THREAT REPORT

FortiGuard Eye of the Storm

FortiGuard Eye of the Storm

Table of Contents

Purpose and Scope of Document

The primary purpose of this document is two fold. First, it presents threat data analysis and findings to show recent trends in cyber threats. Second, it offers contextual research insights and considerations for mitigating risks associated with cyber threats. Additionally, it summarizes the implications of cyber threats on current and upcoming 2016 global events. Our hope is that you find meaningful ideas to consider for your security strategy that will help elevate your security posture.

FortiGuard Labs

These risk and threat implications contained in this document are illustrated using FortiGuard's industry leading threat data, research and analysis. FortiGuard Labs consists of more than 200 expert researchers and analysts around the world. The researchers work with world class, in-house developed tools and patented technology to study, discover, and protect against breaking threats. The team has dedicated experts studying every critical area including malware, botnets, mobile, and zero-day vulnerabilities. Service analysts study breaking code and develop mitigation signatures while technology developers continually create new defense engines to combat continually evolving threats. FortiGuard Labs uses data collected from more than two million sensors around the globe to protect more than 270,000 customers every day.

FortiGuard Distribution Network (FDN)

The FDN is FortiGuard's sophisticated threat analysis fusion center and distribution network that powers the spectrum of Fortinet products and services. Additionally, this network supports compelling research that has been instrumental in creation of over 250 industry patents held by Fortinet. Furthermore it's used in collaboration with FortiGuard's law enforcement partners and government alliances around the world for proactive defense. The FDN is responsible for processing over 50 Billion web requests a day amongst other sensor threat telemetry. This processing includes the use of patented clustering algorithms to generate malicious patterns, behaviors and validated indicators of compromise.

Scope of Data Set

The threat data used in our analysis is based on a subset of the FDN telemetry data for the months of April, May and June 2016. The comprehensive data set spanning 126 countries was reduced to validated anomalies and malicious artifacts. These were then further analyzed to generate the principal data sets of interest which include the following:

Time frame: April, May, June 2016

Total number of artifacts: 2.2+ Billion

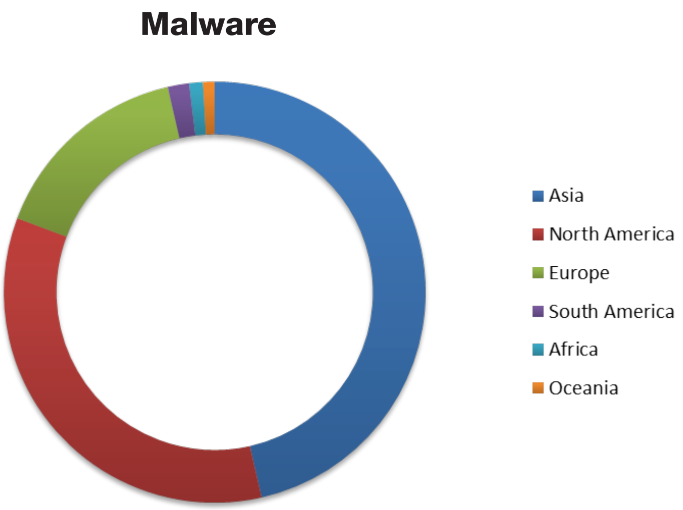
Total number of Malware hits: 59+ Million

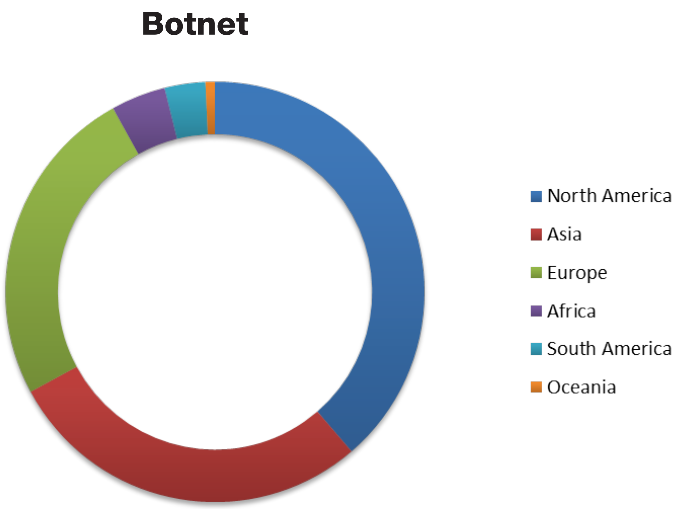
Total number of Botnet activity hits: 2+ Billion

Total number of Exploit Kits: 450+ Thousand

Total number of Countries: 175

Total number of malicious Domains and URLs: 40+ Million





Executive Summary

We all experience storms in life, whether it be with our health, family, personal relationships, or jobs. Sometimes, storms in these different parts of our lives collide coincidentally. When that happens, it feels like the solid ground and the sky are falling at the same time — a perfect storm. The cyber security landscape and climate feels like there's storm after storm happening almost on a daily basis and reminds us that when it rains it pours. Data breaches are not stopping, there are increasing business impacts, new and emerging threats, new regulatory pressures as with the EU General Data Protection Regulation (GDPR), and not enough skilled talent to handle the volume and frequency of these demands. All of these elements combined with global political events such as Brexit, the 2016 U.S. Presidential Election, and the 2016 Rio Olympics only add more complexity to an already stormy situation. Furthermore, we can't ignore the ever-expanding attack surface reflected in the pace of innovative technology such as the Internet of Things (IoT), driverless cars, and evolving block-chain technology applications. The implications of this growing attack surface for both security and privacy cannot be overemphasized. All of this begs the question, "How do organizations and institutions stay centered in reducing their risk and mitigating cyber threats?"

Data Breaches — The Eye of the Storm

Regardless of whatever storms you're going through, establishing a strategy to provide peace and calm amidst all the chaos during the storm is crucial. In the eye of the storm, where the upheaval is strongest, you can barely see, let alone make well-thought-out decisions. The major eye of the cyber storm is during an active data breach, and the secret to stability is advance preparation.

During cyber attacks and data breaches, there are four questions that are central to the successful mitigation of the storm's impact. The answers to these questions must be determined in advance. As is often said, the time to fix the roof is not in the middle of the storm but before. These questions are the first set of questions executive leaders and board members want answers to. Adequate preparation for answering these critical questions will provide a sense of stability in current and future storms. The questions are:

- How do the threat actors get in?
- How do they stay in (evade our defenses)?
- What are they after and why?
- Who are they and why us?

In this document we share our perspective on the answers to these questions and provide some meaningful considerations for how to apply cyber threat intelligence for more proactive results. Additionally, we provide a high-level view of the landscape of cyber threats observed in the wild by FortiGuard Labs. Our hope is that this document will give you insights about where and how to emphasize your efforts in the critical areas of preventing, detecting, and responding to cyber attacks. And the first step in that journey is to understand yourself or, as is often said, "Know thyself."

Technology Attack Surface

At the root of the increase in cyber attacks is our increase in the use and dependency on technology. For many individuals and organizations, information technology (IT) is no longer an ancillary part of the business but a key ingredient for success. As such, there's a proliferation of technology innovations within governments and institutions of all sizes. The pace of change of these technology innovations has a significant influence on the velocity and frequency of cyber attacks. For some perspective on this accelerated pace, consider that it took radio 38 years to get to 50 million users, TV 13 years, Internet four years, and iPod three years. Facebook added 100 million users in less than nine months and iPhone apps hit 1 billion in nine months. — socialnomics.net

The Challenge of New Innovations

This pace has produced a vast attack surface for threat actors, and has subsequently created new and emerging attack vectors and options for intruders. If technology innovation and adoption was limited, then cyber security breaches would be at a bare minimum. It's difficult to imagine hacking into my grandmother's bank account in the '70s when online banking was still in its infancy even for early technology adopters. However, technology innovation and adoption is not limited and is expected to continue to rise with the proliferation of IoT devices. According to Gartner, the number of connected things will reach 20.8 billon devices by 2020. This creates a significant security challenge to keep pace with this rate of technology innovation.

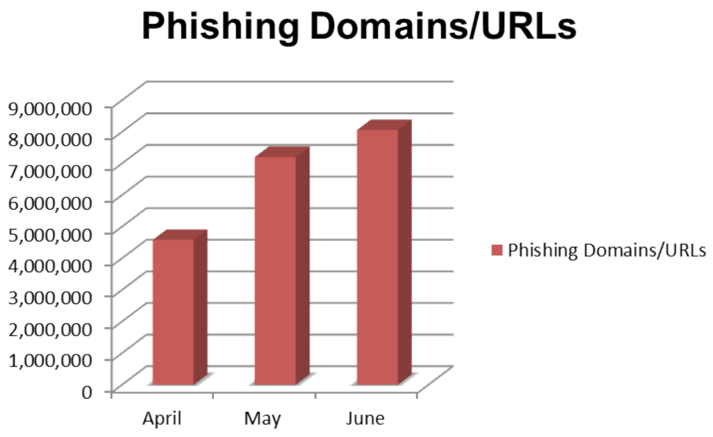
Entry Point for Hackers

Innovation is a good thing because it makes our lives better. But it can also represent another entry point for threat actors and hackers. For example, LinkedIn made it easier for professionals to stay connected but also introduced additional risks. Clearly, there weren't data breach reports about 100 million LinkedIn accounts being compromised 15 years ago because there was no LinkedIn at that time. Why does this matter? Each new innovation is yet another opportunity or entry point for the bad guys to launch an attack against a potential victim. This is foundational to how threat actors get in, and remember that one of the four questions addressed in this document is just that. We therefore turn our attention now to providing answers to the million-dollar threat awareness question, "How do threat actors get in?"

Dominant Threat Delivery Methods

An important question to ask related to cyber threats is, "How do they, the threat actors, get in?" This question presents a challenge to anyone willing to accept it. The challenge implied is how can you stop the threats from getting into your environment, or what is an effective way to stop a majority of them? The key is to first identify the likely entry points. Our telemetry data and research indicates that the two most common delivery methods are:

- Phishing Emails
- Malicious websites



Phishing Email

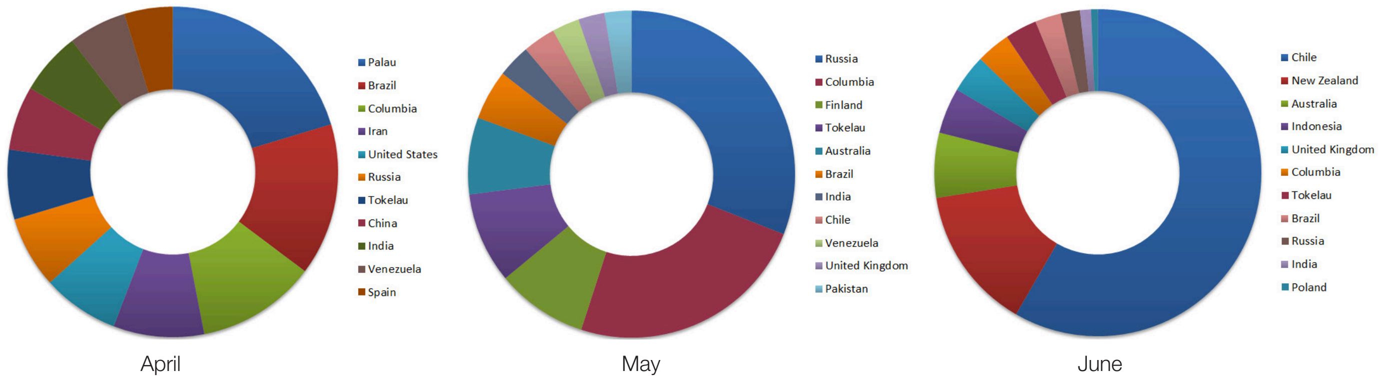
The volume of global phishing activity remains high with a 76% increase in June from April based on FortiGuard Labs' phishing domains and URLs threat data. The percentage of growth from May to June was 11%, which still represents a substantial increase, given the numbers are in the millions. Additional email phishing takeaways are:

- Tokelau: Increased activity from Tokelau country code domains
- Top Countries: Brazil, Colombia, Russia, and India represent the top four country code domains in Q2 2016
- Domain look-alikes: are still very active (e.g. nefflix vs netflix, etc.)

Tokelau

Tokelau (represented as ".tk") showed up consistently in the top phishing domains in the last quarter. For those not familiar with Tokelau, a vacation trip to Tokelau will involve a flight to Hawaii, then to American Samoa, next a small plane to Samoa, a 48-hour boat ride, and finally a canoe to the island shore (according to a CNN report). There were news reports in early 2011 about the rise in the use of the .tk domain for phishing and malicious activity, but few in the last two years. Our data shows that the free .tk domain has been very active in the last three months, indicating it's clearly still being used by threat actors.

Top 11 Countries with Malicious Phishing



Phishing — Top Countries

Besides Tokelau, there were four other countries in the top eleven phishing domains in all three months of April, May and June; Brazil, Columbia, Russia and India. Of these, Brazil has the potential to stay in the top ranks in the next quarter with anticipated increased threat activity, given that it will be hosting the 2016 Olympics in August. We also observed a number of large financial institutions' names included as part of the phishing domains and URLs.

Russia: In May, the top five phishing domains in Russia (top country in May) were a variety of Amazon-related sign-up domains, presumably attempting to get users to sign up for different services. These are phishing scams disguised as Amazon services.

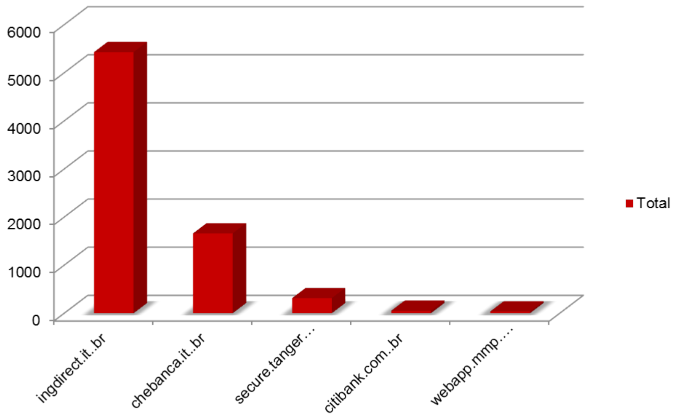
More than 8,000 of these types of domains were active in May and all end with .ru, even though some of them deceptively reference the Germany country code .de.

Domain Look-alikes

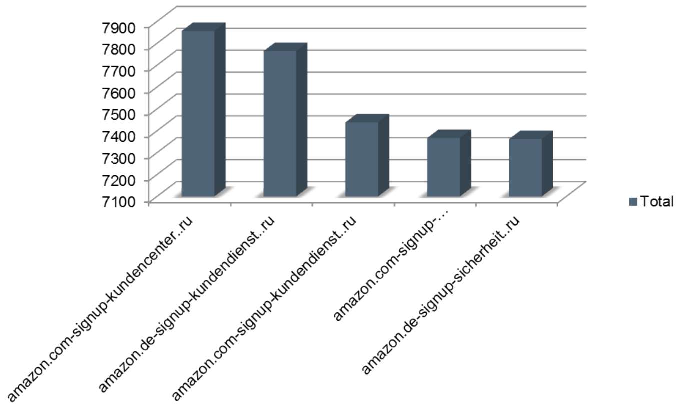
Some domains that didn't make the top five in Brazil but are still noteworthy include the look-alike domains such as nefflix.com. The threat actor group known as Shellcrew (aka Deep Panda) has been known to use domain look-alikes similar to nefflix.com. For example, they used we11point.com (look-alike wellpoint.com) in the 2015 U.S. Anthem breach that comprised over 80 million records including social security numbers.

It's important to note that all of these data points, when analyzed, offer significant threat-detection benefits. Dig through the blocked emails for clues using SIEM threshold alerts. And, even more beneficial is subscribing to quality (timely and validated) threat feeds that can help guard against threats that others are experiencing.

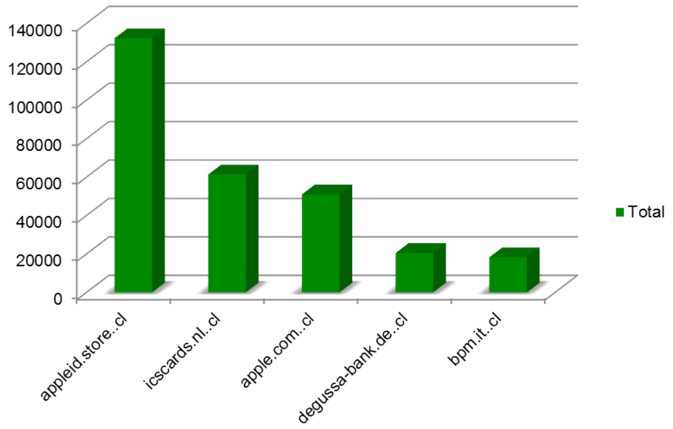
Brazil's Top 5 Phishing Domains in April



Russia's Top 5 Phishing Domains in May



Chile's Top 5 Phishing Domains in June



Phishing Insights and Takeaways

In most enterprise organizations with adequate email and anti-spam security solutions, about 97% of incoming emails are either spam or malicious and are blocked. The 3% remainder or last mile is what gets through and is mostly clean.

The interesting point here is that the 97% that are blocked contain the essential threat intelligence and insights that are often overlooked by some organizations. Those organizations that choose not to review, analyze, or monitor the volume of bad email chatter and logs will often miss out on powerful indicators that may help enrich their threat intelligence capabilities. What insights can you get from this email data that could provide incremental benefits?

Business Context

First, it gives a sense of potential targets within your organization that threat actors are intentionally after, which in turn provides you with additional context and reasons for stepping up protection and detection efforts for these individuals. Second, it may offer business context, if there's an increased volume of spear phishing or spam emails, targeted at specific individuals in a certain part of the business at a particular time of the month. For instance, detecting that a higher-than-normal percentage (e.g., 70%) of phishing URLs was directed at a specific deal desk working a big financial transaction is a meaningful indicator. This may mean that other regions can be targeted based on specific business activity at different times of the year or month. This additional business context can help predict similar volumes and higher risk based on business cycles.

Suspicious Activity

Phishing as a delivery method for malware and malicious payloads continues to be an important threat intelligence source that gives additional context to identifying suspicious activity. A sample of some of the phishing URLs with a ".kr" South Korea Top Level Domain (TLD) is shown and illustrates the potential intelligence value of phishing URLs in identifying suspicious activity.

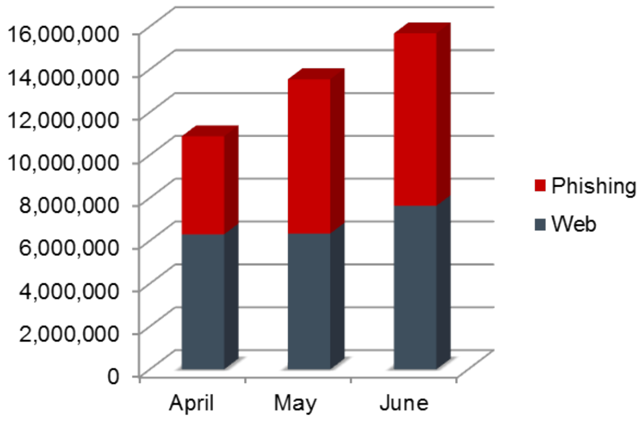
Multiple repeat URL references with the same suggestive company name (FI-name: real name not used) may prove valid and useful in identifying suspicious activity. In this case, trying to mimic the FI-name is suspicious context for the company FI-name. While this is not definitive proof of malicious activity, it's prudent to factor this data into the broader threat data set to inform better detection. As mentioned previously, analyzing this type of blocked spam or phishing emails may offer useful clues about suspicious threat activity. The next section focuses on web activity.

Korea Phishing URL — Sample

- http://www.orientel.co.kr/data/<FI-name>/step1.html
- http://www.sptek.co.kr/wp-content/uploads/<FI-name>
- http://sptek.co.kr/wp-content/ca/<FI-name>.html
- http://www.sptek.co.kr/wp-con../uploads/<FI-name>/index.html
- http://orientel.co.kr/data/<FI-name>/<FI-name>.html
- http://www.orientel.co.kr/data/<FI-name>/<FI-name>.html
- http://www.sptek.co.kr/wp-content/uploads/<FI-name>

Malicious Websites/URLs

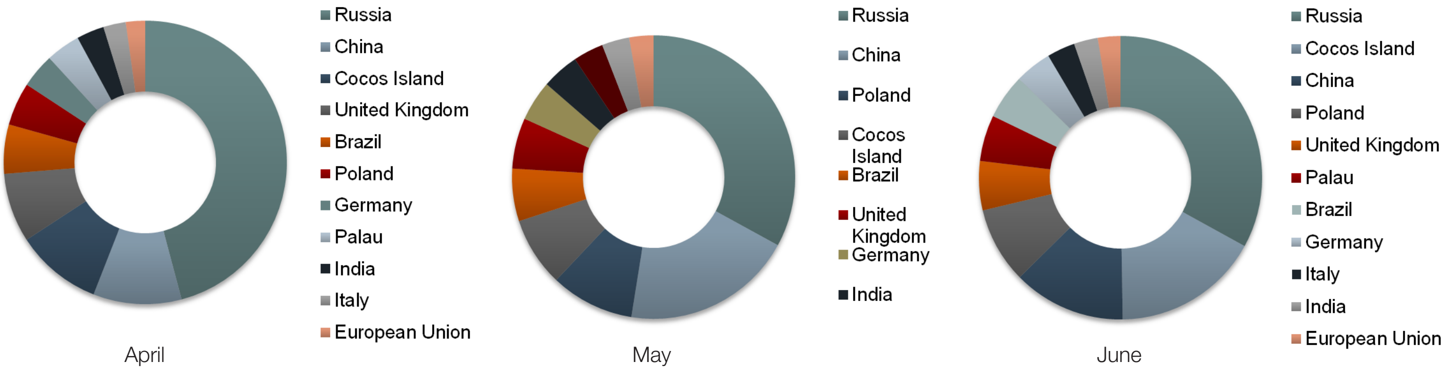
The second most popular delivery mechanism involves the use of malicious websites. Web-based technologies have undergone massive transformations and innovations since the original static HTML-based versions decades ago. Websites now have extremely dynamic content capable of doing things we could only dream of. For example, anyone with a Nest thermostat (IoT) installed at home knows that you can now control the room temperature in your house from a website and/or your smartphone, thanks in part to HTML5.



Web Domains by Country

The top malicious country code (cc) domains are shown below. Russia leads the pack across all three months, followed closely by China and Brazil, in the top 11.

Top 11 Malicious Web Site Domains



Malicious Websites/URLs

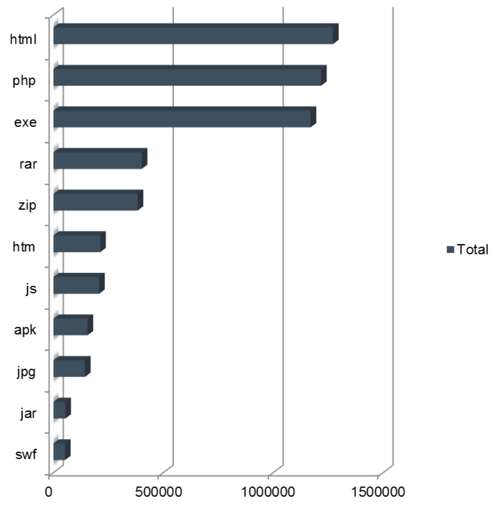
FortiGuard Labs' malicious URL threat data includes file type information, which provides insights regarding the most common malicious file types and/or extensions actively in use by threat actors. The distribution of the global threat data file extensions shows ".html", ".exe," and ".php" are the top three. Furthermore, there's an uptick in the use of JavaScript-based exploit kits (EKs) with malicious URLs to deliver ransomware mostly as first-stage downloader payloads.

URL Port Numbers

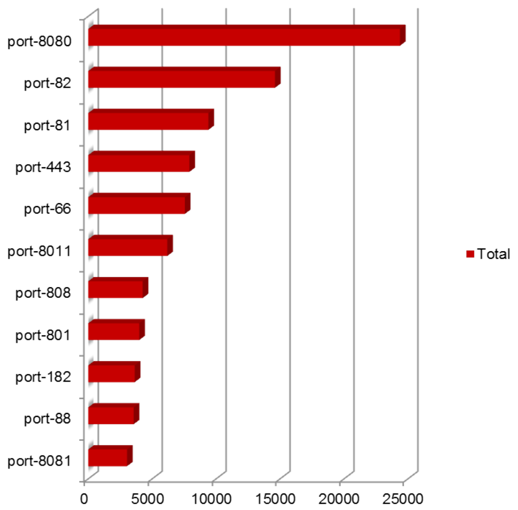
Additional granularity is also available with port numbers, which is beneficial for efficient detection of malicious threats. If the port number that's part of a malicious URL is missing, then more time is required to validate the URL to avoid blocking legitimate traffic. The last thing a security analyst wants to worry about during the storm is trying to figure out the port number(s) associated with a particular URL indicator. We've observed port numbers ranging from 1 to 8082 and above. The top ports over the last three months are 8080 (often used for web proxy services), 82, and 81.

Thus far, we've explored threat indicators related to phishing, malicious domains and URLS, and their applications in understanding suspicious activity. We now turn our attention to exploit kits, one of the most popular delivery methods employed by threat actors.

File Type Extensions



URL: Port Numbers



Exploit Kits

Exploit kits are malicious software that offers an automated way to distribute malicious payloads to a variety of victims and potential targets. They are a numbers game; the higher the volume of victims, the better. They are also referred to as exploit packs and are the foundational platform for drive-by attacks or drive-by downloads (when a user is unknowingly redirected to a malicious website from a legitimate but vulnerable one). The figure below shows the high-level flow.

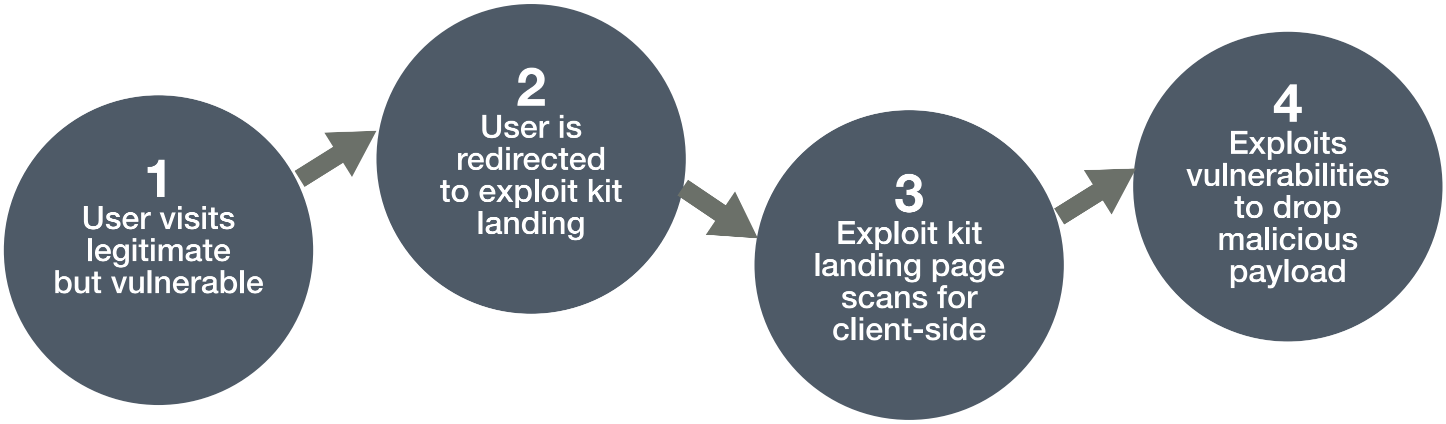
Exploit kits are used by threat actors in different attack methods including watering hole attacks and random, non-targeted attacks. The appeal to the bad guys is threefold: first is automation capabilities, second is ease of use, and third is high success probability.

Automation: Automation makes the process more efficient which would otherwise be time-consuming. The manual process of developing a working exploit can take as much as several weeks depending on the application vulnerability. In many cases, these are known vulnerabilities and not zero days. Automation therefore simplifies the whole process and makes it more attractive to cybercriminals.

Ease of Use: A big selling point for exploit kits is the administrators' interface user-friendliness and as-a-service options. A majority of them require little to no technical expertise, and for assurances, sellers throw in the additional tech support as part of the deal.

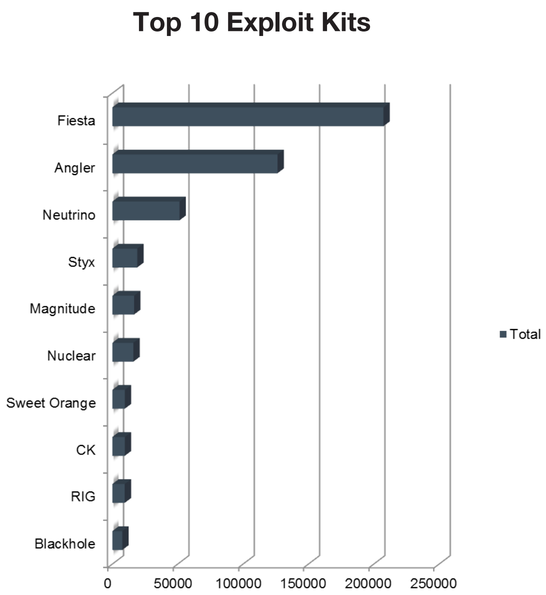
High Success Rate: Exploit kits have been and continue to be very successful in infecting users with desired payloads, and more recently they are now being used to deliver ransomware payloads to victims. Success breeds success as we have seen with the success of ransomware reflected by repeat victims paying the ransom.

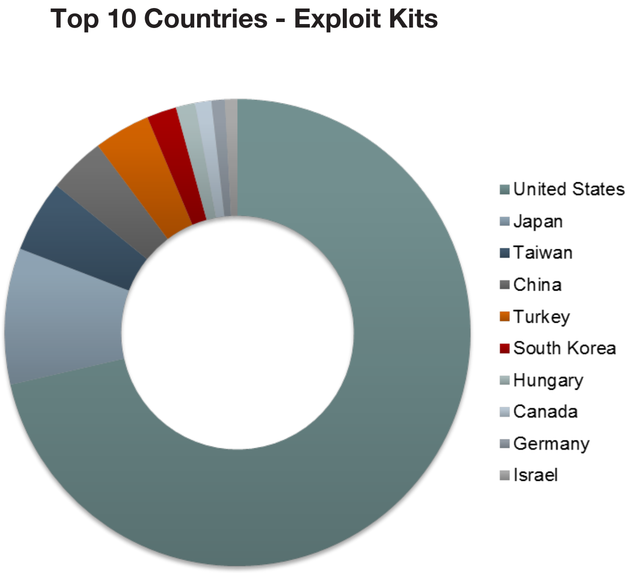
Remember also that web-based traffic is typically permitted by perimeter security controls and is less likely to be blocked.


1
User visits legitimate but vulnerable
2
User is redirected to exploit kit landing
3
Exploit kit landing page scans for client-side
4
Exploits vulnerabilities to drop malicious payload

The popularity and activity of exploit kits in the wild occurs in waves as with most cyber threats. Angler took the reigns as the most prevalent exploit kit globally following the decline of Blackhole. According to some reports, Blackhole's author produced malicious programs resulting in the loss of $866M from several banks. The crimeware author was arrested in October 2013 and that may have caused cybercriminals to switch to Angler.

There's also reason to believe another shift is currently in play from Angler to Fiesta and Neutrino, which both show up consistently in our top 10 exploit kits globally. APAC seems to be well represented in the top 10 countries for exploit kit targets with Japan, Taiwan, China, and South Korea. However, the United States eclipses all other countries in the exploit kit category. Most recently, we've observed an increase in the use of these kits for the delivery of ransomware variants in the U.S. and all over the world.





Insights and Takeaways

So far we've presented the two most common ways that attackers gain an initial foothold into a victim's organization.

We offered an approach to achieving a better understanding of the threats to your organization by digging through the activity logs/blocked email data, but also from other third-party-threat data feeds.

When it comes to exploit kits, there are two things you can do to help reduce your risk.

1: Test Vulnerability Patches

Understand your vulnerabilities through an effective vulnerability management life cycle. Patch, patch, and patch some more, then test that your patches were effective. We know you've heard it said several times already, but it can't be overemphasized and is included here for completeness.

2: Integrate Threat Feeds

Integrate malicious domains and URLs as a key part of your operations, either with a SIEM solution and/or threat intelligence platform. When you combine both phishing and exploit kit operational intelligence, you can begin to reduce your likelihood of falling victim to these cyber attacks. And although this is not a silver bullet, this approach offers a much-improved security posture compared with the alternative of not doing so. Furthermore, being deliberate in understanding these indicators and applying them will help reduce false positives and increase the efficiency and effectiveness of your teams. The better you get at this, the more you will move to some predictive capabilities of identifying attacks in the process before they can wreak havoc.

NOTE: Common Pitfall to Avoid
Information overload — don't subscribe to threat feeds just for the sake of it. Establish a well-thought-out plan for identifying the most effective feeds for your environment. We suggest feeds that help with early detection in the earlier phases of the Kill Chain, namely the delivery phase. Also, feeds that prevent data exfiltration designed to minimize the impact of a breach (e.g., botnet activity) can help detect data loss and/or leakage.

Behavior Blending

How do advanced threats persist in organizations? How do they remain hidden within an organization for months without being detected? Our research, analysis, and experience suggest that advanced threats employ two main techniques for remaining stealth: **(1) behavior blending and (2) evasion/ obfuscation techniques.**

Behavior blending, as the name suggests, implies that the adversary blends in with everyone else. Once they succeed in acquiring valid user credentials through the delivery techniques described earlier, they proceed to assume the full identity of those credentials through learned behaviors. They try to mimic, as best as they can, the normal behavior patterns of the credentials. This requires considerable research for success and oftentimes this stage is where they either go big or go home. They either fail big or win big primarily because it's very difficult to understand the ideal normal behavior patterns. This is difficult even for seasoned blue defenders that have authorized access to systems and that are not trying to hide or do anything malicious. So imagine how much more difficult it is for a cybercriminal. Notwithstanding this obstacle, they still strive to remain stealth by blending in with normal behaviors.

Patterns and Methods

Intentional low and slow data exfiltration as opposed to large bulk extraction in one fell swoop is characteristic of behavior blending patterns. A second anchor point related to behavior blending is that attackers focus on targeting privileged credentials that belong to both business and technology/ security administrators. "Why?" you may ask. Is it so they can get access to more data and credentials? Yes, but more importantly, they can override any controls designed to detect abnormal behaviors. Take, for example, the situation where cybercriminals breached a financial institution using privileged user credentials that were able to override wire transfer restrictions. The criminals disabled two very important restrictions and controls. First, was the requirement to have multi-factor authentication before processing any wire transfers. Second was the maximum amount/limit on wire transfers in the system (i.e. USD $10,000 in most cases). This example shows how critical it is to protect privileged accounts and why cybercriminals deliberately seek to gain this level of access.

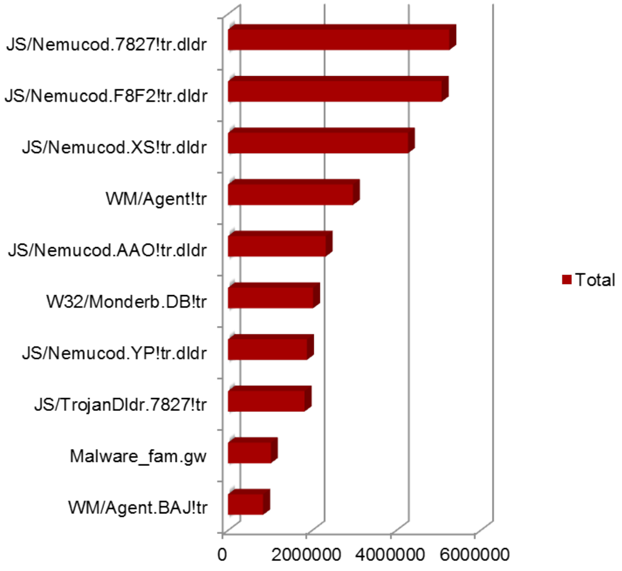
The question you may be asking is, "How in the world did they get the access to begin with?" Recall that the earlier sections on phishing and exploit kits outlined the first stage of the process in stealing a user's credentials by injecting the first-stage payload. If this payload goes undetected, and oftentimes it can, then access is granted. A follow-up question then becomes, "Why would this initial or subsequent malicious payload go undetected?" This is the focus of the second stealth mechanism (evasion/obfuscation techniques) employed by the bad guys.

Types of Advanced Malware

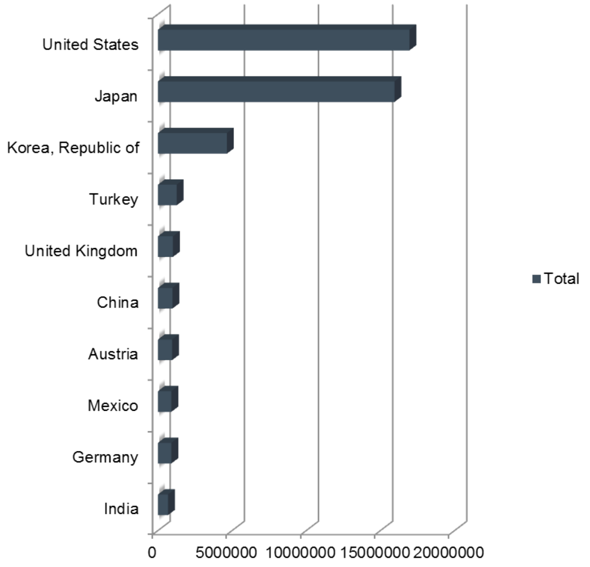
To set the stage for understanding evasions and obfuscation techniques, it's important to briefly review the different types of payloads/malware that are active in the wild today. The sophistication of present-day advanced malware is unparalleled in recent times. Let's take for example the reported data breach of the central bank of Bangladesh. In this instance, malware learned and executed wire transfer instructions to move $81M from The Wall Street Journal in New York to casinos in the Philippines, as reported by the Wall Street Journal. The story from the previous section described how threat actors could bypass or override wire transfer restrictions and controls designed to prevent these types of fraudulent cases. This example shows that malicious intent, when expressed in software, can be self-learning and can cause significant damage and loss.

There are several different types of malware including droppers, downloaders, trojans, self-defending, anti-debugging, mobile malware, etc. The top 10 global malware in the last three months are shown in the graphic. The JS/Nemucod family is the dominant malware family. This family is currently the most active ransomware downloader and, in general, ransomware activity and attacks have increased significantly in the last three months.

Top 10 Malware



Top 10 Countries - Malware



Evasion Techniques

With an understanding of different payload types, we proceed to the obfuscation techniques used by these payloads. A quick reminder about why you care; because understanding evasion techniques helps mitigate the impact of cyber attacks and offers some measure of stability in the eye of the storm. How? Through specific preparation and planning that incorporates these techniques on an operational basis into your security strategy. There are several different obfuscation mechanisms used by threat actors and we've attempted to classify them into two main categories, basic and advanced. For simplicity, we've also opted not to go into the technical details behind these methods but instead provide a high-level explanation and illustration of their underlying concepts.

Basic Obfuscation

Malware changes its appearance (look and feel). Techniques in this category seek to mask the true appearance and physical characteristics of the payload. Imagine a person wearing a Halloween costume or mask. Think Tom Cruise in Mission Impossible. However, don't judge a book by its cover, as these types of payloads repeatedly deceive the untrained eye. An example is a simple trojan that hides suspicious string indicators with basic encoding techniques and will bypass some security solutions.

Advanced Obfuscation

Conversely, malware in this category employs techniques that change both the physical properties as well as the behavior of their payloads through deceptive actions. Detecting these types of payloads requires an extended observation and analysis period for their true characters to be revealed. Think a cheating spouse that's discovered several years into a relationship. True character sometimes takes time to show itself. And paraphrasing Abraham Lincoln, character is the real thing. It's easier to understand why these types of payloads are so difficult to detect and how they can stay in an environment for months undetected. An example in this category is self-defending malware that will only execute its malicious branch if it does not detect common malware-detection solutions. The important point here is that malware is capable of learning existing defenses and controls and then overriding them.

Basic Obfuscation

- Encoding Algorithms
- Base64
- XOR
- ROR/ROL
- ADD-SUB
- Junk Code
- Tricky Jumps
- SEH
- Dynamic Changes
- Polymorphism
- DGAs

Advanced Obfuscation

- Packing
- Nested Encryption
- Anti-debugging
- Self-defending
- Blastware
- Anti-analysis
- Ghostware

Insights and Takeaways

The principal takeaway from this section is to receive regular threat briefings. Threat actor tactics, techniques, and procedures (TTPs) are always evolving and therefore there's an increased need for operational and tactical threat intelligence to help identify these different techniques and deliver them in practical, meaningful, and consumable ways.

Thus far, we've examined the following elements in relation to our four central questions about cyber threats and the actors behind them.

How they get in

- Phishing emails
- Malicious websites
- Exploit kits

How they stay in (evade defenses)

- Behavior blending
- Obfuscation techniques

In the next section, we shift our focus now to what threat actors want and why.

Your Value to Threat Actors

Now that we have a basic understanding of how “they” stay in, the next eye of the storm question to answer is, “What are they after and why?” Because it’s not feasible to answer this question specifically for every individual organization, we have decided to adopt a general approach using object categories. These offer general strategies to help drive specific answers to this question of “What they are after and why, for your organization?” An important reminder is worthy of emphasis here. The goal is to be able to say that nothing was successfully breached or taken; that the intruders were stopped before they could cause material damage. However, in practice, this is not always possible. There will be times (hopefully, few times) when a breach will occur. And when it does, a solid understanding of what was targeted will serve an organization well in mitigating the business impact and in the execution of effective remediation and recovery. There are three main categories of value to threat actors and they are:

Data

Not all data is created equal. The going rate for credit card data is between USD $4 and $10 per record. Healthcare records could be sold as high as 10X depending on source, victim, etc. These data sets are used in a variety of fraudulent activities including identity theft, financial, and healthcare fraud. More recently, there’s been a spike in the use of these PII data (personally identifiable information) in launching more attacks. For example, the ADP and Equifax data breaches were launched by intruders accessing the external-facing W2 web portals using the victim’s social security number and date of birth. The question you may ask is, “Where did they get the SSN and DoB information to begin with?” The darknet is packed with forums where PII data is traded on a regular basis. In the case of ADP and Equifax, this data granted the intruders more data (W2 tax-related) that was used in identity theft in the U.S., as reported by the IRS.

Money

Money is self-explanatory, although the why behind it may not be so obvious. Several digital currencies make it more difficult to track the flow of the money, which could ultimately help determine the who and the why behind the stolen money. A noteworthy point here is that there are several other attribution factors besides the money trail, but none that are quite as definitive.

Intellectual Property

The central element in cyber espionage cases is mostly intellectual property or state secrets that can be used as an economic advantage over the victim. However, some agreements have been established by governments to stop this growing trend of cyber espionage.

Insights and Takeaways

Regardless of whether the ultimate object of the attack is data, money, intellectual property, revenge or all of the above, it’s vital for you to understand your crown jewels. Any of these elements, which are considered critical to your short- and long-term business success, will be a target and represents some value.

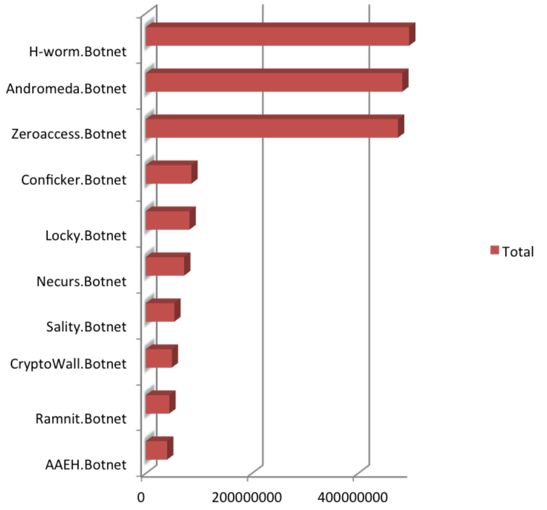
Crown Jewels

Sometimes, determining the crown jewels for an organization isn’t as easy as it sounds. Take, for instance, a household brand name. At first it may seem that the brand is their crown jewel and it is, to some degree, but what is the tangible measure of that brand that is appealing to hackers? Is it the data, money, their intellectual property, or all of the above? Which of these can erode the brand the most? A detailed and careful analysis of the underlying components of the brand reputation is what will be required to arrive at the needed level of risk-mitigation strategy.

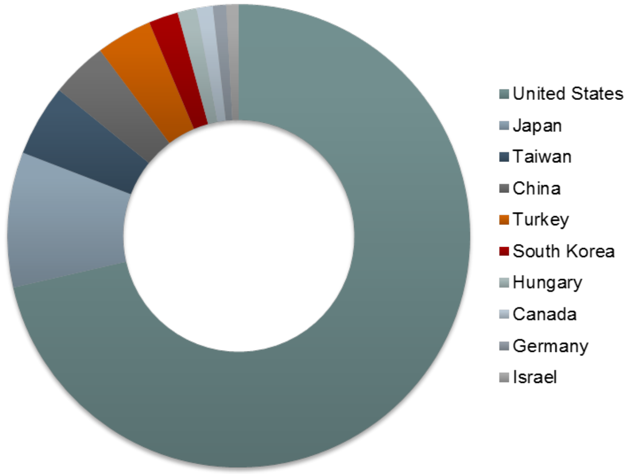
Our advice is to understand your crown jewels and protect them with your life. Furthermore, ensure a disproportionate percentage of investments are allocated for their protection and defense.

Data Exfiltration — Botnet Indicators

Next, understand the techniques and methods that adversaries will use to extract your crown jewels, particularly if they are data related. Data exfiltration indicators such as botnet chatter and beaconing will offer some practical ways to detect such activity. Our threat telemetry shows botnet activity and chatter on the rise and you can see the top 10 target countries and botnet types. Ransomware botnet activity from Locky and CryptoWall are notable names in the top 10.



Top 10 Botnets



Top 10 Countries - Botnets

Advanced Threat Actors

Shellcrew, Syrian Electronic Army (SEA), Guardians of Peace (GOP), Impact Team, Anonymous — these are all names of threat actors or groups that have been responsible for past data breaches. There are several different types of advanced threat actors motivated by different things, but we've grouped them into three main buckets. These are:

Nation States: This group comprises actors that have significant resources and advanced capabilities. Their motives typically have a political, military, and economic flavor to them. This is a highly specialized group.

Cybercriminals (Multi-nationals): The principal motive for actors in this group is money. These are cybercriminals that may be part of a multi-national syndicate or organized crime. It also includes actors developing services such as ransomware as a service and other mass exploit packs and tools for sale to the highest bidder.

Hacktivists: These are a motley crew of different sorts motivated by a wide variety of causes ranging from political to revenge and financial to social embarrassment. We hope that this classification will help provide some additional context for the key questions that are asked in the eye of the storm but more importantly before the storm.

Why am I a target? The answer may sound deceptively simple, but it's true. You're a target because you're target-worthy. But what exactly does it mean to be target-worthy? There are three main characteristics of an organization or individual that is target-worthy and these are:

Digital Footprint/Presence: The more technology dependent you are, the larger your attack surface and the greater your digital footprint/presence. This means you're more attractive to a would-be attacker as opposed to a target without a measurable digital presence.

Substantive Value: We've already addressed this characteristic in the earlier section. Refer to the section titled "Your Value to Threat Actors" Essentially, you are target-worthy to the extent to which you have something of value.

Security Profile: A weak security profile invites threat actors and represents a high rate of return on their investment. Threat actors use a combination of methods including research, reconnaissance, and information sharing to identify target-worthy victims with weak security profiles. Furthermore, it's not impossible for security ratings services (e.g., SecurityScorecard, BitSight, etc.) to be adapted for use by the bad guys, although there have been no known public cases to that effect.

Insights and Takeaways

First, ensure that you're matching your strategy and capabilities to the likely actors that will find your organization attractive, using the groupings we've provided or other groupings. For example, if your attack surface is large and you have government ties, you're most likely going to be targeted by nation state threat actors. Developing countermeasures commensurate with this risk profile and this additional context may prove to be very beneficial.

Information Sharing

Second, actively participate in threat information sharing and collaboration either formally through different Information Sharing and Analysis Centers (ISACs) and CERT agencies or informally through peer organization groups and regular cross-pollination with like organizations in your industry or similar industries. Additionally, engaging resources for this level of information sharing is the key to success and may require institutional knowledge of your organization.

Partnerships with Law Enforcement

Last, establish a stronger partnership and relationship with law enforcement agencies and personnel. As FBI Director James Comey said, "People ask us all the time, 'What do you need us to do?' Get to know us before there is a storm." There's significant value for the industry as a whole when these threat actors are brought to justice. One of the ways this happens is through these types of partnership efforts. The value extends beyond jail time for the culprits to additional intelligence about other potential attacks or victims. Fortinet partners with several agencies including the FBI, NATO, INTERPOL, etc., because we believe in the power of these partnerships to help us get to a more proactive or predictive state rather than a reactive one.

Strategic Intelligence

Strategic Intelligence: focuses on understanding who the threat actors are, their intentions, and capabilities. This level of intelligence has predictive value if applied correctly and consistently over an extended period. Information about threat actors' plans can reveal they're going to hit a series of banks or industries in a particular order or sequence using a variation of techniques for each target. In other words, knowing when and where the category 5 hurricane is going to hit your city is extremely beneficial.

Tactical Intelligence

Tactical Intelligence: refers to the application of tactics, techniques, and procedures (TTPs) of the threat actors and corresponds to the question "How do they stay in (evade)?" For example, understanding TTPs of new ransomware variants that utilize anti-sandbox techniques or those that will delay activation of encryption routines for weeks will help you establish different countermeasures. It's sort of like knowing that the storm won't get detected by U.S. weather models or that it won't gain momentum until 4 p.m. Pacific Time on a Friday afternoon in time for the weekend. You might want to rely on the European weather models in that case.

Operational Intelligence

Operational Intelligence: includes indicators of compromise (IOC) such as those described earlier (e.g., phishing domains/URLs, malicious websites/URLs, port numbers, blacklisted IPs, file types, etc.). The storm is going to start out as wind gusts, then change quickly to a hailstorm and move to heavy snow back to sleeting rain, ultimately covering the roads in black ice, so drive carefully. Benefits of these artifacts include rapid detection, incident prioritization, and resource utilization. Time saved by security analysts from not having to research these artifacts and indicators of communication ensures they can spend their time more effectively.

Answers to the last question, "What are they after and why?" can be extracted from a combination of all three types of intelligence. FortiGuard Labs remains committed to helping our clients and customers prevent, detect, and respond to cyber threats and resolute in our collaboration efforts with law enforcement agencies and partners across the globe. Our hope is that the intentional application of threat intelligence data will guide your preparations before the storm and guard (FortiGuard) you in the eye of the storm.

Conclusion

At the beginning of this document we set out to provide our perspective on and answers to the four critical questions asked during the most intense phase of a cyber attack, the eye of the storm. These questions have a timeless property and will be asked time and again with every intrusion and/or data breach. The answers we've provided may appear simple on the surface, but to ignore their applications and insights would be to increase your risk of falling victim to a cyber storm of incidents and attacks. Threat actors are human just like everyone else and they tend to use simple things that are often overlooked to accomplish their actions or objectives. To them, the path of least resistance is always more appealing when available.

We've touched on varying degrees of FortiGuard Labs research, analysis, and threat intelligence data. We believe that there are three main types of threat intelligence in alignment with our four questions. These are strategic, tactical, and operational threat intelligence.

Appendix A — HTTP URL Obfuscation

In April of this year, there were several repeated http requests obfuscated as shown in the graphic below. This is an example of how threat actors can get into an organization and stay there for months while making repeated http calls to malicious websites and URLs. There was a specific pattern displayed by these requests over the course of thirty days and then on May 1, everything stopped abruptly. We hope that means the victims detected the malicious intruder and stopped them. See if you can determine any familiar names in the URLs listed below.

```
http://dy11.19884.info/kuai/\xcd\xf8\xc9\xcf\xc8\xd5\xd7\xac\xb0\xd9\xd4\xaa\xbd\xcc\xb3\xcc.txt

http://dy11.19884.info/kuai/\xb3\xc9\xc8\xcb\xd0\xa1\xd3\xce\xcf\xb7.txt

http://dy11.19884.info/kuai/\xcc\xd4\xb1\xa6\xc8\xc8\xc2\xf4.txt

http://dy11.19884.info/kuai/\xcd\xf8\xc9\xcf\xc8\xd5\xd7\xac\xb0\xd9\xd4\xaa\xbd\xcc\xb3\xcc.txt

http://dy11.19884.info/kuai/\xcc\xd4\xb1\xa6\xc8\xc8\xc2\xf4.txt

http://dy11.19884.info/kuai/\xb3\xc9\xc8\xcb\xd0\xa1\xd3\xce\xcf\xb7.txt

http://dy11.19884.info/kuai/\xcd\xf8\xc9\xcf\xc8\xd5\xd7\xac\xb0\xd9\xd4\xaa\xbd\xcc\xb3\xcc.txt

http://dy11.19884.info/kuai/\xcc\xd4\xb1\xa6\xc8\xc8\xc2\xf4.txt

http://dy11.19884.info/kuai/\xb3\xc9\xc8\xcb\xd0\xa1\xd3\xce\xcf\xb7.txt

http://dy11.19884.info/kuai/\xcd\xf8\xc9\xcf\xc8\xd5\xd7\xac\xb0\xd9\xd4\xaa\xbd\xcc\xb3\xcc.txt

http://dy11.19884.info/kuai/\xcc\xd4\xb1\xa6\xc8\xc8\xc2\xf4.txt

http://dy11.19884.info/kuai/\xb3\xc9\xc8\xcb\xd0\xa1\xd3\xce\xcf\xb7.txt

http://dy11.19884.info/kuai/\xcd\xf8\xc9\xcf\xc8\xd5\xd7\xac\xb0\xd9\xd4\xaa\xbd\xcc\xb3\xcc.txt

http://dy11.19884.info/kuai/\xcc\xd4\xb1\xa6\xc8\xc8\xc2\xf4.txt

http://dy11.19884.info/kuai/\xb3\xc9\xc8\xcb\xd0\xa1\xd3\xce\xcf\xb7.txt

http://dy11.19884.info/kuai/\xcd\xf8\xc9\xcf\xc8\xd5\xd7\xac\xb0\xd9\xd4\xaa\xbd\xcc\xb3\xcc.txt

http://dy11.19884.info/kuai/\xcc\xd4\xb1\xa6\xc8\xc8\xc2\xf4.txt

http://dy11.19884.info/kuai/\xb3\xc9\xc8\xcb\xd0\xa1\xd3\xce\xcf\xb7.txt

http://dy11.19884.info/kuai/\xcd\xf8\xc9\xcf\xc8\xd5\xd7\xac\xb0\xd9\xd4\xaa\xbd\xcc\xb3\xcc.txt

http://dy11.19884.info/kuai/\xcc\xd4\xb1\xa6\xc8\xc8\xc2\xf4.txt
```

Appendix B — Compromised Email Credentials

We included a sample of some web/email data that gives a glimpse of some of the insights you can extract from this data. See if you can identify users with compromised credentials being used for malicious purposes and spamming.

```
http://ds.forbrukerhuset.com/fur.php?c={“idCli”:”2186”,”idCamp”:”959979”,”email”:”ed.wolters@gmail.com”,”seg”:”nn
vfa6buizbxk3k2m53vs===”}&at=1

http://ds.forbrukerhuset.com/fur.php?c={“idCli”:”2186”,”idCamp”:”949297”,”email”:”ed.wolters@gmail.com”,”seg”:”nn
vfa6buizbxk3k2m53vs===”}&at=1

http://ds.forbrukerhuset.com/fur.php?c={“idCli”:”2186”,”idCamp”:”955770”,”email”:”ed.wolters@gmail.com”,”seg”:”nn
vfa6buizbxk3k2m53vs===”}&at=1

http://ds.forbrukerhuset.com/fur.php?c={“idCli”:”2186”,”idCamp”:”951549”,”email”:”ed.wolters@gmail.com”,”seg”:”nn
vfa6buizbxk3k2m53vs===”}&at=1

http://ds.personal-deals.com/fur.php?c={“idCli”:”2280”,”idCamp”:”996349”,”email”:”wouter@wevon.net”,”seg”:”nnvdk
ubwoqyhaztgn5ggo===”}&at=1

http://ds.personal-deals.com/fur.php?c={“idCli”:”2280”,”idCamp”:”998258”,”email”:”jose20021964@yahoo.com”,”seg”: ”nnvdo2stoj
yvkskmf5cu2===”}&at=1

http://ds.personal-deals.com/fur.php?c={“idCli”:”2280”,”idCamp”:”998258”,”email”:”wouter@wevon.net”,”seg”:”nnvdk
ubwoqyhaztgn5ggo===”}&at=1

http://ds.personal-deals.com/fur.php?c={“idCli”:”2280”,”idCamp”:”996349”,”email”:”wouter@wevon.net”,”seg”:”nnvdk
ubwoqyhaztgn5ggo===”}&at=1

http://ds.personal-deals.com/fur.php?c={“idCli”:”2280”,”idCamp”:”998258”,”email”:”jose20021964@yahoo.com”,”seg”: ”nnvdo2stoj
yvkskmf5cu2===”}&at=1

http://ds.personal-deals.com/fur.php?c={“idCli”:”2280”,”idCamp”:”998258”,”email”:”wouter@wevon.net”,”seg”:”nnvdk
ubwoqyhaztgn5ggo===”}&at=1

http://ds.personal-deals.com/fur.php?c={“idCli”:”2280”,”idCamp”:”996349”,”email”:”wouter@wevon.net”,”seg”:”nnvdk
ubwoqyhaztgn5ggo===”}&at=1

http://ds.personal-deals.com/fur.php?c={“idCli”:”2280”,”idCamp”:”998258”,”email”:”jose20021964@yahoo.com”,”seg”: ”nnvdo2stoj
yvkskmf5cu2===”}&at=1

http://ds.personal-deals.com/fur.php?c={“idCli”:”2280”,”idCamp”:”998258”,”email”:”wouter@wevon.net”,”seg”:”nnvdk
ubwoqyhaztgn5ggo===”}&at=1

http://ds.personal-deals.com/fur.php?c={“idCli”:”2280”,”idCamp”:”1002104”,”email”:”info@ronawellness.nl”,”seg”:”nn
vdqlsjnvfvautboqzfs===”}&at=1

http://ds.personal-deals.com/fur.php?c={“idCli”:”2280”,”idCamp”:”1002104”,”email”:”info@technimation.nl”,”seg”:”nn
veerknli2tk4sxlf5de===”}&at=1

http://ds.personal-deals.com/fur.php?c={“idCli”:”2280”,”idCamp”:”996349”,”email”:”wouter@wevon.net”,”seg”:”nnvdk
ubwoqyhaztgn5ggo===”}&at=1

http://ds.personal-deals.com/fur.php?c={“idCli”:”2280”,”idCamp”:”998258”,”email”:”jose20021964@yahoo.com”,”seg”: ”nnvdo2stoj
yvkskmf5cu2===”}&at=1
```

Appendix C — 2016 Rio Olympics

Cyber attacks during the Olympic games are not new, there were reported cyber attacks as far back as 2004 Summer Olympics in Greece where a large cell phone service providers' switches were hacked and resulted in several individuals (diplomats, athletes, etc) phones being tapped. However, there are two principal reasons why the 2016 Rio Olympics deserves special attention.

Low Priority for Cyber Attacks in Brazil

First, cyber threats and attacks are not a very high priority for Brazil. According to the World Economic Forum (WEF) ranking of global business risks, Brazil ranks cyber attacks #23 and data fraud/theft #16 compared to several other countries that rank cyber attacks #1 (Japan, Germany, Netherlands, US, Switzerland). In other words, it appears investments to protect against cyber attacks will be comparatively low - http://reports.weforum.org/global-risks-2016/eos/#country/BRA. The right level of investments will be required to stop cyber attacks during the games. The volume of these attacks is expected to be high based on historical trends. For example, the 2012 London Olympics experienced 165 million security events. These events were reduced to 97 actual security incidents according to the CIO of the 2012 Olympic games Gary Pennell. This level of aggregation and protection does not happen without the right priority and investments for cyber attacks. Currently, the UK ranks cyber attacks #2 in business risks in the WEF ranking (http://reports.weforum.org/global-risks-2016/eos/#country/GBR) significantly higher than Brazil's ranking of #23.

Increased Threat Activity in Brazil

Second, the volume of malicious and phishing artifacts (i.e. Domain names and URLs) in Brazil is on the rise. In June, Brazil's percentage increase was higher in three of the four categories when compared with the global percentage increase as shown in the table. The highest percentage growth was in the malicious URL category at 83% compared to 16% for the rest of the world. As the 2016 Rio Olympics approaches, the history of these increased attacks will undoubtedly continue and FortiGuard Labs is already seeing indicators of repeat techniques used in past attacks. For example, domain lookalikes such as v1sabancario.k6.com.br associated payment systems fraud and over 3800 malicious websites and URLs with the government designation ".gov.br" targeting government and event officials. These were similar techniques that were used during the 2014 Rio World Cup according to a report by the National Cyber Security Institute. A summary of the notable threat artifacts for Q2 include:

Top malware activity: Nemucod ransomware variant

Top malware types: 1st stage Trojans and downloaders

Top three botnet activity: Andromeda, Sality and Zeroaccess

Top three exploit kits: RIG, Neutrino and Angler

% Increase from May to June

	Brazil	Global
Malicous Domains	18%	29%
Malicious URLs	83%	16%
Phishing Domains	79%	74%
Phishing URLs	12%	1%

Appendix D — U.S. Cyber Threats Ranked Highest Risk

The threat of cyber attacks continues to be a growing concern for governments, organizations, and individuals around the world. According to rankings of business risks by the World Economic Forum, cyber attacks rank #1 in the U.S., Japan, Germany, Netherlands, and a few others. This underscores the significance of understanding the cyber threat landscape and associated insights related to intruder detection.

Why are cyber attacks ranked the highest risk-inducing threat above all others including fiscal crises and, surprisingly, terrorist attacks? Why is this the case for only a subset of countries? The answer to this question lies in being able to understand the dependencies and interconnections of the physical and digital world. In this digital age, our very lives are dependent on technology devices. To get a glimpse of this dependency, imagine a visit to the hospital or ER only to be told that they can't attend to any patients because of an ongoing cyber attack. This was the case across some U.S. healthcare institutions this year. These cyber attacks have far-reaching consequences for businesses and organizations responsible for delivering critical national services. Thus, we ask ourselves again, "Why are cyber attacks ranked so high in overall business risks."

Top 5 Business Risk — U.S.

- Cyber attacks - #1
- Data fraud and theft - #2
- Terrorist attacks - #3
- Fiscal crises - #4
- Asset bubble - #5

Closing Thoughts on Highest Ranking

First, cyber attacks are more scalable than physical threats. For instance, malware, which is the biggest threat category related to cyber attacks, can be in multiple places at the same time while the physical bad guys cannot. Second, cyber threats are capable of controlling physical assets and therefore can wreak the same magnitude of havoc if not more. Third, cyber attacks can be as sophisticated as physical crimes and, in some cases, even more so. Cyber attacks can achieve any malicious intent, provided the threat actors have the resources and the capability.

Fourth, cyber threats are extensible and can easily be upgraded, improved, or obfuscated and as such offer the lowest risk of getting caught because they are difficult to detect. Attribution is very difficult as is persecution across international boundaries. There are several other reasons, but these are the core reasons why cyber threats are the mother of all threats and risks.

FORTINET®

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
Valbonne
06560, Alpes-Maritimes,
France
Tel +33 4 8987 0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428

Aug 1, 2016