

# Q2 2017 Internet Security Insights

WatchGuard Threat Lab

If you don't know what your adversary is doing, you won't know how to protect yourself against their attacks.

## Malware Trends

The Firebox Feed recorded threat data from

**33,590** active Firebox appliances

a **21%** increase in devices reporting in Q1 2017.

Our GAV service blocked

**10,919,403** malware variants

a **35%** increase in overall malware compared to Q1 2017.

APT Blocker stopped an additional

**5,484,320** malware variants

a **53%** increase from last quarter.

**47%** OF MALWARE WAS **ZERO DAY Malware**



**53%** OF MALWARE WAS **Known Malware**

The web continues to be the battleground.

Malware detections jumped

**41%**

compared to Q1, 2017

This marks the third quarter where all top ten attacks target web services; both from the **server** and **client side**.

Legacy firewalls are **not enough protection** from today's threats.

Everyone pokes a web hole in their firewall, so you need additional security scanning service, like **IPS**, to **detect web attacks**.

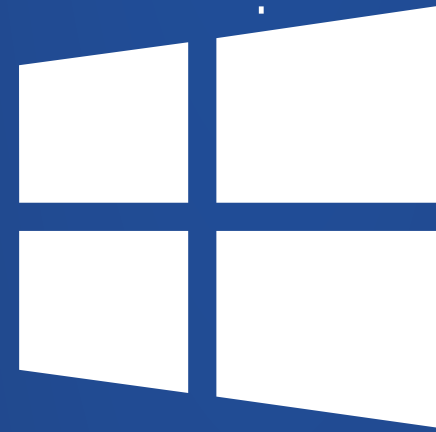
## Trending Threats

### LOGIN/PASSWORD

\*\*\*\*\*

Web-based attacks on authentication

Two different signatures for attacks against authentication in the top 10 network attacks, one covering brute force login attempts and another for remote retrieval of the Linux system password file /etc/passwd.



Basic Windows credential attacks

Slightly over half of the malware delivered via web (HTTP) connections were variations of the "SCGeneric" signature, which primarily matches a tool named **Mimikatz**.



JavaScript via email

A substantial portion of malware delivered via email protocols like SMTP and POP3 is JavaScript-based. JavaScript Downloaders from previous quarters are joined by a new top 10 threat, **JS/Phish** signature.

## WatchGuard for the Win

**2,902,984** network attacks blocked

by WatchGuard in Q2 2017

→ **86** attacks per participating device.



**16,403,723** malware variants blocked

by WatchGuard in Q2 2017

→ **488** variants per participating device.

Read the full Internet Security Report at [www.watchguard.com/security-report](http://www.watchguard.com/security-report)

