Introduction

If you don't know what your adversary is doing, you won't know how to protect yourself against their attacks.

For the third quarter in a row, the WatchGuard Internet Security Report provides analysis of threat data from the Firebox Feed, which comes from more than 33,500 unified threat management (UTM) appliances worldwide. We also deliver deeper insight into the big security stories from the period, and fresh research from WatchGuard's Threat Lab. Armed with this data, you'll know how to adjust your defenses to meet and defeat the latest attacks.

The report for Q2 2017 includes:

WatchGuard Firebox Feed Trends

Tens of thousands of WatchGuard customers have allowed their Firebox appliances to share threat intelligence data, including details about what malware we block and what attacks we defend against worldwide.

Top Story: WannaCry

Every quarter has information security stories that stand out above the rest, and this quarter was no exception. In this report, we analyze the infamous WannaCry ransomware, and discuss how a leaked NSA zero day vulnerability was used to achieve worm-like capabilities. In fact, this "ransomworm" has proven at least two of the WatchGuard Threat Lab's **2017 security predictions** true.

SSH HoneyPot Research

In addition to analyzing data from our Firebox Feed, the WatchGuard Threat Lab constantly runs new security research projects to learn about the latest attacks, tools, and threat actors. This quarter, we share details about the Telnet and SSH attacks we watched with our honeypot. Though automated, remote CLI attacks have been around for a while, monitoring the latest techniques can give you some insight into what current cyber criminals are after.

Tips to Keep Hackers at Bay

We share various protective tips throughout this report, but this section provides the summary of top tips and learnings.

This threat intelligence should be used to help you protect your organization against the network exploits, malware infections, and advanced attacks that are launched by cyber criminals every day, and should become a regular part of your information security awareness training. Thank you for joining us for another quarter of reporting, and read on to learn about Q2's threats.

Executive Summary

We live in an age where malicious ransomworms shut down hospitals, sneaky nation-state malware disrupts international shipping companies, and banks lose tens of millions because of network breaches. To protect yourself from these, and other attacks, you need to stay current on the adversary's latest attack techniques, tools, and trends.

Here's a high-level summary of some of the things you'll learn from this report:

- **Usage of a credential-stealing tool, Mimikatz, accounted for 36% of our top ten malware in Q2.** While we saw many familiar threats in our Q2 malware top ten, we also noticed a significant surge in detection for the Mimikatz tool, which attackers use to steal and replace Windows credentials.
- **Legacy antivirus (AV) missed almost half of the malware delivered in Q2.** Over the past three quarters, we have monitored the number of threats that were caught by our behavioral malware sandbox, but were missed by legacy AV. This quarter that number is the highest we've seen yet, at 47%. This means almost half of the malware we see evades detection by older, signature-based AV.
- **Overall, malware detections jumped 41% compared to Q1 2017.** Though it is still slightly down from the high seen in Q4 2016, cyber criminals seem to have picked up their malware campaigns this spring.
- **Network attacks are down 30% compared to Q1**, Though we saw a new increase in attacks trying to brute force web credentials, network attacks still declined last quarter.
- **Attackers try to steal Linux passwords in the Nordics and Netherlands.** We detected attackers leveraging an old Linux vulnerability to try to steal password hash files. These attacks primarily affected Norway, Finland, and the Netherlands.
- **The top network threat, a generic XSS attack, primarily targeted Spain.** We aren't sure why this particular cross-site scripting exploit was popular in Spain, but it was.
- **Malicious JavaScript also used for phishing.** Beyond malware delivery, we also saw an increase in malicious JavaScript being used to create fake phishing sites.
- **Criminals still exploiting JavaScript in email.** For the past three quarters, we've seen cyber criminals leveraging JavaScript code and downloaders to deliver malware. Though attackers can exploit JavaScript for both web and email threats, there was much more malicious JavaScript in email. We recommend you leverage email security controls to block JavaScript attachments.
- **The web continues to be the battleground.** As has continued for the third quarter in a row, most if not all the top ten network attack targeted web servers and clients. Adding additional security services to your web traffic remains a top priority.

Those are just a few of the many trends this report explores. Dive in to learn more.

In Q2 2017 WatchGuard blocked over

16,403,723
malware variants
(488 per device)*

2,902,984
network attacks
(86 per device)*

* average per participating device