McAfee
Together is power.

Threats Report

McAfee Labs

September 2016

Information Theft

The what, how, and who of data leakage.

53%
of breaches are discovered by someone outside the breached organization.

62%
of breaches involve customer or employee personal data.

40%
of data losses involve some type of physical media.

68%
of breaches involve data loss requiring regulatory reporting.

>25%
of companies do not monitor access to employee or customer information.

37%
of companies use endpoint monitoring, including user activity and physical media.

Crisis in the ER

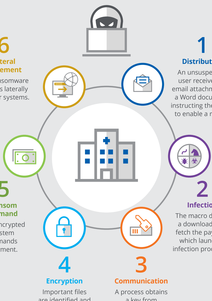
Ransomware infects hospitals.
Ransomware authors target hospitals because...

Legacy Systems
They have legacy systems with weak security.

Medical Devices
They own medical devices with weak or no security.

Patient Care
They need immediate access to information to deliver the best possible patient care.

Stages of a Hospital Ransomware Attack



1 Distribution
An unsuspecting user receives an email attachment as a Word document, instructing the victim to enable a macro.

2 Infection
The macro directs a downloader to fetch the payload, which launches infection processes.

3 Communication
A process obtains a key from an encryption key server.

4 Encryption
Important files are identified and encrypted using the key.

5 Ransom Demand
The encrypted system demands payment.

6 Lateral Movement
The ransomware spreads laterally to other systems.

19 Hospitals
At least 19 hospitals were infected with ransomware in Q1 and Q2.

$17 Thousand
A California hospital in Q1 paid $17,000 to restore its files and systems, suffering a downtime of five working days.

$100 Thousand
McAfee discovered that a related group of Q1 targeted attacks on hospitals generated about $100,000 in ransom payments.

Analytics

Using machine learning to stop attackers.
Machine learning is the action of automating analytics that use computers to learn over time.

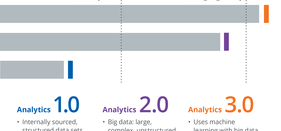
Prescriptive Analytics
"This is what is recommended because that will happen."

Descriptive Analytics
"What happened?"

Predictive Analytics
"What will happen?"

Diagnostic Analytics
"Why did it happen?"

The Evolution of Analytics



Analytics 1.0
- Internally sourced, structured data sets
- Descriptive and diagnostic analytics
- Reactive, but useful

Analytics 2.0
- Big data: large, complex, unstructured
- Data from internal and external sources

Analytics 3.0
- Uses machine learning with big data, deep learning, and cognitive computing
- Fast, proactive discovery and insight

Source: Adapted from the International Institute for Analytics.

Threat Statistics

There are 316 new threats every minute, or more than 5 every second.

↑32%
Malware
The number of new malware samples in Q2—41 million—is the second highest ever tallied. The McAfee Labs malware "zoo" grew 32% in the past year to more than 600 million samples.

↑128%
Ransomware
The number of new ransomware samples—more than 1.3 million—was the highest ever recorded in Q2. Total ransomware has grown 128% in the past year.

↑151%
Mobile Malware
The number of new mobile malware samples—almost 2 million—was the highest ever recorded in Q2. Total mobile malware has grown 151% in the past year.

↑106%
Macro Malware
New downloader Trojans are responsible for the more than 200% increase in new macro malware in Q2. Total macro malware grew 106% in the past year.

McAfee Global Threat Intelligence

McAfee GTI received on average 48.6 billion queries per day.

100 Million
McAfee GTI protections against malicious URLs rose slightly year over year to 100 million per day in Q2.

30 Million
McAfee GTI protections against potentially unwanted programs dropped 83% year over year to 30 million per day in Q2.

104 Million
McAfee GTI protections against malicious files dropped 77% year over year to 104 million per day in Q2.

29 Million
McAfee GTI protections against risky IP addresses show the highest number of protections seen in the last two years, 29 million per day, an increase of 128% quarter over quarter.

Download: *McAfee Labs Threats Report: September 2016*
Visit: www.mcafee.com/September2016ThreatsReport

McAfee
Together is power.