## Preparation

-

- 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

#### 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

<text><text><text><text><text><text><text></text></text></text></text></text></text></text>	o ge	Your files are encrypted. t the key to decrypt files you have to pay 600 USD/EUR IF payment is not made before 12/05/14 - 21:37 the cost decrypting files will increase 2 times and will be 1000 USD/EUR
<text><text><text><text><section-header><list-item><list-item><section-header><section-header><section-header></section-header></section-header></section-header></list-item></list-item></section-header></text></text></text></text>		Prior to increasing the amount left: 103h 37m 58s
Yearen         Yearen         Yearen Y		Your system: Windows 7 (x64) First connect IP: 198.15.79.148 Mill Total encrypted 56 files.
<text></text>		Refresh Payment FAQ Decrypt 1 file for FREE Support
<image/> <section-header><section-header><section-header><section-header><section-header><section-header><list-item><list-item><list-item><list-item><section-header></section-header></list-item></list-item></list-item></list-item></section-header></section-header></section-header></section-header></section-header></section-header>	We	are present a special software - CryptoWall Decrypter - which is allow to decrypt and return control to all your encrypted files. How to buy CryptoWall decrypter?
1. You should register Discon wallet (click here for more information with pictures)     1. You should register Discon wallet (click here for more information with pictures)     1. You should register Discon wallet (click here for more information with pictures)     1. You should register Discon wallet (click here for more information with pictures)     1. You should register Discon wallet (click here for more information with pictures)     1. You should register Discon wallet (click here for more information with pictures)     1. You should register Discon wallet (click here for the pictures)     1. You should register Discon wallet (click here for the pictures)     1. You should register Discon wallet (click here for the pictures)     1. You should register Discon wallet (click here for the pictures)     1. You should register Discon wallet (click here for the pictures)     1. You should register Discon wallet (click here for the pictures)     1. You should register Discon wallet (click here for the pictures)     1. You should register Discon wallet (click here for the pictures)     1. You should register Discon wallet (click here for the pictures)     1. You should register Discon wallet (click here for the pictures)     1. You should register Discon wallet (click here for the pictures)     1. You should register Discon wallet (click here for the pictures)     1. You should register Discon wallet (click here for the pictures)     1. You should register Discon wallet (click here for the pictures)     1. You should register Discon wallet (click here for the pictures)     1. You should register Discon wallet (click here for the pictures)     1. You should register Discon wallet (click here for the pictures)     1. You should register Discon wallet (click here for the pictures)		<b>O</b> bitcoin
Processing Biocles: Advances for the type blockink, it's getting simpler every day. <i>International Concemendations</i> acconcemendations     acconcemendation     acconcemendations     acconcemendations     acco		1. You should register Bitcon wallet (click here for more information with pictures)
Send 1:22 BTC to Discoin address: 1DIALCZOYMouCY5x600005upbet@Hapvr Get.DB code      Enter the Transaction ID and select amount:      E22 BTC == 500 USD      Enter      Meter Transaction IC -you can find in detailed infe about transaction you made     (example 42) feedadent030000020-0012411/022/42017fcfcca2a00114-04/dp)     Select Transaction C -you can find in detailed infe about transaction you made     (example 42) feedadent030000020-0012411/022/42017fcfcca2a00114-04/dp)     Select Transaction C -you can find in detailed infe about transaction you made     (example 42) feedadent030000020-0012411/022/42017fcfcca2a00114-04/dp)     Select Transaction C -you can find in detailed infe about transaction you made     (example 42) feedadent030000020-0012411/022/42017fcfcca2a00114-04/dp)		2. Purchasing blackow: Athloigh Int net yet easy to by hitcomi. It's getting simpler every day. Localizing Lance, The Bertascie and easies any to be set for begets in year community using to sell blackow to you denty. Directly and the set of the the set of the set of the Distance - Recting Set of the set of the Distance - Recting Set of the set of the Distance - Recting Set of the set of the Distance - Recting Set of the set of the Distance - Recting Set of the set of the Distance - Recting Set of the set of the Distance - Recting Set of the
Enter the Transaction ID and select amount     T22 BTC ~= 500 USD      Comment     Inter Transaction (D -yee can thick in detailed into about transaction yee made     reemper 4421 Hetadolet(3)3940000204910341119247421011542480811444110)     Planase richet kan assembli Information and riche "PW"		Annue (Chertele     Annue (Chertelee)     Annue (Ch
122 BTC ~= 500 USD *         Class           Note: Transaction ID - 100 can find in detailed info about transaction you made.         (ceample 44214etx856t139386cdb920c-480541918274-68716414512)           2         Please check the assembling to find and click "PAT".         (Ceample 44214etx856t139386cdb920c-480541918274-68716414512)		clenene. Matazza Gan Mittologua Gan Subgazz - Jabba v a global cash payment network enabling consumers to pay for digital currency: 3. Send 1.32 BTC to Blacoin address: 18h1;xC2076ac0794400784000 Gent GBC code
Nees: Transaction ID - you can find in detaine into about transaction you made (example 442144ta56et039386d5929c40bt73419a27c2870f50fa2a86114c4d1t2)) S. Please check the payment information and click "PAY".		Centerie. Marcas cam Mitchicous com Mitchicous com Angelan - Zhapa - Zhapa is a global cash payment network enabling consumers to pay for digital currency. 2. Send 1.22 BTC to Bhosin address: 11hit.x220r/dev/07p4408054pbe80Phapyr Get DR code 4. Enter the Transaction ID and select amount:
5. Please check the payment information and click "PAY".		Clerence.  ExatUSE.SED EXATUSE CONTRACTOR OF
		Clenete.  Clenet
		Clerente.  ExatUSE SERIE EXAMPLE SERIE SERIES SERIE
PAY		Clerene.  Destant and the second seco

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

2

# Identification

#### 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

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

- 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

#### 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

#### 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

6

- 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.