Ransomware – To Pay or Not to Pay

Jim Olmstead
Incident Response Consultant

Ransomware

- What is Ransomware:
  - Malware that Encrypts files that you may or may not be able to decrypt
  - Malware that Encrypts entire hard drive
  - Malware that either exfiltrates your data or hides it from view holds the files/data for ransom

Ransomware

- Where is the Impact:
  - Mostly Windows OS systems
    - Application Servers
    - File Servers
    - Workstations/Laptops/Other
    - Anything on those related system
      - ICS/SCADA Controls
      - Data Stores/Archives
      - Payment Card Industry (PCI) Data
      - Personal Privacy Information (PII)
      - Medical Records

Ransomware

- It is **Prevalent** and **Profitable**
- **If you Pay** the ransom, **you provide an incentive** for the Bad Actors to continue
- Let's try to break the cycle
- Work towards building Resiliency and Reducing Risk Factors
- Work on your plan before the incident occurs.
    - Follow Best Practices
    - Have a standard

Threat Statistics, Q1 to Q2

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

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.**

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.**

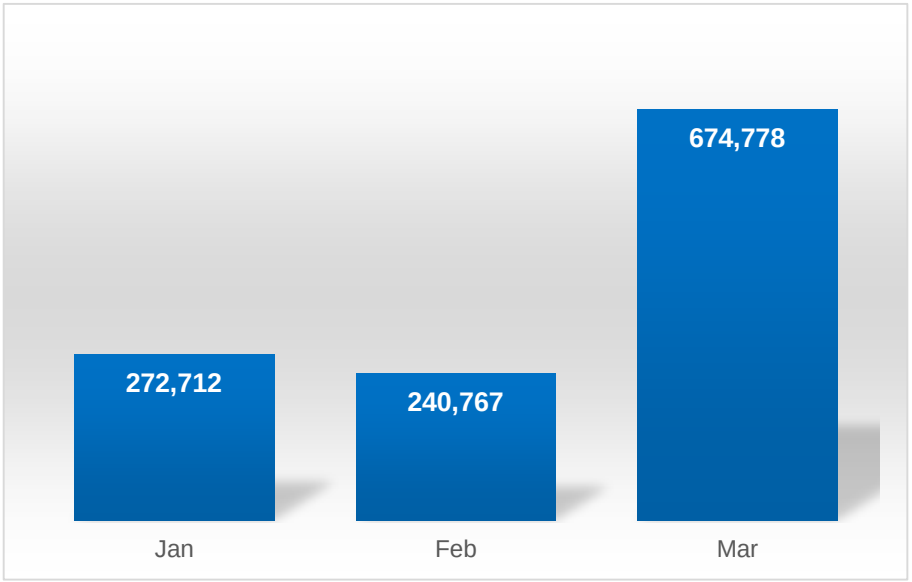
Ransomware

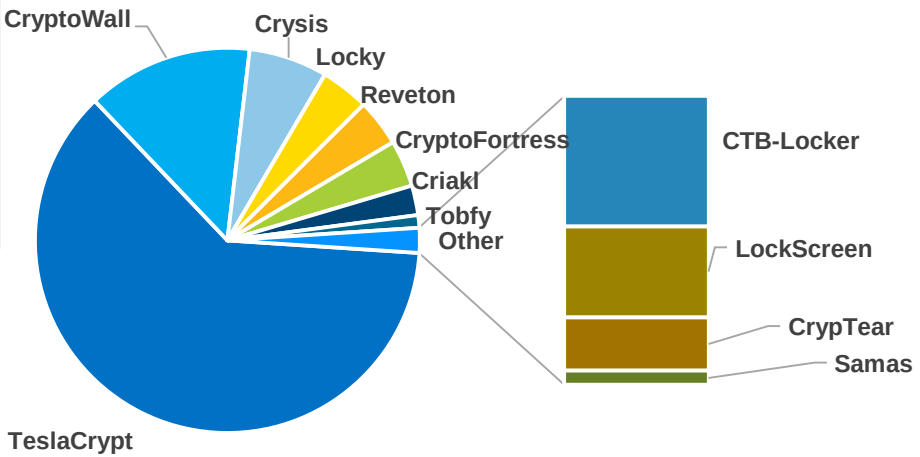
The number of new ransomware samples—more than 1.3 million—was the highest ever recorded in Q2. **Total ransomware has grown 128% in the past year.**

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.**

RansomWare Statistics Q1 - 2016





“Where we started with around 10 families in Jan 2016, Currently we are tracking 57+ different ransomware families..”

World Wide Money
e-gold
www.e-gold.com
Goes out of Business

Bitcoin Invented
2009

CryptoLocker
2013

CTB-Locker
2014

CryptoWall
2014

TorrentLocker
2014

New Event
2014

CryptoDefense
2013

Reveton
2013

Bandarchor
2015

Cryptowall
2015

Ransomware as a Service
2015

AlphaCrypt
2015

TOX
2015

TeslaCrypt
2015

Cryptohasyou
2016

Cerber
2016

Hydracrypt
2016

KeRanger
2016

Kimcilware
2016

LeChiffre
2016

LOCKY
2016

Maktub
2016

Samas
2016

Petya
2016

Troldesh
2016

Ransom32
2016

2009 2010 2011 2012 2013 2014 2015 2016

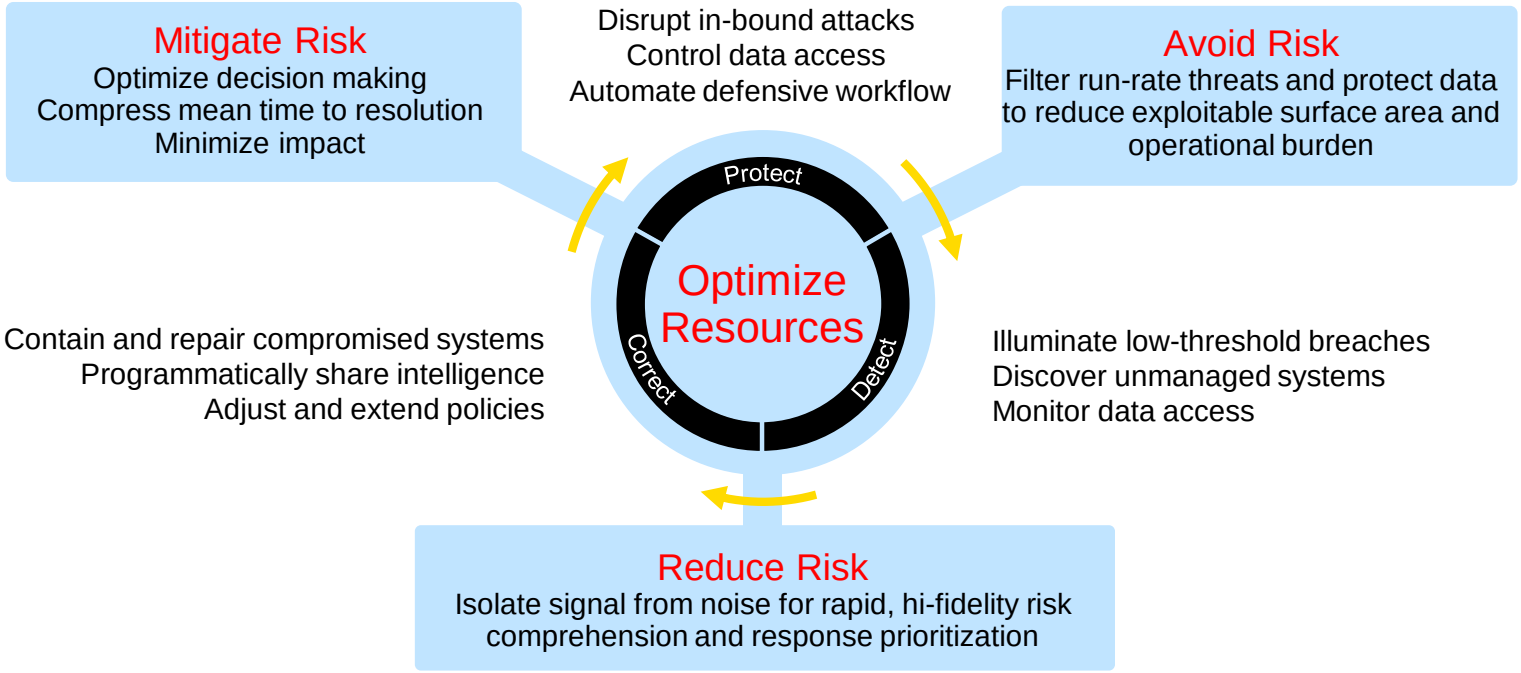
Ransomware Time-Line

Observations in early 2016

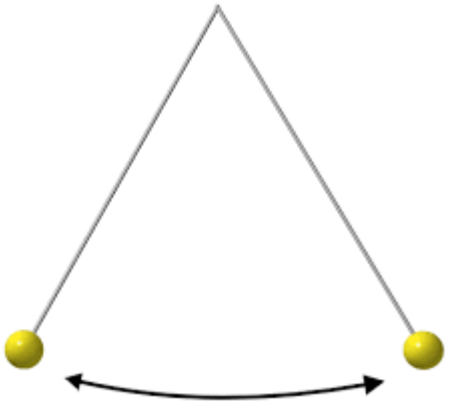
- ***Ransomware as a Service*** **increased massively**
- ***Source-code*** **for ransomware** ***publicly available***
- **Targeted ransomware campaign on mostly Healthcare industry**
- **Ransomware encrypting Master-Boot-Record**
- **Apple users hit with Ransomware**

Threat Defense Lifecycle

Applied integration, automation, and orchestration driving a defense lifecycle

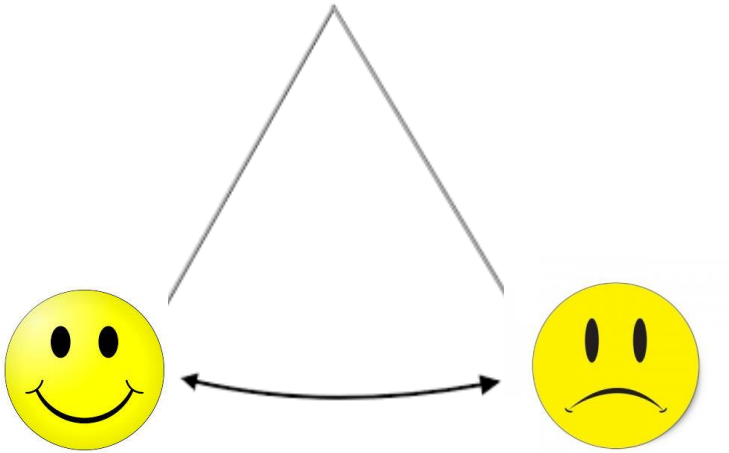


Access vs. Security

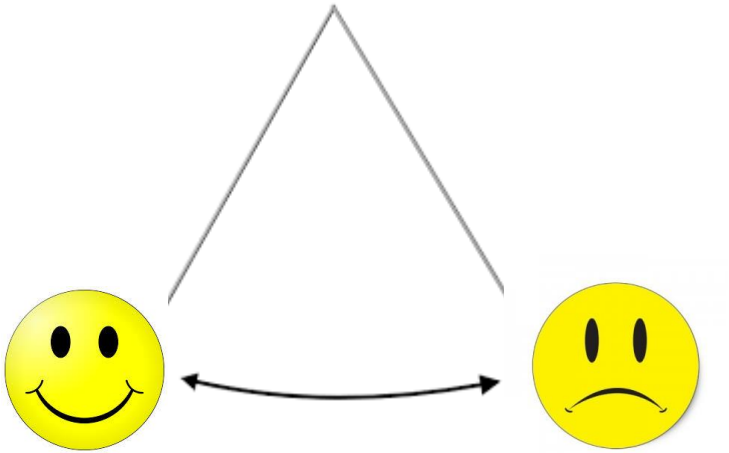


Security Pendulum

Access vs. Security



Access vs. Security



User impact vs Protection of Data

Threat Vectors

- Delivery methods of ransomware
  - Many popular types.. Locky, Teslacrypt, …
    - Exploits weaknesses in your security and unpatched systems
    - Downloaders & Droppers
    - Launched by employees eager to “click” on email

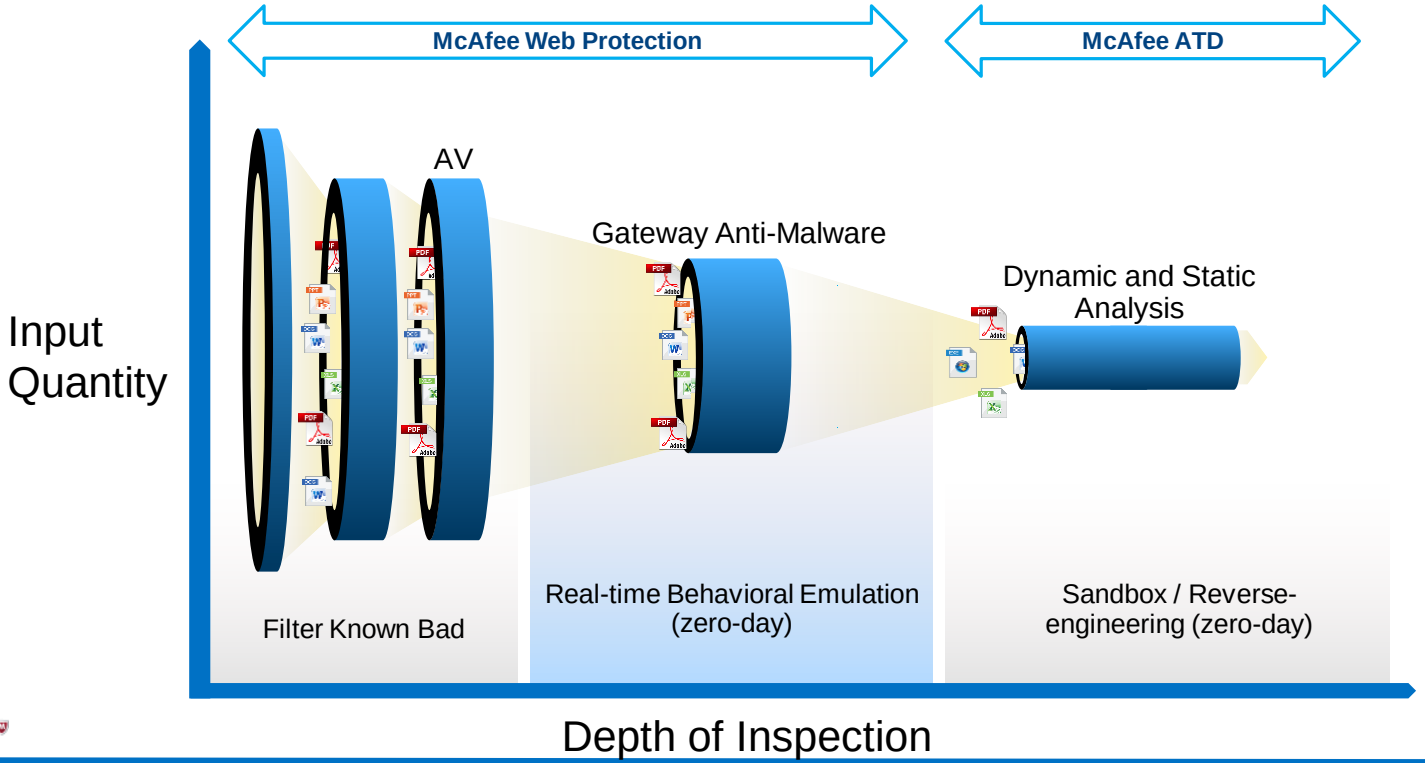
- Compromised websites & Social Media
  - Uncategorized websites
- Email (Mass spam and possible targeted spam)
- Hack and Attack
  - Samsa, Samas (aka, samsam.exe and other variant names)

Secure:

» Computers on your network and under your control (Password & Kerberos Reset)
» 3rd Party Vendor or Unmanaged systems on your network
» Review computers placed in your DMZ and their connectivity back to your network

Protect Recommendations

- Use Web Security to stop threats before they get to the endpoint



Be Ready- Prepare

- Incidents are going to happen
- Incidents are part of doing business
- **Have a Plan** before you have the **Need to Respond**
- Need for an endpoint solution & other security products
- No matter which security product you own… **know how to use it!!**
- Log and report your network and alerts

Response: Be Proactive - Prepare

- Block or reduce access to Open and Mapped Shares
- Disable MS Office Macros
- Update, Upgrade, and patch your Operating System (OS)
- Use Whitelisting / Application Control
- Block and Filter email & attachments
- Remove or reduce Remote Desktop (RDP) use
- Educate your end-users (To be Suspicious of email and attachments)
- Run up-to-date Anti-virus protection & signatures (Use extra.dat's)

How to Reduce Impact of a ransomware attack?

Back-up! Back-up! Back-up! .

- Removable media or tape drives (small)
- USB make sure to disconnect
- Cloud storage (beware)
- Off-site storage which is not mapped or shared

Use robust antivirus software

- Use heuristic scanning
- Use memory and high risk areas
- Scan the full hard drive on a regular basis.

If you discover a rogue or unknown process on your machine, **disconnect it immediately from the internet or other network connections -** this will prevent the infection from spreading.

How to Reduce Impact of a ransomware attack?

- **Keep all the software on your computer up to date.**
  - 3rd Party applications
  - Unsupported Operating Systems are risks
- **Trust no one. Literally.**
  - Contractor & Third Party owned systems
  - BYOD Policies
- **Enable the ‘Show file extensions’ option in the Windows settings on your computer.**

Response: Initial Steps

- If infected, immediately detach the system from your network
  - Physically disconnect system, or use virtual disconnect
    - Host Intrusion Protection System (HIPS) Firewall Policy
      - Automate the response if a detection occurs, or
      - Manually isolate
- Ensure your Anti-Virus Product is up-to-date with signatures
  - Real-time or On-Demand scanning
  - Schedule (Daily) targeted scans
  - Schedule FULL (Daily) workstations and Servers
    - Any excluded systems or portions of systems MUST be scanned
- Access Control Rules
  - Block programs from running in space where they need not run
  - From IOC's specific to the Ransomware block ports, IP's, URL's, etc….

Response: Initial

- Use your Security Applications to identify and remove threats
  - Registry
  - Dependency files not identified by Antivirus application
- Remediate the system or wipe it clean?
- Have you done enough to prepare?

Threat Advisories & White Papers

Combatting_Ransomware: https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/25000/PD25203/en_US/Ransomware_Update_RevJ.pdf

When Minutes Count: http://www.mcafee.com/us/resources/reports/rp-when-minutes-count.pdf

Think Like an Attacker: Six Steps Toward Better Security – Think like an attacker: http://www.mcafee.com/us/resources/white-papers/wp-think-like-an-attacker.pdf

Low Hanging Fruits: The Top Five Easiest Ways to Hack or Get Hacked: http://www.mcafee.com/us/resources/white-papers/foundstone/wp-low-hanging-fruits.pdf

JS/Nemucod https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/26000/PD26309/en_US/McAfee_Labs_Threat_Advisory_JS-Nemucod.pdf

Angler Exploit Kit https://blogs.mcafee.com/mcafee-labs/new-exploit-kits-improve-evasion-techniques/

X97M/Downloader https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/25000/PD25689/en_US/McAfee_Labs_Threat_Advisory-W97MDownloader_X97MDownloader.pdf

L

Jim Olmstead, McAfee

Email: Jim.Olmstead@intel.com
Web: www.foundstone.com