2015

Threats Predictions

McAfee Labs

Cyber Espionage

Cyber espionage attacks will continue to increase in frequency.

Gather Intelligence

Long-term players will become stealthier information gatherers.

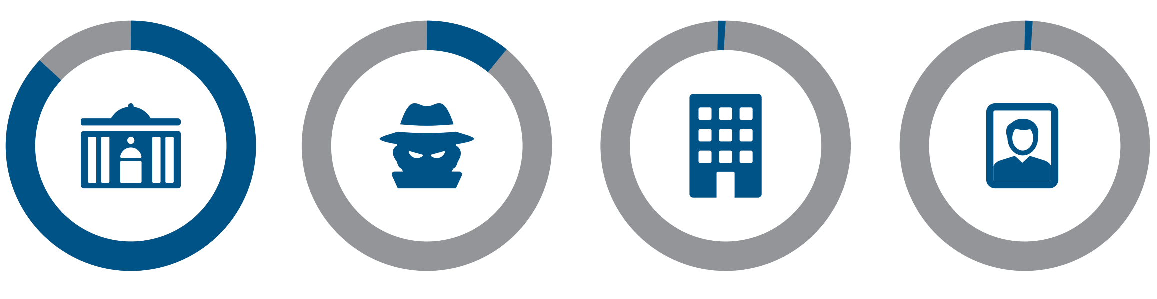
Sophisticated cybercriminals will shift from quick attacks to intelligence gathering.

Steal Money

Newcomers will look for ways to steal money and disrupt their adversaries.

In 2013, there were 511 total cyber espionage incidents, including 306 with confirmed data disclosure.[1]

Types of cyber espionage actors.[2]



87%
State-affiliated

11%
Organized crime

1%
Competitor

1%
Former employee

Internet of Things

Attacks on Internet of Things devices will increase rapidly due to hypergrowth in the number of connected objects, poor security hygiene, and the high value of data on IoT devices.

50 Billion Devices

Over 50 billion global Internet-connected devices **by 2019.[3]**

IoT Devices

Attacks against IoT devices are already commonplace.

- IP cameras.
- smart meters.
- healthcare devices.
- SCADA devices.

A recent study by HP found alarming security statistics in the IoT space. Of 10 popular devices tested:[4]

70%
contained security exposures

25
holes or risks of compromising the home network, on average, found for each device

80%
did not require passwords of sufficient complexity and length

90%
collected at least one piece of personal information

70%
allowed an attacker to identify a valid account through account enumeration

Privacy

Data privacy will remain under threat as governments and businesses grapple with what is fair and authorized access to personal information.

110 Million People

About 110 million Americans—equivalent to **about 50% of US adults—have had their personal data exposed** in some form in the past year.[5]

Regulations

There will be an ever-increasing creep in the scope of **data privacy rules and regulations**.

Passwords

Antiquated role-based systems and **password schemas will fail** and be taken over by those with malicious intent.

Biometrics

Biometrics and IDs in context will be key areas for innovation and likely **the best indicators of presence and intent**.

Ransomware

Ransomware will evolve its methods of propagation, encryption, and targets.

2 Million Samples

The total number of ransomware samples in the McAfee Labs zoo surpassed **2 million in Q3 2014.**

$255,000 Stolen

McAfee Labs observed the theft of **$255,000 in a single month** in one CryptoLocker ransomware instance.

Cloud-based Storage

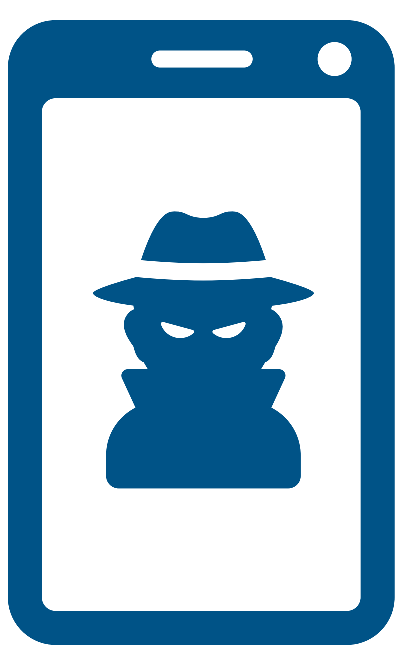
Ransomware will target endpoints that subscribe to cloud-based storage services, attempting to **exploit the stored credentials of logged-on users** to also infect data backed up to the cloud.

Mobile Space

We expect the technique of ransomware **targeting data backed up to the cloud** to be repeated in the mobile space.

Mobile

Mobile attacks will continue to grow rapidly as new technologies expand the attack surface and app store abuse goes unchecked.



Digital Payments

The adoption of **near-field communication (NFC) for digital payments** from mobile devices will attract cyberthieves.

Malvertising

Untrusted app stores will be a major source of mobile malware, driven by "malvertising."

Virtual Currency

We expect a rise in ransomware targeting mobile devices using **virtual currency as the ransom payment method**.

Mobile Malware Kits

The growing availability of malware-generation kits and source code will make it **easier for cybercriminals to target mobile devices**.

Mobile malware samples grew by 16% this quarter and 112% in the past year.

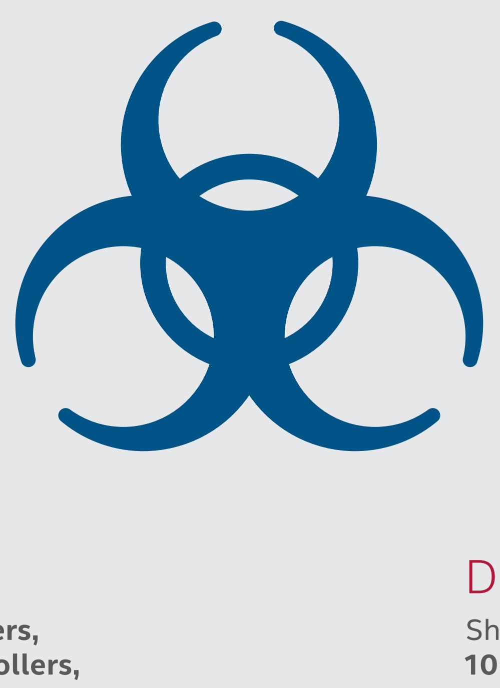
16%
Q3 2014

112%
Q4 2013 – Q3 2014

The total number of mobile malware samples exceeded 5 million in Q3 2014.

Malware Beyond Windows

The Shellshock vulnerability will fuel non-Windows malware attacks that will continue for years.



22,487 Attacking IP Addresses

In the first four days after announcement, **Shellshock-related attacking IP addresses totaled 22,487.**[6]

Devices

Devices such as **routers, TVs, industrial controllers, flight systems, and critical infrastructure** could contain this vulnerability.

Shellshock

Attackers will capitalize on Shellshock by **exfiltrating data, holding systems ransom, and assimilating spam bots.**

Dangerous

Shellshock is rated **10 out of 10 for severity** by the National Vulnerability Database.[7]

Read more about McAfee Labs 2015 Threats Predictions in the November 2014 Threats Report.

Visit www.mcafee.com/November2014ThreatsReport for the full report.

McAfee is now part of Intel Security.

[1] Verizon 2014 Data Breach Investigations Report (DBIR).
[2] Verizon 2014 Data Breach Investigations Report (DBIR).
[3] McAfee, based on research by BI Intelligence, IDC, and Intel.
[4] HP Internet of Things Research Study.
[5] USA Today.
[6] Akamai Security.
[7] The National Vulnerability Database.