WatchGuard

INTERNET SECURITY REPORT

Quarter 4, 2022

Contents

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

Two concepts can seem paradoxical, but both contain truth. Take history, for example. Many famous philosophers and thoughtful people have talked about how we can learn from history – even forecasting potential futures when we see trends repeat.

"Those that fail to learn from history, are doomed to repeat it."
– Winston Churchill, past prime minister of UK and author

At the same time, many smart philosophers and deep thinkers also point out history isn't predictive. New things, never seen before — sometimes called **Black Swans** — do happen.

"You can never plan the future by the past."
– Edmond Burke, author, philosopher

So, which is it? Can following history expose trends that help us prepare for potential futures ahead of time, or will new things happen that you could never predict? Simply put, both are true. You can learn from the past by monitoring and recording long-term trends, but new anomalies happen that can buck the trend, so you need to stay up to date with today's reality as well.

Furthermore, those are both the paradoxical reasons we provide you with this quarterly Internet Security Report (ISR). We track long-term trends in both network and endpoint-based cyber attacks and extrapolate potential future expectations so that you can prepare your defenses ahead of time. However, at the same time, we sometimes find completely new and unexpected threats that require new fortifications and defense strategies too. So whether you lean towards the idea that you can learn from repeating history, or you think the universe is full of entropy with no discernable patterns, our report will help, sharing both the repetitive trends and the random and surprising threat evolutions you need to know about in order to avoid them.

The Q4 2022 report includes:

06 The Latest Firebox Feed Threat Trends

Our Firebox network security products prevent tens of thousands of network and malware attacks around the world every day. This section includes the top malware, network attacks, and threatening domains we blocked during each quarter, including the most widespread attacks and regional effects. Highlights from Q4 include the continuing decline in network malware detections, the prevalence of malware associated with phishing campaigns, network exploit trends like the growth in ProxyLogin exploit attempts, and more.

28 Endpoint malware trends:

We also take a look at malware trends from an endpoint perspective, using data from our products Adaptive Defense 360 (AD360) and WatchGuard EPDR. We share the most popular vectors that malware arrives from and information about the growth or decline of various malware types and families. This quarter we saw an explosion of ransomware contrasted by a sharp decline in crytominers. We also share the latest data about the breach success rate of different ransomware groups.

39 Top Incident – LastPass

Every quarter we include a section that either shares the results of the latest research project from the WatchGuard Threat Labs or covers a widespread security story or issue from the quarter. This quarter, we cover the latest in the LastPass breach that also affects their password manager customers. While the news of this breach was first disclosed last quarter, the company transparently shared more information about the root cause this quarter. We dove into more technical detail on how the threat actor likely infected the LastPass engineer's personal computer at home.

46 Security tips for historical trends and new findings:

As mentioned in the intro, you can both learn from the past, but also adjust to the new unexpected things that happened recently. We highlight all these attack details specifically to help you find strategies to protect yourself from past, current, and future threats. We sprinkle security tips throughout our report, but also share specific defense strategies to conclude.

Executive Summary

At the highest level, during Q4 we saw declines in network detected malware, and an essentially flat volume of network exploits, and yet ransomware increased 627% from an endpoint perspective. Don't let the decline in malware fool you though. While it was down overall, we saw a rise in various malware trends when specifically looking at Fireboxes that decrypt HTTPS (TLS/SSL) traffic. Unfortunately, only ~20 percent of customers enable this free feature, and we believe encrypted traffic is where all the malware action happens these days. You should still pay attention to the latest malware defense tips (which include using our TLS decryption).

Malware also looks a bit different from the endpoint perspective than the network. Not only did we see more detections in Q4 than Q3, but we also saw explosive ransomware growth, which we mentioned above. For the past year, ransomware seemed to have plateaued, but this shows we should still expect occasional surges. We also share some annual endpoint malware trends in this report. Spoiler alert: malicious PowerShell helped deliver a lot of malware during 2022.

WatchGuard's IPS service seemed to detect about the same amount of network attacks as we did last quarter. More specifically, it technically increased by a meager 35 detections, for a whooping (sarcasm) 0.0015 percent increase. Yeah… It pretty much stayed flat. While we always see many of the same offenders (exploits) in our network attack section, we also saw some rising big-name threats too. ProxyLogin, a critical Exchange flaw that threat actors have targeted for many quarters, not only showed up in our top 10, but rose from eighth to fourth place. It even made its first appearance in our widespread malware list, meaning it is affecting most customers, not just some.

Finally, we also highlight some of the suspected technical detail of how a threat actor breached LastPass's defenses by targeting an engineer at home. With so many companies having moved to more regular remote work, you will definitely want to follow this section to learn about how you can separate people's personal computers and activities from any work access you provide them at home.

That's just a sampling of all the data we highlight in our Q4 report, so be sure to keep reading, Meanwhile, below are executive highlights from this quarter's report:

- **Endpoint ransomware detections rose 627%,** showing that you still need to maintain ransomware defenses. Make sure to have both modern security controls that proactively prevent a breach, but good disaster recovery and business continuity (backup) plans too.

- **Network-based malware detections dropped ~9.2% percent quarter over quarter (QoQ)** during Q4. This continues a general decline in malware detections over the last two quarters. However, when you look at encrypted web traffic, malware is up. We believe this trend may not illustrate the full picture, but until more customers take advantage of HTTPS inspection, we won't know for sure.

- **93% of malware hides behind encryption!** We continue to warn that most malware hides in the SSL/TLS encryption used by secured websites. Q4 continues that trend with a rise from 82% to 93%. If you don't inspect this traffic, you are missing most malware – at least with your network security controls (endpoint security does still have a chance to catch it).

- **Zero day or evasive malware has dropped to 43% in unencrypted traffic.** While that is still a significant amount of evasive malware, it's the lowest we've seen for years. That said, the story changes completely when looking at TLS connections. **70% of malware over encrypted connections evades signatures.**

- **We still believe administrators' lack HTTPS decryption veils the true trends.** We believe encryption is hiding the full picture of attack trends. Because so few Firebox users seem to scan encrypted traffic, we only have partial data about what is happening in secure web connections. Meanwhile, almost all of today's web traffic is encrypted, which logically drives you to the conclusion that encryption is where all the action is. When we do look at the data from the small percentage of devices using our free decryption capabilities, we see a much worse story, but until more people do this, our overall stats will likely continue to decline. We recommend you pay closer attention to our encrypted malware lists going forward than to the normal top 10 list.

- **Phishing campaigns have increased.** Three of the malware variants seen in our top 10 list (some also showing on our widespread list) assist in various phishing campaigns. Phishing and business email compromise (BEC) remains one of the top attack vectors, so make sure you have both the right preventative defenses and security awareness training programs to defend against it.

- **Network attack volume is flat QoQ.** Technically, it increased by a miniscule 35 hits, but since we're talking millions, that is only a 0.0015% increase… so it's essentially flat. That said, there are some nasty exploits in our top 10, so don't ignore network attacks.

- **ProxyLogin exploits continue to grow.** An exploit for this well-known, critical Exchange issue rose from eighth place in Q3 to fourth place last quarter. It should be long patched, but if not, you should know attackers are targeting it.

- On average, **Fireboxes blocked ~28 network attacks per appliance**. With network attacks staying flat, and the number of Fireboxes reporting in barely declining, this repeats the Q3 result. That said, we believe the lack of TLS decryption among our customers hides the true network attack story too, since most of the attacks we see are web-based and thus occur over encrypted connections. So perhaps it is not decreasing as much as it seems. Until more customers take the effort to enable TLS decryption, we think the real story remains hidden.

- **Endpoint malware detections increased 22%.** While the amount of network malware detection is down, our endpoint detection rose in Q4. This makes sense if you consider our theories around encrypted traffic. Our network results are likely misleading, since we are missing a lot of data from customers who do not decrypt web traffic. Meanwhile, at the endpoint TLS encryption doesn't matter, as your browser decrypts it for our endpoint software to see.

- **Lockbit remains a very prevalent ransomware group and malware variant.** We continue to see Lockbit variants often, and they are definitely the group that seems to have the most success breaching companies (through their affiliates) with ransomware.

- **Fireboxes blocked just around 3.89 million malicious domains in Q4,** which is a 35 percent decline from the previous quarter.

The full report includes lots of interesting analysis and detail around some of the top malware families and attacks, and what they are doing behind the scenes, as well as many other findings that you can adjust your defenses to. Keep reading to learn more.

Firebox Feed Statistics

What Is the Firebox Feed?

We gather anonymized Firebox feed from devices around the world. This data allows us to identify cyberattack trends. After filtering through the feed, we can identify trends in malware, network attacks, and malicious server activity. These trends include the top threats in each region to watch out for, as well as the most-widespread threats that you will likely encounter. We have recently added more details to this report. With these details, we can not only tell you the threats, but also how a threat is spread. We identify encrypted connections that detect malware or a network attack and what service caught it in the Gateway AntiVirus (GAV), APT Blocker, and Intrusion Prevention Service (IPS) sections. DNSWatch data will also provide details on the reason it blocked the domain. We can see if the server is compromised, spreading malware, or hosting a phishing page. This type of data can become meaningless without context. By including these charts, we contribute our own understanding of the data to highlight trends and anything unusual. We hope business leadership, IT, MSPs, and others can better protect their networks with this information. A Firebox configured to provide anonymized feed provides details from the GAV, APT Blocker, and IPS services. The DNSWatch application provides details on DNSWatch.

- **Gateway AntiVirus (GAV):** Signature-based malware detection
- **APT Blocker:** Sandbox-based behavioral detection for malware
- **Intrusion Prevention Service (IPS):** Detects and blocks network-based server and client software exploits
- **DNSWatch:** Blocks various known malicious sites by domain name

Help Us Improve This Report

Our data comes from Fireboxes in our Firebox Feed and the more Firebox admins that provide the anonymous data the better we can make our reports. If you configure your Firebox to do so, we will have more accurate information in this report to apply to your network. So please configure your Firebox to enable device feedback by following these 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, APT Blocker, and DNSWatch, if available

Malware Trends

Customer Fireboxes send a flurry of malware detections to our threat intelligence database, keeping us apprised of the latest trends. Network administrators who manage these Fireboxes have graciously allowed their devices to provide these anonymized detection reports to us. We analyze their details to understand what the malware landscape looked like last quarter and to investigate any trends or irregularities. With the data from this report, and previous ones, we can sometimes forecast what future malware trends might look like. We also make some conclusions and offer takeaways on defending against the current and future malware landscape.

In Q4, we saw three new phishing campaigns – JS.Agent.UNS, HTML.Agent.WR, and Agent.GBPM. As you know, phishing campaigns attempt to trick users into entering their login details on fake web pages created by the attacker. If the victim enters their details, the web page sends the entered credentials to a server controlled by the attacker. Each phishing campaign works a little differently than the next and we go over these in more detail later.

Lately our IntelligentAV (IAV) service has provided us with more detections that show its effectiveness. It never stopped being a key part of the layered protection that catches significant amounts of suspected malware, but we had removed its results from our quarterly report for around a year or so due to backend changes in our reporting syntax and systems. However, we have sorted its new reporting and analytics out, so we have reintroduced its data to our reports this quarter. Since IAV uses machine learning to identify threats, it has the ability to detect never-before-seen malware almost instantaneously on the Firebox. Because of this, we have identified a new malware sample caught by IAV and examined it in detail later in this report.

With few exceptions, we see malware authors moving to create more advanced malware that traditional detection methods can't immediately detect. Many new malware families can bypass signature detections so we must use advanced techniques if we ever hope to proactively protect our networks.

For your first line of defense, **Gateway AntiVirus (GAV)** will block most traditional malware quickly and easily.

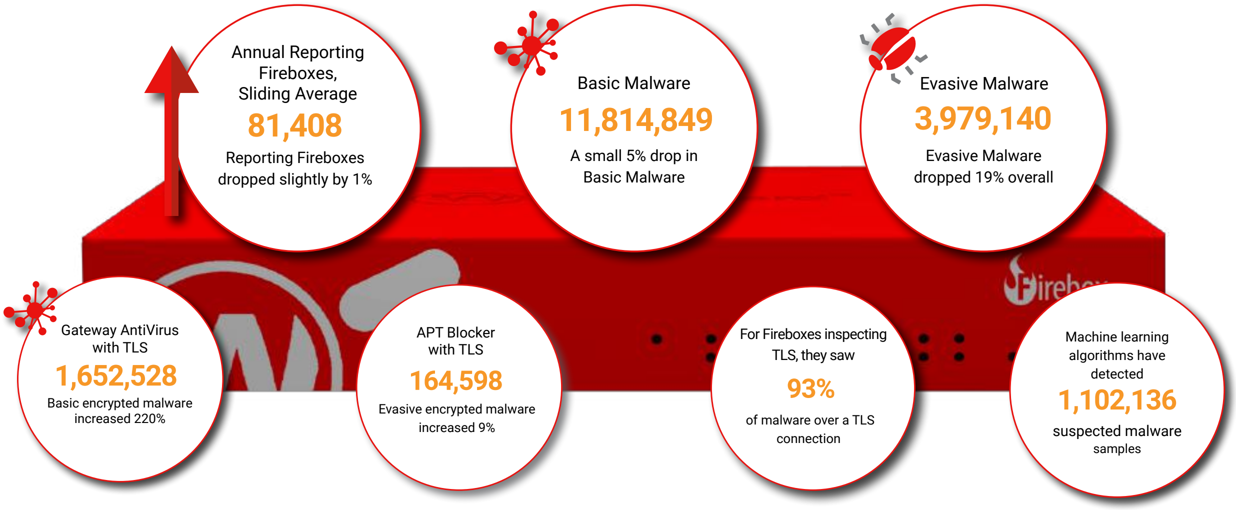
If a GAV signature doesn't exist, **IntelligentAV (IAV)** inspects the file using machine learning to identify any suspicious areas of a file.

Finally, **APT Blocker** has a full behavioral-detection sandbox to proactively detect the true intent of any file.

While not directly related to services on the Firebox, any malware defense requires a layered approach. You should also install endpoint malware protection directly on your servers and workstations. Use **Endpoint Detection and Response (EDR)** and **advanced endpoint protection (EPP)** to protect your devices.

These three layers on the Firebox and an EDR/EPP solution on the endpoint provide excellent protection from malware without interrupting your workflow.

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.



Annual Reporting Fireboxes, Sliding Average
81,408
Reporting Fireboxes dropped slightly by 1%

Basic Malware
11,814,849
A small 5% drop in Basic Malware

Evasive Malware
3,979,140
Evasive Malware dropped 19% overall

Gateway AntiVirus with TLS
1,652,528
Basic encrypted malware increased 220%

APT Blocker with TLS
164,598
Evasive encrypted malware increased 9%

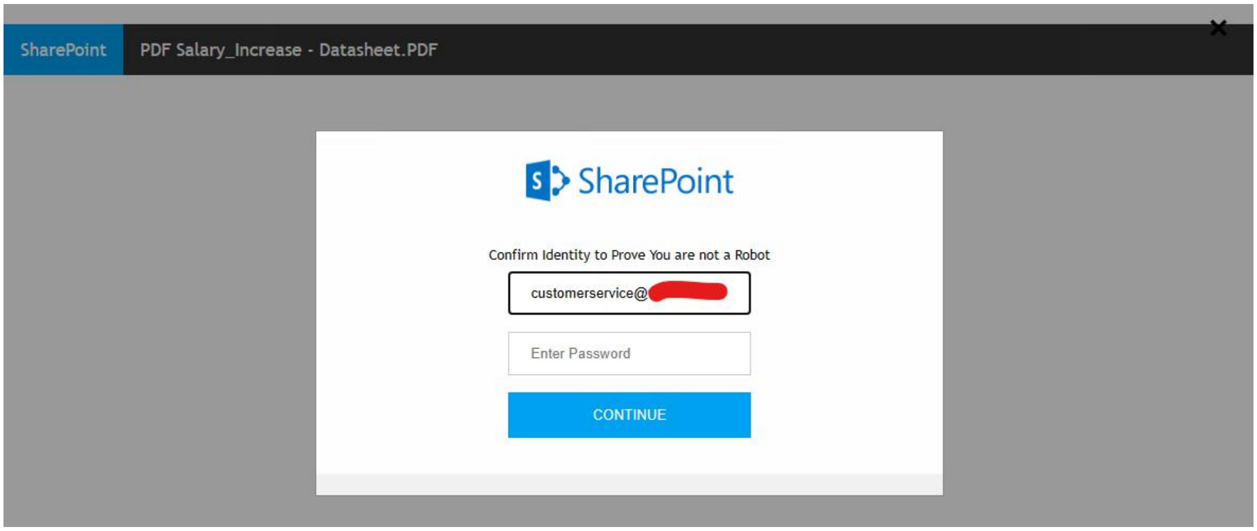
For Fireboxes inspecting TLS, they saw
93%
of malware over a TLS connection

Machine learning algorithms have detected
1,102,136
suspected malware samples

Top 10 Gateway AntiVirus (GAV) Malware Detections

We saw over 1.3 million unique basic malware signatures detected in Q4, but the top 10 malware samples made up 24% of total detections. The top 10 malware table shows the 10 highest volume malware threats, giving us a good overall view of the most common malware spreading in the threat landscape.

The most-detected malware family, JS.Agent.UNS, contains malicious HTML that directs users to legitimate-sounding domains that are masquerading as well-known websites in hopes of tricking your users. For instance, this HTML attempts to trick victims into visiting spoofed sites with domain names like amazon-survey[.]rest and bidenstumulus[.]us, but of course, those malicious domains host sites spoofing the real Amazon and Biden sites, hoping your users will accidentally share their info. Another new malware variant Agent.GBPM creates a SharePoint phishing page titled “PDF Salary_Increase.” You won’t increase your salary by entering your details on this page, but you will give the attacker access to your account.



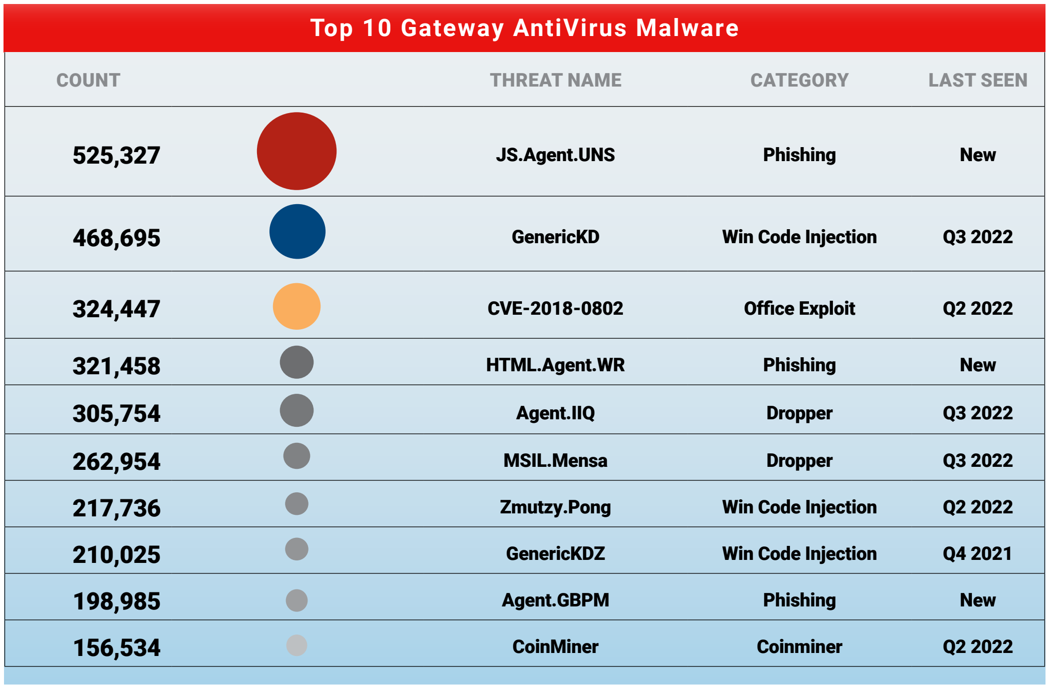
PDF Salary_Increase - Datasheet.PDF

Confirm Identity to Prove You are not a Robot

customerservice@[redacted]

Figure 1: Agent.GBPM

Finally, the last new phishing variant in our top 10, HTML.Agent.WR, opens a fake DHL notification page in French with a login link. The now-broken link previously led to a known phishing domain. HTML.Agent.WR targeted many countries, but we primarily saw it in Germany despite the fact the sample we inspected used French. Below you can find the full top 10 basic malware table.



Top 10 Gateway AntiVirus Malware

COUNT		THREAT NAME	CATEGORY	LAST SEEN
525,327	●	JS.Agent.UNS	Phishing	New
468,695	●	GenericKD	Win Code Injection	Q3 2022
324,447	●	CVE-2018-0802	Office Exploit	Q2 2022
321,458	●	HTML.Agent.WR	Phishing	New
305,754	●	Agent.IIQ	Dropper	Q3 2022
262,954	●	MSIL.Mensa	Dropper	Q3 2022
217,736	●	Zmutzy.Pong	Win Code Injection	Q2 2022
210,025	●	GenericKDZ	Win Code Injection	Q4 2021
198,985	●	Agent.GBPM	Phishing	New
156,534	●	CoinMiner	Coinminer	Q2 2022

Figure 2: Top 10 Gateway AntiVirus Malware Detections

Top 5 Encrypted Malware Detections

Now that you know what malware our customers see the most, let's look at the top 5 encrypted (TLS) malware table. This table contains the top malware Fireboxes detect over an HTTPS connection. We separate this data because many Fireboxes aren't configured to inspect encrypted traffic. In Q4, Fireboxes that scan HTTPS connections saw detections over HTTPS 93% of the time, which tells us that most malware arrives over encrypted connections. If this ratio holds true for all Fireboxes, then HTML.Agent.WR, Agent.IIQ, and Agent.GBPM would be the top 3 most-seen detections on Firebox-protected networks. As we have mentioned in past reports, we believe the encrypted malware view paints the more accurate picture of the threat landscape. We highly encourage all Firebox users to scan encrypted traffic to protect their organization from the most common way malware arrives in their network.

Let's look at the contents of the top 5 encrypted malware table. Besides the three malware variants we already discussed, malware associated with the Chinese government, Generic.Taidoor, and a popular botnet/ransomware family variant, Razy, made the list.

Top 5 Encrypted Malware Detections		
COUNT	THREAT NAME	CATEGORY
321,458	HTML.Agent.WR	Phishing
305,754	Agent.IIQ	Dropper
176,830	Agent.GBPM	Phishing
9,141	Generic.Taidoor	Win Code Injection
8,035	Razy	Botnet/Ransomware

Figure 3: Top 5 Encrypted Malware Detections

Top 5 Most-Widespread Malware Detections

More unique Fireboxes detected malware in the top 5 widespread malware table than any other malware variant. Unlike the top 10 malware by volume that just looks at the samples with the highest raw numbers, even if they repeatedly hit a relatively small number of Fireboxes, this widespread-malware list shows the malware that touches the most individual Fireboxes. For example, if you lived in Greece, you would have had a 25.51% chance of seeing Exploit.CVE-2017-11882 (a malicious Office document) in Q4 even though we don't see it in the top 10 malware table.

We do sometimes see samples that make both the top volume and widespread lists, such as Trojan.JS.Agent.UNS. Another new variant, Trojan.Agent.GAUS targets the US, Dominican Republic and the UK. We don't normally see the US and UK show up on this table, possibly because of the environments Fireboxes are used in in these countries. Also of interest, XLM.Trojan.Abracadabra, a trojan that has spread Emotet in the past, showed up on this list again as the fourth most-widespread malware detected. Among the Asia Pacific (APAC) Fireboxes, 16% saw this malware in Q4. Finally, notice that two of the most-widespread malware samples were both Office exploits that primarily targeted Greece.

Top 5 Most-Widespread Malware	Top 3 Countries by %			EMEA %	APAC %	AMER %
Exploit.CVE-2018-0802	Greece - 27.73%	Hong Kong - 22.28%	Poland - 19.64%	13.48%	5.73%	3.10%
Exploit.CVE-2017-11882	Greece - 25.51%	Turkey - 18.92%	Germany - 17.92%	11.79%	3.87%	2.72%
Trojan.Agent.GAUS	USA - 14.22%	Dominican Republic - 13.21%	United Kingdom - 12.08%	4.65%	2.12%	12.81%
XLM.Trojan.Abracadabra	Japan - 22.87%	Indonesia - 19.05%	Greece - 16.8%	7.55%	16.34%	1.84%
Trojan.JS.Agent.UNS	Italy - 9.99%	Germany - 9.74%	Netherlands - 8.92%	7.63%	6.60%	4.58%

Figure 4: Top 5 Most-Widespread Malware Detections

Geographic Threats by Region

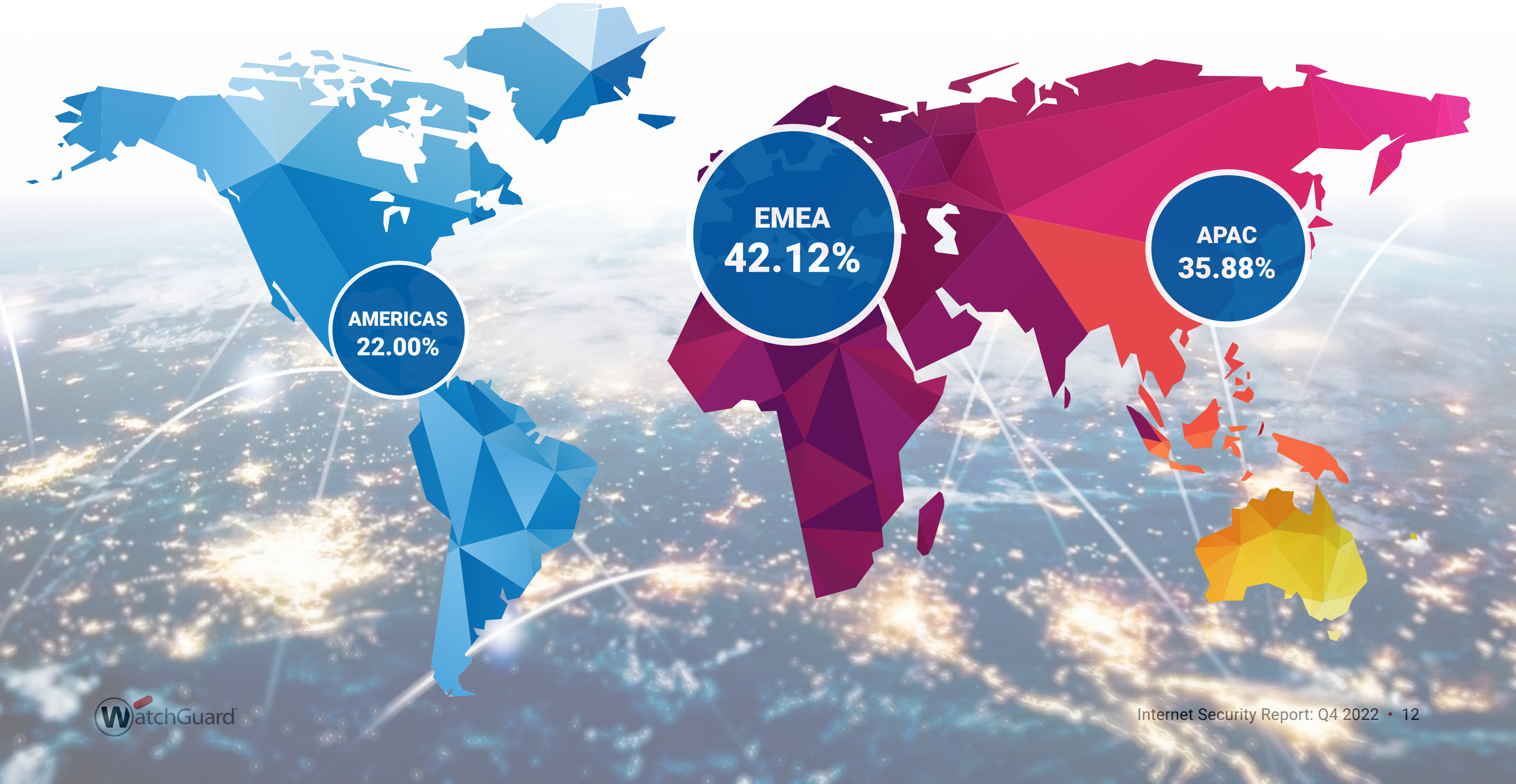
The previous malware tables show what malware we see and some regional details for specific threats, but what about the regional spread in general? In the region table, we separate the total detection by general area to give you an idea of what parts of the world see the most malware. That said, to avoid global sales trends affecting your view, we average these percentages by the number of Fireboxes in each region.

Europe, the Middle East, and Africa (EMEA) saw a drop in malware by 8%. Despite the decrease in XLM.Trojan.Abracadabra, which primarily targeted APAC, we saw an almost 8% increase in general malware in this region. The total APAC detections didn't change much between Q3 and Q4 but EMEA's totals dropped, and Americas' (AMER) totals increased slightly over the same time, causing the 8% increase in APAC.

Region	Detections per Firebox	Average % IPS Detections per Firebox
EMEA	4,687,826	42.12%
AMER	9,011,747	22.00%
APAC	3,196,552	35.88%

Figure 5: Geographic Threats by Region

Malware Detection by Region



Catching Evasive Malware

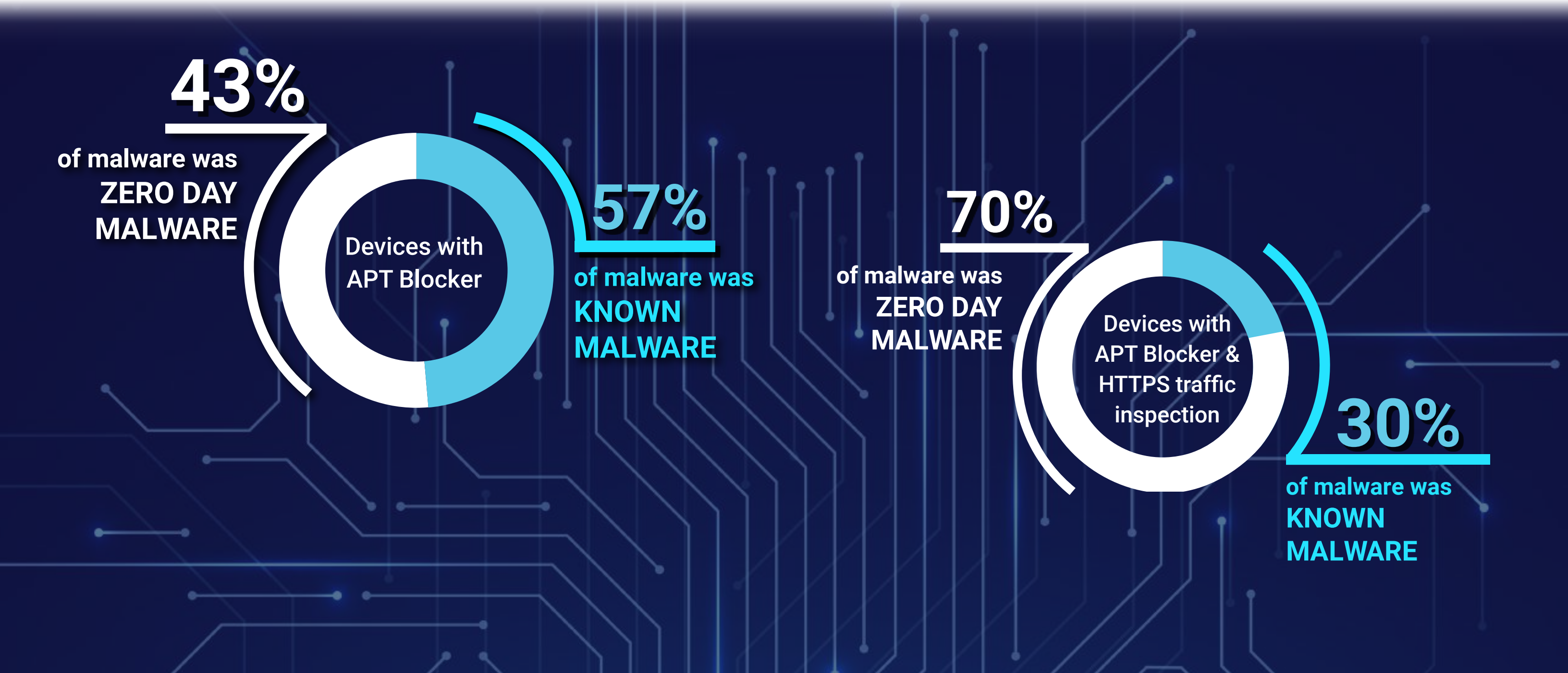
Much of the malware detected in Q4 hadn't been seen before by signature-based antivirus (AV) solutions. Zero day malware bypasses signature protection by changing the contents of the binary it arrives as, which is sometimes called polymorphism. Other malware will bypass signature protection simply because no one has seen that family of malware before, so we have no signature to detect it. To protect networks, APT Blocker, with the use of advanced sandboxing, will detonate suspicious files and executables in a sandbox to extract the behaviors it manifests and determine if it was created to do something malicious. The Firebox receives the result of this analysis, which tells it whether to allow the network traffic or not, or to inform you of the threat if the traffic was allowed before the decision was made.

In Q4 we found 43% of the total malware bypassed our basic, primarily signature-based GAV defense. This represents a 7% drop between Q3 and Q4, but still makes up a significant portion of total malware. You should enable our evasive malware detection services, like APT Blocker and IAV, in order to catch this class of zero day malware. The good news is that this 43% represents the lowest zero day malware volume we have seen for years. The bad news is, we suspect our unencrypted malware view does not paint the real picture. Most malware arrives over encrypted connections, and since so few customers enable our free HTTPS decryption capability, they are missing all those threats.

Speaking of which, Fireboxes with decryption enabled saw 70% zero day malware. A good 27% more than we saw in unencrypted connections. We see a trend of malware attempting to evade detection using encryption and other techniques to bypass signature detection. This gives the malware a good chance of infecting its target unless intercepted through TLS inspection. As mentioned above, we highly recommend you use those advanced malware detection services to stay safe.

As part of defense in depth, you should do your best to block all malware at the perimeter using a breadth of network security services. If malware bypasses basic signature-based malware detection, you should have the ability to catch it another way. With the Firebox, you can enable APT Blocker and IntelligentAV in addition to normal GAV, to provide more layers of defense that can catch more sophisticated threats.

Zero Day Malware



Individual Malware Sample Analysis

Trojan.Agent.GAUS

Agent.GAUS – not the Gauss trojan related to Flame, Stuxnet, and Duqu – contains a signature for a file that fosters communication between an Ethereum cryptocurrency mining node and a malicious server. Usually, this file is part of an application package. One such example we found contains a JavaScript file to mine Ethereum and then send it to sppedtest[.]com. Because of the typosquatting URL and the web page's relation to other malware, we suspect the script came from a malware package.

The script checks that it received real Ethereum mining data and then opens a specialized API "window.ethereum" to communicate between the victim's computer and the malicious web server, sppedtest[.]com. We have not gone into detail about this script since the script itself doesn't contain malware. Only its destination sppedtest[.]com indicates its use as a malicious mining script vs a legitimate one. In analyzing the sppedtest[.]com we found related malware using this domain. The domain is part of a cyptomining campaign that included Monero cyptomining scripts and other multiple malicious files.

Heur.BZC.PZQ.Pantera (njRAT)

A malware sample we found further down in the top malware list, Heur.BZC.PZQ.Pantera, contains a remote access trojan (RAT) called njRAT. njRAT provides an attacker remote access to a victim computer, allowing them to access the keyboard, download software, and run commands. Here is how the sample we found works.

The victim downloads an Office file (docx, xlsx, etc.) through email, or more recently Discord servers. The Office document contains an exploit to download and run a malicious PowerShell script. Often these malicious Office documents use exploits like Exploit.CVE-2018-0802, Exploit.CVE-2017-11882, or other common Office exploits. We don't have the original file that downloaded this malware, but this is how njRAT typically infects victim computers.

This script stops tasks that might prevent the malware from running and prevent analysis of the malware by running the "taskkill" command to stop various running services. Many of these services relate to the analysis of .NET files, a popular Microsoft program framework for Windows. Here are the commands it runs to stop services.

- `taskkill /IM CCleanerBrowser.exe /F`
- `taskkill /IM aspnet_regbrowsers.exe /F`
- `taskkill /IM aspnet_compiler.exe /F`
- `taskkill /IM AppLaunch.exe /F`
- `taskkill /IM InstallUtil.exe /F`
- `taskkill /IM jsc.exe /F`
- `taskkill /IM MSBuild.exe /F`
- `taskkill /IM RegAsm.exe /F`
- `taskkill /IM cvtres.exe /F`

The "/IM" argument means that the command will identify the service by the "ImageName" or executable name and '/F' argument forces the service to stop.

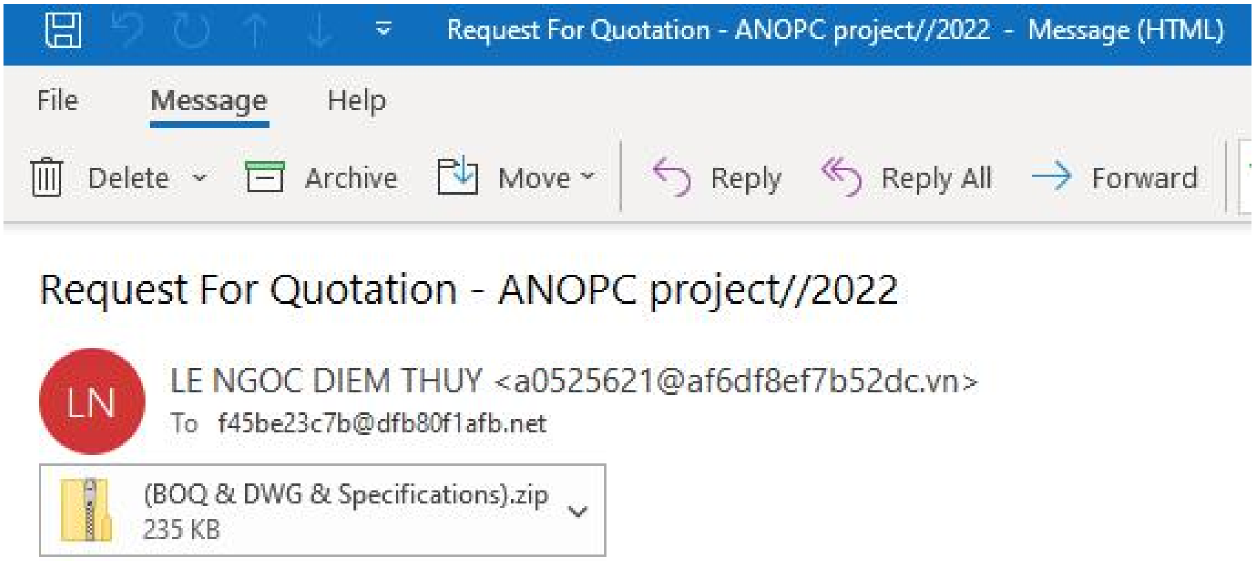
The script creates an archived executable file containing files that run on the .NET framework, which tells you why the script wanted to kill the .NET framework service. These files install the main malicious RAT payload.

The RAT then contacts 2525.libya2020[.]com.ly on port 2525 to communicate with the attacker's server, where it receives commands on what to do next. Malware researchers first saw njRAT around 2015. Since then, it continues infecting victims through Office documents, malicious Discords, and even hacked **government websites**. We've seen many malware samples use techniques like this to prevent analysis. This delays signatures and allows malware to continue to spread. We will look at a malware that successfully bypassed basic AV next.

Malicious file caught by IAV

Our IntelligentAV (IAV) service found a new variant of malware that didn't have a signature at the time of inspection. Fortunately, IAV protected this network by detecting the file through its machine-learning algorithms. If not for IAV's ability to detect this brand-new malware it could have entered the victim's network and taken over.

We identified and analyzed this sample and found it part of the FormBook Phishing campaign. This campaign often starts with an email like the one below.


Request For Quotation - ANOPC project//2022 - Message (HTML)
File
Message
Help
Delete
Archive
Move
Reply
Reply All
Forward
LN

Request For Quotation - ANOPC project//2022

LE NGOC DIEM THUY <a0525621@af6df8ef7b52dc.vn>

To f45be23c7b@dfb80f1afb.net

(BOQ & DWG & Specifications).zip
235 KB

Figure 6: IAV Catch

While we don't have the original email, we did find Fireboxes detect this malware with SMTP proxies, indicating the sample we found is also sent by email.

The file itself "d3e1ff4.exe" contains a Portable Executable (PE) that when run will disable security controls through the Windows **caspol service**. It will also contact the URL **www.darkchocolatebliss[.]com/t5ez**. Inspecting **www.darkchocolatebliss[.]com**, we found recent indicators of compromise. Based on the related malware to the darkchocolatebliss domain, this will likely download Agent Tesla or another similar botnet.

Conclusion

Malware like the samples we analyzed this quarter, including Heur.BZC.PZQ.Pantera, try to bypass normal analysis by disabling security services on the systems they affect. By using network-based malware detection services, which include advanced detection techniques like sandboxing, behavioral analysis, and machine learning, you have a chance to block this type of evasive malware before it gets to your endpoints at all. We consistently recommend layered defenses to protect your network from malware just like this one. Whether a spy balloon or malware, defense in depth means implementing these layered defenses at the perimeter even if you don’t use our product.

Network Attack Trends

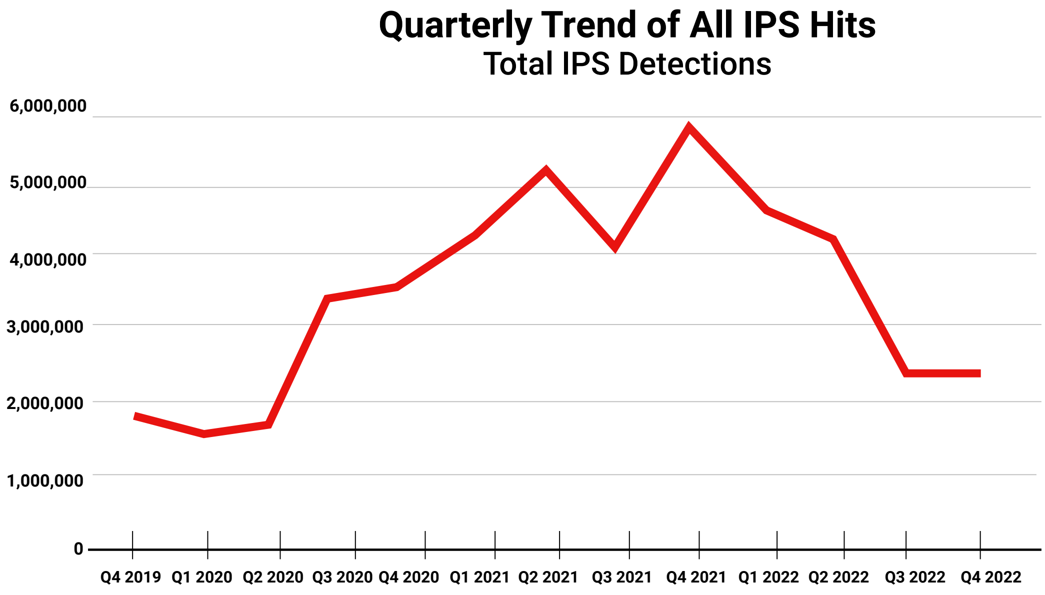
WatchGuard's Firebox Intrusion Prevention Service (IPS) detects unique network traffic patterns from a catalog of documented exploits and vulnerabilities. This signature-based security service adds new signatures regularly once the vulnerabilities or exploits for them are publicly published. As the library of new and old signatures builds, so does the range of protection that the Firebox receives. It's evident from this report, and past ones, that the IPS service protects organizations at different stages in their security posture – some more mature than others. Unfortunately, at less mature organizations plenty of software goes unpatched for months or even years, and that is where IPS protects organizations, even from much older flaws. Some companies may not have the time to find and patch everything or know that a product they use requires an important security update. In addition, organizations with a well-developed security program may still be at risk from newly published vulnerabilities. That is why IPS is essential for protecting your network at the early cyber kill chain delivery stage.

Our total IPS network attack count increased, but only by a meager 35 detections over last quarter. That is a minuscule a 0.0015% increase. The slight change is remarkable as the next smallest change was 91,885 from Q1 to Q2 2020. The new total for this quarter is 2,306,175 detections. There isn't always a rhyme or reason – at least one we can quantitatively prove – for the fluctuation in total detections per quarter. In Q3 2020 it increased by nearly 90%, followed by only a 5% increase in Q4 2020. Then Q1 through Q3 2022 were all decreases, with reductions ranging between 10%-45%. From wild to miniscule fluctuations in detections, the average change since Q4 2019 stands at 4.3%.

Taking a glimpse at the total IPS detections in Figure 7, you'll notice what may resemble a mountain range with two peaks. That taller one to the right is Q4 2021. It represented nearly 5.7 million detections. From then to now, there has been a 146% decrease, or simply put, about half as many detections. Can we explain this difference? Not for sure, but we have a theory. Many of the top signatures from Q2 2022 and before took up an exorbitant percentage of total detection hits. This may have been due to certain Fireboxes amassing the same alerts, and at some point, they had either been taken offline or addressed by the administrator.

In Q4, there was one new signature in the top 10 network attacks. A web SQL injection-based attack sitting in the eighth spot. In addition, three of the signatures were in the top 10 last quarter as well. One of those signatures is associated with the ProxyLogon vulnerability we describe in past reports, and we have continued to track its rise since discussing it last quarter.

Total unique IPS detections, which are how many different types of exploits we see, increased by over 6% this quarter. It's evident from the chart in Figure 8 that unique detections have generally veered upward, meaning threat actors seem to be trying a wider range of exploits. In Q1 2022, we saw 541 unique detections, a noticeable quarter on that chart. With 464 detections this quarter, the number isn't the highest over the past several years, but still considerably larger than previous quarters since Q4 2019.



Quarter/ Year	IPS Hits
Q4, 2019	1,878,730
Q1, 2020	1,660,904
Q2, 2020	1,752,789
Q3, 2020	3,329,620
Q4, 2020	3,498,356
Q1, 2021	4,223,523
Q2, 2021	5,168,506
Q3, 2021	4,095,320
Q4, 2021	5,686,245
Q1, 2022	4,697,568
Q2, 2022	4,232,356
Q3, 2022	2,306,140
Q4, 2022	2,306,175

Figure 7: Total IPS Detections

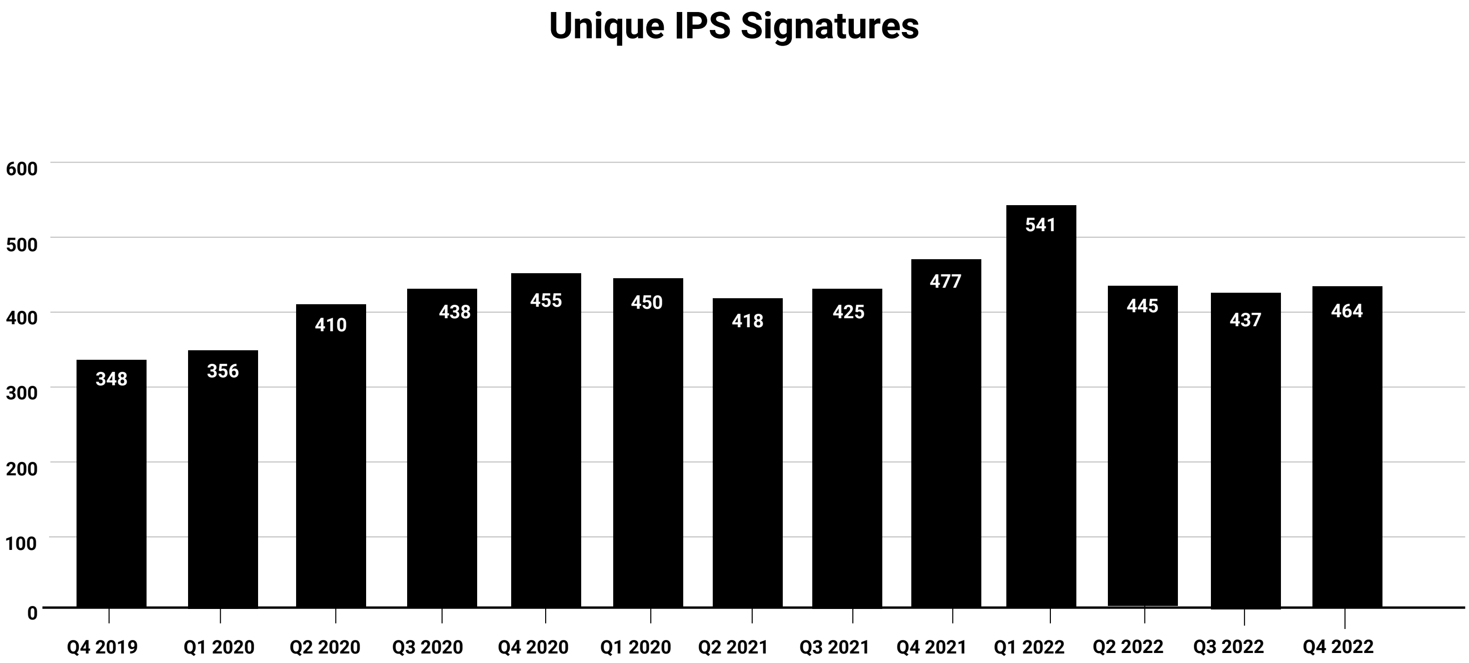


Figure 8: Quarterly Trends of Unique IPS Signatures

Top 10 Network Attacks Review

The top 10 network attacks list is based on total volume. Therefore, these detections may sometimes be concentrated on a small segment of Fireboxes, or possibly spread out among many. There is a separate section that tracks the most-widespread attacks, sometimes with a signature appearing on both lists, like signature 1138800. A few notable signatures from last quarter are discussed in this report as well. It's simply because signature 1138800 (ProxyLogon) and signature 1058077 were new last quarter and continue to hold even more elevated spots in the rankings.

Signature 1058077—'WEB SQL injection attempt -1.b"

Associated CVEs: CVE-2014-0763, CVE-2007-1729, CVE-2017-7973, CVE-2018-8734

We'll say from the get-go that this signature may give a sense of déjà vu after reading about the products affected. It has a lot of overlap with the vendors associated with signature 1058077 discussed above.

This vulnerability impacts Gnew, an open-source content management system using SQL. This software, as far as we can tell, has been discontinued for several years now. It's not surprising to see this, as this vulnerability is from 2013. The near-empty online presence would suggest that this software isn't widely used either. The vendor was unresponsive after the researchers at High-Tech Bridge Security Research Lab submitted their findings, and therefore they produced their own unofficial patch. We can surmise that the signature is being directed to more prominent software.

A software that is still active and impacted by this **SQL vulnerability** is Mantis Bug Tracker (MantisBT). It is an open-source software bug tracker. Like the Gnew vulnerability, it is old (from 2014), so this may not impact too many MantisBT users. The 'admin_config_report.php' file allowed for unsanitized input and therefore an easy SQL injection opportunity. In addition, accessing that file required administrator-level account privileges, which intensified the level of compromise if successful. We can HOPE that 99.99% of long-term (2014 and prior) MantisBT users have updated their software since the vulnerability was released. It's hard to imagine any organization has found a way (or reason) to use such outdated software, but who knows, it could still be hosted in an organization's network gathering dust. We can again surmise that this vulnerability is less relevant to the signature.

The two other CVEs, CVE-2017-7973 and CVE-2018-8734, are likely where the bulk of the intrusion attempts are directed at. This is where the déjà vu kicks in, as CVE-2017-7973 and CVE-2018-8734 were both associated with signature 1058077. CVE-2017-7973 is for a Schneider Electric's U.motion Builder software vulnerability in versions 1.2.1 and prior. This software is a web server used for smart home automation that connects to a smart screen panel, app, or web interface. This is used for a myriad of automations, such as for lighting. CVE-2018-8734 is for the core config manager in Nagios XI 5.2.x through 5.4.x before 5.4.13.

While signature 1058077 and signature 1058486 are separate, their SQL injection techniques line up close enough to share two of the same CVEs. If we were to consider them the same signature and combined the total detections, it would compromise 19.43% of total detections this quarter. That's quite a lot. It is a firm reminder for any customers with Schneider Electric's U.motion Builder or Nagios software to patch their systems, not including vendors already previously mentioned in this and the last report.

While a lot of these issues are old, once threat actors have an exploit in their botnet's "mass scan" framework, it just tries every IP it finds with the right port open against a big library of new and old exploits. We suspect most of these old exploit detections aren't actually targeted attacks but are just the results of attackers who have automated opportunistic mass scans (or even the result of legitimate vulnerability auditing software that essentially does something similar).

Signature 1138800 - 'WEB Microsoft Exchange Server Remote Code Execution Vulnerability -6

Associated CVE: CVE-2021-26855

We are returning to the table from Q3 2022 that documented the rise of the ProxyLogin vulnerability (signature 1138800) among our top 10 network attacks. This time it has risen to fourth place, from eighth last quarter. The consistent rise since Q2 2021 shows how significant this vulnerability is. Attackers are well aware of the returns they can achieve if they can compromise an on-premises Microsoft Exchange Server. We expect to see this vulnerability remain a top signature as attackers will continue to seek compromise via critical assets like Microsoft Exchange Servers.

Quarter	Rank by Volume	Detections	% of Total Volume
Q4 2022	#4	127,738	5.54%
Q3 2022	#8	89,609	3.90%
Q2 2022	#14	74,185	1.80%
Q1 2022	#20	20,052	0.40%
Q4 2021	#26	16,876	0.30%
Q3 2021	#22	20,261	0.50%
Q2 2021	#20	31,991	0.60%

Figure 9: Placement of Signature 1138800 (CVE-2021-26855) since Q2 2021

Signature	Type	Name	Affected OS	Count
1058077	Web Attacks	WEB SQL injection attempt -1.b	Windows, Linux, FreeBSD, Solaris, Other Unix, macOS	368,851
1132092	Buffer Overflow	FILE Invalid XML Version -2	Windows	310,308
1059877	Access Control	WEB Directory Traversal -8	Windows, Linux, FreeBSD, Solaris, Other Unix	144,057
1138800	Web Attacks	WEB Microsoft Exchange Server Remote Code Execution Vulnerability -6	Windows	127,738
1055396	Web Attacks	WEB Cross-site Scripting -9	Windows, Linux, FreeBSD, Solaris, Other Unix, Network Device	106,782
1059958	Web Attacks	WEB Directory Traversal -27	Windows	962,95
1054837	Web Attacks	WEB Remote File Inclusion /etc/ passwd	Windows, Linux, FreeBSD, Solaris, Other Unix	94,077
1058468	Web Attacks	WEB SQL injection attempt -25.a	Windows, Linux, FreeBSD, Solaris, Other Unix	79,287
1230275	Web Attacks	WEB Apache log4j Remote Code Execution -1.h (CVE-2021-44228)	Linux	73,866
1130366	Web Attacks	WEB Directory Traversal -16	Windows, Linux, FreeBSD, Solaris, Other Unix, Mac OS	54,836

Figure 10: Top 10 Network Attacks by Volume

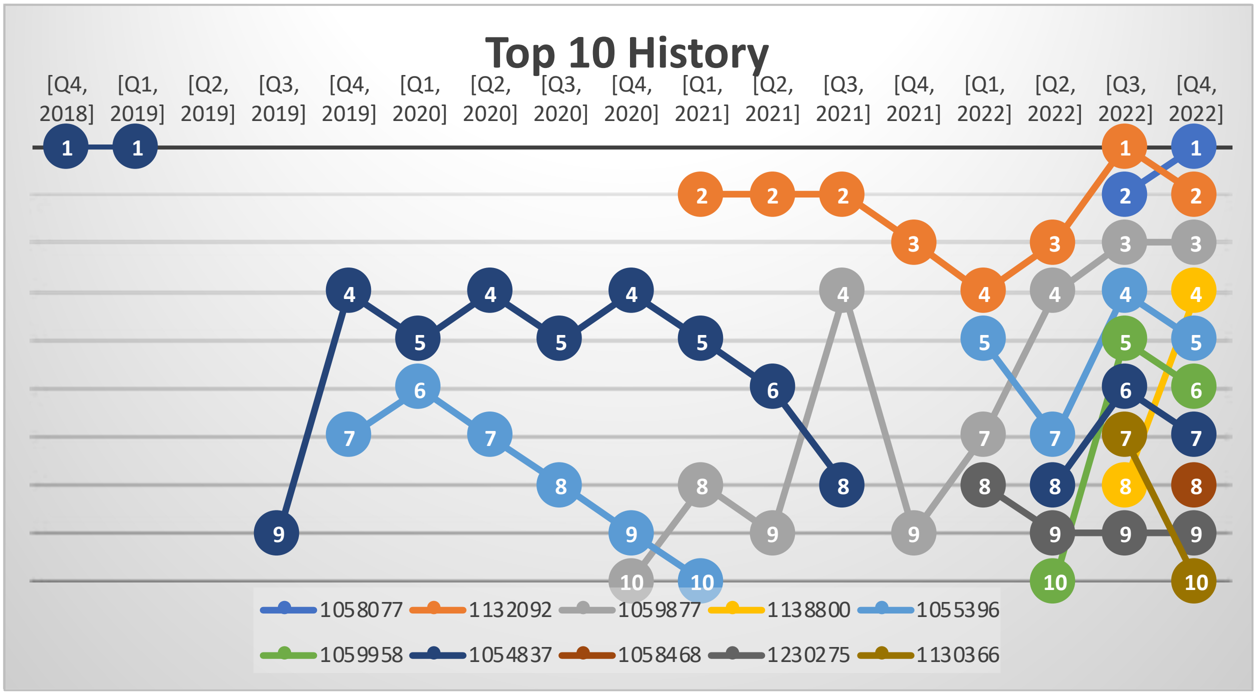


Figure 11: History of Prominent Signatures in the Top 10 since Q4 2018

We include a historical chart of prominent signatures from the top 10 network attacks to give a perspective on the changing (or unchanging) trends. The colors reflect a single signature, and the number within each circle shows the placement in the top 10 during that quarter. You can see signatures such as signature 1059877 in gray works its way up to the third spot in Q2 and hold it again this quarter. One of several CVEs associated with signature 1059877 is a vulnerability in SpecView, a graphical interface for SCADA software used for monitoring and control in different industrial environments. Another signature to spot, 1138800 (the ProxyLogon vulnerability) in yellow, worked its way up from the eighth position last quarter to the fourth this quarter. Overall, many of the signatures that manage to reach the top 10 network attacks tend to last in that position for many years. The position might change by one or two places quarter to quarter. It indicates that attackers will continue to use attacks that they know will work.

The top 3/5/10 signature tally shows how concentrated the traffic is among a few select signatures. We only recently saw, in Q1 2022, that the top 10 signatures consisted of nearly 87% of total detections. The top 5 was almost 80% and the top 3 was just above 65%. Since then, the diversification among all our signatures has continued to expand. Now the top 3 is only 35.7% of total detections. A lot of that is due to some heavily concentrated signatures disappearing from the top 10 list since last quarter, and hence a decrease in total detections as well.

	Top 3	Top 5	Top 10
Hits	823,216	1,057,736	1,456,097
Total Detection %	35.70%	45.87%	63.14%

Figure 12: Top 3/5/10 Total Detection % (From the Top 10 Signatures by Volume)

Most-Widespread Network Attacks

The most-widespread network attacks are the signatures detected against the highest number of unique customer Fireboxes. We highlight the three countries most affected by each signature and also show the level of frequency per region.

Signature 1130592 – 'WEB Apache Struts Wildcard Matching OGNL Code Execution -5')
Associated CVE: CVE-2013-2134

This vulnerability involves the Apache Strut 2 web application framework. Java enterprise web-based applications use Object-Graph Navigation Language (OGNL), which is the technology used in Apache Strut 2. A proof of concept demonstrated that a double evaluation can be used to edit the header, and then in the following request edit the value of the message. We discussed this in more detail in Q2 2022.

The reason for bringing up this signature again is to note that it is the third quarter in a row that this sits at the top of the most-widespread attacks. Attackers cast a wide net since the Apache Strut 2 framework is commonly used. Updating the software to a newer version is the key to staying ahead of a preventable compromise. In addition, signatures 1110932 and 1059877 have been present in the top 5 since Q2 2022. Signature 1132092 has been present since Q1 2021. Whatever vulnerabilities are considered low-hanging fruit can and will be exploited since automation software incentivizes attackers to keep prodding networks. As the effort on the attacker's end is minimal, they take advantage of whatever opportunity presents itself.

Signature 1138800 – 'WEB Microsoft Exchange Server Remote Code Execution Vulnerability -6'
Associated CVE: CVE-2021-26855

This signature is new to the most-widespread attacks, but isn't new to ISR reports. Q3 2022 we discussed signature 1138800, known by the more infamous name ProxyLogon. A table of its progression can be viewed in the top 10 network attacks section. A look at the regions shows an impact between 10.03%-15.77% of affected customers. The numbers are certainly not as widespread as the number one most-widespread signature 1130592, with a 38.26% rate for AMER, but the low teens range is not insignificant. Additionally, when you look at the most impacted countries, customers in Germany and Canada are receiving a large chunk of attempted intrusions via this vulnerability. The ProxyLogon vulnerability is still relatively new compared to some of the other most wide-widespread signatures, so it wouldn't be a surprise to see it rise in the ranks of most-widespread attacks further over the next coming years.

Signature	Name	Top 3 Countries			AMER	EMEA	APAC
1130592	**WEB Apache Struts Wildcard Matching OGNL Code Execution -5**	Brazil 54.7%	France 45.2%	Spain 40.83%	38.26%	30.26%	28.11%
1110932	**FILE Microsoft Windows GDIplus PNG tEXt Chunk Processing Integer Overflow**	Brazil 27.07%	UK 26.13%	France 23.84%	13.76%	23.42%	15.66%
1059877	**WEB Directory Traversal -8**	Germany 29.78%	Italy 17.32%	Canada 16.11%	14.77%	19.25%	16.87%
1138800	**WEB Microsoft Exchange Server Remote Code Execution Vulnerability -6**	Germany 25.43%	Canada 21.48%	Australia 13.91%	10.03%	15.77%	11.65%
1132092	**FILE Invalid XML Version -2**	Italy 24.46%	Australia 23.48%	UK 18.15%	12.83%	13.14%	17.67%

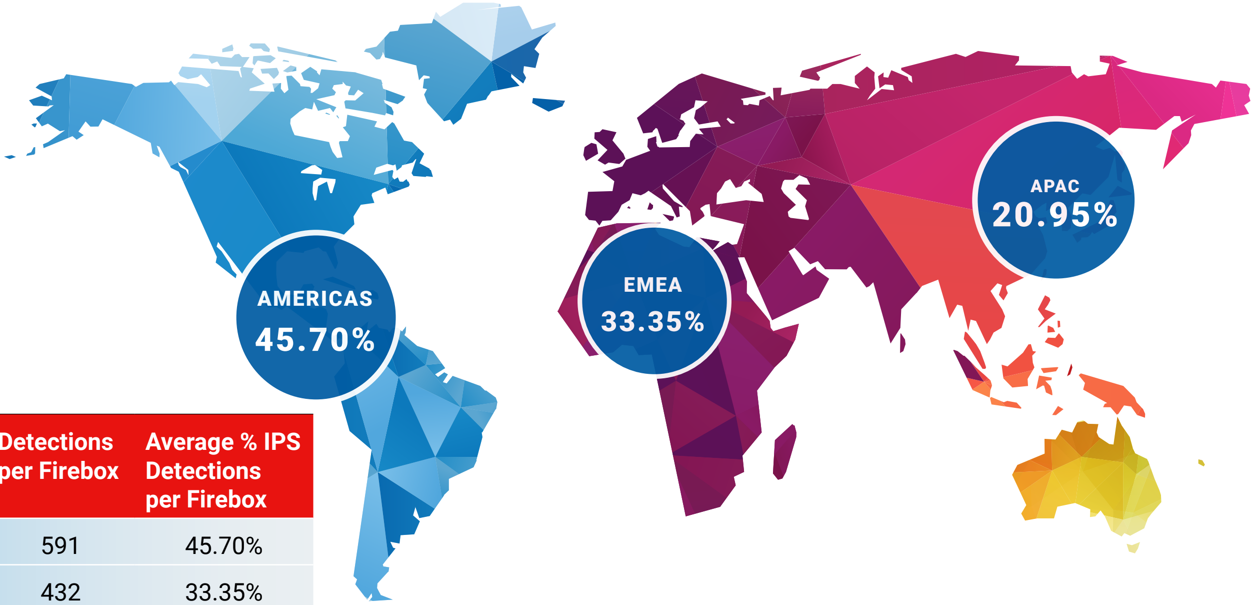
Figure 13: Top 5 Most-Widespread Network Attacks

Until this quarter, it felt "assumed" that the US would be among the countries in green in Figure 14 (probably not a surprising mindset for an American, such as the one writing this). Since forming a chart in Q1 2020 (Q3 2020 and prior quarters not included), to track the top 3 affected countries per most-widespread signatures, the US has consistently been among them. In fact, usually placed among several of the top widespread signatures. Brazil and Canada are the only countries to have been absent once since Q1 2020. It would be too simple to guess that the attackers are diversifying their efforts to countries beyond the US. As we can see, western countries still dominate the landscape. Perhaps the US was only 1% or less away from making it into the top three countries among one of the signatures. Wealthy countries with widely spoken languages are still the most common attack targets among our customer base. Having said all that, we do also know these results may be partially skewed by the regions and countries WatchGuard does the most business in (which often tend toward the wealthier ones). There are certain areas of the world that US-based companies are restricted from doing business in, so we have no real visibility in those countries.

	Canada	USA	Spain	Brazil	Germany	UK	Italy	Australia	France	Switzerland
Q4 2020	🟦	🟦	🟦	🟦	🟦	🟦	🟥	🟥	🟥	🟥
Q1 2021	🟦	🟦	🟦	🟦	🟥	🟦	🟦	🟥	🟥	🟥
Q2 2021	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟥	🟦	🟦
Q3 2021	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
Q4 2021	🟦	🟦	🟦	🟦	🟥	🟦	🟦	🟥	🟦	🟦
Q1 2022	🟦	🟦	🟥	🟦	🟦	🟥	🟦	🟦	🟥	🟦
Q2 2022	🟦	🟦	🟥	🟦	🟦	🟦	🟦	🟦	🟦	🟥
Q3 2022	🟥	🟦	🟥	🟦	🟦	🟦	🟦	🟦	🟦	🟥
Q4 2022	🟦	🟥	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟥

Figure 14: Countries Listed Among One or More Widespread Attack Signatures Who Were Most Affected

Network Attacks by Region



Region	Detections per Firebox	Average % IPS Detections per Firebox
AMER	591	45.70%
EMEA	432	33.35%
APAC	271	20.95%

The average detections per Firebox show the proportional weighting of detections between AMER, EMEA, and APAC. The percentage increased by 6%-7% points for AMER and EMEA, while APAC decreased from 34.67% last quarter to 20.95% now. This metric is often difficult to attribute to a cause. While we can sometimes see patterns in the types of signatures showing up in the top 10 network attacks, trying to give a reason behind a decrease in detections by region is hard without additional data. Occasionally, AMER is the dominant region, and in other quarters it may be EMEA or APAC. It may have to do with how holiday calendars line up in each region, therefore generating less traffic in certain regions, such as in Europe, when many take holidays during the same month. Another reason could simply be a change in which customers share telemetry quarter-to-quarter.

Conclusion

The IPS section often runs into several common themes. One is that old vulnerabilities can be as useful to attackers as new ones, if they achieve the goal of a compromise. Another common theme is that many of the top signatures are attackers going for the jugular, trying to compromise Microsoft Exchange Servers or management systems, considered core assets of any organization. Just as an attacker sets their sights on the big prize, so should organizations in knowing where to put their efforts into defending. It's important to consider other assets in the organization as well. An asset security scanner may list thousands of vulnerabilities among your devices and services. The ones with the highest score can and should get attention first. But to put off the other issues for an indefinite time may come back to haunt you. Meanwhile, use our Intrusion Prevention Service to mitigate your risk to any exploits during your vulnerability window.

DNS Analysis

Q4 2022 saw a decrease in malicious domain activity compared to Q3, with blocked connections dropping to 3,892,570, which is a 34% decline. This was fewer connections overall compared to the previous two quarters. While some of this reduction could be users paying more attention to what they click, we believe it's mostly due to our threat teams updating a few of our malicious domain lists, which were starting to age or become obsolete. Sometimes pruning what's older is necessary to keep products like DNSWatch effective. Regardless of the slight drop in Q4, DNS-based firewalling is an important layer of security that should be observed and maintained to prevent threats and attackers before they can even attempt connections to dangerous domains.

In the following section, we review the top domains in malware, phishing, and compromised websites from Q4.

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

Top Malware Domains

We classify malware domains as ones that host malware distribution sites, infrastructure, or the command and control (C2) network needed for threat actors to manage the malware threats. This quarter, there were a few new additions to the top malware domains list.

greenwidow[.]top
This is a unique domain to report on, at least as this classification. We talked about this domain in another 2022 Internet Security Report, but we originally classified it as a phishing domain. However, some changes have happened on the domain to reclassify this as a malware domain. The domain is hosting a C2 server for malware that is normally delivered via malspam emails. When the user opens the link or file this domain is calling home for instructions on what to do next.

Skyprobar[.]info
In 2022, Emotet saw a strange break in its operation through most of the Northern Hemisphere's summer months, but then in November 2022 Emotet came back. With spamming of malicious emails, Excel files or Word documents, many of the previously malicious sites like Skyprobar[.]info returned to provide commands.

Malware

Domain	Hits
greenwidow[.]top	283,916 *
img1[.]wsimg[.]com	13,292
toknowall[.]com 6075	6,075
xrass[.]com	3,546
xmr-eu1[.]nanopool[.]org	3,204
xmr-eu2[.]nanopool[.]org	3,194
xmr-asia1[.]nanopool[.]org	2,644
skyprobar[.]info *	2,560
pixel-install[.]me	2,250
js.softdl[.]360tpcdn[.]com	1,305

* Denotes the domain has never been in the top 10

Top Compromised Domains

Compromised domains typically host legitimate content but have suffered some sort of breach or attack (often due to a web application vulnerability) that allowed threat actors to add malicious content to them or host other sorts of undesirable content. We block these domains and classify them as dangerous while they host that content but switch them back to legitimate once their owners have cleaned the malicious content. Below is an example of interest from top compromised domains during the quarter.

www[.]granerx[.]com
Traditionally websites like granerx are labeled as Health and Wellness, but this domain is an administrative domain that is not set up or configured correctly. When domains are not configured correctly, they can be attacked without difficulty, and data can be easily lost. This domain is compromised because we have seen vulnerabilities used for malicious actions in the past on this WordPress domain.

Top Phishing Domains

As the name suggests, phishing domains are ones masquerading as some legitimate destination, typically to trick users into sharing credentials and other personal and sensitive information.

inx[.]lv
Many URL shorteners are used for hiding and masking the true domains that house phishing content. inx[.]lv is no exception to this goal. While URL shorteners do not traditionally make our list since there is an abundance of them, this one has been flagged by a few of our partners who help provide data to the listing. The specific domain and URL one had been redirecting to an employee benefits website phishing campaign.

www[.]customer-portal[.]info
This domain has hosted multiple phishing campaigns. These campaigns have been seen to change often to attempt to gain user trust. These range from fictional voicemail messages, fake business proposals, and more recently OneDrive sign-ins. This domain is blocked since the exact contact on any given day is unknown.

Conclusion

Even with an update to aging domains and lists, it is easy to see that attacks on unsuspecting users are still high. The process with which users see attacks through email does not change often, but with early indicators showing up, older malware and phishing attacks are making a comeback. Keeping DNS protection enabled is one of the best ways to keep malware or phishing out of vulnerable users' grasp.

Compromised

Domain	Hits
t[.]co	453,680
archive[.]org	1,183
ssp[.]adriver[.]ru	825
facebook[.]apps[.]fiftyfive[.]co	745
www[.]sharebutton[.]co	469
0[.]nextyourcontent[.]com	338
d[.]zaix[.]ru	275
track[.]dobermanmedia[.]com	80
www[.]granerx[.]com	55 *
dinatds[.]com	42

* Denotes the domain has never been in the top 10

Phishing

Domain	Hits
unitednations-my[.]sharepoint[.]com	67,958
firebasestorage[.]googleapis[.]com	40,205
inx[.]lv	3,858 *
e[.]targito[.]com	2,892
nucor-my[.]sharepoint[.]com	2,067
gm7e[.]com	1,728
t[.]go[.]rac[.]co[.]uk	1,557
data[.]over-blog-kiwi[.]com	1,412
edusoantwerpen-my[.]sharepoint[.]com	687
www[.]customer-portal[.]info	666

* Denotes the domain has never been in the top 10

Firebox Feed: Defense Learnings

Like water that flows in the path of least resistance malware will flow through whatever network has a hole in it. We have many ways to plug these gaps. Network perimeter defenses can dam up the malware, protecting the internal network from the chaotic Internet. And if any slips through, endpoint defense (the next section) helps too. Here are a few ways to protect your network from the key threats we saw in our Firebox Feed this quarter.

1

Machine-learning malware detection at the perimeter

Machine learning advances in recent years provide much needed defenses to your network perimeter through malware detection. Like the ChatGPT tool you hear about in the news, the Firebox's IntelligentAV (IAV) service uses machine learning to more immediately recognize new malware as bad, without waiting for inputs from human researchers. Sure, GPT-3 and 4 does a lot more than one thing, and also uses neural networks, but at the highest level IAV's machine learning can more proactively automate new malware detection.

We know that a ton of malware bypasses basic, signature-based malware protections, which is why you need additional proactive malware detection services, like IAV, to pick up the slack. The quick response provided by IAV blocks malware at the network perimeter immediately, allowing users to continue working without delay.

Maybe once chat GPT-7 comes out we will rely on it to protect our networks. (Well, hopefully not.) Until then we recommend a layered defense that includes the use of machine learning for malware detection.

2

Don't miss malware hidden in plain sight

If most traffic on the Internet travels over an encrypted connection, then it makes sense that most malware comes from encrypted connections. Not only does this make it easy for malware to hide amongst normal traffic, but since many network administrators don't inspect encrypted traffic, it offers malware a hole with which to bypass perimeter defenses. Malware creators know this and take advantage of it regularly.

With 93% of malware detected on an encrypted connection and only 7% unencrypted, if you don't inspect this traffic, you will miss most malware. Host-based detection may catch some of this malware, but to rely on just one program to protect yourself doesn't make sense. Also, many networks contain IoT devices such as printers, climate controls, and security cameras that can't install endpoint malware protections. We often hear the workload of distributing certificates is the biggest hurdle the prevents administrators from setting up the Firebox's free TLS decryption feature. While this can take some time, we do offer easier methods, including importing a corporate root certificate to the Firebox itself. Even if you prefer to distribute certificates to clients, you can start with the most critical areas of your network first. The best practices of decrypting and security scanning encrypted web traffic will save you more time in the long run.

3

Communication is key among medium to large organizations

Security within an organization isn't a one and done activity. It requires reevaluating policies and keeping open lines of communication between different teams. That is why reoccurring meetings can be incredibly useful (if not done too often). This involves collaboration between the security team and IT, but it can also mean pulling other teams from the organization into the mix. Each team and their engineers are focusing on different sprints or work objectives, and a focus on security can easily find its way into the "deal with later" category. For organizations large enough to have separate IT and security teams, reoccurring meetings are a necessary forum for regular communication. There's an array of security and policy topics that requires consistent open dialogue, such as the latest published vulnerabilities, addressing the queue of alerts from vulnerability scanners, alerts from Fireboxes, new phishing campaigning reaching your employees, and user access policies. All of these may have different product owners, but that owner needs not operate in a silo. A habit of sharing news and questions between different teams is important. It ensures that the organization is actively engaged and resilient to new threats as they come. Remember, communication is as important to your defense as the technical security controls you implement.

Endpoint Threat Trends

WatchGuard

Endpoint Threat Trends

Each quarter the WatchGuard Threat Lab logs and ingests telemetry data from endpoints that use our WatchGuard Endpoint Protection, Detection, and Response (EPDR) and Adaptive Defense 360 (AD360) products. Because this quarter also constitutes the end of the year, this section will cover the quarter-over-quarter (QoQ) and year-over-year (YoY) data. This allows us to show microtrends from each quarter and how threat actors leverage resources within a victim's operating system over long periods. For example, we consistently detect high concentrations of malware using PowerShell, and thus, decision-makers should monitor for abnormal commands from PowerShell processes. Another example has been the emergence of cryptominers over the last few years. However, cryptominers have recently declined in detection frequency because analysts and antivirus signatures classify these as information stealers instead of just cryptominers. Those are just some of the patterns we can detect by observing this anonymous endpoint telemetry data.

This quarter we continue to track ransomware and extortion groups external to our EPDR and AD360 services. Providing data on the groups responsible for many of these ransomware attacks adds much-needed context to the overall ransomware threat landscape. You can also expect to see data on malware frequency, attack vectors that threat actors use, browser-based detections, and cryptominers. Although, based on a sharp decrease in cryptominer detections, this will be the last quarter these are tracked. As usual, we will begin this section with the overall detections for Q4.

Malware Frequency

The Malware Frequency section is probably the easiest to understand; it's simply a sum of all detections from each quarter. A detection, hit, alert, or whatever synonym you prefer occurs when a file or process performs a flagged activity against EPDR or AD360 rulesets. The engine then categorizes the file as a potentially unwanted program (PUP) or malware (MW). Finally, the software gives the file a signature based on the known malware family or behavior, resulting in a signature that looks like "PUP/Adware." This means the file could be potentially unwanted by the user because it contains adware.

The final quarter for 2022 showed an increase in detections from the quarter prior. Q3 saw the lowest number of detections for the year at 60,076; in Q4, there were 73,058 detections, a roughly 22% increase QoQ. This sharp increase also reverses a three-quarter decline, beginning in Q1 of this year. Based on 2022's relatively low number of detections, we anticipate this trend to remain steady or increase going into 2023.

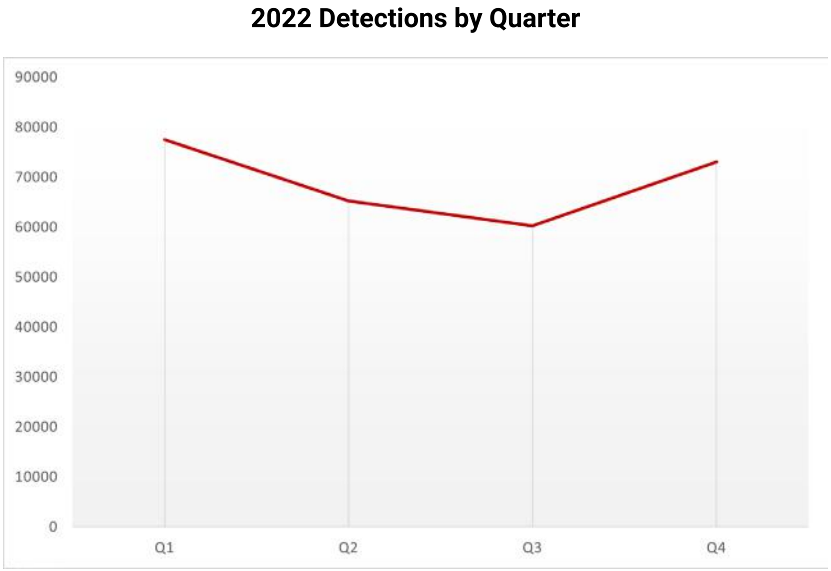


Figure 15: 2022 Total Detections by Quarter

2022 Total Detections by Month

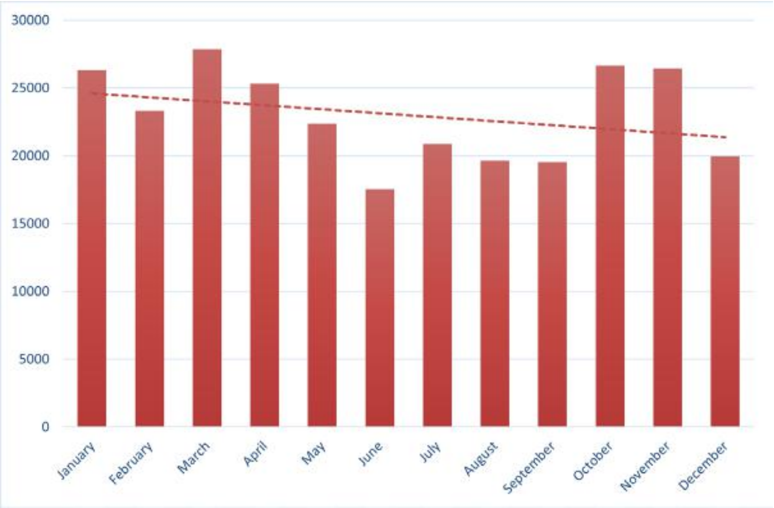


Figure 16: 2022 Total Detections by Month

Note: y = -294.33x + 24904; R2 = 0.0935

As was stated, we observed historically low detections this year since we began tracking this data in 2018. For example, April 2020 saw more detections than Q2 and Q3 of this year. As you can see in the figure below, there was an abnormally low number of detections in the summer months, which is usually the case, but combined with an already slow year the numbers were more pronounced.

Malware Origin

Of the overall detections discussed prior, we break these downs into attack vectors. We define attack vectors by the file or process activity that invokes the detection. For example, if EPDR or AD360 flags excel.exe, we determine that the attacker was leveraging Microsoft-based Office software for their attack. Therefore, that detection would classify as a "Office" attack vector. We group all detected malware into their appropriate attack vectors, which dynamically change every quarter. The usual attack vectors from each quarter are Adobe Acrobat, Browsers, Nvidia, Office, Other, Scripts, and Windows. More information about each attack vector is below.

Attack Vector Definitions

Acrobat – Adobe Acrobat is a suite of software services provided by Adobe, Inc. primarily used to manage and edit PDF files. PDF files' ubiquity and ability to bypass email and file transfer filters make Acrobat services ripe for malicious use.

Browsers – Internet browsers are familiar products for all modern-day computer users that allow access to the World Wide Web (WWW). Common browsers include Chrome, Firefox, Safari, and Edge, among many others. Current browsers store personal information – if you allow them – including passwords, cookies, cryptocurrency private keys, and even stored credit cards, making them common targets for information-stealing malware.

Nvidia – Nvidia is a corporation that designs and manufactures processing units, artificial intelligence systems, and other high-performance hardware and software. They are primarily known for their retail video cards used for gaming, visual design, and cryptomining. Malicious cryptomining utilizes the victim's video card, or processor, to mine cryptocurrency on the attackers' behalf without the user ever knowing.

Office – The Office attack vector is the sum of all detections derived from Microsoft Office documents and executables. This includes Word, Excel, PowerPoint, Outlook, and Office Suite executables. Not only is Microsoft Office one of the most popular business-related suites of tools, but the features of the software, such as macro-enablement, allow for an increased attack surface.

Other – The Other attack vector is everything else. Detections within this category are those that didn't fit any other category. This includes AutoKMS tools, Remote Services, and third-party applications, among many others that change every quarter.

Scripts – Scripts, which always invoke the most detections each quarter, are those files derived from a scripting programming language. Malware utilizes PowerShell, Python, Bash, and AutoIT scripts to download other malware and deliver payloads, among many other things. Considering Windows is the most commonly attacked operating system, it is no wonder PowerShell continues to skew the results for Windows detections.

Windows – Under the hood, Windows-based attack vectors house the most data points of any attack vector. It contains the most detections but not in the highest quantities. The files included under the Windows name are those that ship with the Windows operating system. Examples include explorer.exe, msiexec.exe, rundll32.exe, and notepad.exe. Trojans commonly impersonate these files or inject malicious code into them because they exist on every Windows machine out of the box and are inherently trusted.

Attack Vector Detections

The overall detections for Q4 were greater than Q3 primarily because of Scripts, as usual. Wherever Scripts goes, so does that data. If Script detections are higher than average, the overall detections are higher too, and vice versa. Also, to no surprise, PowerShell is responsible for increased Script detections. This quarter Scripts constituted 90% of all detections. Windows came in at a distant second at 5%. Browsers comprised 2% of all detections, and Acrobat, Nvidia, and Office combined for 1% of all detections each. Finally, the Other category was less than 1% of all detections. See the figure below for a graphical representation of this data.

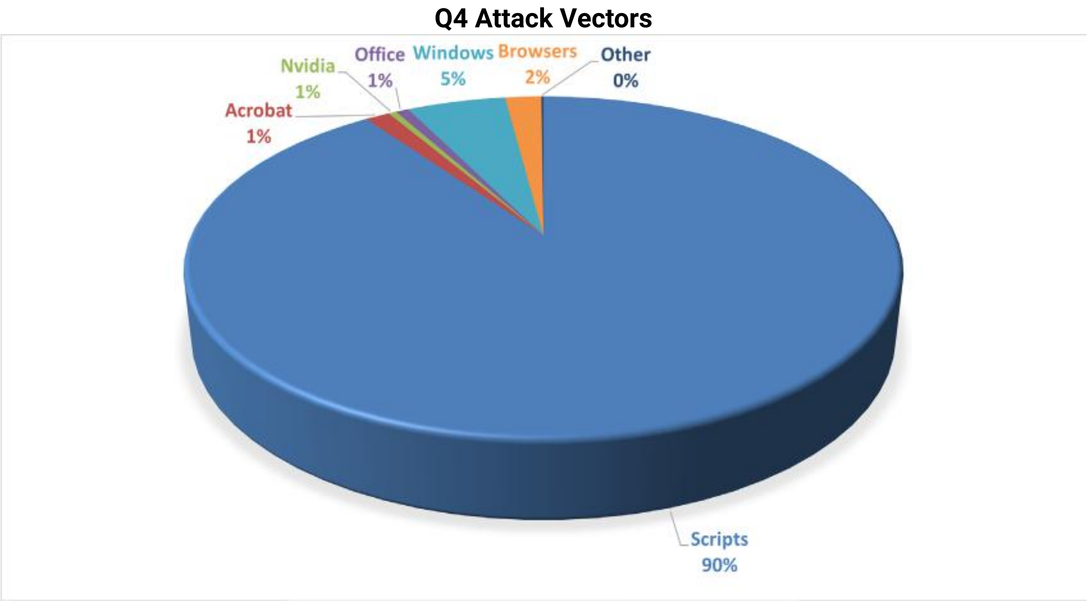


Figure 17: Q4 Attack Vectors

Since Scripts take up all of the data, it's challenging to understand the other attack vectors. As such, we created an additional pie graph with the Scripts attack vector omitted. With this omission, Windows was the attack vector of choice for threat actors. Then Browsers were second at 20%. Followed by Acrobat at 14%, Office at 7%, and Nvidia at 4%. The Other attack vector finally gets on the board with 1%, showcasing how few detections fit this category. See Figure 18: "Q3 Attack Vectors, Scripts Detections Removed" for more information.

Q4 Attack Vectors, Script Detections Removed

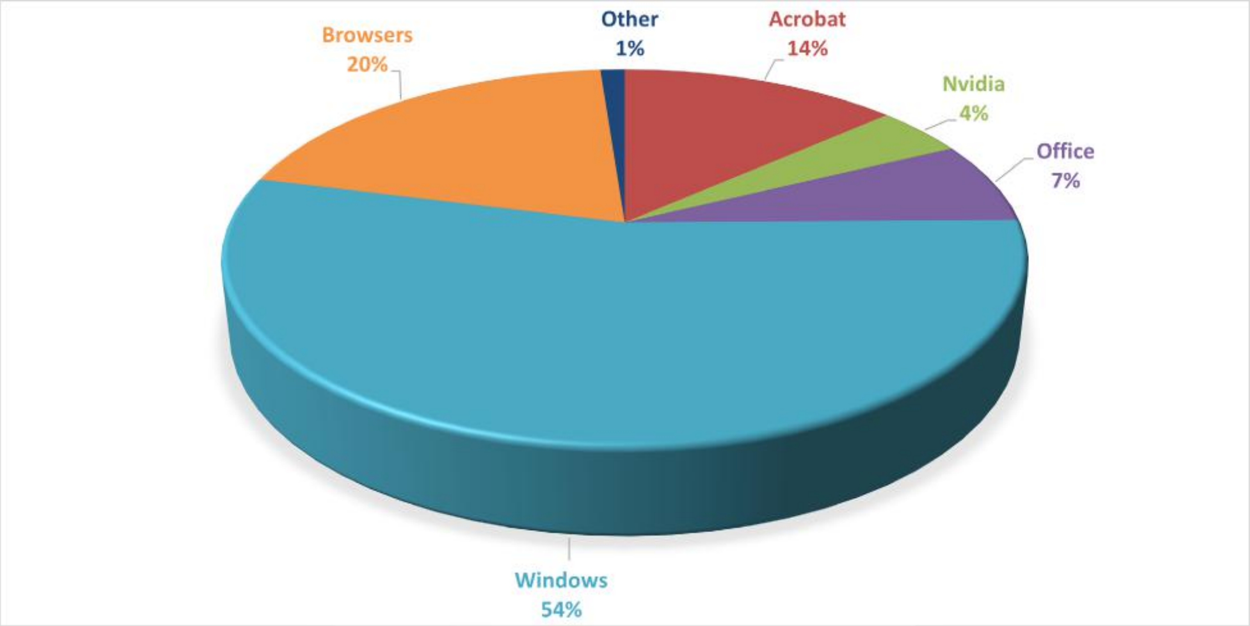


Figure 18: Q4 Attack Vectors, Script Detections Removed

2022 Attack Vectors by Quarter

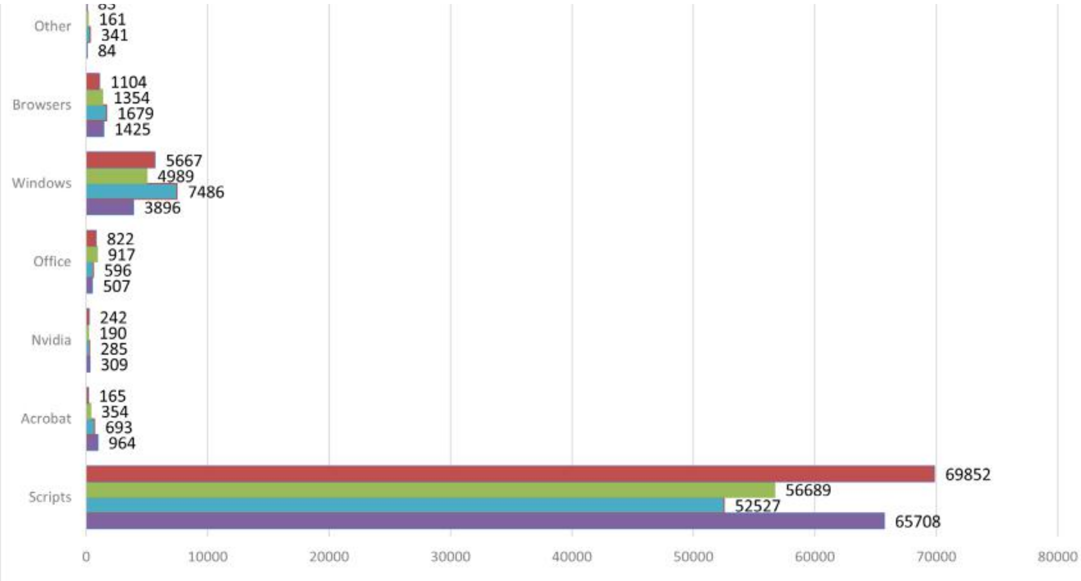


Figure 19: 2022 Attack Vectors by Quarter

Browser Malware Detections

Each quarter we extract the browser-based detections to understand better which browsers threat actors target. The usual suspects include Chrome, Firefox, Internet Explorer (IE), and Edge. However, we occasionally see detections from other not-as-well-known browsers such as Brave and Opera. Since Edge, Opera, and Brave have lower detections than the other browsers, we bundle them together. However, this quarter, there were no Brave or Opera detections; thus, the other four browsers are the only browsers tracked in Q4.

It was close between Firefox and IE for the largest percentage of detections, but Internet Explorer had the most with 42%, followed by Firefox with 38%. Chrome was leveraged by threat actors 19% of the time. Finally, 1% of the detections were from Edge. These numbers reflect Q3 almost precisely.

Q4 Browser Malware Detections

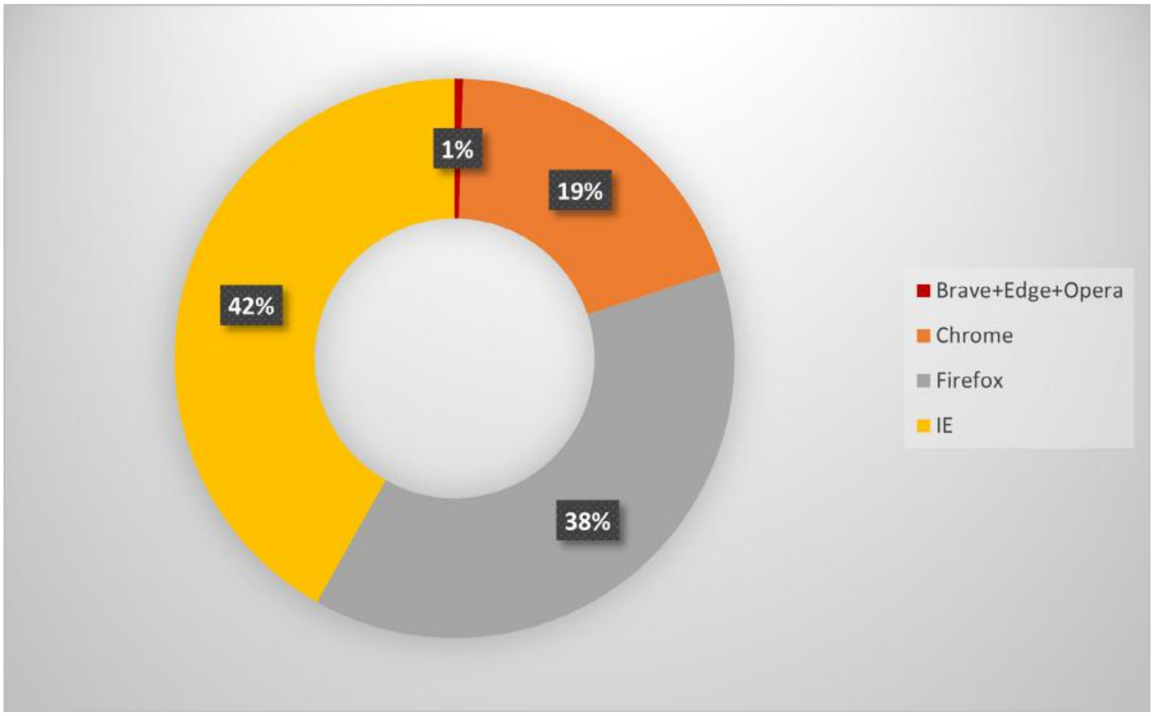


Figure 20: Q4 Browser Malware Detections

Mozilla Detections

We recently began to track Mozilla-based detections because of a sudden spike in threat actors leveraging their services. This includes Firefox discussed above, but it also includes their email client, Thunderbird, and their telemetry service, Ping Sender. These detections for Q4 were slightly lower than Q3, but on the whole they were steady. Overall, Mozilla detections were down a modest 9%. You can observe the QoQ for Mozilla detections below.

2022 Mozilla Detections by Quarter

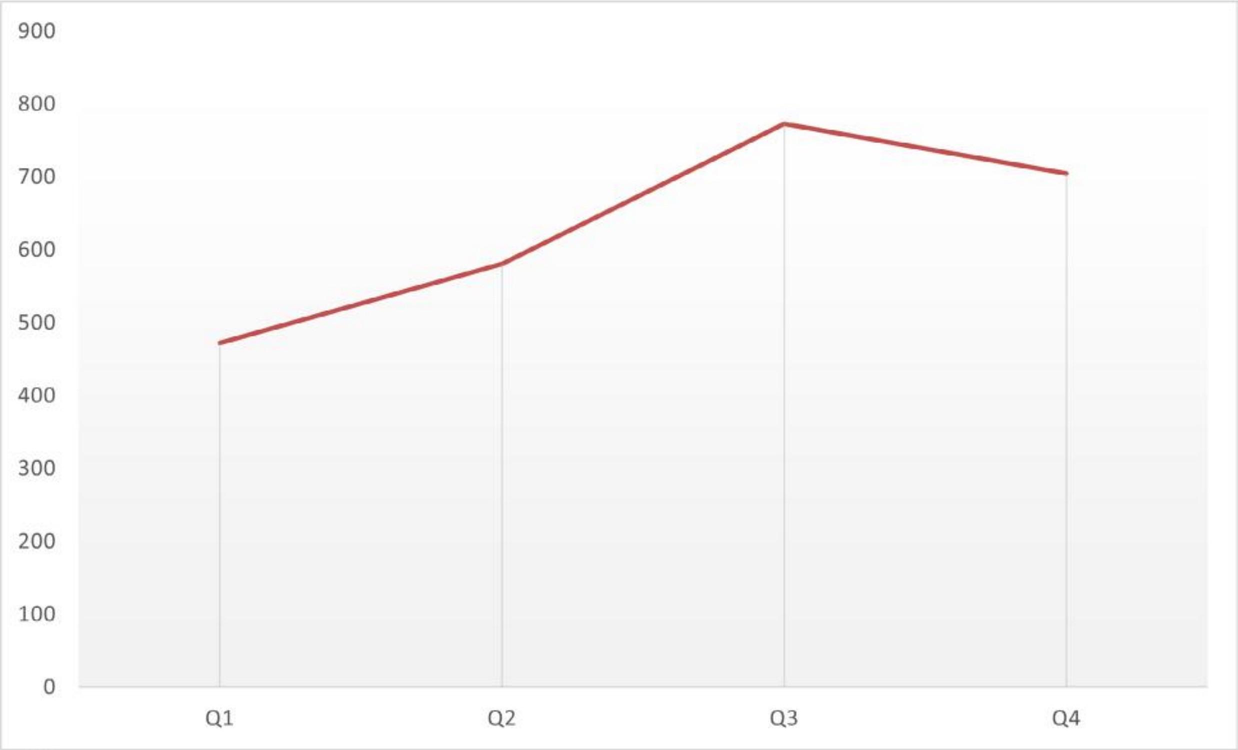


Figure 21: 2022 Mozilla Detections by Quarter

Cryptominers

This will be the very last cryptominers subsection, and that's because there's always very little to talk about with them, and the overall cryptominer detections continuously decrease QoQ and YoY. QoQ, there was an 11% reduction in detections for cryptominers. YoY, cryptominers decreased more rapidly at a 13% reduction. The reason for the consistent decline in detections is simple – analysts usually classify cryptominers as information or password stealers. Most malware with cryptomining capabilities doesn't just drop a cryptominer. Instead, they steal crypto wallets, passwords, files, and other items depending on the malware family, and deploy a cryptominer.

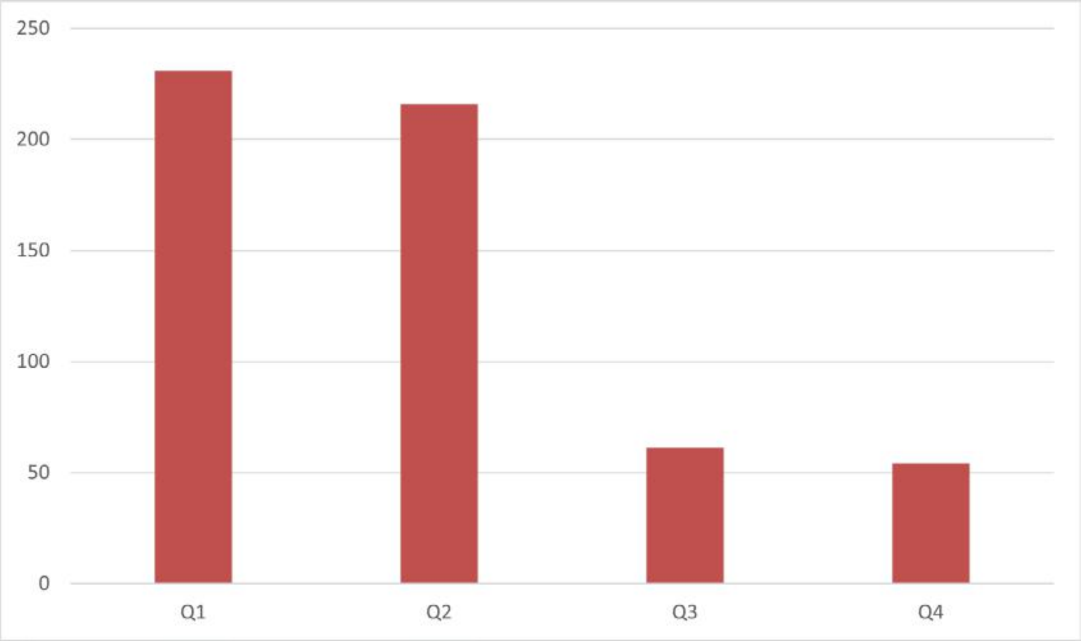


Figure 22: Cryptominer Detections by Quarter

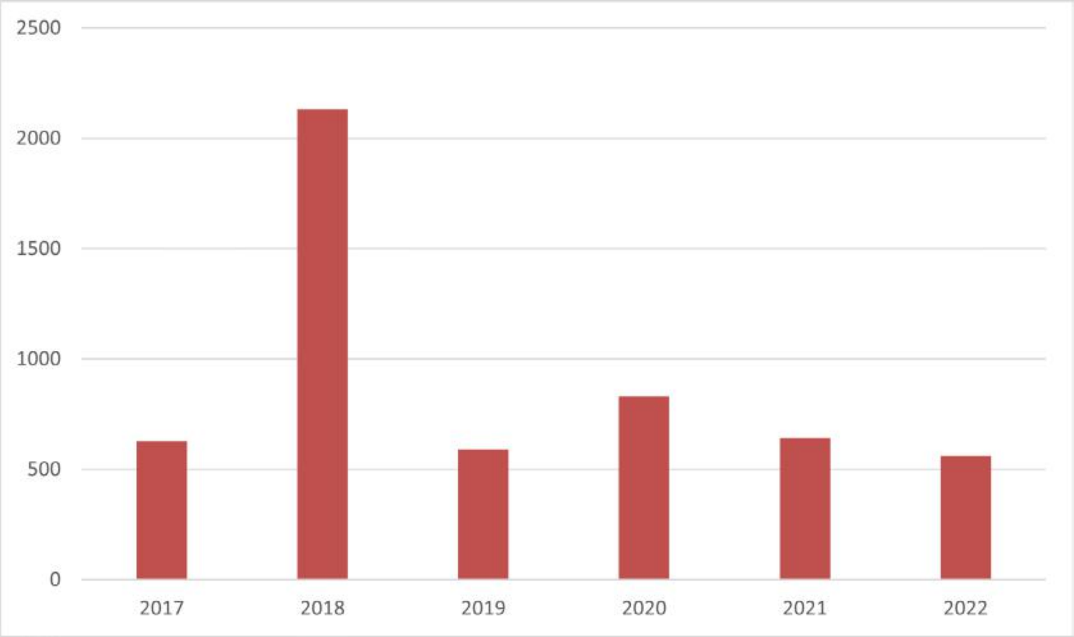


Figure 23: Cryptominer Detections Year-Over-Year

Ransomware Landscape

From our data, ransomware was the grouping that showed the most drastic changes. Q1 of 2022 saw a record number of detections from our sources. That quarter's detections almost doubled the annual ransomware detections in 2021. That number never stumbled, consistently showing many hits throughout the year. Q2 saw a relatively sharp decrease from Q1 but still was high relative to years and quarters prior. The numbers continued to climb into Q3 and increased from Q3 to Q4 as well. To be exact, Q1 to Q2 showed a 39 decrease in detections, but then the trend reversed, rising by 16% from Q2 to Q3 and another 14% from Q3 to Q4. 2022 was a record year of ransomware detections for WatchGuard. The second closest year was 2018, which was 41% less than in 2022, and detections for 2022 were 627% higher than in 2021. An over six-fold increase! You can observe those trends in the two figures below.

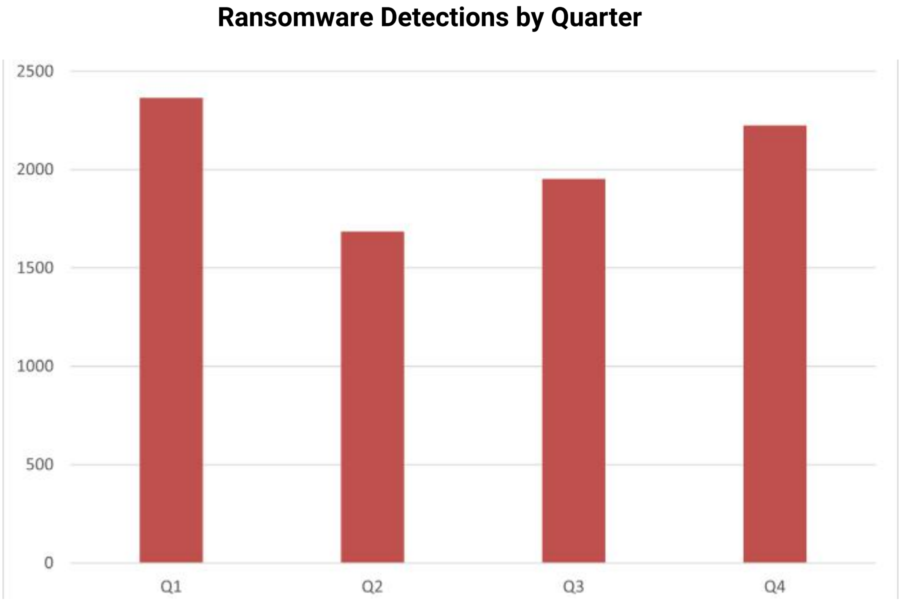


Figure 24: Ransomware Detections by Quarter

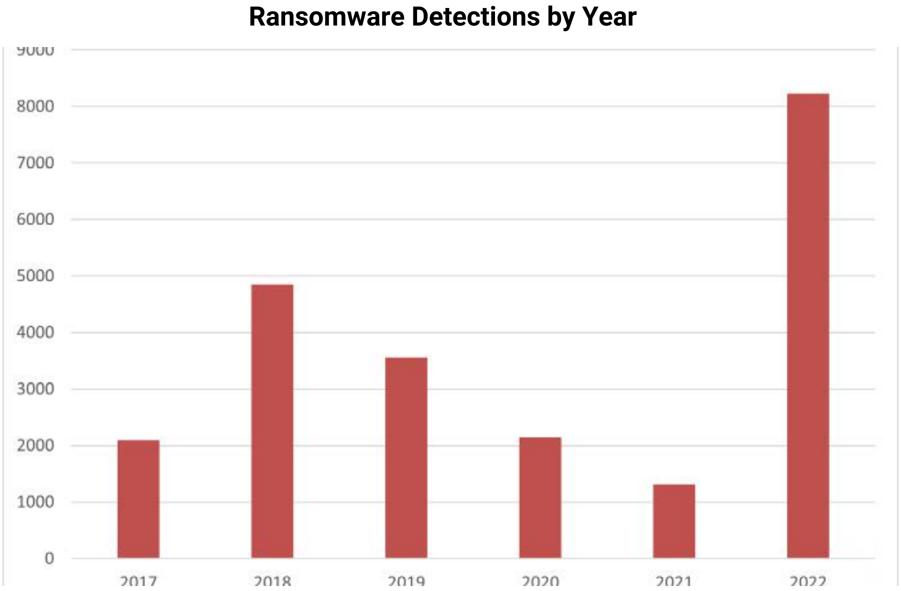


Figure 25: Ransomware Detections by Year

Extortion Groups

The following two sections do not include data derived from the anonymous EPDR and AD360 data. Instead, the WatchGuard Threat Lab collects data from the dark web and other open-source intelligence (OSINT) sources to better understand the ransomware threat landscape. The current data we collect is about active ransomware and data broker extortion groups, and any other newly discovered ransomware groups.

In a surprise to no one, LockBit again had the most public extortion victims, with 149 tracked by the WatchGuard Threat Lab. Although last quarter they had 200, reducing their pace of public extortions in Q4. This does not mean that LockBit and its affiliates reduced their number of attacks. It just means fewer victims didn't pay and were thus publically extorted by LockBit. Do not take public extortions as the total number of victims; this is incorrect. The other top 5 extortion groups, in order, include BlackCat (ALPHV) with 80, Royal with 74, Bian Lian with 56, and Black Basta with 53.

There were several groups with extortions last quarter that didn't have any at all this quarter. Those ransomware groups are:

- 0mega
- Cheers
- Donut Leaks
- IceFire
- Lilith
- Red Alert
- Sparta Group
- STORMOUS
- Yanluowang

We assume many of these groups are no more, including Yanluowang, who had their chat logs leaked, revealing that they weren't a Chinese group as assumed. Rather, they were Russian-speaking operatives, sometimes coordinating with a HelloKitty ransomware operator. We've already observed the re-emergence of 0mega, IceFire, and STORMOUS following Q4, so we will let you know what happens with them next quarter.

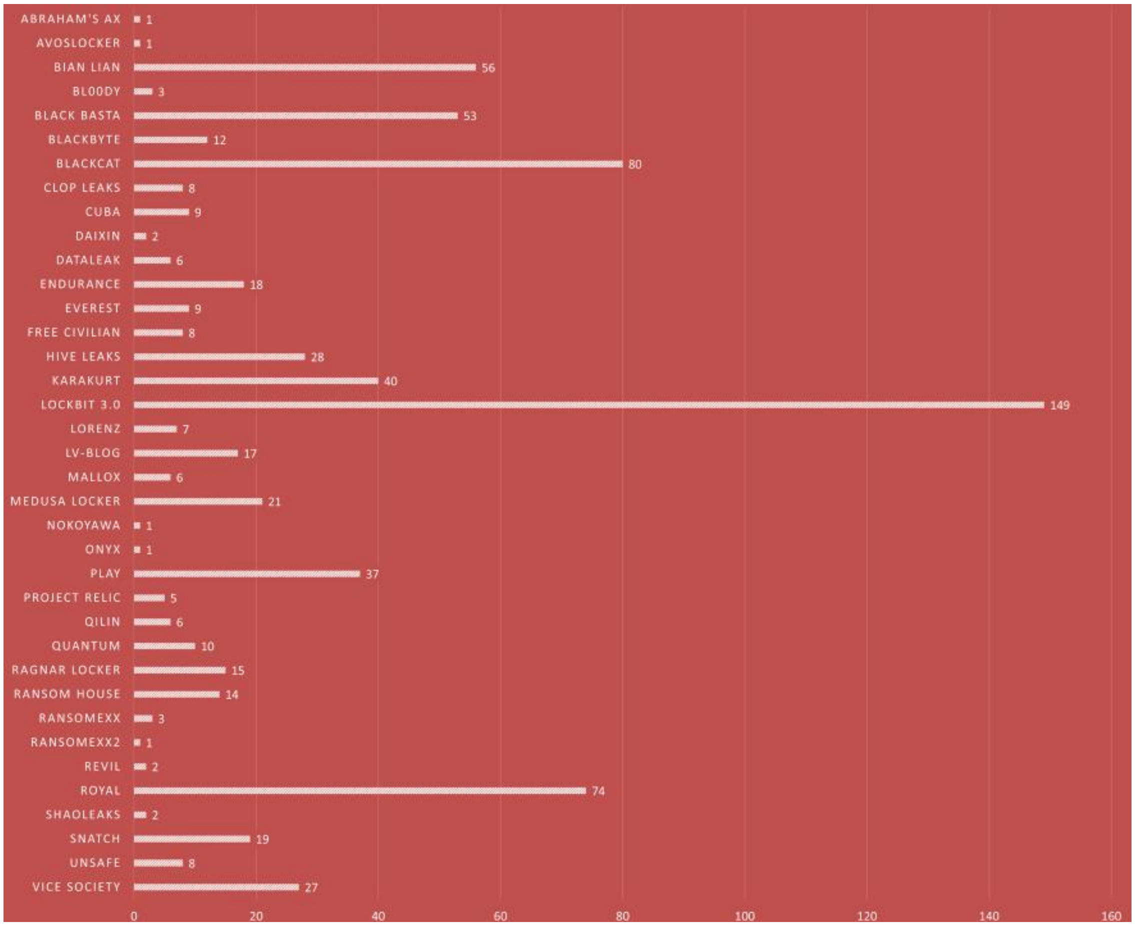


Figure 26: Extortion Groups

New Ransomware

Rounding out the endpoint section, we finish with the new ransomware and extortion groups we discovered in Q4. We detected a whopping 31 new groups. Two of these, Alice and OctoCrypt, are considered ransomware builders and can create custom payloads for users. Three of these are data brokers, or data leakers who aren't known to deploy ransomware. Those entities are DataLeak, ShaoLeaks, and UnSafe. Five of these groups are pseudo-ransomware wipers that masquerade as ransomware but destroy the system. This action usually happens in two manners – not providing a payment method or not sending decryption keys when payment is received, or the malware irreversibly encrypts files or the system. Three wipers come from the conflict in Ukraine – Azov, CryWiper, and Somnia. Reports of QuiDDoSS came out of Saudi Arabia, and VIIPlusLoader is another wiper, not ransomware. The rest of those not mentioned are all ransomware of some sort.

Some notable names we are watching from this list are Endurance, Mallox, Nokoyawa, Play, PolyVice, Project Relic, Qilin, RansomExx2, and Royal. PolyVice and RansomExx2 are updates of previous versions from the Vice Society and RansomExx groups, respectively. Endurance, Mallox, Nokoyawa, Play, Project Relic, Qilin, and Royal are all currently extorting victims. So, you will definitely see them next quarter. With that, we will also see you next quarter!

Ransomware Name
Abraham's Ax
Alice
Anon_by (Anon)
AXLocker
Azov
BlackHuntr
Black Magic
CIA
CryWiper
Dark Angels
Endurance
Mallox
Nokoyawa
OBZ (ObzCrypt)
OctoCrypt Go
Play
PolyVice
Prestige
Project Relic
Qilin
QuiDDoss
RansomExx2
RedKrypt
Royal
Shaoleaks
Somnia
Sullivan
Unsafe
Venus
VIIPlusLoader

Figure 27: Q4 Newly Discovered Ransomware

Top Security Incident

Top Security Incident

LastPass Breach

Most cybersecurity professionals are strong advocates for password managers. It is simply impossible for users to remember strong and unique passwords for every service they use on their own, which means without the aid of a password manager they can fall into poor password practices like reuse. While most reputable password manager providers are significantly more secure than attempting a "roll your own" management solution, that doesn't mean they are completely immune to cyberattacks. This fact was proven for the popular password manager LastPass when they suffered what was ultimately a catastrophic breach that occurred over the course of several months leading into the start of Q4 2022.

LastPass were quick to notify their users about the security incident, matching the precedent they had maintained for years about proactive transparency, but the full details of just what was compromised didn't begin to come out until December of 2022. When those details came to light, it became clear that this breach posed an existential risk to the company as the threat actor had managed to exfiltrate everything from source code to user password vaults and other secret material from Cloud backups at the organization. While you can't ignore the seriousness of the incident, the details LastPass ultimately provided can help any organization learn exactly how a simple mistake can lead to massive consequences.

Initial Access

In a recent update to their breach announcement, LastPass disclosed the threat actor obtained stolen credentials through a vulnerability in third-party media software installed at a senior DevOps engineer's home. This vulnerability allowed the threat actor to install a keylogger that ultimately captured the engineer's password when they logged into a special LastPass corporate vault, which they were one of only four in the company with access to.

With access to the DevOps password vault, the threat actor had access to shared credentials for LastPass's AWS S3 Cloud storage environment where encrypted password vault backups were located. Additionally, they had access to the keys required to decrypt the backups.

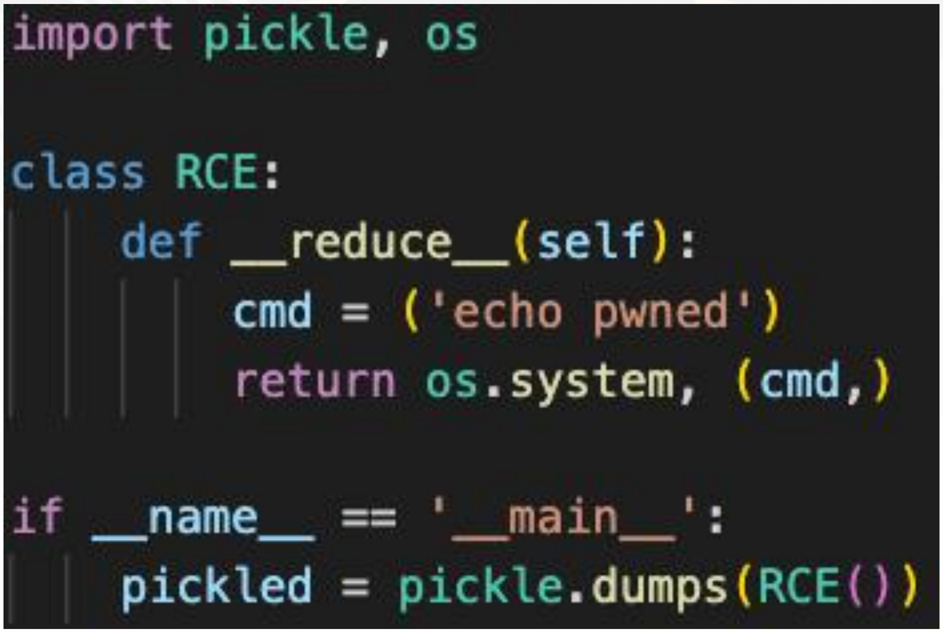
While LastPass did not directly name the "third-party media software" involved in the incident, news reports around the time pointed to Plex, a popular home media storage and streaming platform.

Plex CVE-2020-5741

In May 2020, Plex disclosed CVE-2020-5741, an authenticated remote code execution vulnerability in the Windows version of their media server platform. The issue is a textbook deserialization vulnerability targeting the media server's use of the Python Pickle library. Serialization is the process of converting a code object, like an array or a string variable, into a raw byte stream so it can be easily saved to storage or transmitted over a network. Deserialization is the process of converting the raw byte stream back into the original object. The Pickle library helps Python developers serialize everything from a simple variable to functions and even full classes.

The Pickle library documentation includes a prominent warning to developers that the module is not secure and should not be used to unpickle untrusted data like byte stream objects provided by a user. For an attacker with control over the data being "unpickled," an easy way to exploit the library is by abusing a method called "__reduce__" that Pickle executes automatically while unpickling an object.

The Pickle library's documentation states the __reduce__ method's purpose is to help build a Pickled object's initial state. A developer can pass a callable object (like os.system) and some arguments (like a command) that it will execute while unpacking the object. In the below example, we define a malicious class called RCE with the __reduce__ method defined to execute "echo pwned" using os.system when it is called. attacks, and a domain manager to easily manage phishing domains.

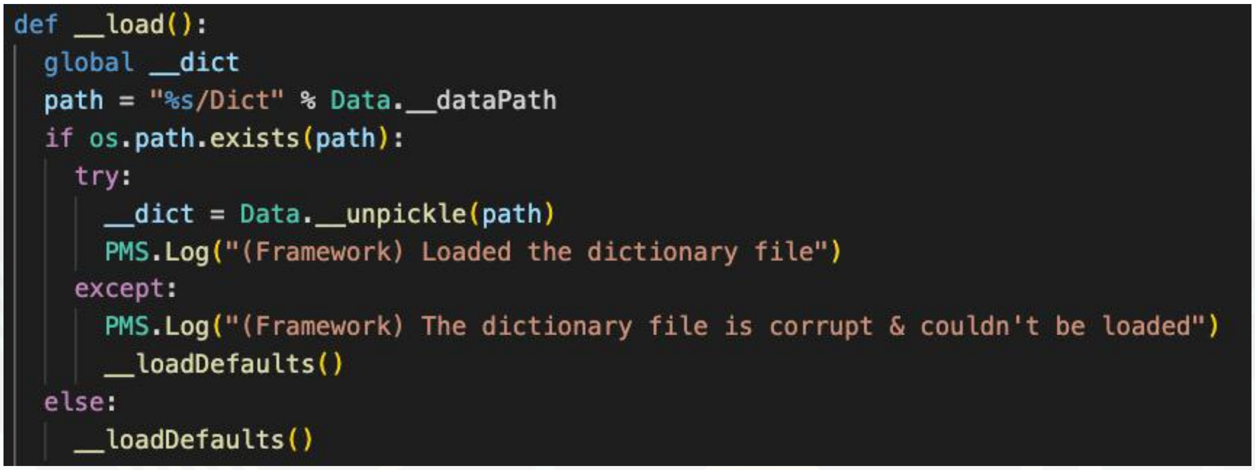


```
import pickle, os

class RCE:
    def __reduce__(self):
        cmd = ('echo pwned')
        return os.system, (cmd,)

if __name__ == '__main__':
    pickled = pickle.dumps(RCE())
```

Figure 28: Malicious Pickled Class

If an attacker can control the object that a Pickle loads, they can use a malicious class like the one described earlier to execute any command they want on the underlying system. This is the vulnerability that **Tenable discovered and reported to Plex** back in early 2020.

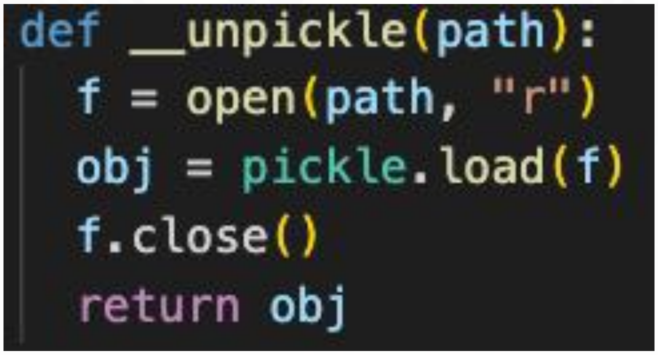
The Windows Plex media server contains a framework module called "Dict.py" that is designed to load pickled dictionaries (Python key/value data storage objects) for plug-ins installed on the server. As shown below, the module checks for a file called "Dict" in the plug-in's "Data" directory and then passes it to the custom __unpickle() method.



```
def __load():
    global __dict
    path = "%s/Dict" % Data.__dataPath
    if os.path.exists(path):
        try:
            __dict = Data.__unpickle(path)
            PMS.Log("(Framework) Loaded the dictionary file")
        except:
            PMS.Log("(Framework) The dictionary file is corrupt & couldn't be loaded")
            __loadDefaults()
    else:
        __loadDefaults()
```

Figure 29: Dict.py snippet

The __unpickle() method then opens the file and passes the contents directly to pickle.load() to deserialize the file.



```
def __unpickle(path):
    f = open(path, "r")
    obj = pickle.load(f)
    f.close()
    return obj
```

Figure 30: Data.py __unpickle method

In theory, the Plex server administrator is the only one with permissions to install new plug-ins or modify system files so this is a relatively safe use for the Pickle library (though an unscrupulous plug-in author could potentially cause problems). Researchers at Tenable found however, they could abuse the (now removed) Camera Upload feature in Plex in combination with a few other authenticated API calls to trick the server into unpickling a malicious file.

Plex deprecated support of the Camera Upload feature in March 2021, but before its retirement the feature allowed Plex users to easily upload photos from their mobile devices to the media server. In the background, Plex creates a directory to save the pictures in as well as a metadata file for uploaded images. By making manual calls to the server's API, Tenable found an attacker could create a new directory in an arbitrary location (like C:\Users\Public) and then upload an arbitrary file to that directory (like a serialized byte stream copy of a malicious Python class).

In the **Proof of Concept (POC)** that Tenable released, they show an authenticated attacker can upload a malicious serialized object called "Dict" to an arbitrary location, mimicking the metadata "Dict" file for a plug-in. Then the attacker could call an API to change the media server's app data path to the new directory containing the malicious "Dict" object and finally restart the Plex server application. When the server starts backup, it attempts to load the malicious Dict object, passing it to pickle.load() as show in the earlier code snippet, which then ultimately calls the __reduce__ method in the malicious object to execute arbitrary commands on the server.

Plex resolved this vulnerability in May 2020 with the release of Plex Media Server version 1.19.3 by removing the API endpoint that allowed authenticated users to change the server's data directory while also limiting the locations where the Camera Upload feature could save files.

All the APIs in this attack require an authenticated admin session on the server. So how did the attacker in the LastPass incident manage to obtain that session? The most likely avenue was a breach involving Plex themselves.

In August 2022, right around when LastPass claims the initial activity in their breach began, Plex notified their users that an attacker had accessed a database containing user account info including usernames and bcrypt-hashed passwords. In their notification, they urged users to change their passwords, which resulted in a surge of users that ultimately overloaded Plex's password change system in the first day of the breach announcement. While not confirmed, it stands to reason that the LastPass DevOps engineer was affected by this breach and failed to change their password quickly enough, potentially because the password change system was down. Bcrypt is a computationally expensive hashing algorithm that makes raw brute-force password cracking hacks difficult, but not impossible. If the DevOps engineer had a weak password, it would not have been difficult for the Plex attacker to quickly crack their credentials.

After breaching the Plex user database, the attacker likely used a tool like Shodan or Censys to identify Internet-exposed Plex media servers. While not a best practice, many Plex users expose their servers directly to the Internet to enable streaming while traveling. While also not confirmed, it looks like either the Plex attacker themselves, or someone they sold the stolen credentials to, potentially hit the jackpot and successfully exploited CVE-2020-5741 on a media server owned by one of only four people with elevated access to the crown jewels of one of the world's most popular password managers. They then just had to wait for the DevOps engineer to access their corporate password vault from this personal Windows computer.

It also isn't entirely impossible that the Plex breach wasn't directly related to the LastPass breach. In LastPass's December 2022 incident notification, LastPass stated the attacker used information stolen from a separate August 2022 breach to specifically target the DevOps engineer. LastPass is an extremely appealing target for a motivated cybercriminal or even a nation-state threat actor. If they identified a Plex media server exposed to the Internet from an IP they knew was associated with a senior DevOps engineer, it isn't outside the realm of possibility that they compromised Plex themselves with hopes of obtaining that engineer's credentials.

What Was Stolen

In their December 2022 incident notification, LastPass updated their initial disclosure to announce the attacker had made off with an encrypted backup of customer vault data and the key required to decrypt it. They were very clear that the decryption key only gave the attacker access to the individually encrypted vaults as well as some unencrypted metadata like URLs. As long as LastPass users had a sufficiently strong master password, it would in theory take the adversary a significant amount of time to crack into the vault.

The threat attacker also stole data from other GoTo-owned companies like MFA settings for a subset of GoToMyPC users and data backups from other products like Central, Pro, join.me, Hamachi and RemotelyAnywhere including usernames and hashed passwords.

Unfortunately for business customers using federated login to LastPass, the attacker also stole key material that severely weakens this style of deployment to the point that users should consider their vaults fully, or at least easily, compromised.

Federated Login for LastPass Vaults

When a normal user accesses their LastPass password vault, a hash of their master password authenticates them to LastPass and allows their browser plugin or mobile app to download their encrypted password vault. Locally on their computer or phone, the plugin or app then uses the master password itself to decrypt and give access to the vault.

Federated Login is a feature only available to business-class users that enables single sign-on (SSO) for LastPass password vaults. Federated Login users don't have a master password and instead use a combination of two "hidden" (at least to them in the UI) keys called K1 and K2 to decrypt their vaults.

K1 is a secret shared by the entire organization. When a user authenticates to their identity provider (IdP) like Active Directory, Google Workspaces, or Okta, that identity provider provides the K1 key to LastPass app. LastPass themselves use the authenticated user info to retrieve the K2 key and the vault itself from their own database and provide it to the app. The app then combines the keys and uses them to unlock the password vault. The benefit of this architecture is that LastPass can provide the vault and a piece of the key without they themselves knowing the full key required to decrypt the vault. Additionally, the organization IdP can provide a piece of the key without knowing the entirety of the key required to decrypt the vault.

The downside of this type of deployment is every user in the organization has access to the K1 key via the authentication response from the IdP. Additionally, the K1 key is not easily rotated. In fact, it can't be rotated without defederating and re-federating every user.

During the October LastPass breach, the attacker was able to steal the K2 keys for organizations enrolled in federated login, as well as metadata about the organizations themselves. With the K2 keys compromised, this leaves only the organization-wide K1 key as the missing half needed to decrypt the vaults. This means a phish or malware targeting a single user is sufficient to decrypt all vaults in the company. With the vault backups already stolen, simply re-tooling the vault isn't enough to protect the already stolen backups encrypted with the compromised K2 keys. This is obviously a serious issue, and any affected organizations should not only re-federate but also consider rotating all keys within their vaults.

Lessons Learned

1

Don't Access Corporate Resources from Personal Devices

In a world full of software as a service (SaaS), it can be difficult to enforce access restrictions to sensitive resources. In many small and midsize organizations, users aren't tied down to accessing resources from their work laptops and can commonly connect to things like corporate email and document stores from personal mobile devices. This access can help employees work on the go, but it doesn't come without risk. The resource access section of your acceptable use policy doesn't necessarily have to be black or white, but it should address access to sensitive resources like corporate password vaults.

2

Personal At Home Security Matters

Push bombing and adversary-in-the-middle toolkits prove that there are still ways for cyber threat actors to circumvent MFA-protected accounts. Just because MFA isn't a silver bullet though, doesn't mean organizations shouldn't deploy it fully wherever possible. Cybersecurity is a game of reducing and mitigating risk wherever possible and MFA remains one of the best tools available to make authentication attacks significantly more difficult to succeed. Fully deploying MFA across your organization, to every user and supported service, should be a top priority.

3

Rotate Your Passwords After Known Breaches

While standards like NIST 800-63b now recommend against arbitrary password expiration dates, they still absolutely do recommend rotating passwords that are known to have been compromised in a breach. Even if the service used strong password storage protections like computationally expensive hashing algorithms, that only buys you more time before your stolen credentials are ultimately cracked. Make sure you've signed up for breach notification tools and pay attention to any attack disclosures from the services you use. If your account credentials were a part of a breach, it's time to immediately rotate them.

Conclusion & Defense Highlights

Conclusion & Defense Highlights

In our introduction, we considered whether history could help you predict the future or if random new things happen too. In either case, this report shares the historical threat trends and unexpected new findings that help you plan your defense. More importantly, whether or not history predicts the future, you have the opportunity to define it by what you do now. As a great person said:

"The best way to predict the future is to create it."
– Abraham Lincoln, 16th President of the US

Knowing the threat trends that have happened and continue to grow in prevalence, combined with learning the latest new and unexpected attack vectors, allows you to prepare defenses that define and create your cybersecurity future today. The most important part of this report is the defensive strategies you deploy in response to any new and continuing findings.

For example, even though malware appears down overall, you know we see a very different story with encrypted network traffic, where it seems to be growing in volume and sophistication. Why not create your positive future by being an administrator that decrypts and inspects encrypted web traffic so that you don't miss the fact that most malware has migrated there.

That's just one example though, so with that in mind, here are some of our defense recommendations based on what we learned in Q4.

Scan encrypted web traffic at your secure gateways

Yes. We have mentioned this tip before, especially in the last few reports. However, we repeat it because the trends continue to prove malware evading network detection via encrypted connections is a big deal, and many people still aren't solving for this problem, at least on a network level.

We still highly recommend you enable the Firebox's HTTPS scanning capability, even if it requires work and tuning to get right. We know the huge majority (~93% in Q4) of malware arrives over encrypted channels, so you are missing a chance to catch most threats early if you don't do this. It is totally worth the effort.

That said, if you aren't going to do this at a network level, at least be sure to deploy multiple layers of good endpoint protection, including an advanced endpoint protection (EPP) and detection and response (EDR) solution, such as WatchGuard EPDR (or AD360). Traffic is decrypted naturally at the endpoint, so these solutions will have a chance to block encrypted threats later in the cyber kill chain. You need at least one solution that has a chance to catch encrypted threats. Having said that, even the most advanced endpoint protection suite is not perfect, which is why we still strongly recommend the additional layer of scanning at the network level, before threats even have a chance to touch the endpoint.

Diligently enforce patching SLAs

You already know you should patch software. Most of the network attacks we see, like the huge amount of ProxyLogin exploits during Q4, target old, fixed vulnerabilities. If you updated the offending software, you wouldn't have to worry about these threats. However, we still see many companies fall significantly behind on patching.

As the team who also support WatchGuard's own corporate security and SOC, we get it. Patching completely is easier said than done. Organizational resources sometimes grow organically, making asset control and identification harder. Often, groups have business reasons why they can't immediately move from a legacy servers or software, restricting your patching ability until they do. However, that is where security governance comes it. Make sure to have best practice SLAs for how quickly internal and external systems must be updated based on flaw severity. **Monitor** those SLAs and report misses to a wider team. If a group is delaying an update for a business reason, document it and make sure to transparently share that with the wider leadership group so everyone realizes the risk you are deciding to defer as a group. Perhaps then, as the severity of the problem increases over time, the group delaying the work needed to update will invest the time to make the changes necessary to fix it.

Separate personal equipment and networks from business, despite remote work.

The LastPass breach perfectly illustrates how an employee — even a good and well-meaning one — can accidentally expose a multimillion-dollar company to a disastrous breach by combining personal practices with business ones.

Remote work is a necessity for many organizations today, so it may be hard to have perfect separation between personal and business. However, you should still strive to make that separation as complete as possible for your business. How? Here are a few tips:

- **Prefer corporate owned devices to BYOD.** There are certainly advantages to BYOD, and perhaps some companies have strong business cases for it, but it is much harder to protect data on something you don't control that in is to force protection on devices you own. If you must allow employees to use personal devices for work, you should invest heavily in containerization solutions, and zero-trust products that really limit what those users can access
- **Verify security before allowing VPN.** VPN is great for remote work. It offers your workers secure connection to private resources. However, if they are using a device on unprotected networks, any malware they get outside of work will have a back door right into your network through VPN. Be sure to use tools that check the security of a remote device before allowing the VPN connection.
- **Where you have no technology, leverage policy.** Sometimes, we don't always have controls that can enforce the rules we want. However, you should have a policy telling users what they can and can't do on your business networks or resources. Even if you have a SaaS app that employees can connect to from any computer, as long as their credential matches, you can have a policy telling them never to connect to that app from a personal computer. Sure, it's even better when you have tools to also enforce that, but if you don't, make sure you have and communicate the policy and behaviors you want.

That covers the Q4 2022 threat landscape from our perspective. We hope you found the content and defense strategies in this report useful. Come back next quarter to see how the trends continue or change then. As always, leave your comments or feedback about our report at **SecurityReport@watchguard.com**, and keep frosty online!

Corey Nachreiner

Chief Security 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

Technical Security Operations Manager

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

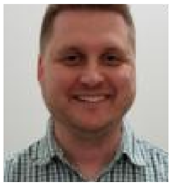
Information Security Analyst

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 Stuifbergen

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 unified cybersecurity. Our Unified Security Platform® approach is uniquely designed for managed service providers to deliver world-class security that increases their business scale and velocity while also improving operational efficiency. Trusted by more than 17,000 security resellers and service providers to protect more than 250,000 customers, the company's award-winning products and services span network security and intelligence, advanced endpoint protection, multi-factor authentication, and secure Wi-Fi. Together, they offer five critical elements of a security platform: comprehensive security, shared knowledge, clarity & control, operational alignment, and automation. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit **WatchGuard.com**.

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

WatchGuard