's economic lifelines. Iran's reactive, tit-for-tat use of cyber attacks to counter its geopolitical competitors—combined with its alleged use of social media trolls and fake news outlets[11]—suggests motive and capability to conduct information warfare against U.S. companies during this conflict. Amid growing international economic strife and information warfare's increasing prevalence, the private sector may soon be caught in the crosshairs of new cyber operations.

What you can do to mitigate this threat:

- Implement a threat intelligence program that provides strategic indication and context of economic and political events that could trigger cyber attacks to harm corporate operations and reputation.
- Keep security, business operations, communications, and risk functions proactively informed of the potential downstream impact to the company of impending shifts in the political and economic environment. Engage teams in joint tabletop exercises to develop education and management plans that creatively and responsibly prepare for a potential threat.

NEW CYBER OPERATIONS TARGET THE PRIVATE SECTOR

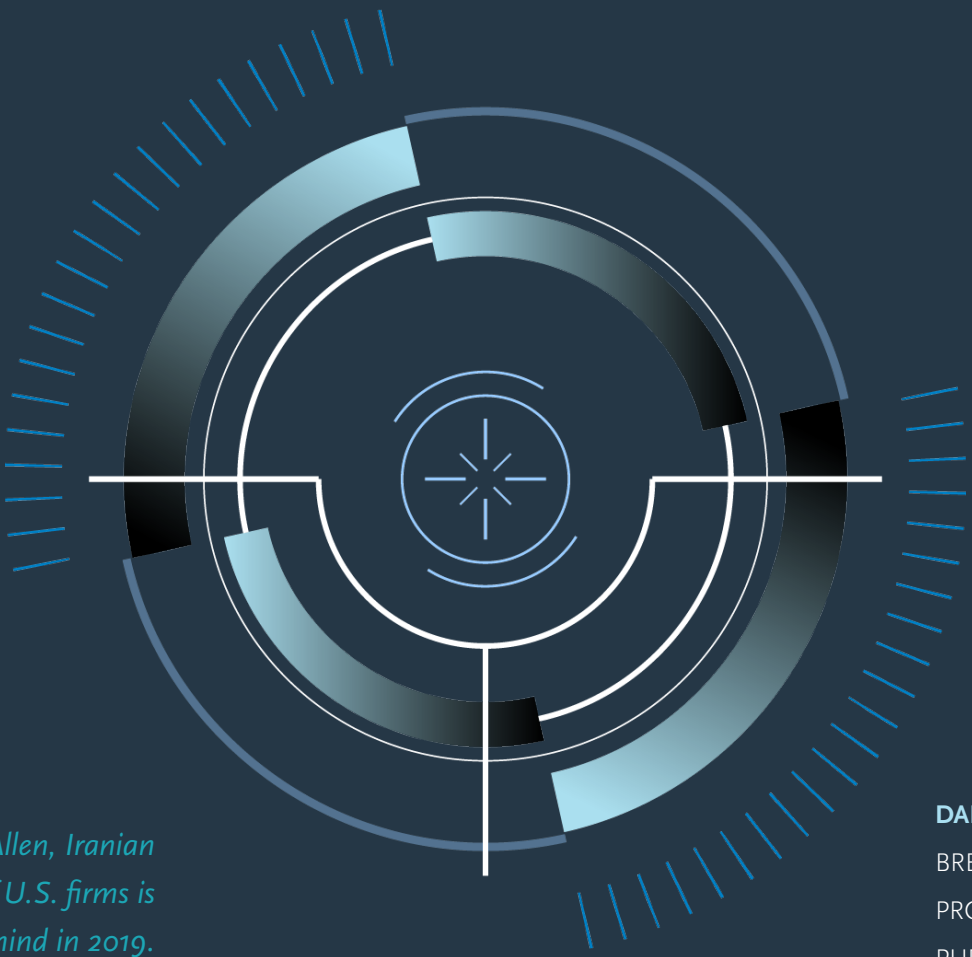
TARGETS

COMPANIES

EXECUTIVES

NEWS MEDIA WEBSITES

SOCIAL MEDIA ACCOUNTS



For Booz Allen, Iranian targeting of U.S. firms is top of mind in 2019.

DAMAGES

BREACH/DATA LEAKS

PROPAGANDA

PUBLIC RELATIONS & REGULATORY CONTROVERSIES

INVESTOR, REGULATORY, CONSUMER, OR POLITICAL BACKLASH

Connected televisions, webcams, and printers have been enlisted to mine cryptocurrency, launch DDoS attacks, and cause other mischief. In 2019, state-linked adversaries will likely increasingly abuse these devices to further their espionage and warfare efforts.

State-linked groups will mainly use IoT devices to build networks for communications proxying.

INFECTED COMPUTERS

Adversaries routinely compromise computers to act as intermediaries between themselves and their ultimate targets.

COMPROMISED ROUTERS

Routers have been a popular target among criminals and espionage groups for creating Tor-like communication infrastructure.

CONNECTED PRINTERS

Connected printers could be targeted to harvest data at scale.

IoT DEVICES BROADEN STATE ESPIONAGE OPERATIONS

In the rush to bring IoT devices to market, sales often trump security. Criminals have capitalized on this reality with for-profit schemes that frequently abuse thousands of near-identical products. Connected televisions, webcams, and printers have been enlisted to mine cryptocurrency, launch DDoS attacks, and cause other mischief. In 2019, state-linked adversaries will likely increasingly abuse these devices to further their espionage and warfare efforts.

Previous activity suggests that state-linked groups will mainly use IoT devices to build networks for communications proxying. Interacting with target computers through secondary compromised devices creates layers of protection from technical attribution. In the simplest incarnation, adversaries routinely compromise computers to act as intermediaries between themselves and their ultimate targets.[12]

Passing traffic through a distributed overlay network akin to the semi-anonymous Tor network heightens obfuscation. Routers have been a popular target for this strategy among criminals and espionage groups. The multi-year Inception espionage campaign provides a model for what this tactic might look like if attempted with IoT devices. In this case, an adversary constructed a proxy network of routers in South Korea. The devices allowed an adversary to compromise them at scale by abusing their insecure default configurations, such as shared default passwords.[13] About 15 percent of IoT device owners don't change their devices' default passwords, and 10 percent of IoT devices use one of the same five passwords for administrative access, according to one 2017 estimate.[14]

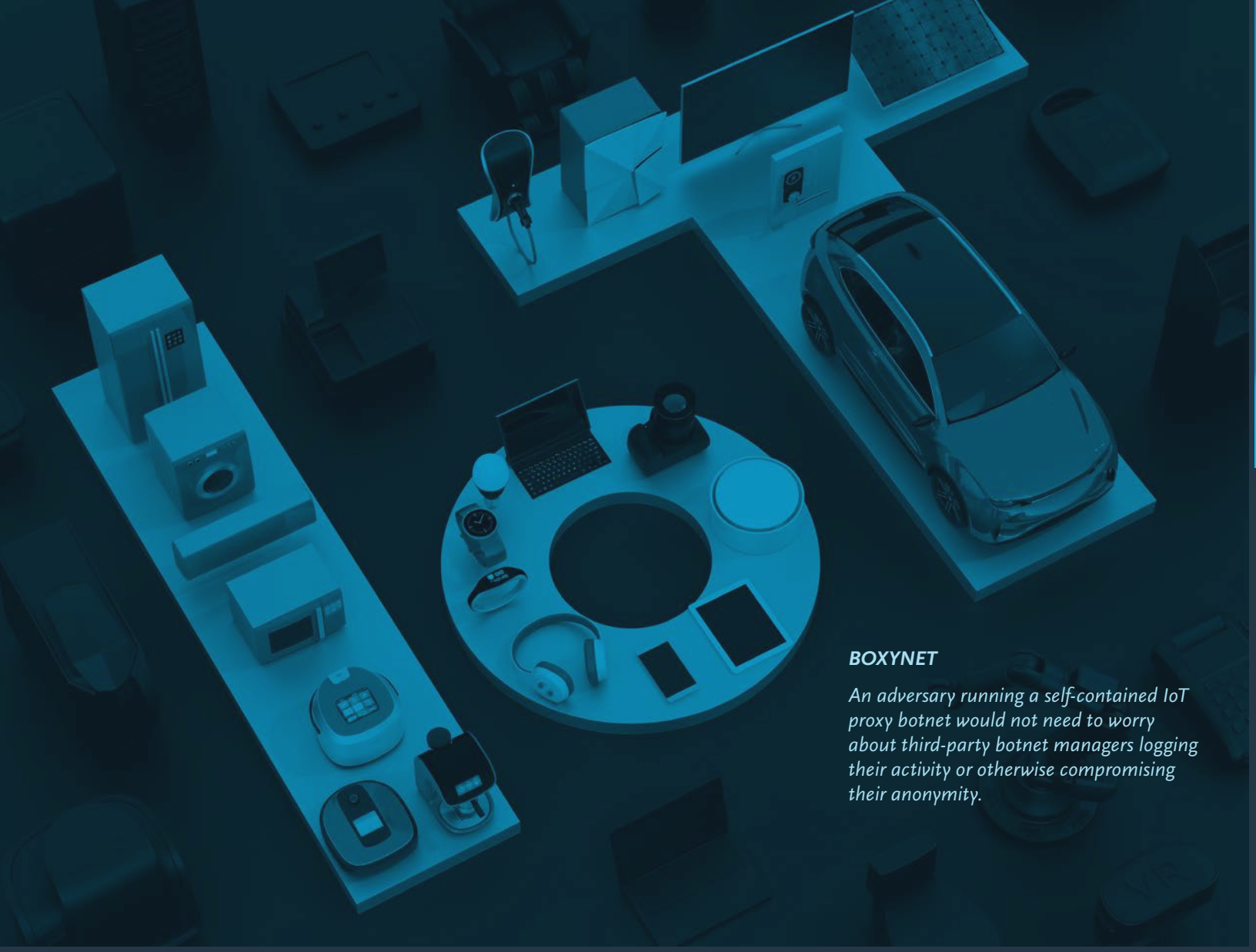
IoT botnets, especially state-owned ones, present difficult challenges for defenders. Attempting to backlist astronomically large volumes of smart televisions and DVRs would probably be impractical. An adversary running a self-contained IoT proxy botnet, which we've dubbed a "boxynet," would not need to worry about third-party botnet managers logging their activity or otherwise compromising their anonymity.

NEW AVENUES FOR IoT BOTNET ABUSE

Though communications proxies would likely be a priority, state adversaries could explore several other avenues for IoT botnet abuse. An IoT botnet might be used for widescale intelligence collection with access to whatever interesting data passes through these devices. For example, in 2013 and 2014, Russia appeared to enlist the criminal Gameover ZeuS botnet to search infected computers for government, military, and intelligence community documents. Connected printers could be similarly targeted to harvest data at scale. State adversaries might cast wide nets to find weak network endpoints for deeper intrusions. This could explain why Russia's VPNfilter malware, which targeted routers, included plugins for identifying protocols typically associated with ICS.

What you can do to mitigate this threat:

- Change default passwords and close all unnecessary open ports on existing IoT devices on your network.
- Establish a process to inventory, identify, scan, and secure new devices as they are integrated into the environment. Where possible, isolate IoT devices on a separate VLAN and allow principle of least access to govern, monitor, use, and connect to the device.
- Include IoT devices and networking devices in your organization's vulnerability management program. Conduct regular external and internal scans for vulnerable devices. Establish and adhere to service-level agreements for patching with real consequences for non-remediation.



BOXYNET

An adversary running a self-contained IoT proxy botnet would not need to worry about third-party botnet managers logging their activity or otherwise compromising their anonymity.

About 15 percent of IoT device owners don't change their devices' default passwords.

About 10 percent of IoT devices use one of the same five passwords for administrative access.

Credit card authentication chips (aka Europay, Mastercard, and Visa—EMV—chips) have finally reached widespread U.S. adoption, catching up on decades of use elsewhere around the world. These chips greatly improve credit card security. Their design blunts magnetic-stripe skimming and traditional point-of-sale (POS) malware. Criminals, unfortunately, won't give up simply because better defenses exist. In 2019, adversaries may adapt to EMV's adoption with several new or evolutionary tactics.

ATM EMV

An evolutionary next-step might be for criminals to repurpose ATM EMV malware for retail environments.

Near-Field Communications (NFC)

In the future, criminals may exploit NFC applications in the same ways that we think they will abuse EMV technology.

CHIP AND PIN MAY FALL SHORT

Criminals may use EMV chip cards for the command-and-control (C2) of malware on infected EMV device readers. This tactic can be traced back to 2013's Skimmer[15] malware and 2016's Ripper[16] malware. These families use a malicious EMV chip to authenticate and grant access to hidden menus within ATMs already infected with the malware.

An evolutionary next-step might be for criminals to repurpose ATM EMV malware for retail environments. In one scenario, a criminal infects a POS machine with EMV malware, possibly by inserting a malicious USB drive. The adversary then, in an otherwise normal transaction, interacts with the malware by introducing an altered EMV chip to the POS terminal.

Criminals, alternatively, might exploit the EMV protocol. Embedded systems generally allow elevated trust when interacting at the hardware level. This trend follows with EMV readers. During an EMV transaction, the card may list functions to perform and files and records to be read. Because the EMV protocol does not specify which files must be read, all files must be read. Adversaries have several potential avenues for executing arbitrary code. The EMV protocol also only has processing restrictions concerning financial authorization, not code integrity.

Looking further to the future, criminals may exploit NFC applications in the same ways that we think they will abuse EMV technology. Instead of interacting with malware via EMV chips, criminals might identify new ways to use NFC-ready devices as consumers increasingly present their mobile phones to authorize transactions.

What you can do to mitigate this threat:

- Ensure that logical and physical access to POS machines is restricted to only the users and accounts that require access, and disable access methods like USB where possible.
- Increase monitoring at the file-system level on EMV-enabled POS machines to alert when files are being accessed outside of normal operations.

Today, adware that can evade antivirus and maintain persistence is pervasive across many industries. In 2019, ambitious criminal and state-linked threat groups may leverage adware in their campaigns, taking advantage of adware networks' recent technical improvements and multitudinous victims, and security organizations' tendency to downplay adware's threat.

Adware no longer confines itself to serving annoying, but generally harmless advertisements.

This year, Booz Allen threat hunters discovered adware installers that use in-memory fileless techniques to install their payload, making them highly resistant to forensic analysis.

THE WEAPONIZATION OF ADWARE NETWORKS

Adware is thought of as a minor nuisance by most organizations and is widely ignored by security operations. Traditionally, adware has not done much more than show advertisements and has been reliably detected by antivirus solutions. However, newer forms of adware have adopted techniques pioneered by state actors to improve their ability to persist on a host and infect more machines. Today, adware that can evade antivirus and maintain persistence is pervasive across many industries. In 2019, ambitious criminal and state-linked threat groups may leverage adware in their campaigns, taking advantage of adware networks' recent technical improvements and multitudinous victims, and security organizations' tendency to downplay adware's threat.

Recent developments

Several recent developments in the adware space make it especially appealing to enterprising adversaries. An early example of advanced adware was found in "Operation Aurora," reported in late 2016.[17] This adware used advanced methods to evade detection and covertly install itself on the victim's machine while providing a backdoor to allow the installation of further payloads. More recently, the Pbot adware adopted additional functionality that allows an adware network owner to install coin-mining software alongside the adware to increase profits.[18] This year, Booz Allen threat hunters discovered adware installers that use in-memory fileless techniques to install their payload, making them highly resistant to forensic analysis.[19] The common factor in these examples is that adware no longer confines itself to serving annoying, but generally harmless advertisements.

A doorway to existing botnets

In 2019, adversaries may leverage the current adware landscape in several ways. Much like botnet vendors have known for years, adware owners may soon also recognize the value of selling information they've collected—typically, large volumes of user profiling data used to serve ads—or selling direct access to infected endpoints. Adversaries could pay for access to existing botnets, which might provide an effective smokescreen against attribution, or, in the case of state groups, coerce criminal owners to share access. Lastly, enterprising actors could retool and redesign their operations to look like adware and benefit from security operators disregarding their access to a network.

What you can do to mitigate this threat:

- Instruct defenders to treat adware alerts as potential threats and/or incidents, rather than a nuisance or low-level issue.
- Create a force-multiplier effect to your security operation by integrating effective managed services that can deliver contextualized defenses combining people, processes, and technology.
- Implement heuristic-based endpoint detection capabilities (vs. traditional antivirus) to detect and prevent more serious attacks that originate from adware networks.
- Restrict standard users' ability to install software and internet browser plugins.

Artificial intelligence (AI) is a major force across many industries and technologies, particularly cybersecurity. Identifying new, potentially malicious applications of AI is important for network defenders, policy planners, and a wide variety of other stakeholders. While AI may enable a range of new cyber threats, one of the most likely threats to emerge in the coming years is the use of AI-generated video content in influence operations.

Examples of deepfakes in 2018 included forged video of a public address by former president Barack Obama—the video itself was produced for a report on the risks of deepfakes technology[20]—as well as modifications of prominent films to replace the faces of actors.

Notably, both examples were made using publicly available software.[21] Consumer apps designed to generate false video and audio content are becoming more prevalent, and advances in academic research lay the groundwork for increasingly realistic forgeries.[22]

DEEPFAKES IN THE WILD—AI IN INFORMATION WARFARE

AI-generated video—commonly referred to as "deepfakes"—use machine-learning algorithms to create highly believable forgeries that can be used to depict individuals saying or doing things that never occurred. The use of these techniques could be particularly appealing to threat actors interested in weaponizing data for influence operations. Attributing false quotes to political leaders is a tactic that has already been used by likely state-sponsored threat actors to significant effect. In May 2017, the website of the Qatar News Agency (QNA) and the Qatari government's Twitter page were defaced with false quotes attributed to the Qatari Emir; the incendiary quotes prompted widespread condemnation of the Qatari government and the severing of diplomatic and economic ties by more than a dozen nations throughout the Middle East and North Africa.[23] In July 2017, U.S. intelligence officials attributed the defacement to Emirati government actors.[24]

The incorporation of malicious deepfakes could be a valuable tactic for increasing the effectiveness of cyber operations intended to spread false information, discredit or damage the reputation of targeted organizations, or even create political turmoil and spur international conflict. Weaponized leaks—in which data is stolen and released publicly, sometimes with falsified data blended in—have increasingly been leveraged in influence operations.[25] This tactic could similarly incorporate false video content mixed among a trove of stolen, but otherwise legitimate data, to increase the believability of the ruse.

Deepfakes may represent a significant, emerging threat, though one potential solution for combating the malicious use of these techniques may be found in existing digital signature technology.

Ubiquitous digital media signing could help determine the integrity and origin of potentially forged content and verify its authenticity, in the same way that other digital communications are signed and verified today. However, this approach would not be without pitfalls. The technology companies producing the rapidly expanding sources of video content—such as video content mobile apps—may not be interested in integrating such security measures, and the individuals who produce potentially impactful real video footage may not want the risk of it being tied back to them.

Regardless of the solution, the threat of weaponized deepfakes is on the horizon.

What you can do to mitigate this threat:

- Develop a reputation-monitoring capability to alert your public relations and communications teams of breaking negative news about your organization, true or not. Conduct regular proactive outreach on social media to establish your public relations team as a trusted source of news to combat these misinformation campaigns.
- Engage your leadership and communications teams in tabletop exercises to plan and practice handling the types of reputation attacks which are most likely to target your organization.

THE RISE OF DEEPFAKES

PREMISE

Threat actors routinely spread false information online to generate controversies, often for political, economic, or ideological gain.

AI can realistically swap out content in video, images, and audio, creating deceptive content commonly called “deepfakes”.

Software to create deepfakes is now freely available and rapidly improving.

IMPLICATIONS...

The application of AI in deepfakes increases the effectiveness of the spread of false information and makes it easy to conduct reputation attacks.

...FOR THE ENTERPRISE

Reputational and/or financial impact is at stake.

The tech companies creating products used to produce or share potentially weaponized digital content may not be aware of the malicious use and downstream impact on them.

Wireless attacks targeting devices communicating via WiFi are well-trodden ground for attackers and network defenders alike. However, the expansion of IoT devices in enterprise networks that may communicate via proprietary or other non-WiFi wireless protocols may be increasing organizations' attack surfaces and exposure to risk. Technologies such as software-defined radio (SDR) are becoming more accessible to researchers, hobbyists, and potential threat actors. This technology could enable the creation of new attack vectors against wireless devices that may not be secured or even considered in network security assessments.

Security researchers have disclosed several high-profile Bluetooth vunerabilities in the past two years:

BlueBorne

BleedingBit

NEW FRONTIERS—THE EXPANDING WIRELESS ATTACK SURFACE

Examples of researchers—and threat actors—expanding the bounds of wireless attacks have already emerged with a wave of vulnerability disclosures and in-the-wild attacks targeting Bluetooth devices. Security researchers have disclosed several high-profile vulnerabilities in the past two years—such as BlueBorne and, more recently, BleedingBit—that impacted billions of devices running major mobile, desktop, and IoT operating systems, as well as networking equipment, including enterprise wireless access points.[26] Though large campaigns targeting these vulnerabilities did not materialize, threat actors have begun to incorporate Bluetooth-based attack vectors into their malicious toolsets. For example, in April 2018, researchers detailed a cyber-espionage campaign distributing the Android malware Henbox, which—in addition to using WiFi-based notifications from smart home devices to trigger espionage functions—had recently expanded its requested permissions on infected devices to enable the malware to discover, pair, and connect with Bluetooth devices.[27]

A "canary in the coal mine"

This activity targeting Bluetooth devices is likely a product of the technology's ubiquitous presence on both commercial and consumer equipment; however, it may serve as the "canary in the coal mine" for similar attacks against other wireless protocols. In recent years, security researchers have used software-defined radio (SDR)—custom hardware and software systems used to interact with wireless devices—to conduct a range of novel attacks, including spoofing satellite-based communications, overriding car locking systems, and conducting command injection attacks against smart home appliances.[28] Most recently, in April 2018, researchers demonstrated an ability to hijack emergency sirens via wireless attacks and issue custom broadcast commands.[29] Also in April 2018, the U.S. Food and Drug Administration (FDA) issued an alert to patients using a particular heart implant to update their device firmware, as the implants were found to be vulnerable to wireless cyber attacks using "commercially available equipment."[30] Though each of these events was the product of research and responsible disclosure, the underlying technology used to demonstrate these vulnerabilities is widely available. For example, professional penetration frameworks have begun incorporating hardware and software extensions to enable testing of wireless devices outside the standard WiFi spectrum.[31]

Potential for novel attacks

These new technologies could pave the way for threat actors to discover new—and insecure—attack vectors, expanding the attack surface on enterprise networks and even creating potential for abuse of vendors' products in attacks against their customers. In response to the increasing access to technologies that may enable threat actors to more effectively probe devices' wireless communications for vulnerabilities, companies producing products that use proprietary wireless protocols—such as implanted medical devices—should prioritize security testing in the product development process. Similarly, companies that may deploy devices using propriety wireless communications—such as IoT used for building automation, safety and security, and industrial control functions—should consider expanding attack surface assessments.

What you can do to mitigate this threat:

- Disable unused wireless protocols where possible, such as Bluetooth on laptops and desktops.
- Expand the scope of existing attack surface and penetration test assessments to include known propriety wireless protocols exposed to the public.

NOVEL TECHNOLOGIES

Security researchers have used software-defined radio (SDR) to conduct a range of novel attacks, including spoofing satellite-based communications, overriding car locking systems, and conducting command injection attacks against smart home appliances.

NOVEL ATTACKS

In April 2018, researchers demonstrated an ability to hijack emergency sirens via wireless attacks and issue custom broadcast commands.

Patients using a particular heart implant were vulnerable to wireless cyber attacks using "commercially available equipment."

These new technologies could potentially pave the way for threat actors to discover new attack vectors, expanding the attack surface on enterprise networks.

For the past few decades, the United States has struggled to solidify its strategy for responding to foreign-government-sponsored cyber operations. Since the Obama administration first used the "name-and-shame"[32] strategy in 2014, the Trump administration has elevated its use from occasional to routine. In 2019, this naming-and-shaming agenda will likely compel state-linked groups to place much greater emphasis on their operational security to deny, deflect, and degrade attribution.

RUSSIA

In 2018, the United States faulted Russia for targeting the U.S. power grid, being involved in the VPNfilter and NotPetya attacks, and surveilling anti-doping and nuclear watchdog groups.

NORTH KOREA

In 2014, U.S. government naming-and-shaming reaffirmed many industry assessments that North Korea had used the "Guardians of Peace" front group to take the blame for the infamous Sony breach.

STATE-SPONSORED THREAT ACTORS DOUBLE-DOWN ON DECEPTION

The United States now regularly and publicly accuses other countries for sponsoring attacks and campaigns. In 2018, the United States faulted Russia for targeting the U.S. power grid,[33] being involved in the VPNfilter[34] and NotPetya[35] attacks, and surveilling anti-doping and nuclear watchdog groups.[36] The United States has, on occasion, coordinated these accusations with other countries, such as the other Five Eyes allies—the United Kingdom, Australia, New Zealand, and Canada—and the Netherlands.[37] While certain other countries have been similarly willing to routinely identify their assailants—Ukraine[38] and South Korea[39] have long called out attacks by Russia and North Korea—the United States' ability to unilaterally issue sanctions and recruit naming-and-shaming allies likely poses a greater risk to adversaries.

Taking precautions to prevent or frustrate clear attribution has long played a role in cyber spycraft, albeit in varying degrees for different groups. That said, major U.S. government naming-and-shaming has not been known to upset common assessments of groups that tried to frustrate attribution, like North Korea's use of the "Guardians of Peace" front group in the Sony breach and Iran's use of the "Qassam Cyber Fighters" front group in U.S. financial sector disruptions. Historically, the private threat intelligence community's consensus has typically been confirmed when the U.S. intelligence community revealed its conclusion.

Raising their game

However, a multitude of muddled private-sector assessments in 2017 and 2018 suggest that state-groups may have raised their game. Conflicting attempts to attribute the Triton malware discovered in Saudi Arabia—with initial reports attributing the malware to Iran[40] only to be contradicted by recent reports of its possible Russian origin[41] —may have stemmed from state-linked groups' improved obfuscation, misdirection, and deception. Similarly, in July 2018, a phishing campaign targeting a U.K. engineering firm was initially attributed to the China-aligned group "Temp. Periscope," or "Leviathan." Further analysis revealed that this campaign had used several tools and tactics historically associated with Russian state actors APT28 and Dragonfly, calling the initial attribution into doubt.[42]

Most recently, in November 2018, the cybersecurity community begrudgingly reigned in its initial excitement after attributing a phishing campaign targeting the U.S. government and commercial sectors to a Russian FSB-managed group (aka Cozy Bear, APT29).[43] Perhaps a group was mimicking APT29 or the otherwise cautious APT29 was deliberately sloppy this time to generate skepticism.

In 2019, redoubled emphasis on deception will likely characterize many cyber operations, making accurate attribution a likely casualty.

Lowering attribution confidence

Adversaries can exploit several weaknesses of current attribution trends. The cybersecurity community sometimes conflates tool use with adversary identity, encouraging adversaries to exploit these expectations by using or deploying other groups' "signature" tools. Confirmation bias occasionally taints analysis when attacks on certain data, industries, and countries occur—attacks seemingly consistent with other "known" threat actors, allowing adversaries to act in "unusual" ways that lowers attribution confidence.

Sparse evidence in some public attributions by government and industry—perhaps held back for national security or proprietary commercial interests rather than a lack of solid evidence—creates room for adversaries to create or promote alternative theories. As attributions initially reported as clear-cut are increasingly refuted, consumer and industry confidence in attribution analysis will likely suffer a corollary decrease, a targeted outcome that serves to further insulate state-linked activity and the motivations of state benefactors. This redoubling of counter-attribution efforts will likely result in lower-confidence assessments, public guessing games, and speculative reporting that will complicate tactical-level detection and strategic threat modeling.

What you can do to mitigate this threat:

- Assume that advanced attackers may utilize commodity malware and advanced tradecraft in some combination with deception in mind.
- Focus your incident response and preparedness efforts beyond attribution; spend time learning from the tactics, techniques, and procedures of the attack to spot future attacks earlier in the kill-chain to mitigate future loss.

For the past decade, the energy sector's industrial control systems (ICS) have been a prime target for state-sponsored attacks. Despite focusing on energy companies, state adversaries could achieve similar goals by targeting other critical ICS-reliant sectors, transferring the same skill set to different ICS operating environments. In 2019, Booz Allen notes a plausible uptick in state-sponsored attacks and intrusions at water utilities, an equally critical but likely less secure sector.

Though it's difficult to say why any specific attack or intrusion occurred, the reasons state adversaries might target energy and water firms are many.

Disruptions of energy companies, like electric utilities and petroleum processors, and water utilities, like dams and sewage treatment facilities, can cause downstream economic and social harm.

Even non-disruptive intrusions, when made public, can ignite general alarm and fear.

WATER-UTILITY TARGETING BUBBLES TO THE SURFACE

The U.S. energy sector is one of better-secured ICS-reliant sectors in the country. Several factors led to this point. The sector has long prioritized cybersecurity, as seen in its mature information-sharing efforts like the electric power industry's Electricity Information Sharing and Analysis Center (E-ISAC) and its collaboration with the government to set security standards and promote best practices. The sector's recent trend toward consolidation[44] likely also shapes its security. Larger companies naturally have greater wherewithal to staff and support security teams than smaller firms and can benefit from unified management, reduced capability duplication, and improved purchasing power.

Meanwhile, U.S. water utilities lag behind on these fronts. According to the American Water Works Association, the industry deals with a "splintered regulatory regime," "a lack of cybersecurity governance protocols," high diversity in organizational size, and personnel who "may lack the knowledge or experience" necessary to prevent and respond to cyber attacks.[45]

Indeed, government regulation of water utilities' cybersecurity is less exhaustive, with a greater focus on improving resilience amid natural disasters, rather than cyber attacks.[46] While water utilities are consolidating,[47] they remain more fractured than the energy industry and likely have not broadly reaped similar security benefits from consolidation.

State-linked adversaries probably consider the water supply to be a vulnerable social and economic pain point, like the electricity supply. Ukrainian security services allege that, in December 2015 and 2016, Russian government hackers twice caused local blackouts by attacking electric utility companies. In July 2018, Ukraine claimed[48] to have disrupted a Russian intrusion at the only Ukrainian facility[49] that provides liquid chlorine for water and sewage treatment plants. The adversary had reportedly accessed the "process control system and [a] system for detecting signs of emergencies." At the time, chlorine distribution was a major domestic issue. Two weeks prior to the attack's unveiling, the plant stopped its operations for alleged economic reasons, resulting in widespread shortages and public concern.[50]

At a minimum, U.S. water companies should expect reconnaissance activity by foreign state-backed groups attempting to gain insight about and access to water utilities. According to the FBI and DHS, U.S. water utilities are already in state-backed adversaries sights. These agencies linked intrusions at U.S. water processing plants to Russia[51] and at a small Connecticut dam to Iran.[52] No disruptions were publicly linked to these intrusions, consistent with reconnaissance and contingency planning.

At present, Booz Allen believes that disruptive state-sponsored cyber attacks on U.S. water utilities are unlikely, but water disruption attacks are relevant for many U.S. companies with global footprints. Such attacks are highly aggressive and would be inflammatory and escalatory if conducted by a U.S. competitor against a U.S. water utility. For this reason, water utilities of several countries already caught in kinetic conflict are more plausible targets for future disruptions, for example, the ongoing Ukraine-Russia[53] and Saudi Arabia-Iran hostilities.[54] These conflicts are highly relevant to foreign companies operating there, as water disruptions may present a business risk necessitating relevant risk-management strategies.

What you can do to mitigate this threat:

- Secure these systems from the ground up with a focus on multi-layered segmentation and threat detection to ensure their ongoing, safe operation.
- Include lack of water access in disaster preparedness activities to plan for the worst case scenario.

WATER UTILITIES: THE NEW TARGET OF CYBER ATTACKS

A PERFECT TARGET

Vulnerable social and economic pain point

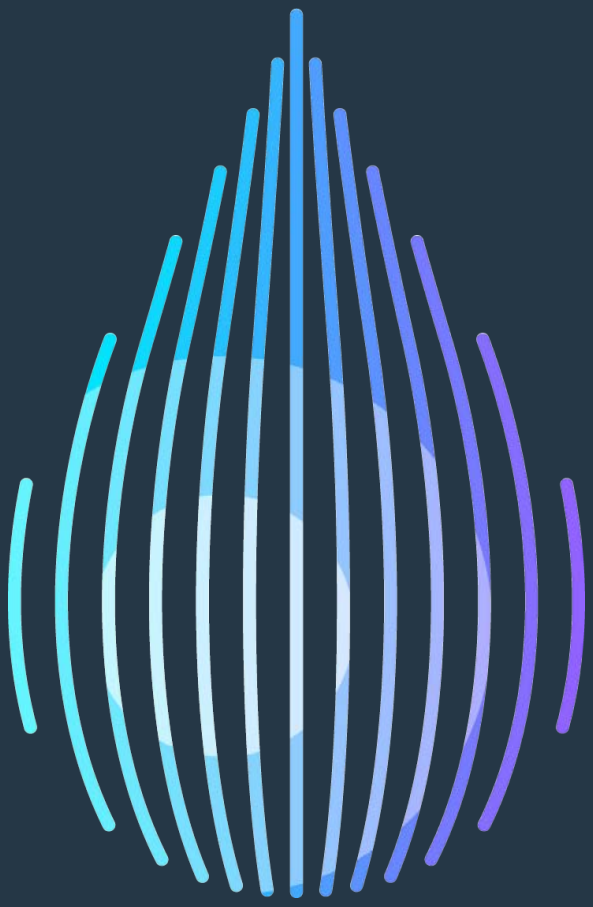
Fragmented sector

Splintered regulatory regime

Lack of cybersecurity goverance protocols

High diversity in organizational size

Inexperienced personnel in cybersecurity



WARNINGS

According to the FBI and DHS, U.S. water utilities are already in state-backed adversary sights.

These agencies linked intrusions at U.S. water processing plants to Russia and at a small Connecticut dam to Iran.

For now, disruptive state-sponsored cyber attacks on U.S. water utilities are unlikely...

...But water disruption attacks are relevant for many U.S. companies with global footprints.

CONCLUSION

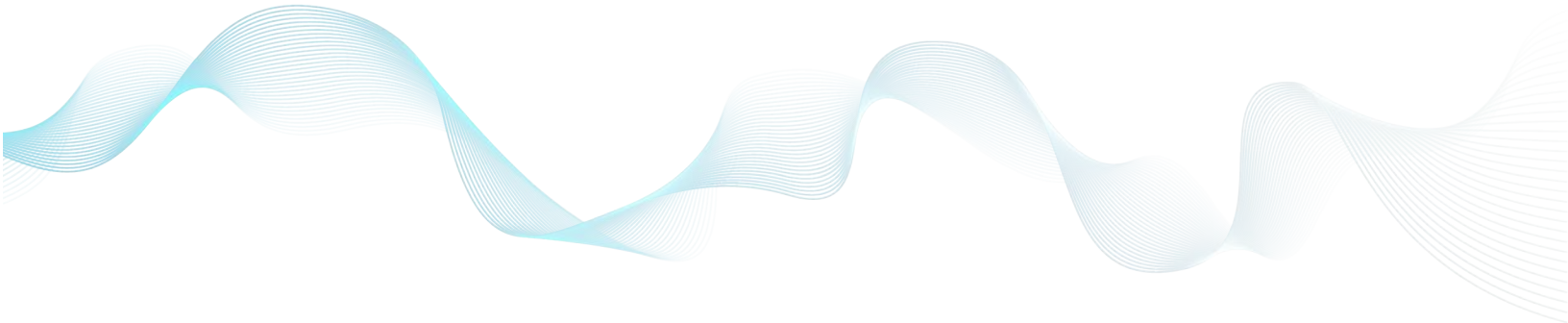
We, like all analysts and defenders, know one of the biggest challenges in managing cyber risk is uncertainty. The most dangerous adversaries force defenders out of their comfort zones and catch organizations flat-footed, using the unexpected to their advantage. These actors shift their targets and objectives suddenly. They are creative, imaginative, and agile. Defenders need to be the same. Organizations can use forward-focused thinking to prepare for uncertainty and think creatively about their security posture. If they don't, they may spend more money on products and compliance box-checking with questionable payoff.

Booz Allen has consistently seen that the most effective cyber defense is having an agile leadership team continuously prioritizing risk based upon relevant threats. We call this approach relentless preparation.

This year, we recommend that organizations shift their approach away from a security compliance focus and develop a culture of security. This culture should permeate not only the different security elements that make up the broader security enterprise but also the interrelated business operations and risk management teams. Converting plans and resources to a security-focused mindset ensures that relentless preparation is a constant, joint effort. Developing talent immediately upon hire to retain junior and skilled professionals—through industry immersion, opportunities for professional advancement and skill-sharpening training—is critical to establishing this culture. Stopping an attack before it happens with the right approach, rather than waiting to react, is evidence of effective relentless preparation.

As we observe the cyber professional talent struggle persist, we also recommend that companies complement their existing detection and intelligence capabilities with a robust service that can optimize their resources and provide constant operational visibility of threats. An intelligence-driven, proactive, and tested security function ultimately drives defensive security.

Some threats may inspire tactically directed threat hunting or operational-level process improvement, while others may spur higher level crisis-response strategy development and new intelligence collection requirements. Whatever the appropriate defensive measure, we believe this relentless preparation will position your organization to be ready for what's next in 2019.



REFERENCES

1. Annaliese Milano, "The Next Petro? Iranian Minister Reveals Cryptocurrency Plans," CoinDesk, last modified February 22, 2018, accessed December 4, 2018, https://www.coindesk.com/next-petro-iranian-minister-reveals-cryptocurrency-plans; "Iran could turn to cryptocurrencies to evade some sanctions," Mehr News Agency, October 29, 2018, accessed November 27, 2018, hxxps://en.mehrnews.com/news/139158/Iran-could-turn-to-cryptocurrencies-to-evade-some-sanctions; "Iran closer to own digital money as sanctions loom," PressTV, last modified July 25, 2018, accessed November 27, 2018, hxxps://www.presstv.com/Detail/2018/07/25/569249/Iran-closer-to-own-digital-money-as-sanctions-loom.

2. Richard Allen, "Russia is considering launching a state-backed cryptocurrency," Chepicap, November 3, 2018, accessed December 4, 2018, https://www.chepicap.com/en/news/4900/russia-considering-launching-a-state-backed-cryptocurrency.html.

3. "North Korean Hackers Stole Cryptocurrencies Worth $571 Million This Year," NDTV, October 20, 2018, accessed December 4, 2018, https://www.ndtv.com/world-news/north-korean-hackers-group-lazarus-steals-cryptocurrencies-worth-571-million-this-year-1934849; "$571 Million: Notorious North Korean Hacker Group Has Stolen a Fortune in Cryptocurrency," CCN, October 19, 2018, accessed December 4, 2018, https://www.ccn.com/571-million-notorious-north-korean-hacker-group-has-stolen-a-fortune-in-cryptocurrency/.

4. "SamSam: Targeted Ransomware Attacks Continue," Symantec, last modified November 29, 2018, accessed December 4, 2018, https://www.symantec.com/blogs/threat-intelligence/samsam-targeted-ransomware-attacks; " SamSam Ransomware Chooses Its Targets Carefully," Sophos, April 2018, accessed December 4, 2018, https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/SamSam-ransomware-chooses-Its-targets-carefully-wpna.pdf.

5. Elia Flori and Lior Ben Porat, "Attack inception: Compromised supply chain within a supply chain poses new risks," Microsoft Secure, July 26, 2018, accessed October 3, 2018, https://cloudblogs.microsoft.com/microsoftsecure/2018/07/26/attack-inception-compromised-supply-chain-within-a-supply-chain-poses-new-risks/.

6. Kim Zetter, "The Crisis of Election Security, " *The New York Times Magazine*, September 26, 2018, accessed December 4, 2018, https://www.nytimes.com/2018/09/26/magazine/election-security-crisis-midterms.html.

7. Graham Lanktree, "Russian Bots Are Sticking Up For Sean Hannity By Attacking Keurig, As Fans Smash Coffee Makers," *Newsweek*, November 13, 2017, accessed November 20, 2018, https://www.newsweek.com/sean-hannity-advertiser-keurig-attacked-russian-bots-after-far-right-protest-709128

8. Rakesh Krishnan Simha, "How Ukraine's new Antonov aircraft may create problems for Russia and India," April 18, 2017, accessed December 19, 2018, hxxps://www.rbth.com/blogs/stranger_than_fiction/2017/04/18/how-ukraines-new-antonov-aircraft-may-create-problems-for-russia-and-india_744997

9. "Авиаконцерн "Антонов" пожаловался на хакерскую атаку," Realist, January 18, 2018, accessed January 19, 2018, hxxps://realist.online/news/aviastroitelnyj-koncern-antonov-pozhalovalsya-na-hakerskuyu-ataku; " "Антонов" обвинил Гройсмана в препятствовании работе предприятия," Realist, January 17, 2018, accessed January 19, 2018, hxxps://realist.online/news/antonov-obvinil-grojsmana-v-prepyatstvovanii-rabote-predpriyatiya.

10. "New Report - Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy," *Freedom House*, November 14, 2017, accessed November 20, 2018, https://freedomhouse.org/article/new-report-freedom-net-2017-manipulating-social-media-undermine-democracy.

11. "Iran's New Facebook Trolls Are Using Russia's Playbook," *Wired*, October 26, 2018, accessed November 20, 2018, https://www.wired.com/story/iran-facebook-trolls-using-russia-playbook/.

12. "Connection Proxy," MITRE ATT&CK, accessed 7 December 2018. https://attack.mitre.org/techniques/T1090/

13. Waylon Grange, "Blue Coat Exposes 'The Inception Framework'; Very Sophisticated, Layered Malware Attack Targeted at Military, Diplomats, and Bus," Symantec official blog, 9 December 2014, accessed 7 December 2018. https://www.symantec.com/connect/blogs/blue-coat-exposes-inception-framework-very-sophisticated-layered-malware-attack-targeted-milit

14. Catalin Cimpanu, " 15% of All IoT Device Owners Don't Change Default Passwords," *Bleeping Computer*, 19 June 2017, accessed 7 December 2018. https://www.bleepingcomputer.com/news/security/15-percent-of-all-iot-device-owners-dont-change-default-passwords/

15. "Trojan.Skimer.18 infects ATMs," Dr. Web, 16 December 2018, accessed 7 December 2018. https://news.drweb.com/show/?i=4167&lng=en

16. Tom Spring, "RIPPER ATM Malware Uses Malicious EMV Chip," *Threatpost*, 29 August 2016, accessed 7 December 2018. https://threatpost.com/ripper-atm-malware-uses-malicious-emv-chip/120192/

17. Ben Tedesco, "Security Advisory: Adware Uses Advanced Nation-State Obfuscation Techniques to Deliver Ransomware," Carbon Black, 23 September 2016, accessed 7 December 2018. https://www.carbonblack.com/2016/09/23/security-advisory-variants-well-known-adware-families-discovered-include-sophisticated-obfuscation-techniques-previously-associated-nation-state-attacks/

18. Anton V. Ivanov, " Pbot: evolving adware," Securelist, 26 June 2018, accessed 7 December 2018. https://securelist.com/pbot-evolving-adware/86242/

19. Jay Novak, Dan Rossell, Ashleigh Moriarty, and Fred Frey, "Advanced Persistent Adware: Analysis of Nation-State Level Tactics," Booz Allen Hamilton blog, accessed 7 December 2018. https://www.boozallen.com/s/insight/blog/advanced-persistent-adware.html

20. Video hosted on Buzzfeed, accessed 7 December 2018: https://video-player.buzzfeed.com/embed?video_id=52602

21. Craig Silverman, "How To Spot A Deepfake Like The Barack Obama–Jordan Peele Video," BuzzFeed News, 17 April 2018, accessed 7 December 2018. https://www.buzzfeed.com/craigsilverman/obama-jordan-peele-deepfake-video-debunk-buzzfeed

22. Aayush Bansal, Shugao Ma, Deva Ramanan, and Yaser Sheikh, " Recycle-GAN: Unsupervised Video Retargeting," Carnegie Melon University, accessed 7 December 2018. https://www.cs.cmu.edu/~aayushb/Recycle-GAN/recycle_gan.pdf

23. "Qatar investigation finds state news agency hacked: foreign ministry," Reuters, accessed August 17, 2017, http://www.reuters.com/article/us-gulf-qatar-cybercrime-idUSKBN18Y2X4; "Qatar-Gulf crisis: Your questions answered," Al Jazeera, 5 December 2017, accessed 22 March 2018, hxxps://www.aljazeera.com/indepth/features/2017/06/qatar-gulf-crisis-questions-answered-170606103033599.html.

24. "UAE orchestrated hacking of Qatari government sites, sparking regional upheaval, according to U.S. intelligence officials," *Washington Post*, 16 July 2017, accessed 22 March 2018, https://www.washingtonpost.com/world/national-security/uae-hacked-qatari-government-sites-sparking-regional-upheaval-according-to-us-intelligence-officials/2017/07/16/00c46e54-698f-11e7-8eb5-cbccc2e7bfbf_story.html?utm_term=.34d907915bc3.

25. Adam Hulcoop, John Scott-Railton, Peter Tanchak, Matt Brooks, and Ron Deibert, " TAINTED LEAKS: Disinformation and Phishing With a Russian Nexus," The Citizen Lab, 25 May 2017, accessed 7 December 2018. https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/

26. "BlueBorne Vulnerabilities Impact Amazon Echo and Google Home." Armis, accessed 7 December 2018. https://armis.com/blueborne/; " BleedingBit Exposes Enterprise Access Points and Unmanaged Devices to Undetectable Chip Level Attack," Armis, accessed 7 December 2018. https://armis.com/bleedingbit/

27. Alex Hinchliffe, Mike Harbison, Jen Miller-Osborn, and Tom Lancaster, " HenBox: Inside the Coop," PaloAlto, 26 April 2018, accessed 26 April 2018, https://researchcenter.paloaltonetworks.com/2018/04/unit42-henbox-inside-coop/#Appendix.

28. Huang Lin, Yang Qing, "GPS Spoofing by Low-cost SDR Tools" Qihoo 360 Technology Co. Ltd., August 2015, accessed September 7, 2017, http://powerofcommunity.net/poc2015/huang.pdf; Andy Greenberg, "Watch this Wireless Hack Pop a Car's Locks in Minutes," *Wired*, August 4, 2014, accessed September 7, 2017, https://www.wired.com/2014/08/wireless-car-hack; Florian Eichelberger, "Using Software Defined Radio to Attack 'Smart Home' Systems," SANS Institute, September 2014, accessed September 7, 2017, https://www.sans.org/reading-room/whitepapers/threats/software-defined-radio-attack-smart-home-systems-35922.

29. Kim Zetter, " This Is Not a Test: Emergency Broadcast Systems Proved Hackable," *Wired*, 7 August 2013, accessed 24 July 2018, https://www.wired.com/2013/07/eas-holes/; Lorenzo Franceschi-Bicchierai, " Researchers Rickrolled Emergency Alert Sirens in Proof-of-Concept Hack," MotherBoard, 10 April 2018, accessed 24 July 2018, https://motherboard.vice.com/en_us/article/9kgn4v/hackers-take-over-san-franciscos-emergency-sirens.

30. https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm604706.htm

31. "Rapid7 Enables IoT Hardware Security Testing with Metasploit," Rapid7, February 2, 2017, accessed September 7, 2017, https://www.rapid7.com/about/press-releases/rapid7-enables-iot-hardware-security-testing-with-metasploit; "Metasploit's RF Transceiver Capabilities," Rapid7, March 21, 2017, accessed September 7, 2017, https://blog.rapid7.com/2017/03/21/metasploits-rf-transceiver-capabilities.

32. Aruna Viswanatha and Joseph Menn, "In cyberattacks such as Sony strike, Obama turns to 'name and shame'," Reuters, January 14, 2015, accessed December 17, 2018, https://www.reuters.com/article/uk-usa-cybersecurity/in-cyberattacks-such-as-sony-strike-obama-turns-to-name-and-shame-idUSKBN0KN2E520150114.

33. Dustin Volz and Timothy Gardner," In a first, U.S. blames Russia for cyber attacks on energy grid," Reuters, 15 March 2018, accessed 7 December 2018. https://www.reuters.com/article/us-usa-russia-sanctions-energygrid/in-a-first-u-s-blames-russia-for-cyber-attacks-on-energy-grid-idUSKCN1GR2G3

34. Shaun Nichols,"FBI agents take aim at VPNFilter botnet, point finger at Russia, yell 'national security threat'" *The Register*, 24 May 2018, accessed 7 December 2018. https://www.theregister.co.uk/2018/05/24/fbi_vpnfilter_botnet/

35. Dustin Volz, " U.S. blames Russia for crippling 2017 'NotPetya' cyber attack," Reuters, 15 February 2018, accessed 7 December 2018. https://www.reuters.com/article/britain-russia-cyber-usa/u-s-blames-russia-for-crippling-2017-notpetya-cyber-attack-idINKCN1FZ2VH

36. Bill Chappell and Carrie Johnson, "U.S. Charges 7 Russian Intelligence Officers With Hacking 40 Sports And Doping Groups," National Public Radio, 4 October 2018, accessed 7 December 2018. https://www.npr.org/2018/10/04/654306774/russian-cyber-unit-accused-of-attacking-opcw-chemical-weapons-watchdog

37. Ellen Nakashima et al., "U.S. and its allies target Russian cyber spies with indictments, public shaming," *Washington Post*, October 4, 2018, accessed December 14, 2018, https://www.washingtonpost.com/world/europe/britain-directly-blames-russian-military-intelligence-for-broad-range-of-cyberattacks/2018/10/04/13a3a1f8-c7b6-11e8-9158-09630a6d8725_story.html

38. "Ukraine Says Hit by 6,500 Hack Attacks, Sees Russian 'Cyberwar'" VOA News, 29 December 2016, accessed 7 December 2018. https://www.voanews.com/a/ukraine-says-hit-by-6500-hack-attacks-sees-russian-cyberwar/3655785.html

39. Se Young Lee, "Seoul Blames North for Bank Hack," *Wall Street Journal*, 4 May 2011, accessed 7 December 2018/ https://www.wsj.com/articles/SB10001424052748703922804576300562037789384

40. Eduard Kovacs, "Iran Used "Triton" Malware to Target Saudi Arabia: Researchers," *SecurityWeek*, 15 Deceber 2017, accessed 6 December 2018. https://www.securityweek.com/iran-used-triton-malware-target-saudi-arabia-researchers

41. "TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers," FireEye, 23 October 2018, accessed 6 December 2018. https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html

42. Insikt Group, "Chinese Threat Actor TEMP.Periscope Targets UK-Based Engineering Company Using Russian APT Techniques," Recorded Future blog, 13 November 2018, accessed 6 December 2018. https://www.recordedfuture.com/chinese-threat-actor-tempperiscope/

43. "Not So Cozy: An Uncomfortable Examination of a Suspected APT29 Phishing Campaign," FireEye, 19 November 2018, accessed 6 December 2018 https://www.fireeye.com/blog/threat-research/2018/11/not-so-cozy-an-uncomfortable-examination-of-a-suspected-apt29-phishing-campaign.html

44. Travis Hoium, " Why Consolidation is the Name of the Game in the Utility Space," The Motley Fool, 4 June 2016, accessed 17 December 2018. https://www.fool.com/investing/2016/06/04/why-consolidation-is-the-name-of-the-game-in-the-u.aspx; Jeff St. John, " The Top Trends Behind the Growing, Multibillion-Dollar Market for Utility Mergers and Acquisitions," Green Tech Media, 30 May 2014, accessed 17 December 2018. https://www.greentechmedia.com/articles/read/the-top-trends-behind-the-growing-multi-billion-market-for-utility-ma

45. "Cybersecurity Risk and Responsibility in the Water Sector (AWWA)" Water ISAC, 25 October 2018, accessed 17 December 2018. https://www.waterisac.org/portal/cybersecurity-risk-and-responsibility-water-sector-awwa-0

46. Carol Brzozowski, " Cybersecurity Strategies for Water Utilities," 7 August 2018, accessed 17 December 2018. Water Efficiency Weekly, Forester Network https://foresternetwork.com/weekly/water-efficiency-weekly/water-treatment/cybersecurity-strategies-for-water-utilities/

47. "The US water sector on the verge of transformation," EY, accessed 17 December 2018. https://www.ey.com/Publication/vwLUAssets/Cleantech_Water_Whitepaper/%24FILE/Cleantech-Water-Whitepaper.pdf

48. "На Дніпропетровщині СБУ попередила кібератаку російських спецслужб на об'єкт критичної інфраструктури, [In the Dnipropetrovsk Region, the SBU warned of a Russian Special Forces cyber attack against a critical infrastructure facility]" Security Service of Ukraine, 7 November 2018, accessed 17 December 2018. https://ssu.gov.ua/ua/news/1/category/2/view/5037#.w9lsUmco.dpbs

49. "О компании Аульская хлоропереливная станция, ООО [About the Auli Chlorine Overflow Station Company, LLC.]," Accessed 17 December 2018. https://aulskayahps.all.biz/info-about

50. Matthew Kupfer, " Chlorine shortage threatens clean water across Ukraine," Kyiv Post, 12 July 2018, accessed 17 December 2018. https://www.kyivpost.com/ukraine-politics/chlorine-shortage-threatens-clean-water-across-ukraine.html

51. "Alert (TA18-074A) Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," US-CERT, 15 March 2018, accessed 17 December 2018. https://www.us-cert.gov/ncas/alerts/TA18-074A; Steven Melendez, " Chlorine shortage threatens clean water across Ukraine," Fast Company, 15 March 2018, accessed 17 December 2018. https://www.fastcompany.com/40545116/the-fbi-makes-it-official-russia-is-attacking-us-energy-water-and-critical-systems

52. Joseph Berger, " A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case," *New York Times*, 25 March 2016, accessed 17 December 2018. https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html

53. Cynthia Buckley, Ralph Clem, Jarod Fox, and Erik Herron, "The war in Ukraine is more devastating than you know," *Washington Post*, 9 April 2018, accessed 17 December 2018. https://www.washingtonpost.com/news/monkey-cage/wp/2018/04/09/the-war-in-ukraine-is-more-devastating-than-you-know/?utm_term=.2da5d9c6a902

54. Julian Borger and Patrick Wintour, "US gives evidence Iran supplied missiles that Yemen rebels fired at Saudi Arabia," *Guardian*, 14 December 2017, accessed 17 December 2018. https://www.theguardian.com/world/2017/dec/14/us-gives-evidence-iran-supplied-missiles-that-yemen-rebels-fired-at-saudi-arabia

ACKNOWLEDGEMENTS

The 2019 Cyber Threat Outlook contributors

Nathaniel Beach-Westmoreland

Robert Brandon

Betsy Carmelite

Susannah Clark

Joshua Guild

Anthony Harris

Alexander Hellie

Brian Klenke

Phillip Mann

Kyle Miller

Gregory Schoeny

Michael Sechrist

Jacob Styczynski

John TerBush

Juliann Tuleya

Jonathan Womack

About Booz Allen

For more than 100 years, business, government, and military leaders have turned to Booz Allen Hamilton to solve their most complex problems. They trust us to bring together the right minds: those who devote themselves to the challenge at hand, who speak with relentless candor, and who act with courage and character. They expect original solutions where there are no roadmaps. They rely on us because they know that—together—we will find the answers and change the world. To learn more, visit BoozAllen.com.

To learn more, visit BoozAllen.com/MTS

Anil Markose
Senior Vice President
markose_anil@bah.com
+1-917-305-8007

Wade Alt
Vice President
alt_wade@bah.com
+1-571-437-7712