WatchGuard

INTERNET SECURITY REPORT

Quarter 1, 2020

Contents

The Firebox Feed™ provides quantifiable data and trends about hackers' latest attacks, and understanding these trends can help us improve our defenses.

Introduction

Sometimes we have bigger problems to address than cyber attacks.

That's how I currently feel as I sit here trying to come up with some "fun" metaphorical illustration of why you should follow the cyber threat trends we present in this report. As I type this, a global pandemic has put lives and livelihoods at risk around the world, with a death rate at nearing half a million, not to mention tens of millions unemployed. Meanwhile, another unjust police murder of a black man in the United States has proven that we have a long way to go in fighting the systemic racism in my country. When there are so many immediate threats, wrongs, pain, fear, and anger going on in our world, all of which affect our lives so directly, it's hard to consider what seems like an abstract, indirect digital threat, let alone come up with a creative way to talk about it. Right now, I would rather skip the niceties and focus on helping you get to what matters most; keeping your families safe, your principles intact, and your businesses running as best they can.

Having said that, cybersecurity awareness and protection still matters to both your personal online safety and digital business viability during this pandemic. In fact, you probably need to stay more vigilant against digital threats during times like these. While your number one priority should remain keeping safe and running your business during this trying time, you should also know that cyber criminals tend to up their illegal activities during tragedies like these. Unfortunately, digital criminals prey on both the fears and philanthropy of disasters, taking advantage of both our uncertainty and generosity. This report shares their tools, tactics and procedures in hopes you can learn enough to defend yourself against their atrocious actions.

By gathering and analyzing data from tens of thousands of network security appliances, WatchGuard's quarterly Internet Security Report (ISR) aims to help you recognize and defend against the statistically relevant cyber threats that affect most businesses today. Our threat team bases most of this report on quantifiable threat intelligence we receive from Fireboxes in the field. This data allows us to measurably identify which threats affected most customers last quarter, thus extrapolating the kinds of threats that will continue to affect you going forward. Using this knowledge, you can prepare the best cyber defenses ahead of time, hopefully giving you back time to concentrate on surviving and thriving during our current global calamity. Let's get into it.

The Q1 report covers:

The world seems dark right now, but there is plenty of light emerging from the shadows. I believe we'll see more goodness from one another helping to solve our shared global problems than we will bad actors taking advantage. We hope our Q1 report helps in a small part to at least shine a little light on the threat landscape, so you have one less thing to worry about.

Executive Summary

During Q1, we saw a drop in overall malware compared to the record-setting Q4 2019; and that despite an increase in reporting Fireboxes. We suspect this slight drop coincides with businesses having to move home in early March. Perhaps malware followed their users home. That said, malware is still up year over year, with ~64% of malware evading traditional, signature-based defenses (zero day malware). However, the biggest news this quarter is just how much malware bypasses security controls through encrypted network traffic. By analyzing the malware split in Fireboxes configured to decrypt TLS connections (like HTTPS traffic), we learned that more than two-thirds of malware arrives over encrypted channels. If you are not decrypting and scanning your secure web connections, you are likely missing a large majority of malware. Beyond this key finding, the report also highlights a few relevant malware samples, shares the top network attacks and malicious domains, and covers some COVID-19-related cyber attacks.

Q1 2020 highlights include:

- **67% of malware uses encrypted communication channels** on boxes that decrypt and scan TLS traffic. If you aren't using HTTPS decryption and content inspection, you're likely missing two-thirds of the malware entering your organization.
- **Zero day malware accounts for 63.7% of all threats on Fireboxes** not decrypting TLS. However, it also jumps to **72% on Fireboxes that decrypt and scan TLS traffic.** This suggests that not only do threat actors hide their attacks using encryption, but they tend to use more sophisticated malware through these encrypted channels.
- Overall, Fireboxes blocked **31.2 million malware samples in Q1**, which is a slight drop over Q4 last year and accounts for **~730 malware samples per Firebox.**
- The **Cryxos trojan** made a comeback attempting to steal credentials from victims.
- **A legitimate greyware remote desktop product, Ammyy Admin, made our top malware lists**. As you move employees home, beware insecure remote desktop programs.
- In Q1, **Fireboxes blocked 1.66 million network attacks,** which splits to about 38 attacks per Firebox. This is a slight **19% decrease** over last quarter.
- For a second quarter, **SQL injection attacks remained the top network threat for Q1.**
- **Bellsyscdn[.]com was responsible for over half the malware domain blocks this quarter**, due to its hosting of the Bondat worm's C&C, Monero cryptomining, and WordPress-related attacks.
- **DNSWatch saw and blocked lots of cryptomining-related campaigns.** Six domains related to Monero cryptomining made our top domains lists.

Those are the report highlights, but let's dive into the interesting additional details. By the end of the report, we'll have shined a light on the dark cyber threat landscape and offered you advice to protect yourself.

Firebox Feed Statistics

WatchGuard

Firebox Feed Statistics

What Is the Firebox Feed?

WatchGuard Fireboxes see billons of connections both from and to our customers' networks. Some of these connections contain malware, network attacks, and other malicious activity, which our Fireboxes block. The Firebox Feed sends anonymized details on these blocked connections to us, the WatchGuard Threat Lab, from WatchGuard customers who have opted in to sharing this threat intelligence. Receiving this intelligence allows us to analyze the data and identify targets and treads of the malicious activity that affects our global customer base. Using the data allows us to build this report.

We appreciate customers and partners who opt in to provide this anonymous feed information. Data sent from the Fireboxes don't contain private or sensitive details, so we encourage others to opt in as well. Specifically, we track threat intelligence from the following Firebox services:

Gateway AntiVirus (GAV): Signature-based malware detection

IntelligentAV (IAV): Machine-learning engine for malware detection

APT Blocker: Sandbox-based detection uses behavioral analysis to catch sophisticated and evasive malware.

I***ntrusion Prevention Service (IPS):*** Detects and blocks network attacks

DNSWatch: Blocks malicious sites through DNS filtering by preventing users from reaching known bad domains

We analyze the data recorded each quarter and provide the results to you in this report. Most importantly, we also share how you can best respond to new and growing threats in the future. We hope our Q1 2020 findings help you protect your valuable data and business.

Help Us Improve This Report

If you're a Firebox customer, you can help us improve this report, as well as improve your neighbor's and your own security, by sharing your device's threat intel. The data from the Firebox Feed comes entirely from customer devices catching real threats in the field. However, we only receive this data if you opt in to sending WatchGuard device feedback to us. Besides helping us build this report, this data and the threat team's analysis also help our company improve our products, making all Firebox owners more secure. Right now, we receive data from about 11% of the active Fireboxes in the field. If you want to improve this number, follow these three steps.

1. Upgrade to Fireware OS 11.8 or higher (we recommend 12.x)
2. Enable device feedback in your Firebox settings
3. Configure WatchGuard proxies and our security services, such as GAV, IPS and APT Blocker, if available

Malware Trends

This last quarter more Fireboxes reported to the Firebox Feed than any previous quarter. The more Fireboxes that participate in the Firebox Feed, the more accurate of a picture we can paint of the cyber threat landscape. Additionally, more Fireboxes gives us access to more samples of malware and attacks that we can analyze.

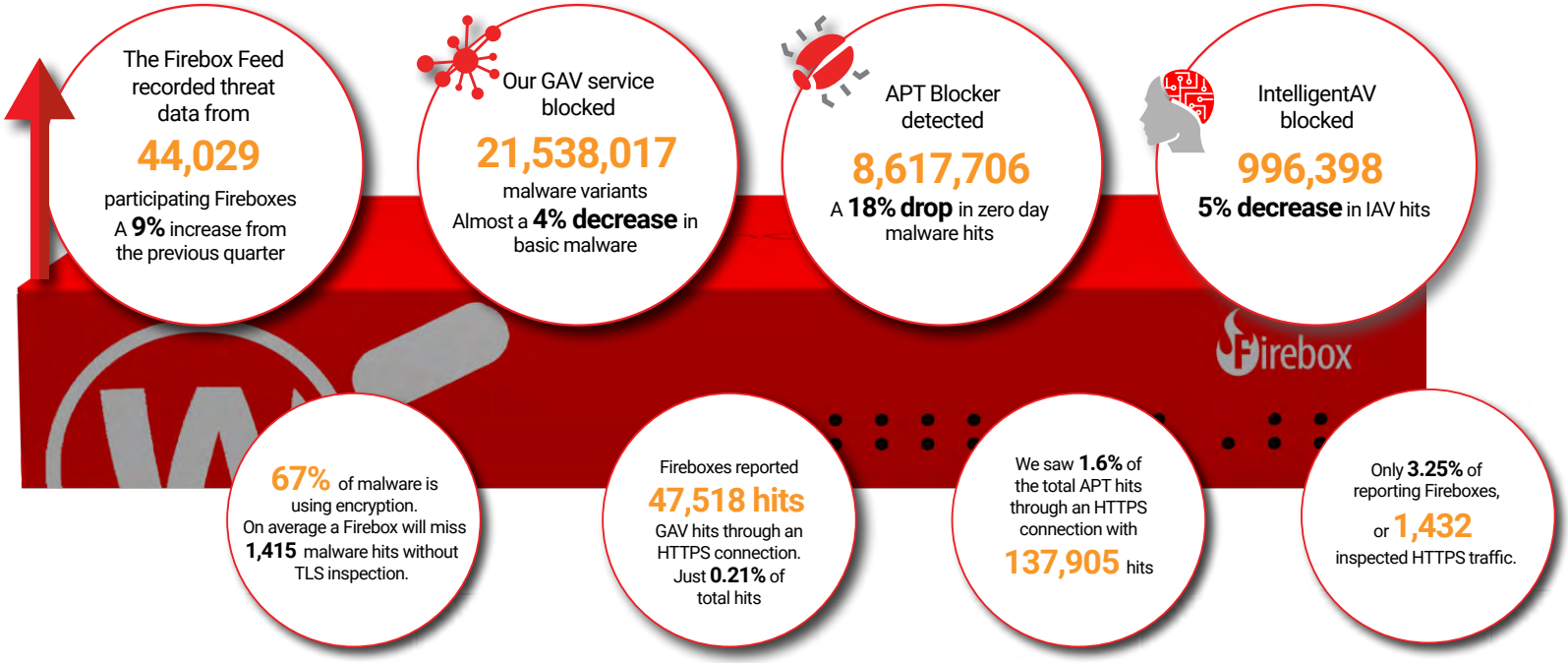
We saw a drop in the reported malware hits in Q1 and when you consider the increase in reporting Fireboxes, that equated to fewer hits per Firebox than in Q4 2019. We don't know if this downward trend represents a true trend in malware for this quarter. Many users in Q1 worked from home due to COVID-19 and Fireboxes may not scan all traffic received by those users. If true, not only does this mean the malware may not have gone down but also that many users working from home don't have the protection provided by the Firebox.

New to this quarter, we've analyzed whether malware detections arrived over an encrypted connection or not. Since many websites now use HTTPS, an encrypted connection, many WatchGuard Firebox administrators have enabled HTTPS decryption through Content Inspection to still detect hidden threats. We've analyzed data from these connections in detail to see if these results match the results we normally find in the Firebox Feed reports. This should provide more information on the type of malware seen on a website using HTTPS and what percentage of malware is sent over an encrypted connection. But first let's look at the totals for Q1.

WatchGuard Fireboxes with Total Security offer strong network protection by combining GAV, IAV, and APT Blocker.

- **Gateway AntiVirus (GAV)** instantly blocks known malware before it enters your network.
- **IAV (intelligentAV)** uses machine-learning techniques to proactively discover new malware based on hundreds of millions of good and bad files previous analyzed.
- **APT Blocker** detonates suspicious files in a complete sandbox environment and uses behavioral analysis to decide whether or not the file is good or bad.

These services block malware, beginning with GAV. Even if GAV passes a file, IAV inspects it further. Since IAV requires more memory, it only runs on rack-mounted Fireboxes. APT Blocker then checks all files that GAV and IAV clear.



Data sent to the Firebox Feed does not include any private or sensitive information. We always encourage customers and partners to opt in whenever possible to help us obtain the most accurate data.

The Firebox Feed contains five different detection services:

- Malware our **Gateway AntiVirus (GAV)** service prevents
- Malware detected by our **IntelligentAV (IAV)** machine-learning engine
- Advanced malware detected by our behavioral analysis service, **APT Blocker**
- Network exploits our **Intrusion Prevention Service (IPS)** blocks
- Connections to malicious domains blocked by **DNSWatch**

In this section, we analyze the most prolific and most widespread malware and exploit trends that we saw in Q1 2020 and provide actionable defensive tips for keeping your networks and systems safe.

Q1 2020 Overall Malware Trends

- After a previous drop last year, there was an increase in the number of reporting Fireboxes for two quarters in a row. As previously mentioned, enabling Firebox reports helps this report. See how to enable it here **WatchGuard Device Feedback**.
- With **21.5 million malicious files** blocked by the Gateway AntiVirus (GAV), we saw a small decrease in the total hits.
- IntelligentAV (IAV) maintained roughly the same number of detections, dropping just under one million hits for the quarter.
- APT Blocker dropped from a high of **10 million to 8.6 million detections.**
- New this quarter, we found that **two-thirds, 67%, of malware arriving over a web connection** comes from an encrypted TLS connection (HTTPS). If you don't inspect encrypted connections, then you miss this two-thirds of malware.

Top 5 Most-Widespread Malware Detections

During Q1, we continue with our analysis of the most widespread malware, which is malware that hit the most individual networks around the world. For each of these samples, we analyzed what percentage of networks within each individual country and region saw these threats. CVE-2017-11882 and Exploit.RTF-ObfsObjDat take the top spots again this quarter. For both malware families, we saw the most detections from email proxies like SMTP, POP3, and IMAP. Additionally, we saw Great Britain and Germany come many times in our widespread malware list, just like in previous quarters.

WatchGuard Fireboxes quickly block malware based on multiple layers of security.

When properly configured, GAV (Gateway AntiVirus) scans file signatures to identify if the signature matches a known malware. If GAV does not find a match then IAV (IntelligentAV) scans the file for in-depth analysis to identify suspicious areas in the file and blocks the file or passes it on to APT Blocker to scan it based on what IAV finds. APT Blocker fully sandboxes the file to determine what actions the file performs, then returns a result for the Firebox to act on.

Top 10 Gateway AntiVirus Malware

COUNT	THREAT NAME	CATEGORY	LAST SEEN
4,517,067	Win32/Heri	Win Code Injection	Q4 2019
1,392,297	Win32/Heim.D	Win Code Injection	Q4 2019
1,194.396	RemoteAdmin (FlawedAmmyy)	Remote Access Trojan	new
1,107,609	GenericKD (SBD)	Generic Win32	Q4 2019
1,039,689	CVE-2017-11882	Office Exploit	Q4 2019
629,913	Razy	Cryptominer/ Win Code Injection	Q4 2019
603,000	Mimikatz	Password stealer	Q4 2019
451,856	Luhe.Exploit.PDF	PDF exploit	Q4 2019
447,668	GenericKD (clusterd)	Generic Win32	Q4 2019
429,715	Hacktool.JQ	Password Stealer	Q4 2019

Figure 1: Top 10 Gateway AntiVirus Malware Detections

The new TLS information also allows us to review the malware sent over an encrypted connection. We took Firebox reports that caught malware hits over HTTPS and found the top five most-prevalent malware over TLS. While we see some threats from this list further down in the top 50 malware detections, the Top 5 Encrypted Malware threats differs from the top 10. This leads us to believe the malware sent over an encrypted connection significantly differs from malware sent unencrypted.

Top 5 Encrypted Malware Detections

COUNT	THREAT NAME	CATEGORY
14,962	JS:Adware.Lnkr	Browser Redirect
7,106	Trojan.Heur	Generic Win32
3,390	JS:Trojan.Cryxos **	Support scam
2,915	GenericKD.33016580	Generic Win32
2,228	Adware.Agent	Generic Adware

** Also seen in the Most-Widespread Malware Detections

Figure 2: Top 5 Encrypted Malware Detections

Top 5 Most Widespread Malware	Top 3 Countries by %			EMEA %	APAC %	AMER %
CVE-2017-11882. Gen (Office) *	Great Britain 36.7%	Germany 35.1%	Netherlands 30.5%	27.0%	12.2%	9.5%
Exploit.RTF-Obfs-ObjDat.Gen	Great Britain 28.8%	Germany 24.5%	Turkey 23.3%	18.1%	9.1%	6.0%
JS:Trojan.Cryxos **	Hong Kong 21.0%	New Zealand 18.9%	Belgium 15.6%	11.9%	6.5%	5.1%
Trojan.AutoIT. Agent	Great Britain 21.4%	Germany 20.1%	Turkey 18.9%	13.1%	3.1%	3.2%
Trojan.GenericKDZ	Switzerland 16.9%	Germany 15.8%	Belgium 15.8%	10.8%	4.6%	4.0%

Figure 3: Top 5 Most-Widespread Malware Detections

* Also seen in the Top 10 Gateway AntiVirus Malware Detections
** Also seen in the Top 5 Encrypted Malware Detections

JS:Trojan.Cryxos

We have seen Trojan.Cryxos many times in this report and recently wrote about **a variant here.** However, this malware doesn't normally target Hong Kong like we saw this quarter. We investigated it further to try to find out why but didn't determine the reason based on the malware. Normally we would see variants that used a specific language as part of their hook but that was not the case here. Nonetheless, we did find some interesting data on this malware.

You will likely see this variant of Trojan.Cryxos attached to an email disguised as an invoice. We couldn't find an example of this email but Trojan.Cryxos malware normally spreads this way. If the victim opens the attachment (an HTML file) a web page opens with information on a fake file. If they try downloading it then the web page asks for a username and password to see the file. Filling out the form doesn't lead you to any file or page, but it does send the username and password to a compromised WordPress site where the attacking server stores the input.

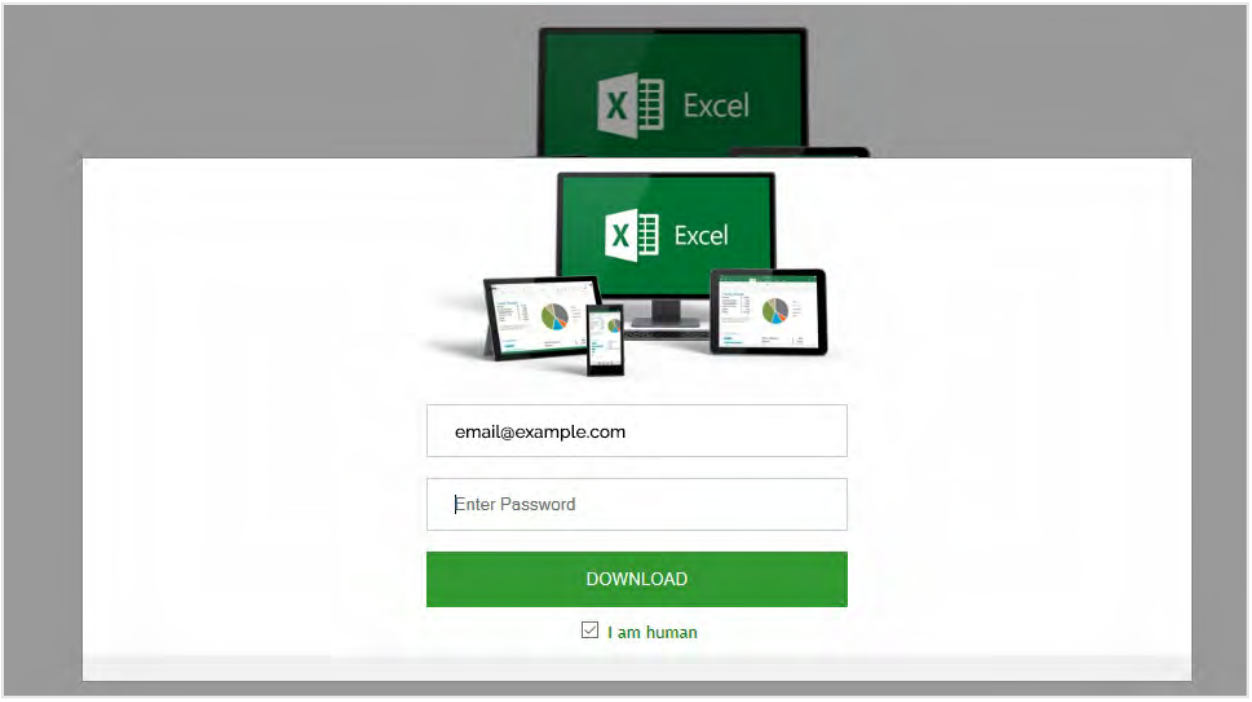


Figure 4: Cryxos fake login to fool victims

This example of Cryxos sends the username and password to **https://tte-japan[.]com/wp-includes/pomo/attach/excel/report-maerskline[.]php**. The title of the page "report-maerskline.php" gives us a hint of what you might see in the email. Maersk Line is a large shipping company often targeted by spam and malware. The email likely asks the recipient to open an invoice like the **one shown here**.

Besides the file showing up in our malware list, we could immediately tell this file contains malware when we opened it. The checkbox for 'I am human' doesn't make sense. It was already checked so serves no purpose. Also, the 'DOWNLOAD' button doesn't lead to an Office365 domain but to the WordPress site we discussed earlier.

With the victim's username and password, the malware creators may take over the victim's email account and other accounts associated with the email.

We verified the malware targeted Hong Kong and the region but couldn't determine who created this malware. If part of a bigger attack, we expect these attacks or similar malware to continue in Hong Kong until the attacker obtains the account information they want.

As a precaution, always check the links you click on by hovering over them, and don't click on any links from emails you don't expect.

Lnkr

Lnkr made it in to the top 5 encrypted malware while also landing in the top 20 unencrypted malware hits. This Chrome extension adds advertisements to websites, and hides behind obfuscated code and code from other Chrome extensions. The original malware came from a hijacked Chrome extension called Flash Player (not the same official Abobe Flash Player used by browsers in the past, but a different Chrome extension).

There are many ways malicious actors can obfuscate code to make it harder for the good guys to analyze. One technique attackers commonly leverage is simple encoding or data transformation tricks. Computers can store the same information in many different types of formats or encoding standards. For example, if you run a normal human-readable script through a base64 encoder, you get something that looks like gibberish to a human, and yet a computer can still understand and run that encoded script. We were able to deobfuscate our Lnkr sample's basic encoding obfuscation and get a clean sample of code to analyze.

However, data transformation is only one of a hacker's obfuscation tricks. Another example is something called code flow obfuscation. At a high level, attackers essentially design their code to be purposely obtuse and complex. They use nonsensically named variables, too many functions, and essentially code everything the hard and illogical way on purpose, to make their code much harder for a programmer to follow. Even with the clean version of Lnkr, we found over 1,000 functions and 48 regex lines of code to hide the true intentions on this malware. In one function, it creates a tracking pixel that identifies the pages you visit. It does this by creating an invisible small picture and forcing your browser to make a request for the picture.

```
var q = f.createElement("img");

            q.setAttribute("style",
"width:0;height:0;display:none;visibility:hidden;");

            q.src = a + (a.indexOf("?") == -1 ? "?" : "&") + "t=" + (new
Date().getTime());

            (document.head || document.documentElement).appendChild(q);
```

The script creates a variable "q" as an HTML image element. The variable "f" likely connects to the HTML document. In the next line the script sets the image attributes to have a width and height of 0,which hides the image and doesn't display it on the page itself. "q.src" adds the image URL to include the web page "serenityart[.]biz/metric/", the variable "a". It also checks if there are any URL request path parameters in URL path variable "a" by looking for the index (location) of the character "?" (the character that signals the start of URL request path parameters). If the URL doesn't already have any request path parameters (signified by an index of -1), it appends the special character "?" and the request path parameter "t", setting it to equal the current time stamp. If the request URL does already have request path parameters, it instead appends the time parameter after the character "&" (indicating an additional request path parameter). The last line adds this image to the document header or the document itself if it doesn't have a header.

Based on the code we reviewed the authors of the Lnkr extension could easily add a script to hijack credentials if they wanted to. Since they stole the extension from another author, we believe this could happen if not taken down.

We reviewed a copy of the malware in our testing environment and found it changed our search preferences from Google to Yahoo. Malware commonly makes this change possibly to make it easier to track users. The copy we received didn't show any additional ads, but we know **from reports**, the original did. The fact that this extension could add code to any site you visit creates a big security hole. Attackers could use it to add arbitrary malicious JavaScript to every site, which among other things could allow them to steal your site credentials.

Watch out for links that lead to Chrome extension addons. These often are malicious and unless you are searching for a particular extension don't add it. You should try to only install extensions from your browser's official extension repository, which at least has slightly more curation than random extensions found on the Internet. If you must install any browser extension, check the author of the extension and see if other extensions they create look suspicious. Don't ever add an extension from a site you don't completely trust.

RemoteAdmin (Flawed-Ammyy)

We saw the malware "RemoteAdmin", also called "Flawed-Ammyy" for the first time in Q1. If you haven't heard of it, Ammyy Admin is free remote desktop software that allows you to control your computers from any location on the Internet. Ammyy Admin's history of weak website and product security doesn't sit well with us and many antivirus creators. Though not malicious by itself, a willful ignorance of security has caused many antivirus programs to mark this file as malicious. Additionally, attackers exceedingly use this free software.

Ammyy Admin allows remote access to your computers, which can be somewhat dangerous even when used legitimately. While many support centers including our own provide support over a remote desktop connection, scammers can also use this to access the computer of an unsuspecting user. Scammers like this software because in the past you could get full access to another computer with just the ID and confirmation from the other side. See more about this scam in our **2018 Q4 report**.

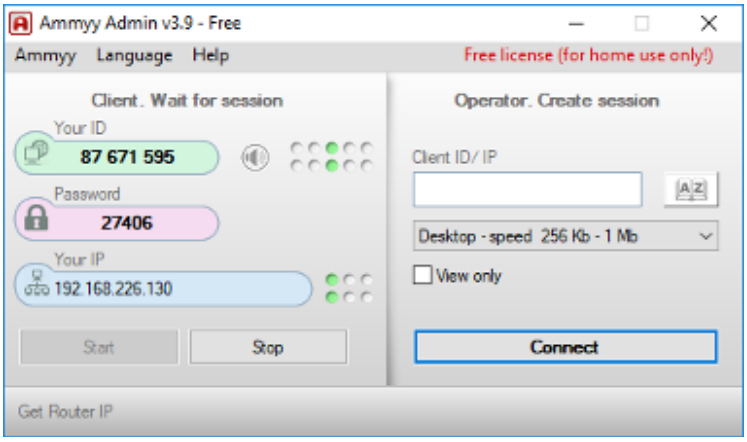


Figure 5: Ammyy starting up

Also, we found out that **Ammyy had the trojan** Lurk and other malware packaged with Ammyy Admin over the last few years. At one point Ammyy Admin and the Ammyy website distributed six different malicious files over the course of just one year.

Recent updates have added some security features, including digitally signing the install package and software and the basic addition of a password to remotely log onto a computer. We hope they continue to improve their software security and the security of their website.

As always, never download files from an untrusted source. Also, know what a Microsoft scam looks like. Microsoft will never call you first and will never give a phone number to call with an error.

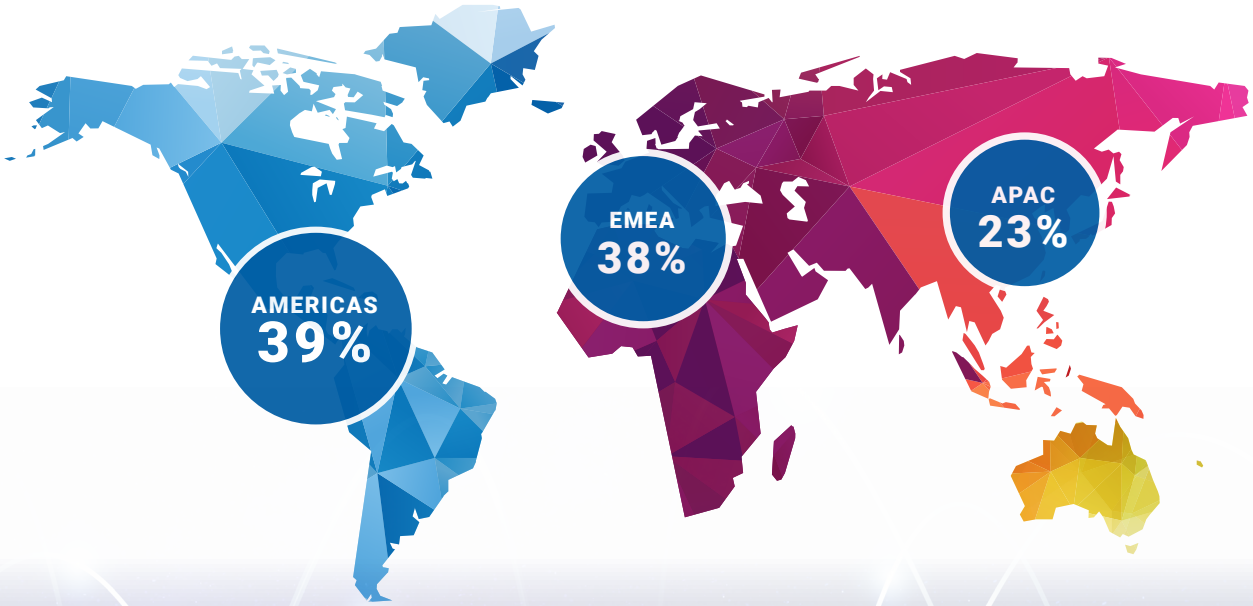
Geographic Threats by Region

Weighted regional data this quarter shows an increase in malware for the EMEA region and a drop in malware in the AMER region. APAC also saw a small drop. As with previous quarters, we weight the malware in each region depending on the number of Fireboxes in that region. That said, this quarter may be an outlier as the global pandemic might have shifted the world's workforce to some extent.

In Q1, Germany saw the majority of Luhe.Exploit.PDF and Exploit.CVE-2017-11882 (a malicious Office file) malware volume, and also saw Exploit.CVE-2017-11882 on their regional widespread list. While Great Britain accounted for the most-widespread use of Exploit.CVE-2017-11882, it didn't see as much total volume as some other countries. Germany and Italy accounted for more of the total detections by volume.

Razy normally targets the APAC region, especially countries in the southeast of APAC. This quarter Chile became the most targeted country in part due to a few devices accounting for most Razy hits. For more on Razy see our review of it in the **2018 Q3 report.**

Malware Attacks by Region



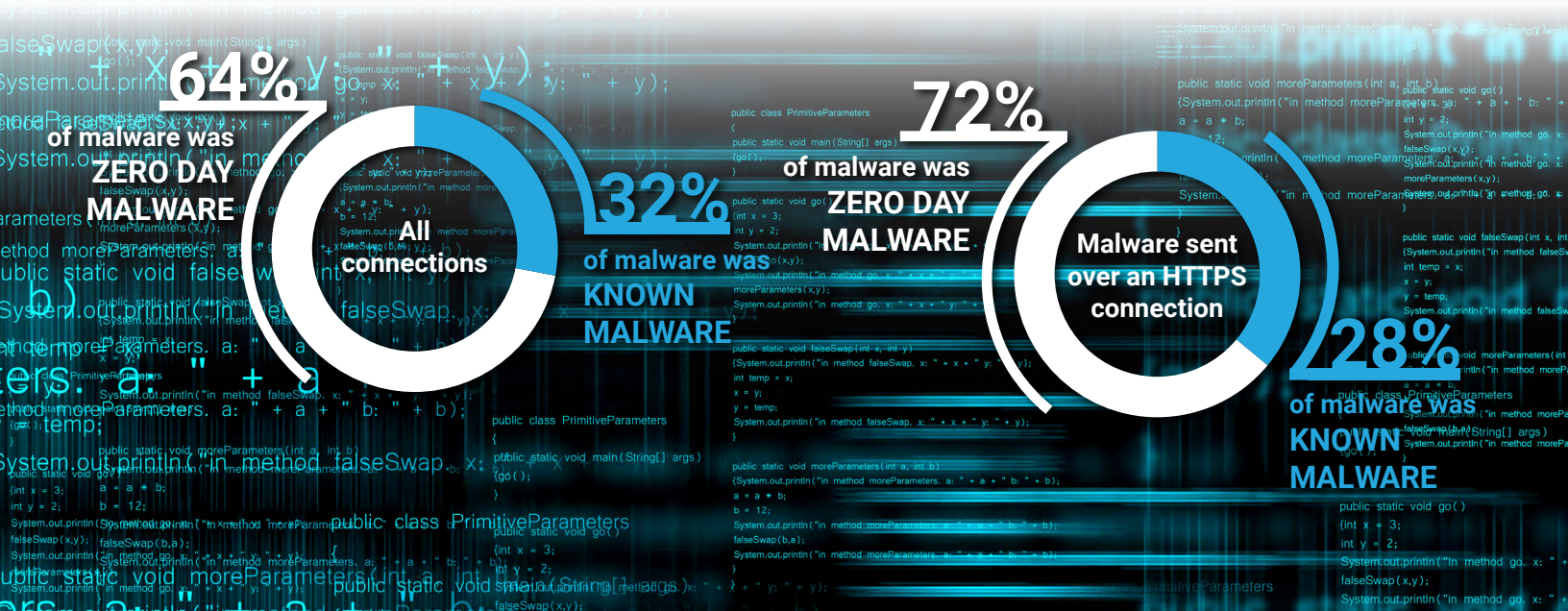
Catching Evasive Malware

During Q4, 2019, we saw record-breaking zero day malware numbers, with over 10 million hits. Fortunately, the zero day malware number dropped some but not back to its normal average (of ~37%). We still saw over 8.6 million hits during Q1. These zero day malware detections are threats that otherwise would pass into the network if not for advanced malware tools like APT Blocker. In short, the zero day malware percentage for this quarter was still at a massive 63%, meaning you'd miss close to two-thirds of malware without more advanced detection technologies.

Web connections come in two flavors, unencrypted HTTP and encrypted HTTPS. A Firebox can easily scan the traffic sent as clear text over unencrypted connections using the appropriate proxy for the traffic, assuming you have enabled security services. However, while a Firebox can totally allow or deny encrypted HTTPS traffic, it can't see into that encrypted traffic by default, which means it can't scan HTTPS traffic for malware by default either. That's where WatchGuard's HTTPS Content Inspection comes in. By enabling the Firebox's HTTPS Content Inspection, you can allow your Firebox to apply its security services to encrypted HTTPS traffic too. Setting this up does require some digital certificate configuration on your clients or Firebox though. The easiest set-up requires a trusted PKI (public key infrastructure) that includes the Firebox's Certificate Authority as a trusted certificate.

As previously mentioned, we analyzed threats that passed over these encrypted channels from Fireboxes with decryption (HTTPS Content Inspection) enabled. In this new data, we see malware caught from all services on the Firebox consists of 67% encrypted traffic and 33% unencrypted. This new analysis of the TLS data provided us a better look at the total malware networks receive. If we assume that all Fireboxes receive the same amount of encrypted malware as these Fireboxes report, then each Firebox receives just over 2,100 threats in Q1 with 1,400 of those threats passing right through if the Firebox doesn't inspect these encrypted connections. Even more frightening, the zero day malware percentage for encrypted threats was even higher, at 72%. If you are not scanning encrypted traffic you are missing a lion share of the most advanced malware.

Removing malware before it enters the network is one part of a layered defense strategy. Additionally, signature-based anti-malware engines do a great job of quickly catching known threats, but they don't block most of the malware we see today unless you combine it with inspection of encrypted traffic and advance anti-malware engines like IntelligentAV and APT Blocker. For the best protection from your Firebox, you should use our Total Security Suite and be sure to enable HTTPS inspection!



Network Attack Trends

The Firebox's Intrusion Prevention Service (IPS) detects and blocks network attacks and application exploit attempts before they can compromise a vulnerable system. IPS uses a set of frequently updated signatures to analyze network traffic and identify these threats, which usually come hidden in web requests or even in application-specific data.

This quarter, Firebox security appliances participating in the Firebox Feed detected and blocked 1,660,904 threats using the IPS service, coming out to about 38 threats per appliance. The total volume of blocked threats is down roughly 11.6% from the previous quarter. This drop, when paired with the increase in reporting Fireboxes, led to a 19% reduction in threats blocked per appliance. On the other hand, the number of unique signatures triggered across all appliances reached 356, up 3% when compared to last quarter.

While the top 10 network attacks by volume rarely changes from quarter to quarter, this quarter saw two brand-new inclusions in the top 10, including a signature matching a SQL injection attack and one matching a 2017 Adobe Acrobat vulnerability. We'll highlight both of these new additions in detail later in this section.

Here are the network attack highlights for Q1 2020:

- During Q1 2020, **Firebox appliances globally blocked 1,660,904 network attacks** equating to 38 threats per appliance.
- Firebox appliances globally detected and **blocked 356 unique attack signatures** this quarter, up slightly from Q4 2019.
- There were **two new attacks in the top 10 by volume**; the remaining eight were all seen previously in other quarters.

Quarter/ Year	IPS Hits
Q4 2016	3,038,088
Q1 2017	4,151,210
Q2 2017	2,902,984
Q3 2017	1,612,303
Q4 2017	6,907,718
Q1 2018	10,516,672
Q2 2018	1,034,606
Q3 2018	851,554
Q4 2018	1,244,146
Q1 2019	989,750
Q2 2019	2,265,425
Q3 2019	2,398,986
Q4 2019	1,878,730
Q1 2020	1,660,904

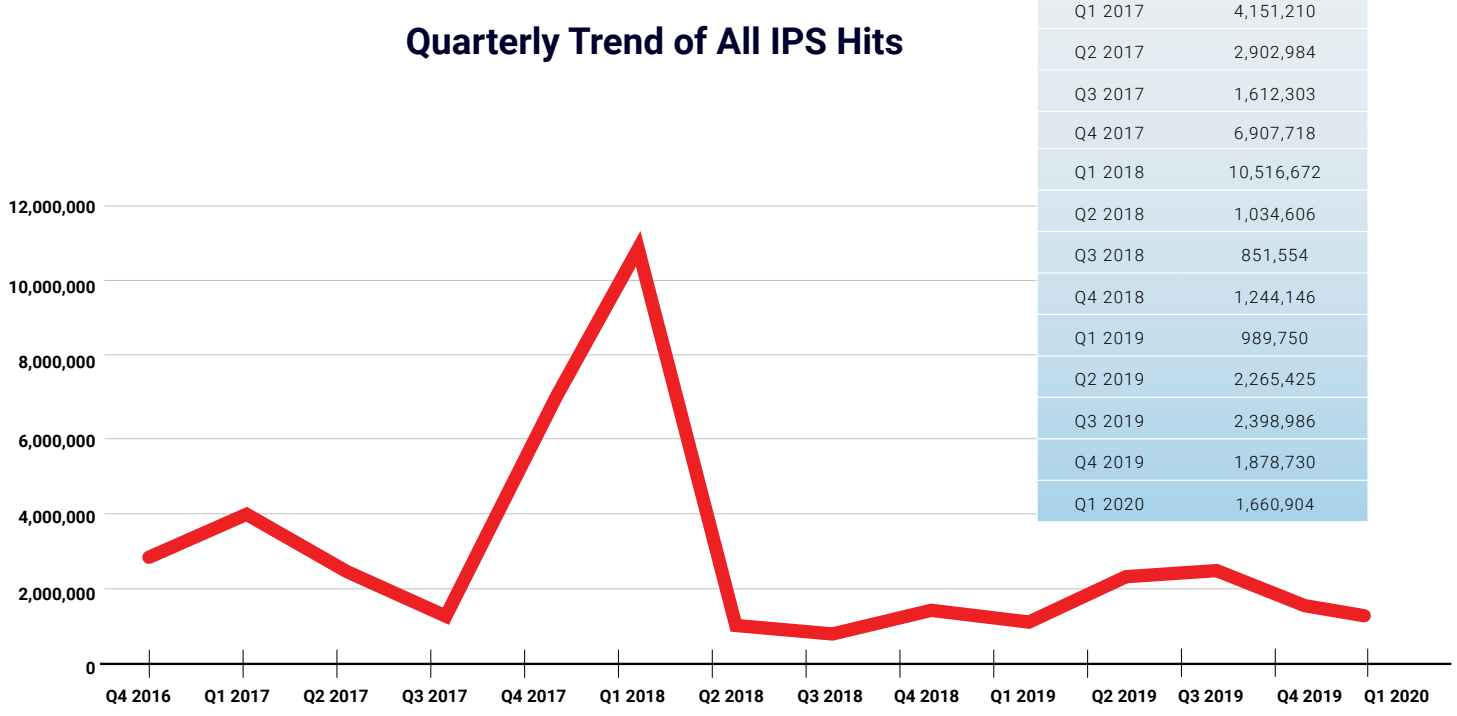


Figure 6: Quarterly Trends of All IPS Hits

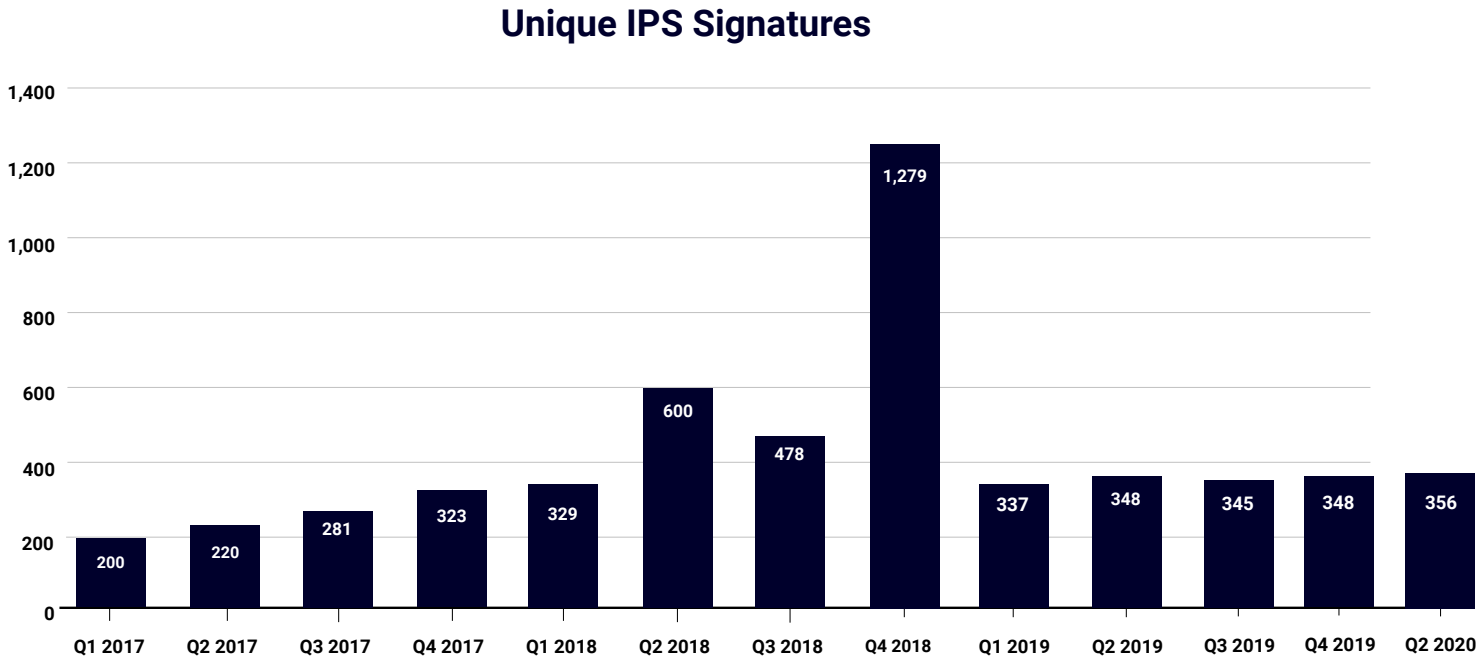


Figure 7: Quarterly Trends of Unique IPS Signatures

Top 10 Network Attacks Review

If you're a regular reader of this report, you've already noticed that the top 10 network attacks by volume remains relatively consistent quarter over quarter with any differences typically limited to individual threats moving to different positions on the leaderboard. This quarter though, the top 10 attacks by volume included two new additions, WEB SQL Injection Attempt -4 and FILE Adobe Acrobat ImageConversion EMF Parsing Integer Overflow (CVE-2017-11227), both of which we will cover in more detail shortly.

The top threat from Q4 2019, a signature that also matches a SQL injection attempt, remained in the leading position this quarter, accounting for **nearly 36% of all network attack detections**. While such a large share of total detections might seem like an anomaly, they were spread across over **2,300 individual networks**, a sizable portion of our dataset.

Signature	Type	Name	Affected OS	CVE	Count
1059160	Web Attacks	WEB SQL injection attempt -33	Windows, Linux, FreeBSD, Solaris, Other Unix	N/A	592,726
1133407	Web Attacks	WEB Brute Force Login -1.1021	Linux, FreeBSD, Solaris, Other Unix, Network Device, Others	N/A	224,610
1133451	Access Control	WEB Cross-site Scripting -36	Windows, Linux, FreeBSD, Solaris, Other Unix, Network Device	CVE-2011-2133	151,363
1057664	Buffer Overflow	WEB Nginx ngx_http_parse_chunked Buffer Overflow -1 (CVE-2013-2028)	Windows, Linux, FreeBSD, Solaris, Other Unix, Mac OS	CVE-2013-2028	83,303
1054837	Web Attacks	WEB Remote File Inclusion /etc/passwd	Windows, Linux, FreeBSD, Solaris, Other Unix	CVE-2014-7863	73,496
1055396	Web Attacks	WEB Cross-site Scripting -9	Windows, Linux, FreeBSD, Solaris, Other Unix, Network Device	CVE-2017-0378	56,527
1056282	Web Attacks	WEB Ruby on Rails Where Hash SQL Injection (CVE-2012-2695)	Windows, Linux, FreeBSD, Solaris, Mac OS	CVE-2012-2695	54,651
1049802	Web Attacks	WEB Directory Traversal -4	Windows, Linux, FreeBSD, Solaris, Other Unix, Mac OS	CVE-2018-15535	49,807
1055065	Web Attacks	WEB SQL Injection Attempt -4	Windows, Linux, FreeBSD, Other Unix	N/A	25,234
1134169	Misc	FILE Adobe Acrobat ImageConversion EMF Parsing Integer Overflow (CVE-2017-11227)	ALL	CVE-2017-11249	24,422

Figure 8: Top 10 Network Attacks, Q1 2020

New Network Attacks

The first new threat to the top 10, WEB SQL Injection Attempt -4 came in at #9. We covered a similar SQL injection signature in the Q1 2019 report when it popped up the top 10 list for the first time. As a refresher, SQL (pronounced see-quil) is a popular database protocol for websites and web apps. If web forms (places where users can enter information like a name or email address) don't properly sanitize input before using it to query the database, it could allow an attacker to escape the bounds of the original query and create their own request to the database. A knowledgeable attacker could use this to modify or delete the user database, bypass authentication, or potentially steal information in large quantities.

SQL injection attacks aren't new, in fact they are one of the oldest web app attacks in the book. Unfortunately, no developer is perfect and occasionally mistakes slip through the cracks and enable this class of attack. In our Q4 2019 report, we noted an 8000% (!) increase in detections of a specific SQL injection signature throughout the year.

The second new signature is a three-year-old memory corruption vulnerability in Adobe Acrobat Reader. Adobe patched this vulnerability back in August 2017 along with over three dozen other memory corruption vulnerabilities in a massive security patch. This particular vulnerability could have allowed an attacker to obtain code execution by tricking a victim into opening a tainted file. Though this vulnerability is extremely old, attackers often keep popular old exploits in their arsenal since they still can get significant hits from users who don't patch for one reason or another.

Most Widespread Network Attacks

Signature	Name	Top 3 Countries			AMER	EMEA	APAC
1133451	WEB Cross-site Scripting -36	Germany 74.36%	Spain 69.3%	Great Britain 60.67%	50.7	60.47	51.59
1059160	WEB SQL Injection attempt -33	Canada 71.97%	USA 68.35%	Great Britain 61.51%	66.72	46.82	46.29
1057877	WEB Apache Struts Wildcard Matching OGNL Code Execution -1	Brazil 45.45%	Great Britain 44.37%	France 43.58%	39.06	35.51	15.9
1131620	WEB Cross-site Scripting -30	Brazil 55.37%	USA 50.18%	Great Britain 46.22%	49.55	30.87	10.95
1055396	Web Cross-site Scripting -9	USA 43.2%	Canada 40.15%	Great Britain 32.94%	40.3	28.43	30.39

Figure 9: Most-Widespread Network Attacks Q1 2020

The top five most-widespread attacks represent the five threats that affected the most individual networks across the world. The above table shows which countries had the highest percentage of networks within their boarders detect and block each of the threats, as well as the percentage of networks within each of the three global regions that detected and blocked the threats.

All five of the threats follow a similar trend, they are easily scriptable for automated attacks. It makes sense that we would see this style of attack affect a large number of individual networks since an attacker could simply spin up a crawler to run through every IP address on the Internet and run code to test and attempt an exploit. Interestingly, Great Britain earned a spot in the top three countries for each of these highlighted threats. In Q1 2020, it appears that networks in Great Britain were popular targets.

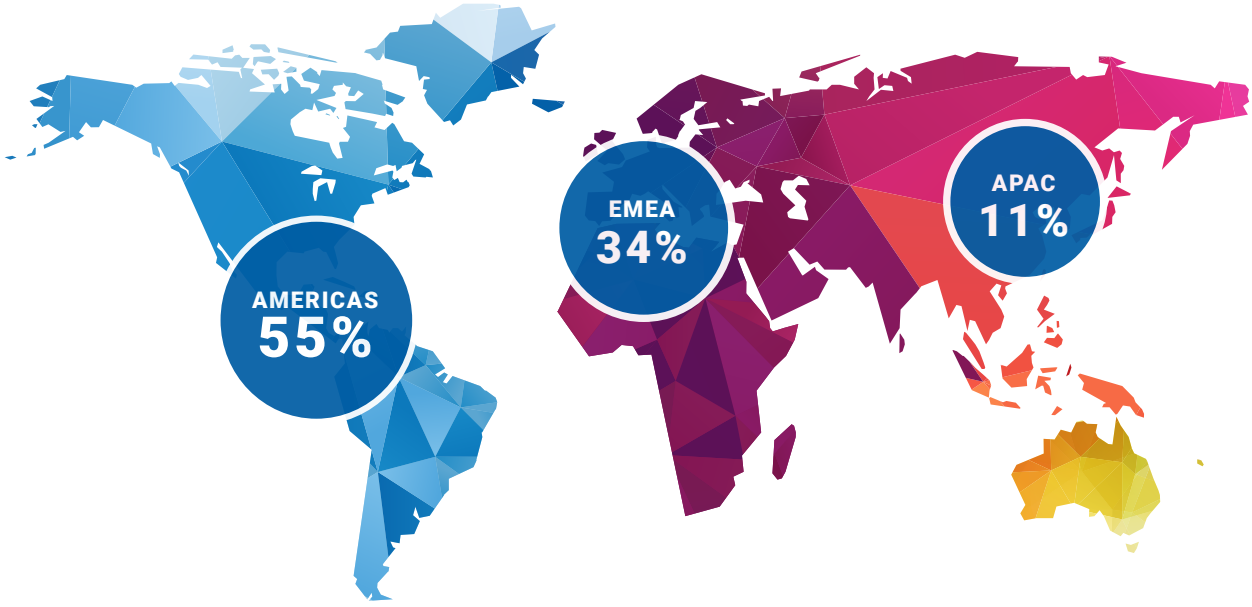
The most-widespread detection, a signature designed to catch generic cross-site scripting (XSS) attacks, impacted more than half of all networks through each of the three major regions across the world. Nearly two-thirds of all Firebox appliances in the Americas region detected and blocked attacks that matched the top network attack by volume mentioned earlier in this section.

Overall Geographic Attack Distribution

Geographically, the Americas (AMER) received 55% of all attacks, Europe, the Middle East and Africa (EMEA) received 34% and the Asia and Pacific (APAC) region accounted for the remaining 11% of the global share.

The global spread of network attacks shifted only slightly from the previous quarter, with AMER and APAC both decreasing from 59% and 16% of the share respectively and EMEA increasing from Q4's 25%. This is the second quarter in a row where the AMER and APAC regions trended downward in their share of detections.

Network Attacks by Region



DNS Analysis

In the first quarter of 2019 we introduced the DNS Analysis subsection under the Network Attack Trends section to showcase malicious trends derived from DNSWatch and DNSWatchGO, WatchGuard's DNS firewall and content filtering services. Now, DNS Analysis has expanded into its own section in order to more thoroughly dissect specific domains the DNSWatch Support Team has uncovered every quarter. DNSWatch is a Cloud-based service that intercepts Domain Name Service (DNS) requests and redirects known malicious domains to the DNSWatch Blackhole. Considering DNSWatch intercepts DNS requests, it can redirect traffic regardless of the application protocol. As more users utilize these DNSWatch services, the more information we are able to triage and relay to protect all of our users.

This section continues similar analyses as last quarter where we cover the top malware domains, compromised domains, and phishing domains, respectively.

WARNING

It should go without saying that you should not visit any of the malicious links we share in this report; at least without knowing exactly what you are doing. Anytime you see us share a domain or URL where we have purposely added brackets around a dot (e.g. www[.]site[.]com), we are both making the hyperlink unclickable and warning you not to visit the malicious site in question. Please avoid these sites unless you are a fellow researcher who knows how to protect yourself.

Top Malware Domains

Only two previous domains managed to stay in the top malware domains list this quarter while a surprising eight domains made their debut. The most predominant, bellsyscdn[.]com, was responsible for over half of the top malware domain blocks for this quarter. This is because the domain is a C&C server for the Bondat worm, which has shown an uncharacteristic increase in activity this quarter. The Bondat worm family seeks to propagate through networks to create a botnet that performs Monero cryptomining, attacks on WordPress sites, and other malicious behaviors depending on the worm variant. Luckily, Anubis Networks has taken control of the domain and diverted all its traffic to their sinkhole. However, that doesn't stop active infections from beaconing out, hence the detections.

Malware	
Domain	**Hits**
bellsyscdn.com *	434836
dc44qjwal3p07.cloud-front.net	112554
d3i1asoswufp5k.cloud-front.net	46331
newage.radnewage.com *	33997
newage.newminersage.com *	33622
hrtests.ru *	12303
profetest.ru *	11857
ms-dll-com.info *	9610
passportinfo.info *	8516
testpsy.ru *	7302

* Denotes the domain has never been in the top 10

Five of the new domains on the list are also included in malicious Monero cryptomining campaigns. The first two, newage[.]radnewage[.]com and newage[.]newminersage[.]com, share the same IP address and are both associated with the malware variant Retadup. Retadup can also deliver different payloads such as ransomware and password harvesters as well. We discovered these two C&C domains almost two years ago when they still ravaged Latin America and South America, the two locations Retadup most hit according to Avast researcher Jan Vojtěšek. Thankfully, Avast worked with the FBI and the French National Gendarmerie's Cybercrime Fighting Center (C3N) to "disinfect" systems with Retadup beginning in July of 2019. This technique drastically slowed down the worm but, considering we are still seeing alerts associated with C2 servers of Retadup, it hasn't gone away just yet. If you want to know more about the Retadup worm, Jan Vojtěšek authored a more detail write-up **here**.

The other three domains, hrtests[.]ru, profetest[.]ru, and testpsy[.]ru, are part of the widespread PhotoMiner worm. Researchers from Guardicore first discovered PhotoMiner in early 2016 when they detected a global automated attack that was rapidly uploading suspicious files to vulnerable FTP servers. It primarily affected Asia, eastern Europe, and the United States but still has the capability to spread further as of this writing. Daniel Goldberg from Guardicore describes PhotoMiner in more detail via their **official blog**.

The final two new domains on the top malware domains list were ms-dll-com[.]info and passportinfo[.]info. First, passportinfo[.]info is very similar to a legitimate informational website for United States passports – passportinfo[.]com. However, the malicious passportinfo[.]info domain is hosting a trojan that changes DNS settings and redirects users to a malicious website. The trojan also gives an attacker the capability to download advertisements, call home to its C&C server, and execute PowerShell commands remotely. The other domain, ms-dll-com[.]info, is part of the **DoppelPaymer ransomware** infrastructure. This ransomware variant was discovered in the early summer of 2019 and asks users for a ransom in the range from 2 Bitcoin (BTC) to 100 Bitcoin (BTC) or $20k to $100k respectively. Even worse news from victims, the DoppelPaymer Tor payment site claims to re-sell encrypted information if the ransom is not paid.

```
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorythm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

        DO NOT RESET OR SHUTDOWN - files may be damaged.
        DO NOT RENAME OR MOVE the encrypted and readme files.
        DO NOT DELETE readme files.
        DO NOT use any recovery software with restoring files overwriting encrypted.
        This may lead to the impossibility of recovery of the certain files.


To get info (decrypt your files) contact us at your personal page:

        1. Download and install Tor Browser: https://www.torproject.org/download/
        2. After a successful installation, run the browser and wait for initialization.
        3. Type in the address bar:

                        REDACTED

        4. Follow the instructions on the site
        5. You should get in contact in 48 HOURS since your systems been infected.
        6. The link above is valid for 7 days.
           After that period if you not get in contact
           your local data would be lost completely.


The faster you get in contact - the lower price you can expect.

DATA
AQAAAD0BAgAAEGYAAACkAAAVZbpNets6EP1bQXd7Gb8IcODGmeKDm5FmsMolp/RYzI0ljRcE2tH4
jZ2CksvKFzlBulRwa7P5l6dvX5VhxEHyj0TeLTwSFpIsBbJyRHNbl/G6biex/0RKKmkCkJ9gqIvi
vy8o9U122c6jdeqr+ViaYpYYODwOwCa2AJsolPYqJ4B9ek7TCOBdjNKMSAyBZ+M5gQrlNeOmYgGs
itXGyCwiwTNJrGDdXFINkSTRwlmMJbg6D@gxOHUnfbjIilVAJikHO3ORs/9kQ0CliOfFJ2owhwLQ
iE66ds59Dq/aSby/JRKuFrPSatuwf6TqLhXTKn6CnCqT1fNJY0dlzZiMxJSV
```

Figure 10: DoppelPaymer Ransom Note taken from **CrowdStrike**

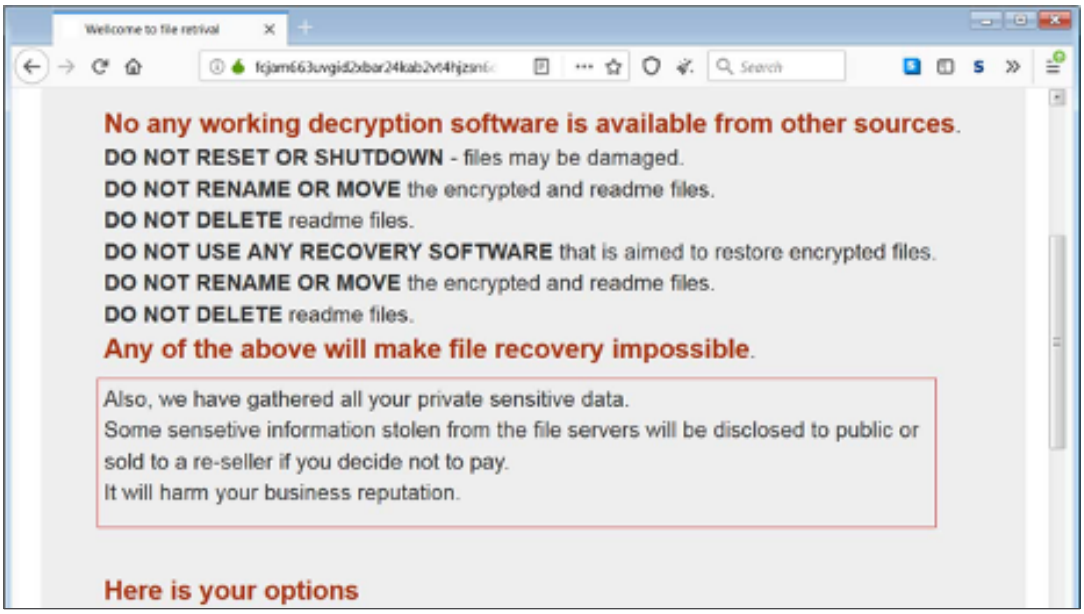
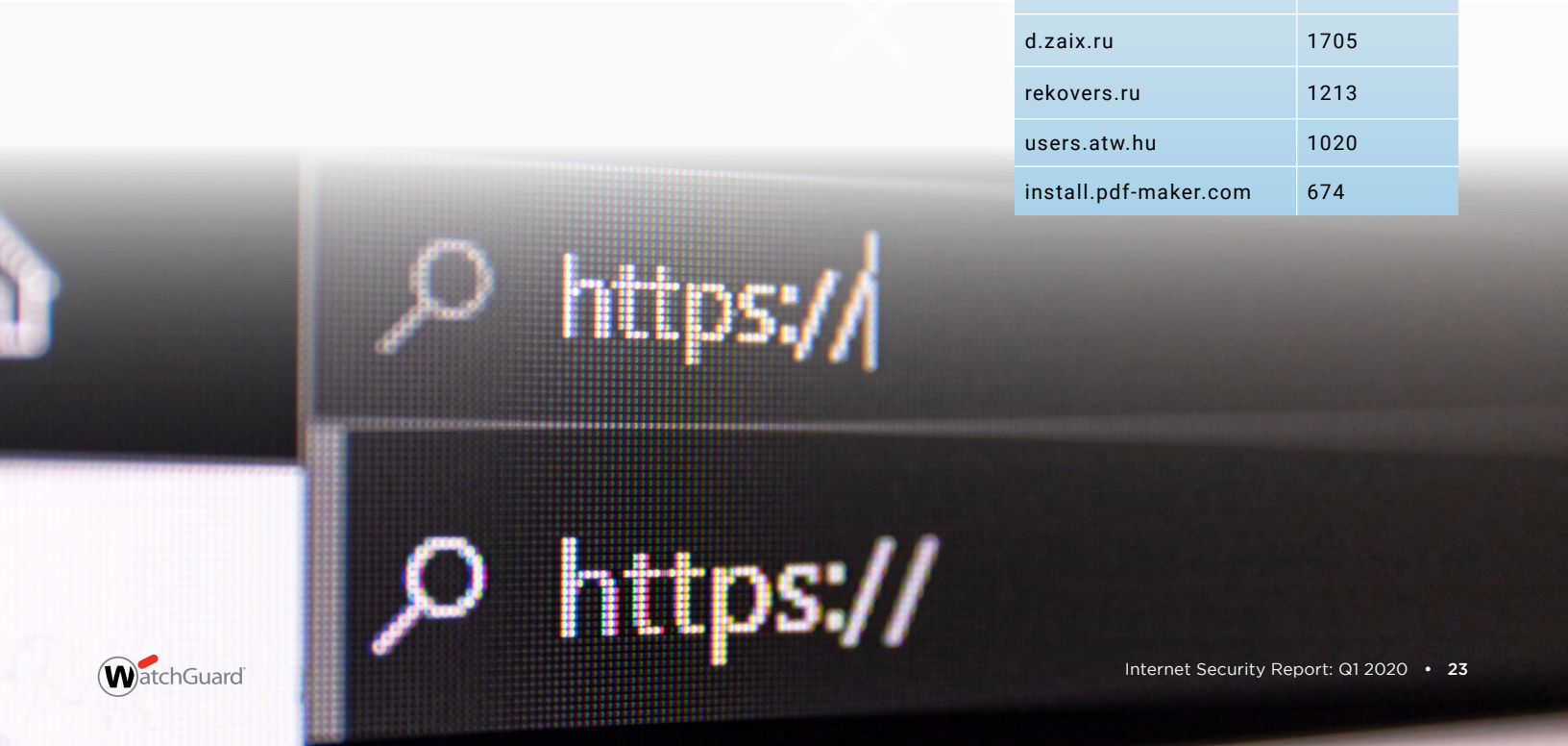


Figure 11: The DoppelPaymer Tor Payment Site for paying ransom taken from BleepingComputer

Top Compromised Websites

We saw a decrease in the number of compromised websites in Q1 of 2020 and as such, we also saw a decrease in the number of hits from the top compromised website domains category as well. Additionally, in this quarter there were no new top compromised domains to report on.

Compromised	
Domain	**Hits**
differentia.ru	1590707
disorderstatus.ru	160990
update.intelliadmin.com	67756
0.nextyourcontent.com	10046
sharebutton.co	6713
o4uxrk33.com	1978
d.zaix.ru	1705
rekovers.ru	1213
users.atw.hu	1020
install.pdf-maker.com	674



Top Phishing Domains

Phishing is a social engineering attack in which an attacker attempts to trick a victim into giving up sensitive information through various communication avenues, the most common being email. This quarter we identified three new domains in our top phishing domains category. The top inclusion, cook[.]shortest-route[.]com, is hosting a phishing campaign that is impersonating Mapp, a digital marketing and analytics company. More specifically, the phishing campaign is impersonating Mapp Engage, Mapp's solution to better interface with customers based on data-driven analytics. Cook[.]shortest-route[.]com appears to be hosting this website as part of a spear phishing campaign of known Mapp Engage users based on our analysis in DNSWatch.

Hacheyou[.]com is another new inclusion to the list and it currently has an ongoing phishing campaign impersonating Bet365, which as you can probably guess, is an online betting platform. The phishing campaign is in Chinese so any non-Chinese speaking victims should become immediately aware of this attempt. The final phishing campaign we tracked, secure[.]counterpath[.]com, is no longer active as of this writing, but it hosted a phishing campaign that was impersonating an AT&T login page.

Phishing	
Domain	**Hits**
uk.at.atwola.com	5865
fres-news.com	5520
cook.shortest-route.com *	3788
app.nihaocloud.com	2384
usd383org-my.share-point.com	1933
secure.counterpath.com *	634
email.veromailer.com	515
hacheyou.com *	392
click.icptrack.com	326
karrasconsulting.net	298

* Denotes the domain has never been in the top 10

Figure 12: Screenshot of the homepage for hacheyou[.]com

This quarter we saw firsthand how cryptocurrency is being leveraged by attackers to increase their theft endeavors. Bondat, Retadup, and Photominer are all cryptojacking worms that mine the Monero (XMR) cryptocurrency. The DoppelPaymer ransomware leverages cryptocurrency as well by using a ransomware attack and demanding payment of Bitcoin on their Tor website. In addition to these findings, we continued to discover phishing pages that spoof genuine organizations such as the United States Passport Informational site, AT&T, Mapp, and Bet365. We anticipate next quarter to see a spike in traffic related to the COVID-19 pandemic as we have already started to discover malicious websites in relation to that.

Firebox Feed: Defense Learnings

Our new insights into malware sent over TLS (primarily secure web connections) allowed us to spot a significant hole in security for many customers. We always suspected there was a significant blind spot and now the data shows the extent of the issue. Luckily, thanks to technologies like TLS inspection (called HTTPS Content Inspection on WatchGuard Fireboxes), network perimeter devices can still secure the network and here we provide some tips on how to do that.

TLS Inspection Is a Necessity

Only inspecting unencrypted traffic doesn't cut it anymore. If you don't inspect TLS encrypted traffic, you will only catch a third of the malware coming into your network. Configure your network perimeter to inspect encrypted traffic in a secure way with the use of trusted certificates. For WatchGuard customers, you can learn how to do so in this guide. While it is a bit of extra work, once completed, the firewall will have visibility into the other two-thirds of malware you'd miss otherwise.

Use a Layered Defense

Using an outdated single layer of defense on your network perimeter is not enough to block most attacks. No antivirus product can protect you from every malware variant but a layered defense — consisting not only of signature-based security but also machine learning, malware sandboxing, and education of the end user — can increase your chances against the current threat landscape significantly. For WatchGuard customers, combining GAV, IntelligentAV, APT Blocker, and DNSWatch provide the services necessary to catch the huge majority of malware at the network perimeter. In addition, we recommend endpoint detection on individual computers for protection against malware that bypasses the perimeter, such as variants spread through USB drives or smartphones. For Firebox owners, the Total Security Suite combines all the network security controls we offer into one easy package.

Block Command and Control (C2C) Channels and Malicious Sites

Ransomware and other malware increasingly spread through compromised sites and name squatting, where the name of the malicious site looks like the name of a popular real site. Network security services need a real-time guard to prevent botnets from accessing Command and Control domains as well as prevent users from visiting phishing sites. Any endpoint detection should also include protection against ransomware by not only blocking the malware but also blocking any actions the ransomware takes against business-critical data. Leverage security services that block these sorts of sites via DNS or normal HTTP queries. If you're a Firebox owner, a combination of DNSWatch and Threat Detection and Response (TDR) protects users and devices themselves from malicious sites and C&C's and blocks most ransomware.

Top Security Incident

WatchGuard

Top Security Incident

COVID-19

It's hard to think of a single event that has caused such a dramatic shift in the cybersecurity landscape as the COVID-19 crisis and its forced changes to the global workforce. Almost overnight, nearly every organization had to either enable their entire workforce to work remotely or even worse, shutter their doors entirely. Entire verticals like retail and food service became less appealing to visitors causing their revenue to dry up, and across the corporate world attack surfaces shifted from the perimeter to the individual.

As with any major event, fear and desire for more information reduce an individual's "tipping point," or the threshold between social engineering success and failure. Attackers abuse this lowered tipping point to launch phishing campaigns that can easily trick their victims into clicking malicious links or giving up credentials. Researchers at FireEye already reported on one such campaign targeting a Chinese government agency.

Meanwhile, a rapid global shift to a remote workforce has opened up cracks in the traditional layered defense employed by most organizations. Employees who were previously protected from cyber attack from the perimeter down to the endpoint, now have more personal responsibility for maintaining their own security. All the while, they are battling with the increased risk of phishing from a reduction of face-to-face interaction.
In this section, we'll cover just how the COVID-19 pandemic has changed the cyber threat landscape and what you can do to protect your organization during these trying times.

A Change of Landscape

When states in the US and countries across the world began ordering their citizens to stay at home, "non-essential" businesses were forced to make the decision of either shutting their doors or rapidly shifting to accommodate a workforce entirely made of remote workers. From January to March, WatchGuard saw an **8.3% increase in mobile VPN usage** on Fireboxes deployed across the world, a substantial increase for such a short time window.

While many organizations quickly enabled mobile VPN access for their employees, other organizations simply exposed services directly to the Internet. Reports by other security vendors have already highlighted the increase in Remote Desktop Protocol (RDP) ports exposed to the Internet during the first quarter of the year, but the risk extends beyond just remote access and into web applications as well. In the Firebox Feed for example, we watched an increase in attacks that triggered IPS signatures for brute force login attempts throughout the quarter.

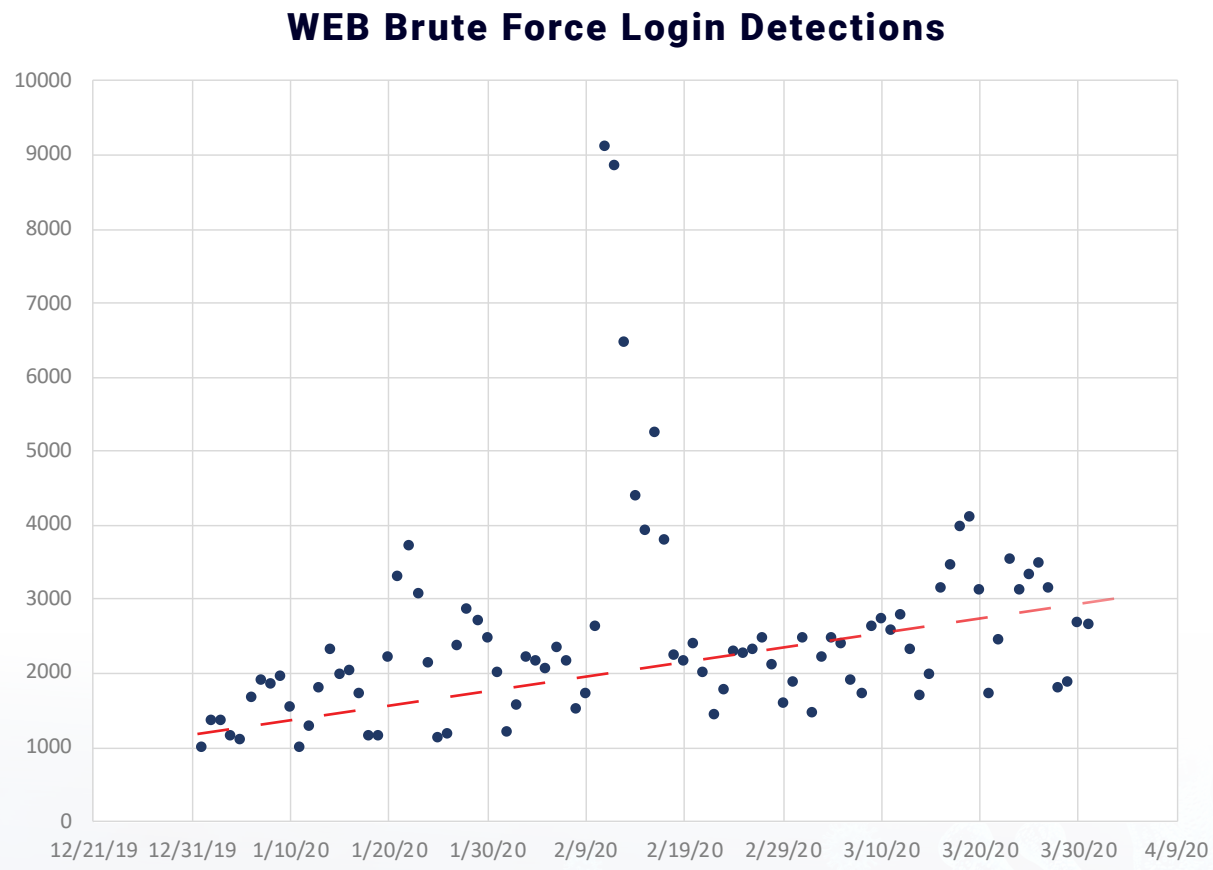


Figure 13: WEB Brute Force Login Detections

Phishing

Phishing relies on convincing a victim to click on a link or open an attachment. In normal times the tipping point, or the baseline believability threshold for a phishing message, is high enough that the majority of individuals don't fall for them. Times of crisis like the current pandemic can lower the tipping point though as individuals look anywhere for more information. Attackers abuse this fact by launching phishing attacks that target the population's fears. Additionally, stay-at-home orders translate to less face-to-face communication and a greater reliance on email, increasing the chance that individuals fall for a phish.

We already highlighted the JavaScript-based phish Cryxos in the malware section of this report but in case you missed it, this particular campaign is designed to steal credentials from victims using a fake file sharing web page. Detections for our most prolific Cryxos signature trended heavily upward over the quarter as more individuals began working remotely.

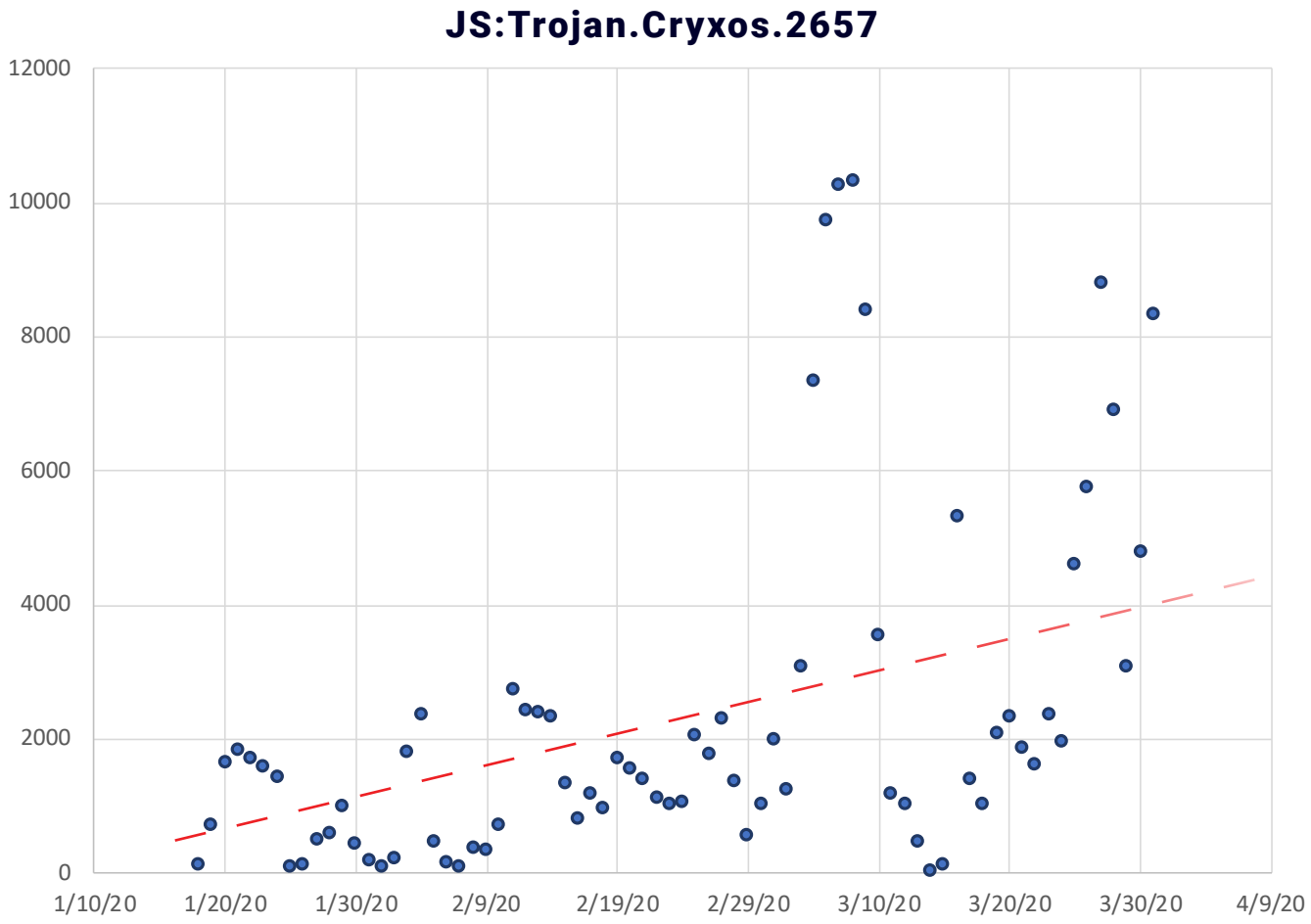


Figure 14: Chart showing the daily volume of Cryxos throughout Q1

Important Takeaways

Q1 2020 was only the start of the massive changes to the cyber threat landscape brought on by the COVID-19 pandemic. Even in just these first three months, we still saw a massive rise in remote workers and attacks targeting individuals. Even as governments begin easing back restrictions, many people will still likely remain working remotely until the spread of the virus is truly controlled. Here are some tips you can follow if you are one of those remote workers or someone who helps facilitate remote workers.

1

Increase Your Communication

Phishing attackers rely on their victims either missing the signs of a phish or not double-checking the legitimacy of the request. You can improve your defenses by communicating frequently with your fellow coworkers in a form other than email. If you receive a request to carry out an action via email, consider sending a chat message or a quick video call to confirm the legitimacy of the request before following through.

2

Consider Security When Setting Up Remote Access

While you're likely in a rush to enable remote access to company resources as quickly as possible, don't take shortcuts on security. Don't expose services to the Internet that shouldn't be exposed to the Internet like Remote Desktop Protocol. Instead use a mobile VPN to connect back to the office securely and access the service as if you were local. If you must enable Internet-facing access to a service, secure it with multiple layers of anti-malware, intrusion prevention, and other security measures.

3

Take Care of Yourself

Stress leads to mistakes. Even if you've maintained your employment through this frightening time, it can still be stressful watching everything happen in the world. Taking care of yourself and your own health should come first and foremost. Then you can take care of the fellow employees and customers that rely on you.

Conclusion & Defense Highlights

Conclusion & Defense Highlights

We hope the findings of our Q1 threat report were enlightening and gave you a better idea of the trending cyber attacks targeting your business today. Though we can't solve all the world's problems alone, we can contribute our expertise where it matters. While a lot of crises threaten businesses, we hope to make malicious hacks one of the problems you worry about less. Here are the best security strategies to survive the latest attacks found during Q1:

Considering these trends, here's our security advice to survive next quarter:

You must decrypt and inspect encrypted web traffic

The WatchGuard Threat Lab team believes that everyone has the right to privacy. We love that most web traffic is being encrypted with TLS today. HTTPS both verifies the legitimacy of the sites we visit and the confidentiality of our communications, and all users deserve those protection. However, cyber criminals can also exploit encryption for their attacks as well. That doesn't mean we should leave backdoors in encryption to intentionally break it, but it does mean we should retain admin-controlled mechanisms that allow you to knowingly decrypt some traffic for security inspections. Many network products, including WatchGuard Fireboxes, offer legitimate mechanisms to allow you to decrypt network traffic like HTTPS at your security gateway. While this ironically seems like a man-in-the-middle attack, it is one knowingly configured by you specifically to allow our anti-malware and intrusion prevention services to secure that encrypted traffic. We do this legitimately, using special digital certificates that you have to add to your PKI or distribute to your clients. We also only do this to allow our technical security services to scan said traffic. We do not expose the contents of user traffic to administrators and we do re-encrypt the traffic on the other side, so it retains its local privacy protection. While we suspected attackers took advantage of web encryption to hide attacks, even we were surprised to learn that 67% of malware spread over encrypted channels. That's more than two-thirds of malware. Frankly, we Firebox owners should take advantage of our HTTPS content inspection capabilities. It does take some extra effort to configure but is not as difficult as some fear. With most malware arriving over encrypted channels, you need to inspect HTTPS traffic. If you don't, I can guarantee malware will get past your network defenses one day.

Continue to enable proactive anti-malware technologies

By now, you are used to us recommending modern anti-malware technologies that can immediately catch new malware without relying on or waiting for a signature update. Our IntelligentAV, APT Blocker, and Threat Detection and Response (TDR) services all have machine-learning and behavioral mechanisms to catch zero day malware (malware not detected by signatures yet). This quarter is no different, with ~64% of malware evading signature-based protection (such as GAV). However, this zero day malware number may be even higher than we fear. Our TLS research shows that most malware arrives over HTTPS, which most Firebox users do not inspect. Furthermore, we've also seen that Fireboxes that do inspect HTTPS traffic see over 72% of zero day malware – even higher than any of our previous records. In short, the malware we see over secure communication channels is more sophisticated and evasive in general. Not only will you miss it if you don't inspect HTTPS, but you will miss it if you are not using the advanced anti-malware services that come with our Total Security package. In short, don't rely on signature-based AV alone. You need proactive and modern malware detection both on your network and endpoints.

Keep your vigilance and skeptical nature on during crisis

2020 has already been a hard year for many reasons, the pandemic being the most obvious. It sucks to always feel like you need your guard up. Furthermore, right now most of you are likely more concerned with just running your core business than you are focusing on cyber threats. That said, criminals take advantage of trying times. As disgusting and unconscionable as it sounds, crises are like Christmas for criminals as they know we sometimes let some of our guards down due to fear and uncertainty. If they phish us with an enticing lure about a subject we're already concerned with, they know we are more likely to click. Don't let their nefarious phishing strategies work. Pay careful attention to how you feel before you click a link or attachment in an email. Have the contents of the email gotten your worried, and that's why you want to click it? If so, calm yourself first, then ask yourself if someone would really use email to communicate something so concerning. Even if the email seems to come from a friend or co-worker, take that time to reach out through another channel, and make sure it was really them. In short, don't let your emotion take over your common sense during crises. It does happen to all of us, but with a little vigilance, you can avoid it.

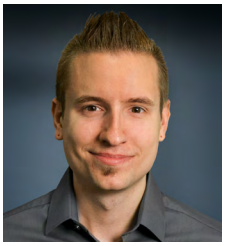
Adjust your security strategy for the new "work from home" reality

As I mentioned last quarter (in this very same spot), we often talk about the threats in this report under the context of your local headquarters network. The truth is, you are just as susceptible to cyber attacks – if not more – while working off-premises. Before the COVID-19 pandemic, employees were already starting to work remotely more regularly. Now, working from home is a forced reality for many of us. Unfortunately, not only will these threats follow us home, but many users have less protections while there. The good news is you can enforce a layered security strategy at home. That strategy starts with a good endpoint protection (EPP) suite, which includes various anti-malware technologies (including the proactive ones mentioned below), endpoint detection and response (EDR) capabilities, patch management, disk encryption, password management, web protection, and much more. The WatchGuard Passport offering also includes things like multi-factor authentication (MFA) and DNS content filtering, both of which keep you safe wherever you are. As an aside, WatchGuard just closed the acquisition of Panda Security, an EPP company. We will offer our own EPP suite soon, but for now, we recommend Panda's Adaptive Defense 360 (AD360). In short, your Firebox gives you a large suite of security services to protect your network. You should also be sure to deploy a similar suite of endpoint security services to protect your work-from-home users too.

In language, we often overuse certain idioms so commonly that they turn into meaningless platitudes – that is until an event so consequential occurs that it reminds us why someone coined that idiom in the first place. One I can't help but think of right now is, "It's always darkest before dawn." I'm not sure if that idiom is physically accurate (I suspect the middle of night is darker than night before dawn), but its intended meaning rings true to me in times like these. 2020 has had a bleak start. We entered the year with polarizing political divides around the world, only then to suffer a pandemic, only then to see even more examples of unjust racism in some countries. All that darkness can seem heavy… BUT… remember humankind has come together and survived worse before. In fact, some of these struggles are what has made us become even stronger and better. While news seems bleak, our attitude to conquer adversity doesn't have to be. While our threat team can't solve the world's larger problems alone, we can at least try to make the technical tools we use to connect online safer. We hope this report helped you identify the threats that target your businesses today and gave you some strategies to employ to solve one of the small problems we face today. As always, leave your comments or feedback about our report at SecurityReport@watchguard.com, and stay safe while you fight the good fight!

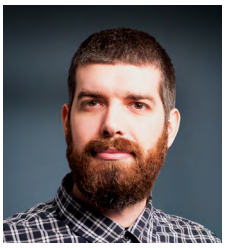
Corey Nachreiner
Chief Technology Officer

Recognized as a thought leader in IT security, Corey spearheads WatchGuard's technology vision and direction. Previously, he was the director of strategy and research at WatchGuard. Corey has operated at the frontline of cybersecurity for 19 years, and for nearly a decade has been evaluating and making accurate predictions about information security trends. As an authority on network security and internationally quoted commentator, Corey has the expertise to dissect complex security topics, making him a sought-after speaker at forums such as Gartner, Infosec and RSA. He is also a regular contributor to leading publications including CNET, Dark Reading, eWeek, Help Net Security, Information Week and Infosecurity, and delivers WatchGuard's "Daily Security Byte" video series on **www.secplicity.org**.



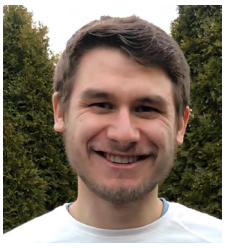
Marc Laliberte
Sr. Security Threat Analyst

Specializing in network security technologies, Marc's industry experience allows him to conduct meaningful information security research and educate audiences on the latest cybersecurity trends and best practices. With speaking appearances at IT conferences and regular contributions to online IT and security publications, Marc is a security expert who enjoys providing unique insights and guidance to all levels of IT personnel.



Trevor Collins
Information Security Analyst

Trevor Collins is a information security analyst at WatchGuard Technologies, specializing in network and wireless security. Trevor earned his security know-how and several certifications through his past military experience in the United States Air Force. Trevor is a regular contributor to Secplicity.org where he provides easily understood data analysis and commentary to IT professionals. Trevor's experience with a wide range of network security vendors and technologies allows him to provide unique perspectives to the industry.



Ryan Estes
Intrusion Analyst

Ryan is an Intrusion Analyst at WatchGuard Technologies operating primarily within DNSWatch, WatchGuard's DNS filtering and security service. For DNSWatch, Ryan helps customers better understand potential threats to their organization using tailored domain analysis and threat intelligence. Outside of DNSWatch, his research interests include web application security, Wi-Fi communications, and malware analysis. Ryan embraces a 'never stop learning' lifestyle allowing him to stay on top of the latest cyber security and malware trends. In turn, Ryan passes this knowledge on to our customers and even shares certain topics on his personal blog.

About WatchGuard Threat Lab

WatchGuard's Threat Lab (previously the LiveSecurity Threat Team) is a group of dedicated threat researchers committed to discovering and studying the latest malware and Internet attacks. The Threat Lab team analyzes data from WatchGuard's Firebox Feed, internal and partner threat intelligence, and a research honeynet, to provide insightful analysis about the top threats on the Internet. Their smart, practical security advice will enable you to better protect your organization in the ever-changing threat landscape.

About WatchGuard Technologies

WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by nearly 10,000 security resellers and service providers to protect more than 80,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for midmarket businesses and distributed enterprises. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit **WatchGuard.com**.

For additional information, promotions and updates, follow WatchGuard on Twitter @WatchGuard, on Facebook, and on the LinkedIn Company page. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at **www.secplicity.org**.