Ransomware – Threats to Storage(NAS/SAN/Cloud) and possible mitigation

Tuesday, May 23, 2017

Anupam Jagdish Chomal
Tech Lead/Principal Software Engineer
DellEMC Isilon

Who am I? – The Eternal Question

- Who am I?
  - Principal software engineer at DellEMC
  - Veritas, LSI, Nevis networks Lineage
  - Mtech Computer Science, IITB
- Why this topic?

Agenda

- How Malware/Ransomware works?
- Types of Ransomware
- Top Ransomwares
- Top research papers in this area
- Top Attacks
- How to protect against Ransomware

How Malware Works

- Exploit a vulnerable application
- A payload is downloaded
- Attacker gets command and control of compromised system
- This allows for privilege escalation and ultimately the acquisition of high value informational assets

How a Malware Infects

- Mutexes are used by malware creators to overcome the effect made by the different instances of the same malware on the system
- When the trojan infects a system, then first of all try to obtain a handle to a “named” mutex, if the process fails, then the malware exits
- One of the easiest way to check whether mutex is present is “CreateMutex Function”. This function is used by malwares for checking if the system is infected so one approach to detect the presence of existence of malware is trying to obtain a handle to the created mutex

What are Attack Vectors?

- An attack vector is a path or means by which a hacker (or cracker) can gain access to a computer or network server in order to deliver a payload or malicious outcome.
- Attack vectors enable hackers to exploit system vulnerabilities, including the human element.
- Attack vectors include viruses, e-mail attachments, Web pages, pop-up windows, instant messages, chat rooms, and deception.

Types of Ransomware

- There are basically two types of Ransomware
  - Locker Ransomware
  - Crypto Ransomware
- In memory Ransomwares

Top Ransomwares of 2016

- WannaCry
- Locky
- CryptoWall
- SamSam
- Jigsaw
- Chimera

https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/top-10-ransomware-strains-2016/

Wannacry (Source - Kaspersky Lab)

- In these attacks, data is encrypted with the extension ".WCRY" added to the filenames
- The attack, dubbed "WannaCry", is initiated through an SMBv2 remote code execution in Microsoft Windows
- This exploit (codenamed "EternalBlue") has been made available on the internet through the Shadowbrokers dump on April 14th, 2017 and patched by Microsoft on March 14
- Unfortunately, it appears that many organizations have not yet installed the patch

Wannacry - Contd

- Unpatched Windows computers exposing their SMB services can be remotely attacked with the “EternalBlue” exploit and infected by the WannaCry ransomware
- For command and control, the malware extracts and uses Tor service executable with all necessary dependencies to access the Tor network
- https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/

Wannacry - Contd

Best Papers – Cutting the Gordian Knot: A look under the hood of Ransomware attacks

- **Kharraz, Amin; Robertson, William; Balzarotti, Davide; Bilge, Leyla; Kirda, Engin**
- DIMVA 2015, 12th Conference on Detection of Intrusions and Malware & Vulnerability Assessment, July 9-10, 2015, Milan, Italy
- http://www.eurecom.fr/en/publication/4548/download/rs-publi-4548.pdf

PayBreak: Defense Against Cryptographic Ransomware

- Eugene Kolodenker Boston University & MITRE, Boston, MA, USA
- Proceeding - ASIA CCS '17 Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security

UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware

- Amin Kharaz and Sajjad Arshad, *Northeastern University;* Collin Mulliner, *Square, Inc.;* William Robertson and Engin Kirda, *Northeastern University*
- *August 2016 – USENIX Security Symposium*
- https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_kharraz.pdf

CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data

- Nolen Scaife - University of Florida
- Henry Carter - Villanova University
- 2016 IEEE 36th International Conference on Distributed Computing Systems
- https://www.cise.ufl.edu/~traynor/papers/scaife-icdcs16.pdf

Top Attacks

- Attack against UK hospital system (NHS) http://phishing.it.umn.edu/2017/05/krebs-uk-hospitals-hit-in-widespread.html
- Hollywood Presbyterian Medical Center - After the hospital's network data was encrypted, they were forced to pay 40 bitcoins, or about $17,000 dollars to decrypt the data
- San Francisco Metro System - http://thehackernews.com/2016/11/transit-system-hacked.html
- The IOT Ransomware threat https://iotsecurityfoundation.org/the-iot-ransomware-threat-is-more-serious-than-you-think/

How to Protect?

- Plan for the possibility
- Backup regularly – but caution
- Patch all systems regularily
- Use a firewall
- Antivirus(Signatures) and Machine learning
- Best Practices
  - Check for permissions. Read-Only when write not needed
  - Review access control settings
  - Don’t give administrative privileges when not needed

References

- http://www.business-standard.com/article/economy-policy/how-hackers-are-minting-digital-cash-through-global-ransomware-attacks-117051700151_1.html
- http://blog.checkpoint.com/2017/03/22/ransomware-not-file-encryption/
- https://www.sans.org/reading-room/whitepapers/incident/deployment-flexible-malware-sandbox-environment-open-source-software-36207