INTRODUCTION

"Perspectives are like batteries. You can see the positive or the negative, and they'll keep you charged up, if you replace them often enough."

~ Curtis Tyrone Jones

Have you ever lived in an area for a while, but one day climbed to the peak of a mountain range, or gone to the roof of the tallest skyscraper in the area and suddenly gotten that feeling of seeing a very familiar area from an entirely new perspective? Places you might have walked many times sometimes seem very different from aloft or you notice new nuances from that novel perspective. Things you felt seemed far apart and different on the surface, might suddenly show closeness and connection once you see it from afar, and start to give a more complete "big picture" with the new data.

How about optical illusions? We've all seen the interesting pictures that hide two or more images. What do you see first in the image to the right? A tree or plant, or a man and a woman looking at each other? Both options are present, easily noticeable with a little effort, but it takes a shift in perspective and focus to find the additional and insightful data.

In other words, new perspectives often deliver new insights. Every peak and valley offer an opportunity to see a new perspective if you are vigilant and observant. More importantly, that new perspective can deepen your understanding and knowledge of a topic. That's the theme of this quarter's Q1 2023 Internet Security Report (ISR); offering a new perspective.

Since we are looking at data from the beginning of a new year (Q1), we wanted to take this opportunity to update the methods we use to normalize, analyze, and present our statistical findings. In the past, we primarily presented our results in the aggregate, as global total volumes. While showing data from this perspective does help present a global view, it sometimes can also inadvertently skew perspective – especially when handfuls of outlier results mask the more common picture.

Starting this quarter, we will present our network security results as "per device" averages for all reporting Fireboxes. We also have done more data curation to normalize some statistical outliers, to show you the results that better match all the average devices in the world. We believe this not only gives a more accurate idea of our malware trend averages, but it also shows you a new perspective about how threats might affect you directly, as a person only managing one, or a handful of devices.

As in our past reports, we still aggregate all the threat intelligence we get from the WatchGuard network and endpoint products that have opted into reporting this anonymized data to us. We look at malware trends from both a network and endpoint perspective, highlight the most common network exploits we see, show the top malicious links end users click on, and more. With our new perspective, we hope this data gives you some insight into how cybercriminals attack most networks so that you can make sure to implement the right security strategies to help protect yours.

The Q1 2023 report includes:

Throughout this report and in our conclusion, we share many timely security tips that will keep you safe, with and without our products.

EXECUTIVE SUMMARY

This Q1 2023 report is about new perspectives, but due to our new measurement methods it's harder to directly compare to historical values in past reports. That said, the high-level volume trends have not changed much over Q4 2022. Network attacks (IPS detections) have remained relatively flat over the last three quarters, technically down a bit more than 3%. We can't compare network malware volume as directly this quarter, due to the "per device" change in how we report it, but the overall volume looks similar to previous quarters. However, zero day malware (which we define as any malware sample that gets past signature-based detection) has increased in both unencrypted and encrypted traffic. We also still see more evasive and sophisticated malware in encrypted traffic in general, so make sure you leverage our network TLS decryption capabilities.

We always get a slightly different perspective when looking at malware from our endpoint product's viewpoint. There, we see that ransomware detection has declined 73% quarter over quarter (QoQ) after increasing significantly (627%) during Q4 2022. Even though ransomware detections are down by volume, ransomware groups are still breaching and extorting many companies, and the Lockbit group continues as the most prolific in successful breaches. Rounding out high-level trends, attackers still leverage malicious scripts, primarily PowerShell, to deliver malware.

Users still mistakenly click malicious links, but luckily domain protection services like DNSWatch can save them. In the report, we share some of the top phishing, malware spreading, and compromised sites users accidentally tried to visit. We also highlight a new browser social engineering trend. Now that web browsers have more protections preventing pop-up abuse, attackers are using the relatively new notification features to force similar types of interactions.

This quarter, we did not include the story of the quarter or a new research project, since our focus was on updating our perspective with new methods to analyze our threat intelligence and numbers. However, we will return to that in future quarters. That said, the report is still chock full of takeaways and defensive learnings you can glean to add to the protection strategies you already deploy.

That's the high-level overview, but below we share some of the top executive highlights from Q1 2023:

- **This quarter, we moved to "per Firebox" malware volume reports,** making it a bit more challenging to compare to previous reports' overall numbers. Below are the malware results for our various malware detection services:
  - **Average total malware detections per Firebox: 932**
  - **Average malware detections by GAV per Firebox: 364** (39% of total malware)
  - **Average malware detections by IAV per Firebox: 236** (25% of total malware)
  - **Average malware detections by APT per Firebox: 332** (36% of total malware)
- We extrapolate that if all the Fireboxes reporting to us had all malware detection services enabled, we would have had **72,704,388 malware detections during Q1 2023.** Note, that number only represents the Fireboxes that have opted into sharing data with us, which is less than one-fifth of the active Fireboxes currently in use.
- **Endpoint ransomware detections declined ~73%,** despite the 627% increases last quarter (Q4 2022). This still translates to a lot of ransomware due to the hundreds of percentile increase last quarter, but it also has declined ~75% year over year (YoY). Nonetheless, ransomware extortion groups like Lockbit remain active, so keep your ransomware defense strategies current.
- **96.4% of malware hides behind encryption!** This increased at least 3 points QoQ. We've mentioned it before, but most malware hides behind the SSL/TLS encryption used by secured websites. If you don't inspect this traffic, you are missing most malware your network security controls. While your endpoint malware protection acts as a safety net, we highly recommend scanning encrypted traffic.
- **Zero day malware accounted for 70% of all malware** when looking at total detections. That increased to 93% of all malware in encrypted connections. After dropping to only 43% of total malware last quarter, it is interesting to see this number rise again.
- **Threat actors from China and Russia were behind 75% of the new threats we saw in our top 10 list.**
- **Office document threats remain common among the most widespread malware.** Our widespread malware list features the malware that touches the most victims, even if it's not technically the highest pure volume. We continue to see document-based threats targeting Office products in this list.
- Network attack detections dropped 3.2% quarter over quarter (QoQ) during Q1. Though technically a decline, our charts show that our intrusion prevention service (IPS) detection has essentially remained flat the last three quarters.
- **The average Firebox had 460 IPS detections per device.**
- **The top 10 network attacks accounted for 57% of all detections**, which means those ten exploits make up a huge majority of the attacks we saw online during Q1.

- **Regionally, EMEA has the most malware detections at 40% of the total, while AMER has the most network attack detections at 56% of the total.**
- **Phishers and web threat actors leverage web browser notifications.** When researching the most common malicious domains we blocked this quarter, we found several of them leveraging a web browser's notification features to do the same social engineering techniques they used to leverage via pop-ups. We theorize that this is because browsers' relatively new notification capabilities don't have the same protections in place as pop-ups.
- **Threat actors still targeting End-of-Life (EOL) Microsoft ISA Firewall.** While it didn't show in our Top 10 Network Attack list, our analysts did notice exploits against Microsoft's now discontinued firewall, and their Internet Security and Acceleration (ISA) Server, having relatively high hits at 37th in our list. Considering this product has been long discontinued and not updated, it is surprising to see attackers targeting it.

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.