accenture

CYBER THREATSCAPE REPORT 2018

MIDYEAR CYBERSECURITY RISK REVIEW

CONTENTS

EXECUTIVE SUMMARY

When Accenture Security asked CISOs about the risks they face, 71 percent of respondents said cyberattacks are still a "bit of a black box; we do not quite know how or when they will affect our organization," a rise of 5 percent over the year.[1] In a more recent study, only 13 percent of organizations consider future threats when drawing up their security budgets.[2] These responses point to a clear need for more effective use of actionable threat intelligence.

71% OF RESPONDENTS SAID CYBERATTACKS ARE STILL A "BIT OF A BLACK BOX; WE DO NOT QUITE KNOW HOW OR WHEN THEY WILL AFFECT OUR ORGANIZATION."

Accenture Security iDefense threat intelligence analysts were not surprised to learn that 71 percent of organizations are still growing and expanding their knowledge of cyberattacks, hacktivist activities, cyber espionage, and other cyber threats. Organizations need to enhance their threat intelligence capabilities to stay ahead of cyber threats, not just activate their incident response plans when their network is breached. They need to expand their team's research capabilities, their ability to provide strategic insights, and grow their use of cyber research tools and technologies. Organizations must focus on building a data-driven approach fueled by threat intelligence to better anticipate potential attacks and develop a more proactive security posture for their businesses based on strategic, operational and tactical demands:

- Strategic—gaining the intelligence that informs decisions on policy, executive decisions and plans
- Operational—creating intelligence that informs decisions on choosing how to handle and respond on a day-to-day basis
- Tactical—having the intelligence to inform decisions on how to technically and specifically execute operations

Organizations should stay as current as possible on both the broader threat landscape and the specific threats that adversaries pose as they relate to the enterprise environment (Figure 1).

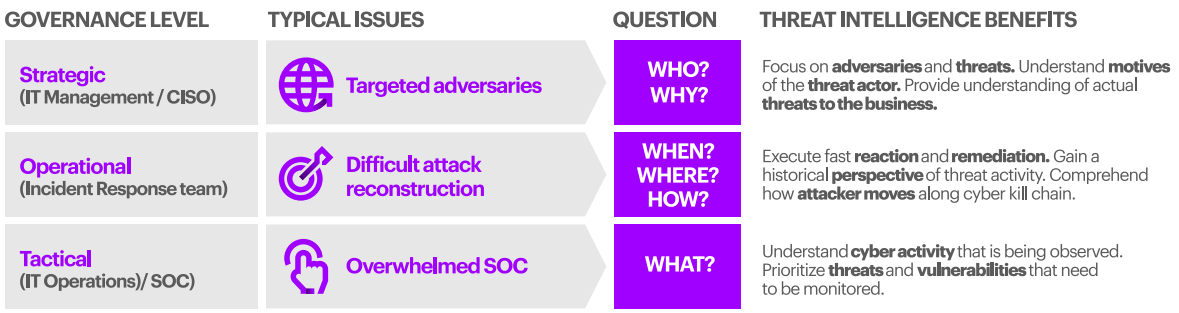

FIGURE 1

Strategic, operational and tactical threat intelligence issues and benefits

What's inside?

Cyber threat actors and threat groups are continuously networking, researching, and testing out new tactics, techniques, and procedures (TTPs). They are also always looking for new ways to disrupt operations, make money, or spy on their targets. iDefense threat intelligence analysts have observed multiple tactical shifts in terms of victim network targeting, use of attack tools and technologies, and use of up-and-coming monetary vehicles to attain maximum return on investment (ROI).

In the 2017 mid-year Cyber Threatscape Report, we discussed the continued development of Iran's cyber-espionage programs and influence operations. The expectations of growth in Iran's cyber-espionage activity described in that report have been realized. The threats posed by Android malware and ransomware developed in Iran and used by actors located in Iran are growing and expanding beyond levels seen prior to the past year. It is not just threat actors located in Iran from which iDefense threat intelligence is seeing more activity; threat actors and threat groups across the globe are broadening their attack scope. They are not just directly attacking chosen targets with spear-phishing campaigns and vulnerability exploitation; they are looking to reach their targets via the networks of third- or fourth-party supply chain partners by exploiting weaknesses in less modern technologies, or by attacking Internet of Things (IoT) and Industrial Internet of Things (IIoT) technologies—in the oil and natural gas industry, in particular—that were not originally designed with cyber defense in mind. The convergence of information technology (IT) and operational technology (OT) is opening doors to adversaries to disrupt operations, deploy crypto-mining malware, or to conduct deep-seated espionage operations.

Although the attribution of attacks is improving, and arrests have been made, when one cyber criminal is captured, a new one quickly emerges. Cyber defenders must continue to be vigilant and pivot their defense patterns quickly to meet the evolving attack vectors. Our observations, explored in detail in this report, identify key areas for concern:

IRANIAN THREAT

IS A GROWING FORCE TO BE RECKONED WITH

Iran-based threat actors and threat groups are likely to continue to grow their malicious activities and capabilities in the foreseeable future. iDefense threat intelligence analysts have uncovered evidence that the number of nation-state-sponsored cyberattacks has grown, and this is likely to continue. iDefense threat intelligence indicates that the Iranian government and hacktivists located in Iran pose a disruptive or destructive cyber threat against the United States, Europe, and the Middle East. Iran will likely focus much of its attention on other Middle Eastern nations; however, Iran-based threat actors have the potential to pivot their attacks to other nations, consumers, or businesses. Organizations, businesses, and governments should not ignore the Iran-based threat; they should proactively build resilience against it, especially against Android-based malware and ransomware, as Iran-based threat actors will likely use these as their cyber weapons of choice.

The attack surface for threat actors and threat groups growing and expanding. iDefense threat intelligence has been closely tracking the growth in number and types of Android-platform-specific malware. Threat actors are capitalizing on unofficial or third-party Android application marketplaces as their key destinations for malicious application delivery using obfuscation techniques. Threat actors also regularly attempt to disseminate malicious applications through the official Google Play Store to appear legitimate and reach a larger installation base.

The development and use of ransomware from Iran is likely to continue. The increased repurposing of popular malware by Iranian actors could lead to the use of ransomware for destructive purposes by state-sponsored organizations.

EXTENDED SUPPLY CHAIN THREATS
ARE CHALLENGING THE ECOSYSTEM

Organizations should think beyond the enterprise to the full ecosystem. Future enterprises might conduct business electronically with hundreds or even thousands of suppliers and partners around the world, each of which can expose such companies to cyberattacks. Organizations should work with their ecosystem partners to jointly protect themselves. Today, however, only 39 percent of companies say that the data exchanged with strategic partners or third parties is adequately protected by their cybersecurity strategy.

Cyber adversaries have slowly shifted their attack patterns to exploiting third- and fourth-party supply chain partner environments to gain entry to target systems, even in verticals with mature cybersecurity standards, frameworks, and regulations.

Organizations operate in a complex and challenging environment. During the past few months, we have collected intelligence on recent campaigns that highlight the challenges of combatting weaponized software updates, prepackaged devices, and supplier ecosystems as these all fall outside the control of victim organizations. iDefense threat intelligence analysts believe cyber criminal, espionage, and hacktivist groups will continue to target supply chains and the strategic business partners that contribute to them for monetary, strategic, and political gain.

CRITICAL INFRASTRUCTURE
IS A HIGH-VALUE TARGET FOR THREAT ACTORS

Nation-state-sponsored, hacktivist-driven, and other adversary-driven attacks on IIoT systems are increasing in the utilities, oil and natural gas (ONG), and manufacturing industries. iDefense threat intelligence profiled the ONG industry as an example. Adversaries are taking advantage of the fact that the ONG industry is slowly moving to digitize its IIoT systems. The current cybersecurity procedures do not seem to be fully prepared to meet the rapid convergence rates of IT and OT. In fact, 66 percent of surveyed ONG IT managers said digitization has made them more vulnerable to security compromises.[3]

The ONG industry will continue to be an attractive target for threat actors, given the high number of entry points along the value chain, rise of IIoT, and the potential damage or disruption that a cyber incident could inflict on the security and economy of a given oil producing country. Our analysis indicates that despite the potential increase in these security vulnerabilities to the OT environment, IT-OT convergence will continue to grow within the ONG sector.

Threats to the ONG industry will continue to broaden. Organizations need to adopt a corporate cybersecurity culture that consists of continuous security awareness and training for all employees, IT teams, and OT teams. The IT and OT teams need to build strong collaborative processes and procedures to reduce or prevent future cyber incidents.

ONG industry organizations need to hire new talent to manage and support emerging technologies, including artificial intelligence (AI)-based technologies at the upstream level, and should make sure the IT-OT convergence aligns with the priorities and concerns of both IT and OT departments.

ADVANCED PERSISTENT THREATS
ARE BECOMING MORE FINANCIALLY MOTIVATED

Financially motivated cyber criminals are stepping up their game. Much reporting on advanced persistent threat (APT) cyberattacks indicates financial attacks are motivated by espionage. Using TTPs akin to their espionage counterparts, groups such as Cobalt Group and FIN7 have allegedly been targeting large financial institutions and restaurant chains successfully.

FIN7 continues to innovate, with analysts having observed a new version of the Bateleur malware, version 1.1.0, in April 2018. iDefense threat intelligence finds that FIN7 has been less active in 2018 than in the previous year, but this decreased activity does not mean this threat is not present. The FIN7 malware did not include major upgrades from the previous version (1.0.8) but instead included only minor changes, such as the addition of a new network traffic encoding prototype function.

Other threat groups have been less active and even dormant. The leader of the Carbanak and the Cobalt Group was arrested by the Spanish National Police on March 26, 2018. The Cobalt Group became dormant in March and April 2018 but renewed attacks in May. This might indicate new threat group leadership. iDefense threat intelligence will continue to monitor these groups closely to see how their attacks might evolve. They might pivot their attention to other industries or other high ROI cyberattacks.

MINER MALWARE
IS CREATING A CRYPTOCURRENCY SURGE

Cyber criminals have grown their use of cryptocurrency miner malware. It has been one of the largest growth areas in malware in 2018, and its growth is likely to continue into 2019. Miner malware rewards its operators with the cryptocurrency mined on infected hosts, with those victim systems potentially benefiting from rapid fluctuations in price. Such fluctuations are caused by rampant speculation. Traditionally, miners have sought Bitcoins due to the currency's wide adoption among cyber criminals and legitimate businesses. iDefense threat intelligence has documented a radical shift toward mining alternative cryptocurrencies, most notably Monero. Monero can be more easily and efficiently mined. Tracking Monero transactions is more difficult than tracking Bitcoin transactions.

GDPR can unleash serious risks for businesses across the globe. GDPR has had significant effects on the risk calculations of organizations holding EU subjects' data. The risk of data theft and manipulation from external actors remains high, despite the increased regulatory burden. iDefense threat intelligence analysts assess it is likely that cyber criminals will try to leverage the threat of GDPR non-compliance in attempts to extort organizations, especially in the immediate aftermath of GDPR implementation in May 2018. iDefense threat intelligence analysts have already identified actors discussing how to leverage GDPR as a social engineering lure when communicating with target organizations.

Ransomware continues to be the most prevalent attack vector for extortion operations, with attacks against organizations doubling from 2016 to 2017, rising from 13 percent to 27 percent of all reported incidents targeting corporations.[4] Cyber criminals are innovating their attack methods and diversifying toward the use of multi-functional ransom malware—encompassing secondary functionality such as miner malware or data exfiltration—to ensure a second layer of possible profitability. iDefense threat intelligence analysts predict that targeted attack groups will continue to use ransomware, with threat actors repurposing malware advertised on the criminal underground to deflect attribution efforts away from APT groups' use of destructive malware.

Our threat intelligence experts and cyber defenders take great pride in uncovering cyber adversaries and their tactics, techniques and procedures (TTPs). We aim to build tactical and strategic threat intelligence for our clients to better defend their networks and make data-driven business decisions to stay ahead of relevant threats to their business.

The Cyber Threatscape Report 2018 relies on iDefense intelligence collection, research, and analysis including research using primary and secondary open-source materials. It covers the increased prevalence of destructive attacks; the aggressive use of information operations by nation-states; growth in the numbers and diversity of threat actors; as well as the greater availability of exploits, tools, encryption, and anonymous payment systems available to malicious actors.

WHAT'S HAPPENING?

IRANIAN THREAT IS A GROWING FORCE TO BE RECKONED WITH

Topline assessment:

- Post the Joint Comprehensive Plan of Action (JCPOA) annulment, the Iranian government's behavior has been defensive. Unless the country is placed under extreme economic pressure, it is unlikely to pose a disruptive or destructive threat against the United States or Europe. However, Saudi Arabia, the United Arab Emirates, Bahrain, and Israel are more likely to face cyberattacks emanating from Iran.
- The attack surface pertaining to Android devices, specifically in Iran and other countries where update adoption is low, will continue to expand. Unofficial and third-party Android application marketplaces continue to be used broadly and will increase in availability and utilization. This increased use will lead to more opportunity for malicious application delivery using obfuscation techniques through the official Google Play Store in an effort to appear legitimate and reach a larger installation base.
- iDefense threat intelligence analysts predict that actors in Iran will continue to develop and deploy ransomware that they have repurposed from popular malware. State-sponsored organizations such as the Islamic Revolutionary Guard Corps (IRGC) Cyber Command could use such ransomware.

Iran's geopolitical trends

iDefense threat intelligence has seen a high increase in the number of cyberattacks, types and uses of ransomware, and malware trade and usage by threat actors based in Iran; hence, iDefense threat intelligence is carefully tracking Iranian cyber threats to ensure clients are adequately protected from this growing and expanding cyber threat.

iDefense threat intelligence analysts predicted that based on the United States President Donald Trump's removal of Secretary of State Rex Tillerson from his position, the nomination of former US CIA Director Mike Pompeo as the secretary of state, and the appointment of former US Ambassador to the United Nations (UN) John Bolton as the National Security Advisor, the Obama-era Iran nuclear agreement better known as "JCPOA" would end.[5] Consequently, the annulment of the JCPOA by the current United States president has put Iran in a defensive position, which has led Iran's supreme leader Ayatollah Ali Khamenei (a hardline cleric) to use harsh rhetoric against the United States president and the United States as a whole and to threaten to resume Iran's nuclear activities, especially if talks with European counterparts fail.[6] Although based on current Iranian policy, the feud may not lead to any disruptive or destructive cyberattack against the United States or European counterparts in the near future. The Iranian government is likely to continue its cyber espionage activities and develop its cyber capabilities for political and strategic influence; however, it might also take a more aggressive posture against its neighboring rivals and regional enemies, such as Saudi Arabia, the United Arab Emirates, Bahrain, and Israel, for encouraging and supporting the United States decision on the annulment of the JCPOA agreement.

On September 14, 2017, the Director of National Intelligence, the Honorable Dan Coats, provided his remarks at the Billington Cybersecurity Summit, stating, "Iran and North Korea are improving their capabilities to launch disruptive or destructive cyberattacks to support their political objectives." Office of the Director of National Intelligence.

iDefense threat intelligence analysts believe that a result of political tensions stemming from the possible abolishment of the JCPOA agreement will be that the IRGC Cyber Command is highly likely to resurrect its cyber threat activity against organizations in multiple industry sectors such as the financial, critical infrastructure, healthcare, government, and military, and energy sectors; consequently, iDefense threat intelligence assesses operational and economic risks to these organizations are likely to increase.[7]

Iran's cyber espionage

Growing POWERSTATS malware family activity

iDefense observed that the POWERSTATS malware family activity is on the rise and continuing to evolve, as seen in targeted attacks that Palo Alto Networks has dubbed "Muddy Water."[8] POWERSTATS is a PowerShell-based first-stage backdoor that uses and drops scripts to contact a command-and-control (C2) server. The malware performs

reconnaissance on a victim system, lowers its Microsoft® Office security settings, and can execute any PowerShell command the threat actor using it sends. This threat activity was first observed and disclosed by iDefense threat intelligence in 2017; however, it has continued to blossom in 2018.

The first generation of POWERSTATS malware used basic PowerShell and VBScript and has grown in complexity and sophistication, mainly due to the public reporting of its activities. This evolution has included more sophisticated and more advanced infection and evasion techniques, such as AppLocker bypass methods, malware analysis tool detection, anti-sandbox checks, extended C2 proxy lists, base64 encoding, and PowerShell obfuscation that is more layered. In addition, new infection vectors have been observed; they include infection via a Java-based version coupled with a BurpSuite-KeyGen and a malicious Microsoft Help file.

In initial reporting from October 2017, iDefense threat intelligence attributed this activity with moderate confidence to Iran-based actors. Evidence of specific strings and metadata found within the malware has strengthened our assessment of the malware's Iranian origin; additionally, the malware's continued changes are consistent with the identified threat group behind this malware. Deep familiarity with this threat group has enabled iDefense threat intelligence to identify previously undetected and unreported samples that have assisted in tracking this group. Furthermore, a third party posed as a victim and participated in sessions with the hacker behind this malware, enabling the third party to discover a tradecraft error made by the operator: the exposure of an IP address in Iran believed to be a final endpoint. This exposed IP address contributed to our assessment.[9] In response to this Iran-based attribution by the security community, iDefense threat intelligence has observed the threat actor embedding Chinese false-flag strings, as reported in the Security Ownage blog by Mo Bustami, that were added in early 2018 to cause misattribution and confusion.[10]

iDefense threat intelligence has observed this threat group continuing to focus its targeting on West and Southwest Asia, North Africa, and the Middle East, most prominently Saudi Arabia. iDefense threat intelligence has noted that the attacks have been very timely and included the targeting of Jordan during a period of political turmoil in May 2018.[11] Accenture Security fully expects this activity to continue and to evolve, as public reporting of the group's TTPs continues to emerge, despite efforts by Microsoft to securely control PowerShell.[12]

More PIPEFISH cyber espionage efforts

iDefense threat intelligence has observed the PIPEFISH (aka OilRig) cyber espionage threat group continues to be active and is advancing its toolset.[13] iDefense threat intelligence assesses that this threat group has been primarily targeting Middle Eastern entities for surveillance and espionage objectives in the energy sector. iDefense threat intelligence has maintained an effective tracking collection of PIPEFISH despite this threat group's continuous changes and shifting of techniques. It has consistently shown a propensity to reuse metadata, IP infrastructure, components of lure documents, and domain registrants, which has enabled analysts to produce high-confidence intelligence against the group.

iDefense threat intelligence analysts identified new ISMDoor variants in early 2018; these variants included an information stealer and remote administration tool (RAT) that was consistent with previous samples created by this threat group.[14] However, in a radical change to earlier variants, this new ISMDoor implant does not visibly implement any persistence mechanisms. Accenture Security believes that the C2 human operator may manually download additional backdoor stages, establish implants, or create scheduled tasks in the compromised machine to achieve persistence in the absence of the persistence module in the ISMDoor. It remains unclear if the persistent component of the malware is

removed to avoid detection or is performed manually to create tailored persistent access based on an interactive operator's assessment of the targeted system. In addition, communication from the malware was performed via the Domain Name System (DNS), which is weak to atomic domain identification and may indicate the use of manual persistence as a method to preserve the longevity of malicious DNS infrastructure.

iDefense threat intelligence also observed activity from a new Trojan from the PIPEFISH Iranian threat group. Palo Alto Networks named this Trojan the "OopsIE trojan"; it is a .NET-based, packed and obfuscated malware.[15] This malware uses the Internet Explorer application object to disguise its communications to make them look like they are part of a legitimate browser session. This Trojan has the ability to execute remote commands and to upload and download files from the victim system.

In addition, iDefense threat intelligence analysts attributed a newly seen PowerShell backdoor to PIPEFISH: the PRB Backdoor, which was named after the function used in the final PowerShell script payload.[16] iDefense threat intelligence observed this malware targeting companies in Egypt, matching previous threat-actor interest in civil aviation organizations in the region. Third-party analysis has linked an IP address to the resolution of a C2 domain associated with the PIPEFISH infrastructure. It is noteworthy that this PowerShell backdoor shares some similarities (obfuscation and substitutions) with the POWERSTATS backdoor, which may indicate code reuse by the "Muddy Water" actors in Iran. While these backdoors are different, their similarities are significant enough to enable analysts to conduct additional monitoring and tracking of the backdoors' repurposed code and may indicate an interesting reorganization or strategies of Iranian cyber threat groups.

Iran-based ransomware

Global ransomware attacks have dramatically increased in number over previous years and have caused millions of dollars of data recovery costs, brand damage recovery costs, operational costs, insurance costs, and other expenses to organizations. Since October 2016, iDefense threat intelligence has identified a number of Iran-based ransomware, indicating that Iranian cybercrime actors are likely to be financially motivated to target global organizations by using ransomware and cryptocurrency miners for financial gain.[17] iDefense threat intelligence has also identified that Iran-based ransomware developed in Iran or used by actors located there is not only limited to the Windows operating system but also is being developed to compromise and encrypt Android mobile devices.[18] iDefense threat intelligence has analyzed and identified at least two ransomware samples (TYRANT and RASTAKHIZ), both of which were repurposed by a single actor.[19] The emergence of Iran-based threat actors and groups developing Iran-based ransomware, in addition to carrying out threat activities and sophisticated TTPs, opens a new cybersecurity challenge for global organizations. The rise of state-affiliated cybercrime, as seen with **Mabna Institute** and its for-profit massive data theft of intellectual property from various universities and private sector organizations, provides a different perspective on Iran-based cyber criminals, their TTPs, and how they shared data with the **Islamic Revolutionary Guard Corps** for future research and development (R&D).[20]

iDefense threat intelligence identified the following ransomware variants as having been developed or repurposed in Iran:

RASTAKHIZ

- Hidden Tear variant discovered in October 2016
- After activation, provides victims with an unlimited amount of time to gather the requested ransom money and pay it
- Related unlock keys and the response sent to and from a Gmail address

TYRANT

- DUMB variant discovered on November 16, 2017
- Disguised itself as a popular virtual private network (VPN) in Iran known as Psiphon and infected Iranian users
- Included Farsi-language ransom note, decryptable in the same way as previous DUMB-based variants
- Message requested only US$15 for unlock key
- Advertised two local and Iran-based payment processors: exchange[.]ir and webmoney[.]ir
- Shared unique and specialized indicators with RASTAKHIZ; iDefense threat intelligence analysts believe this similarity confirms that the same actor was behind the repurposing of both types of ransomware.

WannaSmile

- zCrypt variant discovered on November 17, 2017, one day after the discovery of TYRANT
- Used Farsi-language ransom note asking for a staggering 20 Bitcoin ransom payment
- Also advertised local Iran-based payment processors and exchanges—www.exchangeing[.]ir, www.payment24[.]ir, www.farhadexchange[.]net, and www.digiarz[.]com)—through which Bitcoins could be acquired

Black Ruby

- Discovered on February 6, 2018
- May have been distributed through unknown vectors
- Will not encrypt a machine if its IP address is identified as coming from Iran; this feature enables actors to avoid a particular Iranian cybercrime law that prohibits Iran-based actors from attacking Iranian victims
- Encrypts files on the infected machine, scrambles files, and appends the .BlackRuby extension to them
- Installs a Monero miner on the infected computer that utilizes the machine's maximum CPU power
- Delivers a ransom note in English asking for US$650 in Bitcoins
- Might be installed via Remote Desktop Services

Android ransomware

- Uses APK Editor Pro
- Picks and activates DEX>Smali from APK Editor
- Utilizes LockService application and edits the "const-string v4, value" to a desired unlock key
- Changes contact information within the ransom note
- Once the victim has downloaded the malicious app, the only way to recover its content is to pay the ransom and receive the unlock key.

Iranian android malware

Analysis of multiple malware families in 2018 has shown continued use of the "Application Update" lure for regionally specific applications. Attacks using update lures have been primarily targeting users of messaging and social media platforms (such as, Telegram, Facebook). More-targeted espionage campaigns have gone so far as to create new platforms to act as a new form of watering hole whereby the platform operates as expected, but is designed to compromise the device through which a user is accessing the platform. As most Android malware families originating from and targeting users within Iran are not available in the official Google Play store, probably due to its strict code policies, these malware families are likely disseminated via social media and unofficial Android marketplaces such as **Myket**. While there have been examples of threat actors successfully propagating and distributing malware via Google Play, their success is limited in number probably due to the safeguards and security controls that Google Inc. has implemented.

An overall increase in the number of malware families using multi-stage mechanisms in a manner similar to PE32/PE64 infection chains, whereby

different payload stages are selected based on reconnaissance and an assessment of the victim host, increasingly, has been seen in the wild and within targeted campaigns. The following describes how a targeted malware family attack chain may unfold:

1. The victim opens a benign Microsoft® Office document that has an inline link within the document's body.
2. The victim clicks the link, which leads to the downloading of a malicious Android application package (APK) from a compromised or owned threat actor infrastructure.
3. The Android app continues with the theme and deception of the original document, prompting the victim to either enable Device Administrator access or install a downloader and staging component on the Android device.
   - Users are often additionally prompted to enable a developer or "non-trusted" application installation.
4. If Device Administrator is enabled, a full-featured RAT is installed or an additional payload is retrieved and installed after the malware has completed an assessment of the device.

Due to the nature of bring your own device (BYOD) policies and the inclusion of Android devices on corporate networks, analysis of select (generally more targeted) campaigns have shown Windows (PE32/PE64) executable files being embedded within Android applications. iDefense threat intelligence analysts presently believe this is being done in an effort to use Android devices as an additional entry point to Windows corporate networks. This enables malicious actors to bypass security boundaries and information flow controls by utilizing an Android's cellular data network to bridge a targeted corporate network when the mobile device is plugged into the corporate system for charging or data sharing.

The most prominent change observed within the context of Android malware analysis has been developers' increased focus on evading detection. The primary methods of evading detection seen within newer versions of Android malware are as follows:

- Java reflection and basic string obfuscation (to evade static detection of malware behavior as well as C2 definitions within the application).
- Rotation of C2 servers that provide final-stage domain and IP address destinations within the body of response content from the Web server (to evade static and dynamic detection).
- Embedded resource files called by the application instead of being defined within standard code body and functionality.
- Code packing and class obfuscation.
- Definition of C2 domains and IP addresses within XML fields rather than standard function calls.

Iranian threat trends and predictions

Iranian ransomware development will continue to improve in the future to evade detection. Iranian cybercrime actors may have been using the aforementioned ransomware as test beds for their future attacks against foreign targeted entities or organizations, as targeting Iranian victims is against Iran's cybercrime laws. Cybercrime actors in Iran are now more capable of using, mining, or exchanging cryptocurrencies, as Iranian nationals are becoming more and more familiar with blockchain technology and are better at understanding the concept of cryptocurrencies. The development and repurposing of ransomware on both desktop and mobile platforms may also be used for blackmail or extortion.

Exploitation of the Android platform will continue to expand, especially in regions where adoption of current operating system versions is significantly lower. The availability and delivery of updates from telecommunication providers via over-the-air (OTA) mechanisms will continue to be insufficient for users to apply regularly, further exposing end users to threats, such as by enabling them to inadvertently install spyware, keyloggers, or RATs by a malicious third party. Unofficial Android marketplaces will also continue to increase in number, enabling threat actors to infect more devices at an increasing rate. Threat actors will continue to attempt to utilize legitimate mechanisms (such as, Google Play) to facilitate malware distribution. Due to the level of persistence and complexity that malware can have when it is present in Google Store, iDefense threat intelligence analysts believe this avenue will continue to be used primarily in highly focused cybercrime or espionage campaigns.

EXTENDED SUPPLY CHAIN THREATS ARE CHALLENGING THE ECOSYSTEM

Topline assessment:

- Third- and fourth-party environments provide adversaries with an entry point, even in verticals with mature cybersecurity standards, frameworks, and regulations.
- Recent campaigns highlight the challenges of combatting weaponized software updates, prepackaged devices, and supplier ecosystems as they fall outside the control of victim organizations.
- Cyber criminals, espionage, and hacktivist groups will continue to target supply chains for monetary, strategic and political gain.

Supply chains are an integral component for enterprises as they work to bring their products and services to market. Consisting of N^{th} parties, supply chains are a robust web of large, medium, and small firms that underpin the operations of nearly every organization globally. With such an important role to play, these networks are attractive targets for nefarious cyber activity perpetrated by cyber criminals, hacktivists, and nation-states. Threat actors have identified supply chains as being effective means of infiltrating or affecting victim organizations. Even verticals in which companies have bought into the maintenance of mature security hygiene or in which the regulatory landscape has forced such adoption, supply chains still present openings. Firms that are cornerstones of the supply chains of other institutions bear the burden of evaluating threats as both suppliers and consumers.

Supply chains are not homologous across every organization; however, there are higher-level groupings to which threats can be aligned. Successful attacks involving the supply chain of affected organizations have included software and hardware weaponization, data theft (IP data, personally identifiable information, insider information, etc.), logistics disruption, and intrusions (watering holes, e-mail compromise, etc.).

Overview

Attacks against supply chains have been both opportunistic and targeted. Vulnerabilities with global impact, like Meltdown and Spectre, have exposed a vast pool of potential organizations that could be affected via commodity campaigns. False patches laced with Smokeloader quickly appeared following the end of the embargo placed on the disclosure of the Meltdown and Spectre vulnerabilities.[21] Periods of widespread vulnerability disclosure provide opportune times for actors to distribute malicious communications to users anticipating updates. Targeted attacks against technology supply chains can be especially damaging. The devastating Petya pseudo-ransomware outbreak on June 27, 2017, showed security practitioners worldwide, throughout all verticals and in both public and private sectors, that even attacks intended for limited targets can inflict massive collateral damage on companies with operations in targeted countries or sectors. The attacks, which leveraged widely used applications for financial document-delivery, showed the risks of third-party software and services in the supply chain.[22] While there are tried-and-tested methods of attack, preemptively identifying unique software and technologies within a potential target organization is crucial when forecasting where attackers may look to direct their future activity.

Cyber espionage and the supply chain

Nation-state threat groups have evidenced interest and aptitude in executing supply chain attacks. Suspected Chinese and Russian threat groups have targeted infrastructure with supply chain implications. Compromise of the CCleaner software that Avast developed was used by PIGFISH to perform targeted attacks against specific victim organizations.[23] PIGFISH is a likely Chinese cyber espionage group that Accenture Security believes has dual goals of fulfilling information collection requirements and simultaneously gaining access to additional supply chain attack capabilities and resources.[24] BLACK GHOST KNIFEFISH, a Russian group, has heavily targeted oil, natural gas, energy production, manufacturing, pharmaceutical, education, and IT firms.[25] In 2014, the group successfully compromised software produced by three industrial control systems (ICS) equipment providers in Germany, Switzerland, and Belgium. The infected software was installed by countless victims and led to hundreds of successful compromises throughout Europe. Software supply chain tampering by resourced nation-state or criminal groups will continue to be used as a delivery method for increasingly sophisticated malware families like the SHADOWPAD backdoor Trojan that PIGFISH used.[26]

Third-party concerns

Across multiple ecosystems, third-party providers are often leveraged for business tasks such as conducting transaction settlements and customer assistance. The compromises of processors and even chatbot services expose a vast external attack surface to which businesses in the digital age are connected. The late March and early April 2018 breach of Latitude Technologies' third-party software for an electronic data interchange (EDI) system led to the disruption of scheduling and other EDI-mediated services for at least four pipeline companies.[27]

This incident came at a time of heightened international tension and highlighted the kinship verticals share through mechanisms like data interchanges, which are employed independently in both the oil and gas, and financial services industries. Additionally, actors such as Joker's Stash have advertised large credit card dumps in recent months, with the common points of exposure for their victims being spread across retailers around the world. The entry point for attackers during these compromises has often been through third-party environments. In more severe instances, delayed remediation of such breaches in retail environments has led to the repeated closing and reissuance of cards.

Implications for national security

An ongoing subject of debate is the risk associated with deploying technologies manufactured in or associated with adversarial nations. Government mandates addressing this issue demonstrate the supreme concern Nations have regarding the use of software, firmware, and hardware that is potentially weaponized or weakened prior to delivery. Nations including the United States, China, North Korea and Russia have been accused of leveraging or compromising domestic technology suppliers to support espionage efforts abroad.

iDefense threat intelligence has identified an additional, pertinent example: a Russian information security services company with a presence in numerous countries.[28] Companies like this one, which operate in the shadows, are a considerable threat to the environments of unassuming organizations and their suppliers. Stringent third-party risk assessments, supported by threat intelligence, can aid in steering technology strategy discussions.

Evolving legislative environment

In response to heightened attention focused on third-party threats, the legislative and regulatory landscape addressing supply chain risks from a cyber threat perspective is undergoing a period of resurgence. In the United States, bills have been proposed that highlight cybersecurity risks in federal supply chains and small- and medium-sized enterprises (SMEs). The Federal Acquisition Supply Chain Security Act (FASCSA)[29] and the Small Business Advanced Cybersecurity Enhancements Act ,[30, 31] are not being created in a vacuum, as other nations are also taking considerable steps to evaluate supply chains.

The threat of cybercrime and espionage focused on supply chains is multidirectional, and mitigation methods for supply chain weaknesses are being addressed as part of larger strategic goals.

iDefense threat intelligence anticipates that cyber threat actors motivated by financial, political, or ideological gain will increasingly focus attacks on supplier networks with weaker cybersecurity programs. As adversaries continue to use trusted third parties as vectors of intrusion, attribution and thus intent will become more challenging. This is especially the case for multifunction activities, like state-sponsored hacktivism, where target organizations may have a difficult time discerning commodity from targeted activity. An increasingly complex attack and intrusion vector, supply chains should be considered an inherent component of IT and OT threat models. Third-party assessments, audits, and enhanced monitoring should be considered essential pieces of supply chain defenses.

CRITICAL INFRASTRUCTURE IS A HIGH-VALUE TARGET FOR THREAT ACTORS

Topline assessment:

- Current cybersecurity practices in the oil and gas industry do not seem to be fully prepared to meet the rapid rates of convergence of IT and OT. One survey of OT cyber risk managers found that 66 percent of respondents believed digitization has made their organizations more vulnerable to security compromises.[32]
- The oil and gas industry will continue to be an attractive target for cyber threat actors, given the number of points of entry along the value chain, the rise of the IIoT, and the potential damage or disruption that a cyber incident could inflict on the security and economy of a given oil-producing country.
- Despite the potential increase in security vulnerabilities to the OT environment, IT-OT convergence will continue to grow within the oil and gas sector.
- Oil and gas organizations need to adopt a cybersecurity culture that includes security awareness and training for both IT and OT teams and that fosters collaboration between teams to reduce and prevent future incidents. The industry needs to hire talent to manage and support emerging technologies, including AI-based technologies at the upstream level, and ensure that IT-OT convergence aligns with the priorities and concerns of both IT and OT departments.

Overview

Digitization in industrial and manufacturing industries, including the oil and gas industry used here as a case study, is providing companies with the opportunity to improve their bottom lines, but has created changes in the cyber threat landscape that could erase those profits if digitization is not properly managed. In fact, recent technological progress in big data and analytics, machine learning, artificial intelligence, sensors, and control systems has enabled industrial, manufacturing, and of course ONG companies to significantly reduce operations and business costs by automating high-cost, dangerous, or error-prone tasks.[33]

Industrial Internet of Things (IIoT) is a network of sensors and devices connected to machinery in industries such as oil and gas, energy, and transportation.

This progress was made possible by digitization and the rapid growth of the IIoT, which enabled the convergence of IT and OT—that is, the equipment and processes that control industrial production. These two systems have traditionally operated as independent networks with different objectives, functions, and requirements within the oil and gas industry but, increasingly, are integrated, exposing potentially dangerous physical processes to malicious activity conducted over the Internet.

State of cybersecurity in oil and gas

The increasing convergence of IT and OT service providers, which Gartner predicts will reach 50 percent by 2020,[34] has exposed the OT environment to greater security threats that current cybersecurity practices in the oil and gas industry do not seem fully prepared to meet. Some of the vulnerabilities of ICS or OT are inherent to such systems and include the use of legacy software, default configurations, lack of encryption, and lack of network segmentation. Others are due to increasing network connectivity using IIoT with no embedded security.

- In a 2017 survey of United States oil and gas cybersecurity risk managers conducted by the Ponemon Institute, 66 percent of respondents said that digitization has made their organizations more vulnerable to security compromises, and about 68 percent had lost confidential information or experienced disruption of their operations over the year prior to taking the survey. Only about one-third of respondents viewed their organization's OT cyber readiness as high while the majority considered their current cybersecurity measures as inadequate at keeping pace with the increasing rates of digitization in the industry.[35]
- Another survey of IT, and ICS, and supervisory control and data acquisition (SCADA) security practitioners that the SANS Institute conducted in 2017 showed that about 69 percent of respondents considered threats to ICS systems to be high or severe, and 44 percent considered unsecured IIoT devices added to the network to be the top threat vector to their ICS. This data compares to the only 35 percent of respondents who viewed extortion, including ransomware, to be a top threat vector.[36]

Increased targeting: Threat actors

The oil and gas industry tends to be an attractive target for threat actors, including state-sponsored actors, cyber criminals, hacktivists, and insider threats, given the large number of entry points along the industry's business cycle and the potential damage or disruption that an incident could inflict on the security and economy of a given oil producing country. Several cyber threat types target the oil and gas industry, and some may have a significant impact. Examples include both destructive threats and disruptive threats such as resource theft.

Destructive incidents

Triton, a recently emerged destructive malware threat, alters and disrupts the operations of safety instrumented systems (SIS). These process control systems are commonly used in industrial units across multiple verticals, including oil and gas, utilities, and other energy-related industries, to enable the controlled shutdown of an industrial process when it has encountered unsafe operating conditions.[37] Unknown threat actors have deployed this malware, which is specially designed to exploit weaknesses in ICS and SCADA systems, in at least one critical infrastructure facility, apparently with the intent of developing the ability to cause physical damage.

Upon discovering third-party reports of Triton infections, iDefense threat intelligence researchers captured the full scope of related malware modules and thoroughly analyzed their sub-components. Based on our internal hunting systems and telemetry data, iDefense threat intelligence assesses with high confidence that entities in the Kingdom of Saudi Arabia (KSA) were among the targets of the initial campaign deploying this malware.

Disruptive incidents

Third-party service provider

In late March 2018, third-party software for an EDI system widely used by pipeline companies was compromised, resulting in the shutdown of the EDI service.[38] Although the breach was not the first cyber threat attempt on United States gas pipelines, which did not seem to affect the flow of natural gas, and affected only a few companies, the incident highlighted concerns within the energy industry of possible disruption to business transactions via the theft of intellectual property, the risk of interruption to operations, and increasing vulnerabilities introduced to operational systems by third-party service providers along the industry's supply chain.

Crypto-jacking on ICS and SCADA systems

In early February 2018, Radiflow reported the first incident of Monero cryptocurrency mining malware on a SCADA system in a water utility environment. The analysis showed that the malicious mining activity sapped computing power and network bandwidth. Activity like this could negatively affect the response times of devices used to monitor physical changes in an OT network. A large amount of the Monero malware has been known to damage security devices to allow the malware to remain undetected.[39]

The following developments are likely to increase incentives for state actors to sponsor cyber threat activities:

- The United States is projected to be a net oil and gas exporter by 2022.[40] If this projection comes to fruition, the United States will directly compete with Russia in the European market. Russian state actors could sponsor disruptive or espionage-related cyber operations or support hacktivists in the name of protecting the environment to contain new competition to its largest energy market.

- Newly imposed sanctions on Iran are likely to push that country to intensify state-sponsored cyber threat activities in pursuit of its geopolitical and strategic objectives at the regional level, particularly if Iran fails to keep its European counterparts committed to the Joint Comprehensive Plan of Action (JCPOA) agreement.
- Rising oil prices could create incentives for North Korea to launch ransomware attacks and other financially motivated cyber threat activity such as cryptojacking, which the country has done before to raise money for fuel purchases.

Mitigation methods and recommendations

Given the potential gains in reducing operations and business costs through automation, particularly at the upstream level, IT and OT convergence will continue to grow within the oil and gas sector despite the potential increase in security vulnerabilities to the OT environment. The following recommendations are likely to assist in mitigating cyber risks:

- Promote a cybersecurity culture that consists of providing security awareness and training for both IT and OT teams, and foster collaboration between these teams to reduce or prevent future intrusions.
- Invest in cybersecurity and operational team training to make sure that system processes are considered with cybersecurity in mind.
- Hire talent to manage and support AI-based technologies at the upstream level.
- Ensure that IT-OT convergence aligns with the priorities and concerns of both IT and OT departments.
- Evaluate all third-party service providers along the entire value chain of the business.

ADVANCED PERSISTENT THREATS ARE BECOMING MORE FINANCIALLY MOTIVATED

Topline assessment:

- iDefense threat intelligence observes that FIN7 has been quieter in 2018 than in the previous year.
- FIN7 continues to innovate with the new Bateleur version (1.1.0), observed in April 2018; however, this was not a major upgrade from the previous version (1.0.8), as it included only minor changes, such as the addition of a new network-traffic-encoding prototype function.
- The Spanish National Police arrested the leader of the Carbanak and Cobalt Groups on March 26, 2018.
- The Cobalt Group became dormant in March and April 2018 but renewed attacks in May.

Overview

While much reporting indicates that APT cyberattacks are espionage motivated, financially motivated cyber criminals have also been stepping up their game since as early as 2013. Using TTPs akin to their espionage counterparts, groups such as Cobalt Group and FIN7 have been targeting large financial institutions and restaurant chains with much success. The Cobalt Group alone is said to be responsible for causing 1 billion euros worth (US$1.17 billion) of damage to the financial sector.[41] The distinction between espionage and financial APTs is further blurred by state-sponsored threat groups like NEEDLEFISH (aka Lazarus) that carry out both types of attacks using very similar TTPs, further highlighting the changing threat landscape for organizations that would otherwise not be considered legitimate targets for espionage attacks.

iDefense threat intelligence has been actively tracking financially motivated threat groups over the past 24 months, with FIN7 and Cobalt Group being the two most active and capable groups on the iDefense threat intelligence radar.

Background

FIN7

Often associated with the original Carbanak gang, FIN7 is a financially motivated syndicate that uses the Carbanak malware as part of its TTPs but has a distinctive preference for using script-based backdoors as first-stage backdoors to establish persistent access to a compromised system and plant additional payloads. This group commonly spear-phishes with malicious RTF documents (see Figure 2) to deliver a first-stage backdoor to its intended targets.

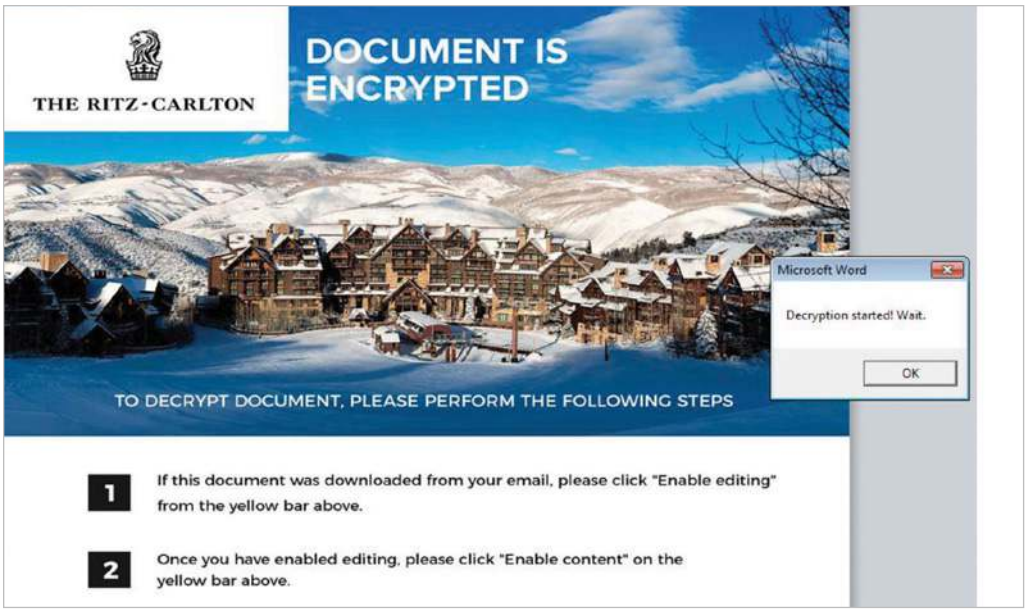

FIGURE 2
Content of malicious RTF document used by FIN7

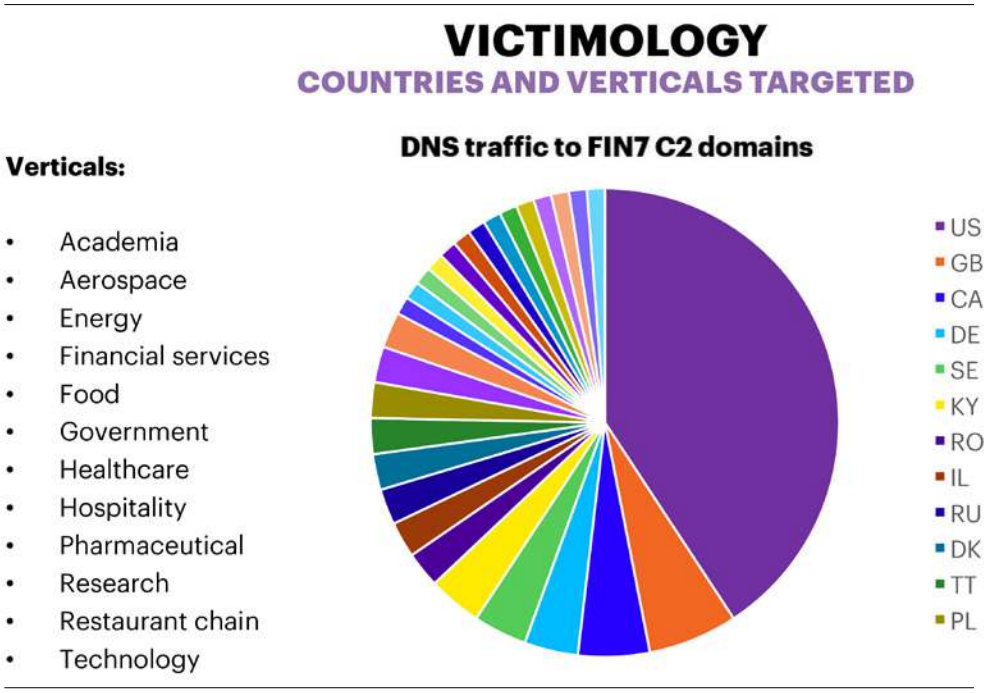

FIGURE 3

Victimology of FIN7 by vertical and country

Based on our observation of FIN7's activities, including the group's frequency of attacks and tool innovation, analysts assess with high confidence that the group is highly skilled and well resourced.

Malware families that FIN7 uses include the following:

- A script-based first-stage malware known as HALFBAKED
- A script-based first-stage malware known as BELLHOP
- A script-based first-stage malware known as Bateleur
- Meterpreter
- Cobalt Strike BEACON

According to iDefense threat intelligence's telemetry, FIN7 targets the verticals and countries in Figure 3.

BATELEUR

	v1.03JS	V1.04	V1.06	V1.08	V1.1.0	Notes
get_information	X	X	X	X	X	Collect system information from the host.
get_process_list	X	X	X	X	X	Otbtain list of running processes.
kill_process	X	X	X	X	X	Kill the process with the given PID.
uninstall	X	X	X	X	X	Remove Bateleur from disk.
update	X	X	X	X	X	Update code.
tinymet			X	X	X	Download TinyMet.
exe	X	X	X	X	X	Download and execute an executable.
wexe		X	X	X	X	Download and execute an executable.
dll	X	X	X	X	X	Download and execute a DLL.
cmd	X	X	X	X	X	Execute a given command.
powershell	X	X	X	X	X	Execute a given PowerShell script.
apowershell		X	X	X	X	Execute a given PowerShell script.
wpowershell		X	X	X	X	Execute a given PowerShell script.
get_screen	X	X	X	X	X	Take a screenshot of the current system.
get_apps				X	X	Download and excecute additional modules.
get_passwords	X	X	X	X	X	Dump credentials including form grabbing.
timeout	X	X	X	X	X	No actions.

FIGURE 4
Evolution of Bateleur functionalities

Evidently, Bateleur is a highly versatile and lightweight first-stage backdoor, and the continued development of the malware suggests that the group has been having success using this tool.
Bateleur version 1.1.0 uses the Schedule tasks named "Adobe Acrobat Updater" and "Adobe Acrobat Player Update" to ensure the Bateleur script is executed every time a Windows session starts.

Cobalt Group

Cobalt Group was first publicly named and reported in October 2016. The group has continued to be actively targeting financial services organizations predominantly in Russian-speaking countries, but also in the United States, Europe, and Southeast Asia. Figure 5 shows the verticals and countries that the Cobalt Group targets.

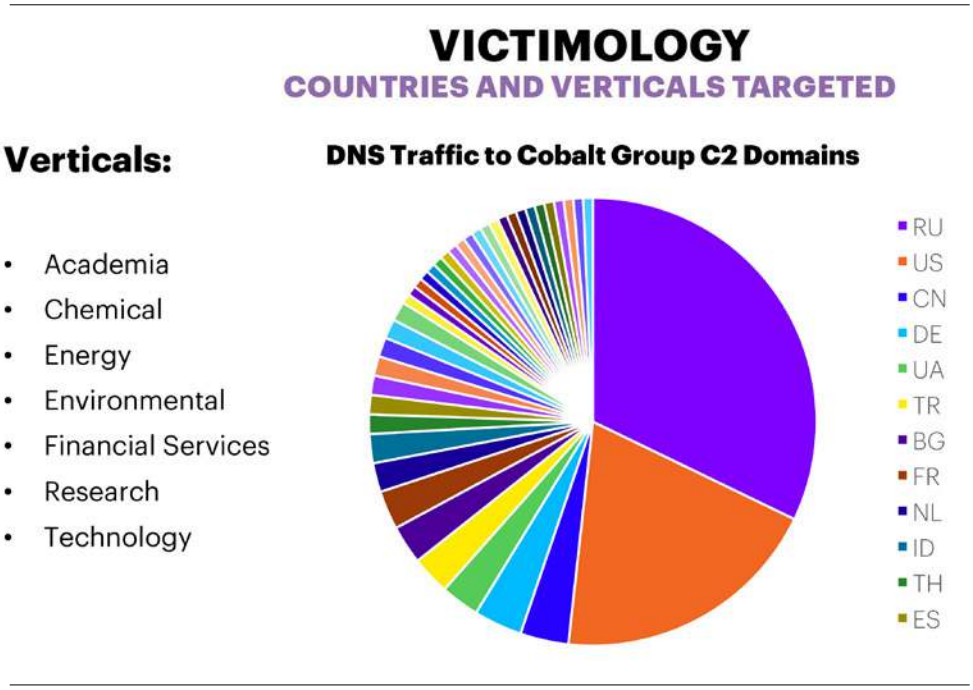

FIGURE 5
Cobalt Group victimology by vertical and country

Like FIN7, Cobalt Group is highly innovative and has been using many different custom malware samples over the past 18 months. The most recent waves of attacks came in mid-May, with three of the four observed waves of attacks involving the use of the Squiblydoo post-exploitation mechanism to plant the main backdoor. The information below illustrates the infection chain of the attack observed on May 21, 2018.

The spear phishing e-mail used in this attack wave was sent from the e-mail address info@apple-istores[.]com. Figure 6 shows the spear phishing e-mail involved in this campaign.

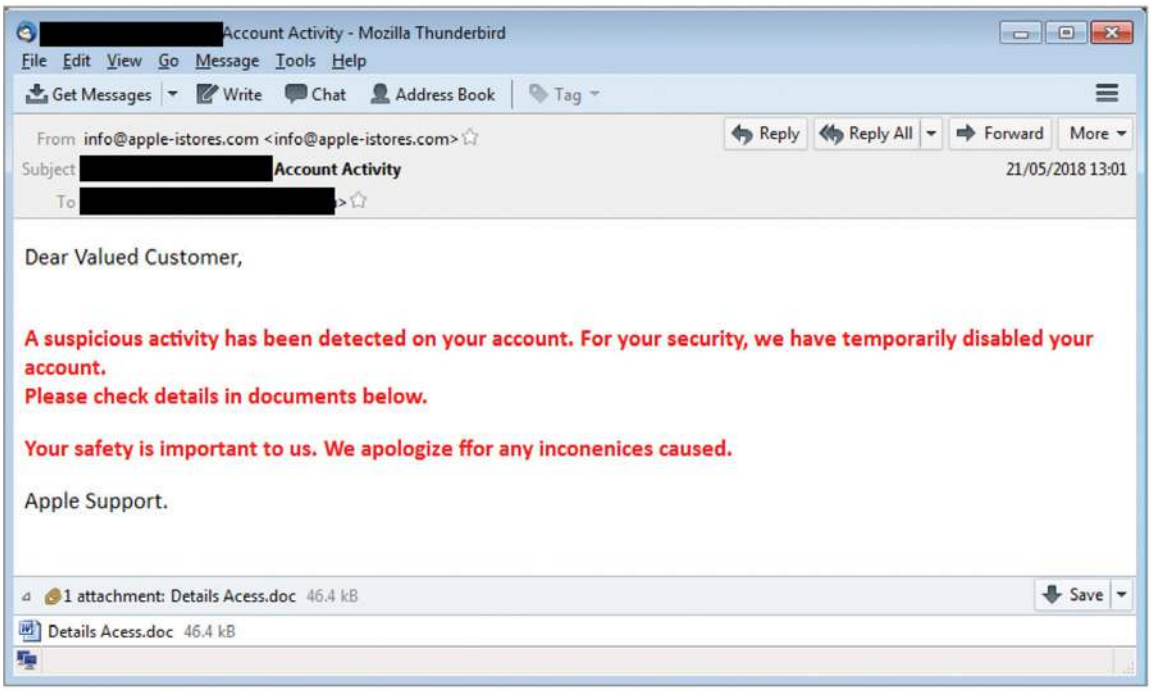

FIGURE 6

Spear-phishing e-mail sent by Cobalt Group on May 18, 2018

The link embedded in the e-mail, hxxps://swift-fraud[.]com/documents/53763987.doc, leads to a Microsoft Word document with the following properties:

- **Filename:** Details Acess.doc
- **MD5:** 298774c49ee2a1e823f8049a34c09609
- **File Size:** 46.4 KB (47,560 bytes)
- **Author:** Admin
- **Creation Time Stamp:** 2017-11-23 01:05:00 (Nov. 23, 2017, 1:05 a.m.)
- **Modified Time Stamp:** 2017:11:23 01:06:00 (Nov. 23, 2017, 1:06 a.m.)

The content of the document is as seen in Figure 7.

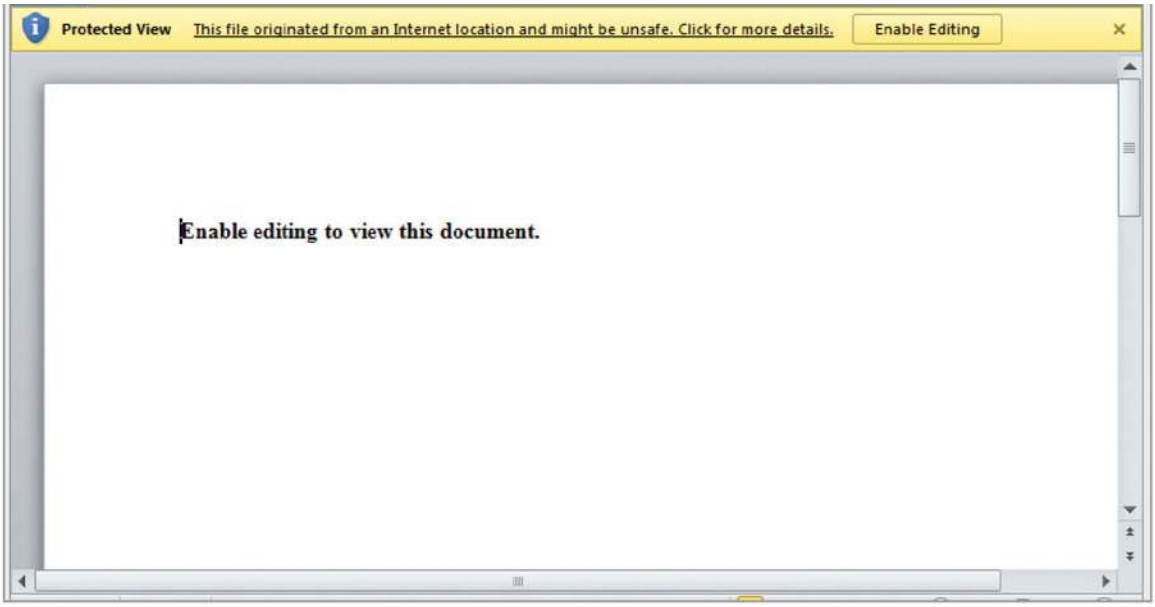

FIGURE 7
Content of malicious Microsoft Word document

Once executed, the infection chain follows that of a post-exploitation infection chain known as Squiblydoo with the use of Windows Script Component (SCT) files to download additional components for subsequent stages.

The malware drops the following files in the victim %temp% directory after infection:

Filename: icWwJarxcTwcABh.sct

- **MD5:** 05aa48a9c536ad644a2e91eddf2c0511
- **Description:** Scriptlet that contains JavaScript to execute MGsCOxPSNK.txt

Filename: RaRaoVewkM.txt

- **MD5:** 9c289f5db447ac00069b76ff5f8009d1

- **Description:** Bash script to delete Registry keys related to Microsoft's Word Resilience, set Zones to null, and execute the script named tCrrDqBQoCcEkbnK.txt using the Microsoft Connection Manager Profile Installer (cmstp.exe); the bash script also deletes KbhpQIcahFCuZwq.sct and wipes content from MGsCOxPSNK.txt

Filename: MyFHPeibBN.doc

- **MD5:** aab98b81b9f899183fd090c5f0fe402b)
- **Description:** Clean decoy file shown to the victim user

Filename: daQMTVvsBig.txt

- **MD5:** e5614d2eec5d2b75c5eb26e059932f25)
- **Description:** Configuration file executed by Microsoft's Connection Manager Profile Installer (cmstp.exe) that will contact the given remote location, safe.my-documents[.]biz, to download an additional file named robot.txt, which is a dropper script that would then drop a malicious DLL onto the victim system.

The dropped malicious DLL has the following properties:

Filename: 10206.txt (the filename may change per infection)

- **Original filename:** tt.dll
- **MD5:** e7702f9585616283b6b412b06b274dbf
- **File Size:** 90.0 KB (92,160 bytes)
- **Compile Time Stamp:** 2018-05-20 20:12:57 (May 20, 2018, 8:12 p.m.)

Once executed, this DLL drops a scriptlet (MD5: 03c6601a7fef76fce7fb63c116ef5fb9) in %APPDATA% that contains obfuscated JavaScript code. The script is a More_Egg downloader configured to download the More_Egg backdoor from hxxps://api.toshiba[.]org.kz/robots.txt.

This script then downloads the full-feature More_Egg backdoor and creates a file on disk in %APPDATA% named in the same format as the More_Egg downloader; this created file has the MD5 signature b36782a9a2b34e8385702ec00cb85065.

Figure 8 shows the de-obfuscated version of the script (MD5: 1a2e7a9bc8b6e6f359b80173c1f3f42d), which is a full-feature More_Egg backdoor with the C2 server configured to be api.toshiba[.]org.kz.

```
var BV = '2.0';
var Gate = 'https://api.toshiba.org.kz/v1';
var js_gate = 'https://api.toshiba.org.kz/robots.txt';
var hit_each = 10;
var error_retry = 2;
var restart_h = 4;
var rcon_max = hit_each * (restart_h * 60) / (hit_each * hit_each);
var Rkey = 'TulME29AZsH47hID';
var rcon_now = 0;
var User = '';
var Build = '';
var gtfo = false;
function obj(xString) {
    return new ActiveXObject(xString);
}
function gObj() {
    var objMain;
    try {
        objMain = GetObject('winmgmts:{impersonationLevel=impersonate}');
        return objMain;
    } catch (wtf111) {
        return false;
    }
}
```

FIGURE 8
More_Egg backdoor configuration

Assessment and implications

The TTPs used by financially motivated attackers are often not too dissimilar from those typically observed in espionage attacks. Therefore, organizations such as financial institutions, not thought of as typical espionage targets, must be ready to detect, respond to, and contain espionage threat actors' TTPs. iDefense threat intelligence assesses with moderate confidence that the level of activities from financially motivated targeted attack threat groups will remain significant but lower in volume in 2018 than in 2017.

To detect and defend against Cobalt Group's TTPs specifically outlined in this section, iDefense threat intelligence recommends searching for the Registry key UserInitMprLogonScript configured with a path pointing to a .txt script in %APPDATA% or %USERPROFILE% and blocking access to the domains safe.my-documents[.]biz and api.toshiba[.]org.kz. In addition, iDefense threat intelligence recommends regular hunting for JavaScript, VBScript and PowerShell scripts stored in %APPDATA% and %USERPROFILE%.

MINER MALWARE IS CREATING A CRYPTOCURRENCY SURGE

Topline assessment:

- Cryptocurrency miner malware has been one of the largest growth areas in malware in 2018, and its growth is likely to continue into 2019. Miner malware rewards its operators with the cryptocurrency mined on the infected hosts of victims, who can potentially benefit from rapid fluctuations in the price of the currency caused by rampant speculation.
- While miner malware has traditionally mined Bitcoins—the first major and most globally popular cryptocurrency—2017 saw a radical shift toward and growth in malware mining alternative cryptocurrencies, or "altcoins."
- Monero has become by far the most popular currency used by miner malware in 2018; Monero miner programs, such as XMRig, are freely available on many open-code repositories and are easily incorporated into malware by even low-capability malware developers.

Overview

Cryptocurrency miner malware has emerged in 2018 as one of the most popular forms of malware due to its ease of use and the possibility for a "quick win"; the return on investment for using this type of malware is simply too high to not use it in a threat campaign. iDefense threat intelligence analysts have observed the use of cryptocurrency miners by both cybercrime and cyber espionage threat groups; an example of such miners is BlackRuby, a ransomware variant that appeared in

February 2018 that would not only encrypt files like typical ransomware, but also included a cryptominer for Monero. On the other hand, a cyber espionage actor known as ARCHERFIST, also known in the public domain as Iron Tiger, was observed using a Monero miner in combination with a modified Gh0st RAT (see Figure 9).

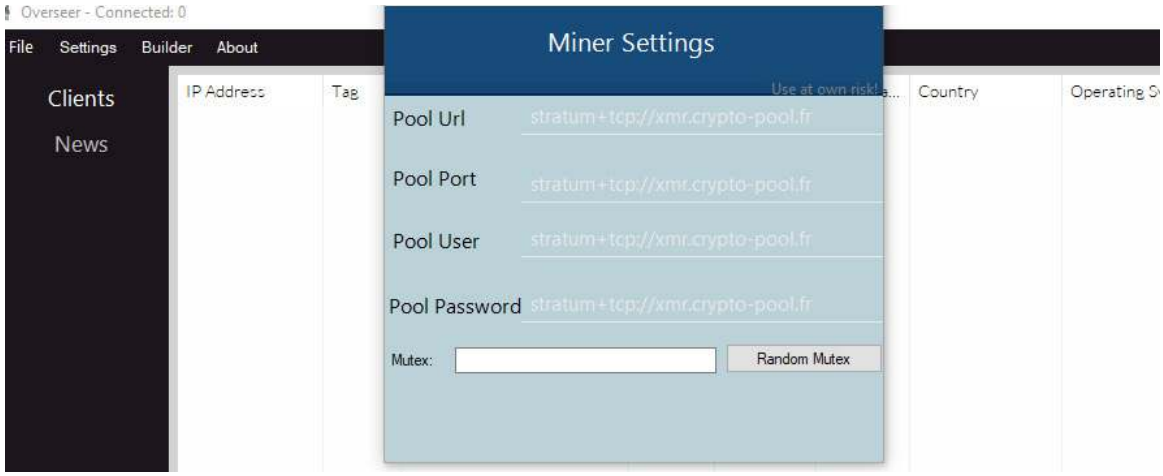

FIGURE 9
Screenshot of Overseer RAT's advertised Monero miner function

Typically, cryptocurrency miner malware and its network traffic are not obfuscated and are therefore easy to detect, depending on the specific type of miner malware creating that traffic. Both CPU and GPU miners exist, and both increase the use of a victim system's CPU or the GPU, respectively. Additionally, network administrators can monitor for network traffic on unusual ports as well as traffic to miner pools.

A significant reason for the growth in miner malware in 2017 and into 2018 is the profitability of mining alternative cryptocurrencies. Monero has a far lower "difficulty rate" for mining than Bitcoins, mining for which is unprofitable without the use of application-specific integrated circuit

chips (ASICs), which is dedicated Bitcoin mining hardware frequently used on an industrial scale by Bitcoin miners. Monero has since risen to become one of the most popular cryptocurrencies used by miner malware. iDefense threat intelligence analysis of cyber criminal underground activity has indicated a plethora of advertisements by malware authors and resellers for Monero miner malware during 2017 and going into 2018. The variety of malware available ranges from generic and cheap entry-level malware to vast botnets of compromised devices infected with custom malware.

Monero has also been linked to threat activities associated with the NEEDLEFISH group, also known as the Lazarus group, a cluster of advanced espionage and financially motivated threat actors likely affiliated with the North Korean state. Operators of Bitcoin wallets previously collected ransom payments for the ransomware WannaCry, which multiple security vendors have publicly attributed to NEEDLEFISH, which the United States government has attributed to the North Korean state, and which may have used Monero to launder funds after emptying victims' wallets, according to cryptocurrency transaction analysis vendor Chainalysis.[42] On several occasions, campaigns associated with NEEDLEFISH have reportedly conducted Monero mining on infrastructure of targeted organizations as part of a wider campaign. It is likely that Monero offers strong benefits for states interested in circumventing economic sanctions, especially financial system sanctions, as well as for states subject to a high level of surveillance of their international trade practices.

GDPR: How GDPR could influence cyber criminal extortion and data-for-ransom attacks

Topline assessment:

- GDPR continues to have a potential impact on the risk calculations of organizations holding EU subjects' data. Several organizations have issued breach notifications following the introduction of GDPR legislation on May 25, 2018, indicating that the risk of data theft and manipulation from external actors still remains, despite the increased regulatory burden.
- iDefense threat intelligence analysts assess it is likely that cyber criminals will attempt to leverage the threat of GDPR non-compliance in attempts to extort organizations, especially in the immediate aftermath of GDPR coming into force. iDefense threat intelligence analysts have already identified actors discussing how to leverage GDPR as a social engineering lure when communicating with target organizations.
- Distorted incentives to disclose breaches may result in more-frequent abuse and misuse of "bug bounty" vulnerability disclosure platforms to keep breaches out of the view of the public and regulators.

Overview

GDPR came into force on May 25, 2018, and is considered to be one of the most important changes in data privacy regulation in the past 20 years. The regulation imposes fines of up to 20 million euros (approximately US$24 million), or 4 percent of global annual turnover, on companies who fail to comply with GDPR. GDPR is designed to protect the data of all EU subjects, regardless of the country in which they reside

or the platform on which their data resides. As a result, a company located and domiciled in the United States that handles the data of EU subjects could be the subject of fines levied by EU member states if that company's data is found to have been misused or mishandled. As a result of GDPR, users must also be notified within 72 hours if their data has been exposed in a breach or be subject to a fine of up to 10 million euros (approximately US$12 million), or 2 percent of global annual turnover.

In the past six months, in the lead up to the deadline for GDPR compliance, iDefense threat intelligence analysts identified an increase in criminal chatter regarding GDPR and news coverage of the issue. The high level of attention of those in the technology community and vertical surrounding the GDPR "cliff edge" of May 25 has also filtered through to the cyber criminal community. Cyber criminals tend to pay a great deal of attention to industry news, with actors frequently sharing news updates and media stories on underground criminal forums and marketplaces. Paying attention to developments in the markets heavily informs actors' TTPs and their targeting of specific verticals.

Cyber extortion using stolen or modified private data, also known as "data-for-ransom," is one of the most prevalent attack techniques that financially motivated cyber criminals use in targeted attacks. Threat actors, by gaining access to internal networks or vulnerable Web-facing infrastructure, siphon off data and threaten to release the data publicly or sell it on the criminal underground unless the victim organization pays a ransom fee to the criminals. Actors frequently spend time reconnoitering an organization to identify the data of most value or sensitivity to the organization, such as customer payment data, intellectual property, or private e-mail messages. Access to this data is then used to blackmail victims by threatening to publicly disclose it or modify it beyond recovery.

FIGURE 10
Cyber extortion Twitter discussion

Whether GDPR will be leveraged by data-for-ransom actors has been the subject of significant discussion within the information security industry. Given the potential threat of punitive financial sanctions, far more than those previously leveraged by a European data protection authority, as well as the EU claiming global jurisdiction of its subjects, threat actors could extract additional leverage against their victims by threatening to report GDPR non-compliance to national data protection authorities. While organizations are still required to issue notifications within 72 hours if they discover a breach, there is still a potential risk that companies will avoid issuing notifications to avoid reputational damage resulting from a breach. As a result, companies may prefer to risk making an extortion payment far smaller than the potential fine to a cyber criminal actor rather than provide a notification that would result in enforcement action.

iDefense threat intelligence analysts assess it highly likely that cyber criminal actors will leverage GDPR when attempting to employ social engineering attacks against an organization's employees. iDefense threat intelligence analysts have already identified actors on a criminal

Tor-based marketplace discussing using GDPR as a social engineering lure to cover up the theft of a publicly exposed customer database by reporting the vulnerability to the company's IT department:

"Your play would be that the company is not compliant with GDPR and that you just wanted to give the IT guy in charge a friendly heads up by pointing out that their database is accessible through a misconfiguration."

This tactic is also likely to also manifest itself in targeted spear-phishing e-mail lures and telephone social engineering attacks through which the mention of GDPR non-compliance could be used to trigger action by a targeted IT department that the attacker could exploit. The United Kingdom's National Cyber Security Centre (NCSC) reported that in May 2018 it identified actors utilizing GDPR notifications as e-mail phishing lures to target Apple Inc. customers with credential theft.[43] iDefense threat intelligence analysts will continue to monitor for malicious e-mail traffic utilizing GDPR as a lure in 2018 and beyond.

Low-skilled threat actors, who routinely target Web-facing infrastructure with automated mass Web application attacks, such as cross-site scripting (XSS) and SQL injection (SQLi) attacks, could also use GDPR as leverage to demand payments by describing them as legitimate vulnerability disclosures. For example, a threat actor could identify an externally accessible database containing sensitive customer information vulnerable to SQLi attacks. The actor could then demand a "bug bounty" payment for the disclosure and to keep the information private; without payment, the actor could threaten to refer the vulnerability and any exfiltrated data to the national regulator. iDefense threat intelligence analysts assess that the potential for the bug bounty process to be manipulated in a GPDR environment may be significant if organizations attempt to classify ransom payments as legitimate bounties to avoid dealing with disclosure and GDPR legislation.

Developments in the ransomware threat

Topline assessment:

- Ransomware continues to be the most prevalent attack vector for extortion operations, with attacks against organizations doubling from 2016 to 2017, rising from 13 percent to 27 percent of all reported incidents targeting corporations.[44]
- High-profile ransomware attacks, such as WannaCry and BadRabbit, have resulted in increased public awareness of the threat, with end users becoming more conscious of operating with improved security measures, including backing up data and not opening unknown attachments.
- Cyber criminals are innovating their attack methods and diversifying toward the use of multi-functional ransom malware that encompasses secondary functionality such as miner malware or data exfiltration to ensure a second layer of possible profitability.
- iDefense threat intelligence analysts predict that targeted attack groups will continue to use ransomware, with threat actors repurposing malware advertised on the criminal underground to deflect attribution efforts away from APT groups' use of the malware for destructive purposes.

Overview

Ransomware continues to target organizations as part of both opportunistic and targeted attacks, with threat actors taking advantage of anonymous cryptocurrencies, underground networks of skilled criminal labor, and

increased dependence on access to data and technology. Through ransomware, attackers can target data that is intrinsically valuable to victims, eradicating the need to seek out a buyer for data on the underground. Attackers are willing to exploit human and technical vulnerabilities and are not afraid to go after so-called softer targets, such as those in the healthcare vertical, in which data and service availability is paramount. iDefense threat intelligence analysts assess that ransom malware continues to be an affordable and lucrative option for threat actors, and its crypto-ransomware and locker-ransomware variants will likely remain popular attack types for financially motivated criminals during the remainder of 2018.

With public awareness of the ransomware threat being significantly heightened following the WanaCrypt0r and NotPetya campaigns of 2017, end users and organizations are likely to have become more knowledgeable and resilient to the ransomware threat. This resilience may result in a natural shift toward cyber criminals exploring alternative, novice attack techniques. Developers continue to work to maintain the effectiveness of their malware by generating new, undetectable strands of crypto-ransomware or blockers. There remains a strong financial incentive associated with extortion, and developers are likely to continue to seek out improved attack methods, looking to diversify away from the typical Windows-variant CryptoLocker malware that has been highly prolific and a consistent threat in recent years.

With end users and corporations moving toward practices including more regular backups of data, malware developers may seek to add additional functionality to that which was previously standard ransomware. With such malware, criminals may add in dual- or tri-functionality to ensure a profitable return on investment. iDefense

threat iIntelligence research indicates that attackers are already adding data exfiltration functionality to ransomware. During August 2017, a Cerber variant was identified with added infostealer features that target passwords stored in browsers and files related to Bitcoin wallet applications. While this example limits attackers' abilities to target data that could contain direct additional financial value, such as banking passwords and cryptocurrency wallets, attackers may target other applications or security systems to access databases, servers, or client applications from victim computers.[45]

Another functionality that criminals are exploring for ransom malware is the inclusion of cryptominer malware, as noted previously in this report with the mention of the BlackRuby ransomware variant.[46] The inclusion of coin miner malware, which has become increasingly prevalent in the wild and is being advertised widely on criminal underground forums, may act as an insurance policy for threat actors to ensure that their victim infections are not without profit should the target opt not to meet ransom demands. Separately, a tactic that emerged in 2017 was the use of ransomware by targeted attack and APT groups to camouflage destructive malicious attack activity. This appears to have been the case with the NotPetya attacks launched in June 2017, in which ransomware that initially appeared to be based on a financially motivated variant sold on the criminal underground, Petya, was reused to carry out destructive, politically motivated attacks. This use of ransomware as a smokescreen—whereby attackers deliver ransomware to distract investigators and deflect attention away from the primary purpose of the attack against the victim—has been seen in the past.

In addition to using ransomware as a smokescreen, it can effectively be deployed to destroy data, with malware appearing to take the form of ransomware infecting targeted individuals or organizations to wipe data. An example of this can be seen in the MBR-ONI campaign that was identified in November 2017. The attacks targeted several Japanese organizations with what initially appeared to be ransomware deployed on hundreds of computers. The "ransomware" provides a ransom note promising the prospect of recovered data if an extortion demand is met; however, researchers assess that MBR-ONI was not actually designed to have a decryption key provided and instead acted to hide evidence of a targeted infiltration and data exfiltration campaign that had been ongoing for up to nine months prior to the identified attack.[47]

PROACTIVE DEFENSE

Organizations should not feel they can only activate their incident response plans in the event of a breach. Today, the best approach is to adopt a continuous response model—always assume you have been breached—and use your incident response and threat hunting teams to look for the next breach.

In summary:

1. **Cyber threats and adversaries located in Iran** continue to be a growing force to be reckoned with. iDefense threat intelligence research indicates that these threat actors and threat groups will continue to grow their malicious activities and capabilities. These threat actors will likely target other Middle Eastern nations with Android malware and repurposed ransomware.
2. Increasingly, adversaries are utilizing third- or fourth-party **supply chain partners** to penetrate target networks. These adversaries will continue to grow their use of weaponized software updates, pre-packaged devices, and supplier ecosystems to take advantage of the fact that these are out of target companies' control.
3. The oil and natural gas industry continues to be an attractive target for adversaries because of the **convergence of IT and OT.** IIoT devices are introducing attack vectors and vulnerabilities into a technology stack that is largely unprepared for malicious cyber threat activities.

4. Financially motivated **cyber criminals are expanding their capabilities** to include traditional cyber espionage TTPs. Adversaries are poised to explore new malicious tools to attain financial rewards and a profitable return on investment for attacks.
5. Cyber criminals are **shifting their cryptocurrency mining malware** from Bitcoins to other cryptocurrencies. They are also expanding their extortion-based attacks using ransomware and uncovering GDPR violations for the purpose of extortion.

By better analyzing data, organizations can start to anticipate risks and adopt a more proactive approach to defensive strategies through actionable threat intelligence.

APPENDIX

About the report

The Cyber Threatscape Report 2018 presents key findings from iDefense threat intelligence research into significant cyber threat trends during the first half of 2018. This report covers cyber threat trends the iDefense threat intelligence team has observed and analyzed from January 2018 until July 2018. It provides an overview of the trends and how iDefense threat intelligence believes they might evolve and grow throughout the year ahead.

This report should serve as a reference and strategic complement to daily intelligence reporting to provide IT security and business operations with actionable and relevant decision support based on iDefense threat intelligence. It aims to inform IT security teams, business operations teams, and organizations' leadership about emerging cyber trends and threats, to help those groups anticipate key cybersecurity developments for the remainder of the 2018 calendar year (and in some cases beyond), and to provide, where appropriate, solutions to help reduce organizations' risk research using primary and secondary open-source material.

iDefense threat intelligence has been creating relevant, timely and actionable threat intelligence for 20 years, by collecting threat data, indicators of compromise, geopolitical-based, regional-based, and industry vertical-based intelligence. Our team was built to provide our clients with actionable and relevant threat intelligence that they use to support decisions that help them enhance their security teams, defend their networks, bolster their security technology investments, their security processes and their business strategy.

Contacts

Joshua Ray

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

Josh Ray is Managing Director for Cyber Defense across Accenture Security globally. Josh has 18 years of combined commercial, government and military experience in the field of cyber intelligence, threat operations and information security. He holds a Bachelor of Science degree in information technology from George Mason University, an Executive Certificate in strategy and innovation from MIT Sloan School of Management and served honorably as a member of the US Navy.

Howard Marshall

Associate Director, Accenture Security | howard.marshall@accenture.com

Howard Marshall focuses on intelligence operations for iDefense. Prior to joining, Howard was FBI Deputy Assistant Director of the Cyber Readiness, Outreach, and Intelligence Branch. He holds a Bachelor of Arts degree in Political Science and a Juris Doctorate from the University of Arkansas.

Rob Coderre

Senior Manager, Accenture Security | robert.c.coderre@accenture.com

Rob Coderre specializes in Product Management for the iDefense Security Intelligence Services. Previous roles include consulting, channel development, sales engineering and product management for emerging technical markets. He holds a Bachelor of Science degree in aerospace engineering from the University of Notre Dame and is an active CISSP and member of ISSA.

Contacts

Emily Cody

Senior Manager, Accenture Security | emily.a.cody@accenture.com

Emily Cody has 14 years of experience in business development and marketing for FTSE 30 and professional services organizations. Prior to joining Accenture, Emily was a Business Account Lead at PWC and Business Development Lead for France and Germany at BAE Systems.

Jayson Jean

Director, Accenture Security—iDefense Business | jayson.jean@accenture.com

Jayson Jean is Director of Business Operations for iDefense in North America and APAC, with responsibility for business development of the Cyber Threat Intelligence portfolio. Prior to this role, Jayson has 14 years of experience building the strategic direction and leading product development for Vulnerability Management at iDefense.

References

1: **2018 State of Cyber Resilience Report,** April 2018, Accenture

2: **Securing the Future Enterprise Today – 2018,** July 2018, Accenture

3: **"The State of Cybersecurity in the Oil &Gas Industry: United States."** February 2017. Ponemon Institute LLC. http://news.usa.siemens.biz/sites/siemensusa.newshq.businesswire.com/files/press_release/additional/Cyber_readiness_in_Oil__Gas_Final_4.pdf.

4: Richards, Kevin; Ryan Lasalle; Floris van den Dool. **"2017 Cost of Cybercrime Study."** Accessed on July 2, 2018. Accenture. https://www.accenture.com/gb-en/insight-cost-of-cybercrime-2017.

5: iDefense security intelligence services. **"Current US Foreign Policy on Iran Could Compromise Nuclear Agreement."** April 12, 2018. IntelGraph reporting.

6: @khamenei_ir "The prediction that came true! #JCPOA http://english.khamenei.ir/news/5706/." May 29, 2018. Twitter. https://twitter.com/khamenei_ir/status/1001481253022044160

7: iDefense security intelligence services. **"Current US Foreign Policy on Iran Could Compromise Nuclear Agreement."** April 12, 2018. IntelGraph reporting.

8: Lancaster, Tom. **"Muddying the Water: Targeted Attacks in the Middle East."** November 15, 2017. Palo Alto Networks. https://researchcenter.paloaltonetworks.com/2017/11/unit42-muddying-the-water-targeted-attacks-in-the-middle-east/

9: ReaQta.. **"A dive into MuddyWater APT targeting Middle-East; 2017."** November 20, 2017. https://reaqta.com/2017/11/muddywater-apt-targeting-middle-east/

10: Bustami, Mo. **"Burping on Muddy Water."** February 1, 2018. Security 0wnage. https://sec0wn.blogspot.com/2018/02/burping-on-muddywater.html

11: iDefense security intelligence services. **"POWERSTATS Targets Jordan."** June 13, 2018. IntelGraph reporting.

12: iDefense security intelligence services. **"POWERSTATS Malware Continues to Evolve."** February 28, 2018. IntelGraph reporting.

13: iDefense security intelligence services. **"PIPEFISH Activity Continues Targeting Organizations in Middle East."** May 16, 2018. IntelGraph reporting.

14: iDefense security intelligence services. **"PIPEFISH returns with new ISMDoor Variant."** April 9, 2018. IntelGraph reporting.

15: Falcone, Robert and Lee, Bryan. **"OopsIE! OilRig uses ThreeDollars to Deliver New Trojan."** February 22, 2018. Palo Alto Networks. https://researchcenter.paloaltonetworks.com/2018/02/unit42-oopsie-oilrig-uses-threedollars-deliver-new-trojan/

16: Bustami, Mo. **"PRB-Backdoor - A Fully Loaded PowerShell Backdoor with Evil Intentions."** May 12, 2018. Security 0wnage. https://sec0wn.blogspot.com/2018/05/prb-backdoor-fully-loaded-powershell.html

17: iDefense security intelligence services. **"Technical Analysis of Rastakhiz."** November 22, 2017. IntelGraph reporting. ; iDefense security intelligence services. **"Technical Analysis of Tyrant."** May 21, 2018.IntelGraph reporting. ; iDefense Security Intelligence Services. **"Technical Analysis of Black Ruby."** June 9, 2018. IntelGraph reporting. ; @malwrhunterteam. "WannaSmile ransomware: https://www[dot]virustotal.com/en/

18: **"How to develop an Android ransomware."** June 20, 2018. Aparat. hxxps://www.aparat[.]com/v/kNz5T.

19: iDefense security intelligence services. **"Iran-based RASTAKHIZ and TYRANT Ransomware Relationships and Developer Profile."** May 18, 2018. IntelGraph reporting.

20: **"Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps."** March 23, 2018. US Department of Justice. IntelGraph reporting.

21: **"BSI warnt vor E-Mails mit gefälschtem BSI-Absender."** January 12, 2018. Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Gefaelschte_BSI- Mails_12012018.html.

22: iDefense security intelligence services. **"Ukrainian Financial Site Delivers Malware But Is Unlikely to Unleash a Repeat of June 2017 Petya.A Outbreak."** January 24, 2018. IntelGraph Reporting.

23: iDefense security intelligence services. **"Targeted Supply-Chain Attack of CCleaner Software."** September 25, 2017. IntelGraph Reporting.

24: iDefense security intelligence services. **"PIGFISH."** February 21, 2017. IntelGraph Reporting.

25: iDefense security intelligence services. **"BLACK GHOST KNIFEFISH."** July 3, 2017. IntelGraph Reporting.

26: iDefense security intelligence services. **"Analysis of NetSarang SHADOWPAD Supply-Chain Attack."** August 21, 2017. IntelGraph Reporting.

27: iDefense security intelligence services. **"Breach at Third-Party Data Transmission Provider Disrupts Work of Pipeline Companies."** April 4, 2017. IntelGraph Reporting.

28: iDefense security intelligence services. **"Russian Cybersecurity Company <Redacted> Exposes Critical Infrastructure Sectors in Europe and North America to Risks of Cybercrime and Espionage."** June 13, 2018. IntelGraph Reporting.

29: "S.3085 - Federal Acquisition Supply Chain Security Act of 2018." June 19, 2018. 115th Congress. https://www.congress.gov/bill/115th-congress/senate-bill/3085.

30: **"H.R.4668 - Small Business Advanced Cybersecurity Enhancements Act of 2017."** December 18, 2017. 115th Congress. https://www.congress.gov/bill/115th-congress/house-bill/4668.

31: **"S.2735 - Small Business Advanced Cybersecurity Enhancements Act of 2018."** April 24, 2018. 115th Congress. https://www.congress.gov/bill/115th-congress/senate-bill/2735.

32: Ponemon Institute LLC **"The State of Cybersecurity in the Oil & Gas Industry: United States."** February 2017. http://news.usa.siemens.biz/sites/siemensusa.newshq.businesswire.com/files/press_release/additional/Cyber_readiness_in_Oil__Gas_Final_4.pdf

33: Martinotti, Stefano. **"Digitizing oil and gas production."** August 2014. McKinsey & Company. https://www.mckinsey.com/industries/oil-and-gas/our-insights/digitizing-oil-and-gas-production

34: Pettey, Christy. **"When IT and Operational Technology Converge."** January 13, 2017. Gartner. https://www.gartner.com/smarterwithgartner/when-it-and-operational-technology-converge/

35: Ponemon Institute LLC **"The State of Cybersecurity in the Oil &Gas Industry: United States."** February 2017. http://news.usa.siemens.biz/sites/siemensusa.newshq.businesswire.com/files/press_release/additional/Cyber_readiness_in_Oil__Gas_Final_4.pdf

36: Gregory-Brown, Bengt. **"Securing Industrial Control Systems-2017."** June 2017. SANS. https://www.sans.org/reading-room/whitepapers/analyst/securing-industrial-control-systems-2017-37860

37: iDefense security intelligence services. **"Technical Analysis of Triton, a Disruptive ICS Malware."** January 1, 2018. IntelGraph reporting.

38: Olenick, Doug. **"Cyberattack knocks Energy Services Group offline."** April 6, 2018. *SC Magazine*. https://www.scmagazine.com/cyber-attack-knocks-energy-services-group-offline/article/755983/

39: **"Radiflow Reveals First Documented Cryptocurrency Malware Attack on a SCADA Network."** February 8, 2018. *PR Newswire*. https://www.prnewswire.com/news-releases/radiflow-reveals-first-documented-cryptocurrency-malware-attack-on-a-scada-network-300595714.html; Newman, Lily Hay. **"Now Cryptojacking Threatens Critical Infrastructure, Too."** February 12, 2018. *Wired*. https://www.wired.com/story/cryptojacking-critical-infrastructure/

40: Slav, Irina. **"U.S. To Become Net Oil And Gas Exporter In 5 Years."** February 11, 2018. *OilPrice.com*. https://oilprice.com/Energy/Energy-General/US-To-Become-Net-Oil-And-Gas-Exporter-In-5-Years.html

41: **"MASTERMIND BEHIND EUR 1 BILLION CYBER BANK ROBBERY ARRESTED IN SPAIN."** March 26, 2018. Europol. https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain

42: **"WannaCry Hackers Are Using This Swiss Company To Launder $142,000 Bitcoin Ransoms"** August 3, 2017. *Forbes*. https://www.forbes.com/sites/thomasbrewster/2017/08/03/wannacry-hackers-use-shapeshift-to-launder-bitcoin/#691e11573d0d

43: **"Weekly Threat Report 18th May 2018."** May 18, 2018. National Cyber Security Centre. https://www.ncsc.gov.uk/report/weekly-threat-report-18th-may-2018

44: Lasalle, Ryan, Kevin Richards, and Floris van den Dool. **"2017 Cost of Cybercrime Study."** Accenture. https://www.accenture.com/gb-en/insight-cost-of-cybercrime-2017 Accessed on July 2, 2018.

45: Palmer, Danny. **"This destructive wiper ransomware was used to hide a stealthy hacking campaign."** November 1, 2017. ZDNet. https://www.zdnet.com/article/this-destructive-wiper-ransomware-was-used-to-hide-a-stealthy-hacking-campaign/

46: Tiwari, Ravikant. **"Black Ruby: Combining Ransomware and Coin Miner Malware."** February 28, 2018. Acronis. https://www.acronis.com/en-us/blog/posts/black-ruby-combining-ransomware-and-coin-miner-malware

47: Ghibu, Calin. **"Cerber ransomware evolves to steal passwords and Bitcoin wallets."** August 11, 2017. Temasoft. https://temasoft.com/information/cerber-ransomware-steals-data/

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 449,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at **www.accenture.com.**

ABOUT ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organization's valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit the Accenture Security blog.