The Case of the Crypto-Attacks

TALOS

TALOS Group - Security Intelligence and Research Group of ***CISCO Systems***

The TALOS Group

- Security Intelligence and Research Group of Cisco Systems
- Talos researchers create threat intelligence for Cisco security products to protect customers from both known and emerging threats
- Many sub-teams inside it: malware team, analysts, vulnerability research, developers, ...
- The Malware Team is an advanced team that focuses on malware analysis. Some of its deliverables are to produce content for malware detection across many Cisco products, as well as media outreach. I am an active member of this team.
- Vulnerability Research Team deals with Security vulnerabilities, live incidents, Security fixes and patches analysis. Some of us study exploits and release defense.

Outline

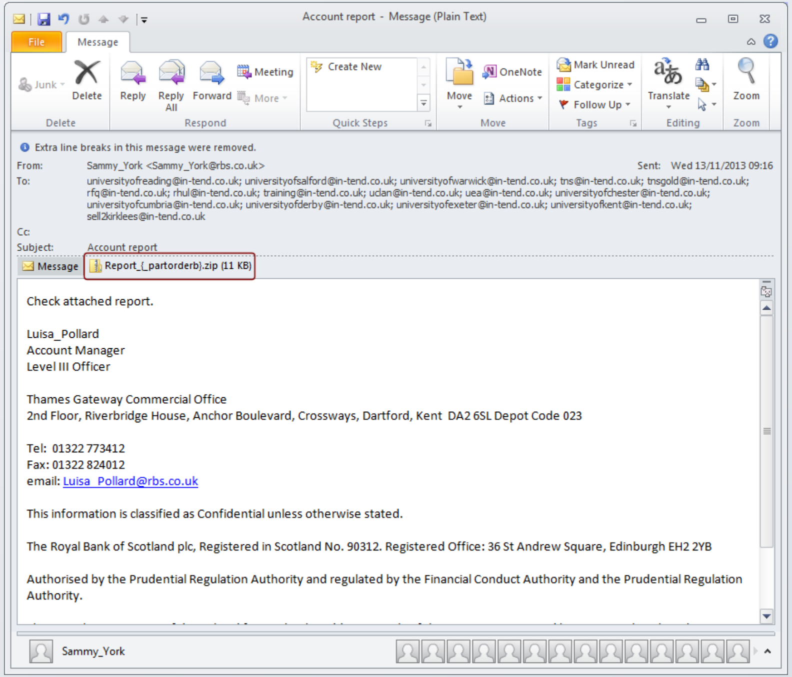
1. What is a ransomware?
2. The Crypto malware spread modality
3. What is an Exploit?
4. Cryptowall case – its dangerous features, and peculiar characteristics
5. How can I protect from CryptoWall?
6. Can I recover my encrypted files?
7. Conclusions

What is a Ransomware

- **Ransomware** is a type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed
- Some forms of ransomware encrypt files on the system's hard drive, while some may simply lock the system and display messages intended to coax the user into paying *

*definition from Wikipedia

The Crypto malware spread modality



Extra line breaks in this message were removed.

From: Sammy_York <Sammy_York@rbs.co.uk>
Sent: Wed 13/11/2013 09:16
To: universityofreading@in-tend.co.uk; universityofsalford@in-tend.co.uk; universityofwarwick@in-tend.co.uk; tns@in-tend.co.uk; tnsgold@in-tend.co.uk; rfq@in-tend.co.uk; rhul@in-tend.co.uk; training@in-tend.co.uk; uclan@in-tend.co.uk; uea@in-tend.co.uk; universityofchester@in-tend.co.uk; universityofcumbria@in-tend.co.uk; universityofderby@in-tend.co.uk; universityofexeter@in-tend.co.uk; universityofkent@in-tend.co.uk; sell2kirklees@in-tend.co.uk
Cc:
Subject: Account report

Check attached report.

Luisa_Pollard
Account Manager
Level III Officer

Thames Gateway Commercial Office
2nd Floor, Riverbridge House, Anchor Boulevard, Crossways, Dartford, Kent DA2 6SL Depot Code 023

Tel: 01322 773412
Fax: 01322 824012
email: Luisa_Pollard@rbs.co.uk

This information is classified as Confidential unless otherwise stated.

The Royal Bank of Scotland plc, Registered in Scotland No. 90312. Registered Office: 36 St Andrew Square, Edinburgh EH2 2YB

Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.

1. E-mails attachments
2. Un-patched bugs in software
3. Removable drives
4. LAN Networks

What is an Exploit?

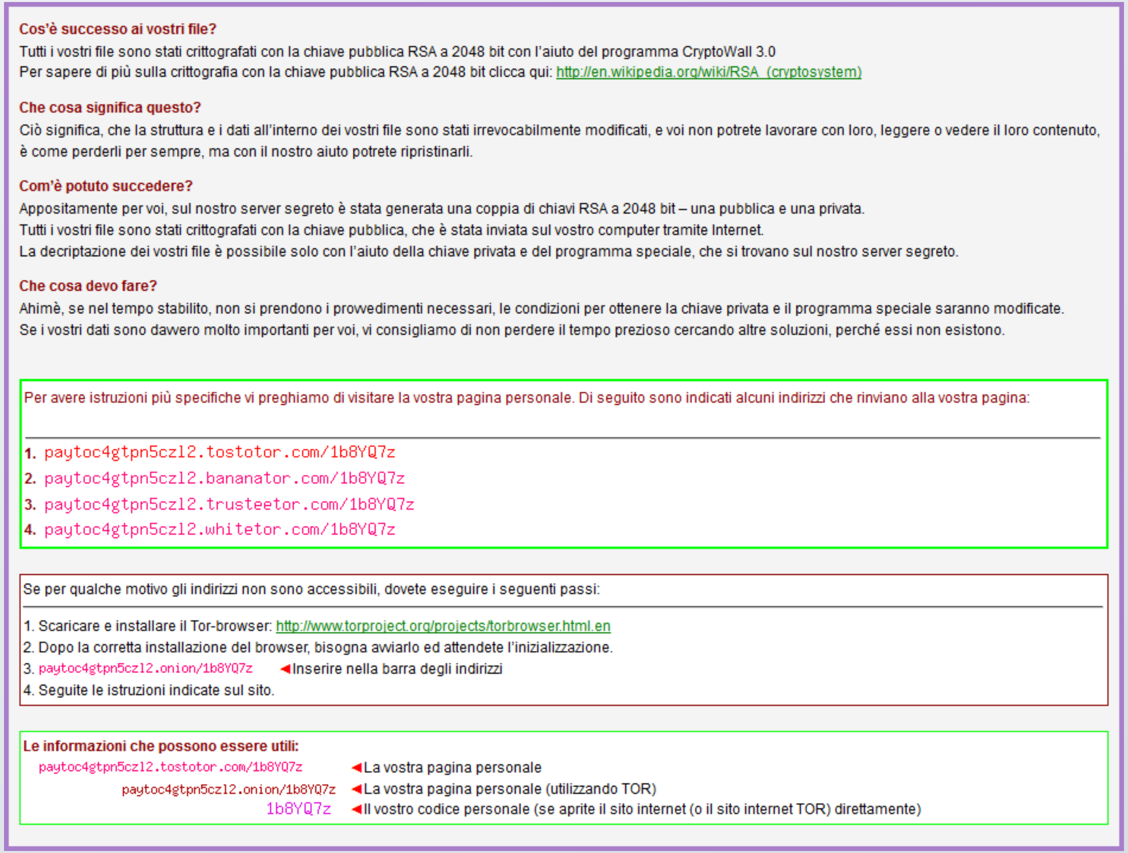
1. An **exploit** is a piece of software or a chunk of data that takes advantage of a bug or vulnerability in order to cause unintended behavior to occur on computer software, hardware, or something electronic (usually computerized)
2. The unintended behavior often means the execution of malicious code or the acquire of administrative privileges
3. Cryptowall uses exploits to spread the infection code inside legal documents (a PDF file for example), or to overcome some Windows’ protections

Exploitation results

Even a Word or a PDF Document (maybe sent as an attachment) could potentially contains a form of Crypto-Malware

The CryptoWall Case

1. CryptoWall is the ransomware that, together with all its variants (CryptoLocker, TorrentLocker, …), has infected a lot of Italian networks and organization (Hacker infettano i comuni - dipendenti pagano il riscatto)
2. The malware infects the target host -> communicates with the C&C server -> the server generates a RSA public/private key pair
3. **Only the public key is transferred to the victim workstation**.
4. The malware starts to encrypt each file found in all local disks, removable devices **and remote drives**
5. Finally a message is shown to the user



Cos'è successo ai vostri file?

Tutti i vostri file sono stati crittografati con la chiave pubblica RSA a 2048 bit con l'aiuto del programma CryptoWall 3.0
Per sapere di più sulla crittografia con la chiave pubblica RSA a 2048 bit clicca qui: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

Che cosa significa questo?

Ciò significa, che la struttura e i dati all'interno dei vostri file sono stati irrevocabilmente modificati, e voi non potrete lavorare con loro, leggere o vedere il loro contenuto, è come perderli per sempre, ma con il nostro aiuto potrete ripristinarli.

Com'è potuto succedere?

Appositamente per voi, sul nostro server segreto è stata generata una coppia di chiavi RSA a 2048 bit – una pubblica e una privata.
Tutti i vostri file sono stati crittografati con la chiave pubblica, che è stata inviata sul vostro computer tramite Internet.
La decriptazione dei vostri file è possibile solo con l'aiuto della chiave privata e del programma speciale, che si trovano sul nostro server segreto.

Che cosa devo fare?

Ahimè, se nel tempo stabilito, non si prendono i provvedimenti necessari, le condizioni per ottenere la chiave privata e il programma speciale saranno modificate.
Se i vostri dati sono davvero molto importanti per voi, vi consigliamo di non perdere il tempo prezioso cercando altre soluzioni, perché essi non esistono.

Per avere istruzioni più specifiche vi preghiamo di visitare la vostra pagina personale. Di seguito sono indicati alcuni indirizzi che rinviano alla vostra pagina:

1. paytoc4gtpn5czl2.tostotor.com/1b8YQ7z
2. paytoc4gtpn5czl2.bananator.com/1b8YQ7z
3. paytoc4gtpn5czl2.trusteetor.com/1b8YQ7z
4. paytoc4gtpn5czl2.whitetor.com/1b8YQ7z

Se per qualche motivo gli indirizzi non sono accessibili, dovete eseguire i seguenti passi:

1. Scaricare e installare il Tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2. Dopo la corretta installazione del browser, bisogna avviarlo ed attendete l'inizializzazione.
3. paytoc4gtpn5czl2.onion/1b8YQ7z ◀Inserire nella barra degli indirizzi
4. Seguite le istruzioni indicate sul sito.

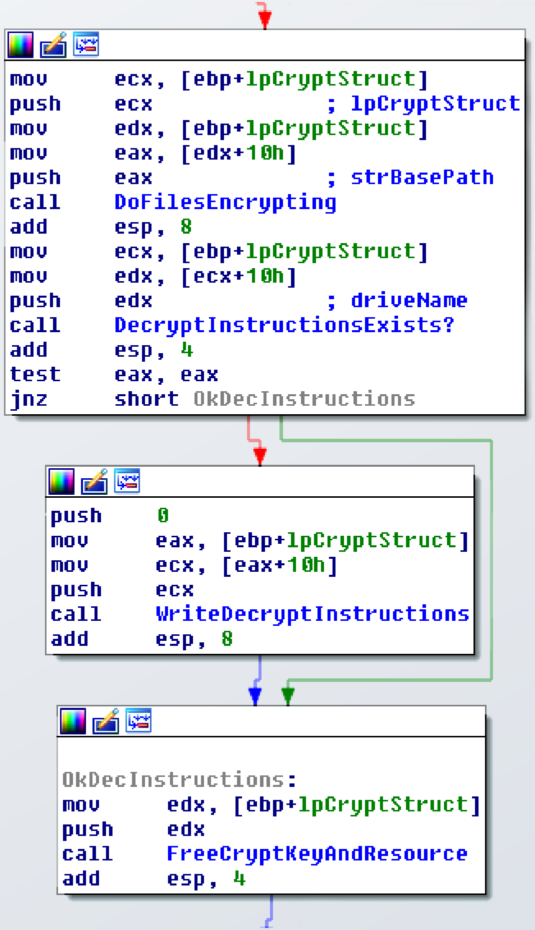
Le informazioni che possono essere utili:

paytoc4gtpn5czl2.tostotor.com/1b8YQ7z ◀La vostra pagina personale
paytoc4gtpn5czl2.onion/1b8YQ7z ◀La vostra pagina personale (utilizzando TOR)
1b8YQ7z ◀Il vostro codice personale (se aprite il sito internet (o il sito internet TOR) direttamente)

The CryptoWall Case

Its peculiar characteristics are the following:

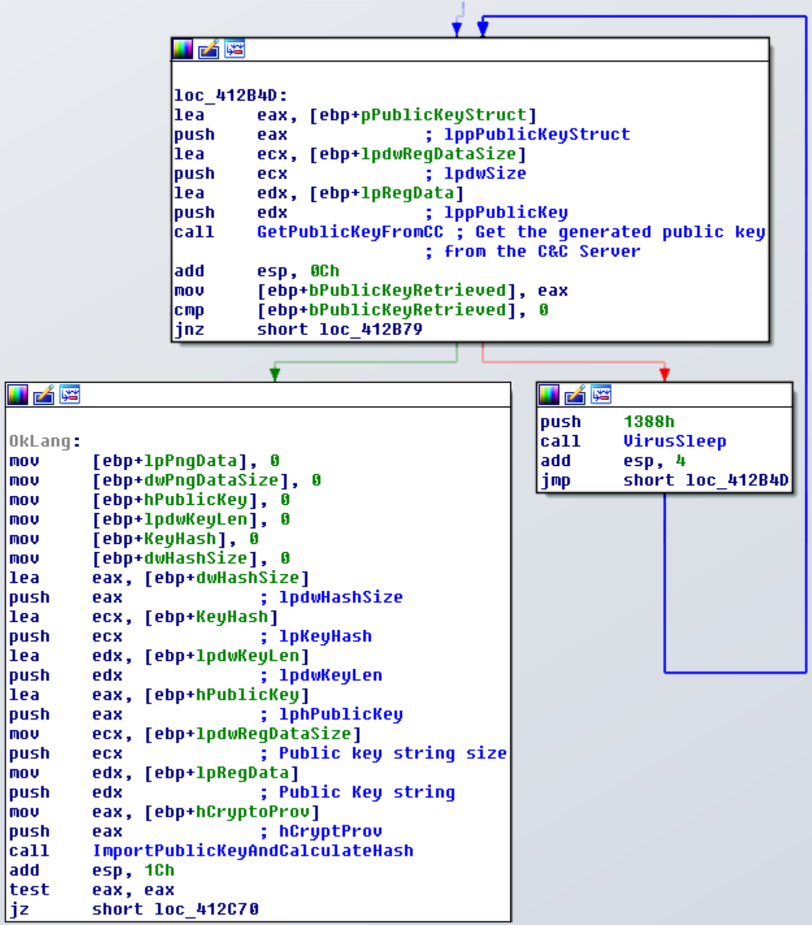
1. 3 different versions (from the fall of 2012 till now)
2. Anti-Vm and Anti-Debug code – the malware doesn’t run if it detects a Virtual Machine
3. Usage of the TOR and I2P anonymous networks – the bad guys and the money transfer could not be tracked
4. Usage of exploits to spread itself and to gain privilege escalation
5. Mix of 32-bit and 64-bit code



```
mov     ecx, [ebp+lpCryptStruct]
push    ecx             ; lpCryptStruct
mov     edx, [ebp+lpCryptStruct]
mov     eax, [edx+10h]
push    eax             ; strBasePath
call    DoFilesEncrypting
add     esp, 8
mov     ecx, [ebp+lpCryptStruct]
mov     edx, [ecx+10h]
push    edx             ; driveName
call    DecryptInstructionsExists?
add     esp, 4
test    eax, eax
jnz     short OkDecInstructions
```

```
push    0
mov     eax, [ebp+lpCryptStruct]
mov     ecx, [eax+10h]
push    ecx
call    WriteDecryptInstructions
add     esp, 8
```

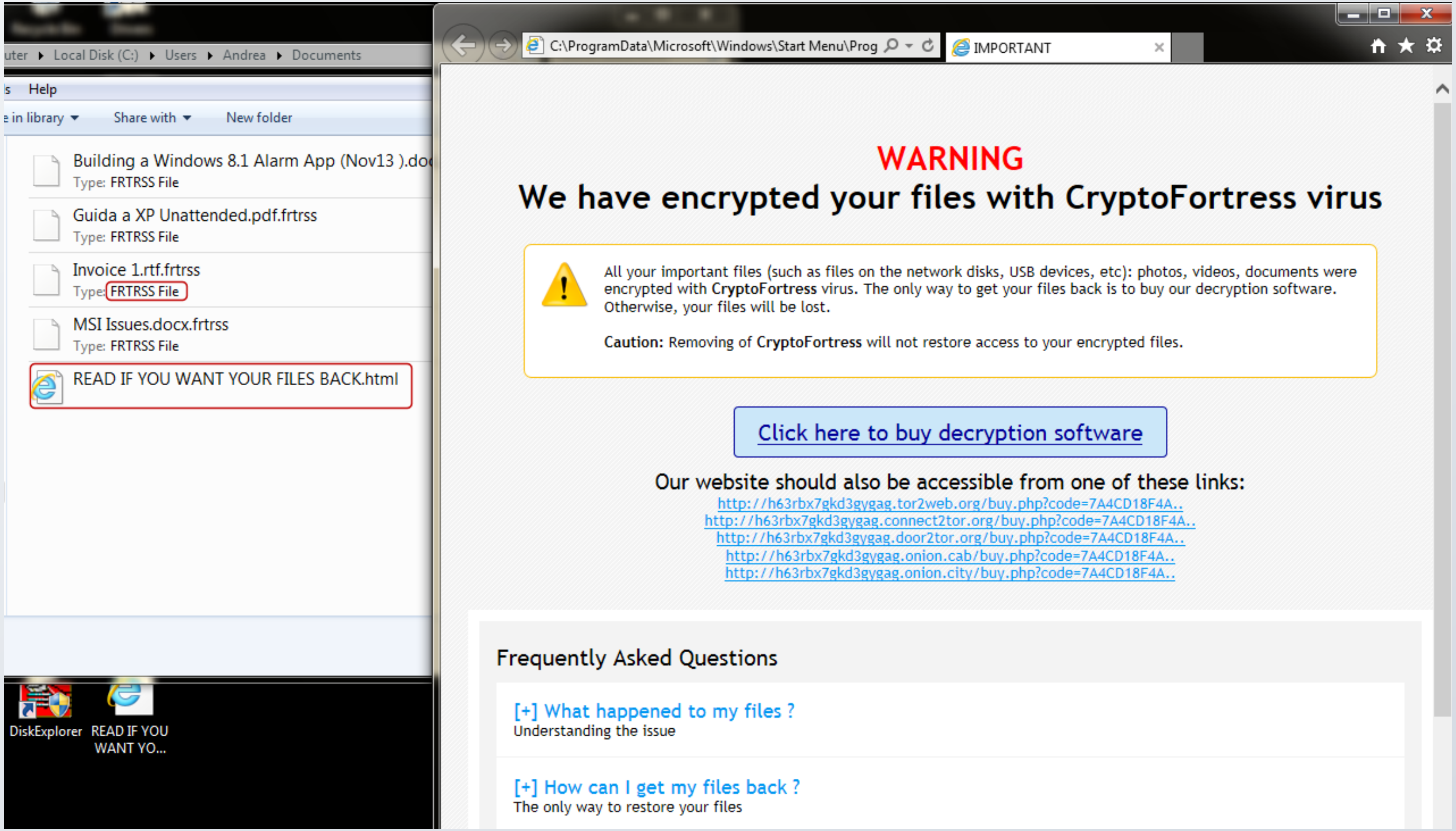
```
OkDecInstructions:
mov     edx, [ebp+lpCryptStruct]
push    edx
call    FreeCryptKeyAndResource
add     esp, 4
```



```
loc_412B4D:
lea     eax, [ebp+pPublicKeyStruct]
push    eax                 ; lppPublicKeyStruct
lea     ecx, [ebp+lpdwRegDataSize]
push    ecx                 ; lpdwSize
lea     edx, [ebp+lpRegData]
push    edx                 ; lppPublicKey
call    GetPublicKeyFromCC ; Get the generated public key
                            ; from the C&C Server
add     esp, 0Ch
mov     [ebp+bPublicKeyRetrieved], eax
cmp     [ebp+bPublicKeyRetrieved], 0
jnz     short loc_412B79
```

```
OkLang:
mov     [ebp+lpPngData], 0
mov     [ebp+dwPngDataSize], 0
mov     [ebp+hPublicKey], 0
mov     [ebp+lpdwKeyLen], 0
mov     [ebp+KeyHash], 0
mov     [ebp+dwHashSize], 0
lea     eax, [ebp+dwHashSize]
push    eax                 ; lpdwHashSize
lea     ecx, [ebp+KeyHash]
push    ecx                 ; lpKeyHash
lea     edx, [ebp+lpdwKeyLen]
push    edx                 ; lpdwKeyLen
lea     eax, [ebp+hPublicKey]
push    eax                 ; lphPublicKey
mov     ecx, [ebp+lpdwRegDataSize]
push    ecx                 ; Public key string size
mov     edx, [ebp+lpRegData]
push    edx                 ; Public Key string
mov     eax, [ebp+hCryptoProv]
push    eax                 ; hCryptProv
call    ImportPublicKeyAndCalculateHash
add     esp, 1Ch
test    eax, eax
jz      short loc_412C70
```

```
push    1388h
call    VirusSleep
add     esp, 4
jmp     short loc_412B4D
```


uter ▸ Local Disk (C:) ▸ Users ▸ Andrea ▸ Documents
s Help
e in library ▾ Share with ▾ New folder
C:\ProgramData\Microsoft\Windows\Start Menu\Prog
IMPORTANT
DiskExplorer
READ IF YOU WANT YO...

Building a Windows 8.1 Alarm App (Nov13).doc
Type: FRTRSS File

Guida a XP Unattended.pdf.frtrss
Type: FRTRSS File

Invoice 1.rtf.frtrss
Type: FRTRSS File

MSI Issues.docx.frtrss
Type: FRTRSS File

READ IF YOU WANT YOUR FILES BACK.html

WARNING
We have encrypted your files with CryptoFortress virus

All your important files (such as files on the network disks, USB devices, etc): photos, videos, documents were encrypted with **CryptoFortress** virus. The only way to get your files back is to buy our decryption software. Otherwise, your files will be lost.

Caution: Removing of **CryptoFortress** will not restore access to your encrypted files.

Click here to buy decryption software

Our website should also be accessible from one of these links:

http://h63rbx7gkd3gygag.tor2web.org/buy.php?code=7A4CD18F4A..
http://h63rbx7gkd3gygag.connect2tor.org/buy.php?code=7A4CD18F4A..
http://h63rbx7gkd3gygag.door2tor.org/buy.php?code=7A4CD18F4A..
http://h63rbx7gkd3gygag.onion.cab/buy.php?code=7A4CD18F4A..
http://h63rbx7gkd3gygag.onion.city/buy.php?code=7A4CD18F4A..

Frequently Asked Questions

[+] What happened to my files ?
Understanding the issue

[+] How can I get my files back ?
The only way to restore your files

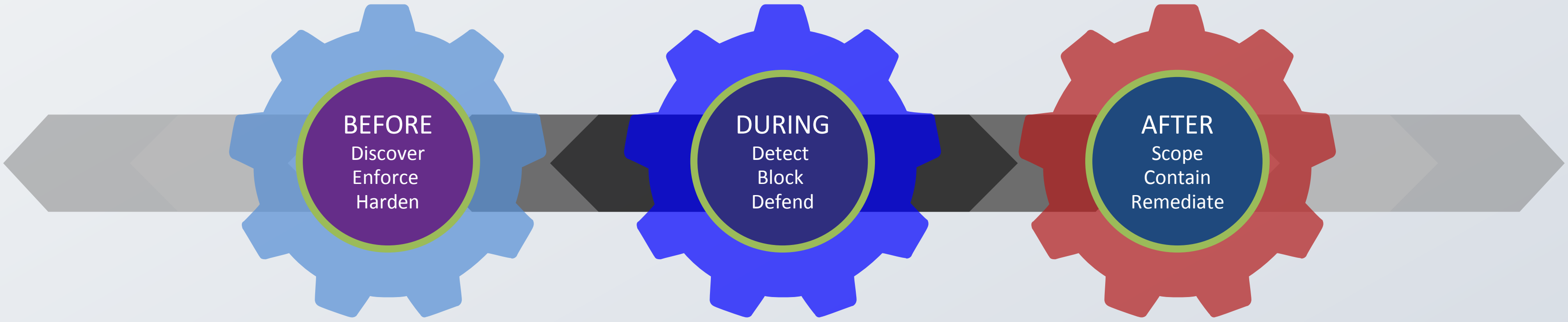
How Can I protect my environment?

- To protect from Crypto ransomwares, a good AV product and firewall should be enough
- **BUT** the new variants of the virus can overcome even the AV, Firewall and IPS *
- A Very important step is to do a **regular Backup** with a professional software on an external destination (CryptoWall can even encrypt the backup archive)

* For the detailed technical explanation send me a mail at aallievi@cisco.com

The New Security Model

Attack Continuum



Network Endpoint Mobile Virtual Cloud Email & Web

Point-in-time Continuous

Can I recover my files?

- Theoretically the last versions of Cryptowall makes the manual decryption of the target files **IMPOSSIBLE** because the private key will never been communicated to the infected host
- The first versions of CryptoLocker have used the symmetric encryption: the key used for the encryption was the same needed for the decryption. In this case a manual decryption was possible
- The infection has evolved over and over the years
- In September 2014 some researchers built a solution that leverage a weakness in the implementation of some TorrentLocker samples, but very low rate of success: http://www.ilsoftware.it/articoli.asp?tag=Esiste-una-soluzione-per-Cryptolocker_11949 -> The malware author’s then updated their code

Conclusions

- Ransomware attacks could be very destructive
- Following the best security practises could help in defend versus this kind of malware
- **Secure your company network!**

If you are interested in all the nitty-gritty details about CryptoWall and other ransomwares check our TALOS blog:

- https://blogs.cisco.com/security/talos/cryptowall-2
- https://blogs.cisco.com/security/talos/cryptowall-3-0

For any questions mail me at:

aallievi@cisco.com

Or follow me on Twitter:

@aall86

THE END

THANKS FOR ATTENDING