Topics in Privacy & Security

Ransomware

Y1481702

March 5, 2018

Contents

1 Technical Report

1.1 Introduction

2017 saw a significant rise in frequency of ransomware attacks[cite], with WannaCry[1, 2] and NotPetya[3] being two particularly damaging examples. These attacks becoming more prevalent is likely driven by the rise of untraceable cryptocurrencies (such as bitcoin) which allows easy money laundering as more devices become dependent on complex software and IOT
Ransomware FALLS under the category of a VIRUS as it is self-multiplying and can infect the host program (i.e. OS, documents, etc.)
The main aim of ransomware is for users to be denied access to services that are so vital they will pay to avoid the inconvenience that this lack of access causes. This violates the security goal of availability For obvious reasons, timely access to medical data may be the difference between life and death for some patients.
As with other criminal ransom acts, there is absolutely no guarantee that paying the ransom will return the files successfully. As such, this kind of attack also violates the goal of integrity as data and software is irreversibly modified.
It should be noted that while ransomware does not specifically threaten the goal of privacy and confidentiality, it could be used to disguise some form of dual layer attack which does.
-McAfee Labs 2018:[4] "cyber sabotage and disruption of organisations" profit is the key driver of ransomware: criminals aim to make money from inconveniencing a user
criminals will focus on: inconvenience and disruption through dos rather than malicious fatal damage specifically those who can AFFORD to pay to quickly recover from the attack
-Cyber Security Breaches Survey 2017[5] ransomware has highlighted the VALUE of any electronic data other than personal/financial data the value of this data for health organisations was likely ALREADY known
Can enter a system in the same way as other forms of malware by phishing by baiting (infected USB drives, etc.)
can spread by downloads (as above) or self-replication via internal or external networks

1.2 Prevent

Install latest security updates for OS / Software Tight access control (read access only where necessary) should minimize access of users to corrupt data

1.3 Detect

Security controls can be employed to detect ransomware. In particular, detecting altering of files-ransomware may attempt to modify ANY/ALL files on the system Detect virus signatures, actions beyond specifications, statistical changes?
Anti-virus software (keeping it up to date regularly)
Once an attack has been discovered, all affected PCs and network connections from them should be shut down immediately.

1.4 Recover

regular (OFFLINE) back ups while regular backups must be kept as a last resort, prevention and detection is preferable as recovery from a backup may take considerable amounts of time for large data AND aiming to stop access to data

2 Email

2.1 Memo

200,000 computers across 150 countries (Europol)[1] 48 NHS trusts hit[2]

2.2 Justification

refer to BS EN ISO standards relate this to the technical report in previous section
As analogy has been used to help the users relate to the explanation

3 References

[1] Reuters Staff, "Cyber attack hits 200,000 in at least 150 countries: Europol," *Reuters*, May 2017. [Online]. Available: https://www.reuters.com/article/us-cyber-attack-europol/cyber-attack-hits-200000-in-at-least-150-countries-europol-idUSKCN18A0FX [Accessed: 5 Mar. 2018]

[2] BBC, "Cyber-attack: Europol says it was unprecendented in scale," *BBC News*, May 2017. [Online]. Available: http://www.bbc.co.uk/news/world-europe-39907965 [Accessed: 5 Mar. 2018]

[3] A. Griffin, "'petya' cyber attack: Chernobyl's radiation monitoring system hit by worldwide hack," *The Independent*, Jun. 2017. [Online]. Available: http://www.independent.co.uk/news/world/europe/chernobyl-ukraine-petya-cyber-attack-hack-nuclear-power-plant-danger-latest-a7810941.html [Accessed: 28 Feb. 2018]

[4] McAfee Labs, "McAfee Labs 2018 Threats Predictions Report," Nov. 2017.

[5] Department for Culture, Media & Sport, "Cyber Security Breaches Survey 2017," Apr. 2017.

4 Appendix