Preparation 1

- A good knowledge of the usual operating systems security policies is needed.
- A good knowledge of the usual users' profile policies is needed.
- Ensure that the endpoint and perimetric (email gateway, proxy caches) security products are up to date
- Since this threat is often detected by end-users, raise your IT support awareness regarding the ransomware threat
- **Make sure to have exhaustive, recent and reliable backups of local and network users' data**

Identification 2

General signs of ransomware presence

Several leads might hint that the system could be compromised by ransomware:

- Odd professional emails (often masquerading as invoices) containing attachments are being received
- A ransom message explaining that the documents have been encrypted and asking for money is displayed on user's desktop

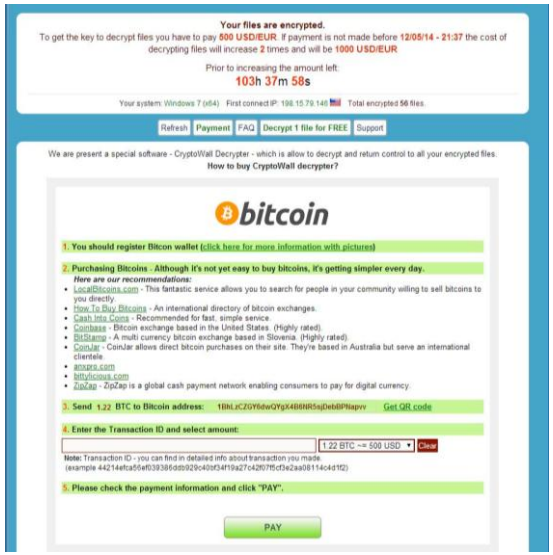

Figure 1 - Cryptowall ransom message

- People are complaining about their files not being available or corrupted on their computers or their network shares with unusual extensions (.abc, .xyz, .aaa, etc..).
- Numerous files are being modified in a very short period of time on the network shares

Identification 2

Host based identification

- Look for unusual executable binaries in users' profiles (%ALLUSERSPROFILE% or %APPDATA%) and %SystemDrive%
- Look for the aforementioned extensions or ransom notes
- Capture a memory image of the computer (if possible)
- Look for unusual processes
- Look for unusual email attachment patterns
- Look for unusual network or web browsing activities; especially connections to Tor or I2P IP, Tor gateways (tor2web, etc) or Bitcoin payment websites

Network based identification

- Look for connection patterns to Exploit Kits
- Look for connection patterns to ransomware C&C
- Look for unusual network or web browsing activities; especially connections to Tor or I2P IP, Tor gateways (tor2web, etc) or Bitcoin payment websites
- Look for unusual email attachment patterns

Containment 3

- Disconnect all computers that have been detected as compromised from the network
- If you cannot isolate the computer, disconnect/cancel the shared drives (NET USE x: \\unc\path\ /DELETE)
- Block traffic to identified ransomware's C&C
- Send the undetected samples to your endpoint security provider
- Send the uncategorized malicious URL, domain names and IP to your perimetric security provider

Remediation 4

- Remove the binaries and the related registry entries (if any) from compromised profiles (%ALLUSERSPROFILE% or %APPDATA%) and %SystemDrive%
- If the above step is not possible reimage the computer with a clean install

Recovery 5

Objective: Restore the system to normal operations.

1. Update antivirus signatures for identified malicious binaries to be blocked
2. Ensure that no malicious binaries are present on the systems before reconnecting them
3. Ensure that the network traffic is back to normal
4. Restore user's documents from backups

All of these steps shall be made in a step-by-step manner and with technical monitoring.

Aftermath 6

Report

An incident report should be written and made available to all of the stakeholders.

The following themes should be described:

- Initial detection.
- Actions and timelines.
- What went right.
- What went wrong.
- Incident cost.

Capitalize

Actions to improve malware and network intrusion detection processes should be defined to capitalize on this experience.

IRM #17

Ransomware

Guidelines to handle and respond to ransomware infection

Abstract

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue.
Who should use IRM sheets?

- Administrators
- Security Operation Center
- CISOs and deputies
- CERTs (Computer Emergency Response Team)

Remember: If you face an incident, follow IRM, take notes. Keep calm and contact your business line's Incident Response team or CERT immediately if needed.

Incident handling steps

6 steps are defined to handle security Incidents

- **Preparation: get ready to handle the incident**
- **Identification: detect the incident**
- **Containment: limit the impact of the incident**
- **Remediation: remove the threat**
- **Recovery: recover to a normal stage**
- **Aftermath: draw up and improve the process**

IRM provides detailed information for each step.