Introduction

Life is change and survival requires adaptation.

I've surely said that before and will likely say it again, simply because it applies so well to many aspects of life. For instance, you've surely heard us, and others, say something like this about the cyber threat landscape. "Cyber security is a cat and mouse game. As cyber criminals continually evolve their attacks, so must you adapt your defenses. Information security is a constant arms race." All of that is true, of course, but this time the change and adaptation I'm referring to is to this report itself.

As regular readers may know, the goal of our quarterly Internet Security Report is to share valuable details about the changes we see in the threat landscape so that our readers can adapt to those evolutions with the proper defenses and security policies. The WatchGuard Threat Lab quantifies and analyzes the real-world threats we see attackers use every day, so that you can adjust your protections accordingly. However, over the years of doing this report, we've started seeing the common trends repeat regularly. While there is nothing wrong with highlighting common trends, we also need to discover the new, up-and-coming threat evolutions in order to offer you the best chance to adapt and survive.

With that in mind, we've made a few small adaptations to our report to help highlight the more subtle changes to the threat landscape. For example, this quarter's malware section includes a new segment about widespread malware, which are threats that affect that broadest range of victims even if they don't have the highest volume. We also introduce new threat intelligence based on our latest anti-malware service, IntelligentAV (IAV). In our network attack section, we've started tracking the number of *unique* network exploits we detect each quarter, rather than just looking at the top 10 attacks by volume. In short, we are making sure our report adapts and changes so that it continues to retain its value and insights for our readers.

Also, don't expect these adaptations to end here. In upcoming reports, we hope to add information from WatchGuard's additional security services, such as our DNS firewall called DNSWatch, and our breach prevention system called Threat Detection and Response. In short, we believe strongly in the concept of adapt or die, and we intend to continually redefine this report to make sure it adequately covers the change we see happening in information security every day.

The report for Q4 2018 includes:

The quarterly Firebox Feed trends.

In this updated section, we analyze threat intelligence from well over 40,000 WatchGuard Fireboxes. We cover the top ten malware, some quarter-over-quarter and year-over-year analysis, and regional trends. We also introduce you to a new section covering the most widespread malware, and share the most prevalent network attacks. As always, we finish with tips that can protect you from these threat trends.

Q3 Research: Dissecting the Exobot backend.

Months ago, source code for a well-known Android botnet leaked to the public. Our team got our hands on the source and have spent some time over the last few quarters analyzing how it works. This quarter, we share that analysis and give you strategies to avoid an Exobot infection yourself.

Top Story: Google & Cloudflare BGP Hijack.

During Q4, traffic destined for Google got temporarily redirected through Russia and China for 74 minutes. While this turned out to be an accident, it also illustrates a major weakness to our Internet infrastructure. In this report, we detail this under-covered story, and share our thoughts on how the industry can prevent BGP from getting abused in a more malicious attack.

Regular defensive advice.

What good is knowing about change if you have no clue how you might adapt to it. The true point of our report isn't to sensationalize the threats, but to ensure we give you the tools to adapt and defend against these attacks. Look for regular tips throughout the report, and some summarized tips at the end.

Some people are afraid of change, but I find that if you keep aware of it, you can easily adapt to much of it, retaining a semblance of safety and control. Let our report highlight the important infosec changes to worry about, so you can focus on making the adaptations necessary to survive and flourish.

Executive Summary

This quarter, we saw an increase in phishing attack campaigns, a rise in zero day malware, the continuation of cryptominers prevalence, and more unique network attacks than ever seen before. We also saw an ISP accidentally hijack Google's network traffic via BGP, and we share our analysis on a leaked Android botnet kit. As always, WatchGuard Fireboxes prevented these attacks, which is why we have the data around them. Nonetheless, read the full report to learn additional defenses that can protect you in the future.

Here are the highlights from the Q4 2018 ISR report:

- **Phishing attacks increased** during Q4 with one sextortion scam hitting the number two malware spot and **accounting for 5% of all malware.** This phishing email also had the most unique variations by hash. Besides that, we also saw a banking phish make our most widespread malware list.
- **Our newly launched IntelligentAV (IAV) service caught 23.1% of advanced malware** *on* the boxes that were running it. This service relies on machine learning (ML) and artificial intelligence (AI) training to proactively recognize malware never seen before, and it's doing a good job so far.
- **Zero day malware increased this quarter accounting for just under 37%** of all threats. This despite general malware decreasing 51% year-over-year (YoY).
- **Overall malware decreased for the first time during Q4.** Historically, the last quarter of the year tends to have the highest malware volume, presumably due to malware campaigns associated with various holiday shopping seasons. However, this quarter malware is down 28% quarter-over-quarter (QoQ) and 51% YoY. Even so, our Firebox GAV service blocked 11.2 million malware variants during Q4.
- **Mimikatz tops the list again accounting for an astonishing 18% of all malware.** It primarily affected the America and Europe regions.
- **APAC malware returns to its usual low volumes.** Historically, we saw the lowest malware volumes in the Asia-Pacific (APAC) region. However, during Q2 and Q3, APAC malware volume skyrocketed, giving it first place. This quarter, however, APAC drops back to its typical third place with only **17% of the malware total.**
- **After three quarters of drops, network attacks rose during Q4.** We saw a 46% QoQ increase in intrusion prevention hits this quarter.
- **We saw more unique network attacks than ever before.** During Q4, we saw well over 1,200 different network exploits attempted against our customers. This is more than double any previous quarter.
- **Attackers target a new-ish Cisco Webex vulnerability.** 7.4% of all network attacks targeted a 2017 flaw in the popular Cisco webinar framework.
- **Less than 1% of Internet ASs validate their BGP routes.** During Q4, an ISP's BGP mistake resulted in Google's traffic routing through Russia and China. Unfortunately, less than 1% of the Internet uses the BGP security extensions that can prevent this.
- In Q4 2018, WatchGuard Fireboxes **blocked over 16,074,782 malware variants (382 per device) and 1,244,146 network attacks (29 per device).**