FLASHPOINT

BUSINESS RISK INTELLIGENCE
DECISION REPORT

2017 MID-YEAR UPDATE

FLASHPOINT

BUSINESS RISK INTELLIGENCE DECISION REPORT

2017 MID-YEAR UPDATE

INTRODUCTION

Risk management remains crucial for large commercial and government organizations. This midyear update to Flashpoint's Business Risk Intelligence (BRI) Decision Report reinforces this notion by demonstrating the significant extent to which threat actors', nation state actors', and even jihadi actors' activities, tactics, and motivations have changed in a span of six months. In response, organizations seeking to assess emerging threats, vulnerabilities, and potential impacts accurately and while accounting for existing mitigations need to maintain an ongoing and strategic view of risk.

The decision report also underpins the necessity for organizations to move beyond traditional threat intelligence and tactical digital risk management to instead incorporate Business Risk Intelligence (BRI) into their security and risk strategies. Indeed, BRI produced from the same combination of proprietary technology and Deep & Dark Web data on which our intelligence subject matter experts and customers alike have come to rely enabled us to design this report specifically in support of risk-based decision-making.
Business Risk Intelligence has become especially important given the numerous notable shifts in the cyber and geopolitical threat environments that have occurred during the last six months, some of which include: the continued influence operation attempts emanating out of Russia; the dormancy and then re-emergency of The Shadow Brokers (TSB), most notably with their release of stolen National Security Agency (NSA) exploits utilized in major attacks; the continued drop in Chinese APT activity against the west; tensions in the Korean peninsula and how this impacts both the cyber and physical security landscape; and the continued lack of coordination and sophistication of jihadi cyber groups.

Understanding the geopolitical landscape allows organizations to effectively apply BRI to bolster cybersecurity, confront fraud, detect insider threats, enhance physical security, assess M&A opportunities, and address third-party risk. Organizations with robust BRI programs continue to successfully gain an increased understanding of the impact, relevancy, and corresponding business risks from malicious insiders, hacktivist groups, nation state and cyber threat actors, and radical jihadists.

This report, much like its previous iteration, will help senior-level decision makers and analysts in risk, fraud, physical security, and threat intelligence put potential threats in the context of the current geopolitical and cyber threat climate.

MEASURING THREATS

FLASHPOINT CAPABILITY SCALE

Tier 1	The cyber actor(s) possess extremely limited technical capabilities and largely make use of publicly-available attack tools and malware. Sensitive data supposedly leaked by the attackers are often linked back to previous breaches and publicly-available data.
Tier 2	Attackers can develop rudimentary tools and scripts to achieve desired ends in combination with the use of publicly-available resources. They may make use of known vulnerabilities and exploits.
Tier 3	Actors maintain a moderate degree of technical sophistication and can carry out moderately-damaging attacks on target systems using a combination of custom and publicly-available resources. They may be capable of authoring rudimentary custom malware.
Tier 4	Attackers are part of a larger and well-resourced syndicate with a moderate-to-high level of technical sophistication. The actors are capable of writing custom tools and malware and can conduct targeted reconnaissance and staging prior to conducting attack campaigns. Tier 4 attackers and above will attempt to make use of publicly-available tools prior to deploying more sophisticated and valuable toolkits.
Tier 5	Actors are part of a larger and well-resourced organization with high levels of technical capabilities such as those exhibited by Tier 4 actor sets. In addition, Tier 5 actors have the capability of introducing vulnerabilities in target products and systems, or the supply chain, to facilitate subsequent exploitation.
Tier 6	Nation-state supported actors possessing the highest levels of technical sophistication reserved for only a select set of countries. The actors can engage in full-spectrum operations, utilizing the full breadth of capabilities available in cyber operations in concert with other elements of state power, including conventional military force and foreign intelligence services with global reach.

[1]This scale is borrowed heavily and adapted from the U.S. Department of Defense Science Board's "Resilient Military Systems" report. The full report can be found at http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.

FLASHPOINT POTENTIAL IMPACT SCALE

Negligible	Damages from these attacks are highly unlikely or are unable to adversely affect the targeted systems and infrastructure. Such incidents may result in minor reputational damage. Sensitive systems and data remain intact, confidential, and available.
Low	Attacks have the capacity to disrupt some non-critical business functions, and the impact is likely intermittent and non-uniform across the user-base. User data and sensitive information remain protected.
Moderate	Attacks have the potential to disrupt some core business functions, although the impact may be intermittent and non-uniform across the user-base. Critical assets and infrastructure remain functional, even if they suffer from moderate disruption. Some non-sensitive data may be exposed. Actors at this level might also expose sensitive data.
Severe	Cyber attacks emanating from this actor set have the capacity to disrupt regular business operations and governmental functions severely. Such incidents may result in the temporary outage of critical services and the compromise of sensitive data.
Catastrophic	Kinetic and cyber attacks conducted by the threat actor(s) have the potential to cause complete paralysis and/or destruction of critical systems and infrastructure. Such attacks have the capacity to result in significant destruction of property and/or loss of life. Under such circumstances, regular business operations and/or government functions cease and data confidentiality, integrity, and availability are completely compromised for extended periods.

THREAT MATRIX

	VERTICALS									RISK RANKINGS	
Threat Actors	*Financial Services*	*Retail*	*Legal*	*Energy*	*Healthcare*	*Tech / Entertainment*	*Telecom*	*Gov't / Military*	*NGO's / Civil Society*	*Capability*	*Potential Impact*
China	×		×	×	×	×	×	×	×	Tier 6	Catastrophic
Five Eyes*	×			×		×	×	×		Tier 6	Catastrophic
Iran	×			×			×	×	×	Tier 4	Moderate/Severe
North Korea	×			×		×	×	×		Tier 4**	Severe
Russia	×		×	×		×	×	×	×	Tier 6	Catastrophic
Disruptive/Attention-Seeking Actors						×		×		Tier 3	Moderate
Cybercriminals	×	×	×	×	×	×	×			Tier 4	Severe
Hacktivists	×	×		×		×	×	×	×	Tier 3	Moderate
Jihadi Hackers	×					×		×		Tier 2	Negligible

* Non-threat nation-states of the U.S. and its allies represent the high-water mark for top-tier nation-state cyber capabilities. Risk assessments should measure adversarial nation-states against these top-tier actors when estimating cyber capability.
** Although assessed as a Tier 4 actor, North Korea is a unique case, as the state is able to marshal state resources as necessary, which may enable capabilities that are generally ascribed to higher tier actors. North Korea in particular is likely capable of using destructive and highly disruptive attacks in kinetic conflict scenarios to support military objectives — a key differentiator of Tier 6 actors.

2017 MID-YEAR FLASHPOINTS

In our inaugural Business Risk Intelligence Decision Report released in January 2017, we highlighted various bellwethers for the upcoming year that may prove to prompt shifts in the cyber threat environment. These “Flashpoints” were not intended to be near-term predictions, but instead to serve as potential events to monitor given the global geopolitical environment. We have amended our original bellwethers to account for events that have occurred since the beginning of the year.

- Tensions in East Asia over the North Korean conundrum boil over into more direct and heated conflict between North and South Korea, the United States, and potentially China. A potential trigger for such an incident may be the conducting of North Korea’s sixth nuclear test, about which there is widespread speculation that the country is nearly prepared.

- The Trump administration adopts a less-compromising approach towards U.S.-China relations or otherwise enacts policies that threaten Chinese “core interests.” Alternatively, China adopts an increasingly aggressive policy towards securing its vital “core interests,” including the South China Sea and the questions of Taiwan’s and Hong Kong’s political sovereignty.

- Official U.S. policy changes dismantle or otherwise substantially revise the terms of the Joint Comprehensive Plan of Action, otherwise known as the Iranian nuclear accord.

- U.S.- and European Union-led economic sanctions in place on Russia are extended or tightened, further harming the already-fragile Russian economy.

- Russia is found to have interfered in additional European elections, including the upcoming German federal election in September 2017.

- The situation in Syria deteriorates further into armed conflict between major states with differing interests in the region.

- The capitulation of key ISIS strongholds fragments the Islamist political movement

- Other nation-states, such as China, Iran, and North Korea adopt the Russian model of engaging in “cyber influence operations” via proxies, resulting in the exposure of such a campaign.

FLASHPOINT

2017 MID-YEAR TRENDS & INDICATORS

RUSSIA

Russia, one of a handful of the U.S.'s peer competitors in cyberspace, remained highly active during the first half of 2017. For the most part, malicious cyber activity emanating out of Russia has been linked to Moscow's efforts to influence various elections in Western European countries, not the least of which include France and Germany, through compromising political opposition groups and engaging in disinformation campaigns. This behavior is reminiscent of the campaign against the U.S. Democratic National Committee and the Hillary Clinton campaign at the end of 2016—over which the U.S. government is still debating an appropriate response.

Russia's attempts at election interference in 2017 appear to have begun in earnest in January, when it was revealed that the German parliament fended off spear-phishing attacks on at least ten different German politicians across the political spectrum. This was not the first time that the German parliament was targeted by Russian actors—the first known instance occurred in May 2015 and was linked to APT28. Germany's national elections are scheduled for September 24, 2017. In early May, German officials renewed warnings over the potential for increased cyber activity, including direct targeting and disinformation campaigns emanating out of Russian leading up to the elections. Additionally, in early May on the eve of the French presidential elections, a data dump consisting of then presidential candidate Emmanuel Macron's emails was released, with initial analysis again implicating APT28. In the days following the incident, U.S. intelligence officials stated they had been passively observing the Russian actors prior to the attack on the Macron campaign and had alerted French officials before the incident became public knowledge.

Aside from attempts to influence high-profile elections, in April the UK Foreign Office stated that several civil servants were targeted by a spear-phishing campaign with direct links to the group that perpetrated the attack on the U.S. Democratic National Committee in 2016. Likewise, Denmark subsequently accused APT28 of carrying out attacks on the Danish Defense and Foreign Ministries in 2015 and 2016.

Moreover, and while there is no concrete evidence linking the Shadow Brokers — the group responsible for releasing data ostensibly stolen from the U.S. NSA beginning in late 2016 — to Russia, there remains widespread speculation that the group is an extension of Russia's influence operations against the United States.

Domestically, Moscow has continued its crackdown on digital dissent since the start of the year. New regulations require so-called "organizers of information distribution on the internet" — a term which is likely intentionally left vague and broad so as to apply to as many services as possible — to retain logs of all data flowing to and from its servers for a period of six months beginning on July 1, 2018. The regulations also require metadata to be stored for one year for websites and three years for all other services falling under this designation. These logs are very likely to be utilized by Russian law enforcement and the domestic security apparatus to crack down on individuals and organizations critical of the regime. Moreover, in spring 2017 Moscow moved to ban popular chat applications for alleged non-compliance with new regulations, including China's popular mobile chat app WeChat, Blackberry Messenger, Imo, and LINE.

In another unusual saga, Moscow recently arrested several high-profile cybersecurity investigators and intelligence officials, including Ruslan Stoyanov, Sergey Mikhailov, and Dmitry Dokuchaev on treason charges, although their actual offenses have yet to be released publicly. Stoyanov in particular made the news after the release of letters he dictated from prison. In the letters, he warns the regime of the consequences of partnering with domestic "patriot-thieves" (cybercriminals)—allegations which may bolster claims often made by Western nations of Russia's tacit acceptance, if not outright support for cybercriminal gangs within its borders. Taken together, the new regulations, the crackdown on popular online services, and the arrest of prominent cybersecurity personalities suggest that Moscow is moving quickly towards establishing an unprecedented level of information control within the country's borders, further segmenting the Russian populace from the broader global Internet and cementing the state's authority over online activities.

CHINA

While China remains a highly capable actor in cyberspace and a demonstrated threat to Western and East Asian entities, Chinese state-sponsored actors have continued their relative quiescence during the first half of 2017. In our previous report, we noted that Chinese state-sponsored cyber espionage activity had decreased over the course of 2016 likely due to a confluence of factors, not the least of which include the Xi-Obama agreement made in September 2015 to refrain from industrial espionage, the ongoing military reforms within China that have likely disrupted day-to-day operations, and/or the improvements in operations security on the part of Chinese cyber actors.

Nevertheless, in the first half of 2017 several organizations linked China to a handful of attacks against Western and East Asian targets. In particular, in early March the U.S. Department of Homeland Security released a report detailing recent activity under the "Pleasantly Surprised" campaign, which involved spear-phishing attempts against commercial entities in the financial, retail, and technology sectors. In at least one other case, the suspected Chinese Advanced Persistent Threat (APT) group APT10 was linked to a campaign targeting the U.S.-based National Foreign Trade Council (NFTC) at time that coincided with Chinese President Xi Jinping's and U.S. President Donald Trump's summit in the United States in early April. Around that same time period, a joint report between PricewaterhouseCoopers and BAE Systems detailed APT10 activity against unnamed international Managed Service Providers and a host of Japanese entities. Finally, in early May FireEye reported that its researchers had observed Chinese threat actors attempting to compromise an organization associated with the deployment of the Terminal High Altitude Area Defense (THAAD) anti-ballistic missile system in South Korea. In its totality, suspected Chinese state-sponsored cyber activity in the first half of 2017 suggests that China remains a potent force both technically-capable and intent on compromising foreign targets in support of its national objectives. However, it is worth noting that the overall volume of such attacks appears to have dropped precipitously since its zenith; and targeting has pivoted substantially towards entities and governments in East Asia and China's geographic neighborhood in particular.

Internally, China has been swiftly moving ahead with the drafting and implementation of new regulations governing the behavior of specific industries in cyberspace, as well as continuing to cement its control over the use of online services. In the first months of 2017, Beijing rolled out new regulations governing the use and deployment of internet-enabled medical devices, published a white paper on China's strategy for international cooperation in cyberspace, and published new regulations on the operating of Virtual Private Networks and "unauthorized internet services" as well as on data flows bound for servers outside of mainland China. The rapidity with which Beijing has rolled out these new regulations and policies is highly-tied to the implementation of the National Cybersecurity Law on June 1, 2017. The bill, which has considerable consequences for businesses and individuals doing business in mainland China, as well as for Chinese netizens themselves, was the subject of much controversy on the run up to its enactment, with much opposition coming from Western firms operating in China who argued that the bill was overly vague and did not provide the requisite specifics to enable compliance with the new regulations. Nevertheless, Beijing moved ahead with the implementation of the law, although reportedly delayed enforcement on at least one suite of provisions governing cross-border data flows until December 31, 2018.

On the Deep & Dark Web as well as the open web, China continues to crack down on illicit activity and online anonymity. In efforts to reduce the anonymity with which Chinese internet users can evade law enforcement and monitoring, Baidu itself announced in early May that it would be implementing the real-name verification system across each and every one of its services starting on June 1.

FIVE EYES

U,K., U.S., CANADA, AUSTRALIA, NEW ZEALAND

While the “Five Eyes” countries together represent the pinnacle of cyber capabilities of all actors in cyberspace, they do not carry out highly-disruptive or destructive attacks against allied or Western systems, especially during peacetime. As such, the Five Eyes are unlikely to be considered threat actors for Western organizations and individuals. Nevertheless, their broad reach, unparalleled levels of technical sophistication, and high levels of coordination make them formidable adversaries for those who are targeted for either the purposes of intelligence collection, disruption, or destruction during wartime.

As was noted in our previous report, the American intelligence community in 2016 suffered from a series of damaging leaks by a mysterious online group dubbed the “Shadow Brokers.” This trend has continued into 2017, with the Shadow Brokers releasing additional alleged U.S. National Security Agency (NSA) data. Despite “going dark” in mid-January with the release of the so-called “EquationDrug” files, the Shadow Brokers once again emerged in early April to release the encryption key for the original batch of Equation Group data that it had attempted, unsuccessfully, to auction off in August 2016. Only a few days later, the Shadow Brokers emerged again to release the so-called “Lost in Translation” dump, detailing SWIFT and Windows OS-based exploits and payloads allegedly stolen from the NSA. Included in this release was evidence pointing to an ostensible NSA-backed campaign targeting financial institutions, particularly those located in the Middle East. In early May, unknown attackers leveraged the so-called “EternalBlue” exploit, discovered by the NSA and subsequently leaked, in a global ransomware worm campaign dubbed “WannaCry.” The Shadow Brokers once again made headlines in mid-May following the group’s announcement of a new subscription-based service for access to stolen data.

Around the same time period as the Shadow Brokers’s resurgence, Wikileaks released the “Year Zero” dump as part of a larger campaign dubbed “Vault 7.” This release comprised some 8,761 documents dated from 2013 to 2016 that reportedly come from a hacking arsenal maintained by the U.S. Central Intelligence Agency (CIA). According to WikiLeaks, the arsenal includes "malware, viruses, trojans, weaponized ‘zero day' exploits, malware remote control systems and associated documentation.” Despite the synchronicity between the Shadow Brokers releases and the Wikileaks dump, there is no known connection between the two.

“[The Five Eyes's] broad reach, unparalleled levels of technical sophistication, and high levels of coordination make them formidable adversaries.”

IRAN

Iran continues to be a moderately-capable threat actor in cyberspace that is believed to have invested much in cyber weapons as a means both of countering the U.S.'s conventional military clout and of projecting power regionally. Iran also boasts a relatively robust cadre of researchers and technology enthusiasts known to comprise various well-known hacking groups, such as the Ashiyane Digital Security Team and OffSec. One notable aspect of Iran's cyber strategy is the overwhelming focus on exploiting vulnerabilities in critical infrastructure systems, largely due to such targeting's ability to cause widespread damage and disruption even for more classically-powerful adversaries, such as the U.S.

However, Iran and Iranian activities in cyberspace have largely fallen off of headlines in the West thus far in 2017, despite the February imposition of new sanctions against Iranian companies and individuals associated with the country's ballistic missile program. During the U.S. presidential campaign season, then presidential candidate Donald Trump referred to the Joint Comprehensive Plan of Action (JCPOA), otherwise known as the Iranian nuclear accord, as a "bad deal," suggesting that his administration would adopt a new track on U.S.-Iranian relations. Given the Iranian interest in preserving the JCPOA (and its accompanying sanctions relief), Flashpoint believes any substantive revisions to or reneging of the agreement on the side of the U.S. are likely to be accompanied by renewed Iranian efforts in the cyber domain.

> *"One notable aspect of Iran's cyber strategy is the overwhelming focus on exploiting vulnerabilities in critical infrastructure systems"*

Iranian cyber actors have likewise been relatively quiescent throughout the first half of 2017, with some notable exceptions. In early February, the Iran Threats Team detailed a new malware sample linked to Iranian actors dubbed "MacDownloader" that was being used against the defense industrial base and a human rights advocate. The malware poses as installers for Adobe Flash or Bitdefender Adware Removal Tool, and once successfully implanted, attempts to extract system information and copies of Apple OS X keychain databases. Additionally, OilRig, a suspected Iranian cyber espionage group believed to have been in existence since 2015, again surfaced in early 2017. Having been linked to a number of incidents primarily affecting entities in the Middle East in countries such as Saudi Arabia, the United Arab Emirates, Qatar, Kuwait, Lebanon, Turkey, and Israel. In at least one campaign, OilRig was found to have compromised the code-signing certificate issued by Symantec to Vermont-based technology firm AI Squared, which was then used to sign the group's malware.

Flashpoint assesses with a moderate level of confidence that the May 19 re-election of Iranian President Hassan Rouhani is likely to have a stabilizing effect on Iranian cyber activities, whereas the election of a more conservative candidate would likely have intensified cyber campaigns emanating from the country as the new leader attempts to demonstrate their strength on security issues.

NORTH KOREA

Despite its reputation for opacity and its isolation from the international community, North Korea is widely believed to remain a potent threat in cyberspace. In the past, the reclusive country has proven its capability to strike foreign targets both in the United States and South Korea in particular with significant effect. Pyongyang's capabilities in cyberspace are believed to be heavily contingent on Chinese infrastructural and, at a minimum, tacit political, support from Beijing. The latter appears to have waned somewhat in the first half of 2017, as tensions on the Korean peninsula increased and China implemented import bans on North Korean goods while running highly -unusual editorials critical of Pyongyang in well-known state-run periodicals.

Nevertheless, and in the midst of heightened tensions in the region, Pyongyang appears to have been for the most part quiet in cyberspace thus far in 2017, with at least two exceptions affecting neighboring South Korea. In January, South Korean media reported on a series of phishing emails ostensibly sent by North Korean threat actors to South Korean organizations focused on North Korea research and policy, as well as human rights issues, using clever lures that would likely be of interest to the victims. Again in late March, phishing emails were disseminated to North Korean defectors and organizations whose main missions revolve around the cause of human rights in North Korea; the attackers feigned affiliation with the "South Korean Public Relations Department." Perhaps another exception to this rule is the emergence and spread of the WannaCry ransomware in May. Many researchers have linked the WannaCry malware to the "Lazarus Group," which is itself believed to be affiliated with North Korea. Flashpoint's own analysis of the 28 odd foreign language ransom notes, however, strongly suggests a Chinese-speaking author of the notes themselves. These two findings—the link to North Korea and a Chinese-speaking author of the ransom notes—are not mutually exclusive, however.

Considerable uncertainty lingers over the potential resolution of the North Korean problem. The Trump administration has adopted a much less-compromising approach to the North's nuclear program, even going so far as to state that the "era of strategic patience is over," although the exact consequences of this policy shift are far more ambiguous. As long as tensions continue to run hot in the region, the likelihood for North Korean-backed cyber activity remains high. In this same vein, in April, United States Department of Homeland Security Secretary John Kelly warned that North Korea is more likely to conduct a cyber campaign against the United States than it is a kinetic military strike. The North's current apparent quiescence in cyberspace may come to a swift end in the event that the United States reacts strongly to the country's sixth nuclear test, for which many analysts believe that Pyongyang is preparing.

DISRUPTIVE & ATTENTION-SEEKING ACTORS

Although 2016 was marked by a relatively high level of activity from disruptive and attention-seeking actors, as was the case with the Crackas with Attitude (CWA), the opposite has been the case for the most part in 2017.

One potential cause for this decrease in effectiveness of attention-seeking actors' attacks is successful law enforcement efforts that have led to the arrest of members of key groups, such as the CWA. These arrests have likely also deterred other would-be individuals from wading into this space. Another potential explanation lies in the fact that these actors tend to thrive on media coverage. Since the start of 2017, the Western media has been dominated primarily with other items of news, such as the new U.S. administration and, since April, the FBI's investigation into Russian election interference both at home and abroad. Nevertheless, Flashpoint has observed such actors remaining active, yet to lesser effect than previously. CyberZeist is one such example of a low-skill disruptive threat actor who was active in January 2017 yet appears to have gone dark following the suspension of their Twitter account.

Moreover, as disruptive and attention-seeking actors are generally characterized as low-to-moderate skill, the decrease in apparent effectiveness may also be explained by stronger security regimes on the part of historical targets, such as gaming companies. In particular, online gaming services have recently invested significantly in DDoS mitigation services and hardened their customers' user accounts by deploying additional security mechanisms such as two-factor authentication. Increased awareness amongst police departments of SWATTING techniques used by disruptive and attention-seeking actors has also led to a decrease in successful attacks.

Internet-of-Things (IoT) botnets, such as Mirai, have also proliferated in the first half of 2017 and have at times been leveraged by disruptive and attention-seeking threat actors for attacks on various targets of interest to varying effect. Variants of Mirai have also cropped up in the wild, such as in China; and Mirai has for the most part been absorbed into the wider ecosystem of Linux-based IoT botnets.

“Increased awareness amongst police departments of SWATTING techniques used by disruptive and attention-seeking actors has also led to a decrease in successful attacks.”

CYBERCRIMINALS

Financially-motivated cybercriminals have continued to innovate in 2017. In our previous report, we highlighted the growing trend across the underground cybercriminal economy towards targeting organizations rather than their customers as a means of obtaining monetizable information and maximizing gains from their illicit activities. This trend has shown no sign of faltering thus far in 2017, with cybercriminals across the digital underground expressing their interest in targeting large organizations and/or successfully doing so. Another notable trend in 2016 was cybercriminal targeting of healthcare organizations as a means of obtaining sensitive and exploitable personally identifiable information (PII). In the first few months of 2017, Flashpoint has observed a variety of actors such as “svako,” “hackworld,” “covrig3500,” and more targeting healthcare clinics across the United States in efforts to monetize the stolen data.

Business Email Compromise in particular appears to be an area of rapid growth, with newly-released statistics finding that the various iterations of the scheme have led to some $5.3 billion dollars in losses globally in the period between October 2013 and December 2016. This figure was recently revised upwards from the previous estimate of $3.1 billion between October 2013 and June 2016—an increase of $2.2 billion in a mere 6 months. BEC is especially pernicious because it often does not require compromise of the target organization and can affect small and large organizations alike. In late April, for example, it was revealed that Google and Facebook had together been the victims of a BEC scam that netted the attackers some $100 million in illicit profits.

Overall, cybercriminals have continued to evolve in order to circumvent additional protections and new technologies designed to reduce fraud, such as EMV chips in payment cards. Underground communities remain as active as ever. Likewise, discussions of new schemes and TTPs (Tactics, Techniques, and Procedures) are still commonplace despite increased law enforcement attention and the cybersecurity industry’s growing understanding of the most prominent Deep & Dark Web communities.

Noteworthy Trends Observed in the Cybercriminal Underground During the First Half of 2017

- Efforts to circumvent or otherwise crack EMV chip technology, including via physical exploitation;
- Continued interest in SWIFT exploitation, including attempts to target three Indian financial institutions;
- Consistent discussions of and recruitment for insider trading schemes leveraging data stolen from financial institutions, news agencies, and law firms;
- The return of banking malware such as Dridex, with new User Account Control bypassing techniques;
- Growing rates of tax fraud leveraging stolen W-2 documents;
- Substantially increased monetary losses due to Business Email Compromise (BEC) schemes;
- Increasing sophistication of cybercriminal communities outside of Eastern Europe, such as the Brazilian underground;
- The emergence of the “WannaCry” ransomware worm that infected tens of thousands of systems globally in mid-May by leveraging the recently-leaked NSA exploit “EternalBlue.”

HACKTIVISTS

In the first half of 2017, hacktivism has displayed a decidedly non-Western flair. While the more prominent groups of the recent past, such as the Anonymous movement, got their start in the West, such groups have continued their relative decline while their iconography and nomenclature have often been reused by new groups formed abroad. Overall, hacktivism remains a moderate threat to targeted organizations, although the groups are increasingly international and non-Western in nature. Thus far in 2017, the hacktivist landscape has been dominated by a small subset of largely-ineffectual hacktivist operations linked to the Anonymous collective, as well as activity emanating out of Turkey and China in particular.

ANONYMOUS CAMPAIGNS

The Anonymous collective, an amorphous and tenuously-linked set of "hacker activists," has served as the face of Western hacktivism for roughly a decade. Yet in recent years, Anonymous-linked activity, at least from the Western branches of the movement, has declined considerably. For the most part, the myriad of "operations" that have been launched have fallen flat without adequate or enthusiastic support. In 2017, Flashpoint has observed a number of Anonymous-backed operations, most of which have fizzled out, including the long-running OpIsrael, OpSaudi, and OpKillingBay campaigns targeting Israel, Saudi Arabia, and Japan, respectively. Other more nascent campaigns have included OpSingleGateway in Thailand, OpOperadoras in Brazil, and OpResistance in the United States as a reaction to the election of U.S. President Donald Trump. Despite the relative diversity in campaigns, however, these efforts have borne little in the way of malicious cyber activity beyond low-level attacks such as Denial of Service, website defacement, or (likely automated) SQL injection attacks.

TURKISH ASLAN NEFERLER TIM

Far and away the most prolific hacktivist group active since the start of 2017 has been Aslan Neferler Tim (ANT), believed to be operating out of Turkey, Austria, and the United States. Since October 2016, the group has carried out a string of Distributed Denial of Service (DDoS) attacks leveraging the "Susqun" stresser against Middle Eastern, European, and American entities seemingly indiscriminately and often with little to no particular justification. While the group is nationalist in nature, it has on occasion targeted Turkish assets and individuals, likely to gain notoriety within Turkey and highlight vulnerabilities in target systems. In its international targeting, the group has attacked airports in Florida, government ministries in Greece, Russia, Austria, Belarus, and Israel, the Bank of England, Halliburton, Comcast, and many more, and often does so due to current or historical hostility between the target government and/or entity and the Turkish state and its people.

CHINESE ANTI-LOTTE CAMPAIGN

In late February and through March 2017, the relatively-dormant Chinese hacktivist community sprung back to life following a finalized agreement between the South Korean government and the Lotte Group, a large South Korean retail conglomerate. The agreement ceded a portion of a Lotte-owned golf course to the government for the deployment of the Terminal High Altitude Area Defense (THAAD) anti-ballistic missile system.

In response, the Chinese government expressed its displeasure with the deal while anti-Lotte and anti-Korean protests broke out across mainland China. At the same time, patriotic netizens, including hacktivists, began to organize boycotts of Korean-made goods, and of Lotte in particular, and quickly pivoted to calling for and organizing attacks on Lotte websites. For several weeks stretching into the month of April, Lotte was the subject of sustained Distributed Denial of Service (DDoS) and website defacement attacks from various Chinese hacktivist groups, such as the Panda Intelligence Bureau, the China Hacker Alliance, affiliates of the Honker Union of China, among others. Notably, Chinese hacktivists were observed leveraging newly-discovered CVE-2017-5638 in Apache Struts 2 in their attacks after more technically-oriented users integrated an exploit into attack tools only hours following the vulnerability's release.

JIHADI ACTORS

CYBER

Over the first half of 2017, jihadi cyber actors appear to have shown little growth in terms of accumulating the requisite technical skills in order to pose a more potent cyber threat. As was the case in 2016, the individuals comprising the limited number of jihadi-affiliated hacker groups remain low-skilled, uncoordinated, and continue to rely on attack methods such as website defacements and social media hijacking. As a result, victims continue to be targets largely of opportunity and happenstance rather than of more directed efforts. Due to the lack of technical acumen within most jihadi hacker groups, their victims tend to be poorly-defended or smaller, low-hanging-fruit websites.

In late 2016, Flashpoint observed jihadi hackers on the top-tier ISIS-affiliated Deep Web forums expressing an interest in cyber attacks, and in particular Denial of Service (DoS) attacks against "sensitive targets" such as financial institutions and social media services. Subsequently in early 2017, Flashpoint observed one actor developing his own rudimentary DoS tool which came to be known as the "Caliphate Cannon." Nevertheless, discussions surrounding the development of proprietary attack tools and in DoS attacks in particular appear to have died out in Q2 2017.

The United Cyber Caliphate (UCC) remains the most active jihadi hacker group. Despite espousing a pro-ISIS ideology, there is no evidence that UCC is directed, or supported, by ISIS main. The UCC continues its recruitment efforts within pro-ISIS communities and has called for all pro-ISIS hackers to unite under one banner, including the newly-created "Caliphate Cyber Terrorism Army (CCTA)." In the first half of 2017, UCC claimed responsibility for a string of DDoS attacks, website defacements, account takeovers, and releases of "kill lists," which Flashpoint has previously and consistently found to be drawn from open resources rather than from successful compromises. In March 2017, the group suffered a significant blow after its leader, an individual by the name of Osed Agha, was allegedly killed by a U.S. airstrike in Raqqa, Syria. Agha is believed to have been an ISIS fighter who fought within the organization's ranks in Syria. He is the third such pro-ISIS jihadi hacker to be killed by airstrikes in the recent past—the most notable among them being Junaid Hussain, or "TriCk" of TeaMp0isoN, who was widely considered the pioneer of jihadi hacking communities.

PHYSICAL

The physical threat emanating from jihadists has continued to evolve in 2017 and largely pivoted toward the West as the shift toward external operations via low-tech means has solidified. As ISIS's so-called Caliphate continues to dwindle while al-Qaida's affiliates in Yemen, Somalia, and elsewhere come under heavier bombardment from Western forces, these organizations are increasingly turning their focus outward, culminating in the overwhelming outreach to, and direction of, the "lone mujahid in the West."

This trend has been exemplified by both rhetoric and action, as jihadist organizations have not only increased their calls for supporters to launch attacks in their homelands, but they have also claimed responsibility for a slew of such operations in 2017, including the January 1 nightclub shooting in Istanbul, the March 22 London attack, the April 3 St. Petersburg metro bombing, the April 20 Paris shooting, and the May 22 Manchester Arena bombing.

This proclivity for attacks outside of traditional conflict zones presents a threat that is further compounded by the endorsement of low-tech operations that employ otherwise mundane objects such as vehicles, thereby rendering plot disruption more difficult. Al-Qaida in the Arabian Peninsula (AQAP) communicated this approach best in its April 7, 2017 issue of Inspire Guide, when it explained that the "success" of an attack "is not measured by strength of the employed weapon or by an abundance of soldiers."

> *"Jihadi-affiliated hacker groups remain low-skilled, uncoordinated, and continue to rely on attack methods such as website defacements and social media hijacking"*

FLASHPOINT

ABOUT FLASHPOINT

Flashpoint delivers Business Risk Intelligence (BRI) to empower business units and functions across organizations with a decision advantage over potential threats and adversaries. The company's sophisticated technology and human-powered analysis enable enterprises and public sector organizations globally to bolster cybersecurity, confront fraud, detect insider threats, enhance physical security, assess M&A opportunities, and address vendor risk and supply chain integrity.

For more information, visit **flashpoint-intel.com**
Follow us on Twitter at **@FlashpointIntel**.

CREDITS

Report by **Jon Condra**

Special thanks to **Rob Cook, Alex Kassirer, Vitali Kremez, Allison Nixon, Luke Rodeheffer, Roman Sannikov, Leroy Terrelonge, and Ken Wolf**.