Introduction

In Ender's Game, a famous sci-fi novel by Orson Scott Card, a military instructor whispered this to Enders Wiggen.

"I am your enemy, the first one you've ever had who was smarter than you. There is no teacher but the enemy. No one but the enemy will tell you what the enemy is going to do. No one but the enemy will ever teach you how to destroy and conquer. Only the enemy shows you where you are weak. Only the enemy tells you where he is strong. And the rules of the game are what you can do to him and what you can stop him from doing to you. I am your enemy from now on. From now on I am your teacher."

The instructor's point was that you can learn from your enemy, and that statement rings as true in the "cyber" battle, as it does in real military conflict. If you don't know your enemy, and follow his or her latest tactics, you will never know your weaknesses and how to defend them.

This marks the first full year of our WatchGuard Internet Security Report, where we provide valuable threat trend analysis based on data from our Firebox Feed. By monitoring the different types of malware and network attacks seen (and blocked) by tens of thousands of Firebox appliances around the world, we can tell you the latest cyber attack trends, so that you know where you are weak, and what you can do to stop the enemy.

Our quarterly report also covers some of the big security stories from the past three months, focusing on technical details you probably didn't see in the news. Finally, we share some of the research products and tools used by the WatchGuard Threat Labs team.

We publish this timely threat intelligence in hopes that you use it to update and perfect your defenses, and thus protect your organization from the latest network exploits, malware, and advanced attacks. Like Ender, you can leverage this knowledge to master your enemies.

The report for Q3 2017 includes:

WatchGuard Firebox Feed Trends

In this section, we analyze threat intelligence shared by tens of thousands of WatchGuard security appliances. This analysis includes details about the top malware and network attacks we saw globally throughout the quarter. Using that data, we identify the top attack trends, and how you might defend against them.

Top Stories: Software Supply Chain Attacks.

This quarter, our researchers noticed a number of stories with a similar pattern; cyber criminals infiltrating legitimate software supply chains to deliver malware. We share three of these news stories, and what they might tell us about future attack trends. We also analyze how one of these supply chain attacks worked on a technical level.

Artemis Honeynet Research and Release

In addition to analyzing data from our Firebox Feed, the WatchGuard Threat Lab constantly runs security research projects. This quarter, we share details about some of the phishing findings the team discovered from emails captured by our spam honeynet, which we call Artemis. More excitingly, we detail all the Artemis components and how they work, and have released these components to the public on GitHub. You can download and use it now.

Updated Defensive Strategies

The whole point of our report is to provide analysis of our enemies so you can adjust your defenses. Throughout the report, we'll share defensive learnings and tips you can implement today, to protect your company from the latest threats.

We hope this report becomes a regular stop in your quest for constant security education and awareness. Thank you for joining us for another quarter, and read on to learn about Q3's threats.

Executive Summary

How does the average small business stand a chance of defending against threats like those seen in Q3 2017? For example, a major credit-reporting organization suffered a cyber attack resulting in the loss of sensitive information concerning half of all U.S. citizens. Also, an extremely popular Windows utility was hijacked to deliver malware. And cyber criminals released a new, seemingly geographically targeted ransomware variant called Bad Rabbit. Attacks like these rightfully cause fear in small and large businesses alike, because they show that no one is safe. But, there is hope, if you stay abreast of the latest attack trends, and update your network defenses. This report helps you do just that.

Here are some of the high-level trends and takeaways from this quarter's report:

- **Scripting attacks accounted for 68% of total malware hits.** Our Gateway AntiVirus (GAV) solution has many signatures that catch generic and specific JavaScript and Visual Basic Script threats, such as downloaders. When we combine all these scripting threats, they account for the majority of malware we detected in Q3. Be sure you have security controls that can detect and block malicious scripts.
- **In Q3, legacy antivirus (AV) only missed 24% of malware.** Since the inception of this report, we have monitored the number of threats that were caught by our behavioral malware sandbox, but were missed by legacy AV. Over the past three quarters, we found legacy AV missing more and more malware, peaking at almost 47% last quarter. However, this quarter's number dropped to an all-time low of only 23.77%. It could have to do with a recent change in our GAV engine.
- **Overall, malware quantities jumped significantly in Q3.** Using signatures and anti-malware, our Firebox appliances blocked well over 19 million malware variants in the past three months, which is an 81% increase over last quarter. We suspect malware attempts will continue to increase next quarter – driven by the holiday season.
- **Network attacks, however, are way down.** We saw a 44% decrease in IPS hits this quarter. Granted, that is in part because we decided to remove a particular signature from our results (or it would have been a big increase) due to the potential it was a false positive.
- **Evil iframes show up everywhere.** Both our malware detection and IPS results showed plenty of evidence that attackers continue to evolve how they leverage the HTML iframe tag to force unsuspecting victims to suspicious, and often malicious, sites. In this report, we share some detailed analysis on how these threat actors try to hide their evil iframes.
- **Cross-site Scripting (XSS) attacks continue to plague web browsers.** We continue to see a slow growth in the use of XSS attacks. This time, however, we saw these attacks affect many regions and countries, rather than just a few.
- **Authentication is still a big target.** Though it dropped a bit from last quarter, we see a lot of authentication-related malware hits (like Mimikatz) and IPS hits related to brute-forcing credentials. Don't forget that your credentials are your weakest link. You need to protect them.
- **We saw less Word Macro-related malware in Q3.** Though we did still see other malware related to Word documents, including a threat that seemed to leverage some Word DDE-related issues.
- **Most network exploits still target web servers, browsers, and applications.** All of our IPS top ten, which account for the majority of IPS hits, represent web threats.
- **We saw a lot of Linux/Flooder malware hits in Italy.** Linux/Flooder can detect malicious and legitimate tools that might be used in DDoS attacks.
- **In Q3 2017, WatchGuard's GAV and APT Blocker blocked over 22,867,935 malware variants** (764 per device) and **2,902,984 network attacks** (54 per device).