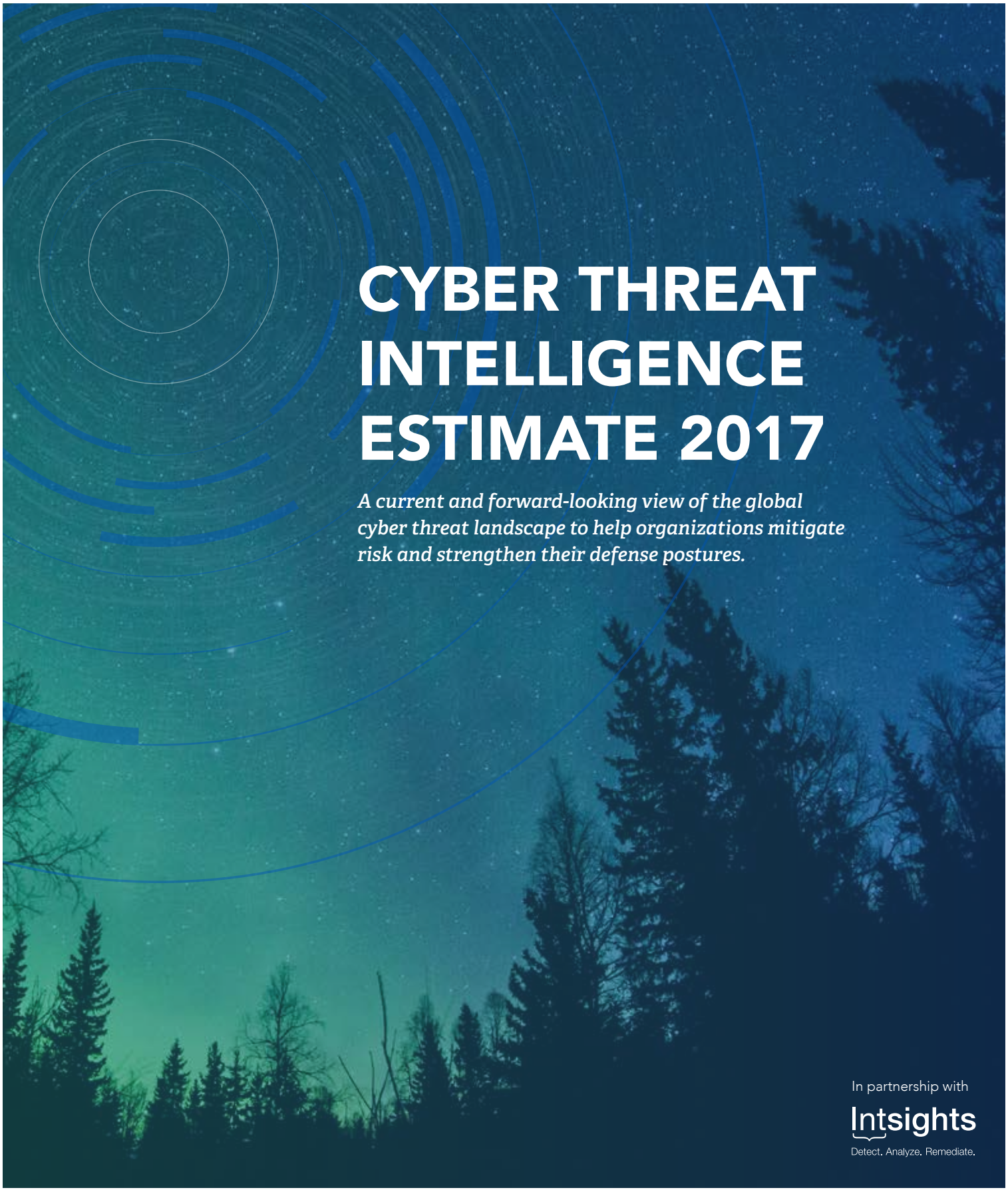
OPTIV



CYBER THREAT INTELLIGENCE ESTIMATE 2017

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

In partnership with

Intsights

Detect. Analyze. Remediate.

TABLE OF CONTENTS

PROPRIETARY AND CONFIDENTIAL. © 2017 OPTIV SECURITY INC.

INTRODUCTION

The 2017 Optiv Cyber Threat Intelligence Estimate is part analysis and part forecast. The analysis portion dissects the security themes seen in 2016 while the forecast extrapolates the analysis through the subsequent 12 months. This is modelled after the National Intelligence Estimate, which is a classified report provided to the Congress of the United States.

The goal for Optiv's report is to provide guidance to policy makers, influence strategic decisions concerning security operations, and provide situational awareness on the state of cyber security. Optiv believes that cyber threat intelligence has a role to play in supporting security operations by:

1. Performing situation development
2. Supporting organizational and asset protection
3. Providing indications and warning
4. Enabling machine readable threat intelligence

Optiv's report consists of three main sections. **The first section discusses threats that focus on particular business verticals.** Optiv organizes and examines its clients according to which business vertical they fit in. Knowing other like companies can aid in security awareness when new threats emerge and start to spread through a vertical. Some cyberattack campaigns are specifically focused on a particular vertical or set of verticals. **The second section deals with threat actors.** Threat intelligence is first and foremost concerned with identifying actors, their intentions, and targets. **The final section deals with tools and techniques.** When the threat intelligence picture is incomplete, there is still value to be found in threat indicators that alert on the presence of these tools and techniques.

Some themes of this report are general and cut across the sections previously outlined. Chief among them are:

1. Criminals are becoming increasingly specialized in a particular field and commodifying their services.
2. The traditional understanding of threat actors is becoming blurred as actors perform attacks typically associated with other roles.
3. The main driver behind malicious activity remains to be for financial gain.

If the theme of 2015 was supervisory control and data acquisition (SCADA) systems and industrial control systems (ICS), then the theme of 2016 was the use of cyber methods to facilitate social action. Neither theme was unprecedented. For SCADA and ICS, awareness of potential attacks built gradually over time. In 2007, the Idaho National Labs proved with their Project Aurora work that cyberattacks, used to manipulate SCADA systems, can have real world, physical effects. The Iranian Stuxnet incident of 2010 created fear about cyber weapons infecting critical systems worldwide. Then, 2015 had the Sandworm Team shutting down power for an entire region of Ukraine.

VERTICALS

Severity and type of cyberattack varies across industry verticals. Optiv Managed Security Services data from escalated tickets show that our clients in the financial and retail verticals lead other verticals in terms of the number of remote network attacks and malware infections that they observe.

Healthcare

By number of malware incidents, healthcare was among the top two targeted verticals among Optiv clients for all four quarters of 2016. Healthcare attracts attackers looking for personally identifiable information (PII) because healthcare providers have a treasure trove of it, including social security numbers, birth dates, and other financial and insurance data. Ransomware campaigns also targeted this vertical throughout 2016. For ransomware attackers, the allure of the healthcare sector comes from the sense of urgency. Healthcare providers need to access patient data frequently and quickly in order to maintain quality of care. Being unable to do so not only has regulatory consequences, but also risks lives. Healthcare was such an attractive target for ransomware attackers in 2016 that a major strain, SamSa, focused specifically on that industry. Though SamSa is the prominent ransomware strain that targets healthcare, it is not the only one we saw in the vertical during 2016. More general-purpose malware strains, often transmitted via infected macro-enabled Microsoft Word documents, affected the healthcare sector as well.

Financial Services and Insurance

In addition to healthcare, the financial services and insurance vertical saw a large portion of malware activity throughout 2016. Most malware campaigns in the wild have a financial motivation. Successfully attacking businesses in this sector can provide direct access to money, or can provide personally identifiable information that can lead to financial gain in the future. Many of the malware incidents associated with those companies involved information stealers, including continued Pony and Vawtrak campaigns. Like the healthcare sector, and all other sectors, the financial services and insurance sector also saw ransomware activity across the year. Common infection vectors in this sector included macro-enabled Microsoft Word documents as well as exploit kits that target unpatched browsers and Flash plugins.

Tech, Media and Telecom

Tickets generated from IntSights-collected intelligence show telecommunications companies to be the most frequently discussed topic among hacker black markets. Combined with electronics companies, the two groups account for 40 percent of such tickets. For less than $10, someone with access to the right forums can purchase a hacked user account. Buyer beware, however, because sellers of hacked accounts do not guarantee much in the way of the services to which the account has access. Compare this to selling credit card and bank accounts where the seller often makes a claim about how many accounts are still active.

Optiv's Escalated Tickets for Remote Network Attacks in 2016

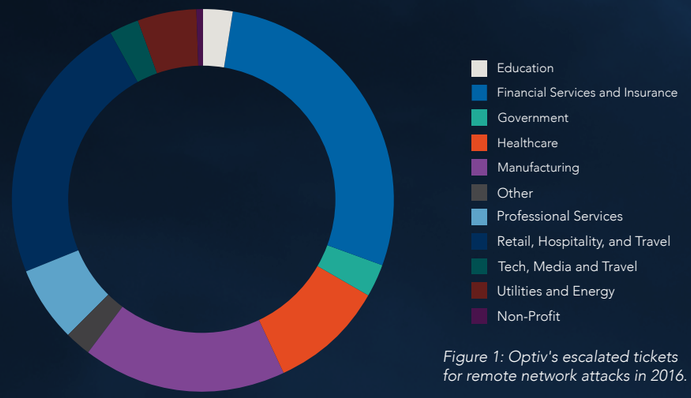


Figure 1: Optiv's escalated tickets for remote network attacks in 2016.

Optiv's Escalated Tickets for Malware Infections in 2016

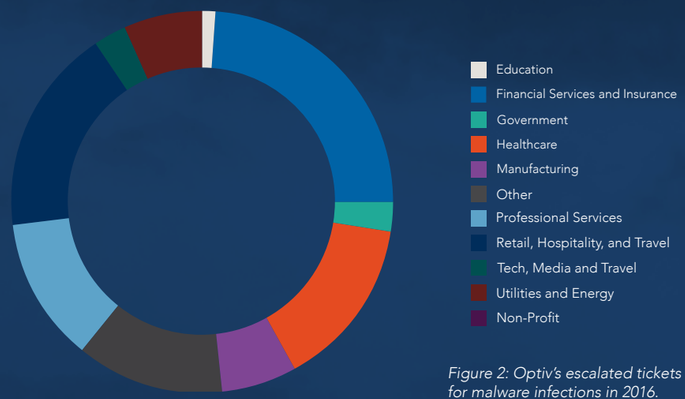


Figure 2: Optiv's escalated tickets for malware infections in 2016.

Black Market Alerts Generated by IntSights Based on Darknet Collection in 2016

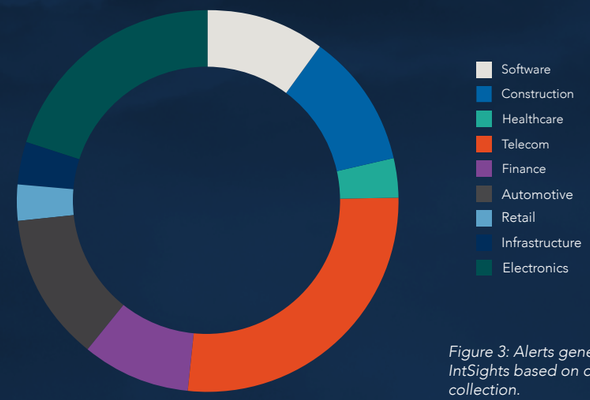


Figure 3: Alerts generated by IntSights based on darknet collection.

Alerts Generated by IntSights Based on Threat Type Across Verticals in 2016

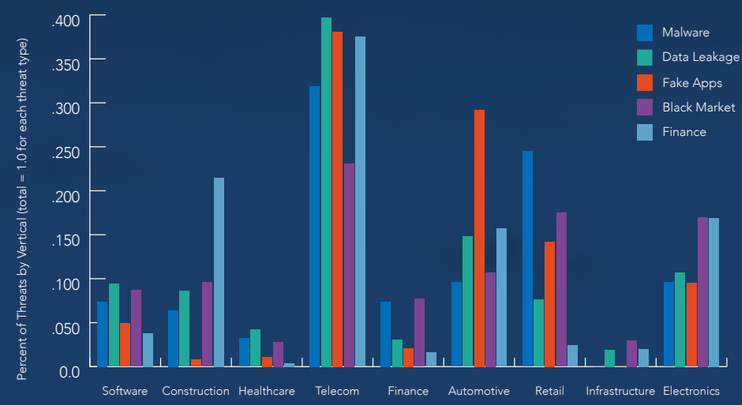


Figure 4: Alerts generated by IntSights based on threat type across verticals.

THREAT ACTORS

When security professionals talk about threat actors, they tend to use the same fixed list of categories over and over again. These definitions were never very robust to begin with. But current trends show how the lines between the traditional categories of threat actors are blurring, making it difficult to have meaningful conversations about threats and current events.

Cybercrime

Yesterday's script kiddie is today's underground entrepreneur. Not all young hackers stop at copying and pasting instructions they find on forums, or downloading and running tools with GUIs. Some script kiddies take their lessons learned to build upon their success.

The Lizard Squad hacking group embodies the theme of threat evolution. Lizard Squad specializes in distributed denial-of-service (DDoS) attacks. Their most infamous attack took place during the Christmas holiday of 2014 when they took down several large game manufacturer networks. This attack was so visible that it incited copycats Phantom Squad to attempt to recreate the DDoS during the Christmas Holiday of 2015 with limited success.

Lizard Squad was emboldened by their notoriety. They took the capitalist spirit to heart and began marketing DDoS-as-a-service under the PoodleCorp brand (Krebs, 2016). Fortunately for the general public, arrests of PoodleCorp/Lizard Squad members in Maryland and the Netherlands halted their criminal endeavor.

Figure 5: PoodleCorp's order page with pricing in US dollars (image credits to KrebsOnSecurity.com)

Nation-State

2015 showed nation-state actors using cyber-physical effects; cyberattacks with consequences in the physical world. One of Ukraine's regions went dark when a utility company's automated systems were taken offline. After the Stuxnet attack, Ukraine is the first confirmed situation where a cyberattack directly affected a civilian population.

The trend in 2016 was moving from cyber-physical to cyber-social; manipulating online resources to affect social change. Nation-state actors took notice when hacktivist strategies of data theft were coupled with public shaming. A recent example of this is when Russian actors at least partly succeeded in their goal to create confusion and discord in the 2016 U.S. presidential election (Department of Homeland Security, 2016) (Able Squadron, 2016). This should come as no surprise because the idea was put forward by Russian thinkers years before the presidential election (Dubovitsky, 2014).

The concern in 2017 is that nation-state actors are no longer content with indirect cyber-social attacks and instead resort to direct election interference, manipulating or corrupting vote tallies to destroy confidence in the fairness of the democratic process. There are already concerns about Russian interference in the French and German elections of 2017.

Hacktivist

Hacktivists commit cyberattacks to support an ideology or belief system. There are any number of hacktivist ideologies such as social justice, religion, ecology, or national pride. Different types of threat actors can masquerade as a hacktivist group by pronouncing a particular ideology in order to distract from their real intentions. This deception improves security operations for the attacker while complicating attribution for the defenders.

Hacktivism began with website defacements. When the Chinese embassy in Belgrade, Serbia was accidentally hit by American bombs in 1999, pro-China hackers modified a website belonging to U.S. government agencies as a protest. Once botnets grew and matured they enabled DDoS attacks. And now the latest trend of hacktivism, theft and exposure of confidential data. This new form of attack serves the purposes of boosting the image of the hacktivist group while simultaneously airing sensitive and potentially damaging information.

Anonymous is one of the best recognized hacktivist groups, known for their high-profile attacks. It is often reported that Anonymous lacks a formal hierarchical command structure. Anonymous is more of a brand where hackers can self-organize into like-minded ad hoc sub-groups.

The abridged list of Anonymous' 2016 hacks shown in Table 1 indicates a diverse target set with a slant towards pro-Western ideals of social justice. Islamist groups are targeted for attacking civilians, large corporations are targeted for greedy practices and organizations with different political leanings are targeted for pursuing policies that Anonymous members feel are contrary to liberal democracy.

A key part of threat intelligence is being aware of how decision making impacts exposure. An organization should consider how the way it operates might bring it into conflict with the ideologies of different hacktivist groups. For instance, a bank may be primarily concerned with fraud and other forms of cybercrime. But if that bank begins investing in petrochemical companies they may find themselves targeted by ecology-focused hacktivist groups for enabling environmental exploitation.

Event	Motivation	Target
#OpISIS	Vigilante/Revenge	Islamic State (ISIS)
#OpWhales	Environmentalism	Japan, Iceland
#OpNice	Vigilante/Revenge	Terrorist accomplices
#OpOlympicHacking	Social Justice	Rio 2016 Summer Olympics
#OpKillingBay	Environmentalism	Japan, Faroe Islands (Denmark)
#OpParis	Vigilante/Revenge	Terrorist accomplices
#OpKKK	Social Justice	Ku Klux Klan
#OpTrump	Political	Donald Trump

Table 1: Anonymous campaigns during 2016

TOOLS AND TECHNIQUES

Each category in the Tools and Techniques section begins by highlighting the business verticals most likely to be affected by that tool or technique. The category then closes with a list of suggested mitigations that concerned organizations can implement to best protect themselves.

Phishing

Phishing attacks are an area of cybercrime that has matured greatly. In the past, phishing required advanced technical skills. Nowadays every part of a phishing attack can be bought on the black markets, or downloaded and copied from cybercrime forums, lowering the barrier of entry for conducting a phishing campaign.

An impersonation phishing scam requires several components in order to successfully harvest user credentials:

1. Fake Domain: preferably deceptively similar to a known good site
2. Fake Login Page: preferably one that resembles the original
3. SMTP Server: one of several methods to send a large amount of spam (In all of these methods it is difficult to determine the original attacker)
4. Bulk Mailer Software
5. Leads: lists of target email addresses

The black markets offer SMTP servers, email lists per country, and phony login pages with many different types of targets from banks to email providers and social networks. Cybercrime forums are filled with "beginner guides" that include a step-by-step description of the phishing scam, and lists of free web hosting servers, URL hiders, and recommended sites at which to phish. The only thing required is to find a forum and register (Figure 6).

Figure 6: An ad from a cybercrime forum that advertises for phishing resources.

Figure 7: Hacking forum advertisement for all the components of a spam campaign.

From DIY to a Service Offering

The current trend in phishing attacks is towards using phishing-as-a-service (PhaaS) systems, which lower cost and make phishing campaigns more accessible than ever.

In the past, attackers on the hunt for credentials had to utilize an array of operations such as building a scam website using HTML, CSS, and PHP in order to avoid search engine recognition. The attackers also had to obtain a server in order to host the phishing website, and an SMTP server used to send massive amounts of emails. These emails went out to addresses taken from a bulk email list bought online, or a carefully crafted list of targets belonging to a specific company or organization (spear phishing).

The proliferation of phishing campaigns created a booming secondary market for spamming tools. The potential profits of a phishing campaign made it worthwhile for attackers to buy the various required tools online instead of creating them for themselves (Figure 7).

PhaaS is a full-kit solution for attackers, covering a domain, scam page, and database for the received credentials. A new store on the Russian black market opened in 2016, offering a complete solution for the beginning scammer, which includes all the necessary components.

Once a user logs into his account on the store, he can choose from a variety of scam pages. After the page is chosen, the site generates a link to be sent to an intended victim, and the credentials are stored on the user's dashboard. Some pages are provided for free, whereas for other fake pages, one must buy a VIP account (Figure 8).

Research conducted by IntSights and Imperva showed that PhaaS is redefining market pricing. As our below calculations show, it can cut the costs of a standard phishing campaign up to a quarter of current prices if you consider the cost of the services. Once you add the labor costs, PhaaS can be more than twice as profitable as an unmanaged (DIY) service option. Also, one could run several managed campaigns simultaneously even if they are new to the business of phishing.

	Managed (PhaaS)	**Unmanaged**
Minimum Cost	$4.20	$27.65
Account Value:		
Value Per Account	$0.01	
Average Stolen Accounts	14,000	
Total Value	$140.00	
Hourly Labor	½ hour at $15 = $7.50	4 hours at $15 = $60.00
Profit	$128.30	$52.35

Table 2: Comparing the costs of an unmanaged phishing campaign against a managed one.

Mitigations

We recommend regular and periodic security awareness training for all members of the organization. There are multiple companies today that specialize in evaluating the success of training efforts.

2017 Forecast

- Phishing will continue at historical levels. Changes to the phishing ecosystem only facilitate its continued success.

- Demand for PhaaS continues to rise, creating a higher rate of return for attackers.

Figure 8: Advertisement for VIP-level PhaaS services with prices in Russian rubles.

Ransomware

Most Affected Verticals

- Financial Services and Insurance
- Healthcare

Ransomware events often go hand-in-hand with phishing attacks. Phishing is the preferred mechanism for distributing ransomware. Some less common distribution channels involved exploiting web servers and embedding ransomware with the existing content (Green, 2016).

If 2016 was a year characterized as "the year of ransomware," 2017 is expected to see a rise in the use of simpler and cheaper extortion methods to enable the engagement of distributors with low technological capabilities. Attackers are actively looking for simpler and more cost efficient ways to gain the same profit. Ransomware already left an impact that prepared the ground for these simple extortion schemes. Monitoring of hacker conversations shows that the use of less expensive methods to extort an organization is becoming more popular.

A good example for such extortion methods is the Armada Collective, a cyber-crime group who threatened their victims with massive DDoS attacks on the scale of 500 Gbps to 1 Tbps if they did not pay their "protection fee". The group went silent in November 2015, but since then many copycats pretended to be Armada Collective members, sending extortion emails to organizations all the while not following through on their threats (Prince, 2016).

Figure 9: Hackers on a forum discussing the effectiveness of extortion.

Mitigations

- Have a verified backup and restoration policy in place both for data and machine images.

- Paying the ransom is an option, but it is no guarantee of a successful recovery. Organizations that consider paying the ransom should also consider how this might support the ransomware economy, encouraging attacks on other targets.

2017 Forecast

- Ransomware attacks will ebb and flow according to which techniques they utilize in infecting and encrypting data.

- Extortion attacks will gain in popularity due to their low risk. Extortion will only lose popularity once a majority of organizations have sufficient preparations in place to feel confident in rejecting extortion demands.

Targeting Third Parties

Most Affected Verticals

- Professional services
- Healthcare
- Financial

Third-party attacks are multi-stage operations. An attack on a third party looks to exploit a trust relationship with the intended target. The third party is entrusted with access or resources critical to the intended target's business. Examples of trusted assets include:

- **Direct access to networks or network credentials**
- **Sensitive personal information (healthcare, bank accounts, intellectual property, etc.)**

Third-party attacks are not a new development. In recent years there have been highly publicized breaches where attackers found their way into corporate networks by stealing credentials from service providers (Kassner, 2015). This threat vector continues to be a problem across multiple business verticals.

Targets in third-party attacks vary widely. Data from SurfWatch shows that over half of third-party cyber-attacks were tied to software, IT services, consumer lending, and healthcare companies (Peters, 2016). Other sub-verticals that had been linked to third-party breaches included professional associations, taxation, construction and engineering, and higher education (Peters, 2016). If a company's business involves gaining access to multiple clients' stores of personally identifiable or otherwise valuable information then they may be a target for an attacker taking the third-party route.

2016 data breaches in the healthcare sector happened not only at individual hospitals or doctor's offices, but also at third-party firms that manage and maintain patient records for multiple medical offices. Healthcare providers and insurance companies can find third parties to be attractive solutions to lessen the paperwork burden, but these third parties can cause severe liability if their security is not up to the standards that laws and regulations require of healthcare or insurance providers.

The financial sector is beset by attacks against its SWIFT messaging system. SWIFT is the Belgian-based, member-owned system for interbank transfers. $81 million was successfully stolen from the central bank of Bangladesh via SWIFT transfers, which was a fraction of the almost $1 billion the attackers attempted to take (Finkle, 2016). Since then attackers continue attempts to get on bank networks, access SWIFT, and send messages requesting money (Riley and Mullen, 2016). Increased security controls for SWIFT are on the horizon, but have neither been finalized nor implemented (Heller, 2016).

Not only are traditional financial institutions targeted; law firms specializing in mergers and acquisitions also find themselves the victims of breaches. For example several large corporate law firms have been attacked in an effort to steal data related to upcoming deals (Riley and Mullen, 2016). This type of information was likely targeted to enable insider trading and in at least one case became a high profile international incident (Smith, 2016).

Concerns about third-party attacks exist in the manufacturing sector as well. The United States Air Force has turned its focus to hardening its supply chain for the production of new aircraft and weapons in order to minimize the chance that state secrets will be stolen from the contractors entrusted with the design and creation of defense equipment (Drew, 2016). (Figure 10)

In the civilian manufacturing sector, automotive manufacturers have increased their attention regarding third-party security concerns.

Third-party attacks are a concern of the civilian manufacturing sector too. Members of the automotive sector formed their own information sharing analysis center (ISAC). The Automotive ISAC, like other sector-specific ISACs, advises manufacturers to consider risks associated with the supply chain (AUTO-ISAC, 2016).

Mitigations

- Vet the security practices of a third-party before entering into a relationship. Attackers often look to third parties because their security processes may be weaker than that of the intended target's.
- Enforce the principle of least privilege with the access granted to third-party partners. Determine who at the third party requires access, and ensure that they have been trained in the company's security practices and procedures. Document any and all accesses granted.
- Continuously monitor and audit accesses granted to partners. Ensure their actions are logged, and ensure that a SIEM has been configured to alert on suspicious activities such as privilege escalation attempts, attempts to connect to resources to which the account does not have access, outbound transfer of large amounts of data, or communications with suspicious domains or IP addresses not needed for business purposes.

2017 Forecast

- Third-party attacks are a part of the new normal. Because attacking a third party adds another link to the attack chain it will be seen more in situations where there is a single large valuable target or many small targets at once.

Figure 10: Chinese J-31: Danny Yu CC SA 4.0 International

American F-35A: MSgt John Nimmo Sr., Public Domain

Internet of Things

Most Affected Verticals

- Manufacturing
- Healthcare
- Tech, Media, and Telecommunications
- Utilities and Energy

Internet of Things (IoT) envisions a world where every device is network enabled. Your appliances may already have IP addresses along with your children's toys or even your clothing. IoT technology has the ability to increase productivity, decrease cost, and provide a wide array of services and solutions across every industry. But every new device introduced online expands a user's attack surface. Failing to secure IoT technology leaves systems vulnerable to exploitation. More than half of major new business processes and systems will include an IoT component by 2020 (Maddox, 2016).

2016 saw the largest DDoS in history when portions of a large DNS resolution service was taken off-line (Khandelwal, 2016). The impact of this attack was felt across the east coast of the United States as major sites and services using this service experienced unexpected outages and downtime. The culprit was the Mirai botnet, a botnet built from 175,000 compromised IoT devices. Manufacturers used a default set of login credentials, which attackers exploited in order to compromise the devices.

Once attackers settle on an attack vector, it is simple for them to find targets. Security-focused search engines like Shodan and Thingful index IoT devices and allow for quick discovery of potential targets. Thingful also allows for filtering based on the intended usage of the IoT device such as energy, home, environment and transport.

A 2015 breach at a large toy manufacturer leaked registered customers' personally identifiable information and download histories (Victor, 2015). Even more alarming, the breached data could allow attackers to target children. The toy manufacturer's representatives acknowledged the breach, but told customers that they would not be committing damage control resources. In addition to their online systems, the company produces toys with embedded IoT technology that if left unsecured could lead to future compromises.

Global markets for IoT embedded technology are projected to increase significantly over the next 10 years. Governments and organizations still lack certification, regulation requirements and guidelines on how to securely implement IoT. A study conducted by the Ponemon Institute found that 80 percent of IoT apps don't undergo testing for security vulnerabilities, contributing to more than a half million compromised devices (Abel, 2017). The study also reported that although concern has been expressed over IoT weaknesses, many manufacturers do not include a budget for implementing secure coding fundamentals, proactive testing, or encrypting databases and data transfers.

Mitigations

- Change default settings prior to deployment, especially passwords and account names.
- Don't unnecessarily expose IoT devices to remote access from the Internet. Placing them behind a NAT or firewall is ideal.
- Have adequate policies governing personal use of devices on organizational networks, including IoT devices.
- Where computing power supports it, use cryptographic and security protections endorsed by NIST.
- Software deployed on IoT devices should go through the same levels of tests as that of any other software package does.

2017 Forecast

- The novelty of an IoT-based botnet is a thing of the past. Expect at least one major IoT-facilitated security incident. DDoS attacks are the most likely scenario, but more powerful IoT devices are useful in cryptocurrency mining, SPAM email generation, etc.

Figure 11: Thingful's Homepage

Cryptography

Most Affected Verticals

- Manufacturing
- Healthcare
- Tech, Media, and Telecommunications
- Utilities and Energy

"Block chain" is the hot trend in cryptography. The block chain is a cryptographic concept first popularized with the Bitcoin cryptocurrency (Nakamoto, 2008). Since Bitcoin's success, researchers and entrepreneurs have searched for new applications of the block chain technology to other problems.

The decentralized autonomous organization (DAO) investment fund built their decentralized autonomous organization around the Ethereum block chain. Think of DAO as crowdsourced investment decisions. That was until a hacker found a logical flaw in the way that DAO processed transactions and made off with $50 million worth of the Ether cryptocurrency (Finley, 2016).

Block chain technology is also being applied to problems outside of finance. Secure online voting benefits from the verifiable logs provided by block chain models. Other projects want to use block chain as a mechanism to spur collaboration in research tasks as opposed to pure competition. A compromise of the core block chain technology would undermine these and more projects.

2017 Forecast

- Cryptocurrencies will remain a highly volatile currency option when compared to the fluctuations seen in more traditional currencies. Technical hurdles involved with getting and using cryptocurrencies will continue to hamper their mass market acceptance.
- The success of applications built upon block chain technologies ultimately depend on the rigorous examination of their models. Poorly tested and analyzed applications create new risks.

CONCLUSIONS

This report offers evidence and support to policymakers looking to improve their preparedness against cyberattacks. Threats facing computer networks continue to grow and evolve. Sometimes the evolution creates a more complex threat environment.

Attackers now look to exploit third-party trust relationships in order to gain access to their intended target. Sophisticated malware and phishing campaigns can be pieced together with little more than a modest bankroll.

But then there is evolution that leads to simplification. Success in ransomware attacks creates an environment of fear, uncertainty and doubt. Attackers can exploit that fear to extort money from victims who were never in any real danger but were worried about the consequences of not being prepared.

Organizations are charged with protecting their users and sensitive data. Cyber threat intelligence, when applied correctly, can support this mission through situation development, providing indications and warning of pending or successful attacks.

References

1. **Abel, R.,** 2017. 80 percent of IoT apps not tested for security flaws, study. [Online] Available at: https://www.scmagazine.com/iot-app-remain-untested-and-lack-of-urgency-to-fix-problem/article/632714/
2. **Able Squadron,** 2016. Russian New-Generation Warfare. Journal of Asymmetric Warfare, 1(2), pp. 1-8.
3. **AUTO-ISAC,** 2016. Automotive Cybersecurity Best Practices. [Online] Available at: https://www.automotiveisac.com/best-practices/
4. **Bergin, T. and Finkle, J.,** 2016. Exclusive: SWIFT confirms new cyber thefts, hacking tactics. [Online] Available at: http://www.reuters.com/article/us-usa-cyber-swift-exclusive-idUSKBN1412NT
5. **Brook, C.,** 2016. Massachusetts General Hospital Confirms Third-Party Breach. [Online] Available at: https://threatpost.com/massachusetts-general-hospital-confirms-third-party-breach/119000/
6. **Department of Homeland Security,** 2016. GRIZZLY STEPPE - Russian Malicious Cyber Activity. [Online] Available at: https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf
7. **Drew, J.,** 2016. USAF Wants Cyber-Hard Supply Chain For B-21. [Online] Available at: http://aviationweek.com/shownews/usaf-wants-cyber-hard-supply-chain-b-21
8. **Dubovitsky, N.,** 2014. Without the sky. [Online] Available at: http://ruspioner.ru/honest/m/single/4131 [Accessed 12 March].
9. **Finkle, J.,** 2016. Bangladesh Bank hackers compromised SWIFT software, warning issued. [Online] Available at: http://www.reuters.com/article/us-usa-nyfed-bangladesh-malware-exclusiv-idUSKCN0XM0DR
10. **Finley, K.,** 2016. A $50 Million Hack Just Showed That the DAO Was All Too Human. [Online] Available at: https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/ [Accessed 18 June].
11. **Green, A.,** 2016. New SamSam Ransomware Exploiting Old JBoss Vulnerability. [Online] Available at: https://blog.varonis.com/new-samsam-ransomware-still-exploits-old-jboss-vulnerability/
12. **Heller, M.,** 2016. SWIFT security controls to be mandatory by 2018. [Online] Available at: http://searchsecurity.techtarget.com/news/450305198/SWIFT-security-controls-to-be-mandatory-by-2018
13. **Kassner, M.,** 2015. Anatomy of the Target data breach: Missed opportunities and lessons learned. [Online] Available at: http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned
14. **Kellan, A.,** 1999. Hackers hit government Web sites after China embassy bombing. [Online] Available at: http://www.cnn.com/TECH/computing/9905/10/hack.attack.02/
15. **Khandelwal, S.,** 2016. Massive DDoS Attack Against Dyn DNS Service Knocks Popular Sites Offline. [Online] Available at: http://thehackernews.com/2016/10/dyn-dns-ddos.html [Accessed 21 October].
16. **Krebs, B.,** 2016. Akamai on the Record KrebsOnSecurity Attack. [Online] Available at: https://krebsonsecurity.com/2016/11/akamai-on-the-record-krebsonsecurity-attack/
17. **Krebs, B.,** 2016. Feds Charge Two In Lizard Squad Investigation. [Online] Available at: https://krebsonsecurity.com/2016/10/feds-charge-two-in-lizard-squad-investigation/ [Accessed 16 October].
18. **Maddox, T.,** 2016. Here are the biggest IoT security threats facing the enterprise in 2017. [Online] Available at: http://www.techrepublic.com/article/here-are-the-biggest-iot-security-threats-facing-the-enterprise-in-2017/
19. **Morgan, J.,** 2014. A Simple Explanation Of 'The Internet Of Things'. [Online] Available at: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#71f73eb81d09 [Accessed 13 May].
20. **Nakamoto, S.,** 2008. Bitcoin: A Peer-to-Peer Electronic Cash System.
21. **Peters, J.,** 2016. Supply Chains and Third Parties Continue to Cause Data Breaches. [Online] Available at: https://blog.surfwatchlabs.com/2016/07/28/supply-chains-and-third-party-breaches/
22. **Prince, M.,** 2016. Empty DDoS Threats: Meet the Armada Collective. [Online] Available at: https://blog.cloudflare.com/empty-ddos-threats-meet-the-armada-collective/
23. **Riley, C. and Mullen, J.,** 2016. Banks urged to tighten security as hacks continue. [Online] Available at: http://money.cnn.com/2016/08/31/technology/swift-bank-hacks/
24. **Shah, S.,** 2016. Large-scale IoT security breach coming in 2017, Forrester predicts. [Online] Available at: https://internetofbusiness.com/iot-security-breach-2017-forrester/
25. **Smith, C.,** 2016. MandA hack attack on 48 elite law firms. [Online] Available at: https://www.lawgazette.co.uk/practice/manda-hack-attack-on-48-elite-law-firms/5054524.article [Accessed 4 April].
26. **Stafford, D.,** 2016. Hundreds of thousands of Blue KC cardholders affected by data breach. The Kansas City Star, 5 August.
27. **Victor, D.,** 2015. Security Breach at Toy Maker VTech Includes Data on Children. The New York Times, 30 Novemer.

ABOUT

Optiv is a market-leading provider of end-to-end cyber security solutions. We help clients plan, build and run successful cyber security programs that achieve business objectives through our depth and breadth of cyber security offerings, extensive capabilities and proven expertise in cyber security strategy, managed security services, incident response, risk and compliance, security consulting, training and support, integration and architecture services, and security technology. Optiv maintains premium partnerships with more than 350 of the leading security technology manufacturers. For more information, visit www.optiv.com or follow us at www.twitter.com/optiv, www.facebook.com/optivinc and www.linkedin.com/company/optiv-inc.

Optiv Global Threat Intelligence Center (GTIC)

Optiv's Global Threat Intelligence Center expert staff of threat analysts performs advanced threat research and analysis that is leveraged by Optiv clients. By providing a set of threat intelligence deliverables, the GTIC enables Optiv clients to maintain a decision advantage over their adversaries and stay up to date on the latest threat landscape developments.

Contributing Partner: IntSights

IntSights offers a unified solution that presents customers with threat intelligence, mitigation and remediation measures, and research capabilities. The company was founded by veterans of military and intelligence cyber security teams, and is financially backed by Glilot Capital Partners, Blumberg Capital, Blackstone and Wipro Ventures.

Analytic contributions from IntSights describe the evolving ecosystem around phishing scams, which includes a thriving black market for cyber-criminals (see the Phishing section). Additionally, IntSights' data provided statistics of global security events used in analyzing cyber security trends for the upcoming year (see the Verticals section).

CONTRIBUTIONS

Courtney Falk
Optiv Global Threat Intelligence Center (GTIC)

Danny Pickens
Optiv Global Threat Intelligence Center (GTIC)

Jonathan Drake
Optiv Global Threat Intelligence Center (GTIC)

Nicolle Neulist
Optiv Global Threat Intelligence Center (GTIC)

Dane Disimino
Optiv Solutions Management

Roei Amit
IntSights

Tirza Bardach
IntSights

Ido Wulkan
IntSights

Irenne Zbarsky
IntSights

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 - Whitepaper

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

Cyber Threat Intelligence Program Workshop - At-a-Glance Brief

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

OPTIV

1125 17th Street, Suite 1700
Denver, CO 80202
800.574.0896
www.optiv.com