A current and forward-looking view of the cyber threat landscape to help organizations mitigate risk and strengthen their defense postures.
# TABLE OF CONTENTS

ABOUT........................................................................................................3  
INTRODUCTION..........................................................................................4-5  
2017 CTIE RECAP......................................................................................6-7  
EXECUTIVE SUMMARY..............................................................................8-13  
ALERTS........................................................................................................14-15  
MALWARE..................................................................................................16-18  
VERTICALS.................................................................................................19-21  
TECHNOLOGIES..........................................................................................22-30  
ACTORS.......................................................................................................31-37  
DDoS COMMODIFICATION.........................................................................38-40  
CONCLUSION...............................................................................................41  
CONTRIBUTORS..........................................................................................42  
REFERENCES...............................................................................................42-43
Optiv Security is a security solutions integrator that enables clients to significantly reduce enterprise risk by taking a strategic “inside out” approach to cybersecurity. While the traditional threat centric “outside in” approach focuses first on identifying specific threats and then reacting with technology procurement, Optiv starts with core requirements of every enterprise business strategy and risk mitigation and builds outwards from there with strategy, infrastructure rationalization, operations optimization and ongoing measurement. This enables clients to build a sustainable risk centric foundation for implementing proactive and measurable security programs that are far more effective at reducing current and future risk than is possible with the reactive outside in model.
The cyber threat landscape continues to evolve. Having the latest intelligence on what security threats have occurred and where the new threats will take advantage is the first step in gaining the upper hand. Many organizations may be exploited beyond their perimeter and require a complete view of their digital footprint. These organizations may not have the resources nor specialized skills to conduct threat hunting, detecting, analysis, and response or mitigation. Organizations look to develop a tailored intelligence gathering process that results in actionable information to use as an immediate response to improve their security posture.

The 2018 Cyber Threat Intelligence Estimate is based on security digital footprint assessments conducted by Optiv’s Global Threat Intelligence Center (gTIC) in 2017 with three key contributing sets of data: 1) Basic Intelligence 2) Current Intelligence 3) Estimative Intelligence. Optiv’s Cyber Threat Intelligence Estimate (CTIE) triangulates and validates the information using Optiv’s proprietary advanced threat intelligence and data from our client base. The analysis uses the three areas of data from over 7,000 tickets to project the estimate through 2018. It is designed to be a forward-looking view reflecting the cyber threat landscape to help organizations mitigate risk and strengthen their defense postures.

**Basic Intelligence:**
Threats to specific types of organizations by vertical or industry

**Current Intelligence:**
Threats that focus on a specific technology vulnerability

**Estimative Intelligence:**
Threats by a specific actor or actors.
BASIC INTELLIGENCE

Some threats focus on certain types of organizations. For instance, there are campaigns against financial institutions that spread banking-focused malware. An organization should be aware of the threat activity in their particular business vertical because it can prepare them for similar exploits.

CURRENT INTELLIGENCE

Threat actors are not always interested in every technology. Certain technologies may lend themselves to certain applications. For example: Industrial Control Systems (ICS) or Supervisory Control and Data Acquisition (SCADA) devices are common in manufacturing and utility providers. Companies who work with ICS or SCADA devices should follow security developments the specific technologies. A threat actor targeting ICS or SCADA is often very skilled acquiring sample devices.

ESTIMATIVE INTELLIGENCE

A specific threat actor or group of actors attribution to a cyberattack is notoriously difficult and prone to false positives. The information gathered and learned from the threat actors becomes a glue that can tie together targets, technologies, and campaigns, even if it is difficult to identify the specific actor.

As a reader, we encourage you to concentrate on the sections that are relevant to your organization and your vertical. Use this information to enact policy changes and situational awareness to interdict these threats in your environment. As we look forward through this report for the remainder of 2018, three things are evident:

01 Specific organizations or industries will continue to see the use of crypto-mining malware and cryptocurrencies. The basic intelligence area will continue to expand as cyber threat actors continue to leverage exploitation of certain vectors for financial gain.

02 Cyber threat actors to offer bundled exploitation packages targeting specific technologies and by doing so, they will lower the cost of conducting such attacks.

03 To stop the threat from specific actors, the end user will still be the greatest asset to any security team. As a result training and knowledge sharing is imperative.
Optiv’s 2017 threat intelligence report made predictions for a time period that is now over. We can review those predictions and compare them to actual developments. What follows is a selection of analyses from the 2017 report along with an honest assessment of their accuracy.
THIRD PARTY RISK

**Prediction:** Exploits on third parties are a valid strategy for cyber threat actors. The most desirable targets will be organizations that use central hubs for handling data for a large number of clients.

**Result:** Correct

Globalization is a fact of life now. Companies looking to realize business efficiencies can outsource their manned call centers, move their data storage to an offsite cloud provider, and bring on remote contract employees as needed. One downside to this trend is that third party partners become a prime target, offering a weak link in the cybersecurity wall, such as the case of the Target breach, or providing a huge trove of data for multiple clients, as in the Equifax breach.

FROM CYBER-PHYSICAL TO CYBER-SOCIAL

**Prediction:** Cyber threat actors, especially nation-state actors, are increasingly interested in cyber-social exploits as opposed to cyber-physical exploits. While cyber-physical exploits can have real-world repercussions such as floods or blackouts, cyber-social exploits are useful to nation-states as a way to undermine their opponents in an asymmetric way.

**Result:** Correct

Cyber-social exploits are proving to be very cost effective for nation-state threat actors. For a small investment, an actor can cause a disproportionate response from an opponent. This report devotes an entire section to discussing the problem of cyber-social exploits in greater depth.

RANSOMWARE

**Prediction:** 2017 would see peak ransomware with the number of exploits leveling out.

**Result:** Incorrect

Several unprecedented events happened while the 2017 CTIE was in publication review. Chief among them was the WannaCry ransomware outbreak. WannaCry was a perfect storm that combined existing ransomware with worm functionality and a wide-reaching exploit, the so-called “Eternal Blue.” The exposure of the Eternal Blue and related exploits warrants its own report. But such a release is a black swan event, something truly unprecedented and unpredictable, when an exploit so damaging is released.
Optiv’s Global Threat Intelligence Center (gTIC) received over seven thousand tickets for support from clients in 2017. The Optiv team of threat intelligence analysts use this information as well as threat feeds and other intelligence gathering, to create the 2018 Threat Intelligence Landscape Estimate.
Phishing exploits were the most common way to deliver malware, making end user training and awareness critical.

Malware continues to be the largest threat launched by threat actors.

WannaCry and NotPetya significantly increased in the malware incidents reported.

Data Analysis

Verticals Takeaways

Retail, Hospitality and Travel were targeted with phishing emails intending credential theft to acquire customer credit cards and PII.

The Healthcare industry averaged over one breach per day, an increase of 6% from 2016. Of these, 37% were external hacking and 37% were caused by internal errors or malicious behavior.

Tech, Media and Telecom industries experienced a significant rise in cryptomining and cryptojacking incidents due to longer session times.

477 reported total breaches

The Healthcare industry averaged over one breach per day, an increase of 6% from 2016. Of these, 37% were external hacking and 37% were caused by internal errors or malicious behavior.
Vulnerabilities

Cryptocurrency and Cryptomining

Cryptocurrencies are attractive to hackers because they appeal to the early adopter nature of people who work with technology, and because cryptocurrencies provide an amount of anonymity to transactions.

Cryptomining is a novel way of monetizing an intrusion by using the victim’s compromised computer to produce money.

High utilization rates on a CPU can be a sign that your browser is being used to mine cryptocurrency.

The Internet of Things (IoT), continues to suffer from weak security fundamentals and unmitigated vulnerabilities, typically linked back to a combination of improper device deployment, failure to manage device settings, and vulnerabilities in hardware and software.

Combined with the weak security fundamentals, industry policies, procedures, standards and regulations continue to fall behind on properly securing IoT-based technology despite increased rates of adoption globally.
Software-Specific Exploits

2017’s vulnerabilities were unique as they featured three events unprecedented in scope and severity that each occurred at different points in systems: KRACK, Meltdown and Spectre, and Eternal family of exploits. Their impacts were felt far and wide by disrupting entire industries and the global economy.

KRACK targeted vulnerabilities in the WPA2 standard protocols, creating a weakness in the 4-way handshake protocol used to negotiate a new cryptographic key for communications.

Remediation for KRACK includes upgrading the firmware on all wireless devices and disabling Wi-Fi protected Setup (WPS).

Meltdown and Spectre are separate exploits that function in similar ways, using CPU features meant for performance enhancement to read restricted data. Meltdown allows a normal user to read data from the highly-guarded kernel portion of the operating system while Spectre tricks applications into accessing arbitrary location in their memory through misdirection so an adversary can extract information through a side channel.

Affected vendors are individually addressing the problem with a range of success.

The Eternal family of exploits had the greatest impact on the global economy in 2017. These target Microsoft’s Server Message Block (SMB) protocol.

The first observed use of the Eternal exploits was in May 2017, launched as the WannaCry ransomware-dropping worm. This exploit is estimated to have affected more than 150 countries and over 200,000 computers. Damages are estimated to be in the hundreds of millions to billions of dollars.

The second use of Eternal Blue was NotPetya, launched one month later in June 2017 which infected organizations in over 80 countries. Identified as a destructive variant of the Petya ransomware strain, this exploit destroyed the master boot record of those systems infected, making recovery impossible.
2017 saw the trend of state-sponsored exploits shift from cyber-physical to cyber-social with interference in several elections across Europe. 2018 is showing sharp repercussions for this information warfare with criminal indictments.

Distributed Denial of Service (DDoS) attacks remain a lucrative business, used mainly as a means of revenge or protest in 2017. China, the United States and South Korea all experienced a sharp increase in attacks above the normal average in 2017.

Lesser-known nation states such as Lebanon and the Netherlands are rising in the ranks of threat actors, using more traditional means of exploits with combinations of open source and custom built tools. They, and other actors like them, will continue to become more disruptive as they refine their tactics.
2018 Predictions

1. Expanding use of cryptomining malware and cryptocurrencies due to the lure of financial gain

2. Increases in IoT botnet exploits until IoT technology becomes more secure.

3. Continued threat from bundled, cost-efficient exploitation packages

4. Continued attempts from nation-state actors to execute cyber-social attacks, including activity revolving around the 2018 US mid-term elections

5. Progressing DDoS attacks will continue to be a problem for organizations of all sizes due to the willingness to pay ransom and the thousands of IoT devices connected to the internet each day that have weak security protections.

6. End users continue to be the best line of defense. Training and knowledge sharing is key.
As a managed security solutions provider, Optiv has clients from a diverse range of industries. Optiv tracks ten different client verticals.

Some threat actors, or types of cyberattacks, focus on specific industry verticals. For instance, nation-state actors focus on Government or Utilities & Energy. Meanwhile, criminal actors are stealing credit card numbers from Financial Services & Insurance companies, or installing malware on the critical systems used by Healthcare companies. Knowing something about the client’s industry helps focus requirements and targeting that result in better intelligence products.

Figure 1, visualizes how Optiv’s support tickets for each vertical changed over 2017. Notice the ebb and flow between the different verticals. The bottom chart is a sparkline that shows how the total ticket count changed month-by-month. The largest monthly increase was seen in July, which correlates to the NotPetya ransomware outbreak.
Tickets by Industry Vertical

Figure 1: Tickets of Optiv customers organized by business vertical.

Tickets by Category

Figure 2: Optiv tickets organized according to their category.
Optiv maintains in-depth visibility into all industry verticals. This allows security operations center (SOC) analysts, threat analysts, research analysts, intelligence analysts, and malware analysts to identify, assess, and track the latest threats. Similar to the prior few years, 2017 saw some heavy hitters when it came to malware and cyber-attacks. Although there were thousands of incidents that made headlines, a few of the big name exploits and breaches were:

- WannaCry and all the ‘Eternal’ malware families that followed
- Equifax with the largest data-breach on record affecting 148 million – or about 45% of the US population
- The Shadow Brokers with NSA data leakage
- The Wikileaks Vault7 leak of CIA hacking tools
- The Uber breach of 57 million user records
- The Verizon breach of 14 million accounts’ information

**STATISTICS**

Figure 3 shows the count of malware incidences seen by Optiv in 2017. Malware activity maintained a consistent level overall during 2017 across all customers. This suggests either a constant churn in the development of new malware, failure to adequately improve security postures, or a combination of the two.

There were two significant spikes in malware activity that tell the story of 2017: WannaCry which began May 12 and NotPetya families which began June 27. Ransomware exploits of unprecedented scope cut across industries. Optiv customers represent an overall view of those affected.
PHISHING ATTACKS

While zero-days and exploits get the security community’s attention along the lines of the release of a new Quentin Tarantino movie, phishing exploits are more like this summer’s Transformers sequel. Lacking originality and overuse of lens flare, phishing attacks are still the most common way for attackers to gain a foothold into the target environment (Zurier, 2016). And just like Fast and the Furious 19, they are still very much profitable.

In 2017, Optiv’s most commonly investigated malware was delivered via phishing exploits. We found that most phishing emails contained either attached documents with malicious VBA macros or hyperlinked URLs for credential theft. While most malicious attachments are caught by advanced security appliances before ever getting to the recipient, emails with hyperlinks to credential theft sites are still delivered.

Open source tools like the Social Engineering Toolkit and Phisery make the entry level for starting a phishing campaign frighteningly easy. Phisery, for example, is a one-two punch tool that can be setup in minutes on a compromised webserver or cloud instance to host a simple credential theft and malware drop website. As a bonus it is also precompiled for use on either Windows or Linux. The simplicity of this tool is shown here.

After installing the Phisery package, the attacker simply has to run the Phisery binary to start hosting a generic login page over https:

Navigating to this host will prompt the following login page:

If an end user gets tricked into supplying their credentials, the server grabs and stores them.

This tool can be configured to run with signed certificates, host fake login pages that appear legitimate and deliver the flavor of the month malicious Word Document. Because of the speed and ease in which these servers can be setup, it becomes increasingly difficult to track malware domains in order to block end users from falling prey to these attacks. This also creates another vector for
Recommendations:
1. If not needed in your environment, disable macro support in Office.
2. Conduct regular, recurring training.
3. Consider adding a report function in your email client to forward suspicious emails to security teams.

2018 Predictions:
We predict with high confidence that the use of phishing exploits, primarily for credential theft, will increase over 2018. This is due to tools becoming easier for threat actors to implement and advanced security appliances leaving attackers with fewer vectors for initial foothold.

INTSIGHS ALERTS
IntSights and Optiv collect data using different category systems. The following charts use the Optiv category system with the IntSights categories mapped onto it.

Figure 4 shows the share of alerts across business verticals. The top three verticals in descending order were: 1) Tech, Media & Telecom; 2) Financial Services & Insurance; and 3) Retail, Hospitality & Travel. All three of these verticals feature prominently in terms of handling money.

User accounts in Tech often link against bank accounts for payments, micro transactions, etc. Financial Services literally handles money. And Retail processes payment transactions for goods and services. This suggests an ongoing need to protect customers’ personally identifiable information (PII) and payment card information.

Figure 5 describes how IntSights alerts break down according to the type of potential incident. Information security professionals will not be surprised to see that the largest category was Phishing, which correlates to the Optiv data. Phishing continues to be an effective, low-cost, low-risk way for intruders to gain initial access into a target network. The next two largest categories were Brand Security and Data Leakage. Brand Security is concerned with phony, misleading, or malicious sites. Data Leakage is concerned with sensitive customer or company data being publicly released. Together, these two categories highlight how organizations should be concerned about their reputation both in terms of enforcing trademarks and in terms of protecting the data for which they have a responsibility.

Figure 4: IntSights alerts by business vertical.
Figure 5: IntSights alerts by incident category.
Certain threat actors and attack vectors are more common in some business verticals than in others. Phishing exploits that spread banking Trojans are likely of high interest to Financial Services. Intellectual property theft is likely of high interest to Manufacturing. The list goes on. In a world of limited resources, a business that understands the threats present in its vertical will be better prepared against those threats.

**UTILITIES AND ENERGY**

Utilities and energy providers saw some troubling trends during 2017. Despite the indicators of exploitation activity, there were not any high-profile impacts from breaches. Why would attackers take the time to infiltrate networks belonging to utilities without using that access? The answer hints at the kind of threat actors who are likely behind these exploits. The Ukrainian power outage caused by a cyberattack in 2016 showed that the cyber-physical effects of such an exploit are quickly mitigated (Szoldra, 2016). In that situation, power was lost to a single region for an hour while utility workers took the affected systems under manual control. This example suggests that an attacker will have just one attempt to make the most use of their access into a power system. There were some follow-on effects from the Ukrainian incident in that it caused a sense of awareness and unease even among civilians.

One possible scenario is that an attacker could use exploits on utilities and energy companies in conjunction with some other cybernetic or physical exploits. This would explain why threat actors are interested in utilities’ computer networks, but are not yet making their presence known; the actors are waiting to launch their attacks when directed to do so by some coordinating authority. For instance, if country A planned a kinetic, military confrontation with country B, and A had access to critical systems used in B, then A could shut down those critical systems to distract B during a coordinated attack. Country B would then effectively be fighting on two fronts; both domestic and foreign, trying to regain control of their own infrastructure while mobilizing to confront A.

In the case of the United States, it is probable that countries such as Russia and North Korea (DPRK) want to develop these kinds of accesses in case of a military confrontation. Russia has embraced the concept of asymmetric warfare, avoiding going might-for-might with the US’s superior military force (Thomas, 2011). A cyberattack capable of disabling critical infrastructure would lower the US’s military effectiveness. Similarly, North Korea exists in a constant state of paranoia regarding another war on the Korean peninsula against the United States and its allies.
Along with nuclear warheads mounted on intercontinental ballistic missiles (ICBMs), cyberattacks on critical infrastructure are a way for the smaller DPRK to take the fight to their opponent’s homeland. 2017 was a year of increasing tension and confrontation between the US and DPRK.

Energy firms in Saudi Arabia saw targeted attacks on their infrastructure during 2017 (Shemshaddine, 2017). Attribution for this attack is tentative but suggests neighbor Iran as the culprit. This makes sense given that Saudi Arabia and Iran are regional rivals and are both embroiled in the Yemeni civil war by supporting opposing factions. This is also not the first time that a cyberattack against Saudi state interests was attributed to Iranian threat actors. The 2012 attack on Saudi Aramco saw destructive malware take tens of thousands of computers offline (Perlroth, 2012). This demonstrates how malicious actors, when they determine the impact of a cyber-physical attack is significant enough, will burn their accesses in order to deliver a concrete message.

2018 Predictions:

- We assess with medium confidence that utilities will continue to see reconnaissance and pre-attack activity against their networks.
- We assess with low confidence that attackers will save accesses into utility and critical infrastructure networks, using them in conjunction with some other coordinated action.

RETAIL, HOSPITALITY AND TRAVEL INDUSTRY

For the retail, hospitality and travel industry, employee credential access was one of the primary driving forces for the malicious exploits so that the acquired customer credit cards and PII could then be sold on a darknet market. The method whereupon this happens is by the attackers masquerading as a trusted associate through email. The victim is then prompted to take action by the email, which can include being blank with only a malicious attachment such as a Microsoft Word document, be a claim from another section of the company that they need to check out the attachment/link, or even be a link to a malicious website that will then download the malware.

Another attack vector for the retail, hospitality and travel industry was ransomware. Near the end of 2017, browser-based cryptojacking saw a rise in popularity within this industry. Common attack vectors were infected Microsoft Word documents with macros enabled and with PowerShell downloaders.

2018 Predictions:

- We assess with high confidence a continued rise of cryptojacking browser-based exploits.
- We assess with high confidence that the usage of more “file-less” malicious exploits utilizing PowerShell and Windows Management Instrumentation (WMI) will be used to establish footholds and enumerate networks.

HEALTHCARE

The year 2017 was tumultuous regarding cybersecurity in the healthcare industry which experienced high levels of breaches and data leakage, ransomware, and potential emerging threats in medical devices. The healthcare industry has always had a large target on its back due to the value of personal identifiable information (PII) on the black market. Being a high-profile target becomes even more attractive to attackers given sometimes weaker security postures observed in the vertical.

Over the course of the year, healthcare as an industry averaged over one breach per day with 477 reported in total. A breach would be either an external exploitation or an insider threat situation. This marks a slight increase of about 6% in activity over 2016. While the total number of breaches increased, the number of records that were exposed or stolen sharply decreased – down from 27,314,647 in 2016 to 5,579,438 in 2017 (HIPAA Journal, 2018). While it is unknown what specifically caused the amount of records exposed to drop, it is possible that the industry is starting to take the loss of PII much more seriously than in previous years.

The cause of breaches is still of large concern. During 2017, 74% of breaches were caused by either hacking (37%) or by an issue with individuals within the company (37%), whether by error or wrongdoing (Snell, 2017). 2017 recorded 178 external hacking incidents compared to 120 in 2016. This increase in the amount of exploits alongside the decrease in amount of records accessed can be attributed to the lack of large-scale breaches like those seen in 2016 (Mimecast Limited, 2017).

Insider threats are much harder to deal with than external hackers. Insider threats have been on-going for decades, but experts in cryptographic design believe they could be mitigated through the use of encryption on patient records. It is believed that 2018 will fare a bit better...
for healthcare as security programs and postures are implemented in earnest.

The healthcare vertical saw a rise in reported ransomware exploits during 2017. In a survey conducted in December 2017 (Mimecast Limited, 2017), 78% of providers reported they had experienced a ransomware or malware attack over the course of the year. This isn’t surprising given that 2016 saw several high-profile ransomware attacks; but, since the exploits were fairly new, most companies didn’t know how to report them. This changed in 2017 when the Office for Civil Rights (OCR) recommended that ransomware attacks be reported alongside hacking incidents. Due to the new reporting guidelines, it is likely that this is the cause in the increase of reports.

Cybercriminals realize that organizations, and potentially people’s lives, rely on the data they store and the technology they employ. Actors realize that organizations will likely pay ransoms instead of face the risk that comes alongside ransomware attacks. With incidents like WannaCry and NotPetya having a massive effect on some of the largest healthcare providers in the world (National Health - ISAC, 2017), it is unlikely the trend of targeting healthcare will change, and the industry will continue to be viewed as an extremely high-value target.

Throughout 2017, one of the largest topics of concern was how the Internet of Things (IoT) would affect the healthcare industry. As providers strive to improve the care they give their patients, more and more technology is being introduced into hospitals and healthcare facilities. From Internet-connected printers and thermostats all the way to insulin pumps and pacemakers that doctors can monitor from anywhere in the world, the attack surface for healthcare is growing. Marred by non-existent or lacking security protections, Internet-connected medical devices are opening a whole new world for attackers.

During the year, the FDA warned and even shamed manufacturers for their lack of protocols to protect patients. In September 2017, the FDA recalled 500,000 Internet-connected pacemakers over hacking fears. There has been much discussion in the last year as to whether the benefits of Internet-connected devices outweigh the potential consequences should something go wrong. 2018 will be a very important year in the hardening and strengthening of cybersecurity in medical devices. Fortunately, to date, there have not been any known compromises leading to loss of life. But unfortunately the possibility is growing, and the healthcare industry must figure out how to secure and protect these devices.

Mitigations:
• Ensure personnel with access to PII are both trained and trustworthy to be handling the information.
• Develop and follow a mature patching plan to keep systems and devices up-to-date.
• Train employees to understand when they may be targeted by cybercriminals in order to protect themselves and their companies from data loss.

2018 Predictions:
• We assess with high confidence that the healthcare industry will continue to be a massive target for malicious actors due to the lucravity of PII on the black market.
• We assess with moderate confidence that the number of reported ransomware attacks will level out as organizations familiarize themselves with reporting procedures.

TECH, MEDIA AND TELECOM

The Tech, Media and Telecom Industry in 2017 was no stranger to cyberattacks. The Bell Canada Telecom breach in May 2017 was one of the largest of the year (Kumar, 2017). In this hack, the sensitive data of 1.9 million customers was stolen and a portion released onto a Pastebin when Bell Canada “failed to co-operate” with the hacker’s ransomware demands. There is still uncertainty as to what kind of co-operation the hackers were demanding. In January 2018, a second Bell Canada breach was reported related to the exposure of sensitive data for 100k users. (Jackson, 2018).

WannaCry ransomware was the source for a large amount of the support tickets Optiv received for Tech, Media and Telecom companies. Second behind ransomware was cryptomining/cryptojacking. Media sites are a prime target for cryptojacking exploits because they keep visitors on for longer session times, which is useful when mining cryptocurrency.

2018 Predictions:
• We assess with high confidence the Tech, Media and Telecom industry will be impacted by more “file-less” malicious exploits utilizing PowerShell and Windows Management Instrumentation (WMI) to establish footholds and enumerate networks.
• We assess with medium confidence that cryptomining/cryptojacking based exploits will move on to targeting utilities and other critical infrastructure within 2018.
As we have discussed to this point, many newer technologies and vulnerabilities are affecting multiple industries. It is important to understand the root of the technologies and the effect they have had on the threat landscape of 2017, as well as the continuing impact we predict to see in 2018.

**CRYPTOCURRENCY**

Cryptocurrencies are a libertarian ideal: a monetary system outside the control of big government. The modern digital world provides the necessary components for a cryptocurrency to succeed. Computing power has advanced sufficiently to lower the processing burden of cryptography. Now systems are both powerful enough and affordable enough that there is a sufficiently large audience for a cryptocurrency system. But where cryptocurrencies solve some of the fundamental problems of centralized currencies, they also introduce some new problems while still falling victim to other, age-old problems.

Bitcoin is synonymous with cryptocurrency for a lot of people as it was an early cryptocurrency system and the first to achieve a large scale of adoption. Since 2007 when Bitcoin appeared, the cryptocurrency space has increased exponentially. Special-purpose cryptocurrencies add new features. But Bitcoin includes two pieces of technology that are applicable to a wide variety of cryptocurrencies: blockchain and proof-of-work functions.

![Market Capitalization](image-url)

*Figure 6: Market capitalization for the largest cryptocurrencies as of November 15, 2017.*
Blockchain technology is what enables cryptocurrencies to exist outside of centralized, third-party control. It is a distributed ledger that records all transactions of a currency with guarantees of cryptographic integrity. The blockchain is append-only, which means that the records in the ledger cannot be altered once they are written.

When enough transactions are available, volunteers collect them and begin computing. These volunteers operate on a proof-of-work function that shows the transactions were validated. The transactions and the function's output become a new block in the blockchain. Volunteers are incentivized to perform the computations with rewards of the actual cryptocurrency itself.

There are additional pieces of technology required to make a cryptocurrency work as well: protocols that specify how the network traffic functions, accounts for storing amounts of currency, and associated services for facilitating the use of a currency. All of these components increase the attack surface for someone looking to exploit a cryptocurrency system.

Two different cryptocurrencies serve as the staple for two different kinds of cybercrime. Bitcoin still reigns as the means to pay the fee demanded by ransomware. Bitcoin is the most widely used and available of all cryptocurrencies. Meanwhile, Monero is king when it comes to mining cryptocurrency on a victim's machine. This is because the Monero cryptocurrency system has additional privacy-enabling features built in that are not seen in Bitcoin.

FOLLOW THE MONEY

Cryptocurrency has become associated with deep web and dark net sites. When ransomware prompts a victim to pay, the amount demanded is sometimes given in bitcoin. Cryptocurrencies are attractive to hackers both because they appeal to the early adopter nature of people who work with technology, and because cryptocurrencies provide some amount of anonymity in their transactions. But traditional law enforcement is quickly learning how to exploit these tools as Ross Ulbricht of Silk Road notoriety would know (Tiku, 2017).

Designs vary among the different cryptocurrencies. Newer systems like Monero and Zcash have extensive built-in privacy mechanisms. Older systems like Bitcoin have adapted when users roll out services like coin tumbling, which passes Bitcoin back and forth through several transactions to hide its source. This is money laundering.

PICK POCKETING

When a user converts real-world currency into cryptocurrency, or receives cryptocurrency as payment, they store those coins in special-purpose software called a “wallet.” The wallet is just one point at which an attacker can steal cryptocurrency belonging to someone else. If an attacker is able to access your wallet, just as if they were able to access your bank account, they would be able to transfer your coins to themselves.

Gaining access to wallets, like gaining access to bank accounts, requires a certain amount of social engineering. Cryptocurrency wallets, like traditional online banking applications, look to solutions like multi-factor authentication in order to better secure their user's accounts. Even nation-state actors like Lazarus Group (North Korea) are getting in on the action, stealing Bitcoin out of victims’ wallets (McNamara, 2017).

THE BIG HEIST

To steal the most money at one time, a criminal must go to where the largest amounts of money are kept. For cryptocurrencies this means the coin exchanges. Exchanges are where one currency gets changed into another like dollars for Bitcoin, pounds for Monero, or Litecoin for Ether. The following are a couple of high-profile examples.

Mt. Gox was a large bitcoin exchange in Japan that was put out of business due to the theft of cryptocurrency. Mt. Gox went bankrupt in 2014 when it found that hundreds of millions of dollars’ worth of Bitcoin went missing from the site. Subsequent investigations suggest that the theft started as far back as 2011 (Nilsson, 2015). The situation remains mired in multiple legal proceedings.

A second example is that of the DAO, a distributed autonomous organization, a smart contract able to exist in the Ethereum infrastructure. DAO was an investment fund intended for venture capital funding. At time of inception, the DAO was worth $150 million. A successful hack was able to divert $50 million worth of the currency (Price, 2016). In order to remediate the situation, the Ether cryptocurrency was forked, much like how an open source software project might be split into two different projects. The result was a large drop in the value of Ether and two different cryptocurrency systems: Ethereum and Ethereum Classic.
CRYPTOJACKING

Coin miners are the pieces of software that grind through the proof-of-work functions.

When a miner finds a solution, then the person running the miner is rewarded with a certain amount of the cryptocurrency in question. The product of coin mining serves as the basis for the cryptocurrency system. Coin miners also provide a completely novel way of monetizing an intrusion.

Hackers are good about monetizing the computers they compromise. If a hacker installs a coin miner on a compromised computer, they can turn the victim’s electricity into money. Fortunately, coin mining is computationally intensive and the slowdown of the infected system may alert system administrators to the anomaly. Kaspersky Lab has data showing millions of such infections in recent years with 2017 on track to top previous records (“Mining” Botnets Are Back - Infecting Thousands of PCs, Generating Hundreds of Thousands of Dollars for Criminals, 2017).

There are too many web sites that were compromised with cryptocurrency miners for it to be practical to list them all but here are a few examples:

- Showtime (McCarthy, 2017)
- Ultimate Fighting Championship (Thomson, Let’s get ready to grumble! UFC secretly choke slams browsers with Monero miners, 2017)
- CookieScript (Cimpanu, 2017)

But not all web sites hosting cryptocurrency miners are necessarily compromised. The intended use of software like Coinhive is for web site monetization. The Pirate Bay tried monetizing with Coinhive, but neglected to tell its user base beforehand (Oberhaus, 2017). Examples of other sites that tested cryptocurrency monetization are:

- Iridium (Chrome extension, YouTube interface)
- Salon (O’Neill, 2018)

Monero is an attractive cryptocurrency to criminals because it has a feature called “stealth addresses.” A stealth address insulates a Monero user’s wallet from being associated with a transaction. Instead, a random address is generated and the transaction is sent to that stealth address instead of to the Monero wallet directly. For a criminal, this is a useful way to prevent illegally mined coin from being traced.

Cryptocurrency is a double-edged sword like many other technical developments. It promises to expand the boundaries of discourse and finance around the globe. But it does so equally for all who participate, and this includes criminals. Cyber criminals are quick to adapt new tools and techniques that will help them earn the most money in the least risky way possible.

Mitigations:

- Watch for unusual resource utilization rates. Cryptocurrency mining software will utilize at least half of available CPU cores at near 100% utilization.
- If you think that your browser is being used to mine cryptocurrency, close the browser completely. When the browser stops running so does the JavaScript engine in which the mining software is running.
- Organizations should blacklist cryptocurrency mining software. The applications are usually open source packages that are readily downloaded.
- Use multi-factor authentication on cryptocurrency wallets the same way one would for a bank account.

2018 Predictions:

- We assess with high confidence that cryptojacking exploits will increase in frequency over 2018.
- We assess with high confidence that distribution of cryptomining software via exploit kits will continue to increase over 2018.

VULNERABILITIES

The landscape for vulnerabilities and exploits shifts slowly over time. It used to be the case that Microsoft Windows was the desired target for attackers due not just to its market penetration but also due to the prolific nature of vulnerabilities that could be found. Microsoft took deliberate action and drastically improved the quality of the code it was releasing. Consider the perennial whipping boy of World Wide Web multi-media, Adobe Flash. Eventually the market decided to move beyond Flash and abandoned it completely in favor of the vendor-neutral HTML5 standard.

2017’s vulnerabilities were something different. Their impacts were felt far and wide, disrupting entire industries and the global economy. As such, Optiv’s gTIC is without a clear reference to say whether or not these kinds of events will be seen again. However, it’s important to look at three of these key events that were unprecedented in terms of their scope and severity. Each vulnerability occurred at a
different point in the system. KRACK occurred due to a flaw in the design standard meaning all deployed systems that met the standard were vulnerable. EternalBlue was a software flaw found in virtually all versions of Windows over the past decade and was remotely exploitable. Finally, Meltdown/Spectre was a hardware flaw found in the dominant market product. This means it requires physical replacement to fully remediate.

**KRACK**

In October 2017, security researchers publicly disclosed an exploit targeting vulnerabilities in the WPA2 standard protocols which are required to be implemented by all WPA2-certified consumer and enterprise wireless network devices (Vanhoef & Piessens, 2017). Based upon a vulnerability initially discovered by Dutch researchers in 2016, their now working proof-of-concept exploit, named the Key Reinstall AttaCK (KRACK), could significantly reduce the security of network connections against man-in-the-middle interception, inspection, and hijacking.

In their research, they discovered a weakness in the 4-way handshake protocol which is used to negotiate a new cryptographic key for subsequent communication. By forcing the retransmission of the third packet of the handshake, a device can be forced to re-install the same cryptographic key.

It is not at all common for a vulnerability to exist in such a widely adopted standard in computer science. Much more common cryptographic exploits are side-channel exploits or scenarios in which it is not a standard that is being exploited, but instead a poor or improper implementation of a standard. Furthermore, when these types of vulnerabilities are disclosed, it can often be months or years before any kind of viable proof-of-concept exploit can be achieved which does not require considerable computational resources to achieve. This makes KRACK rather novel.

An interesting comparison, also from 2017, is the Return of Bleichenbacher’s Oracle Threat (ROBOT) exploit against TLS_RSA (Böck, Somorovsky, & Young, 2017). As the name suggests, this is a new spin on an old vulnerability, in this instance one which was first discovered in 1998. Prior to this discovery, the classification of adaptive chosen-ciphertext exploits were purely theoretical. Originally known as the million message attack, subsequent research completed in the nearly two decades since its discovery has gradually improved the efficiency, and thus, the practicality of the exploit. One such example of this incremental research is a well-publicized vulnerability from 2016: Decrypting RSA with Obsolete and Weakened eNcryption (DROWN; CVE-2016-0800). Today, ROBOT has effectively proven these exploits to be practical enough that the recommendation is to completely disable TLS_RSA.

Although the number of devices, and therefore software and hardware manufacturers, impacted by KRACK was
huge, the industry was quick to respond with patches. However, limited information is known about the total cost incurred by this vulnerability.

KRACK is not the first flaw from which WPA2 has suffered. First, although not specific to WPA2, there is the Wi-Fi De-authentication (DEAUTH) Attack in which spoofed packets are used to force a victim client to have to re-authenticate to the Wi-Fi base station. This attack is used for two purposes – to attempt to trick the client into connecting to an attacker-controlled rogue access point, or to sniff the 4-way handshake between the client and the base station for the purposes of attempting a brute-force attack of the network password.

Also, in 2011 a design flaw in the Wi-Fi Protected Setup (WPS) standard was discovered which made brute-force attacks on WPS PINs practical (Viehböck, 2011). Researchers had discovered that the messages passed while attempting to verify the 8-digit WPS PINs handle the messages in such a way that the true number of possible PINs was \(10^8 \times 10^3\) instead of \(10^8\) as one would expect – a reduction by three orders of magnitude! As a proof of concept, a tool named reaver-wps was released which was capable of cracking WPS access PINs in less than four hours. This tool was later updated to include 2014’s Pixie Dust attack, which exploited a lack of randomness in the cryptographic nonce in specific vendor implementations and enabled offline cracking of the PINs of affected devices’ networks within minutes.

In January 2018, Wi-Fi Alliance announced details of the WPA3 standard, including the cryptographic and security improvements intended to address KRACK. Specifically, cryptographic key strength is being increased to 192-bits, connections will be protected with individual per-session encryption, and implementation of the Simultaneous Authentication of Equals (Dragonfly) protocol will be implemented to further secure the cryptographic handshake and provide more robust security against brute-force attacks (Clarke & Hao, 2014). And, although details have yet to be provided, it has been stated that the security of WPS will be improved – likely to mitigate the Reaver attack.

**Recommendations:**

- Upgrade the firmware on all wireless devices. Firmware upgrades should be addressed by any organization’s upgrade policy.
- Disable WPS as it is inherently insecure.

**Figure 8: Wi-Fi security developments over time.**

<table>
<thead>
<tr>
<th>2004</th>
<th>2011</th>
<th>2014</th>
<th>2017</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WPA2</strong></td>
<td><strong>REAPER</strong></td>
<td><strong>PIXIE DUST</strong></td>
<td><strong>KRACK</strong></td>
<td><strong>WPA3</strong></td>
</tr>
<tr>
<td>CCMP/AES encryption improves protection against interception and traffic replay exploits</td>
<td>Practical brute-force attack of WPS PINs</td>
<td>Offline password brute-force bypasses lock-out protections</td>
<td>KRACK effectively defeats the WPA2 security improvements provided by AES</td>
<td>192-bit keys, Weak password mitigation, WPS security improvements</td>
</tr>
</tbody>
</table>

2017 CYBER THREAT INTELLIGENCE ESTIMATE, OPTIV | 26
2018 Predictions:

• We assess with high confidence that initial deployments of proposed WPA3 standard will begin appearing in devices.

• We assess with high confidence that attackers will experiment with this vector in situations where they can connect to a target's wireless network.

MELTDOWN AND SPECTRE

On January 3, just three days into 2018, researchers at the Graz University of Technology and Google’s Project Zero (Horn, 2018) released their papers on identified vulnerabilities dubbed “Meltdown” and “Spectre” via the websites https://meltdownattack.com and https://spectreattack.com/ (Kocher, et al., 2018) (Lipp, et al., 2018). Within the papers, they went over these critical vulnerabilities that could be exploited in modern processors from hardware bugs that would allow programs to steal data that is currently being processed on the computer. These exploits affect desktop, laptop, cloud computing and smartphone platforms. (table 1)

The researchers also showed that they were able to take advantage of hardware flaws by abstracting them to the software level. What makes this new vector stand out even more is that it’s harder to stop with conventional anti-malware protections and may demand a whole new type of protection.

Meltdown and Spectre are two separate exploits that function in similar ways. Both exploits use CPU features meant for performance enhancement to read restricted data.

Meltdown is an exploit that allows a normal user to read data from the highly-guarded kernel portion of the operating system. In Intel CPUs, certain instructions are speculatively executed which can increase CPU performance depending on the task. Attackers can exploit this lack of checking and trick the CPU into executing instructions which make the CPU reveal bits of data stored in system memory. This side channel can leak sensitive information such as user credentials from high-security parts of the operating system.

AMD processors do not speculatively execute instructions, so they are not affected by the Meltdown exploit. However, they are affected by the Spectre exploit, as are Intel and ARM processors.

Spectre operates differently than Meltdown. Spectre tricks applications into accessing arbitrary locations in their memory by misdirecting the processor so that later on it will make an exploitable error. As the misdirection is happening, the adversary prepares a side channel that will be used for extracting the victim's information by performing a flush+reload or evict+reload attack.

The CPU then speculatively executes instructions that transfer confidential information from the victim context into the side channel. This may be triggered by having the attacker request that the victim perform an action by a syscall, socket, or file. In other cases, the attackers may leverage the speculative misdirection of its own code in order to obtain sensitive information from the same process.

The final phase of the Spectre exploit recovers the exposed sensitive data using the aforementioned flush+reload or evict+reload. The recovery process then consists of timing how long it takes to read from the memory addresses that are being monitored.

Spectre exploits assume that speculatively executed instructions can be read from memory that the victim process could access normally without triggering a page fault or exception. For example, if a processor prevents speculative execution of instructions in user processes from accessing kernel memory, the attack will still work.

Affected vendors are individually addressing the problem:

• Amazon - Amazon’s EC2 fleet is protected from all known threat vectors from Meltdown and Spectre (see Table 1 above). The recommendation however for all

<table>
<thead>
<tr>
<th>Description</th>
<th>Vulnerability</th>
<th>CVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bounds check bypass</td>
<td>Spectre</td>
<td>2017-5753</td>
</tr>
<tr>
<td>Branch target injection</td>
<td>Spectre</td>
<td>2017-5715</td>
</tr>
<tr>
<td>Rogue data cache load</td>
<td>Meltdown</td>
<td>2017-5754</td>
</tr>
</tbody>
</table>

Table 1: Formal and informal vulnerability descriptions.
customers on their AWS Batch, Amazon EC2, Amazon Elastic Beanstalk, Amazon Elastic Container Service, Amazon Elastic MapReduce, and Amazon Lightsail is to patch their instance operating systems.

- **AMD** - AMD has worked with Microsoft and Linux vendors to distribute patches for Spectre Variant 1 and 2 (AMD, 2018). Initially, there were issues with older AMD processors on Windows, but it has been corrected and Microsoft resumed updating. They are also contributing to the development of Retpoline which will be discussed further in this paper. Their new server CPU, Zen 2, is planned to include hardware mitigations for the Spectre vulnerabilities with a release slated for late 2018.


- **Apple** - Apple addressed Meltdown and Spectre within iOS 11.2.2, macOS 10.13.3, OS X El Capitan 10.11.6 and macOS Sierra 10.12.6.

- **ARM** - The majority of ARM processors are not impacted by any variation of Meltdown or Spectre; however, there is small subset of ARM-designed processors that are susceptible and have mitigation instructions with updates on their website (Arm Limited, 2018). All future ARM Cortex processors will be resilient to this style of attack or allow mitigation through kernel patches.

- **Intel** - Due to the release of the whitepapers, Intel has formed their own internal Product Assurance and Security group, with undisclosed immediate tasks and strategic goals, as well as naming a new CTO, Dr. Michael Mayberry (Intel, 2018). The patches Intel has released for Meltdown and Spectre were released and then retracted almost immediately due to issues they introduced. Microsoft and RedHat have both disabled the fixes. Until the updated Intel microcode comes out, true mitigation of all variants cannot be completed for systems using Intel processors.

- **Microsoft** - Microsoft has been on the forefront of releasing patches for both AMD and Intel processors for Windows while even blocking Intel’s buggy fixes on Windows 10. Along with updating Edge and Internet Explorer 11 with security update KB4056890, Microsoft has added new capabilities in Windows Analytics service display for the now weary IT workers that support Windows 7 with Service Pack 1, Windows 8.1 and Windows 10.

A small number of antivirus software products have issues installing the January 2018 and February 2018 Windows security updates due to making unsupported calls into Windows kernel memory. To fix this, the antivirus software has to set a required registry key, generally done with an update, but there are a few that require the user to set it manually. The antivirus software still affected by this issue are: Carbon Black, Cisco (AMP), FireEye (Endpoint Security), Nyotron (PARANOID), and SentinelOne (EPP). Google introduced a new approach known as Retpoline for dealing with Spectre Variant 2 (Turner, 2018). Retpoline is to prevent branch-target-injections, comparing speculative execution to an overly energetic 7-year old that we must now build a warehouse of trampolines around. As this is a brand-new attack vector, multiple proof-of-concept (PoC) exploits have been developed by the researches themselves and outside sources. Utilizing PowerShell or JavaScript, the PoCs that have been released showcase possible attack vectors, with the JavaScript PoC able to be run from inside a victim’s browser utilizing Variant 1. At the beginning of February 2018, some malware authors have been trying to test out the JavaScript Variant 1 with 139 samples that have been discovered so far by AV-TEST. Throughout the rest of 2018, the cost of the Meltdown and Spectre vulnerabilities will become clearer, including the 32 lawsuits that Intel now faces from both Meltdown and Spectre (Lumb, 2018). There will undoubtedly be more malware authors developing and testing exploits that will take advantage of the Meltdown and Spectre vulnerabilities in a race against vendors to who will continue to release their own patches.

**ETERNAL EXPLOITS**

In 2017, multiple weaponized exploits and campaigns were observed targeting Microsoft’s Server Message Block (SMB) protocol. SMB is a file and print sharing protocol. The SMB service is on by default on all versions of Windows because it is central to building a Windows network on a LAN.

The exploits with the greatest impact were the so-called “Eternal” family of exploits. The Shadow Brokers group released the exploits along with other hacking tools they claimed originated with the United States National Security Agency (NSA) (Goodin, Mysterious Microsoft patch killed 0-days released by NSA-leaking Shadow Brokers, 2017). There are four different exploits in total but all target SMB. Affected versions of Windows span a decade worth of releases. This wide window of vulnerability, coupled with the default-on nature of the SMB service, created a huge potential for exploitation. Microsoft issued their patch and bulletin for the exploits in March of 2017.
A network self-replicating worm was created from the Eternal series that chained together seven different exploits. Identified as EternalRocks, this worm was designed to spread through the use of EternalBlue, EternalChampion, EternalRomance, EternalSynergy, DoublePulsar, ArchiTong, and SMBTouch (Mimoso, 2017). Other names for EternalRocks include ‘Doomsday’ and ‘BlueDoom’.

The first observed use of the Eternal exploits was the ransomware-dropping worm, WannaCry (Islam, Oppenheim, & Thomas, 2017). Launched in May 2017, two months after the patch was released, malicious attackers crafted a specialized malware package targeting Microsoft Windows distributions. This weaponized malware leveraged the EternalBlue exploit. EternalBlue is a SMBv2 exploit for Windows 7 Service Pack 1. Successful exploitation resulted in victims being infected with ransomware, causing significant impact to organizations around the globe. The attack is estimated to have affected more than 150 countries and over 200,000 computers. Damages caused by WannaCry are estimated to be in the hundreds of millions to billions of dollars. It is believed that WannaCry was just a test of the leaked exploits.

The second observed use of the Eternal exploits was NotPetya (Bedwell, 2017). Launched in late June 2017, this malware strain infected organizations in over 80 countries. NotPetya attempted to mimic the structure and motivation of Petya, a predominant ransomware strain believed to have Russian origins (Meyer, 2018). It was only later that NotPetya was identified as a destructive variant. The ransomware component of the attack was an attempt to redirect attention away from its ability to destroy the master boot record (MBR). The destruction of the MBR, and encryption of drive data, makes recovery impossible. While infections were reported across verticals, the victim hardest hit by NotPetya was Danish shipping giant Maersk. Maersk spent over $300 million to replace tens of thousands of PCs and servers (Chirgwin, 2018).

The leak of the Eternal exploits was an unforeseen obstacle for cyber security professionals across the globe. Since the leak, Eternal code has been added and/or modified to popular tools such as metasploit and exploit-db. Proofs of concepts and real world cases have shown just how dangerous the Eternal series can be and highlights how organizations continue to struggle when applying patches. MS17-010, which would have rendered WannaCry and NotPetya ineffective, had been released months before the WannaCry outbreak. The quick adaptation of publicly available proof-of-concept exploits spotlights the resourcefulness and dedication of cyber criminals. Security leaders can expect to continue seeing this type of evolution in future high profile campaigns. Malware, botnets, and campaigns will continue to grow in complexity as they evolve to defeat traditional security solutions.

**Mitigations:**

- Define an update policy with specific timetables for when patches should be fully deployed.
- Be sure to implement strong passwords and secure authentication processes for any internet-facing services or devices necessary for critical business functions.

**2018 Predictions:**

- We assess with high confidence that the Eternal exploits will continue to be used successfully throughout 2018.
- We assess with moderate confidence that exploits released in 2018 will not have such a high degree of impact as Eternal.

---

**Table 2: The Eternal SMB exploits and the affected Windows versions.**

<table>
<thead>
<tr>
<th>Exploit</th>
<th>SMB</th>
<th>Windows</th>
<th>CVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>EternalBlue</td>
<td>2</td>
<td>7</td>
<td>2017-0143 through 2017-0148</td>
</tr>
<tr>
<td>EternalRomance</td>
<td>1</td>
<td>XP, 2K3, Vista, 7, 8, 2K8, 2K8R2</td>
<td>2017-0143, 2017-0147</td>
</tr>
<tr>
<td>EternalSynergy</td>
<td>3</td>
<td>8 and Server 2012 SPO</td>
<td>2017-0143, 2017-0146</td>
</tr>
<tr>
<td>EternalChampion</td>
<td>1</td>
<td></td>
<td>2017-0146</td>
</tr>
</tbody>
</table>
INTERNET OF THINGS

Internet of things (IoT) is a system of networked, low-power computing devices. Since its inception, IoT-based technology continues to suffer from weak security fundamentals and long-standing unmitigated vulnerabilities. Security events involving IoT-based technology can typically be linked back to a combination of improper device deployment, failure to manage device settings, and vulnerabilities in hardware/software. Vulnerabilities in IoT-based technology allow malicious actors to leverage its weaknesses for nefarious activities.

In 2016, the world’s first IoT botnet, Mirai, enslaved hundreds of thousands of IoT devices and leveraged them in a massive distributed denial-of-service (DDoS) attack that successfully knocked hundreds of sites offline (Bursztein, 2017). Mirai compromised IoT devices using default factory set logins.

In the wake of Mirai came IoTrooper, or Reaper (Buntz, 2017). IoTrooper was seen recruiting thousands of vulnerable IoT devices across the globe in late 2017. Even though IoTrooper shared code with Mirai, there are key changes that made it more dangerous. IoTrooper does not specifically focus on brute-forcing to compromise IoT devices. Instead, IoTrooper was designed to leverage nine known vulnerabilities and can target twelve different kinds of IoT technology. According to information security experts, IoTrooper is estimated to include millions of devices around the globe from the United States to Australia. IoTrooper has been called a massive zombie botnet capable of taking down the Internet, and its collective continues to grow on a daily basis. Information security experts were unable to identify IoTrooper targets, and recruitment continues into 2018.

Industry policies, procedures, standards, and government regulations continue to fall behind on properly securing IoT-based technology despite increased rates of IoT adoption across the globe. Because of this failure, cyber-criminals continue to leverage these weaknesses for monetary gain. In early 2018, a new IoT botnet was seen offering distributed denial-of-service attacks. Dubbed JenX, attackers leverage enslaved IoT devices to launch DDoS attacks (Goodin, New IoT botnet offers DDoSes of once-unimaginable sizes for $20, 2018). JenX is capable of rendering 290-300 gigabits per second DDoS attacks starting at $20 with larger exploits available at higher prices. JenX operators utilize non-IoT servers to scan the Internet for vulnerable IoT technology. These devices are then exploited to install JenX.

Mitigations:

• Change factory default settings such as passwords, IP addresses, etc.
• Place IoT devices between a NAT or other type of firewall to prevent their discovery/access from the wider Internet.

2018 Predictions:

• We assess with high confidence that there will be an increase in IoT botnet exploits until IoT technology becomes more secure.
• We assess with high confidence that more IoT as-a-service solutions will surface in 2018, enabling cyber-criminals across the globe to continue exploiting organizations.
Threat actors give away information by how they behave. Are they sneaky or noisy? Do they use year-old exploits found in open source toolkits, or are they deploying zero-days that do not yet have a patch? Why is this particular actor carrying out a sneaky attack on this particular target? Asking these kinds of questions begins the intelligence cycle, resulting in the kind of intelligence products that are useful to a wide variety of Optiv clients.

**CYBER-SOCIAL ATTACKS**

The 2017 CTIE discussed a shift in state-sponsored attacks from cyber-physical to cyber-social. An in-depth review of how those predictions played out is provided in the Recap section. But it is safe to say that 2016 was an unprecedented year for cyber-social attacks. 2017 saw those trends continue around the globe (Le Miere, 2017):

- June 8, 2017: British snap general election (Press Association, 2017)
- September 24, 2017: German federal election (Stelzenmüller, 2017)
- October 1, 2017: Catalan independence (from Spain) vote (Emmott, 2017)

2018 is showing stark repercussions for information warfare. Criminal indictments in American federal courts name both organizations and individuals who conducted operations against the 2016 US presidential elections (Mueller, 2018). This includes the Internet Research Agency, a Russian firm located in St. Petersburg. The Internet Research Agency was long a butt of Internet jokes about pro-Russian forum trolls, and later a topic of discussion in information security circles and US Congressional hearings.

There is a fundamental difference in how Americans and Russians view information warfare. The American military views information warfare as a tool against an opposing military force. The civil society surrounding that opposing force is a target insofar as they directly support the military. Conversely, Russians view the entirety of an opponent’s civil society as a valid target for information warfare (Klimburg, 2017).

Differences in scoping information warfare exist as well. American information warfare is focused on a specific objective, and the role of information warfare is to support other units in achieving that objective. But Russian information warfare doesn’t limit itself to a specific scope.
Rather, it works to undermine the functioning of civil society as a whole so that support for military operations falters (Thomas, 2011). To this end, Russian information warfare pits different factions of a society against one another instead of advocating for just one side (Lucas, 2017). This is a very cost-effective strategy. One analysis shows that the Internet Research Agency spent $46,000 on Facebook ads in the same time period that the Donald Trump and Hillary Clinton campaigns spent $81 million (Constine, 2017).

Researchers and tech companies continue to search for a technological solution to a problem with deep cultural and behavioral roots. In the meantime, underdog adversaries have taken note of the effectiveness of asymmetric operations such as cyber-social exploits. The low barrier to entry makes such attacks available to any party with limited financial or technical resources.

**Mitigations:**

- Establish good cyber hygiene when consuming news sources. Look for sources with long histories and a wide sense of trust. Scrutinize sensational headlines.

**2018 Predictions:**

- We assess with high confidence that cyber-social attacks will revolve around the 2018 United States elections.
- We assess with medium confidence that other nation-state actors will imitate the success of the Russians and attempt their own cyber-social campaigns.

**DDoS CREWS**

Botnets capable of executing record-breaking Distributed Denial of Service attacks have almost become something of a commodity thanks to vulnerabilities and the lack of proper security precautions on IoT devices. In years past, assembling a network of infected devices required much more work on the part of attackers. But as the landscape of the Internet changed, so did the targets. DDoS attacks remained a lucrative business for cybercriminals. The larger the botnet, and therefore the scale of the attack, the more money the criminals could make by carrying out attacks. The business became a means of revenge or protest, and was leveraged as such throughout 2017.

**Figure 9: Chart of the amount of DDoS attacks by country with data indicating victim of attack. (Data from Akamai quarterly reports.)**

- China
- United States
- South Korea
- Russia
- Great Britain
- France
- Netherlands
- Canada

Q1, Q2, Q3, Q4, Average

---

2017 CYBER THREAT INTELLIGENCE ESTIMATE, OPTIV | 32
2017 started off with several potentially major threats – including a DDoS attack against the White House website in protest of Donald Trump’s inauguration – that didn’t actually amount to anything. The first part of the year is historically a time of calm as far as DDoS attacks go, but researchers noted a modest increase over the years prior. This indicates a general increase in the frequency of DDoS attacks, which was expected, and was aided by events such as the release of the Mirai source code. Though the growth of IoT botnets was expected, DDoS attacks in the first quarter of 2017 were actually primarily infected Windows-based machines – representing nearly 60% of all attacks.

It is important to note that there were several high-profile attacks during the beginning of the year, including the taking down of the Austrian Parliament website (Pudwell, 2017) and rendering the Lloyd’s Banking online system unusable for several days (McCaskill, 2017). The unique thing about these attacks was not how they were conducted, but that no group claimed responsibility for them. Generally, DDoS attacks are either monetarily driven, or used to make a statement. These could have either been tests of power or growing concern by attackers about repercussions after several large groups were disbanded by law enforcement.

The second quarter of 2017 brought heavier DDoS attacks that were focused on making political statements. During the Qatar crisis, the middle-eastern news website Al Jazeera was brought to its knees by an attack aiming to prevent users from accessing articles on the site. In addition, several major French websites were targeted to prevent access during the height of the French presidential election. These incidents demonstrated how information could be controlled and even twisted by preventing access.

As money continued to be the driving force behind DDoS attacks, Q2 2017 saw a large spike in the trend of “Ransom DDoS”. Several groups claiming to have the power to disrupt major financial institutions demanded payment before attacks even started. One of the largest threats came from a group that calls itself Armada Collective in which they demanded over $300,000 from South Korean banks in exchange for not taking their online services down. This wasn’t the first threat from Armada, as the group has been active since 2015 but did not make the mainstream news much during 2016. The group has spawned many copycats making attribution extremely difficult. As a result, researchers have had a difficult time trying to pinpoint the capabilities of the groups making threats. Financial institutions continue to be the most frequently extorted groups as cybercriminals know that the institutions cannot afford disruptions. Many targeted institutions were willing to pay the ransom before attacks even started, as they had decided it wouldn’t be worth taking chances. This showed weakness, which led to even more groups attempting to profit from threats of DDoS.

This quarter demonstrated that companies perceived the DDoS attack threat as quite serious. This is likely due to fears following the largest DDoS attack to date being recorded late last year against Dyn DNS, and that attacks capable of taking down Microsoft’s Skype servers were observed during Q2 (ITV, 2017). Companies are fearful that the financial implications related to DDoS attacks could be worse than paying ransom. Some companies were prepared to pay ransoms upfront rather than waiting for anything to happen, spawning a slew of groups to issue similar demands. It’s worth noting that many of these were empty threats, and nothing ever came of the demands, but it is likely that a group with the right capabilities will eventually show itself with similar demands.

Trends that began in the first half of 2017 continued to evolve during Q3 of the year. The amount of DDoS attacks around the world increased, and the prices of solutions to protect against attacks followed suit. Attackers discovered a new vulnerability in hybrid and cloud technologies – dubbed Pulse Wave technology (Zeifman, 2017) – enabling them to increase throughput of attacks, and they began utilizing extremely short powerful attacks to disrupt services that could be spread out over several hours or days.

Cybercriminals’ targets of interest remained relatively the same, with attacks being directed for political or financial gain. The increase of activity in the political ring has even led to beliefs that DDoS attacks could be a form of democratic protest. This belief is probably flawed as, to date, DDoS attacks have been relatively ineffective in instituting change. Generally, attacks have only brought victims into the spotlight, while leaving the reasoning for the attack out of the discussion.

Ransom DDoS continued to be a problem for many companies. Due to the success in the previous quarter, more and more groups attempted to use the same extortion techniques. Though they usually weren’t successful in extorting companies for ransom, it still caused problems for many organizations. In an effort to weed out the fakers, more prominent groups switched to a new technique for limiting the damage and pressure the victims into paying the ransom.
extortion. The group would initially demonstrate force by taking a website offline or disrupting services for a short period of time before demanding ransom. One of the most prominent examples of this during Q3 was the Americas Cardroom online poker site. The attackers disrupted play on the website, and then demanded a ransom. When management of the site refused to pay the ransom, they were forced to delay a championship poker tournament due to the incident.

Also of note this quarter is the lingering effects the release of the Mirai botnet source code has had. During the first half of 2017, attackers had not been able to leverage exploits even close to the strength of the Dyn attack. Likely due to the fact that cybercriminals had to rebuild botnets back up to sizable levels, it wasn’t until Q3 that significant attacks were seen utilizing Mirai. Akamai noted that they began seeing large attacks with fingerprints extremely similar to the Mirai botnet. While not as large as the 623 Gbps attack occurring in Q3 2016, these attacks were no slouch and could be extremely disruptive to any organization.

One of the biggest successes of the year in combating DDoS attacks occurred during Q3 with the takedown of the WireX botnet (Thomson, Tech firms take down WireX Android botnet, 2017). The botnet was comprised of hundreds of thousands of Android devices in more than a hundred countries. The botnet was identified proliferating itself via legitimate Google Play applications that were trojanized, and had been overlooked by Google’s Bouncer system. Bouncer is a machine learning system charged with finding and blocking malware-laden applications from the Play Store, but the system has had a rough time of it this year with several high-profile pieces of malware getting through undetected. The takedown of WireX required joint work between Google, Samsung, and several large IT security vendors.

Q4 Q4 was the quietest part of 2017 as far as the number of incidents went, but was probably the most significant in the fight against DDoS attacks and the actors behind them. In addition, as cryptocurrency entered the mainstream spotlight due to surging prices, it also fell victim to the effects of DDoS attacks and showcased the effects disruptions can have on the different currencies. As new currencies were released, such as Bitcoin Gold (BTG), websites were hammered by DDoS attacks. Researchers believe that due to the new currency and the fluctuation it caused in Bitcoin, attackers were attempting to capitalize through market manipulation by disrupting normal services.

In December 2017, news of a large joint effort to take down the Andromeda botnet emerged. The operation involved police in 15 countries in an effort to break up the network. The botnet was mostly used to spread additional malware as well as steal credentials from home users. The secondary malware included Neutrino bot, used to conduct DDoS attacks. Authorities said that during a 48 hour sinkholing, during which they commandeered the command and control addresses to monitor for communications, approximately 2 million unique Andromeda victim IP addresses were captured. Officials believe that this was only a fraction of the total machines infected. The takedown shut down operations of one of the largest for-profit and for-hire groups that were active (Solomon, 2017).

The takedown of Andromeda wasn’t the only step taken in the fight against DDoS and botnet activity. Late in the year, several high-profile actors behind some of the most famous DDoS attacks in recent history were charged with their crimes. In mid-December, three defendants confessed to be the masterminds behind the Mirai botnet – Paras Jha, Josiah White, and Dalton Norman (Krebs, 2017). The three were not thought to be involved in the Dyn attack of 2016 which took down several major US websites, but were indicted for their creation of the tool. The culprits of the attack remain at large.

In late December, the founders of the groups Lizard Squad and PoodleCorp – known for their antics against popular video game servers and personalities – were convicted for their involvement in destructive attacks dating back to 2014. Zachary Buchta from the United States and Jan Willem van Rooy from the Netherlands were sent to prison as well as required to pay back losses to some of the businesses affected by their attacks.

Even with these takedowns and attests in 2017, it is expected that these types of exploits will not slow. This year will likely follow similar trends to previous years as more and more vulnerabilities are discovered and utilized to create botnets. The for-profit model is becoming simpler for cybercriminals to maintain as botnets large enough to do serious damage are becoming accessible to those wishing to do so. We also expect that with the downfall of larger groups, there will be others who will attempt to step into the spotlight. 2017 was a quiet year for “DDoS crews” to make themselves known, compared to years prior, and it is likely this will continue to be the case. The motivations behind DDoS attacks will likely stay...
the same, typically involving financial gain or as a protest to decisions being made around the world; but, after witnessing the trouble and attention “fame” brings, it is probable that groups will attempt to stay underground, only offering their services to those they trust or those with deep pockets.

**Mitigations:**

- Ensure proper mitigation techniques or services are in place for protection.
- Create and implement a comprehensive backup plan should services be disabled by attackers.

**2018 Predictions:**

- We assess with medium confidence that major DDoS attacks will continue to be a problem for organizations of all size. As organizations continue to pay ransoms to avoid falling victim, actors will continue extortion techniques for financial gain.
- We assess with high confidence that DDoS attacks on a large scale will continue to be commonplace. With thousands of devices lacking proper security protections being connected to the internet each day, the possibility for massive DDoS attacks will grow throughout 2018.

**LESSER-KNOWN NATION-STATES**

Names such as Cozy Bear, APT1, and Lazarus are familiar in the information security world. They are commonly attributed to Russia, China, and North Korea respectively. With seemingly unlimited manpower and budget, they are what we think of when someone mentions an advanced nation-state threat. Last year, saw security incidents such as the DNC hack, WannaCry, and NotPetya. While these stories make waves in the headlines, many of the less glamorous incidents go all but unmentioned.

Lacking the resources and toolkits of the big players, some smaller groups have come up through the ranks recently using more ‘traditional’ means. Don’t let what is trending in Twitter dissuade you, groups backed by smaller nation states as well as groups from unknown origins were very much active throughout 2017. Using mostly open source and built-in tools, they are still successfully accomplishing their mission without the zero-day exploits or advanced targeted campaigns of larger groups.

One of the more notable groups in 2017 was the Lebanese General Directorate of General Security, or Bld3F6. They were identified as being behind the Dark Caracal attacks in which the group used various techniques to harvest data. Then, watering hole attacks were employed to host spyware masquerading as various legitimate application updates. Fake mobile apps were uploaded to 3rd party application stores to harvest data off mobile devices. By hosting these malware laden applications, successful data exfiltration amongst thousands of mobile devices and endpoints was possible without much effort. Information was gathered from multiple sources that were seemingly unrelated. Because of this, it is difficult to attribute their actions to a particular end goal or target (Satter, 2018).

**The Dutch** also gained some media attention last year with their support in validating the Russian involvement in the DNC hack. It is unknown how they gained access to the Russian internal network, but they managed to gain control of security cameras that were able to watch the Russians in action. Most notably it was reported that the Dutch group had access as far back as 2014 (Noack, 2018).

Another group of unknown origin dubbed Dragonfly has been back in the scene during 2017 as well. Now referred to as Dragonfly 2.0, they have been seen using open source malware and techniques to infiltrate utility companies in the western United States. They have been successful with social engineering tools such as Phisery to gain access to targeted networks. Once a foothold is established, they use administrative tools such as PowerShell and PsExec to move laterally and establish persistence (Starkey, 2017).

Regardless of the differing agendas, these groups do have some commonalities that are trending upwards. All the groups mentioned are leveraging open source tools and less sophisticated attacks with great success. Tactics such as using watering holes that provide malicious Java, Flash and mobile applications are being used to gather sensitive data while possibly masking what the true target of the campaign could be. Social engineering tools available on GitHub and Kali Linux seem to be the standard for penetrating the perimeter. Lateral movement and persistence are accomplished by “living off the land” techniques, which is when the actor uses available administrative tools such as PSEnc and PowerShell to strengthen their foothold while hiding in everyday network noise.

The low level of technical knowledge needed to carry out these successful attacks should be a cause for concern amongst security professionals going into 2018. These groups have shown that the bar for conducting successful operations is not as high as one might think, and that they can hide within the noise of modern day networks.
### Descriptive Statistics of Countries Involved in Nation-State Activity

<table>
<thead>
<tr>
<th>Country</th>
<th>Agency</th>
<th>Population</th>
<th>Per Capita GDP</th>
<th>IDI</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>NSA</td>
<td>325,719,178</td>
<td>$61,687 (11th overall)</td>
<td>8.18 (16th overall)</td>
</tr>
<tr>
<td>Russia</td>
<td>FSB</td>
<td>144,526,636</td>
<td>$28,198 (49th overall)</td>
<td>7.07 (45th overall)</td>
</tr>
<tr>
<td>China</td>
<td>3rd Dept. of the GSD</td>
<td>1,403,500,365</td>
<td>$16,624 (77th overall)</td>
<td>5.60 (80th overall)</td>
</tr>
<tr>
<td>Lebanon</td>
<td>GDSD</td>
<td>6,006,668</td>
<td>$19,128 (80th overall)</td>
<td>6.30 (64th overall)</td>
</tr>
<tr>
<td>Netherlands</td>
<td>AIVD</td>
<td>17,600,671</td>
<td>$44,654 (13th overall)</td>
<td>8.49 (7th overall)</td>
</tr>
</tbody>
</table>
for as long as needed. These groups seem to thrive at maintaining low levels of persistent access, possibly waiting for the release of the next exploit to further their positioning.

While we cannot be sure of the specific goals that each of the groups mentioned above are trying to accomplish, it is very likely that 2018 will see an increase amongst players at the table. Living in the shadows of the Vault 7 toolset leak (MacAskill, Thielman, & Oltermann, 2017) and large ransomware scares, in 2017 these smaller groups have shown us just how easily initial access can be achieved and how long that access can be maintained.

**Mitigations:**

- Conduct regular, recurring phishing awareness training.
- Define and implement a comprehensive update policy.
- Downloads need to be verified, and when possible, only pushed to devices via management software.
- Mobile applications should only be installed from reputable stores.

**2018 Prediction:**

- We assess with high confidence that open source tools will remain popular with cyber threat actors operating on a budget.
- We assess with medium confidence that lesser-known threat actors will become more disruptive as they refine tactics.
DDoS attacks are an old phenomenon. The first DDoS attack dates to 1974 (Radware, 2017). They were always a malicious way to disrupt or shutdown an online service for various reasons. In the early days, DDoS tools required certain skill to write, distribute, and execute to successfully implement a coordinated attack.

As the Internet evolved, and the capacity of sites to handle thousands then millions of requests per second grew, so did DDoS attacks. Attack infrastructure needed to evolve to gather more resources to successfully execute a meaningful attack. Building and maintaining botnets to provide the infrastructure needed for such attacks became a technologically demanding job. As cyber criminals who operated their own botnets functioned more as businesses, it became advantageous to them to sell their services to the highest bidder, instead of employing the tools on their own. This fundamentally changed botnets from just a means to an end to the end unto themselves.

Thus came the age of commodification. In the last few years, criminals established a cybercrime business model. More sophisticated and skilled hackers focused on building the infrastructure for DDoS attacks and attached them to professional web interfaces while offering their services to less technically inclined hackers. This mirrors closely the development of the software-as-a-service (SaaS) market among legitimate IT companies. As the main cost of erecting the infrastructure for these attacks fell on those so called “Vendors”, they could focus on selling their DDoS services according to certain criteria.

Criteria for DDoS attack pricing:

1. **Number of Attackers**: 10 bots, 100, bots, 1000 bots

2. **Lease Period**: day, week, month

3. **Attack Bandwidth**: 500Mbps, 5Gbps, 50Gbps

4. **Types of Target**: Personal/Home Router, Small-Medium Businesses, Big Businesses, Governmental authorities

The vendors themselves vary greatly. Some of them are reputable and reliable, and some of them are small vendors running their operation as partners of the big vendors. As the darknet goes, some vendors are just scammers, selling services they cannot supply and tricking unsuspecting users into paying for services they will never get.
Some vendors won’t deal with big businesses or governmental agencies, as they do not want to draw the attention of law enforcement agencies to their existence, or just lack the technical infrastructure to perform such attacks. Other vendors will avoid attacking certain states (usually their state of origin and other neighboring states) to avoid their local authorities. Except for the basic services offered, other services offered are additional charges, according to the hassle for the hacker: support services, rebuilding payloads or network resources, and attacking high value/risk targets. Some vendors will help you to learn the system from scratch; others will just sell you the access to system and will leave you to learn for yourself.

As in any other service, the quality of the product is a key factor. In darknet forums where nobody knows who is who, the problem is compounded by an inability to associate online personas with claimed attacks. So as with any other service, testimonials from satisfied customers are important to evaluate the quality of the service that is given. Other users who bought the service comment on the quality of the service, price, the responsiveness of the vendor to problems and requests, and the overall happiness from the service. Prices range from $5 for an attack lasting minutes, to hundreds of dollars for a coordinated sustained attack of thousands of bots (see Figures 9, 11, and 13).

Some known and reliable markets also certify some members with a “Site Approved Vendor” mark in order to further strengthen the reputation of the service. And as with any other commodity, there are also end of year sales and discounts, or even refunds in case of any mishap or problem (see Figures 10–11). Some vendors will give away free licenses if a known user agrees to write a review of their product (see Figure 12), others will advertise their products by showing off their latest attacks as a demonstration of their capabilities (see Figure 13).
Secondary markets exist among buyers of DDoS services who barter and resell unused or partially used licenses. Their different motivations for attack are also a concern for the different vendors, as they want to know how to market their products and to which crowds. Buying a DDoS service by a business to attack its competitor isn’t a farfetched idea (see Figure 14). The thinking goes that if two competing companies offer similar services then the one with the better uptime is the superior choice.

The impact of this evolving ecosystem is making cybercrime affordable, anonymous, and more accessible. Putting exploit tools like these in the hands of whomever can afford it is a recipe for disaster. As commodification keeps intensifying, we foresee that the amount of DDoS attacks will become more prevalent, but also more focused, as to represent the different intentions and motivations of the attackers/customers.
Being aware of the latest threats and vulnerabilities in order to protect our organizations is a responsibility that falls to many – from the board room to the server room and everywhere in between. Intelligence estimation for 2017 was difficult due to unprecedented vulnerabilities like KRACK and the EternalBlue exploits as well as the focus of cybercriminals on new approaches like cryptojacking while nation-states both large and small saw their CNO programs disclosed.

But regardless of these new vulnerabilities, old threats and attacks vectors are still present. Even as black swan events happen, phishing attacks are common and cheap to execute. We continue to embed IoT devices in every aspect of our lives with little consideration to the risks they pose. Ransomware becomes a larger force to reckon with, affecting infrastructure availability and real loss of business for many organizations.

In an uncertain security environment, cyber threat intelligence is one way to gain a footing and understand the lay of the land. The art behind successful security operations lies not only within people, process and technology, but within the ability to make good, judgement-based decisions. Intelligence is all about gaining advantage over cyber adversaries and influencing decision making from the Threat Analyst to the Board of Directors.

Threat intelligence advocates for studying the wider world and thinking critically about how the lessons learned can be applied to our own lives. At Optiv, we believe that Threat Intelligence is more than just a list of IOCs or threat feeds. True Threat Intelligence should be relevant and supportive of the decisions people make in terms of risk and protecting their organization.

The Optiv gTIC will continue to work to improve the security posture for ourselves and our clients by bringing this knowledge and these lessons home. For more information on how you can apply Optiv gTIC intelligence, visit https://www.optiv.com/services/threat-and-vulnerability-management/cyber-threat-intelligence.
INTSIGHTS

As a contributor to the Optiv 2018 Cyber Threat Intelligence Estimate, IntSights brings together threat intelligence coming from the dark web using an array of advanced intelligence skills and the expertise of its analysts. IntSights infiltrates the dark web to detect and analyze planned or potential attacks. The IntSights intelligence team is comprised of experienced analysts with a rich background in cyber intelligence and intelligence collection. IntSights provides customers with a one-stop-shop solution combining rapid and actionable intelligence, threat-intelligence, research platforms, threat mitigation and remediation.

The company was founded by veterans from elite military cybersecurity and intelligence units, where they acquired a deep understanding of how hackers think, collaborate and act. All backed by Blumberg Capital Partners, Blumberg Capital, Blackstone and Wipro Ventures.

CONTRIBUTORS

Ariel Ainhoren, Cyber Threat Intelligence Researcher, IntSights
Mike Devegas, Senior Intelligence Analyst, Optiv gTIC
Jonathan Drake, Intelligence Analyst, Optiv gTIC
Courtney Falk, Senior Research Scientist, Optiv gTIC
McKade Ivancic, Malware Analyst, Optiv Malware Analysis and Countermeasures
Itay Kozuch, Director of Research, IntSights

REFERENCES

Want to learn more?

Insight on Cyber Threat Intelligence is an ongoing series of thought leadership at Optiv. Click the links below to download other corresponding materials on the subject.

Cyber Threat Intelligence-as-a-Services
At-a-Glance Brief