

The Threat Landscape – Big Numbers

Web Threats

More than 1 Billion

Web requests analyzed each day

Up 3% from 2016

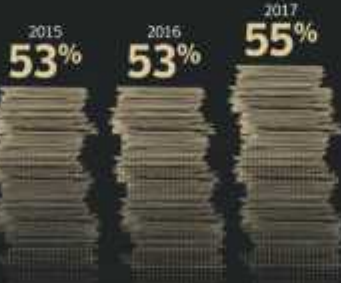
1 in 13

Web requests lead to malware

Up 3% from 2016

Email

Percentage Spam Rate



IoT

600%

Increase in Attacks



Vulnerabilities

Overall increase in reported vulnerabilities

13%

Malware

92%
Increase in new downloader variants

80%
Increase in new malware on Macs

8,500%

Increase in coinminer detections

Ransomware

5.4B

WannaCry attacks blocked

46%

Increase in new ransomware variants

Mobile

Number of new variants

2016
17K

2017
27K

Increase in mobile malware variants

54%

24,000

Average number of malicious mobile apps blocked each day



Increase in industrial control system (ICS) related vulnerabilities

29%

Key Messages

With a low barrier of entry – only requiring a couple lines of code to operate – cyber criminals are harnessing stolen processing power and cloud CPU usage from consumers and enterprises to mine crypto currency.

Symantec identified a **200 percent increase** in attackers injecting malware implants into the supply chain.

The number of new mobile malware variants increase by **54 percent year over year**. The use of older operating systems makes the problem worse.

In the last two years, the profitability of Ransomware led to a crowded market. Now, the market made a correction, lowering the average ransom cost (**average demand \$522**) and signaling that ransomware had become a commodity.

The number of targeted attack groups is on the rise with Symantec now tracking **140 organized groups**. The use of zero days is falling out of favour for Spear Phishing.



Attack Themes

Trust



Infiltration of well-protected organizations by leveraging a trusted channel

Fast



number of infections can grow quickly as users update automatically

Focus



Targeting of specific regions or sectors

Reach



Infiltration of isolated targets, such as those in industrial environments

Hidden



Difficult for victims to identify attacks as trusted processes are hijacked

Privileges



May provide attacker with elevated privileges during installation

Thank You



MENA
INFORMATION SECURITY
CONFERENCE **2018**