Accenture Security

CYBER THREAT-SCAPE REPORT

MIDYEAR CYBERSECURITY RISK REVIEW FORECAST AND REMEDIATIONS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Cyber Threat-scape Report examines cyber-threat trends during the first half of 2017 and offers an overview of how those trends might unfold in the latter half of the year. This report should serve as a reference and strategic complement to Accenture Security iDefense's daily intelligence reporting to provide IT security and business operations with actionable and relevant decision support. By informing IT security teams, business operations teams, and organization leadership about emerging trends and threats, the report helps those groups anticipate key cybersecurity developments for the coming year; and provides, where appropriate, solutions to help reduce organizations' risk related to cybersecurity. The report relies on iDefense intelligence collection, research, and analysis as well as research using primary and secondary open-source material. Four key findings result from iDefense research into significant cyber-threat trends during the first half of 2017 in the areas of cyber espionage, financially motivated cyber crime, and hacktivism.

DESTRUCTIVE CYBER-THREAT ACTIVITY IS BECOMING MORE COMMON AND ATTRIBUTION IS GETTING HARDER

The WannaCry and Petya malware outbreaks wreaked havoc against worldwide businesses, governments, and non-profit institutions in mid-2017, using Windows exploits leaked to the public by the hacking group SHADOW BROKERS, widely reported as stolen from government entities. These leaks, which exposed numerous zero-day vulnerabilities, created multiple worst-case network defense scenarios. Although governments are trying hard to avoid future leaks, Accenture Security iDefense anticipates that more exploit arsenals will be exposed in the coming years. While software vendors (such as Web browser providers) are attempting to harden their products, eliminate entire classes of vulnerabilities, and reduce windows of opportunity for threat actors, new exploit releases will undoubtedly result in the broad compromise of those organizations which lack sufficient controls.

WannaCry (linked to North Korea by defense agencies in the United States and United Kingdom) and Petya (with reported links to sources in Russia) are examples of a new strain of high-profile, global-scale, debilitating attacks, that appear to be government-sponsored and aimed at creating chaos and achieving strategic geopolitical goals. Meanwhile, governments struggle to find an acceptable and proportionate response and deterrence actions, as more of what appear to be state-sponsored hackers use tools and techniques traditionally used by financially motivated cyber criminals, complicating attribution and assessments of motive.

Accenture Security iDefense has also observed increasing cyber criminal use of deception tactics, including anti-analysis code, steganography, and expendable command-and-control (C2) servers used for concealment. Greater public reporting on cyber-threat activity and attribution may accelerate this denial and deception trend, increasing the complexity, cost of cyber defense efforts and resource allocation.

Phishing campaigns continue to use familiar lures—subject lines mentioning invoices, shipments, resumes, wire transfers, missed payments, and more—but ransomware has displaced banking Trojans as one of the most common malware types delivered via phishing techniques. Increased user awareness and campaign publicity is driving greater sophistication of the spear phishes observed. Users are still a company's greatest weakness and greatest asset for network defense.

Bitcoin continues to be the currency of choice among cyber criminals; however, with monetization being the end goal of conducting financially motivated cyber crime, iDefense has observed threat actors are taking additional measures to conceal bitcoin transactions. This manifests itself in cyber criminals either developing and leveraging bitcoin-laundering techniques or adopting alternative crypto-currencies.

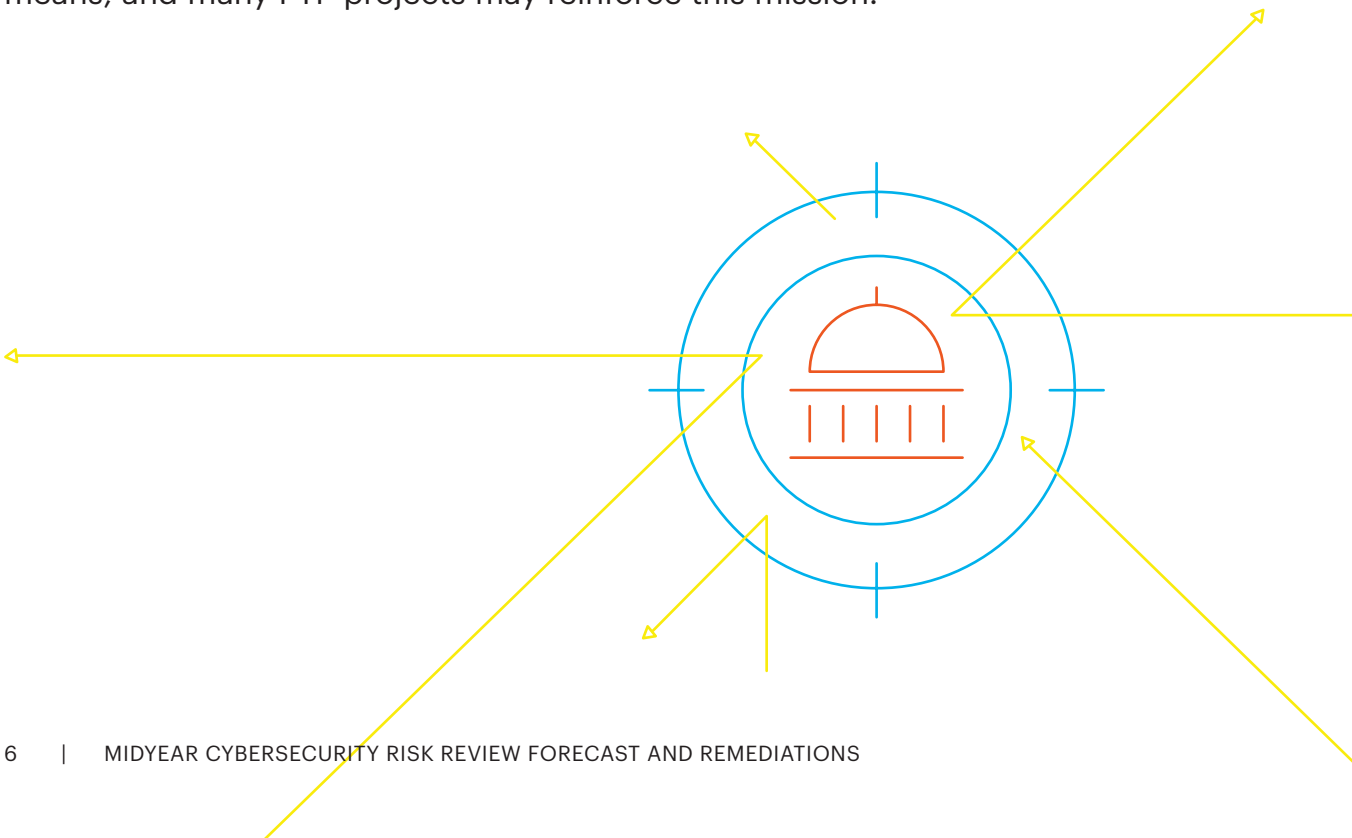
CRIMINAL MARKETPLACES ARE PROFITABLE AND TOOLS ARE MORE ACCESSIBLE TO ALL

An increasingly lucrative criminal marketplace is driving differentiated criminal offerings, emboldening and enabling more actors with better capabilities. The continued evolution of ransomware during 2016 and the first half of 2017 produced variants that were more customizable and richer in features than before. For the remainder of 2017, iDefense expects to see ransomware variants targeting non-Windows platforms, such as Linux and OSX, as well as mobile platforms, such as iOS and Android. Low-end booter and stresser distributed denial of service (DDoS)-for-hire services have given way to a thriving DDoS-for-hire botnet ecosystem primarily employing domain name system (DNS) amplification. The rapid adoption of Internet of Things (IoT) devices has created a rise of IoT botnets, which will continue to grow as more diverse devices join the global network.

GOVERNMENTS
ARE STRENGTHENING CAPABILITIES TO MEET STRATEGIC GOALS

Between October 2016 and June 2017, North Korea is reported to have unleashed several large-scale and noisy operations aimed at exfiltrating foreign intellectual property, stealing money from foreign governments, and probing vulnerabilities within United States and European key critical infrastructure. Iran, meanwhile, has focused cyber espionage and disruption efforts on critical infrastructure verticals such as: financial, energy, aviation, and government. North Korea and Iran continue to improve their national level cyber-threat capabilities, and iDefense expects to see a growth in cyber-espionage and disruption activity from both countries in the next few months, not only in response to geopolitical triggers, such as economic sanctions and military exercises, but also in continuing service to national strategic goals.

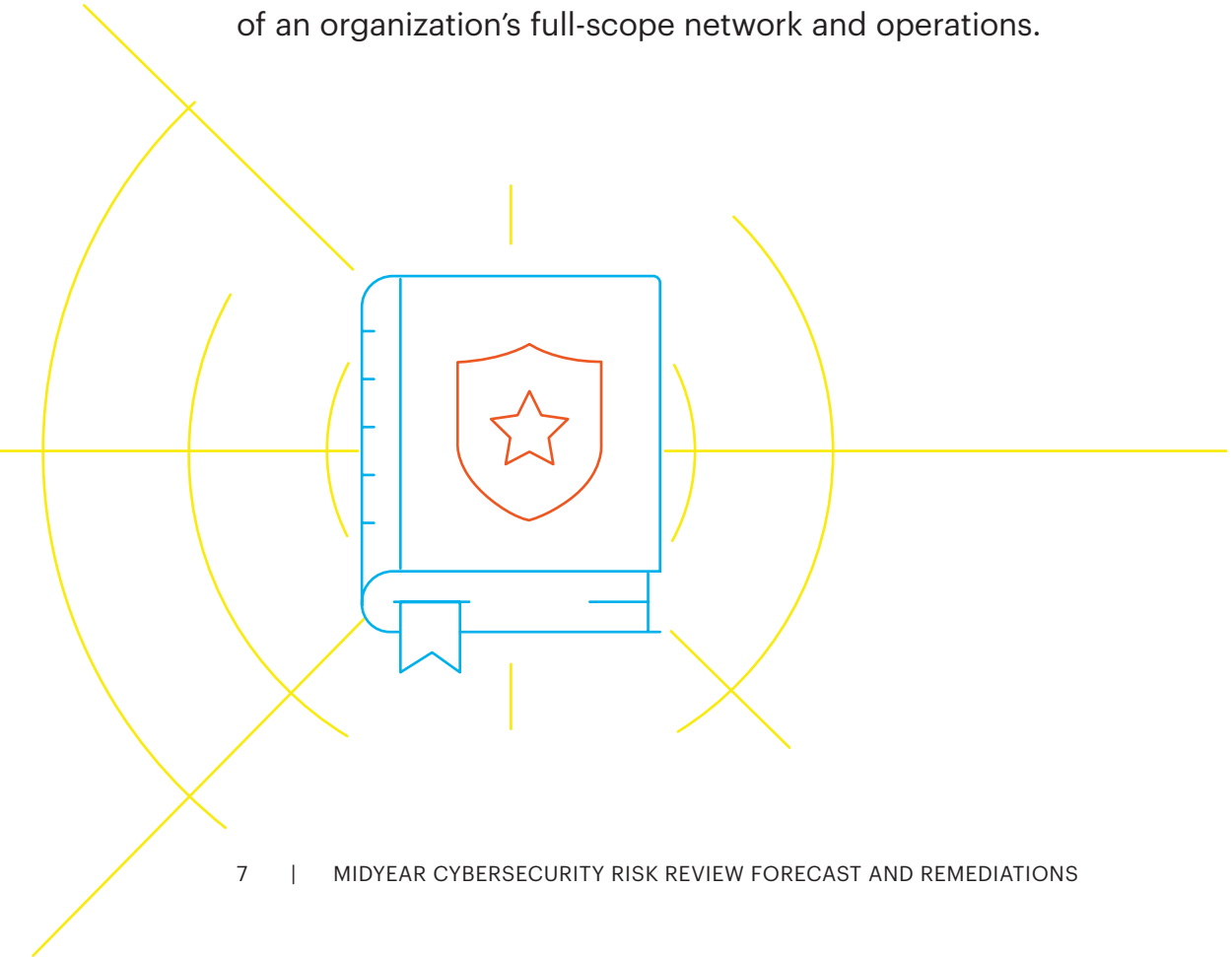
After observing a downturn of activity in China, iDefense expects China's cyber-espionage activities aimed at technology transfer to regain historic levels. China's 13th Five-Year Plan (FYP), which is now underway, may prompt the targeting of companies active in the areas of cybersecurity, cloud computing and big data, new energy automobiles, high-performance computing, biomedical materials, repair and replacement of tissues and organs, deep sea key technology and equipment, and smart grid technology and equipment. Historically, Chinese cyber-espionage operations have heavily targeted foreign technologies that overlap with FYP goals. Newly created after a military-wide restructuring, the Strategic Support Force of the People's Liberation Army (PLA) is also tasked with supporting innovation and military development, including support through cyber espionage means, and many FYP projects may reinforce this mission.



Russian hybrid operations and active measures reached a feverish pitch in the first half of 2017 as election seasons swept over Western Europe. These efforts integrate cyber attacks with psychological operations to exploit media, social media, and influence groups in a bid to exacerbate existing social rifts and solidify pro-Russia policies in targeted countries. Although unsuccessful in bringing victory to Russia's favored candidates in the Netherlands and France, Russia may continue its attempts as German and United States legislative elections approach in late 2017 and 2018.

LAW ENFORCEMENT IS BECOMING OVERWHELMED

Due to a wide range of factors, underground cyber criminal communities are culturally varied. In Brazil, where law enforcement is overburdened and, as a result, criminal conviction low, knowledge and tools (with a heavy emphasis on fraud linked to abuse of personal information) are openly disseminated in “clearnet" (non darknet) hacking forums to maximize visibility to the market, whereas direct transactions occur largely in mobile messaging platforms. The increasing entanglement of financially motivated cyber crime with organized criminal groups has prompted a growth in malware sophistication, although in cases like Brazil’s “off-the-shelf” malware, versions are modified for local environments prior to deployment. Familiarity with local cyber-threat environment is essential to the security of an organization’s full-scope network and operations.



The destructiveness of increasing ransomware and DDoS attacks; the aggressive use of information operations by nation-states; growth in the numbers and diversity of cyber-threat actors; and the greater availability of exploits, tools, encryption, and anonymous payment systems in 2017 pave the way for a rapid growth of cybersecurity challenges across all industry verticals in the coming year. Industry will have to meet these challenges with equally aggressive defense strategies, including user education and the integration of threat intelligence and risk assessment into business operations across the enterprise.

NATION-STATE SPONSORED ACTIVITY IN THE CYBER THREAT LANDSCAPE

REVIEW OF GOVERNMENT/ STATE SPONSORED USE OF INFORMATION OPERATIONS TO FULFILL STRATEGIC OBJECTIVES

SUMMARY

In May 2017, new United States Director of National Intelligence (DNI), Dan Coats, identified Russia, China, Iran, and North Korea as key global cyber-threats, consistent with DNI reporting since at least 2012. Government sponsored cyber espionage continues unabated across all four of these countries, serving each country's national development and strategic priorities; but, in a trend toward hybridization, state-sponsored actors increasingly rely on tools and techniques normally used by financially motivated cyber criminals, complicating both attack attribution and assessments of motive for launching attacks. In early to mid-2017, industry analysts assessed an increasing boldness on the part of government-sponsored cyber threat actors, illustrated by the WannaCry and Petya variant ransomware worm outbreaks which were tentatively attributed to North Korea and Russia, respectively.

Russian state-sponsored information operations dominated the media in the past year. In line with the Russian doctrine of information confrontation and of "hybrid" or non-linear conflict, Russian intelligence services and state-sponsored cyber-threat actors have deftly combined computer network operations (CNO) with psychological operations to pursue their strategic objectives. Hoping to overcome Russia's pariah status and preserve Russian President Vladimir Putin's administration, Russian intelligence services supported United States and European

electoral candidates perceived to be sympathetic to Russia and tried to soften the sanctions regime by distracting attention from Russia's misdeeds and dividing and discrediting the Western liberal establishment. The 2016 United States presidential election showcased Russian information operations, including the compromise and selective leaking of e-mails of campaign workers, the persistent probing of state election commissions' computer systems, and the use of troll-bots and impressionable bloggers to spread disinformation.[1] These operations did not stop after the election of Donald Trump. The first half of 2017 saw renewed efforts to sway European elections,[2] infiltrate Pentagon networks,[3] and discredit non-governmental organizations (NGOs) and think tanks hostile to Russia.[4] Russian intelligence agencies' tactics include the use of criminal hackers and other proxies for plausible deniability[5] and the placement of numerous "small bets" conducted by supporting divisive fringe elements on all sides of the political spectrum in target countries. Russia's efforts have had mixed results: the populist candidates they supported in France and the Netherlands lost elections, and the new United States president's intentions regarding Russia are difficult to discern. Furthermore, competition and conflict within Russia's intelligence agencies themselves create a culture of risk taking and backbiting and has led to arrests and personnel reshuffles. Faced with unpredictable world politics and internal turmoil, Russia's intelligence agencies may to continue their risky information operations to stoke turmoil and confusion in Europe, the Middle East, and elsewhere.

While the world has been transfixed with Russian state operations, Iranian and North Korean cyber-espionage operators have gained valuable experience and made significant gains against global targets across a wide range of industry verticals. As the United States defense industrial base and other high-value targets have shifted defense postures and operations to protect themselves against Russia, Chinese cyber-threat groups appear to have remobilized after a period of relative inactivity. Recent campaigns that iDefense identified illustrate that Chinese actors may, once again, be probing United States' organizations and showing a new willingness to conduct patriotic hacktivist operations.

KEY POINTS

- Increasingly, government/State sponsored operations appear willing to use large-scale, debilitating attacks to conduct successful information operations. The ransomware outbreak WannaCry, which has tentatively been attributed to North Korea, and the Petya variant of June 2017, which has tentatively been attributed to sources in Russia, exemplify a new strain of high-profile, global-scale operations apparently aimed at creating chaos and upending the geopolitical status quo.

- Russian hybrid operations that integrate cyber attacks with psychological operations exploit media, social media, and influence groups to exacerbate existing social rifts in targeted countries. Tactics include making "small bets" by supporting a variety of political extremists, radical activists, and other disruptive forces in target countries. Ostensible hacktivist groups like Bozkurtlar, Anpoland, and Pravvy Sector appear to continue to use Russian-sponsored false-flag operations—exemplified by the 2015 attack on France's TV5 television network—to hype up Islamic threats and stoke dissension between Poland and Ukraine.[6]
- For plausible deniability, Russian intelligence services are reported to have used criminal hackers in return for protection from prosecution. In a recent case, United States prosecutors indicted several officials from Russia's Federal Security Service (FSB) and several criminal hackers, saying they had carried out and exploited the 2014 compromise of a Yahoo! user database for both political espionage and criminal enrichment.[7] Putin encouraged "patriotic hackers" in a June 1, 2017 interview in which he famously smirked, "Hackers are free people, just like artists who wake up in the morning in a good mood and start painting. ... [The hackers] would wake up, read about something going on in interstate relations and if they have patriotic leanings, they may try to add their contribution to the fight against those who speak badly about Russia."[8] The operations of these hackers adds an element of impunity, but also unpredictability to Russian information operations.
- Adding to the unpredictability are reported conflicts and competition within Russian intelligence services encourage them to take risky actions[9] and undermine each other. In Spring 2016, investigators of the Democratic National Committee (DNC) server breach found that two different groups—JACKMACKEREL (APT29), thought to be associated with the FSB, and SNAKEMACKEREL (APT28), thought to be associated with Russian military intelligence—had compromised the same machines without apparently being aware of each other's presence. The late-2016 arrests of top FSB information security officials and members of the hacktivist group Shaltay-Boltay may have resulted from rivalries among the FSB and factions of Russia's Main Intelligence Directorate known in English as "GRU."[10]
- Over the last 12 months, Iranian state-sponsored operations have caused a flurry of cyber-espionage- and cyber-warfare-related attacks, stunning intended targets and outside spectators. Aside from the Shamoon attacks of 2012, the bulk of Iranian cyber activity had traditionally been levied against Iranian dissidents, human rights activists, and other "enemies of the state"; however, 2016 saw wide-scale assaults against foreign governments and militaries, aerospace and defense industries, key critical infrastructure, and other industries ranging from finance to telecommunications.

- North Korea's cyber operations have become commonplace as the country looks to gain legitimacy via homegrown CNO and nuclear capabilities. Over the course of the last eight months, the state has unleashed several large-scale and noisy operations aimed at illegally exfiltrating foreign intellectual property, stealing money from foreign governments, and probing vulnerabilities within United States and European key critical infrastructure.
- Shortly after several scathing reports were released during 2013 that detailed Chinese cyber-espionage operations, the targeting of United States organizations by Chinese state-sponsored groups plummeted. iDefense is again beginning to see Chinese cyber-espionage operations emerge and is anticipating a high tempo of operations similar to those that overran many organizations' defenses in the latter half of the last decade.

GEO-POLITICAL CONTEXT

Russia

Seen in hindsight, early hints seemingly indicated Russian plans to upend the United States' political system with information weapons. At a February 2016 conference in Moscow—before the DNC discovered the compromise of its servers—presidential information security aide Andrey Krutskikh reportedly divulged that "Russia was working on new strategies for the 'information arena' that would be equivalent to testing a nuclear bomb and would 'allow us to talk to the Americans as equals,'" according to a columnist from *The Washington Post* who cited a translated version of notes made by a Russian attendee.[11] iDefense tracked down records of this speech and found that while it may not have been an obvious prediction of Russian operations in the 2016 election, it does exemplify key aspects of Russian approaches to information operations.

According to a press summary of his speech, Krutskikh compared the current situation with the nuclear arms race of 1945 to 1948, raising the specter of "information wars, or as they are called in the West, cyber wars," which are potentially even more destructive than nuclear ones. Krutskikh warned, "the sovereignty, economy and security of the Russian Federation will depend on the quality of reaction to this danger in the next two years." He may also have added more inflammatory remarks not quoted in the press; one Russian blogger, like the attendee cited in *The Washington Post*, says Krutskikh spoke of creating a weapon that would "force America to talk with us as equals."[12]

Krutskikh's speech can be considered a pitch for funding Russia's domestic IT industry, but it also sums up several key aspects of Russian strategists' view of information operations, which are as follows:

- Krutskikh points out that what Westerners call "cyber wars" are more broadly called "information wars" in Russia. This mix of technical cyber attacks and psychological operations can be categorized in terms of color: Russian information operations combine "white" methods (state media), "gray" methods (other sympathetic media), and "black" methods (hackers, trolls, and honeypots).[13] Information operations, in turn, are part of an arsenal of nonmilitary and covert military techniques to undermine adversaries while avoiding overt conflict. Ranging from propaganda and economic leverage to fomenting unrest and introducing special operations forces in the guise of peacekeepers, these types of operations comprise so-called "hybrid" or non-linear conflict, also known as the "Gerasimov Doctrine" of 2013.[14] The use of criminal and "patriotic" hackers also falls into this category.
- Krutskikh portrays this informational arms race as an existential battle for Russia. His call for decisive action against perceived threats to Russia's sovereignty exemplifies what analyst Mark Galeotti has termed the "aggressive defensiveness" of Russian strategists.[15] Indeed, facing domestic discontent, economic stagnation, setbacks in its military modernization program, and international pariah status, Putin and his advisors view the country as encircled by hostile "Russophobic" forces who wield their mass media, tempting consumer goods, and superior technology to undermine Russian sovereignty.[16] Some strategists have warned darkly over the years that the United States and other adversaries are seeking to gain control over Russia and its abundant natural resources.
- Russian information operations exploit the political and informational marketplace of more open Western societies that act against them. As one example, Russian information operations seek to disrupt other countries' politics by making "small bets" on a variety of anti-establishment groups. A prime example is the famous picture of former DIA chief and future Trump advisor Michael Flynn sitting near Putin at the head table of a December 2015 dinner celebrating the RT[17] propaganda outlet. Another figure at the table is Jill Stein, the Green Party candidate, who served as another person who might potentially draw away votes from Hillary Clinton. Kremlin-linked Russian organizations also invited Californian or Catalan separatists to conferences and paid a Czech Stalinist and other fringe activists to stage anti-establishment protests in their countries.[18]

The recent outbreak of the June 2017 Petya ransomware variant, attributed by many to Russia, is another illustration of Krutskikh's observations. Occurring shortly before the international G20 summit in Hamburg, Germany, the Petya re-release appeared to be a Russian effort to isolate Ukraine by persuading multinational corporations to cease operations in that country due to the constant risks that cyber-threat activity poses there. The "NoPetya" incident caused major financial hardship to numerous multinational corporations across a broad spectrum of industry verticals and served to concurrently wound Ukraine, punish Western companies doing business there, and create an opportunity for Russia to influence aspects of the G20 agenda to its advantage.

Russia's efforts have had mixed results. Montenegro joined NATO on June 5, 2017, despite a Russian-backed coup attempt and targeting by SNAKEMACKEREL (APT28).[19] The US-initiated arrests of Russian hackers Stanislav Lisov, Yevgeniy Nikulin, Petr Levashov, and Karim Baratov and the conviction of Roman Seleznev—all criminal hackers who appear to have worked with or received protection from Russian intelligence services—may provide Western law enforcement with more information on higher-level accomplices. Several ongoing United States investigations threaten to uncover more information on Russian operations in the 2016 elections, and the United States Senate has already passed a measure to impose new sanctions. Putin has tried to make a virtue of Russia's international isolation, saying it will make Russia's domestic industries stronger, but falling living standards have led to rising protests. Putin may fear that discontented voters will fail to deliver him a resounding victory in the Russian presidential elections planned for March 2018.

Within the Russia intelligence agencies themselves, competition and conflict have led to arrests and personnel reshuffles that could distract the intelligence services from pursuing foreign targets. At the same time, each faction could seek to prove itself through risky gambits in the information sphere.

Faced with unpredictable world politics and internal turmoil, Russia's intelligence agencies may continue their risky information operations to stoke turmoil and confusion in Europe, the Middle East, and elsewhere. They are continuing to infiltrate and probe political targets and seek new ones. In June 2017, iDefense discovered four newly registered domains—possibly created by the SNAKEMACKEREL (APT28) group, which is probably affiliated with the GRU—that could potentially be used to deliver exploits.[20] Top criminal hackers like Aleksey Belan and Yevgeniy Bogachev remain in Russia, apparently immune from prosecution. Russia may continue to use these criminal hackers and false flags to maintain deniability. The difficulties of attribution make it hard for targeted NATO members to invoke Article 5 in

collective self-defense and even to classify an operation by non-state actors as one carried out "on the instructions of, or under the direction or control of" a state, according to the non-binding International Law Commission's definition.[21]

In a worst-case scenario, Russian strategists may be honing potential destructive attacks against the critical infrastructure of whole countries. The December 2016 cyber attack that briefly shut down a power plant in Ukraine was not an isolated incident but rather part of a two-week series of outages in the systems of Ukraine's Treasury, Defense Ministry, and state railway, and parts of its financial and physical infrastructure, followed by an upsurge in fighting in eastern Ukraine. This rash of cyber attacks appears to have been carried out by people linked with the Russia-sponsored Sandworm team (iDefense-termed "SANDFISH") in what iDefense assesses was an attempt to further weaken and discredit the anti-Russian Kyiv government and force it to make concessions to the Russia-backed separatists. Analyses of the electrical outage, dubbed CRASHOVERRIDE or INDUSTROYER, have shown that with some effort, such an outage attack could be adapted to target power plants and other infrastructure facilities in other countries as well.[22] Assuming Russia indeed stood behind this series of outages in Ukraine, it may try to carry out such an attack again against other countries.[23] The planned Russian-Belarus Zapad-2017 (West-2017) military exercises scheduled for September 14 to 20, 2017, may also include tests of strategies that integrate cyber attacks with kinetic ones, with some fearing that such exercises could turn into a surprise attack on the Baltic states.

For most of 2015 and 2016, Russian CNO dominated open-source reporting and the news, which allowed Iranian and North Korean activity to operate highly effectively in the background. During this time, state-sponsored actors from both of those countries made substantial strides in both malware development and campaign management.

Iran

High visibility reports over the past year or so have detailed recent Iranian cyber-threat activity that usually occurs when a sophisticated or daring cyber campaign hits a large or high-value target, typically in the utilities, key critical infrastructure, or financial verticals. For example, in March 2016, major news outlets carried stories about government-affiliated Iranian actors gaining access and probing the infrastructure of the Bowman Avenue Dam, a small flood-control structure located about 20 miles north of New York, NY. The United States FBI named seven Iranian nationals and two Iranian companies that they said potentially carried out the attack. Another major Iranian campaign that set off global concern was the late 2016/early 2017 targeting of Saudi infrastructure and Saudi companies with Shamoon 2 malware (also known as Disttrack

or StoneDrill). Iranian actors may have designed this sophisticated malware for the sole purpose of destroying data and disrupting networks throughout the Middle East and Europe. Victims included organizations in the energy, aviation, government, finance, and education verticals.[24]

Iran has made significant strides in terms of cyber-espionage capabilities during the past few months. Several recent, successful cyber espionage campaigns attributed to Iranian actors have taken aim at Western defense and aerospace companies with the intent of stealing defense-related intellectual property used by Western-backed countries in the Middle East. In one series of examples in 2016, Iranian cyber actors targeted United States, Israeli, and Turkish organizations with upgraded versions of those countries' own malware. These particular attacks displayed sophisticated levels of social engineering and prior knowledge of the victims, marking a sharp reversal from earlier Iranian campaigns that leveraged primitive malware such as TinyZbot. Iran may continue to develop its cyber-espionage programs as it continues to enable the transfer of technology and strengthen its influence operations.

North Korea

In a likely effort to take attention away from its nuclear program, North Korea has seemingly forced its portfolio of information operations into the mainstream by launching a number of noisy and spectacular cyber-campaigns in rapid succession. Although many of North Korea's ambitious political plots have failed over the years, many of its recent cyber-threat campaigns have succeeded in causing serious damage and have now caught the world's attention.

It is widely assumed that most of North Korea's cyber-threat actors (presumed to be state sponsored because the majority of the country does not have access to the Internet) are trained in China and may operate there as well. Credible open-source reporting indicates that key North Korean cyber campaigns originated from the Chilbosan Hotel located in Shenyang, China.[25] It is from locations such as this that North Korea's cyber-threat actors are probably launching waves of cyber espionage and criminal campaigns against victims located within South Korea, Japan, and the United States, ranging across a number of industry verticals. In a series of recent operations, North Korean state-sponsored cyber-threat actors are thought to have been successful in stealing an estimated US$80 million or more from the Central Bank of Bangladesh and launching WannaCry, one of the largest ransomware campaigns to date.

North Korean actors have also advanced their malware capabilities and sharpened their espionage skill sets. According to a recent report jointly released by the FBI and Department of Homeland Security (DHS), North Korea has conducted cyber-espionage activity against aerospace and defense companies since at least 2009. While many of the early campaigns leveraged open-source toolkits, according to the report, recent espionage-related activity has used customized malware which may have been authored by North Korean actors trained in China.[26]

China

After being publicly outed by the United States government and having individual operators placed on FBI "Wanted" posters in 2013, Chinese cyber-espionage operations against United States commercial targets largely went dormant in late 2015, entering a period of relative quiet spanning at least 18 months. During this time, the People's Liberation Army (PLA) conducted a top-down reorganization, resulting in the consolidation of its space, cyber, and electronic warfare departments under a "Strategic Support Force, to which the PLA gave the task of advancing China's military innovation through "leapfrog development"—a theme that closely parallels the guidelines of China's 13th FYP economic development roadmap.[27] In the first half of 2017, Chinese state-sponsored cyber-threat actors began to reassert their interest in high-value United States targets in a renewed bid to collect United States defense data and government secrets.

An example of this emergence took place in February 2017, when Chinese state-sponsored actors targeted a major United States defense contractor and South Korea's government, military, and businesses in opposition against the deployment of the United States Terminal High Altitude Area Defense (THAAD) air defense system to South Korea. China has strongly opposed the THAAD system as a threat to its national security and regional stability. The targeting of United States defense contractors may be an attempt to collect intelligence that would enable the Chinese government to development countermeasures and identify specific THAAD deployments inside South Korea.

In concert with the targeting of the United States defense contractor, Chinese hacktivists launched a DDoS attack against the Chinese-language website of Lotte, a South Korean retail giant that sold a golf course to be used for the THAAD deployment; South Korea's Ministry of Foreign Affairs also confirmed that several on-and-off DDoS attack attempts originating from China were levied against South Korean government websites, including that of the Ministry of Foreign Affairs. These attacks, though not

necessarily coordinated with the PRC's cyber-espionage operations, went unpunished by the Chinese. This eruption of patriotic hacktivism evokes the "UnitedStates-China Hacker Wars" of the late 1990s and early 2000s, when Chinese patriotic hacktivists responded aggressively to United States actions they deemed harmful to China's dignity, including the 1999 United States bombing of the Chinese embassy in Belgrade, Yugoslavia, and the 2001 in-air collision between a United States EP-3 surveillance aircraft and a Chinese J-8 fighter jet.

The new Chinese patriotic hacktivism is not limited to the Lotte attacks. In July 2016, a group claiming to be the Chinese hacktivist collective "1937CN Team" defaced the website of Vietnam Airlines with a message declaring its defense of China's "territorial inviolability"—a response to the decision by the Permanent Court of Arbitration favoring Philippine territorial claims over Chinese claims in the South China Sea. In addition to the defacement, the 1937CN Team gained control of sound systems and took over multiple flight status display screens at Vietnam's Noi Bai and Tan Son Nhat airports, causing panic among fliers and airport staff. As with the Lotte attack, the Chinese government largely ignored the 1937CN Team's cyber attack, though its crossover into airport messaging systems signaled an escalation in Chinese patriotic hacktivist behavior.

If more hacktivist groups join the bandwagon, this trend could cultivate a new generation of "politically useful" hackers and potentially a new generation of IT leaders, as the first generation of patriotic hacktivists became.

iDefense anticipates that Chinese state-sponsored information operations will reemerge at scale against the United States and other global targets, with cyber-espionage operations being carried out on an ongoing basis to fulfill national development goals and hacktivist activities being conducted at times of high-profile conflict. This may lead to potential victim organizations becoming overwhelmed despite their attempts to defend against coordinated and persistent Chinese cyber-espionage campaigns and occasional hacktivist operations while also fending off influence campaigns and other information operations from multiple other nation-states at the same time. Timely, measured, and actionable intelligence may mean the difference between compromise or debilitation, and prevention.

CHINA'S 13TH FIVE-YEAR PLAN AND ECONOMIC CYBER ESPIONAGE AGAINST KEY INDUSTRIES

SUMMARY

Over the past decade and a half, economic cyber-espionage activity from the People's Republic of China (PRC) has repeatedly targeted industries defined as strategic within China's Five-Year Plan for Economic and Social Development of the People's Republic of China (中华人民共和国国民经济和社会发展五年规划纲要), also called the Five-Year-Plan (五年计划／规划) or FYP, which is China's long-term plan for the country's economic and social development. The 13th FYP (covering the years 2016 to 2020), ratified by China's top legislative body (the National People's Congress) in March 2016, is the first FYP under President Xi Jinping's leadership and a bellwether of national strategic development priorities under the Xi administration and beyond. One of the major differences between the 13th FYP and previous FYPs is a focus on innovation.

The 13th FYP emphasizes innovation through a series of national research and development (R&D) projects and recommends the implementation of an "Innovation-Driven Development Strategy" (创新驱动发展战略), which would establish this emphasis for years to come. Among other areas, the Innovation-Driven Development Strategy targets breakthroughs in core technologies, including IT, new energy, new materials, aviation, biological medicine, and intelligent manufacturing, advancing scientific research on the origins and development of the universe, material structures, and the science of the brain and cognition. To meet these strategic targets, government organizations, institutions, and businesses may compete for government funding and resources. The extreme pressure placed on these entities to succeed in reaching their goals may encourage cyber-threat activity to help fulfill them.

A careful look at the focus for China's innovation strategy and related key state R&D projects shows that iDefense clients in various industries—including energy, aerospace, pharmaceutical, healthcare, and IT—are in line with the current FYP's strategic focused industries. An understanding of the specifics of China's key state R&D projects will help iDefense clients strategically plan their own research projects, protect trade secrets (especially those related to parallel technologies), and focus the development of computer network defenses on key programs to proactively avoid future cyber attacks and intellectual property theft.

KEY POINTS

- Established in 1953, FYP was created as a means to guide the direction of China's social and economic development. FYPs are designed to serve as blueprints to fulfill the social, economic and political objectives of the Chinese Communist Party (CCP). FYPs provide guidance to ministries, local governments, and industry players on central government priorities and indicate the government's long-term future development vision. As such, FYPs are helpful guides for an understanding of the likely direction of China's economic development.
- The current (13th) FYP highlights the stimulation of "high-end" innovation through a series of national R&D projects and the implementation of the Innovation-Driven Development Strategy. The strategy seeks to "vigorously initiate" major international science projects and foster new competitive advantages for China in foreign trade by enabling the export of more high-end equipment and cutting-edge products with high levels of added value.
- Driven by the 13th FYP and its Innovation-Driven Development Strategy, the National Key R&D Plan (NKR&DP) is the first of China's five reformed national science and technology plans to be implemented in February 2016. The NKR&DP reorganizes and streamlines numerous pre-existing state-funded science and technology programs. Under the plan, the first round of national key R&D projects in 2016 includes work in areas such as cybersecurity, cloud computing, big data, new energy automobiles, high performance computing, biomedical materials, repair and replacement of tissues and organs, deep sea key technology and equipment, and smart grid technology and equipment.
- Several cyber-enabled economic espionage activities tied to China have been associated with various PRC government national strategic plans, including FYPs, in the past 15 years. These espionage activities have affected United States firms as well as other businesses globally.
- Organizations and companies aligned with China's FYP priorities may be potential cyber-espionage targets and should take special precautions to protect their intellectual property.

BACKGROUND

Since 2008, iDefense has observed numerous computer network intrusion activities from China deemed to be examples of cyber-enabled economic espionage. These activities include campaigns by groups iDefense has named, such as SWORDFISH, DESERT PUPFISH, SILVERCARP, FLAGFISH, DOGFISH, and SNIPEFISH.[28] These activities have targeted industries including aerospace, alternative energy, IT, telecommunications, and defense in the United States, Japan, the United Kingdom and South Korea—industries closely aligned with

China's strategic priorities under the 11th and 12th FYPs. China's 11th FYP lists strategic industries such as armaments, power generation and distribution, oil and petrochemicals, telecommunications, coal, civil aviation, and shipping; the 12th FYP's strategic emerging industries are identified as clean energy technologies, next-generation IT, biotechnology, high-end equipment manufacturing, alternative energy, new materials, and new energy vehicles.

In 2013, the world first learned publicly about cyber-espionage activities by the Chinese PLA unit 61398, which iDefense refers to as FLAGFISH. Cyber-security vendors observed that the targets of this group matched industries in four of the seven strategic emerging industries in China's 12th FYP. According to public reports, FLAGFISH targeted industries in clean energy technologies, next-generation IT, alternative energy, and new materials, all of which were listed as strategic emerging industries in the 12th FYP.

In 2014, in an indictment against five members of the PLA for alleged targeting of United States firms for commercial advantage, the United States Department of Justice also identified United States targets in line with PRC government economic development priorities. Victims included WestingHouse Electric Co., SolarWorld AG, and United Steel Corp. and represented industries in clean energy technologies, high-end equipment manufacturing, and new materials. The technologies and products of these companies were also within the scope of the strategic emerging industries in the 12th FYP, further suggesting that China's national strategic plans may be driving portions of China's cyber-enabled economic espionage activities.

ASSESSMENT/IMPLICATIONS

iDefense fully expects that cyber-enabled economic espionage will continue as the implementation of China's 13th FYP unfolds. Many key state R&D projects have already emerged from the various science and technology plans directed under the 13th FYP. By June 15, 2017, a total of 42 special key projects consisting of 1,163 programs had been published as the part of the National Key R&D Plan for 2017. The program's total funding exceeds 22.3 billion yuan (US$3.2 billion). Universities, research institutions, enterprises, and key state laboratories that undertake these projects are under heavy pressure to fulfill their tasks on time. As the cases discussed above have shown, this pressure to succeed may encourage cyber-threat activity against companies whose technologies parallel the FYP's priorities. iDefense recommends that clients exercise caution when meeting with counterparts from China or participating in conferences in the region, gain an understanding of the FYP-funded projects, study where those projects overlap with their company's own key projects and business drivers, stand up a vigorous form of defense in areas identified as vulnerable to cyber-espionage targeting, and adjust business operations to counter the threat.

MALICIOUS CYBER ACTIVITY: GROUPS AND THREATS

IMPLICATIONS OF SHADOW BROKERS' GROUP RELEASE OF EQUATIONGROUP WINDOWS EXPLOITS AND TOOLS

SUMMARY

On April 14, 2017, the SHADOW BROKERS group released a cache of Windows exploits and tools thought to be from the EQUATIONGROUP DRUG Windows espionage tool set. This tool set contains tools that target SWIFT Alliance Access (SAA) systems. iDefense assessed that the exploits were legitimate and targeted various versions of products, including Microsoft Windows, Lotus, and Alt-n.

The real identity of the actors behind the SHADOW BROKERS group is still unknown, but iDefense continues to monitor this group's actions.

KEY POINTS

The following are some key points from the SHADOW BROKERS dump:

- Exploits targeted Microsoft and Lotus products, and SWIFT Alliance Access systems.
- The dump included various tools, exploit frameworks, and other custom binaries.
- All files were from circa 2013.
- Microsoft patched the exploited vulnerabilities in March 2017.
- The WannaCrypt[29] ransomware repurposed one of the SMB vulnerabilities to spread.

BACKGROUND

On August 13, 2016, a collective calling itself SHADOW BROKERS posted a message on various public forums. The message was cryptographically signed on August 13, 2016, and 2:26:52 a.m. ET. In this message, the group established that it had in its possession a stash of exploits from EQUATIONGROUP. It also established that it was willing to sell those exploits to the highest bidder. To prove the authenticity of the exploits, SHADOW BROKERS gave away a "free file," which was widely accepted to contain accurate information. This was the first of many messages to come, eventually leading to a public release of the full cache of exploits in April 2017. iDefense has detailed coverage[30] of this message and others[31] that followed it.[32]

In the months leading up to April 2017, the SHADOW BROKERS group issued a lot of communiqués. It went from announcing a bidding war for one million bitcoins (US$590 million at the time) to later cancelling it and then choosing to eventually release all exploit files for free. iDefense's detailed report is available on the IntelGraph.

The exploits primarily target Microsoft, Lotus, and Alt-n. They targeted various versions of Microsoft Windows and Microsoft Outlook Web Access (OWA). The primary attack vector for Microsoft Windows was the SMB service. Multiple SMB exploits that potentially target different vulnerabilities in the SMB stack exist for both SMBv1 and SMBv2, including ETERNALBLUE and ETERNALROMANCE. Most of these SMB exploits can be used against various versions of Microsoft Windows.

A Metasploit-like exploitation framework was also in the cache of files. The framework supports the targeting various platforms like Windows, Linux, and Sun SPARC. It is a Python-based framework that uses XML to build configuration files for exploits. This makes the framework highly configurable in terms of target versions, payloads, parameters, and transport mechanisms.

One of the interesting elements of the cache is a set of runtime libraries for Microsoft Windows (dynamic-link library [DLL] files). These libraries encompass a great deal of the common functionality required to build post-exploitation tools and capabilities. Some of the interesting libraries are as follows:

cnli-0.dll – Function to wrap various file, socket, and thread functions, as well as other data structures like trees, heaps, etc.

pcla-0.dll – Function to prepare, upload, and launch persistence modules

xdvl-0.dll – Function to work on shellcode

tibe-2.dll – Function to work on SMB

riar-2.dll – Function to work on payloads

trfo-2.dll – Function for file operations like compression, encryption, and hashing

trch-1.dll – Function to parse exploit and payload Manifest files

exma.dll – Library to connect to target

coli-0.dll – Logging system

The cache also includes various other scripts and persistence modules (implants). One of the implants is Managed Object Format (MOF)-based, which is not something that iDefense comes across frequently.

In February 2017, Microsoft abruptly canceled its monthly patches. iDefense analysts now speculate the reason for cancellation to be the SHADOW BROKERS dump. After the group's "MESSAGE FINALE" on January 23, 2017, analysts report that Microsoft might have received information about the impending cache of exploits, which might have led the company to prioritize the patching of these vulnerabilities over its monthly patch cycle. Subsequently, in March 2017, Microsoft fixed the SMB vulnerabilities in MS17-010.

Microsoft addressed its patching of SHADOW BROKERS exploits in a blog posted one day after the public release of the exploit tools; these patched the following exploits:

- EternalBlue, addressed by MS17-010
- EternalRomance, addressed by MS17-010
- EternalSynergy, addressed by MS17-010
- EternalChampion, addressed by CVE-2017-0146 and CVE-2017-0147
- EsikmoRol, addressed by MS14-068
- EmeraldThread, addressed by MS10-061
- EducatedScholar, addressed by MS09-050
- EclipsedWin, addressed by MS08-067
- ErraticGophe, addressed prior to the release of Windows Vista

Interestingly, the SHADOW BROKERS group chose to dump the cache after Microsoft patched the vulnerabilities. In hindsight, this helped control the damage that threats like WannaCry would have inflicted on the Internet.

IMPLICATIONS

Since 2013, leaks have become commonplace in the news. Various government agencies added many new checks and policies to stop leaks.

The April 2017 leak from SHADOW BROKERS is probably the worst leak from them yet. It not only made public various zero-day vulnerabilities in critical programs but also enabled widespread damage by crimeware like the WannaCrypt ransomware. The leak practically demonstrated various worst-case scenarios. While the likelihood of another leak of such magnitude is suspect, defenders should always be vigilant.

In its communiqué on June 2017, SHADOW BROKERS announced a "Monthly Dump Service" for paying customers. Not knowing what might come out of such a service makes it hard to defend against it; however, there are precautions that can be taken in preparation for such an event. These precautions include the following:

- Apply the latest software patches.
- Upgrade to the latest versions of operating systems when possible.
- Automatically curb exploits like ETERNALBLUE and ETERNALROMANCE.
- Use mitigation technologies such as the Enhanced Mitigation Experience Toolkit (EMET) when upgrading to the latest version of an operating system poses an issue.
- Plan meticulously, and prioritize critical and out-of-band patches.

FUTURE THREAT OUTLOOK
POST-WANNACRY ATTACK

SUMMARY

WannaCry's success demonstrated the effectiveness of remote compromises by weaponizing leaked exploits, which may entice actors to refine the tactics, techniques, and procedures (TTPs) used during the WannaCry attacks for future attacks as new exploits are leaked. iDefense has already observed several new malware families using the ETERNALBLUE exploit; these families include UIWIX, ETERNALROCKS, ADYLKUZZ, and new remote access Trojans. Considering the SHADOW BROKERS' claim to plan to drop additional exploits and tools in June 2017, there may be an emerging trend of these types of WannaCry worm attacks in the near future.

KEY POINTS

- Should additional leaks in the future contain usable source code or executables, it is almost certain that malicious actors will quickly attempt to implement them in new attacks within three to five weeks of release; however, vendors may provide patches before threat actors can utilize source code and executables in widespread attacks, as seen by Microsoft Corp.'s early patch of the CVE-2017-0145 vulnerability.
- Many of the exploits that EQUATIONGROUP or other advanced threat groups are believed to have developed do not necessitate the need for phishing e-mails or watering hole attacks that require user interaction for exploitation. "Always-on" and Internet-accessible components enable vulnerabilities to be exploited without the need for user interaction.
- In the case of the recent WannaCry worm attack, victims did not have to perform any action to propagate the malware. The worm exploited a vulnerability in the Sever Message Block 1 (SMB1) protocol and was able to self-propagate by scanning the victim network for new potential victims, exploit them, and then repeat those steps.
- The WannaCry malware was exploiting an already-patched vulnerability popularly known as ETERNALBLUE (CVE-2017-0145). The mitigating measures for worms that exploit already-patched vulnerabilities and worms that exploit zero-day (unpatched) vulnerabilities are similar with the exception of one critical difference: to mitigate attacks leveraging worms that exploit already-patched vulnerabilities, the most important task is detecting unpatched systems and patching them rapidly.
- Threat actors may study previous successful worms such as STUXNET, SASSER, and CONFICKER to accelerate development of their TTPs to avoid the propagation flaws found in WannaCry.

BACKGROUND

WannaCry is ransomware that gained prominence in a large-scale attack observed on May 12, 2017, using version 2.0 of the malware. Version 1.0 was first observed in use in April 2017. WannaCry exhibits several interesting features such as using Tor (The Onion Router) and spreading via Server Message Block (SMB) shares. WannaCry exploits the vulnerabilities associated with Microsoft's Security Bulletin MS17-010, which is linked to vulnerabilities tracked by the following CVE IDs:

CVE-2017-0143	CVE-2017-0146
CVE-2017-0144	CVE-2017-0147
CVE-2017-0145	CVE-2017-0148

SMB Vulnerability Exploit PoC (patched via MS17-101)

Original PoC: RiskSense's MS17-010

- Prior to April 28, 2017, security company RiskSense had been attempting to create a proof-of-concept (PoC) Metasploit module for the ETERNALBLUE vulnerability.
- On April 28, 2017, security researcher zerosum0x0 started to document their work publicly on their GitHub repository.
- The following analysis is based on the additions to the original repository, made between April 28, 2017, and May 16, 2017.
- RiskSenseOps MS17-010 Repository Commits
- On May 16, 2017, RiskSense deleted the MS17-010 repository from GitHub, as it was preparing to merge all of the repository's code into the Metasploit project; the group then started the new repository, which is now part of this project. The following URL leads to a fork of the project, with the last official addition made on May 14, 2017: https://github.com/TheCodeArchiveProject/MS17-010_SUBNET/commits/master. This page has additions from other people made after May 14, 2017, but it serves as a good source for the addition timeline.

Language analysis and attribution leads

The 28 ransom messages contained in the WannaCry malware presented semantic differences and language-specific anomalies. Whereas the English-language and other messages contained obvious errors in grammar, syntax, and word choices—indicative of a machine translation or a poorly executed human translation—others appeared fluent and even erudite. These include the Russian- and Chinese-language messages. In an effort to determine the likely native language of the message author, iDefense analyzed the English, Portuguese, Italian, Russian, and Chinese texts. iDefense concluded the following:

- The Chinese-language version of the ransom note is probably the original version of the text and was probably written by someone who speaks a style of Chinese prevalent in the Northeastern provinces bordering North Korea.
- This analysis creates a reasonable suspicion that the actors behind WannaCry (or at least behind the Chinese-language WannaCry ransom notes) may include native Chinese speakers, actors familiar with Chinese online jargon, and actors from China's northeastern region bordering North Korea.

Cross-comparison of malware with other malware families

Followed by claims of possible attribution with the Lazarus group, iDefense captured two sets of samples and investigated the possible code overlap and use of similar algorithms in both sample sets.

When comparing an older variant of the u.wnry module and a more recent sample, iDefense noted that one specific function indicates that the malware samples are using the same custom SSL implementation. These functions are sub_402560 in the older u.wnry variant and sub_10004BA0 in the more recent sample. The more recent sample is a variant of the Backdoor.Contopee backdoor that was reportedly used in attacks against Swift and major banks by the Lazarus threat group.

- Based on the code similarities and overlap between one set of samples, and code sharing between another set of samples, iDefense assesses that the actors behind WannaCry have access to the same source code that the Lazarus threat group used.
- Based on analysis of these samples, iDefense assesses that it is likely the actors behind the development of the WannaCry ransomware either had access to the tool set the Lazarus group used or that the same threat group developed both that tool set and the WannaCry malware.

ASSESSMENT/IMPLICATIONS

iDefense recommends reviewing network interconnections, Internet-accessible systems, and enabled services in a given environment with the goal of reducing attack surfaces and visibility to an extent that is acceptable at a given organization. iDefense's analysis of SHADOW BROKERS' previously advertised tools and exploits indicates that the following items are possible targets:

- SMB
- Local Security Authority (LSA)
- WinSock API (WSA)
- RDP
- RPC DCOM
- MSSQL
- IIS
- Oracle Database (Oracle RDBMS)
- Lotus Notes
- SolarWinds
- Chrome
- Firefox
- Skype
- Dropbox
- Anti-virus endpoint agents
- NetBIOS
- Active Directory (AD) / Lightweight Directory Access Protocol (LDAP)

CONCLUSION

Because organized threat groups often separate their malware programmers from the people who carry out malicious operations, iDefense is not able to tie the WannaCry malware developer to the WannaCry operatives.

The use of a kill switch indicates it is highly likely that the developers intended to implement such a mechanism to prevent infection of the compromised infrastructure being used to conduct operations. In other words, because the worm has the capability to scan the whole Internet to find vulnerable systems, it is possible that the WannaCry threat actors implemented a local DNS resolver for the developing systems to prevent self-infection.

During the course of investigation, iDefense exhausted its internal and external sources and found no trace of any e-mail delivering the malware. Many third-party security vendors came to the same conclusion.

ADVERSARY OBFUSCATION AND DECEPTION TACTICS

SUMMARY

As security awareness rises, defenses harden, and cyber intelligence increases in visibility, iDefense has observed threat actors' implementation of denial and deception (D&D) tactics expand. D&D includes information operations that incorporate falsehoods while also concealing or obfuscating observable evidence of the objective; use of this tactic can increase the success of cyber-criminal and espionage group operations before the global security community discovers and mitigates them. iDefense believes that threat actors' repeated use of D&D tactics may help these actors progressively hone their ability to deceive network defenders and victims, which will lead victims to take additional actions that will further weaken resiliency against threats. Furthermore, iDefense predicts that the increasing public reporting, actor attribution, and recent scrutiny of threats in the news may accelerate this D&D trend and its subsequent operational sophistication as threat actors learn from public detailed analysis of similar actors to avoid investigation. The key points to these trending D&D tactics that iDefense has documented include the following:

- Increased use of anti-analysis code in malware to deny accurate run-time analysis in debuggers and virtual machines

- Reappearance of steganography in malware to obfuscate and hide information
- Progressive concealment techniques of C2 infrastructure using disguises and camouflage to hide behind layers of more-expendable C2 servers, DGA domains, or other distractions
- Prevalence of packaged malware or obfuscated script code to mask its detection.

Cyber-crime malware concealment and defensive strategies in use

Detecting the environment

Malware has been attempting to detect the environment of a victim computer for many years. The methods of detection may change over time, but in general, malware attempts to detect the presence of virtual machines and security tools. These checks are often conducted by checking for the presence of certain Registry keys, paths, and files pertaining to virtual machines and tools.

The script code in Web-based malware may contain exploit code to leverage an information disclosure vulnerability. In March 2017, the actors behind the Astrum exploit kit added exploit code for this vulnerability to the kit. This enabled the kit to determine if certain anti-virus software might be installed on the victim system.

Stenography

Malware hides necessary information such as additional malware or URLs in images. In early December 2016, an AdGholas malvertising campaign used stenography to hide script code in the alpha channel of an advertising banner. Victims were served either the malicious banner or a clear banner based on the malvertising server's processing of potential victim machine information. The script code in the malicious banner would eventually redirect the victim browser to the Astrum exploit kit.

Obscuring C2 communications

The banking Trojan Blockade (aka Dridex) hides its main C2 servers behind proxying layers. The proxying layers are a series of peer-to-peer (P2P) C2 servers that are specified in the banking Trojan's configuration file.

The YuppiBanker malware (aka Dreambot, Gozi, and Usrnif) generally uses a hardcoded C2 server from its configuration file as its primary C2 server; however, the banking Trojan also uses two other methods of C2 communication that can potentially obscure traffic. One method is to build C2 domains through domain generation algorithms (DGAs) on the fly by using Web content returned from a request to URLs such as hxxp://www.gnu.org/licenses/gpl.txt. The second method is to use a Tor .onion address to obscure the real IP address of the C2 server.

Despite industry efforts to prohibit deceptive internationalized domain name (IDN) registrations (that is, IDNA 2008 protocol and IEFT Standard), iDefense continues to observe malicious threat actors registering spoofed PUNYCODE domains to conduct attacks. Visually, these spoofed domains deceptively resemble the principal identity of the target domain, and the spoofed domain can be utilized in various spear-phishing or social engineering attacks. Exhibit 7-1 displays recent examples of these identified domains.

Exhibit 7-1: Recent examples of identified spoofed domains

IDNA	PUNYCODE
goȍgle[.]com	xn--gogle-e7b[.]com
paýpał[.]com	xn--papa-6ra03b[.]com
amazon[.]com	xn--amazn-p29a[.]com
fạcẹ̣book[.]com	xn--fcook-t90b60csf[.]com
github[.]com	xn--githu-5jb[.]com
apṗle[.]com	xn--aple-mg5a[.]com

In addition to cyber-crime registrations, iDefense has seen suspected cyber-espionage groups start to register domains for likely future operations; Exhibit 7-2 displays several such observed domain registrations.

Exhibit 7-2: Examples of domains registered for future operations

IDNA	PUNYCODE
amazon[.]com	xn--amazo-d8a[.]com
microsoft[.]com	xn--mirosoft-hw7c[.]com
youtube[.]com	xn--youtbe-635b[.]com
facebook[.]com	xn--faebook-wx1c[.]com

To respond to this emerging trend, iDefense has built a capability to alert clients to newly registered IDN homograph attacks targeting those organizations' domains in 48 hours or less so that those clients may proactively take countermeasures and mitigation actions against the threat.

iDefense has also observed many threat actors trending toward the use of multiple sub-domains when using C2 or infection links—a move from the previously popular dynamically generated domains, typo-squatting, and hyphenated spoofs. Analysts assess that this technique is used to create a mixture of distraction, camouflage, and disguise to elicit the intended reaction from targeted victims. This technique may exploit flaws in browsers that truncate domains of excessive length, word wrapping in system logs, and human factors of imperfect visual URL parsing and

laziness, combined with the mimicry of familiar technology names or principal identity keywords or acronyms, such as encrypt, login .com, SSL, and VPN. The following are examples of recent cyber-crime domains demonstrating this technique:

- id.system.update.cgi.icloud.aspx.webscmd.apple-id.apple.com.eu2.kmx-check1[.]com
- secure1.apple.co.jp.ssl-encrypt.menban-hachitect[.]com
- appleid.apple.com.signin-us.locale-us[.]tech
- mobile.security-paypal.com-mysupport[.]info
- paypal.com.verify-payment[.]support
- secure-apple.com.appleld-onlineservices[.]com

iDefense has also observed cyber-espionage actors using this technique, as seen in the domains below:

- mail.mail2.mod.gov.af.mail[.]al
- outlook.profile.com.hmail[.]us
- profiles.googlemembers.com.home[.]kg
- login.office365.uk[.]to
- youtube.com.now[.]im

Packaging malware and obfuscating code to avoid detection

Attackers use packaging techniques in the hopes that their malware will evade signature-based malware detection. Packaging techniques include employing commodity and commercial packers, abusing installers such as NSIS, 7Zip, and WinRAR, and deploying custom packer and encryption algorithms. With script code such as JavaScript, actors can obfuscate code to avoid detection through network-based signatures. Sometimes such concealment encompasses three to four layers of obfuscation. A recent Web injection attack used three to four layers of the Dean Edwards' JavaScript Packer to conceal the final code.

CONCLUSION

Should the D&D trend continue to gain popularity and demonstrable success for threat actors, it may potentially drive the development of "counter D&D" operations on behalf of security companies and network defenders as a countermeasure. Other reactions to adversary D&D techniques may include efforts to further advance threat detection capabilities or to reduce environmental deception opportunities and strategic D&D risk evaluation for organizations. This trend could hamper

a defender's ability to effectively detect and respond to threats as new cyber D&D tactics are created. iDefense recommends developing an understanding of threat actors' behaviors, TTPs for organizations to more accurately assess risks and respond to D&D threats.

DENIAL-AS-A-SERVICE: THE DDOS-FOR-HIRE MARKET LANDSCAPE

SUMMARY

During 2016, iDefense's Threat Analysis and Reconnaissance (TAR) unit conducted a wide-ranging analysis of the trade of Distributed Denial-of-service (DDoS) attack tools on underground criminal and notoriety-orientated hacking forums. The analysis sheds significant light on the cyber-crime actors and groups that provide a wide range of DDoS attack capabilities for hire on both clearnet and darknet websites. The paper, available in full via iDefense's IntelGraph platform, also provides a deep dive into two of the biggest DDoS-for-hire providers—vDoS and Lizard Squad's Shenron—both of which were shut down during the Fall of 2016 through the combined efforts of several global law enforcement agencies.

iDefense meticulously mapped more than 100 DDoS-for-hire providers through both manual and automated cyber intelligence collection methods, identifying two main clusters of criminal networks specializing in DDoS attacks. The first cluster consists primarily of English-speaking young adult males located primarily in Western countries who offer "stresser or "booter" Web-based DDoS tools paid for through monthly subscriptions. The second cluster centers on the Russian-speaking criminal underground community, which typically offers DDoS services that use botnets of compromised computers to generate malicious traffic. Since the release of packages known as "denial as-a-service" at the end of 2016, the first cluster of stresser/booter services has declined dramatically, due in large part to law enforcement action targeting the largest providers and the closure of the largest DDoS-for-hire marketplace on the notorious hacking community HackForums. The second cluster of Russian-language DDoS-for-hire groups remains highly active across the Russian cyber-criminal underground community.

KEY POINTS

- DDoS attacks are continuously increasing in ubiquity, duration, and potency. The rise of cloud computing, cheap hosting, available bandwidth, and open-source attack tools have made generating DDoS attacks more accessible to garden-variety hackers. With more devices continuously connected to the Internet, the available pool of potential targets has also increased. iDefense routinely identifies botnets that successfully co-opt devices ranging from smart refrigerators to industrial routers, which participate in traffic generation that can successfully overwhelm even large-scale corporate networks.
- The increase in the number of DDoS attacks has also led to various threat actors monetizing that attack vector. From low-skilled teenagers aiming to cheat while playing online games to criminal bot herders looking to supplement their incomes by renting out their botnets for opportunistic attacks, the available market for DDoS attack aids has increased explosively during the last five years. Some of these services have set up fully automated storefronts with monthly membership plans and benefits while others operate clandestinely, offering indirect, mediated access to botnets.
- iDefense research indicates that the proliferation of low-end DDoS capabilities for hire is associated primarily with Western, English-speaking, young individuals who congregate around a small number of high-trust communities. Analysis of the services offered, the traffic generated, and the backend code itself reveals a high degree of overlap indicative of direct cloning capabilities. The available attack methods include a standard mix of direct bandwidth attacks (UDP/TCP floods), HTTP-based session exhaustion, common amplification techniques (Network Time Protocol [NTP] and DNS), and gaming-specific protocols (Steam and TeamSpeak). The throughput generated, while sufficient to initially overwhelm small websites, servers, or home devices, chiefly falls in the one to 20 gigabits per second range.
- Botnets offer a wider range of capabilities than that of denial of service (DoS)-for-hire services such as booter/stressers. The meteoric increase in network-capable home-use devices is commensurate with the rise of IoT botnets, demonstrated by the Mirai botnet attacks on DNS services provider Dyn in October 2016. These botnets are relatively easy to generate and enable botnet operators to drive significantly higher throughputs of direct bandwidth without relying on proxied amplification-attack vectors. The attack capabilities themselves are often standard implementations of well-known attack vectors, as these are still sufficient to overwhelm unprepared services.

- Mitigation of DoS, DDoS, and botnet-for-hire capabilities is often straightforward, as repetitious traffic patterns eliminate the need to continuously update rule-based systems. DNS and NTP amplification attacks still exploit the same protocol features, both of which are easily filtered with no consequences to legitimate network traffic.
- Understanding the actors and communities behind the different forms of DDoS services can contribute significantly toward a better understanding of the threat landscape.

ANALYSIS

iDefense conducted an analysis of the stresser ecosystem of DDoS rental services via extensive open-source research and long-term monitoring of underground forums related to stresser development and sales. iDefense analysts also conducted analyses of stresser websites and source code to identify patterns of development and shared code bases. This research suggests that while booters and stressers are abundant, they exhibit an overwhelmingly high level of crossover in features, capabilities, and generated attack patterns between each other. As a whole, the market appears geared toward convenient replication of a small subset of abilities rather than a large, distinct spectrum of attack methods.

iDefense research concludes that while stresser services are advertised across the English-speaking cyber-criminal underground, until October 28, 2016, the core group of stresser developers and operators is primarily based around HackForums, specifically in the forum subsection "Server Stress Testing." The subsection was closed and deleted by the forum administrator who cited a need to "protect the community" following "recent events." iDefense analysts assess that the closure may be motivated by increased scrutiny of the forum by law enforcement authorities following the arrest of the operators behind the vDoS DDoS platform (those operators had openly advertised the stresser service on a subsection of the HackForums marketplace). In addition, the operators were probably inclined to close the subsection after actor Anna-Senpai released some of the Mirai DDoS botnet source code on the forum. iDefense analysis indicates that the development and expansion of the stresser ecosystem began in approximately 2011, with large spikes in the number of stresser websites registered or updated in mid-2013 and mid-2015. Stresser services appear to be primarily developed and operated by English-speaking young, adult males based either in North America or Western Europe who identify as part of the notoriety-orientated hacker community, which is based on forums and social media platforms. There is also a high degree of crossover between the online video gaming enthusiast community and actors operating or using stressers, with

booter/stresser services frequently used to target other online gamers, video gaming servers, or platforms and video game streaming services such as Twitch.tv.

iDefense also conducted an in-depth assessment of several notable botnets that provide DDoS functionality. While numerous variations of malware can support the generation of malicious DoS traffic, this analysis particularly focuses on botnets whose prime functionality was the generation of traffic and botnets to which it was clear that the operating actors were providing access as a paid service. The provided research is strategic more than tactical; it is designed to indicate trends and overall impressions with available platforms as a whole rather than provide in-depth analysis of specific variants.

iDefense analysis indicates that a vibrant DDoS-for-hire botnet ecosystem is thriving. Several notable underground forums are now routinely populated by malicious actors offering access to their botnets and providing direct contact details to facilitate such transactions. In contrast with the more-static stresser scene, botnet operators are fully willing to create a tailored experience for customers by recommending throughputs and the most appropriate attack vectors. The communities that DDoS-for-hire botnet providers inhabit are bereft of any apparent trust between their respective members, as they frequently scam each other with minimal consequences. Poor reputation management means that it is difficult to identify legitimate botnet operators. Irrespective of the volume of scamming, iDefense can confirm that several of the actors providing services are indeed legitimate, with prices for their services ranging between US$20 and US$70. The throughput is highly variable, but most available services are capable of generating traffic of 20 to 50 gbps or more, which is usually sufficient to take down an unprotected target.

ASSESSMENT/IMPLICATIONS

Because most DDoS-for-hire services share characteristics, identifying and filtering popular DDoS techniques would result in successfully mitigating a wide range of online DoS platforms. The primary caveat to this scalability is that with the increased availability of cheap bandwidth, server access, and open-source attack tools, generating ever-increasing attack throughputs becomes easier. Consequently, even properly identifying the unique traffic characteristics generated by DoS platforms may not be sufficient to successfully and reliably mitigate all attack attempts.

Arguably the most prolific and popular DDoS technique is the aforementioned DNS amplification attack. It relies on the exploitation of open, recursive resolvers responding to DNS ANY requests, with

the resolving domain often chosen for the size of its corresponding DNS response. As a result, resolving the United States government domain cpsc.gov has become a popular choice among booters, stressers, and even some botnets. With this in mind, iDefense recommends restricting the resolution of internal network DNS servers to only directly managed assets to avoid unwitting co-opting of network resources in DDoS attacks.

PLATFORMS FOR CYBER-CRIMINALITY: BRAZILIAN CYBER-CRIME COMMUNITIES

SUMMARY

iDefense analysts conducted research into the Brazilian cyber-criminal threat landscape, concentrating on the use of hacking forums as platforms for financially motivated cyber-criminality and the expansion of mobile messaging platforms and social media outlets as modern-day marketplaces. Aggregated intelligence involving collection on the clearnet, darknet, and deep Web, alongside human intelligence (HUMINT) interaction, provided iDefense analysts with comprehensive knowledge on the workings of Brazil's cyber-threat landscape. The research project assessed the indigenous nature of the country's threat landscape and the complex ideologies that underpin this unique and pervasive criminal community.

Research into the Brazilian cyber-criminal community was driven by a motivation to better understand the workings of one of the world's most active and unique domestic cyber-criminal landscapes. The Brazilian threat landscape is one that eludes many researchers who are blocked from gathering intelligence about criminal groups by language barriers and access points to those groups. Without such barriers, iDefense was able to carry out research and analysis over a three-month period; this research resulted in the following key findings:

- Brazilian mainstream clearnet hacking forums are used to freely disseminate knowledge, tools, and wares. Forum administrators have moved to eliminate the hosting of criminal trade marketplaces, with transactional dealings being channeled off-platform.
- There is widespread use of mobile messaging platforms, such as Telegram Messenger and WhatsApp, to facilitate cyber-criminality in Brazil, which heavily revolves around fraud linked to personal information and low-level financial fraud.

- There is a high volume of limited-use malicious goods and services that have low contributions to financial fraud or malicious threat activity, such as personal information fraud products, databases, and remote administration tools (RATs), being advertised across all platforms that iDefense analyzed.
- Brazilian malware being sold or shared among the Brazilian cyber-underground community are often modified versions of previously advertised malware from international marketplaces. While these have historically been relatively unsophisticated, increasing malware development and sophistication is occurring as cyber crime becomes entangled with organized crime.
- A diverse amalgam of factors has resulted in Brazilian cyber crime concentrating heavily on domestic targeting. These factors include Portuguese-language barriers, ample domestic opportunities, "Robin Hood" ideology concepts, and law enforcement challenges.

OVERVIEW

Brazil's cyber-crime community has a unique behavioral profile compared to English-language and Russian-language communities. Distinctively, the Brazilian cyber-crime community has moved away from carrying out business on popular Portuguese-language underground forums and marketplaces, opting instead to trade through mobile messaging platforms and chat channels. iDefense has observed Brazilian cyber criminals openly utilizing social media platforms such as Facebook, Twitter, and YouTube to advertise cyber-criminal tools and wares, taking advantage of overburdened domestic law enforcement agencies, modest penalties, and low conviction rates against cyber criminals. Using such tools enables Brazilian actors to gain high visibility of their advertised products with potential buyers.

Compared to most international criminal communities, the Brazilian cyber-crime community has historically concentrated on domestic targets, exploiting the boom in Internet connectivity and the spread of telecommunication devices among Brazil's population while profiting from weaker associated security infrastructure. The ability of Brazilian cyber criminals to operate in a discreet manner and evade international law enforcement interference allows cyber criminals to act with relative impunity, enabling threat actors and groups to candidly interact and conduct business on a variety of platforms.

The Brazilian cyber-crime landscape is vast and complex, with communities organized around social media, hacking forums, and mobile messaging applications channels. The Brazilian underground community boasts several clearnet technical hacking forums that operate as focal

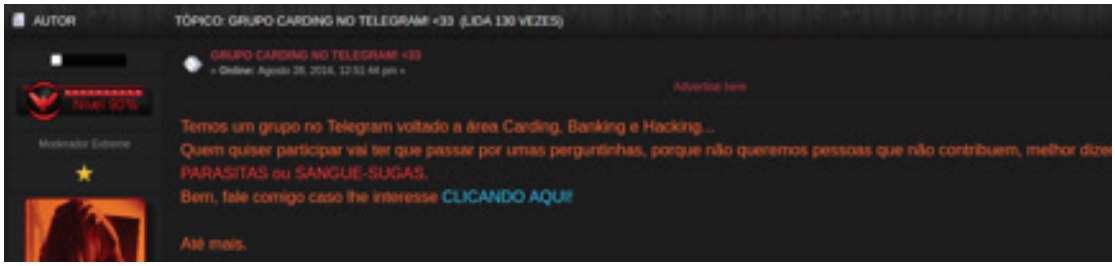
points for both entry and experienced cyber criminals alike. While these forums prohibit the trading of goods or services on forum boards—a concept that is relatively unique to the Brazilian scene—the forums support widespread cyber-criminality in two distinct ways.

First, users facilitate the high-volume of low-skilled cyber criminals who are active within Brazil by sharing tutorials and basic hacking tools for forum users to exploit. This zero-cost approach encourages would-be criminals to enter this line of criminality, enabling novice actors to develop their skills and techniques to a point at which they can begin to financially profit from cyber criminal acts. Examples of malicious tools and wares that iDefense identified on these forums can be seen below:

- Zemra Botnet 2012
- Neutrino v3.9.4
- Diamond fox botnet 4.2.0650
- K.I.N.S 2.0.0.0 Botnet
- Black MorM v4.1
- Dark-wOrm v.0.3.6
- Qi-w0rm v0.1.2
- kBot v.2.0
- Juniper Trojan 3.7
- Trojan Sub 7 0.10
- Predat0r Logger 15.0
- AUX LOGGER V3.0.0.0
- DarkCometRAT 5.3
- Babylon RAT 1.6
- Black Stealer v3.1
- Darkddoser v5.6c

Secondly, forums act as go-between spaces for vendors who capitalize on the vast reach of the platforms, directing users to more-business-friendly environments in which to conduct sales. Cyber criminals use forum spaces to direct potential buyers to external conversations on social media or mobile messaging application groups, or where they can take advantage of encrypted-messaging protocols for added security. Exhibit 9-1 is a screenshot illustrating the use of a popular Brazilian hacking forum to advertise an alleged criminal Brazilian Telegram Messenger channel.

Exhibit 9-1: Screenshot of popular Brazilian hacking forum to advertise an alleged criminal Brazilian Telegram Messenger channel



iDefense research indicates that Telegram Messenger is the current mobile messaging platform of preference for Brazilian cyber criminals. iDefense analysts gained access to more than a dozen Telegram Messenger criminal communities, each with participant numbers fluctuating between 100 to more than 30,000 members. Fraud linked to personal information and low-level tools and wares control most of the market space, with researchers identifying only limited instances of malware or high-level tools and wares. Notable distinctions in the quality and quantity of products being distributed and advertised on channels often directly correlate to the barriers to entry for that group.

iDefense research identified a trend in the modification of international malware being made available to online Brazilian communities. These tools and wares often originate from international criminal forums where threat actors can buy products from Russian- or English-language sellers and modify them to suit their domestic market. According to iDefense internal sources, experienced Brazilian cyber criminals are exploring avenues to learn Russian-language skills to open business partnership opportunities with these international actors. Furthermore, as organized crime percolates into cyber-criminality in Brazil, with small groups of developers working on behalf of criminal organizations to develop and modify sophisticated malware that is unique to the Brazilian ecosphere, the complexity and sophistication of Brazilian malware may improve, causing challenges for organizations operating in the country.

MITIGATIONS

Organizations that are established or seeking to establish a presence in Brazil should be conscious of the vast scope of the Brazilian cyber-threat landscape. The indigenous nature of the Brazilian threat greatly determines the targeting strategy for most of Brazil's cyber criminals, affecting attack surface considerations for corporations. As such, iDefense recommends that companies operating in Brazil do so with a high familiarity of the Brazilian cyber-criminal ecosystem. When deciding how best to protect a company and its assets operating in Brazil, iDefense advises consulting with an established Brazilian security operations advisory service that can offer direction on how best to protect and mitigate against domestic cyber threats.

From basic fraud linked to personal information to ATM skimming to wide-cast phishing campaigns, Brazilian cyber criminals have exhibited proficiency in exploiting domestic citizens' low levels of awareness of security practices. This element of human fallibility translates into potentially substantial risks for organizations conducting business in Brazil; people remain the weakest link. Organizations operating out

of Brazil are likely to experience some form of either opportunistic or carefully planned cyber-criminality. Companies should be prepared for intrusions, plan security measures, and create scenarios by which to operating accordingly. Additionally, companies should expect lower levels of collaboration with local Brazilian law enforcement agencies comparable to Western counterparts should a successful attack occur against a target organization. Corporations operating across all verticals are advised to engage in information security awareness training and cyber-hygiene education initiatives for all employees operating within Brazil, as the levels of familiarity with cyber threats are perceived to be lower in that country than they are in European and North American countries.

While iDefense has seen Brazilian cyber criminals making effective use of relatively dated tools found in English and Russian criminal marketplaces, challenges present themselves when actors modify these known malicious tools and wares for the Brazilian market. These challenges are further exacerbated by the developing landscape, such as the proliferation of more-advanced Brazil-targeting banking malware, the expansion of the modified ransomware market, and the continued proliferation of novice cyber-criminals in underground communities. iDefense advises that companies make use of comprehensive malware detection solutions and maintain familiarity with the products being sold and shared in the evolving threat landscape and underground communities.

PHISHING LANDSCAPE ASSESSMENT

SUMMARY

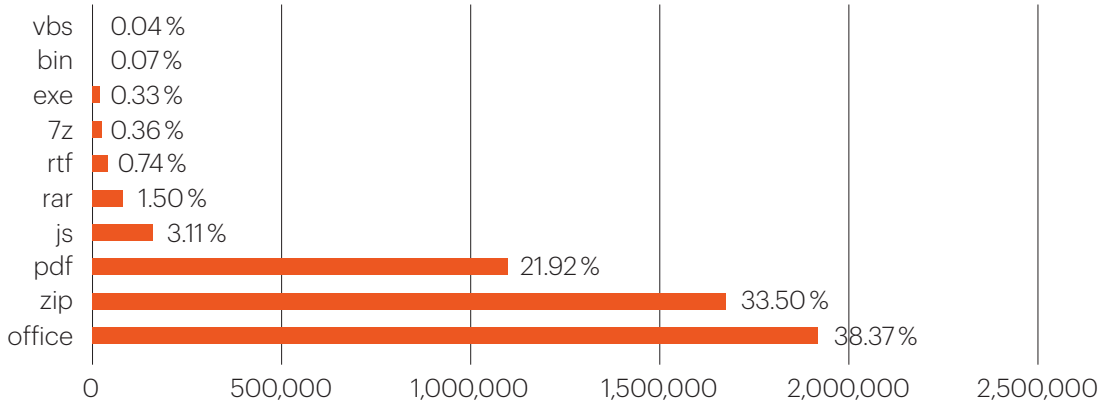
Since the beginning of 2017, iDefense's proprietary e-mail analysis system has analyzed more than eight million unique e-mails and nearly six million file attachments. Only 6 percent of these attachments were unique; many of the attachments, unique or otherwise, ultimately led to the same smaller set of final malware payloads or used some type of shared infrastructure. This insight highlights one of the key points above: threat actors are quickly breaking up their campaigns into smaller batches to avoid detection during the delivery stage. These batches are distinguished by automated and variable obfuscation methods that make it difficult to identify the campaigns underway via automated means. iDefense believes the threat actors behind the delivery of spam e-mails and the actors using the malware itself are two distinct groups, and the delivery actors offer their services based on infection or click percentages, turning larger and ongoing campaigns into more "batch"-based campaigns that are consistent with the statistics noted.

During the first half of 2017, many core phishing trends from 2016 have remained largely the same, with similar phishing lures being used and ultimate infection responsibility lying with a victim's willingness to click a link or open an attachment as opposed to malicious actors using exploits to phish for information. Significant changes appear to be in how malicious actors are delivering malware, which file types those actors are using, and which malware families these actors are dropping from use.

Users remain the biggest threat to organizations; even sophisticated and highly educated individuals remain part of the biggest potential exploit vector present in an organization. Role-appropriate user access rights and privileges, substantive security education that is tied into performance reviews, and robust and well-rehearsed backup and disaster recovery plans remain the best defense against destructive incidents such as ransomware attacks.

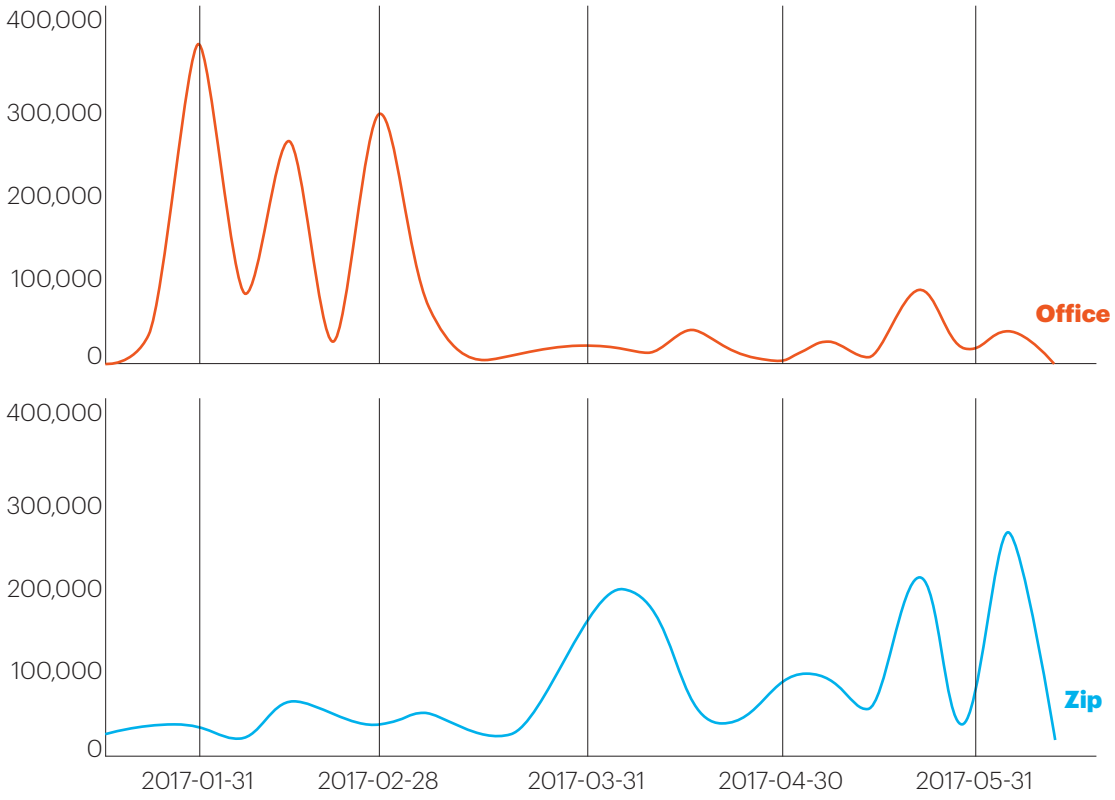
Exhibit 10-1 shows the number of direct e-mail attachments by file type since the beginning of 2017. Note the very low numbers of attachments such as VB script, JavaScript, executable, and binary attachments in relation to the high volume of Office documents and .zip file attachments.

Exhibit 10-1: Direct e-mail attachments by file type (this graph has been curated to remove file types found to be directly non-malicious such as plaintext documents and images)



As noted in Exhibit 10-1, .zip files and Office documents are the predominant e-mail attachment types among campaigns; however, iDefense also observed a trend in time between the decline of Office document attachments correlating almost directly with an increase in the number of .zip file attachments, as pictured in Exhibit 10-2, illustrating a further shift in delivery tactics. This, again, correlates directly with iDefense's findings of a change in the initial delivery tactics from using direct malicious attachments to more-obfuscated methods.

Exhibit 10-2: Graph showing iDefense-observed trend in decline of Office document attachments and Increase in .zip file attachments. Files per week, sum of submission count.



KEY POINTS

- Common phishing lures have historically remained prevalent within cyber-crime campaigns across all observed languages; these include subject lines mentioning the following:
  - Invoices
  - Shipping notifications (DHL, FedEx, UPS, and USPS)
  - Resumes
  - ACH and wire transfers
  - Missed payments
  - Lures directly associated to targets' lines of business to carry out vertical-specific targeting.
- Today, ransomware is one of the most commonly distributed types of malware, while in previous years banking Trojans formed the primary malware type seen delivered through phishing campaigns.

- Threat actors are leveraging more thorough obfuscation techniques than before, likely in reaction to increased phishing awareness by users and detection products. iDefense observed a significant drop in the number of unprotected Microsoft Office documents or JavaScript e-mail attachments that correlate in time directly to an increased number of .zip or otherwise compressed file attachments containing such documents for obfuscation purposes.
- Campaigns for a given malware family typically last one to four weeks using a given lure style, set of sender e-mail addresses, and file attachments before changing to different parameters. The changes in file attachments, lures, and senders do not correlate to changes in malware or shared infrastructure though; this is likely a method to avoid detection by blacklists, anti-virus software, and mail protection products.
- People simultaneously remain every organization's greatest asset and greatest vulnerability. Security awareness training throughout organizations is still strongly needed to help employees avoid falling victim to phishing campaigns and the infections that result from them. In addition, organizations should implement robust IT controls and procedures to mitigate the impact of incidents when they do occur.

BACKGROUND

Geography, verticals, and languages used were diverse in the phishing campaigns that iDefense studied. The most common regions targeted were Western Europe and North America; the Middle East and North Africa (MENA) region was targeted less frequently. These campaigns primarily used English, though iDefense observed phishing campaigns in other languages such as German, Norwegian, Italian, and French. Targeted verticals in cyber-crime phishing have remained largely consistent since 2016, with threat actors following money and continuing to target organizations and users with access to financial information or services. Financial services institutions remain popular targets, with iDefense having observed specific targeting of high-net-worth (HNW) and ultra-high-net-worth (UHNW) institutions (for instance, the private bank of a large international bank as opposed to the entire organization). iDefense also noticed the targeting of energy and extractive organizations (both commercial and governmental entities) and of some regional and municipal government organizations. In many instances, the targeting of government e-mail addresses may not be the act of direct targeting or spear-phishing, as iDefense observed those addresses in the context of larger cyber-crime phishing campaigns that often targeted thousands of users across both organizational verticals and regions.

In terms of malware deployed, while there was some diversity in malware families used, in general all malware delivered by phishing campaigns can be broken down into the general categories of Trojans, remote access Trojans, and ransomware. Specific malware families that iDefense observed include the following:

TROJANS	RANSOMWARE	REMOTE ACCESS TROJANS:
Emotet	Cerber	Adwind
Kovter	CryptOlocker	jRAT
Loki Bot	Cryptomix Mole	Luminosity
Panda Banker	Jaff	
TrickBot (a descendent of the Dyre/Dyreza malware family)	Mordor	
Ursnif (tracked by iDefense under the malware family name "YuppiBanker")	Sage	
	Troldesh	

The use of Locky, which had been very popular in 2016, significantly dropped in 2017, though it should be noted that iDefense observed a single Locky Osiris campaign in February 2017. WannaCry does not make the list in terms of phishing, as iDefense has not verified any instance of this ransomware being delivered via an e-mail vector.

Phishing lures remained fairly consistent in the first half of 2017 compared to 2016. Lure themes tend to revolve around actors' perceptions of what their victims would be compelled to open, such as the following:

- Failed delivery notifications (from UPS, USPS, DHL, FedEx, etc.)
- Parking or other violation notices
- Invoices
- Purchase orders
- Money transfers (MoneyGram, Western Union, etc.)
- Topical themes such as fake HM Revenue and Customs, or IRS notifications
- Phishing lures crafted to appear to be part of a victim's legitimate infrastructure

One emerging theme that is different from iDefense observations in 2016 is the more-regular use of Office 365-themed phishing pages, which may be the result of organizations pushing to move from legacy systems to this current iteration of Office. Most phishing lures remain as poorly crafted as ever: e-mails are badly written in the target language, formatting is mediocre at best, and links are almost never something that would appear legitimate to most users. However, iDefense researchers did note that some campaigns that targeted United States (IRS-themed) and United Kingdom (HM Revenue and Customs- and Companies House-themed) targets were exceptionally well-crafted compared with other phishing campaigns analysts observed in terms of the quality of English and formatting. The HMRC has been working hard to tackle this sophisticated phishing by gradually implementing security controls across all its e-mail domains. The government body has already managed to reduce phishing e-mails by 300 million this year through spearheading the use of DMARC (Domain-based Message Authentication, Reporting and Conformance) and it has been able to take down more than 14,000 fraudulent websites that were attempting to harvest customer data.[34] iDefense research experience indicates that the higher quality of these lures might have been due to the potentially lucrative payouts the threat actors behind them hoped to gain with these phishing e-mails; therefore, the actors crafted better-quality lures in such cases. The better phishing lures often incorporate links to logos and other graphics from legitimate organizations to help make the lures appear legitimate.

While many phishing e-mails simply deliver a malicious link, almost always to a compromised but legitimate third-party website that is merely hosting a single phishing page, other phishing e-mails deliver actual malware. The malware delivered through such e-mails is typically of the downloader type, involving an ultimate payload of a heavily obfuscated script of some type (JavaScript or Visual Basic). Lately, malicious actors have been using simple methods such as compressing a malicious downloader one or more times to bypass security restrictions by mail server and protection products. For instance, iDefense researchers observed campaigns that delivered a .zip file, which in turn contained a JavaScript file that downloaded and executed malware. Analysts also observed .zip files containing additional .zip files that then contain malware downloaders, usually as either a JavaScript or VBScript file. Documents containing malicious macros for malware download remain popular as well. A relatively recent trend has been the delivery of Adobe Acrobat documents that contain Microsoft Office files that in turn contain malicious macros that download a malicious executable payload. A common delivery method, especially for ransomware (Crypt0l0cker and Cerber in particular) has been the delivery of a Word document or Excel spreadsheet with malicious macros. The macros, when executed, invoke a PowerShell process that downloads and executes an additional

malware payload. Finally, iDefense has observed (though less frequently) malicious actors sometimes delivering executable files that have been renamed to appear to be another file type, such as an Adobe Acrobat file. For example, naming a file "invoice.pdf.exe" can result in a file that will appear as "invoice.pdf" on many Windows machines, which can at times fool a victim into thinking that they are opening a relatively innocuous file.

Tor is fairly popular for C2 communication for malware delivered via phishing e-mails.[35] While iDefense does not advise blocking individual Tor nodes, it may be beneficial to an organization to restrict access to the entire Tor service because analysts have frequently observed this service being used for malware C2 communications.

While ransomware is a common malware type used in phishing, and while there is a high-infection rate when ransomware is used, there is little evidence pointing to large ransom payouts by infected users. Due to the increase of ransomware variants and ransomware-as-a-service (RaaS), threat actors appear to be drawn to this malware type in the hopes of "get rich quick" schemes. With ransomware, bitcoin remains the most popular choice for payment, with only the most amateur threat actors demanding payment via other means such as Western Union money transfers or PayPal payments.

One final note is that so-called "inert document phishing" remains a popular phishing method for threat actors. This method involves sending a phishing e-mail containing a form (either inline text within the phishing e-mail or an attached document) that the victim is to fill out manually and then either e-mail, fax, or mail through the postal service to the threat actors. While it may seem hard to believe, this form of phishing resulted in at least one security incident at an organization in Western Europe. This drives home the point that human beings remain the biggest vulnerability in organizations—a trend that iDefense observed consistently in 2016 and for many years prior, and that may remain the biggest vulnerability in every organization for the foreseeable future.

ASSESSMENT AND IMPLICATIONS

Past performance is indicative of future results

While iDefense researchers did observe some variations on historical themes, overall phishing activity continues to exploit a vulnerability present in every organization: users themselves. Providing substantive, results-oriented security training as well as security-oriented policies (such as ensuring that users have appropriate rights and privileges

based on their roles) will go far in combatting phishing and other threats. Well-practiced backup and recovery plans and systems provide the best defense against ransomware incidents. System administrators may also want to prefix external e-mail subject lines with the string "[EXTERNAL]" as a clear indicator to end users that an e-mail with such a note is from a non-internal source and should be examined with extra scrutiny.

Prevalence of malware and emergence of malware-as-a-service will continue to lower barrier to entry for threat actors

Actors with low levels of sophistication will continue to find the barrier to entry low, as malware source code is freely available on innumerable underground communities. In addition, "affiliate-marketing" based malware-as-a-service, (MaaS) such as Satan or Spora ransomware, will continue to put professionally developed malware in the hands of those without the technical skills to otherwise deploy such malware.

"Malware assembly line" will continue to provide specialization opportunities for threat actors

iDefense has observed increased specialization in underground communities, with threat actors specializing in various parts of the malware lifecycle. Some specialize in providing botnet access while others develop malware, sell stolen credentials and personal information, or are other types of specialists. This is a trend that may continue through 2017 and beyond.

VENDOR ADVANCEMENTS MAKE VULNERABILITY EXPLOITATION MORE DIFFICULT

KEY POINTS

With Windows 10, Microsoft continued its mantra of moving beyond "hand-to-hand combat" as a means of finding and fixing individual vulnerabilities, instead they identified ways to eliminate entire classes of vulnerabilities.[36] Indeed, this trend of eliminating entire classes of vulnerabilities by introducing exploitation mitigation measures is a recent trend across various software vendors that iDefense has observed over the past five years. For instance, with Microsoft and Google's assistance, Adobe Systems Inc. has been incrementally adding new exploitation mitigation measures for Flash since 2010. Google's Chrome Web browser team has also provided users with various exploitation mitigation measures in the past few years.

SUMMARY

The year 2017 has so far turned out to be another big year for ransomware. In 2016, iDefense noticed multiple ransomware attacks. This year, iDefense witnessed what may be called the highest-profile ransomware attack ever: the WannaCry attack. The WannaCry attack inadvertently served as a case in point for the effectiveness of the mitigation and exploitation hardening measures that Microsoft added to the Windows 10 operating system.

BACKGROUND

Microsoft has been working on exploitation mitigation strategies and including them within its operating systems from a long time; while Windows 10 has the best and most complete exploitation mitigations built within it, some of the mitigation measures such as "UEFI Secure Boot" were also available in some form or other in earlier operating systems such as Windows 8. Microsoft released the "Creators Update" for Windows 10 in April 2017. This update had many new mitigation measures introduced within it that kill and mitigate exploitation attempts.[37] Other key security enhancements in Windows 10 include the following:

- Kernel Address Space Layout Randomization (kASLR)
- Kernel Data Execution Prevention (DEP)
- Virtualization-based security (VBS)
- Kernel Control Flow Guard (kCFG)
- Unified Extensible Firmware Interface (UEFI) Secure Boot
- Device Guard[38]

Windows 10 mitigation methods that prevent ETERNALROMANCE and ETERNALBLUE

VBS provided with Device Guard on Windows 10 and kCFG enhancements with "Creators Update" stop common exploitation techniques, including those used by ETERNALROMANCE and ETERNALBLUE.[39]

On systems that have Device Guard VBS enabled, writing and then executing shellcode, such as the ETERNALROMANCE backdoor in the kernel, is not possible due to policies in the hypervisor. These policies ensure that a kernel memory page is never both writable and executable at any given time.[40]

In the case of the ETERNALROMANCE exploit, the subverted function pointer leads to a security fault when invoked, making the exploit non-functional in that form. The same applies for ETERNALBLUE, which also relies on a corrupted function pointer to achieve code execution.

Exploitation mitigation strategies by other vendors

As mentioned earlier, Microsoft is not the only software vendor leading the charge of introducing exploitation mitigation features. Apple Inc. has developed its own deterrents in the recent past. Apple's biggest anti-exploit endeavor came with Mac OS X 10.11 (El Capitan): System Integrity Protection. System Integrity Protection is "a feature designed to prevent a privileged user or software running as root from modifying or tampering with certain important system files and folders, as well as every running process."[41] Likewise, Google Chrome implemented a substantial measure to prevent exploitation by creating a sandbox within Chrome that executes code inside the application instead of within the operating system.

A general rule of thumb for choosing secure hardware platforms is to choose 64-bit architectures over 32-bit architectures because a modern operating system running on a 64-bit architecture can use its larger address space as a security feature. For instance, heap partitioning is highly effective on 64-bit builds whereas on 32-bit builds, the address space limitations limit the effectiveness of this mitigation feature.

CONCLUSION

Windows 10 security mitigation features have the following goals in mind:[42]

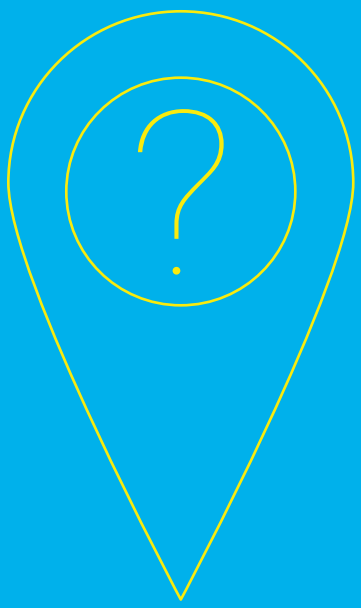
- Eliminate entire classes of vulnerabilities
- Break exploitation techniques
- Contain damage and prevent persistence
- Limit windows of opportunity in which actors can exploit vulnerabilities.

Enterprises wishing to make full use of the exploitation mitigations within Windows 10 should ensure that hardware purchases are made keeping Windows 10 hardware requirements in mind. This will enable enterprises to use the most powerful Windows 10 security features that require compatible hardware. Apart from using exploitation mitigation measures, enterprises should also work on their patching strategies to ahieve the speediest patching of vulnerable systems anytime a vendor releases patches.

THE FRONT LINE OF DEFENSE

Activity in the first half of 2017 across all categories of cyber-threat behavior—cyber-espionage, cyber crime, and hacktivism—shows that threats are growing in their destructiveness to business operations. As examples, DDoS campaigns abound and ransomware attacks have risen to the top of the threat spectrum across almost all industries. Threat actors are perfecting their ability to avoid detection; growing more diverse; and expanding their numbers thanks to factors such as the proliferation of affordable, customizable and localizable tools and bots, easy access to anonymous payment methods and encrypted communications, cheaper and faster Internet access, and the usefulness of cyber-threat activity in helping meet national strategic goals. Organizations encounter more harmful threats and are held to increasingly demanding industry cybersecurity standards, and the cost of network defense is being pushed to greater levels than ever before. Vendors have begun to assist by eliminating entire classes of vulnerabilities and incorporating exploitation mitigation

measures into their products. Cyber-threat intelligence and risk analysis are beginning to merge, in a promising trend towards the incorporation of cyber-threat defense strategies into routine business operations. And smart organizations are achieving significant return on cybersecurity investment through user training to protect proprietary and other sensitive information through safe and secure online behavior. As threats continue to evolve, organizations must do more than respond and evolve alongside them; they must plan and grow their defensive strategies faster, and smarter, than the threats themselves.



REFERENCES

[1] "Aggressive Defensiveness: Russian Information Operations against the US Political System." Jan. 7, 2017. iDefense. iDefense IntelGraph Reporting.

[2] "Upcoming European Elections Are Likely Targets for Russian Information Operations." Jan. 26, 2017. iDefense. iDefense IntelGraph Reporting.

[3] Chalfant, Morgan, "Russia tried to take over Pentagon Twitter accounts: report." May 18, 2017. TIME. http://time.com/4783932/inside-russia-social-media-war-america/ http://thehill.com/policy/cybersecurity/334045-russia-tried-to-gain-access-to-pentagon-twitter-accounts-report;
Schreckinger, Ben. "How Russia Targets the U.S. Military." June 12, 2017. POLITICO. http://www.politico.com/magazine/story/2017/06/12/how-russia-targets-the-us-military-215247.

[4] Greenberg, Andy "Russian Hackers Are Using 'Tainted' Leaks to Sow Disinformation." May 25, 2017. Wired. https://www.wired.com/2017/05/russian-hackers-using-tainted-leaks-sow-disinformation/.

[5] "Under the Wing of the Kremlin: Synergy Between Russian Intelligence Services and Criminals Multiplies Cyber-crime and Cyber-espionage Threats." June 12, 2017. iDefense. iDefense IntelGraph Reporting.

[6] "Pravyy Sector." July 19, 2016. iDefense. iDefense IntelGraph Reporting; "Possible Connections between Caucasian or Russian Actors to Bozkurtlar Bank Breaches." May 23, 2016. iDefense. iDefense IntelGraph Reporting.

[7] "US Charges FSB Officers and Russian Criminal Hackers With Breaching Yahoo and Webmail Accounts of Political and Economic Targets." March 21, 2017. iDefense. iDefense IntelGraph Reporting.

[8] Calamur, Krishnadev. "Putin Says 'Patriotic Hackers' May Have Targeted U.S. Election." June 1, 2017. The Atlantic. https://www.theatlantic.com/news/archive/2017/06/putin-russia-us-election/528825/.

[9] Galeotti, Mark. "Putin's hydra: Inside Russia's intelligence services." May 11, 2016. European Council on Foreign Relations. http://www.ecfr.eu/publications/summary/putins_hydra_inside_russias_intelligence_services.

[10] "Center for Information Security (Центр Информационной Безопасности) of the Federal Security Service of the Russian Federation." July 5, 2017. iDefense. iDefense IntelGraph Reporting;
«Мы просто ответили ФСБ за их подставы и подлянки»: Разоблачение «Шалтая Болтая»—
следствие войны между ФСБ и ГРУ
('We Were Simply Paying Back the FSB for their Frameups and Dirty Tricks':
The Unmasking of Shaltay-Boltay Is the Consequence of a War Between the FSB and the GRU)." June 18, 2017, https://medium.com/@tzurrealism/fsb-vs-gru-c82f0b93b311.

[11] Ignatius, David. "Russia's radical new strategy for information warfare." Jan. 18, 2017. The Washington Post. https://www.washingtonpost.com/blogs/post-partisan/wp/2017/01/18/russias-radical-new-strategy-for-information-warfare/.

[12] Dmitriy Chekalkin Profile Page. March 23, 2017. Facebook. https://www.facebook.com/Dmitriy.Chekalkin/posts/2011430855549824; Khamdamov, Timur. "«Инфофорум-2016»: итоги" ("Infoforum-2016: Results"). Feb. 8, 2016. GR NEWS. http://gr-news.ru/2016/02/08/infoforum-2016-itogi.

[13] Berger, J.M., Clint Watts, and Andrew A. Weisburd. "Trolling for Trump: How Russia Is Trying to Destroy Our Democracy," Nov. 9, 2016. War on the Rocks. https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/.

[14] Galeotti, Mark. "New Book: Hybrid War or Gibridnaya Voina? Getting Russia's non-linear military challenge right." November 2016. In Moscow's Shadows. https://inmoscowsshadows.wordpress.com/2016/11/28/new-report-hybrid-war-or-gibridnaya-voina-getting-russias-non-linear-military-challenge-right/.

[15] Galeotti, Mark. "Aleppo is paying for Russia's imagined global threat." Oct. 10, 2016. European Council on Foreign Relations. http://www.ecfr.eu/article/commentary_aleppo_is_paying_for_russias_imagined_global_threat.

[16] For an example, see the interview with National Guard chief Viktor Zolotov in the following article: "Glaucus Rosgvardii: ensuring social security of citizens—our main goal." June 19, 2017. Interfax. http://www.interfax.ru/interview/566808.

[17] The television channel and website formerly known as Russia Today.

[18] Higgins, Andrew. "Foot Soldiers in a Shadowy Battle Between Russia and the West." May 28, 2017. The New York Times. https://www.nytimes.com/2017/05/28/world/europe/slovakia-czech-republic-hungary-poland-russia-agitation.html?_r=0.

[19] Kovacs, Eduard. "Russian Hackers Target Montenegro as Country Joins NATO." June 7, 2017. SecurityWeek. http://www.securityweek.com/russian-hackers-target-montenegro-country-joins-nato.

[20] "SNAKEMACKEREL Possibly behind Newly Registered Fake News and Malware Download Sites." June 14, 2017. iDefense. iDefense IntelGraph Reporting.

[21] Schmitt, Michael N. "Grey Zones in the International Law of Cyberspace." Yale University. https://campuspress.yale.edu/yjil/files/2017/05/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1c52av8.pdf.

[22] "iDefense Explains: CRASHOVERRIDE (INDUSTROYER) Strategic Assessment." July 6, 2017. iDefense. iDefense IntelGraph Reporting. "Industroyer: Biggest threat to industrial control systems since Stuxnet." June 12, 2017. WeLiveSecurity. https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/; "Alert (TA17-163A): CrashOverride Malware." July 7, 2017. United States Computer Emergency Readiness Team. https://www.us-cert.gov/ncas/alerts/TA17-163A.

[23] Greenberg, Andy. "How an Entire Nation Became Russia's Test Lab for Cyberwar." June 20, 2017. Wired. https://www.wired.com/story/russian-hackers-attack-ukraine/.

[24] "Shamoon2: Second Round of Wiper Activity." Feb. 8, 2017. iDefense. iDefense IntelGraph Reporting.

[25] Sin, Steve. "Cyber Threat posed by North Korea and China to South Korea and US Forces Korea." May 2009. saber_fencer. https://www.scribd.com/document/15078953/Cyber-Threat-Posed-by-North-Korea-and-China-to-South-Korea-and-US-Forces-Korea.

[26] "Alert (TA17-164A): HIDDEN COBRA: North Korea's DDoS Botnet Infrastructure." June 13, 2017. United States Computer Emergency Readiness Team. https://www.us-cert.gov/ncas/alerts/TA17-164A.

[27] Kania, Elsa. "China's Strategic Support Force: A Force for Innovation?" Feb. 18, 2017. The Diplomat. http://thediplomat.com/2017/02/chinas-strategic-support-force-a-force-for-innovation/.

[28] "Cyber-Espionage Threat Group Table." July 9, 2017. iDefense. iDefense IntelGraph Reporting. Cyber-operations and Capabilities." July 28, 2016. iDefense. iDefense IntelGraph Reporting.

[29] "Technical Analysis of WanaCrypt0r." May 19, 2017. iDefense. iDefense IntelGraph Reporting.

[30] "Shadow Brokers Group Advertises Exploits and Cyber-espionage Tools Allegedly Obtained from Equation Group." Aug. 18, 2016. iDefense. iDefense IntelGraph Reporting.

[31] "SHADOW BROKERS Group Leaks Additional Information on Potential EQUATION GROUP Activity." Nov. 1, 2016. iDefense. iDefense IntelGraph Reporting.

[32] "SHADOW BROKERS Group Advertises EQUATIONGROUP Tools and Exploits for Individual Sale." Dec. 16, 2016. iDefense. iDefense IntelGraph Reporting.

[33] "SHADOW BROKERS Group Releases EQUATIONGROUP Windows Exploits and Tools." April 17, 2017. iDefense. iDefense IntelGraph Reporting.

[34] "Combating phishing -- a (very) big milestone." November 25, 2016. https://hmrcdigital.blog.gov.uk/2016/11/25/combatting-phishing-a-very-big-milestone/

[35] Crypt0l0cker is a prime example of such malware, with several campaigns targeting banks and governmental institutions in Italy and Western Europe in Q2 2017.

[36] "Windows 10 Mitigation Improvements." August 2016. Microsoft. https://www.blackhat.com/docs/us-16/materials/us-16-Weston-Windows-10-Mitigation-Improvements.pdf.

[37] "What's new in Windows 10, version 1703 IT pro content." May 4, 2017. Microsoft. https://docs.microsoft.com/en-us/windows/whats-new/whats-new-windows-10-version-1703.

[38] "What's New in Windows 10, Versions 1507 and 1511." May 4, 2017. Microsoft. https://technet.microsoft.com/en-us/itpro/windows/whats-new/whats-new-windows-10-version-1507-and-1511.

[39] "Analysis of the shadow brokers release and mitigation with Windows 10 virtualization-based security." June 16, 2017. Microsoft. https://blogs.technet.microsoft.com/mmpc/2017/06/16/analysis-of-the-shadow-brokers-release-and-mitigation-with-windows-10-virtualization-based-security/.

[40] Ibid.

[41] Long, Joshua. "The Evolution of Mac OS X Security and Privacy Features." Feb. 17, 2016. Intego. https://www.intego.com/mac-security-blog/mac-os-x-security-features-timeline/.

[42] "Mitigate threats by using Windows 10 security features." April 5, 2017. Microsoft. https://docs.microsoft.com/en-us/windows/threat-protection/overview-of-threat-mitigations-in-windows.

CONTACTS

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

Justin Harvey
Managing Director, Accenture Security
Incident Response & Threat Hunting
justin.harvey@accenture.com

Rick Hemsley
Managing Director, Accenture Security
rick.hemsley@accenture.com

Uwe Kissmann
Managing Director, Accenture Security
uwe.kissmann@accenture.com

Gareth Russell
Managing Director, Accenture Security
gareth.russell@accenture.com

Visit us at http://www.accenture.com/security

Follow us @AccentureSecure

Connect with us

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 411,000 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.

Copyright © 2017 Accenture
All rights reserved.

Accenture, its logo, and
High Performance Delivered
are trademarks of Accenture.

This document is intended for general informational purposes only and does not take into account the reader's specific circumstances, and may not reflect the most current developments. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.