# Q4 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

**Annual Reporting Fireboxes, Sliding Average**
**76,267**
We now count all Fireboxes reporting in the last year. Quarterly numbers remain unchanged.

**Basic Malware**
**13,071,706**
malware variants
GAV jumped by one-third to one of the highest levels we have seen.

**Evasive Malware**
**10,792,306**
additional threats
An increase of 33% for APT Blocker means more zero day threats than evenr before.

**The Top Malware Detections Included**
**2**
new threat detections, both with code injection capabilities.

**65.6%** OF MALWARE WAS **ZERO DAY**

**34.4%** OF MALWARE WAS **Known Malware**

## High-Level Threat Trends for Q4 of 2021

**Malware increased almost 40 percent quarter over quarter (QoQ),**

Network attack volume reached a four-year high with **~5.7 million network exploits in Q4.**

## New and Notable Threats

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

**Trojan.Agent.FPXV**

This quarter, we detected for the first time a JavaScript malware family called Trojan.Agent.FPXV in the top 5 TLS-encrypted malware. This malware spread with the help of a once-compromised WordPress site. A casual overview of the malware file wouldn't normally raise any alarms.

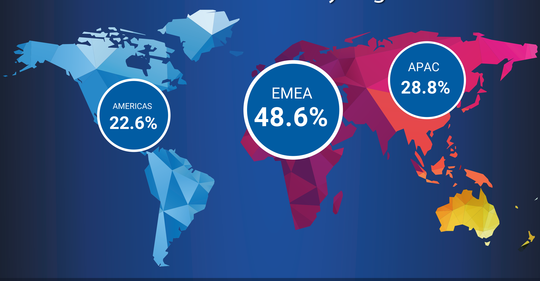
**Zum.Androm**

Fireboxes detected Zum.Androm in the top 10 threats for the first time as well as in the most widespread threats. This malware family and the Trojan.Zmutzy malware have significant overlap but Zum.Androm differs by contacting several domains using the same absolute path (a URL without the domain name).

**Heur.BZC.PZQ.Boxter (nishang)**

Heur.BZC.PZQ.Boxter contains a Debian package used in the Hacking OS Kali. This hacking tool, called Nishang, contains PowerShell scripts to bypass Windows defenses including the use of the same exploits used by Amsi.disable, Mimikatz, and others.

## Malware Detection by Region




Win32/Heim.D took the number one spot again this quarter with **819,287** detections.

| COUNT | THREAT NAME | CATEGORY | LAST SEEN |
|---|---|---|---|
| 724,792 | GenericKD (Adaware) | (PUP) | Q3 2021 |

Firebox Feed included threats captured from **76,267 Firebox appliances** deployed across the world

In Q4 2021, WatchGuard Fireboxes blocked over **5.5 million** malicious domains

**75** attacks per device

**23,864,012**
malware variants blocked by WatchGuard in Q4 2021

**a significant increase** in malware

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

WatchGuard