Introduction

For decades, most American football coaches and players – from high schools to the NFL – have understood the importance of studying their opponent's offense in order to put up a good defense.

Ever since we **started recording games in the 1960s** and earlier with television cameras, football coaches have tried to get their hands on their opponent's game film to study their strategies. Coaches and **players agree** that this film study can make an average player good, a good player great, and a great player phenomenal. This makes obvious sense. The more you know about your opponent's offensive strategies, the easier it is to craft effective defenses.

The goal of our quarterly Internet Security Report (ISR) is to act as that critical "game film" to show you how your criminal adversaries target you, and try and defeat your defenses. For instance, the report includes valuable threat trends and 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, helping you identify your weaknesses, and update your defenses accordingly.

Our quarterly report also sometimes includes interesting research performed by the WatchGuard Threat Lab team. This may include primary research on a wide-range of information security topics, or additional technical analysis around the biggest security stories from the quarter.

We share this threat intelligence in hopes of helping you win the cyber security war. If you make reading our quarterly report a habit, we expect your security skills to improve accordingly. Like football players studying the latest films to find their opponent's weakness, we hope that by reading our report regularly, you improve your security game.

The report for Q1 2018 includes:

WatchGuard Firebox Feed Trends

In this regular 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 Story: GitHub DDoS Attack

In Q1 2018, attackers launched a record-breaking distributed denial of service (DDoS) attack against GitHub using a technique called UDP amplification. In this section we analyze this attack and describe how the lesser-known Memcached service allowed this huge amplification.

Announcing The 443 Podcast

Rather than our normal threat research section, this quarter we announce a new podcast from the WatchGuard Threat Labs team, and the authors of this report. Learn what this new podcast contains and come subscribe wherever podcasts are found.

The Latest Defense Tips

As usual, this report isn't just meant to inform you of the latest threats, but to help you update your defenses based on the latest attacks. Throughout the report, we share defensive learnings and tips, with a summary of the most important defenses at the end.

As always, we hope this report keeps you aware of your opponent's offensive strategies in the same way football films do for NFL players and coaches. Thank you for reading this report, and feel free to share any comments or feedback on Secplicity.org.

Executive Summary

This quarter, GitHub suffered the largest DDoS attack in history, an old worm called Ramnit made a comeback, malicious cryptocurrency miners quietly sprouted, and we saw a large increase in network attack volume. The good news is WatchGuard's Firebox security services blocked most of these threats and the defense tips within this report can help round out your protection.

Below are the main points from this quarter's report:

- **Old Ramnit malware makes a comeback in Italy.**
  An older trojan/worm from 2010 has resurged in the scene, almost entirely in Italy (98.8%). The Ramnit.A malware has done many bad things in the past, but this latest variant seems to be a banking trojan that spreads via HTML files.
- **Malicious Office documents continue to target U.S victims.** A new Office exploit made the top 10 network attack list during Q1 2018, and 94.6% of this attack targeted victims in the United States.
- **Malicious cryptocurrency miners quietly spread.** Though they didn't directly make our top 10 list, Q1 includes many indicators that malware designed to steal your computer's processing power to mine cryptocurrency is on the rise.
- **Scripting attacks continue to drop, only accounting for 30.3% of top malware.** Our Gateway AntiVirus (GAV) solution has many signatures that catch generic JavaScript and Visual Basic Script threats, such as downloaders and droppers. However, we continue to see these types of attacks decline in Q1.
- **Malware is down 23% from Q4.** Our Firebox appliances blocked 23.7 million malware variants during Q1, which is a 23% decline from Q4. We expect this decline every year since Q4 historically has the highest malware volume due to the holiday season. However, zero day malware rose slightly despite the overall malware decline, as you will see in this report.
- **You still need advanced malware protection to catch 46% of malware.** This quarter, 45.9% of malware evaded the basic signature-based protection of our GAV service. This was actually a small 0.2% rise over last quarter. In short, if you only rely on legacy antivirus services, you are missing close to half the malware out there.
- **Network attacks grew 52%.** Our IPS system caught over 10 million network exploits in Q1, 2018; an increase of 52% over Q4.
- **GitHub saw a record-breaking DDoS of 1.35 Tbps.** This attack proves that UDP-based amplification attacks can create more malicious traffic volume than even the largest botnets.
- **Watch out for drive-by downloads in the U.S.**
  An exploit that targets Internet Explorer made the top 10 IPS list this quarter, with 74% of its volume affecting U.S. victims.
- **Mimikatz credential stealers continue to make the top 10, primarily in the U.S.** Mimikatz, a well-know Windows credential stealing tool, continues to find its way onto our top 10 malware list. This quarter, two-thirds of this threat was found in the United States.
- In Q1 2018, WatchGuard **blocked over 23,734,724 malware variants** (628 per device) and **10,516,672 network attacks** (278 per device).

Those are just a few of the many trends covered in this report. Keep reading to learn more.