WatchGuard

# INTERNET SECURITY REPORT

Quarter 3, 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

Have you ever suffered a hardship or disaster and in retrospect couldn't help but think, "If I had just done X, none of this would have happened?" I certainly have and it's a feeling I want to avoid! Even when we suffer from misdeeds carried out by others, like theft or assault, we often can't help but speculate what we could have done to avoid the calamity; even when it literally wasn't our fault. I imagine some avoidable tragedy helped coin the phrase, "hindsight is 20/20."

We write this quarterly report in hopes of giving you 20/20 foresight against the latest cyber threats. Cyber attacks are very much the kind of unexpected transgression that we logically know is not our fault (the blame lies entirely with criminal attackers) but still wonder what we could have done to avoid. In the same way you might regret leaving a door unlocked after a theft, you'd probably wonder what you could have done to prevent a damaging cyber attack if one hit you. We hope to help you avoid this contemplation completely by sharing the latest cyber-attack trends along with the "hindsight 20/20" tips that could help avoid them.

Our quarterly Internet Security Report (ISR) is designed to be the one-two punch of data you need to understand and avoid the latest information security attacks. We start by helping you understand the threat landscape by analyzing the latest real-world attacks. To do this, we gather and analyze a deluge of threat indicators from over 45 thousand WatchGuard Fireboxes and synthesize that data into the most common and widespread cyber threats from last quarter. This gives us cutting-edge insight into what adversaries target and how they carry out their malicious campaigns.

Once we know what the criminal hackers are doing, we can tell you how to stop it. To help you avoid an incident that makes you feel bad about a missed defense, we highlight the top protection strategies you can deploy to avoid the incident in the first place. We share these defensive tips throughout this report, relating to the latest attacks we see. At the end, we even summarize general high-level defense strategies that will always help your organization mitigate cyber threats.

At the end of the day, it's much better to make someone else's hindsight your foresight, so you can avoid preventable hardships they suffered. It's never your fault if you're hacked by criminals, but it's still better to avoid hacks in the first place. This report intends to unveil the right safety measures for today's threat, so you have the foresight to evade successful attacks in the future.

## The Q3 report covers:

Now you know why we do the report, it's time to dive into the details. Read on to learn about the biggest cyber threats from last quarter, and how you can continue to defend against them in the future.

# Executive Summary

In Q3, malware volume at the office perimeter dropped for the third quarter in a row, which we'd typically consider unusual, but has become an expected result of COVID-19. The pandemic has greatly affected many tech or knowledge-based organizations' network topology, with most of their employees working from home since March. Malware targets the user, so we expect to see it follow employees and their endpoints wherever they work. That's why endpoint protection (EPP) products, like WatchGuard's recently acquired Adaptive Defense 360, are such an important aspect of a layered security strategy – especially during the pandemic.

Meanwhile, you can't relax defenses at your network perimeter either. Last quarter we also saw a significant 90% increase in network attack volume, which reached its highest level in the last two years. Even though malware is targeting users at home, cyber criminals know you still have critical networks services at your office, which must remain functional, often specifically in order to give your remote users access to them. They also know you may have fewer folks on location monitoring these services. In short, attackers have ramped up their attacks on office-based network services at the same time they've focus their malware efforts on home users.

Beyond the raw volume, zero day malware (malware that evades signature-based protection) dropped some in Q3, but still remains over half of all malware. At the same time, encrypted threats hiding in TLS communications increased to 54%. In other words, attackers continue to grow sophisticated and evade traditional defense, even as they refocus their targets due to the pandemic.

This report covers a lot more trends, including increased phishing (much COVID-19 related), an older SCADA vulnerability and attack resurfacing, and quite a few active botnet campaigns like Emotet, FareIt, and more.

**Other Q3 2020 highlights include:**

- Overall perimeter detected **malware is down 26% quarter-over-quarter** (QoQ), which we have started to expect due to COVID-19, and many employees working from home.
- **Over 50% of malicious files are zero day malware,** meaning the malware is not detected using signature-based protections. This is actually **down 64% compared to last quarter,** but still represents a high volume of malware missed by some AV solutions.
- We saw an increase in malware arriving over encrypted communication channels, with **54% of malware using TLS (HTTPS).** This malware also tends to be more sophisticated than average, with **~61% of it being zero day malware.**
- **Network attacks and unique exploit detections hit two-year highs**. Network attacks swelled to more than **3.3 million in Q3, representing a 90% increase QoQ.** Unique network attack signatures also continued on an upward trajectory, reaching a two-year high in Q3 as well**.**
- During Q3 2020, Firebox appliances' Intrusion Prevention Service (IPS) blocked an **average of 70 attacks per appliance.**
- **Attackers probed nearly half of the Fireboxes in the United States for weaknesses in a popular SCADA-related industrial control system solution.**
- **Network attacks targeting countries in the Asia and Pacific (APAC) regions** were up for the second quarter in a row.
- During Q3, **DNSWatch blocked a combined 2,764,736 malicious domain connections,** which translates to **499 blocked connections per organization.**
- Breaking it down further, **DNSWatch blocked 262 malware domains, 71 compromised websites and 52 clicked phishes per organization** in Q3.
- **COVID-19 scams grow in prevalence.** In Q3, a COVID-19 adware campaign running on websites used for legitimate pandemic support purposes made WatchGuard's Top 10 Compromised Websites list.
- **A LokiBot look-a-like debuted in our top widespread malware list.** FareIt, a password stealer that resembles LokiBot, made its way into WatchGuard's top five most widespread malware detections list in Q3. Other popular botnets/trojans, like Emotet and Zusy, also made the top malware lists.

Those are the top highlights for those who are busy. However, if you have the time, we have many more interesting details, and more importantly, many defense strategies and tips, throughout this report. Read on for your 20/20 security foresight into the next quarter.

# Firebox Feed Statistics

# Firebox Feed Statistics

## What Is the Firebox Feed?

Each quarter we receive data from our customers who graciously allow us to review anonymous data from their Fireboxes. We call this data the Firebox Feed. We then analyze this data using various resources and come away with the top threat highlights each quarter. Next, we then leverage this threat intelligence to extrapolate other attack trends and, most importantly, share defensive strategies to combat these trends. Finally, we use this data internally to improve the Firebox and its services.

Some of this Firebox Feed data comes from DNSWatch, which has both a network and client component, depending on your product. DNSWatch monitors DNS requests and blocks request to malicious, phishing, and compromised domains. We analyzed more DNSWatch data than ever this quarter and learned that the service blocked an average of almost 500 attempts per organization of employees clicking on dangerous domain links.

**In general, more Fireboxes reported data to our Firebox Feed than ever before, with 47,866 devices reporting in this quarter.** The Q3 data from the Firebox Feed and DNSWatch also showed an increase in the Emotet botnet as well as other general botnets. These increases may lead to larger botnets capable of distributed denial of service (DDoS) attacks that could take down large corporate networks like they have in the past. Our Intrusion Prevention Service (IPS) on the Firebox can mitigate these threats as botnets continue to grow in the coming months.

We hope you find the data in this report valuable and if you would like to help us improve, please enable device feedback on your **Firebox appliances**.

## 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 helps our company improve our products, making all Firebox owners more secure. Right now, we receive data from about 12% 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

In Q3 2020, we saw a drop in overall malware despite an increase in the number of Fireboxes reporting threat intelligence to the Firebox Feed. Throughout the quarter, malware increasingly arrived over encrypted network connections when compared to Q2. Additionally, well-known botnets and banking trojans like Emotet, FareIt, and Zusy appeared and rose to the top of our lists. These findings fall in line with the recent surge in other botnets like Lokibot as noted by other anti-malware venders in the US. You will rarely download these malware variants directly, but an unsuspecting victim may find that the attachment in an email is actually a dropper that downloads the malware.

Previous mainstays, like the remote access trojan (RAT) Razy and the password stealer Mimikatz made a comeback on our top 10 malware by volume list, coming in at spots three and four. Meanwhile, the established banking trojan Emotet showed up at the bottom of the top 10 list.

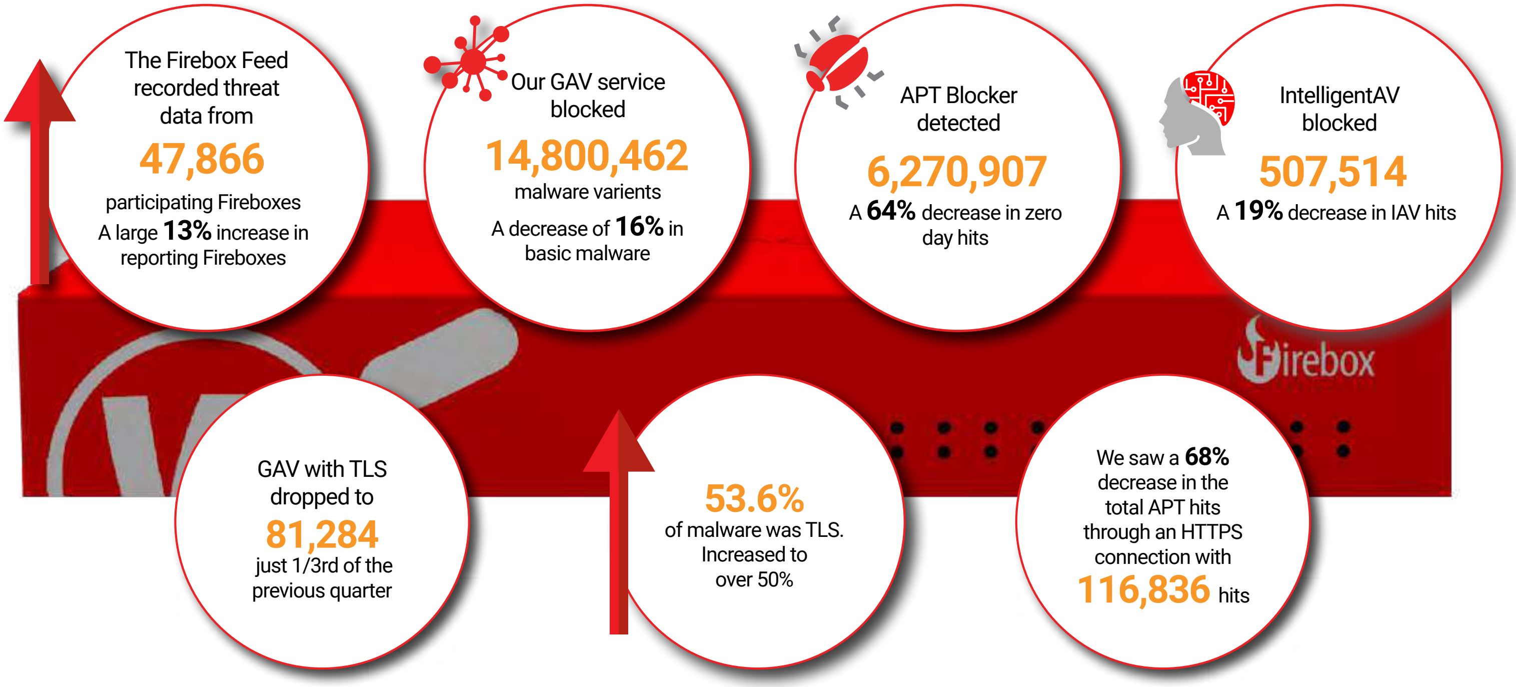
Some malware payloads had global impacts this quarter. Over a third of Fireboxes in Cyprus encountered a malicious Office document that utilized CVE-2017-11882. Over a fourth of Fireboxes saw the same exploit in Greece and Germany. In our research, we found the spread of Office documents utilizing CVE-2017-11882 leads to more malware like the botnets and banking trojans we mentioned previously. Before getting into more details on the malware itself let's look at the big-picture statistics.

We encourage our users to use a layered defense to protect themselves from malware. We follow this principal in our own product by using three separate methods to block the malware.

**Gateway AntiVirus (GAV)** uses signatures to identify malware and quickly block it without any significant load on the Firebox itself.

**IntelligentAV (IAV)** inspects the suspect file for identifying features using machine-learning algorithms. Based on the results it gives a score. We use the score to determine if we allow the file or not.

**APT Blocker** uses a full sandbox to inspect suspect files. Doing so allows us to determine the intent of the file and identify even well-hidden malware since the malware believes it infected a real device.



The Firebox Feed recorded threat data from **47,866** participating Fireboxes
A large **13%** increase in reporting Fireboxes

Our GAV service blocked **14,800,462** malware varients
A decrease of **16%** in basic malware

APT Blocker detected **6,270,907**
A **64%** decrease in zero day hits

IntelligentAV blocked **507,514**
A **19%** decrease in IAV hits

GAV with TLS dropped to **81,284** just 1/3rd of the previous quarter

**53.6%** of malware was TLS. Increased to over 50%

We saw a **68%** decrease in the total APT hits through an HTTPS connection with **116,836** hits

## Top 5 Most-Widespread Malware Detections

Our top malware volume list shows the most prevalent malware, but our widespread list shows how likely you may see this malware no matter the size, category, or region of your business.

You'll notice some returning malware payloads from Q2, including two version of the Popunder adware we wrote about in that report. A new malware sample, FareIt, showed up for the first time this quarter, primarily targeting Hungary and Cyprus with some detections in Greece as well. Interestingly, we didn't see this malware as widespread outside of Europe. We cover FareIt in detail later in this section.

Fireboxes in Cyprus also detected a significant number of malicious documents that contained the CVE-2017-11882 exploit and RTF-ObfsStrm.Gen malware payloads. A few samples we reviewed leads us to believe the malicious documents downloaded FareIt in many cases.

Regionally the Americas (AMER) saw more widespread adware but Europe, the Middle East and Africa (EMEA) saw the most widespread malware overall.

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

When properly configured, GAV (Gateway AntiVirus) scans files to identify if a malware signature matches a known threat. If GAV does not find a match then IntelligentAV applies machine-learning models to identify malicious files. If IAV calls it good, APT Blocker still fully sandboxes the file to determine what actions and behaviors the file performs, then returns a good or malicious result for the Firebox to pass or block.

**Top 10 Gateway AntiVirus Malware**

| COUNT | | THREAT NAME | CATEGORY | LAST SEEN |
|---|---|---|---|---|
| 394,253 | ● | Win32/Heri | Win Code Injection | Q2 2020 |
| 312,594 | ● | Win32/Heim.D | Win Code Injection | Q2 2020 |
| 302,525 | ● | Razy | Cryptominer/ Win Code Injection | Q2 2020 |
| 283,387 | ● | Mimikatz | Password Stealer | Q1 2020 |
| 220,958 | ● | CVE-2017-11882 | Office Exploit | Q2 2020 |
| 198,493 | ● | RTF-ObfsStrm.Gen | Office Exploit | Q2 2020 |
| 394,253 | ● | Cryxos (variants) | Scam File | Q2 2020 |
| 312,594 | ● | GenericKD (variants) | Win Code Injection | Q2 2020 |
| 302,525 | ● | Gnaeus | Scam Script | Q2 2020 |
| 283,387 | ● | VBA.Heur.Logan (emotet) | Password Stealer | new |

*Figure 1: Top 10 Gateway AntiVirus Malware Detections*

## Top 5 Encrypted Malware Detections

Over the last decade most websites have enabled HTTPS encryption. In Q3, over half the malware Fireboxes saw used encrypted connections, according to Fireboxes configured to inspect HTTPS. We also know that on average each Firebox detected 440 malware variants during Q3, meaning Fireboxes not scanning encrypted connections will likely miss 236 pieces of malware and pass it into the victim.

In our previous Top 10 Malware table we review all malware found but only a small percentage of devices scan encrypted HTTP traffic leading to underrepresentation of malware over HTTPS. To provide a full picture we list the top threats for encrypted connections. To block these threats, we recommend our users **enable encrypted traffic inspection.**

**Top 5 Encrypted Malware Detections**

| COUNT | THREAT NAME | CATEGORY |
|---|---|---|
| 186,56 | GenericKD | Generic Win32 |
| 10,890 | Adware.Popunder | Generic Adware |
| 7,423 | Mail.RKR ( Zusy*) | Win Code Injection |
| 4,364 | Trojan.MultiDrop ( Zusy*) | Win Code Injection |
| 4,228 | SpamMalware-RAR | Spam malware |

**We found samples of Mail.RKR and Trojan.MultiDrop downloaded the Zusy malware*

*Figure 2: Top 5 Encrypted Malware Detections*

| Top 5 Most-Widespread Malware | Top 3 Countries by % | | | EMEA % | APAC % | AMER % |
|---|---|---|---|---|---|---|
| Adware. Popunder.B | Indonesia 57.69% | Thailand 56.12% | Dominican Republic 52.14% | 17.69% | 15.86% | 22.89% |
| CVE-2017-11882. Gen | Cyprus 34.04% | Greece 27.68% | Germany 25.57% | 18.00% | 7.58% | 5.74% |
| RTF-ObfsStrm.Gen | Cyprus 30.85% | Greece 22.24% | Hungary 21.21% | 13.15% | 5.38% | 4.20% |
| Adware. Popunder.D | Morocco 25.9% | Chile - 25.31% | Indonesia 25% | 7.53% | 7.98% | 9.11% |
| Delf.FareIt.Gen.7 | Hungary 33.33% | Cyprus - 28.72% | Greece 18.97% | 11.76% | 4.06% | 3.36% |

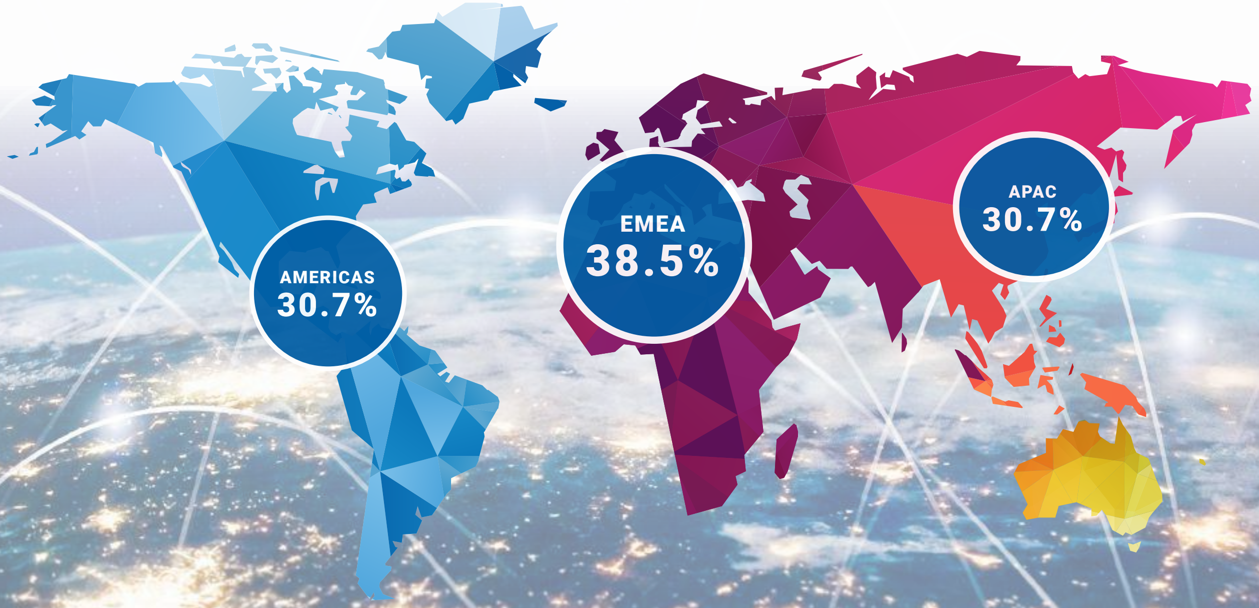
*Figure 3: Top 5 Most-Widespread Malware Detections*

## Geographic Threats by Region

Total malware detections in each region differ. For a more detailed investigation on what regions receive the most malware we separate the malware detections into each region here.

We continue to see EMEA receiving the most malware detections, increasing their lead slightly overall from the previous quarter. AMER saw less of a percentage of hits over the previous quarter while APAC saw more.

## Malware Detection by Region



## Catching Evasive Malware

Evasive and zero day malware continues to threaten networks. Many zero day malware samples frequently change while others morph on every copy, making signature-based anti-malware less effective. Over half the malware we saw in Q3 can bypass basic signature-based malware protection, even if you scan encrypted traffic. With over six million detections this quarter, network and security administrators must use other layers of anti-malware services to block these threats.

On the Firebox appliance, the APT Blocker service submits files to a Cloud sandbox and analyzes their behavior to detect malicious applications. Additionally, the IntelligentAV service uses machine learning to identify potential malicious code before it makes it through the perimeter. No single malware detection service can catch all malware. This is why having multiple layers as we discussed earlier is critical for the strongest defense.

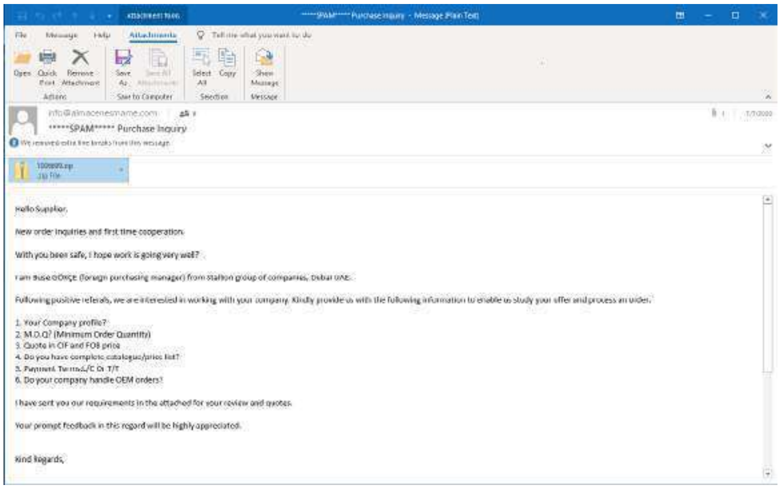
## Malware Found

### Delf.FareIt, AKA Pony [S0453]

In Q3, we found a password stealer that resembles LokiBot **[S0447]** in our top widespread-malware list. Some **malware campaigns** distribute both LockiBot and FareIt indicating further connections between these malware families. While researching this further, we found the data might not show the extent of how widespread this threat has become. Based on our research, Office documents that use the CVE-2017-11882 exploit as a dropper eventually downloaded FareIt in many cases. Because the Firebox blocks most malware droppers, like CVE-2017-11882, we never see the final payload. Also, the US government recently released **an alert** about LokiBot due to the widespread nature of this attack. From these findings we believe the malware targeted many more victims not shown in our data.

**Many believe** the threat group SilverTerrier **[G0083]** is responsible for this password stealing bot but we don't know for sure. LokiBot, created by SilverTerrier, can infect Android devices but FareIt only targets Windows machines. SilverTerrier also created Agent Tesla **[S0331]** which we wrote about in Q4 of 2019.

The main infection path for this botnet starts off as a phishing email **[T1566.001]** with a Word document attachment containing a malicious macro **[T1137.001]**. The victim opens the email, downloads the Word document, and opens it. If they allow the malicious macro to run, then the document launches PowerShell **[T1059.001]** to download and install FareIt. This malware will sometimes come as an executable inside a compressed file.



info@almacenesmame.com

*****SPAM***** Purchase Inquiry

Hello Supplier,

New order inquiries and first time cooperation.

With you been safe, I hope work is going very well?

I am Buse GÖKÇE (foreign purchasing manager) from Stallion group of companies, Dubai UAE.

Following positive referals, we are interested in working with your company. Kindly provide us with the following information to enable us study your offer and process an order.

1. Your Company profile?
2. M.D.Q? (Minimum Order Quantity)
3. Quote in CIF and FOB price
4. Do you have complete catalogue/price list?
5. Payment Terms L/C Or T/T
6. Do your company handle OEM orders?

I have sent you our requirements in the attached for your review and quotes.

Your prompt feedback in this regard will be highly appreciated.

Kind Regards,

*Figure 4: FareIt email screenshot*

After executing, FareIt steals passwords from the victim's computer and sends the results over an encrypted connection to the command and control [TA0011] server. It steals passwords by looking for them in Windows OS credentials, email clients, browsers, and FTP clients. Commands from the C&C can activate an additional keylogger [T1065.001] to capture passwords. Once SilverTerrier has these passwords they will usually sell them on the dark web or use them for their own purposes.

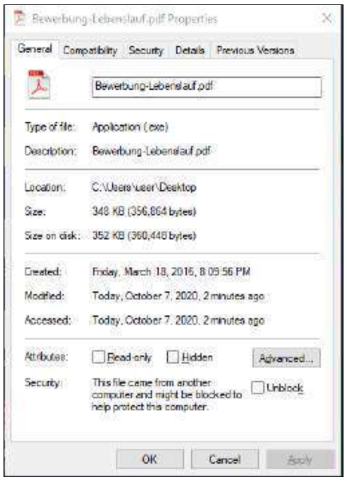
This botnet takes many steps to bypass anti-malware engines and fool users into installing the payload. Luckily, you can stop the attack in many ways. For example, watch for suspicious emails. If you receive one, check directly with the sender, preferably over the phone. Never allow macros from an untrusted source and always have a layered defense for malware including network and endpoint-based antivirus.

### Zusy

We found the Zusy malware near the top of the list for malware downloaded over an encrypted connection. It actually showed up twice from two droppers that primarily downloads Zusy as their  payload.  These Zusy variants tried to connect to a server in Poland on TCP port 6318 [TA0011] but as of our analysis of the server appears to have been taken down. We know this server in Poland has spread malware in the past from information we found on the IP address.

Zusy spreads by email [T1566.001] and malicious documents. Because it tries to connect to a server, we believe it creates a backdoor to enable remote access.  Zusy also tries to steal passwords, spy on the victim, and steal banking credentials.

In one sample we analyzed, the file looks like a PDF and even has the PDF extension but when we looked at the properties it showed an executable. The author of this variant of Zusy used the .Net framework to create their payload.



Bewerbung-Lebenslauf.pdf

Type of file: Application (.exe)
Description: Bewerbung-Lebenslauf.pdf

Location: C:\Users\user\Desktop
Size: 348 KB (356,864 bytes)
Size on disk: 352 KB (360,448 bytes)

Created: Friday, March 18, 2016, 8:09:56 PM
Modified: Today, October 7, 2020, 2 minutes ago
Accessed: Today, October 7, 2020, 2 minutes ago

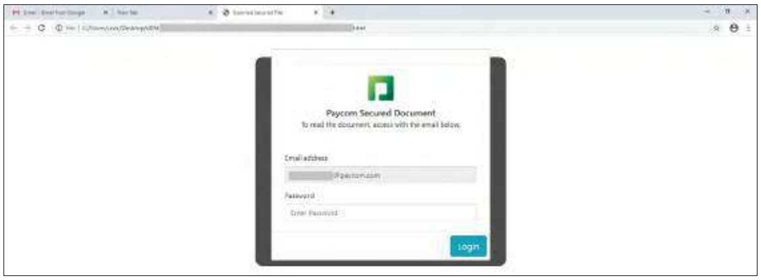
Attributes: □ Read-only □ Hidden
Security: This file came from another computer and might be blocked to help protect this computer. □ Unblock

***Figure 5: Zusy properties screenshot***

As with FareIt, protecting your devices starts with blocking the malware before it reaches the endpoint. This means deploying a network-level anti-malware solution [M1049] that can block these files. This adds additional security to your network so users can focus on work. As always, watch out for emails from unknown senders. Check with the sender directly or have an IT security professional review the email before clicking on suspicious links.

### Cryxos

We have seen Cryxos in or near the top 10 malware list for the last few quarters and every time we review it, we see a different attempt to fool users. These all have the same goal, steal your credentials using a fake login page. [T1185]



Paycom Secured Document

To read the document, access with the email below.

Email address

[redacted]@paycom.com

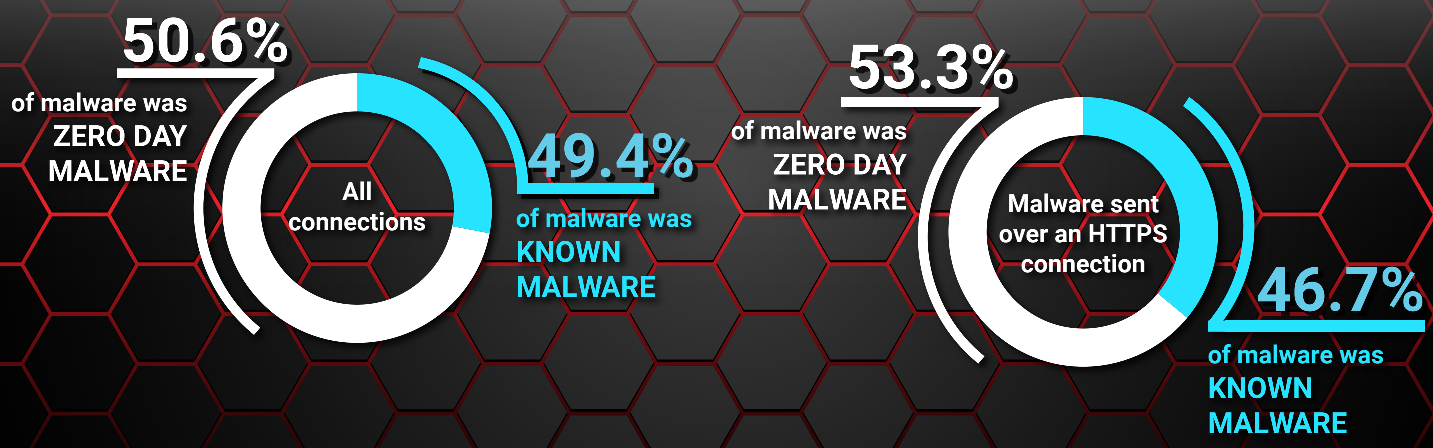
Password

Enter Password

*Figure 6: Cryxos fake login screenshot*

In this latest case they try to steal credentials for Paycom, a payroll and human resource online software provider. Access to a business online payroll account could devastate a company not only monetarily but also in trust from the employees. Out of curiosity, we tested this form in a safe environment and found the form sends the email address and passwords to a server in clear text, but the server doesn't respond. Fortunately, the Firebox catches these fake login pages.

As you may have heard, Chrome will roll out an update to make it easy for users to check the domain of the website they access. In most cases this will help, and it has shown some success. The problem comes when credential-stealing websites appear on trusted domains like sharepoint.com or googleapi.com. Check the full URL for the domain if you don't have the Chrome update that shows the domain only and check that the domain matches what you expect before entering credentials.



# Network Attack Trends

The Firebox Feed includes threat intelligence on network attacks and application exploit attempts that the Firebox's Intrusion Prevention Service (IPS) detects and blocks on networks across the globe. These detections range from attempted web application exploits like SQL injections and cross-site scripting to attack payloads targeting specific applications like Adobe Acrobat. IPS uses a set of frequently updated signatures to detect these threats across all ports and protocols by analyzing network traffic as it traverses the Firebox.

In the third quarter of 2020, Fireboxes participating in the Firebox Feed identified 3,329,620 network attacks, a massive 90% increase from Q2. This averages to about 70 detections per participating appliance, a 67% increase over Q2. Additionally, the number of unique attack signatures increased from 410 in Q2 2020 to 438 in Q3 2020.

We've been tracking a steady increase in network attacks on the perimeter since Q1, despite the pandemic forcing much of the world's workforce to work from home. This is in contrast to the drop in malware detections through the perimeter that we noted earlier in this report and in previous reports this year. Just because most of your workforce may now be remote, doesn't mean you can let your guard down on protecting network-based services.

Much of the network attack volume detailed in this report comes from automated tools. Threat actors are constantly scanning the Internet to identify exposed services and automatically exploit any unpatched vulnerabilities. Because of this, the top network attacks by volume rarely change from quarter to quarter. This held true for Q3 2020 where we saw no new additions to the top 10 network attacks by volume.

**The network attack highlights for Q3 2020 are:**

- **During Q3 2020**, **Firebox appliances blocked 3,329,620 network attacks** in total, averaging to 70 detections per appliance.
- Firebox appliances continued their upward trend of unique signature detections, **identifying 438 unique threats during the quarter.**
- **Nearly half of all networks in the United States** saw attackers probe for weaknesses in a popular industrial control system.
- Network attacks targeting countries in the Asia and Pacific regions were **up for the second quarter in a row.**

| Quarter/ Year | IPS Hits |
|---|---|
| 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 |
| Q2, 2020 | 1,752,789 |
| Q3, 2020 | 3,329,620 |

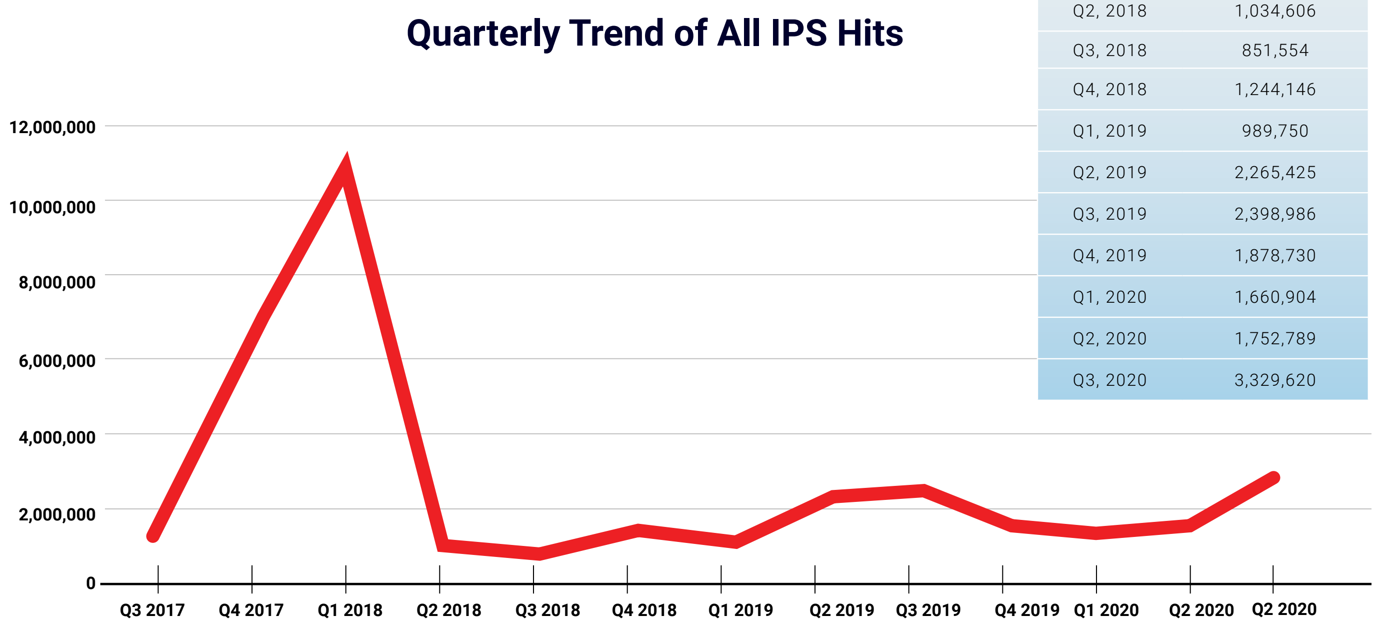


*Figure 7: Quarterly Trends of All IPS Hits*

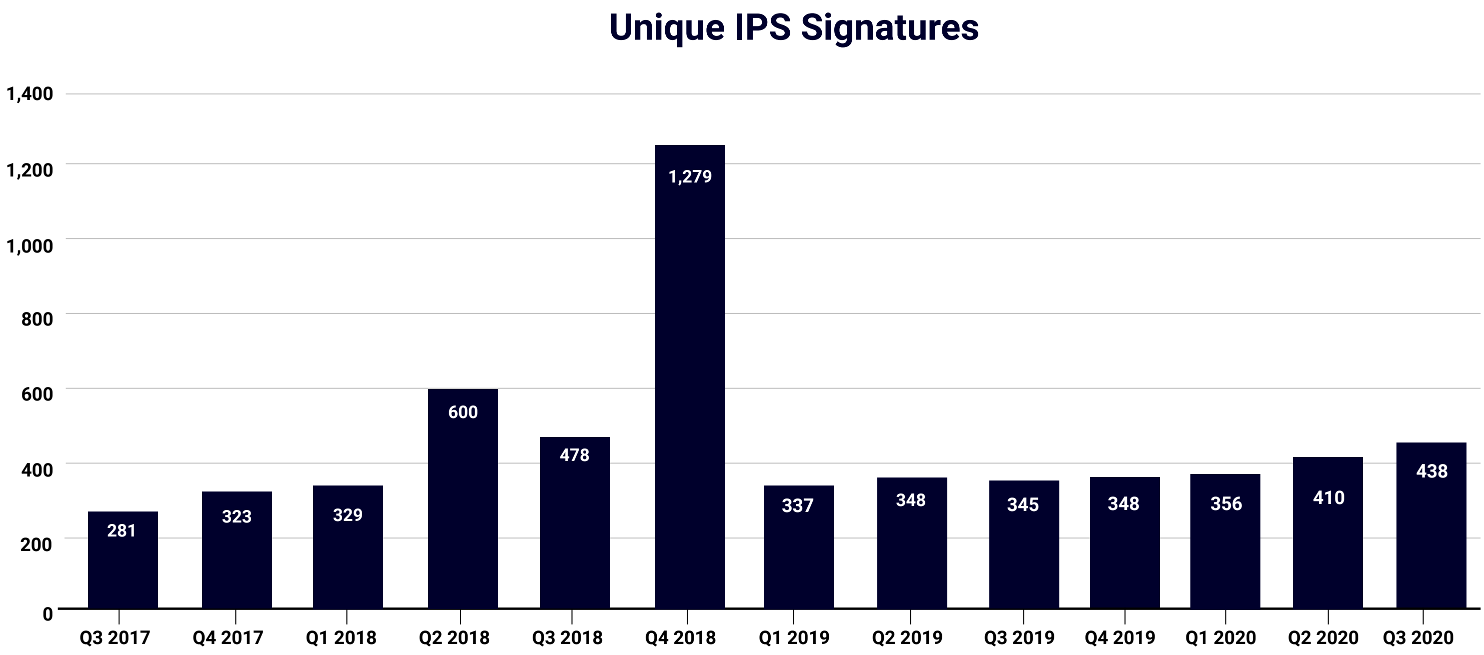


*Figure 8: Quarterly Trends of Unique IPS Signatures*

## Top 10 Network Attacks Review

| Signature | Type | Name | Affected OS | CVE | Count |
|---|---|---|---|---|---|
| 1059160 | Web Attacks | WEB SQL injection attempt -33 | Windows, Linux, FreeBSD, Solaris, Other Unix | N/A | 1,118,842 |
| 1049802 | Web Attacks | WEB Directory Traversal -4 | Windows, Linux, FreeBSD, Solaris, Other Unix, macOS | Multiple | 312,652 |
| 1133451 | Access Control | WEB Cross-site Scripting -36 | Windows, Linux, FreeBSD, Solaris, Other Unix, Network Device | CVE-2014-4116 | 289,072 |
| 1133407 | Web Attacks | WEB Brute Force Login -1.1021 | Linux, FreeBSD, Solaris, Other Unix, Network Device, Others | N/A | 210,201 |
| 1054837 | Web Attacks | WEB Remote File Inclusion /etc/passwd | Windows, Linux, FreeBSD, Solaris, Other Unix | Multiple | 135,471 |
| 1059146 | Buffer Overflow | FILE Winamp ID3v2 Tag Handling Buffer Overflow -3 (CVE-2005-2310) | Windows | CVE-2005-2310 | 128,588 |
| 1130065 | DoS Attacks | RPC Drupal Core XML-RPC Endpoint xmlrpc.php Tags Denial of Service -1 (CVE-2014-5266) | Linux, Freebsd, Solaris, Other Unix, macOS | CVE-2014-5266 | 109,086 |
| 1055396 | Web Attacks | WEB Cross-site Scripting -9 | Windows, Linux, FreeBSD, Solaris, Other Unix, Network Device | Multiple | 104,498 |
| 1055065 | Web Attacks | WEB SQL Injection Attempt -4 | Windows, Linux, FreeBSD, Other Unix | Multiple | 66,975 |
| 1136841 | Web Attacks | WEB SQL Injection Attempt -97.2 | Windows, Linux, FreeBSD, Other Unix | Multiple | 64,881 |

*Figure 9: Top 10 Network Attacks, Q3 2020*

## Most-Widespread Network Attacks

The most-widespread network attacks represent the five threats that affected the most individual networks across the world. In the previous table, we show how those attacks impacted each region and which countries encountered each threat the most. Specifically, we show what percentage of networks within the country or region were targeted by the attack.

We saw one new addition to the most-widespread network attack list this quarter. Signature 1133499 detects attempted exploits of a vulnerability in a popular supervisory control and data acquisition (SCADA) control system. Back in 2016, Trihedral patched CVE-2016-4510 in their VTScada control software, a vulnerability that could have allowed an attacker to bypass authentication and read arbitrary files off of the server. While this class of vulnerability isn't as serious as a remote code execution flaw that could allow an attacker to take full control of a vulnerable server, it could still allow an attacker to take control of the SCADA software running on the server.

SCADA systems are the computer systems behind industrial technology. VTScada has deployments across multiple industries including powerplants, oil and natural gas extraction, communications and aviation. 46% of SCADA networks in the United States were targeted by this threat in Q3 2020, highlighting a potential increased interest in targeting industrial systems in the country.

| Signature | Name | Top 3 Countries | | | AMER | EMEA | APAC |
|---|---|---|---|---|---|---|---|
| 1136841 | WEB SQL Injection Attempt -97.2 | USA<br>66.16% | Italy<br>61.92% | Canada<br>61.82% | 63.47% | 53.86% | 57.28% |
| 1059160 | WEB SQL injection attempt -33 | USA<br>55.68% | Canada<br>53.33% | Spain<br>46.12% | 50.81% | 40.62% | 44.66% |
| 1133451 | WEB Cross-site Scripting -36 | Germany<br>52.43% | UK<br>48.3% | Spain<br>42.47% | 33.82% | 44.30% | 36.25% |
| 1055396 | WEB Cross-site Scripting -9 | USA<br>42.49% | Canada<br>41.82% | Spain<br>35.62% | 38.65% | 26.48% | 28.48% |
| 1133499 | WEB NULL-Byte Injection -7 | Brazil<br>50% | Canada<br>46.67% | USA<br>45.62 | 45.90% | 18.95% | 16.83% |

*Figure 10: Most-Widespread Network Attacks Q3 2020*

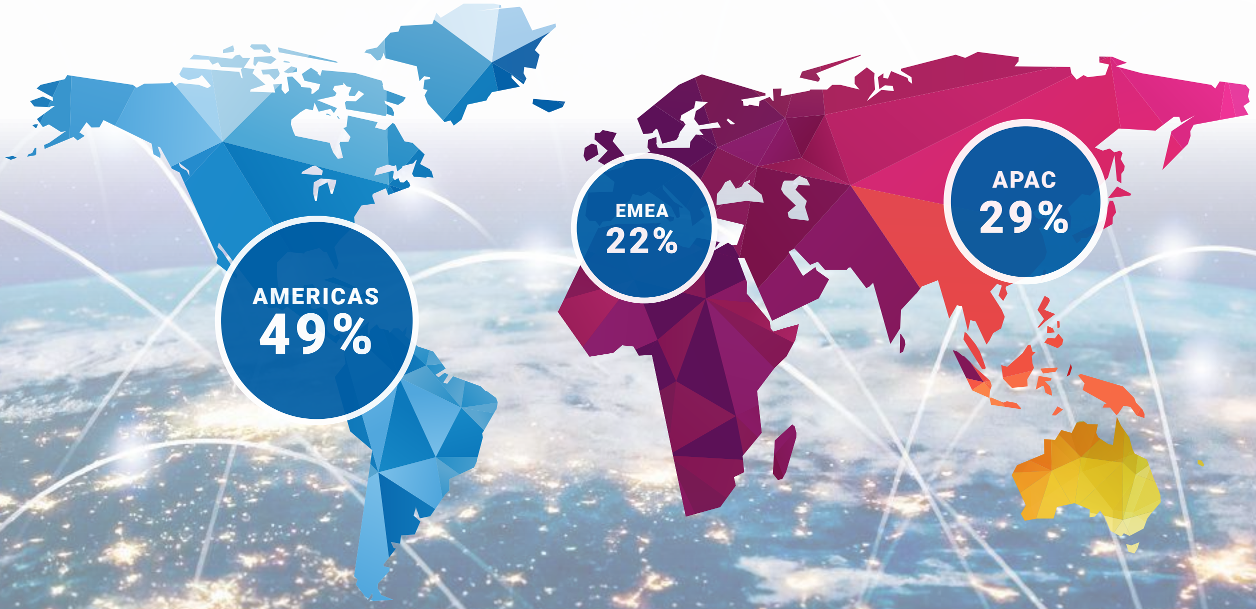
## Overall Geographic Attack Distribution

The Asia and Pacific (APAC) region saw the largest growth in detected threats from Q2 to Q3 going from 18% of the global share in Q2 to 29% of the share in Q3. This is the second quarter of growth for the region, showing increased interest by threat actors. It's possible that a return to working in a traditional office setting by many Asian countries, and the associated increase in network traffic traversing the perimeter, could account for their increase.

## Network Attack Conclusions

So far in 2020 we've seen a dramatic shake-up of the cyber threat landscape thanks to a shift to remote working across most of the world. Even with the changes that the pandemic has brought, securing network-exposed services must remain a top priority for administrators. Threat actors are constantly running probes of network-exposed services looking for weak spots, usually in the form of unpatched vulnerabilities. Keeping your systems up to date with the latest security updates and protecting them with a network intrusion prevention service are both easy steps you can take to ensuring your critical infrastructure remains out of attackers' control.

## Network Attacks by Region



# DNS Analysis

DNS, or Domain Name System, is the protocol responsible for resolving domain names to the appropriate IP address where a website is being hosted. WatchGuard's DNS-level firewalling service, DNSWatch, processes and filters domain names for known malicious behaviors before resolving them to their corresponding IP address if they are safe, or a secure black hole if not. This ensures malicious domains are blocked before any additional network traffic is sent to the website. DNSWatch checks each domain against our ever-increasing repository of domain feeds and internal intelligence. If the service identifies the domain on one of these feeds, it throws an alert and the DNSWatch Tailored Analysis team further triages the destination to guarantee it is clear of malware or any other malicious indicators before restoring access.

The DNS Analysis section of this report explores domains that have been blocked the most during the quarter. We unveil the top ten most blocked malware domains, compromised websites, and phishing domains and discuss and analyze any domains new to our lists that haven't appeared in previous quarters.

Additionally, this quarter we're introducing statistics for the total number of malicious domains blocked by DNSWatch, the average number of  malicious domains blocked per organization, and the average number of blocked domains for the Malware domain, Compromised Website, and Phishing domain classifications, respectively. Let's start off with those new general statistical highlights now.

During Q3, DNSWatch blocked a combined 2,764,736 malicious domain connections for all  DNSWatch customers who actively used it during the quarter. This translates to an average of 499 blocked connections per customer organization. Breaking it down further, DNSWatch blocked 262 malware domains, 71 compromised websites and 52 clicked phishes per organization in Q3.

**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

The top 10 malware domains list contains domains that are hosting malicious files or those that are used as command and control (C2) servers for malware. Although the overall connection count was higher for malware domains in Q3 compared to the previous quarter there were no new domains in our Top 10 Malware Domains list for this quarter. However, we did want to highlight a domain that was only a few blocked connections away from reaching this list.

**Domain: agenciacoruja[.]com (3628 hits)**

Agenciacoruja[.]com was added to our blocklists when we discovered that it was hosting a malicious file containing Emotet. We mentioned Emotet in the malware section of the report, but as a refresher, attackers originally developed Emotet as a banking trojan that has continuously evolved over the years, causing havoc to organizations from all industries and geographical regions. Coincidentally, this domain cleaned the malicious file the very same day we discovered it. Emotet shows no signs of slowing down. We, and other researchers, have seen current Emotet infections dropping additional payloads like Trickbot and even the Ryuk ransomware.

| Malware | |
|---|---|
| **Domain** | **Hits** |
| dc44qjwal3p07.cloudfront[.]net | 925,927 |
| bellsyscdn[.]com | 344,238 |
| toknowall[.]com | 38,354 |
| orzdwjtvmein[.]in | 23,353 |
| newage.newminersage[.]com | 19,267 |
| newage.radnewage[.]com | 19,005 |
| d3i1asoswufp5k.cloudfront[.]net | 18,050 |
| h1.ripway[.]com | 14,825 |
| findresults[.]site | 13,664 |
| d3l4qa0kmel7is.cloudfront[.]net | 3,827 |

* Denotes the domain has never been in the top 10

## Top Compromised Websites

Compromised websites are defined by DNSWatch as domains that attackers have hijacked, defaced, or modified to contain malicious behaviors such as a redirect to an external website that leads to further exploitation of an unsuspecting victim. The primary difference between a compromised website and a malware domain is that a compromised website served a genuine purpose before attackers took it over, either fully or partially. On the other hand, a malware domain's specific purpose is to facilitate malicious activities. In Q3, we found two new domains in the Top 10 Compromised Websites list.

**Domain: best[.]prizedea2040[.]info**

We added the first domain in our Top 10 Compromised Websites list to our blocklists in July, after we discovered it was part of a COVID-19 adware campaign. If you visit the small subset of domains related to this campaign, you're immediately redirected to best[.]prizedea2040[.]info via malicious advertisements. Additionally, the website produces an ad bar that asks you to "update for latest version." The malicious advertising redirect does offer valid justification for us to label this as malvertising under the DNSWatch definition. However, we chose the Compromised Website classification because the original set of domains that redirected you were used for legitimate COVID-19 related purposes.

**Domain: stonecalcom[.]com**

We first discovered Stonecalcom[.]com almost three years ago and it just now made its way into the Top 10 Compromised Websites list. Attackers compromised the domain by injecting a malicious JavaScript payload into the website. The payload uses the victim's CPU to mine the Monero cryptocurrency in what is commonly called a drive-by cryptomining attack. The campaign responsible for this drive-by cryptomining attack primarily targets Android users, and thus, uses a victim's Android device to unsuspectingly mine Monero cryptocurrency using the phone's CPU. The only silver lining here is that the Android user must be on the compromised website for any cryptomining to occur and closing the browser tab stops the attack.

| Compromised | |
|---|---|
| **Domain** | **Hits** |
| update.intelliadmin[.]com | 320,327 |
| disorderstatus[.]ru | 39,868 |
| 0.nextyourcontent[.]com | 9,978 |
| differentia[.]ru | 8,183 |
| ssp.adriver[.]ru | 4,592 |
| www.sharebutton[.]co | 2,092 |
| best.prizedea2040[.]info * | 1,454 |
| rekovers[.]ru | 1,283 |
| d.zaix[.]ru | 429 |
| stonecalcom[.]com * | 371 |

* Denotes the domain has never been in the top 10

## Top Phishing Domains

Phishing has become one of the most ubiquitous social engineering attacks faced by organizations for the past several years. These attacks attempt to trick their victims into providing sensitive information unknowingly or downloading malware without their knowledge. Phishing attack campaigns last an average of a few days to a week, and as such, there are commonly new domains that are placed on our Top 10 Phishing Domains list. For this quarter, there were six new domains that haven't appeared on any prior Top 10 list. They are described below.

**Domain: unitednations-my[.]sharepoint[.]com**

As the domain implies, this phishing attack utilizes Microsoft SharePoint to host a pseudo-login page impersonating the United Nations. Phishing attacks increasingly utilize Cloud services such as Microsoft SharePoint, Google APIs, and Amazon Web Services (AWS) to quickly create phishing campaigns with little risk to the attacker. Not only that, attackers can easily spin up duplicate phishing campaigns if they are cleaned by administrators. The email hook for this domain contained messaging about small business relief by the UN due to COVID-19. Always be cognizant of any SharePoint links you click on to ensure they originate from a trusted source.

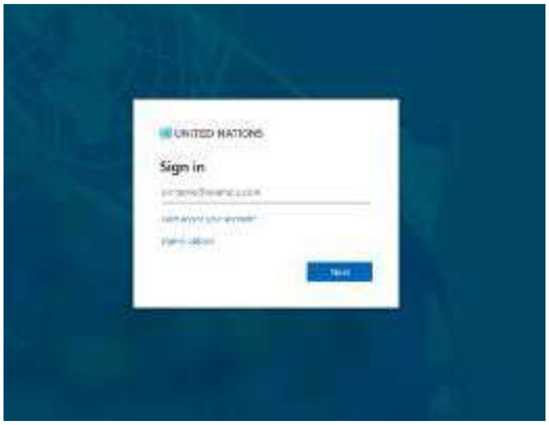


*Figure 11: United Nations phishing campaign*

| Phishing | |
|---|---|
| **Domain** | **Hits** |
| paste[.]ee | 143,526 |
| mytoprightgroup-my.sharepoint[.]com | 18,070 |
| unitednations-my.sharepoint[.]com * | 8,161 |
| cook.shortest-route[.]com | 7,034 |
| bestrevie[.]ws | 3,864 |
| data.travelzoo[.]com * | 1,999 |
| siriusxmradio-inc-mid-prod1-t.adobe-campaign[.]com * | 1,119 |
| gm7e[.]com * | 895 |
| e.targito[.]com * | 875 |
| run.plnkr.co | 690 |

* Denotes the domain has never been in the top 10

**Domain: data[.]travelzoo[.]com**

The next domain on our Top 10 Phishing Domains list is data[.]travelzoo[.]com. This phishing attack, like the United Nations phishing attack above, utilizes Cloud services to host their impersonated login page. Although, this time, the Cloud service is Firebase and the attack is impersonating Microsoft. The screenshot below shows the impersonated Microsoft login page and the Firebase domain the resulting phishing redirect leads to.

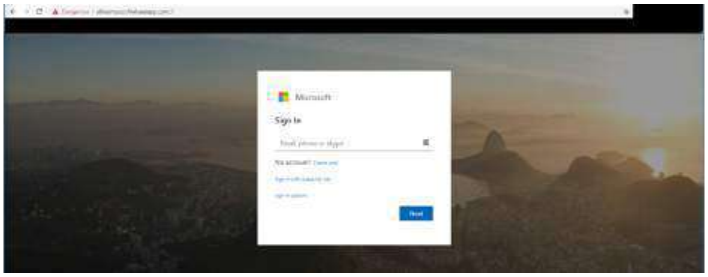


*Figure 12: Travelzoo phishing attack*

**Domain: siriusxmradioinc-mid-prod1-t[.]adobe-campaign[.]com**

The assumption from this domain name is that this either targets Adobe or SiriusXM users. However, the DNSWatch Tailored Analysis team only acquired evidence that this is targeting Microsoft Office 365 users because the landing page is of a generic Microsoft login, similar to the phishing campaign above from data[.]travelzoo[.]com.

**Domain: gm7e[.]com**

The domain, gm7e[.]com, was shared with us by one of our DNSWatch customers. This phishing attack was cleaned before our DNSWatch Tailored Analysis Team could analyze it further, but our customer shared with us that this domain was impersonating GreenMail Inc. Email Marketing. Gm7e[.]com is not a domain that is owned by GreenMail Inc., and thus is a phishing attack targeting the users of this service.

**Domain: e[.]targito[.]com**

The final phishing domain on our Top 10 Phishing Domains list is, coincidentally, another impersonation of an email marketing company that one of our DNSWatch customers submitted to us. Although, instead of attempting to harvest credentials of their victims, this attack presented potential victims with an eFax. Unfortunately, our DNSWatch Tailored Analysis team was unable to analyze the eFax further to discover any potential malicious behaviors. This domain, and the domain prior, are prime examples of customers sharing malicious domains that ultimately ensure all DNSWatch users are protected from the same threats.

## Conclusion

Phishing remains an incredibly successful method for initiating a breach. Outside of malware bacons, every single detection in this section of the report comes from someone clicking on a phishing link. That means the user has already lost and was only saved because of the technical controls in place to catch their mistake. Phishing awareness training for your users should be a top priority for defending against this style of attack, but that doesn't mean you can slack on other tools to catch what your users miss.

# Firebox Feed: Defense Learnings

As continued lockdowns in Europe and possible lockdowns in the US push more users to work from home, we believe the rise in botnets we saw in Q3 will become worse. Network attacks continue to poke for weaknesses on servers, many trying to steal data or install ransomware. Users at their home computers, remote servers, and services create targets for malicious actors to exploit. We gathered here some tips to keep your devices safe in the coming months.

1

## Watch out for Emotet

Never trust documents sent by unknown users. PDF, Excel, and Word documents often load malware like Emotet. Even if you receive a document from someone you know ensure you check the file for malware, and better yet, verify the sender really sent you that document. If you must review the document, ensure you have the latest Microsoft Office updates and update your PDF reader. Finally, never allow macros from an unknown source. Remember that malicious websites may also download Emotet if you don't block it or check your links.

2

## Speaking of website links...

Sites like unitednations-my[.]sharepoint[.]com try to steal credentials while other malicious sites load malware. Use a DNS-based security to protect users from accessing malicious domains. With almost 500 clicks blocked for each network, DNSWatch stopped users from reaching these sites before entering private information even when they clicked.

3

## Follow password best practices

This allows them to sometimes access online accounts using the same credentials. If you use the same password everywhere then they have access to every account. A password manager allows you to use secure unique passwords on each account. This provides better security for a stolen or leaked password, since they are stored as a hash that stills need to be cracked. A longer, random password – like those used in password managers – would take far too long to crack. This means even if an attacker steals your hasked credential from some site, it won't get cracked and they will not gain access to your actual password.

# Top Security Incident

# Top Security Incident

## Twitter Breach

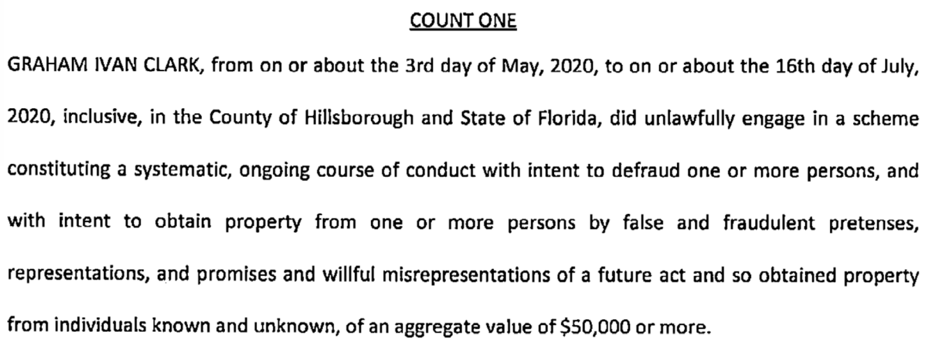
If you checked your Twitter feed on July 15, you may have noticed some strange tweets from prominent individuals like Amazon CEO Jeff Bezos, Tesla/SpaceX front man Elon Musk, and even former president Barack Obama. Within a few minutes of each other, several dozen high-profile accounts began tweeting out similar messages that contained promises of doubling any Bitcoin sent to a wallet address listed in the tweet. While the messages may seem like obvious scams to some, they were met with success. Before Twitter caught on and took down the offending tweets, one of the Bitcoin wallets had amassed over $100,000 in incoming transactions.

Twitter, to their credit, were swift with their response. It took less than two hours for them to regain control of the accounts and implement temporary restrictive measures to prevent additional scam tweets while they investigated. Over the following days and weeks, Twitter proactively reached out with additional details on the breach. Even then, this breach highlighted a serious vulnerability in our connected age. Multiple compromised accounts were high-profile US politicians. We were lucky that they only tweeted a Bitcoin scam and not something that could have caused a global conflict.

In this section, we will dive into the July Twitter breach. We'll analyze how it happened, how Twitter could have prevented it, and how law enforcement was ultimately able to track down the three individuals responsible for it.

### The Breach

Thanks to federal indictments related to the breach, paired with Twitter's own commendable transparency, we can paint a relatively detailed picture of how the attack occurred. According to the indictment against the alleged "mastermind," the breach began on May 3, 2020, a full two months before the compromised accounts began tweeting out cryptocurrency scams.

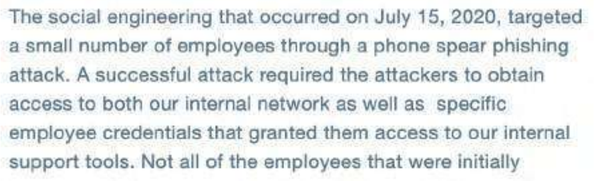


COUNT ONE

GRAHAM IVAN CLARK, from on or about the 3rd day of May, 2020, to on or about the 16th day of July, 2020, inclusive, in the County of Hillsborough and State of Florida, did unlawfully engage in a scheme constituting a systematic, ongoing course of conduct with intent to defraud one or more persons, and with intent to obtain property from one or more persons by false and fraudulent pretenses, representations, and promises and willful misrepresentations of a future act and so obtained property from individuals known and unknown, of an aggregate value of $50,000 or more.

*Figure 13: Excerpt from court documents*

According to reporting by the New York Times, the individual obtained basic access to a Twitter employee administrative tool during this time. In order to use the tool though, they still needed to authenticate to an employee account protected by MFA. Thanks to a blog post from Twitter, we know the individual successfully spear-phished at least one twitter employee, giving them access to the required credentials.



The social engineering that occurred on July 15, 2020, targeted a small number of employees through a phone spear phishing attack. A successful attack required the attackers to obtain access to both our internal network as well as specific employee credentials that granted them access to our internal support tools. Not all of the employees that were initially

*Figure 14: Twitter's response*

Using the tool, the individual was then able to take control of individual accounts by changing the associated email address and issuing a password reset. Multi-factor authentication (MFA) served no protection in this case because the attacker wasn't logging in to individual accounts but was instead changing the account info to something under their control. This is generally the case for insider threats, both willing and unwilling. Many security controls are rendered useless if someone with administrative access is the one carrying out the attack.

Through their access, the threat actor then sold off the ability to send messages from high-profile accounts in exchange for Bitcoin. One of those sales resulted in the cryptocurrency scams that began popping up during the breach.

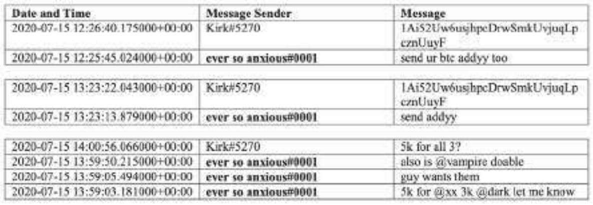
You might find it surprising that this attack didn't involve sophisticated malware or complicated "hacking," but it's increasingly common for threat actors to accomplish major breaches with little more than a well-crafted phish. The Twitter breach simply showed us another example of the risk our own employees potentially pose to security.

## Tracking Down the Threat Actor

On July 31, prosecutors in Hillsborough county Florida filed 30 felony charges against Graham Ivan Clark, a 17-year-old resident of Tampa. Soon after, the US Department of Justice announced charges against two other individuals involved in the breach, 19-year-old Mason Sheppard of Bognor Regis, UK and 22-year-old Nima Fazeli of Orlando, Florida. These arrests and charges came just 16 days after the breach, an extremely short period of time from incident to indictment in the world of cybersecurity. Through the court filings, we can piece together the operational security (OpSec) failures by the three threat actors that ultimately lead to their quick arrest.

The trail starts with OGUsers, a marketplace for username and account access for various services ranging from Twitter to Playstation Network. The name comes from the term "OG Account" meaning one of the original accounts for a service that typically comes with a much sought-after shorter or unique username like "@hack" or "@ok." Clark, Sheppard and Fazeli were all frequenters of the OGUsers forum and Discord chat server. And after Clark obtained access to Twitter's internal tools, he reached out to Sheppard and Fazeli on the sit's Discord chat server to sell access to several Twitter handles. The discussions ultimately lead to the three posting advertisements on the OGUsers forum promoting the sale of their near-indiscriminate access to Twitter accounts.

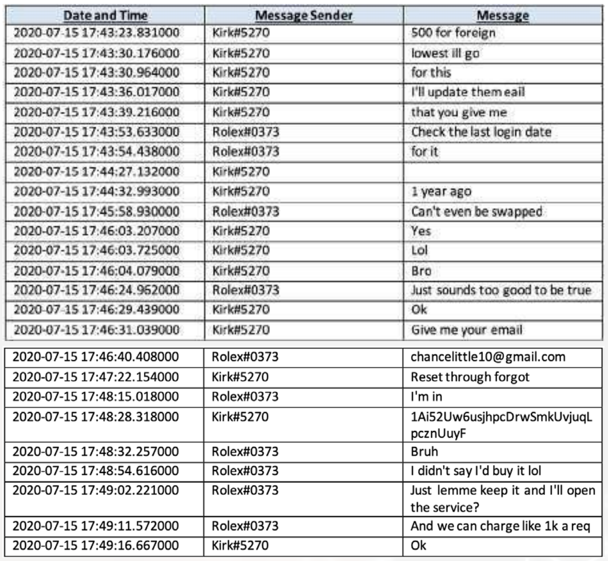
Here is where they made their first mistake. Both Fazeli and Sheppard linked their Discord usernames to their OGUsers profiles, making it trivial for law enforcement to subpoena chat logs from Discord. In the Discord chat logs presented in the indictment against Sheppard, you can see him (username ever so anxious#0001) discuss buying access to several accounts with Clark (username Kirk#5270).



| Date and Time | Message Sender | Message |
|---|---|---|
| 2020-07-15 12:26:40.175000+00:00 | Kirk#5270 | 1Ai52Uw6usjhpcDrwSmkUvjuqLp<br>cznUuyF |
| 2020-07-15 12:25:45.024000+00:00 | **ever so anxious#0001** | send ur btc addyy too |
| 2020-07-15 13:23:22.043000+00:00 | Kirk#5270 | 1Ai52Uw6usjhpcDrwSmkUvjuqLp<br>cznUuyF |
| 2020-07-15 13:23:13.879000+00:00 | **ever so anxious#0001** | send addyy |
| 2020-07-15 14:00:56.066000+00:00 | Kirk#5270 | 5k for all 3? |
| 2020-07-15 13:59:50.215000+00:00 | **ever so anxious#0001** | also is @vampire doable |
| 2020-07-15 13:59:05.494000+00:00 | **ever so anxious#0001** | guy wants them |
| 2020-07-15 13:59:03.181000+00:00 | **ever so anxious#0001** | 5k for @xx 3k @dark let me know |

***Figure 15: Account purchases from court documents***

Each of the accounts discussed in the chat were among those compromised on the day of the breach. In a separate conversation with Fazeli (username Rolex#0373), Clark completes the sale of the Twitter handle "Foreign" for $500, changing the account's email address to one provided by Fazeli.



| Date and Time | Message Sender | Message |
|---|---|---|
| 2020-07-15 17:43:23.831000 | Kirk#5270 | 500 for foreign |
| 2020-07-15 17:43:30.176000 | Kirk#5270 | lowest ill go |
| 2020-07-15 17:43:30.964000 | Kirk#5270 | for this |
| 2020-07-15 17:43:36.017000 | Kirk#5270 | I'll update them eail |
| 2020-07-15 17:43:39.216000 | Kirk#5270 | that you give me |
| 2020-07-15 17:43:53.633000 | Rolex#0373 | Check the last login date |
| 2020-07-15 17:43:54.438000 | Rolex#0373 | for it |
| 2020-07-15 17:44:27.132000 | Kirk#5270 | |
| 2020-07-15 17:44:32.993000 | Kirk#5270 | 1 year ago |
| 2020-07-15 17:45:58.930000 | Rolex#0373 | Can't even be swapped |
| 2020-07-15 17:46:03.207000 | Kirk#5270 | Yes |
| 2020-07-15 17:46:03.725000 | Kirk#5270 | Lol |
| 2020-07-15 17:46:04.079000 | Kirk#5270 | Bro |
| 2020-07-15 17:46:24.962000 | Rolex#0373 | Just sounds too good to be true |
| 2020-07-15 17:46:29.439000 | Kirk#5270 | Ok |
| 2020-07-15 17:46:31.039000 | Kirk#5270 | Give me your email |
| 2020-07-15 17:46:40.408000 | Rolex#0373 | chancelittle10@gmail.com |
| 2020-07-15 17:47:22.154000 | Kirk#5270 | Reset through forgot |
| 2020-07-15 17:48:15.018000 | Rolex#0373 | I'm in |
| 2020-07-15 17:48:28.318000 | Kirk#5270 | 1Ai52Uw6usjhpcDrwSmkUvjuqL<br>pcznUuyF |
| 2020-07-15 17:48:32.257000 | Rolex#0373 | Bruh |
| 2020-07-15 17:48:54.616000 | Rolex#0373 | I didn't say I'd buy it lol |
| 2020-07-15 17:49:02.221000 | Rolex#0373 | Just lemme keep it and I'll open the service? |
| 2020-07-15 17:49:11.572000 | Rolex#0373 | And we can charge like 1k a req |
| 2020-07-15 17:49:16.667000 | Kirk#5270 | Ok |

***Figure 16: Account purchases from court documents***

When it came to linking these identities to actual humans, the FBI was aided by a bit of an ironic incident. On April 2, 2020, the OGUsers forum suffered a data breach of their own, leaking the information of all of their users including registration email addresses, connection IP addresses and private chat logs. Starting with Sheppard, the FBI was able to link his OGUsers account to the email address masonshppy@gmail.com (a play on his first name Mason). They then subpoenaed the Bitcoin exchanges CoinBase and Binance, for information relating to accounts registered with those email addresses. Both cryptocurrency exchanges provided uploaded photographs of a driver's license issued to Mason Sheppard (US financial crimes laws require additional verification like ID photographs when opening cryptocurrency exchange accounts).

Fazeli suffered from similar lapses in OpSec that ultimately lead to his downfall. Through the same OGUsers breach, the FBI identified Fazeli's registration email address as damniamevil20@gmail.com. Through the private chat logs in the breach, the FBI also identified the email address chancelittle10@gmail.com as one Fazeli used for payments related to sales back in 2018. Fazeli also used these same email addresses to open accounts with the CoinBase cryptocurrency exchange and PayPal respectively. Thanks to a subpoena of the CoinBase account, the FBI obtained a photo of Fazeli's driver's license.

There are fewer details in the indictment against Clark, largely because it was shifted down to the State level because he was a minor, but the FBI confirmed later that they had similar evidence linking Clark to his online personas. In either case, you would think that individuals who were trafficking stolen accounts would at least use different email addresses for cryptocurreny exchanges where they had uploaded their photo ID.

## What Could Twitter Have Done Differently

The unfortunate reality is, there are some individuals on social media that have exceptional influence over their followers and the public as a whole. These accounts need additional protections in addition to the security features that Twitter provides to the rest of us. Of note, President Donald Trump's account was not compromised, likely due to additional protections put in place after a rogue Twitter employee deactivated his account in November 2017. The President is not the only Twitter user that could benefit from these protections.

The threat actor had access to an internal tool that let them modify account information like email addresses and issue password resets for various accounts. It is safe to assume that Twitter at least logs modifications made through this tool. A single set of employee credentials modifying several high-profile accounts, or even just verified accounts, should set off red flags that could trigger restrictions.

It is hard to identify a legitimate case where a single employee, without sign-off from a superior, would need to modify the registration info for dozens of high-profile users in a short period of time.

Additionally, Twitter already monitors the contents of Tweet messages for features like "trending" topics. Multiple high-profile accounts all tweeting identical or near-identical messages should set off alarm bells too. It is possible that this is exactly what originally notified Twitter of the incident, but they have not confirmed that publicly.

Anomaly detection as a whole is another tool that a massive organization like Twitter could and should employ. With the massive amounts of posting and historical behavior data at their control, identifying anomalies like dozens of extremely popular accounts suddenly changing their email address and then tweeting the same message should be possible. And when it comes to changing the contact info itself, there are some accounts that might warrant having a "two key" approach where the request needs to be confirmed by a second employee before it can be completed.

# Important Takeaways

The Twitter breach proved that sometimes security is entirely out of the control of a platform's end users. All it takes is one employee falling for a phish to completely undo much of the protections you put in place to secure your systems. This is simply the latest example of why security training for your employees and tools that detect abnormal behavior are so critical. That said, there are some things we can all learn from the Twitter breach and apply to our own organizations.

1

## Phishing training is critical

More often than not, a username and password are all that stands between a successful and a thwarted cyber attack. While we can use tools like password managers to generate strong passwords that resist brute force guessing and MFA to make it more difficult to use stolen credentials, we can't slack on helping secure employees from giving up those credentials and MFA tokens willingly. Make sure you are conducting phishing awareness training and testing regularly with test scenarios where an attacker might try to phish an MFA credential from an unsuspecting employee.

2

## Look for anomalies

Know what normal behavior looks like both for computer activity and employee behavior and keep an eye out for deviations. Even something as simple as multiple employees all logging in to a VPN from the same IP address is suspicious enough to warrant investigation. This is where visibility is key. Make sure you have the visibility tools in place to identify and act on suspicious behavior before it is too late.

3

## Privileged accounts require additional security

Some of your employees, or even yourself if you work in IT, need elevated access to accomplish their day-to-day responsibilities. With that additional power comes the responsibility of keeping it out of the hands of cyber criminals. Consider what would happen if one of your elevated accounts ended up under the control of an attacker and consider mitigations like multi-account sign-off for the most critical tasks.

# Conclusion & Defense Highlights

# Conclusion & Defense Highlights

If you've reached this far, hopefully you've already gleaned some 20/20 security foresights to help protect your organization going forward. We gave some threat-specific defense tips in the Firebox Feed Defense section of this report, and some additional tips related to the Twitter breach in that section. We even sprinkled a number of protection strategies through the report itself. In this section, I typically summarize the most important tips from the report. However, to increase your 20/20 foresights even more, I will continue a tradition I started last quarter and end with some general, but high-value, security strategies that will help protect you no matter the threat.

## Have you done a data audit lately?

One of the biggest cybersecurity mistakes many make is focusing their protections on devices or technology, rather than the real asset – information. They call it information security for a reason. The device your digital information resides on is just a thing and can be replaced. More importantly, digital information is transient; it rarely stays in just one place. Before you worry about what types of defenses to deploy, you need to understand best positions for those protections, and you'll only know that if you have tracked where your most valuable, sensitive, and confidential data resides in your business. What types of data are most important, and where that data resides, are different for every organization. If you are an ecommerce retailer, your website's database may be the most important datastore, as it contains both your customers' PII, and all the means with which to allow your site to sell stuff. If you're a law firm, that data may reside on individual partners' computers, or some central file repository. Wherever that data is for you, the first step to securing any organization is locating all your important data, prioritizing it based on its business value, and only then can you select the right type of defenses based on what you find. If you haven't refreshed your data audit in a few years, or worse yet have never done one before, we highly recommend you do.

## Focus protection on your users

Ultimately, wherever your data resides, your users or employees will have access to it. That's why you must strongly protect them, wherever they might work from. Start that protection with strong user authentication. If an attacker can pretend to be your user, they don't have to "hack" at all, as that user has the key to skate right past security and access data as a trusted user. Multi-factor authentication (MFA) is one of the best ways to protect users, by making sure people really are who they say. Meanwhile, our users have left our offices due to the pandemic, but some aspect of this change will likely continue long after it. Protecting the user includes focusing on security controls that travel with them. Endpoint Protection (EPP) solutions like WatchGuard's Adaptive Defense 360 provide a full suite of security to your users. Products like WatchGuard Passport can combine MFA with strong DNS security, to make sure users don't reach phishing sites they click on. As the world has shifted to a remote workforce, be sure you bolster your user-based protections.

## You still can't neglect the perimeter

While you need to focus on protections that follow the user, don't forget the critical assets and network workloads that remain behind your corporate perimeter and the Cloud. Sure, people are working from home, but the network services and assets still sit in your office. Worse yet, you need to allow remote access to them in some way for your remote workers. Though malware targets users, we still saw a huge increase in network attacks targeting network service software that still sits in your data centers. As you rebalance your end-user protections, remember you still need defenses like firewalls and IPS in front of your server workloads.

## Pay attention to the evolving threat landscape

If you have read this far, and gotten to this last tip, you've already partially succeeded in fulfilling it. Cybersecurity isn't stagnant (though there are some days I wish it were for ease). You've heard security pros describe this constant vigilance as a constant game of cat and mouse, or war games. For every new defense we erect, attackers imagine some new attack technique. The primary reason we publish this report is to learn their new techniques so we can evolve our defenses. Unfortunately, older defenses aren't always as effective over time, which is why protectors have to stay aware of the latest and keep up with new technology. It may sound trite (especially since it's from a childhood cartoon) but knowing really is half the battle. Continue to read research, security blogs, and reports like this to learn how the threat landscape has shifted, that way it won't shift out from under you.

I hope you've learned enough here to not have to rely on hindsight after a cyber attack. Thanks for reading our report this quarter, and we hope to see you next time. As always, leave your comments or feedback about our report at SecurityReport@watchguard.com, and stay safe.

**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 cybersecurity 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 18,000 security resellers and service providers to protect more than 250,000 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.

WatchGuard