Introduction

For over a decade, WatchGuard's Threat Lab (previously the LiveSecurity Threat team) has closely monitored the latest computer and network security threats affecting small to midsize businesses (SMBs) and distributed enterprises (DEs), and shared our research and analysis with the world via our blog, Secplicity.org.

Our threat intelligence has come from many sources in the past, including individual malware and threat research projects, data from our internal honeynet, research into underground forums and economies, and shared data from WatchGuard's many industry-leading partners. However, most recently we've added the Firebox Feed to our arsenal of threat data.

The Firebox Feed is the name we've given to the anonymized threat data gathered from the tens of thousands of unified threat management (UTM) appliances protecting our customers around the world. These globally distributed security appliances constantly identify and block millions of network exploits, malware infections, and advanced attacks every month, and provide valuable insight into exactly how cyber criminals are evolving and re-targeting their attacks. We plan to share these trends and insights with you every quarter in this Internet threat report.

Our Firebox Feed and latest research projects have given us a deeper insight into the biggest threats our customers face and how cyber criminals craft their latest attacks. We are excited to continually share these kinds of insights with you in our quarterly security reports. We hope this report becomes a regular stop in your quest for information security knowledge, and invite you to share any feedback you have that could make it more valuable. Thanks for joining us this quarter, and read on to learn more about the latest computer and network threats.

In general, the quarterly report will consist of:

The latest Firebox Feed trends and analysis

This includes the top network attacks, top malware trends, and our analysis on what contributes to these trends. We'll also share protection tips to avoid these top attacks.

Analysis on the top information security (infosec) stories from the quarter

Today, you're flooded with infosec stories every week. In this section, the Threat Lab team analyzes the top security incidents from the quarter, focusing on the issues with the widest impact. When possible, the team provides deeper technical analysis on these issues than the original news, and shares practical tips to help you avoid the issue.

New Security Research and Discoveries

WatchGuard's Threat Lab constantly runs security research projects to study the threats or issues affecting organizations today. For example, last quarter the team began a project looking into the lack of security of random Internet of Things (IoT) devices. Every quarter, we'll share the results from primary security research projects like these.

Tips to protect your organization from the latest threats

While the Threat Lab team is fascinated—even obsessed—with following the latest evolutions in criminal hacking and malware, we don't do it just for fun. For every report, our goal is to provide you with practical defense tips that can help you survive the current threat landscape. More than anything, this report is intended to offer you the tools you need to minimize the online risk of your organization.

Executive Summary

As has been the trend of late, Q4 2016 was a very eventful time for information security. Businesses are getting inundated with ransomware attempts through phishing emails and malicious websites. Banks are getting targeted by sophisticated criminals who have been able to steal millions of dollars at a time.

Even nation-states have gotten involved, with the U.S. officially blaming the Russian government for an election-related breach. To survive this dynamic threat landscape, you need to understand the latest attack trends. This report provides some details around those trends. Here's a high-level summary of some of the things you'll learn from this report:

- **30% of malware was "zero day"** and wasn't caught by legacy antivirus (AV) solutions. You'll miss almost 1/3 of malware without an advanced threat prevention solution.
- **Macro-based malware is still prevalent.** Despite being an old trick, many spear-phishing attempts include documents with malicious macros.
- **JavaScript is a popular malware delivery and obfuscation mechanism.** Our feeds see a rise in malicious JavaScript, both in email and over the web.
- Most network attacks target web services and browsers. In fact, **73% of the top attacks target web browsers in drive-by download attacks.**
- **Exploit Kits (EKs) are a popular malware delivery mechanism**, and likely account for the prevalence of malicious JavaScript.
- Sophisticated attackers continue to target banks with evasive malware.
- We see a significant amount of Linux-based trojans, likely connected with **IoT attacks.**
- **Nation-state hackers** use similar hacking tools as criminals, but with more **sophisticated obfuscation and evasion techniques.**

Those are just a few of the many trends this report explores. Read on for more in-depth explanations and deeper technical analysis.

In Q4, 2016 WatchGuard blocked over

3,038,088
network attacks
(123 attacks per device)*

18.7 MILLION
malware variants
(758 variants per device)*

* average per participating device

Get the full Internet Security Report now.

WatchGuard®