Q2 2021 Internet Security Insights

WatchGuard Threat Lab

The WatchGuard Threat Lab team is a group of analytical, science-based threat experts who want to help you truly quantify the cyber threats your business faces. By statistically measuring the most relevant risks, we help you validate your security strategy with practical defense tips and mitigations. Our quarterly Internet Security Report (ISR) contains measurable threat intelligence on the most prevalent and far-reaching malware, the top network attacks seen in the wild, and the common malicious domains victimizing your employees and users.

Malware Trends

The **Firebox Feed** recorded threat data from **37,788** participating Fireboxes

A slight **1%** increase from the previous quarter

Our **GAV** service blocked **9,568,240** malware variants

10% increase in basic malware

APT Blocker detected **6,966,595** additional threats

21% decrease in zero day hits

IntelligentAV blocked **34,687** malware hits

Total IAV detections dropped to just over a fifth of the previous quarter

61.1% OF MALWARE WAS **ZERO DAY**

35.9% OF MALWARE WAS **Known Malware**

High-Level Threat Trends for Q2 of 2021

91.5% of malware detections arrived over an encrypted connection

WatchGuard Firebox appliances blocked an average of **438 malware threats each** in Q2 2021

New and Notable Threats

Let's take a look at a few of the top threats from this quarter's report.

AMSI.disable

This malware family was especially interesting as we found code capable of disabling the Antimalware Scan Interface (AMSI) in Windows. AMSI scans PowerShell scripts, VBA macros, JavaScript and other scripts using the Windows Script Host technology to identify potentially malicious code.

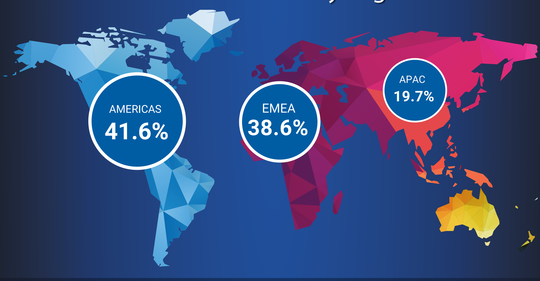
Trojan.AgentWDCR

The AgentWDCR trojan contains a basic downloader. In some of the samples we analyzed, it attempted to contact the domain doc[.]conf1g[.]com and download additional malware. One sample we analyzed downloaded a Monero coinminer. While coinminers aren't nearly as damaging as ransomware, they will slow down your PC and generate more heat, which you may even notice as more fan noise.

Application.Agent.IIQ/JS.Agent.IIQ

We looked deeper into the top malware list, beyond the top 10, and found an interesting sample that recently targeted IoT devices, similar to the New Moon sample from last quarter. The first version of this sample targeted Linux servers running WordPress.

Malware Detection by Region



Win32/Heim.D took the number one spot again this quarter with **1,105,780** detections.

COUNT	THREAT NAME	CATEGORY	LAST SEEN
1,105,780	Win32/Heim.D	Win Code Injection	Q1 2021

Firebox Feed included threats captured from **37,788 Firebox appliances** deployed across the world

In Q2 2021, WatchGuard Fireboxes blocked over **5.2 million** network attacks

137 attacks per device

16.6 million malware variants blocked by WatchGuard in Q2 2021

10% increase in malware

Read the full Internet Security Report at **www.watchguard.com/security-report**

WatchGuard