Introduction

Cybersecurity is all about staying one step ahead of your adversaries, managing and mitigating risk before threat actors can execute their attack. However, knowing what step to take next is often the most difficult challenge organizations face. In a perfect world we'd all have infinite resources to devote to securing our assets and users, but the unfortunate fact is that is never the case. In lieu of the perfect world, we instead need to know where to focus our attention to receive the biggest return on investment and to do that, we need to understand the latest adversarial tools, tactics, and procedures.

Shared threat intelligence makes the entire security community stronger. Knowledge from cyberattacks affecting organizations can help other organizations know what they need to watch out for. Thanks to WatchGuard partners and customers that have opted in to sharing threat intelligence from their networks, we're able to build this report with an accurate picture of the current threats targeting midsize and distributed enterprises. Without this valuable data we wouldn't have visibility into the malware variants and network attacks that adversaries are leveraging, and we wouldn't be able to help guide you down the path to strong security.

Thanks to the tens of thousands of perimeter appliances that opted in to threat intelligence sharing and tens of millions of endpoints reporting in with the latest blocked threats, the rest of this report will guide you through the real-world attack trends. With those trends, we can offer you defensive strategy guidance on where to focus your attention so you too can stay one step of current threat actors.

Our Q3 2021 report includes:

06 **The Latest Firebox Feed Threat Trends**
In this section we dive into the latest malware and network attack trends as well as the top malicious domains from the quarter. We'll break them down both by total volume and by most individual organizations impacted. This quarter, we highlight a few new threats including recent attacks exploiting a Microsoft Office vulnerability and a popular credential-stealing phishing campaign

28 **Endpoint Security Trends**
We continue our look into malware arriving at the endpoint this quarter with the latest trends for malware infection origins. In this section, we take a closer look at the tactics threat actors are leveraging to attack the endpoint. We also continue our analysis of ransomware trends through 2021.

33 **Top Incident – Kaseya Ransomware Attacks**
It's tough to think of a more high-profile (at least in the IT space) ransomware attack in recent years than the early-July attacks involving Kaseya VSA-managed endpoints. Adversaries exploited several zero day vulnerabilities in the popular remote monitoring and management (RMM) system to deliver the REvil ransomware variant to upwards of a million endpoints. In this section, we analyze the attack and provide guidance on defending networks against the growing threat of digital supply chain attacks.

35 **Defensive Strategies**
It wouldn't be enough to share the latest threat trends without knowing what you could do to combat them. Our primary goal for this report is to help provide defensive strategies to combat the evolving threat landscape. We end the report with a summary of the latest techniques you can use to get the leg up on cyber adversaries.

Executive Summary

Malware and network volume decreased during Q3 –at 3.4% and 21% respectively. This downward trend came after several quarters of gains in detections across several products. While we did see a downward trend in this area, there was an increase in endpoint malware detections that has surpassed the total volume of 2020 detections.

A significant percentage of malware continued to arrive over encrypted connections. This is a consistent trend we noticed with network signatures detected over our Intrusion Prevention Service. As a reminder from our observations, it's still common for this traffic to go uninspected. This is why we and others in the security industry practice defense-in-depth strategies. While there has been a decline in total malware detections, on average the Fireboxes have seen more detections this quarter.

A snapshot of the Q3 2021 threat landscape:

- **Total perimeter malware detections between Gateway AntiVirus (GAV) and APT Blocker services reached ~16 million**. This is a 3.4% decline since Q2. Although a reduction in malware volume, the average Firebox saw 454 detections – an increase from 438 per device in Q2.
- **Malware arrived by TLS for 69.8% of the total connections**. This is less than last quarter but still a considerable size. IT administrators may want to consider decrypting these connections as they arrive, or else be left with an overall visibility gap.
- **We saw zero day malware increase to 67.2% this quarter – about a 3-point increase**. A noticeable rise involved zero day malware over TLS, which rose to 47% from 31.6% last quarter.
- The XML.JSLoader variant held its top spot for the most-trafficked encrypted malware. **In addition, the variant with the second most hits was Tearspear, a downloader new to our top list.**
- Network attack volume returned to just below Q1 2021 levels, with Firebox Intrusion Prevention Service (IPS) detecting ~4.1 million network exploits in Q3. **This is a 21% decrease following two quarters of 20+% growth.**
- Following a similar trend to total volume, average detections per Firebox returned to Q1 2021 levels. Firebox appliances blocked an average of 116 attacks. **That is a 21% decrease from Q2 but a 3-point increase from Q1.**
- The top 5 most-widespread IPS attacks signatures continue to expand the number of unique countries listed among its top targets. **This quarter includes Australia, for a total of ten unique countries facing our most-widespread attacks.** The range of unique countries switched between six or seven quarter-over-quarter (QoQ) until Q2, when it reached nine.
- **DNSWatch detected 5.6 million visits to malicious domains, a 23% decrease from last quarter.** We recorded 7.3 million detections last quarter. The stark decrease isn't significant when considering that the count was at 1.3 million blocked domains in Q4 2020.
- **Endpoint products in 2021 have already handled a cumulative 10% increase in malware originating from scripting attacks** compared to total volume in 2020.
- **Ransomware detections up until the end of this quarter have also surpassed the 2020's total volume.** It is sitting at 105% of 2020's volume and we can expect the total to rise after combining next quarter's data, or it could remain at 105%, but we wouldn't bet on that.

These statistics can frame your thinking as you review our Q3 2021 security report. The ups and downs of volume QoQ is important to look at, but it is also necessary to consider the context of the year as a whole and years prior. Continue on for a review of this past quarter's activities and what these indicators may mean for your company moving forward.