APNIC 50

APNIC – FIRST Security 2
Track 01

Enterprise Ransomware: Sri Lankan Case Studies

by TechCERT

TechCERT
HELPING YOU SECURE YOUR INFORMATION ASSETS

Who am I?

- Kalana Guniyangoda
- Lead Security Engineer – Digital Forensic Investigations
- kalana@techcert.lk

Outline

- Enterprise Ransomware
- Case studies
- Takeaways

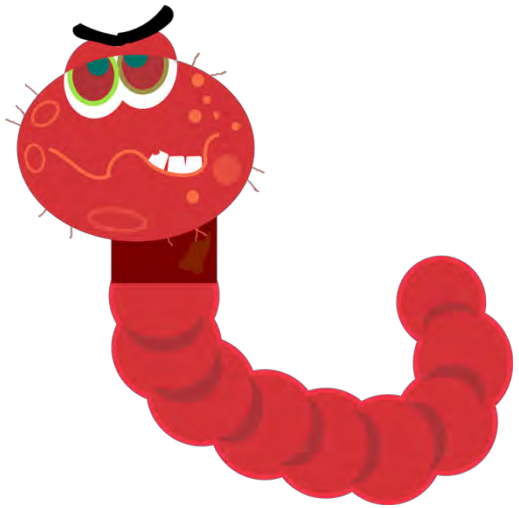
Enterprise Ransomware

- Prior to 2018 it's only a gullible user.

Credit: John Klossner, jklossner.com

Enterprise Ransomware

- Prior to 2018
  - It’s just one or two computers
  - More user awareness sessions recommended
  - Can become nasty with wormable vulnerability:
    - WannaCry



TechCERT

Enterprise Ransomware

- But after 2018…
  - Starts with a sophisticated targeted attack on your network.
  - Longer dwell time
  - Infiltrate the network as much as possible
  - Data exfiltration used to force victims into paying the ransom

Case 01

- Year : 2019
- Ransomware: GandCrab
- Network : Critical network segment

- Initial Access : RDP brute forcing
  - Weak password
  - FW rule change exposed the server
- Not in a Domain
  - Reuse password for a privileged account
  - Attacker jumped from server to server
- Attack only lasted for two days

Case 02

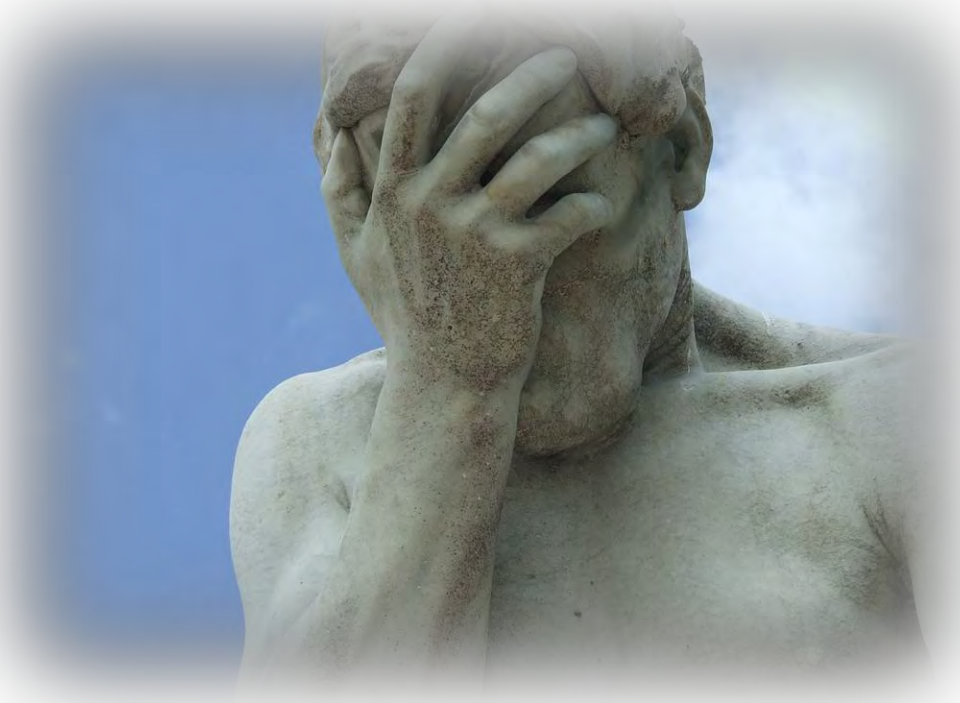
- Year : 2020
- Ransomware: Sodinokibi
- Network: IT Operations

- Initial Access : Citrix VDI account compromise
  - WFH restrictions kicks in
  - Unclear how the passwords leak
- Gain access to Domain Account
  - Used Mimikatz & Bloodhound
- Lateral movement through RDP
  - Goal was to own Domain Controller

TechCERT

Case 02 – Continued…

- Domain Controller
  - Used for network enumeration
  - Had Internet connection
  - Pushed a scheduled task to download and run ransomware
- Dwell time : 5 days
- Alerts from security controls
  - No one noticed



TechCERT

Case 03

- Year : 2020
- Ransomware: Sodinokibi
- Network : IT Operations

- Initial Access : Web server compromise
  - Development errors/ Lack of VA
  - Network not segmented properly
- Lateral Movement
  - Use of ‘BlueKeep’ vulnerability
  - AV server capability to deploy executable

Case 03 – Continued…

- Alerts from security control
  - Attacker created an account in DC
- Weeks long IR battle ensues
  - Attacker switched to Living of the Land techniques
- Persistence
  - Backdoor malware
  - Web Shells
- Issues
  - Poor network segmentation
  - Internet access (even Domain Controller?)
- Outcome
  - Attacker only able to execute on leaf nodes

Takeaways…

- Hackers are always probing your network
  - Sooner or later they will find a way in
- Get your security controls in line.
  - Proper configuration is essential
  - Do red team exercises and check effectiveness
  - Consider the possibility of 24/7 monitoring
- Conduct VA/PT
  - Helps to identify loop holes
- Network segmentation
  - Idea is to stop lateral movement

Takeaways…

- Offline backups are a must
  - Attackers actively search for backups and deletes
- Security hardening for critical servers
  - Internet access for DC?
  - Remote administration service?
  - Application whitelisting
  - Privilege separation
  - Patch management
- Threat hunting/ Compromise assessment
  - Your network already compromised?
- Incident Response Plan

TechCERT

TechCERT

Helping You Secure Your Information Assets