Q3 2017 Internet Security Insights

WatchGuard Threat Lab

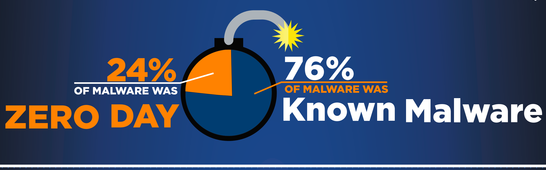
If you don't know your enemy's latest tactics, you can't implement the proper defenses.

Malware Trends

The **Firebox Feed** recorded threat data from **29,934** active Firebox appliances

Our GAV service blocked 19,793,401 malware variants

APT Blocker stopped an additional **3,074,534** malware variants



Web Attacks Still Dominate

Scripting attacks accounted for 68% of total malware hits.

For the past year, web attacks targeting both **web servers** and **client browsers** have **dominated our IPS top ten list**.

Trending Threats

Authentication Remains a High-priority Target

This included both malware that focuses on credentials (Mimikatz), and various network attacks that target credentials or authentication systems.

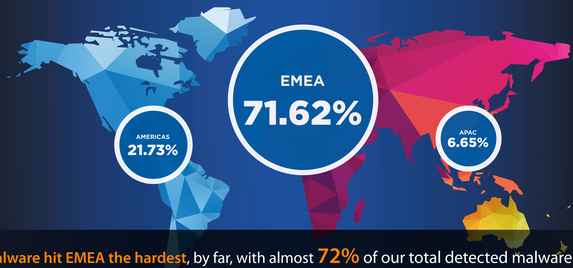
Two XSS Exploits Target Specific Products

Both are titled WEB Cross-site Scripting, but have the numbers 1.x or 36. The 1.x signature detects a web app vulnerability in **SharePoint Foundation 2010**, while the 36 signature catches a flaw in **Adobe's Robo Help**. That said, some XSS signatures are written in a way that they can catch other generic XSS flaws as well.

Criminals DoS Web Servers

One complete newcomer: **WEB Hashtable Collisions** This signature catches an attack designed to cause a **denial of service (DoS)** condition on many web servers.

Malware Detection by Region



Malware hit EMEA the hardest, by far, with almost **72%** of our total detected malware.

The Americas have usually followed EMEA very closely in the past, but dropped to about **22% of the malware** this quarter.

Finally, Asia Pacific only accounted for about **6% of malware**, which is similar to many quarters past.

WatchGuard for the Win

2,902,984
network attacks blocked by WatchGuard in Q3 2017

→ **54 intrusion attempts** per Firebox.

22,867,935
malware variants blocked by WatchGuard in Q3 2017

→ **764** variants per participating **device.**

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

WatchGuard