

## THREAT LANDSCAPE REPORT Q1 2017

### ATTACK TOOLS— ANYWHERE ANYTIME SERVICE

#### RANSOMWARE EXPANDS

Almost **10%** of organizations detected ransomware activity last quarter

Malicious ransomware like WannaCry can scale-out to hundreds of organizations across the world at once

#### AUTOMATIC ATTACKS

**80%** of organizations reported high-or critical-severity exploits

Distribution was consistent worldwide, likely due to fully automated tools that methodically scan the Internet for opportunities

### MOBILITY ACCELERATES THE SPREAD OF MALWARE

#### MORE MOBILE MALWARE

BYOD policies makes protecting against malware on mobile devices challenging

Its percentage of the

#### TOTAL MALWARE VOLUME

jumped from **1.7%** IN Q4 2016 **TO** **8.7%** IN Q1 2017

#### ANDROID ON THE RISE

**3** families of Android malware broke into the top of the charts

Up from only one in the previous quarter

#### REGIONAL PREVALENCE

Mobile malware prevalence **ROSE IN EVERY REGION** except the Middle East

### DIMINISHING NETWORK VISIBILITY & CONTROL

#### ENCRYPTED TRAFFIC JAM

HTTPS traffic hit a **MEDIAN RATIO OF 55%** this quarter

01 010 1101010 101 0 101011 1011 01 01010

Many defensive tools have poor visibility into encrypted communications to inspect for hidden threats

#### THE CLOUDINESS OF CLOUD APPS

Organizations use a median of

**62 CLOUD APPLICATIONS**

(roughly one-third of all applications detected) with IaaS hitting a new high point

The challenge is that data visibility can drop significantly within the cloud

#### VERTICAL VULNERABILITY

Analysis shows that the attack surface across most vertical industries was the same. Using automated tools, cyber criminals can **EXPLOIT SIMILAR ATTACK SURFACES** more easily.

### WHAT CAN YOU DO?

Most of today's threats are opportunistic.

**For effective protection, security leaders should:**



Review their security posture



Expand visibility and control across distributed networks (from IoT to the cloud)



Minimize the accessible attack surface



Automate—attacks using automated tools require automated responses

**READ THE COMPLETE FORTINET THREAT LANDSCAPE REPORT FOR Q1 2017**

[www.fortinet.com/threatreport](http://www.fortinet.com/threatreport)