# Ransomware incident handling and mitigation

Csaba VIRÁG – Cyber Security Competence Centre

# Portfolio – Cyber Security Services

## Preventive (Proactive) Defence

- APPLIED INTELLIGENCE or CTI (CYBER THREAT INTELLIGENCE)
- AWARENESS
- ETHICAL HACKING
- GAMIFICATION
- CYBER EXERCISES

## Managed Security Services

- MONITORING
- LOG MANAGEMENT
- INCIDENT MANAGEMENT
- VULNERABILITY MANAGEMENT
- APT and ZERODAY MANAGEMENT

## Incident Response

- INCIDENT INVESTIGATION
- COMPUTER AND NETWORK FORENSICS
- MALWARE ANALYSIS

## Mitigation

- RISK AND IMPACT MITIGATION
- SYSTEM HARDENING
- SOFTWARE REFACTORING

## Information Exchange

- EARLY WARNING (VULNERABILITY INFORMATION EXCHANGE)
- BUSINESS PROCESS REENGINEERING
- TEAM DEVELOPMENT
- DECISION SUPPORT
- 3rd PARTIES IIEX

CyberServices

# Advanced Cyber Security Services Portfolio

## Proactive and Active Defence

- APPLIED INTELLIGENCE (CTI)
- AWARENESS
- ETHICAL HACKING
- REPUTATION MANAGEMENT
- GAMIFICATION
- CYBER EXERCISES

## Managed Security Services

- MONITORING
- LOG MANAGEMENT
- INCIDENT MANAGEMENT
- VULNERABILITY MANAGEMENT
- APT and 0day MANAGEMENT

## Incident Response

- INCIDENT INVESTIGATION
- COMPUTER AND NETWORK FORENSICS
- MALWARE ANALYSIS

## Mitigation

- RISK AND IMPACT MITIGATION
- SYSTEM HARDENING
- SOFTWARE REFACTORING

## Information Exchange

- EARLY WARNING
- BUSINESS PROCESS REENGINEERING
- TEAM DEVELOPMENT
- DECISION SUPPORT
- 3rd PARTIES IIEX

## Strategic Planning

- POLICY DEVELOPMENT
- CYBER DEFENCE MANAGEMENT SUPPORT AND CONSULTING

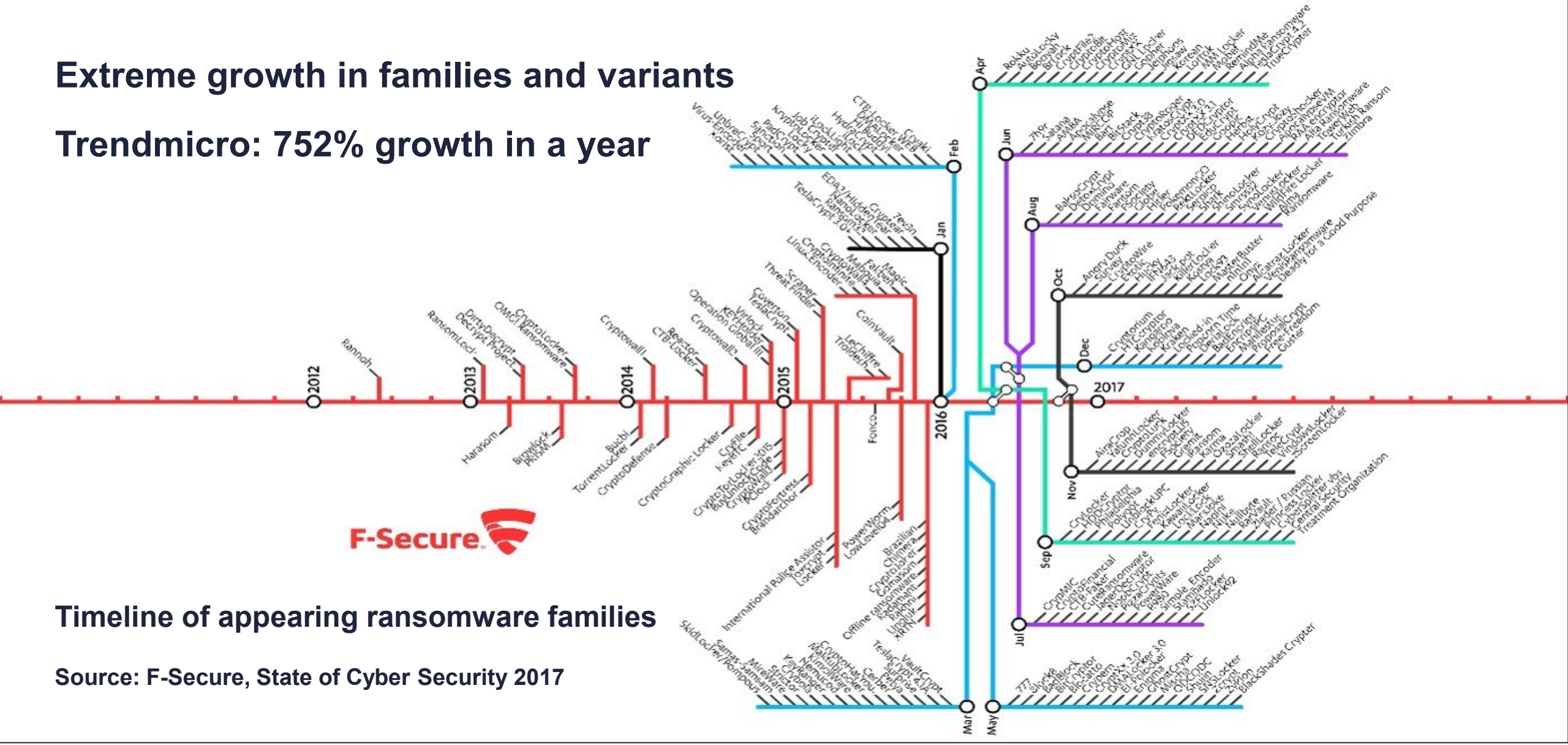
## Research and Development

- STARTUP INCUBATION
- AUTOMATED METHODS DEVELOPMENT
- BIGDATA ANALYSIS DEVELOPMENT

# Ransomware families

**Extreme growth in families and variants**

**Trendmicro: 752% growth in a year**




**Timeline of appearing ransomware families**

**Source: F-Secure, State of Cyber Security 2017**

# Questions

How can such a great threat be handled?

What is the most important measure to take when a ransomware attack is on?

How do you know who attacks and what method the attacker uses?

Why not to pay ransom? If one does not pay, how can it be guaranteed that the files can be restored?

How does a ransomware attack look like?

CybeServices MADE IN EUROPE

# Ransomware Cyber-kill Chain

The ransomware executable is delivered via

- Attachments or web links in phishing emails
- Malvertising on malicious web pages
- Drive-by downloads (e.g. fake antivirus)

↓

The payload is executed on the end user's device

↓

The ransomware installs itself on the victim's computer

↓

The ransomware generates a unique encryption/decryption key pair

↓

The ransomware contacts a C2 server on the Internet to deposit the decryption key

↓

The malware starts encrypting the files on the hard disk, mapped network drives and USB devices with the encryption key

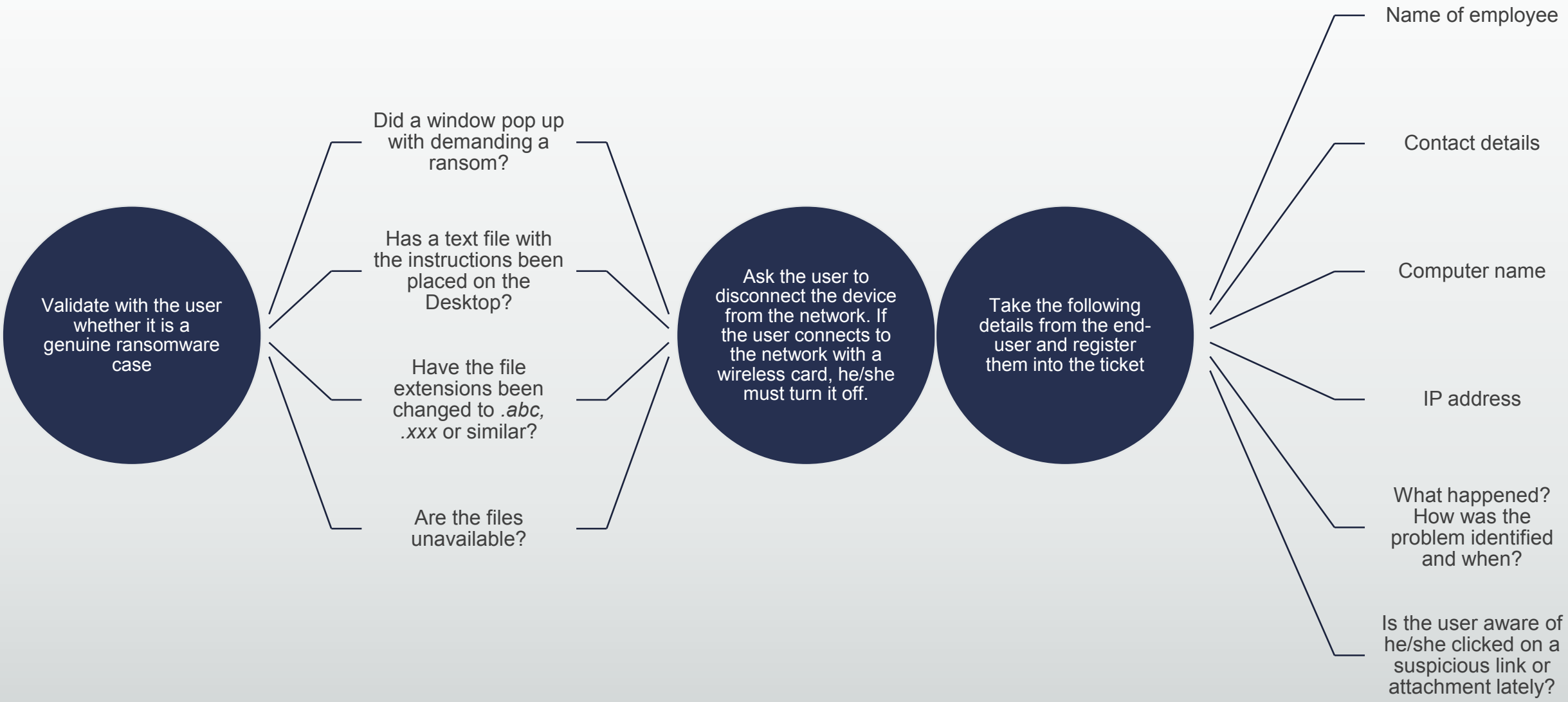
↓

Once the process finishes, the files become inaccessible.

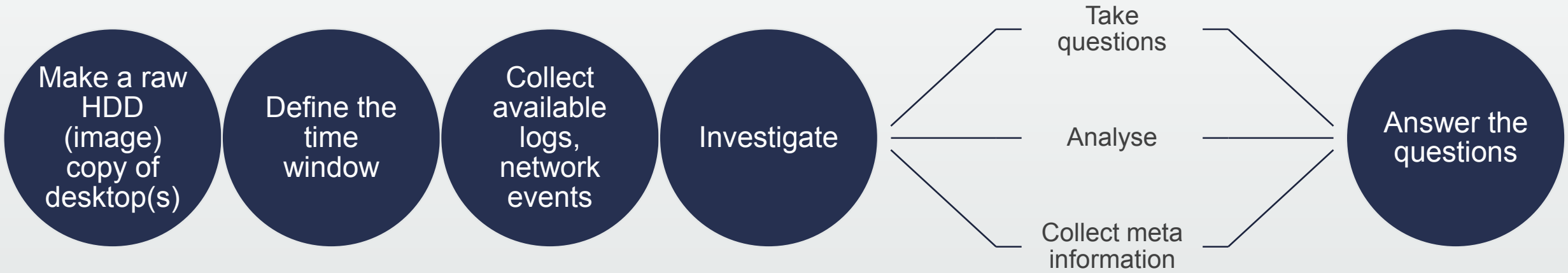
The malware places a text file on the desktop and/or a splash screen pops-up with the instructions to pay and restore the original files.

CybeServices MADE IN EUROPE

# Incident handling procedure



# Incident handling procedure



# Some questions to ask

## Some questions to ask a national CERT tasked by examining received files from an incident.

- What happened at these organisations?
- When did it happen?
- What kind of company assets have been involved?
- Which files can be evaluated?
- Which traces can be the ones originating from the attacker(s)?
- What is the timeline of events recorded?
- What is the attack vector?
- Are there possible further victims?
- Shall one pay for restoring the files to keep operations running? Has the attacker used a C&C (Command and Control) Server?
- Based on the analysis of the malicious files is it possible to restore the files by getting passwords or keys from the attacker?

# Recommendations

- Block incoming emails on the SMTP server, remove emails from user inboxes, warn users to not click on certain links and attachments
- Block malicious URLs on the web proxy, identify computers that visited malicious websites on certain URLs using the proxy logs
- Block malicious URLs on the web proxy, identify computers that visited malicious websites using the proxy logs, deploy custom AV signatures to block certain files to be downloaded, identify PCs with ETDR that downloaded files with certain IoCs
- Apply application whitelisting, identify PCs using the HIDS logs that executed certain files
- Identify and/or block traffic on NIDS and on the proxy(ies)
- Monitor end-user devices and shared folders for certain file extensions, such as .abc, .xxx, .yyy, .zzz
- Monitor endpoints for ransomware related text or HTML files in the desktop folder

| Program Name | Free | Beta | Ransomware | Real-time Protection | Disinfection | Supported OS | Comments |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| **Bitdefender Anti-Ransomware** | yes | no | CTBLocker, Locky, TeslaCrypt | yes | no | all supported versions of Windows | |
| **CryptoPrevent** | yes | no | unknown, developer cites "large number of cryptoware" | yes | no | Windows XP to Windows 10 | Paid versions available, protects against other malware |
| **HitmanPro.Alert** | no | no | Cryptoware protection | yes | no | Windows XP to Windows 7 | requires HitmanPro |
| **HitmanPro.Kickstart** | no | no | Lock Screen only | no | yes | Windows XP to Windows 10 | requires HitmanPro |
| **Kaspersky Anti-Ransomware** | yes | no | unknown | yes | rollback | all supported versions of Windows | |
| **Malwarebytes Anti-Ransomware** | yes | yes | CryptoLocker, CryptoWall, CTBLocker, Tesla | yes | no | all supported versions of Windows | Proactive Protection against new ransomware |
| **RansomFree** | yes | no | against more than 40 tested variants | yes | no | all supported versions of Windows | Honeypot system |
| **SBGuard** | yes | no | hardens the system | no | no | all supported versions of Windows | |
| **Trend Micro Anti-Ransomware** | yes | no | Lock Screen only | no | yes | all supported versions of Windows | |
| **Winantiransom** | no | no | most, if not all, ransomware | yes | no | all supported versions of Windows | Layered protection, File, network and Registry protection |

Source: ghacks.net, By Martin Brinkmann on March 30, 2016 in Security - Last Update:December 20, 2016.
http://www.ghacks.net/2016/03/30/anti-ransomware-overview/

Thank you for your attention
www.cyber.services