ADVENTURES IN RANSOMWARELAND

Vecchie minacce e nuove tecniche di attacco

Pietro Delsante – Engineering & R&D Manager - Certego

certego

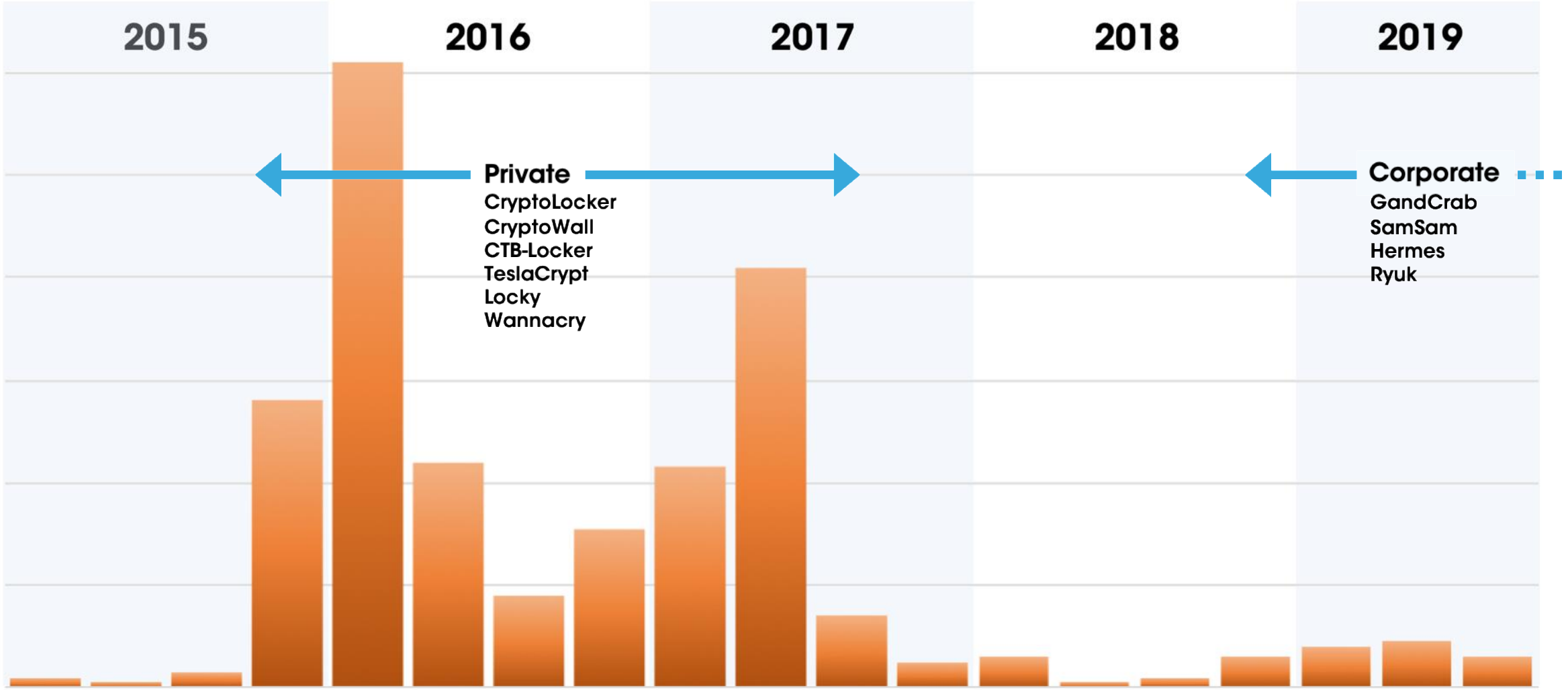
CERTEGO THREAT INTELLIGENCE & INCIDENT RESPONSE SERVICES

- Società del gruppo VEM Sistemi specializzata nell'erogazione di servizi di **Cyber Threat Intelligence & Incident Response**
- Ha sviluppato la piattaforma **Certego PanOptikon** per l'orchestrazione e l'automazione dei processi di rilevamento, analisi e gestione degli incidenti
- **120.000+ asset protetti** in Europa, America, Cina e Giappone
- Riconosciuta da Gartner come **Regional Player** per l'erogazione dei servizi di **Cyber Threat Intelligence**

TÜV SÜD ISO 9001 · TÜV SÜD ISO 27001 · CARNEGIE MELLON UNIVERSITY SOFTWARE ENGINEERING INSTITUTE CERT · FIRST Improving Security Together · EUROPOL EC3 European Cybercrime Centre · TF-CSIRT Trusted Introducer

certego

RANSOMWARE: STATISTICHE 2015 - 2019



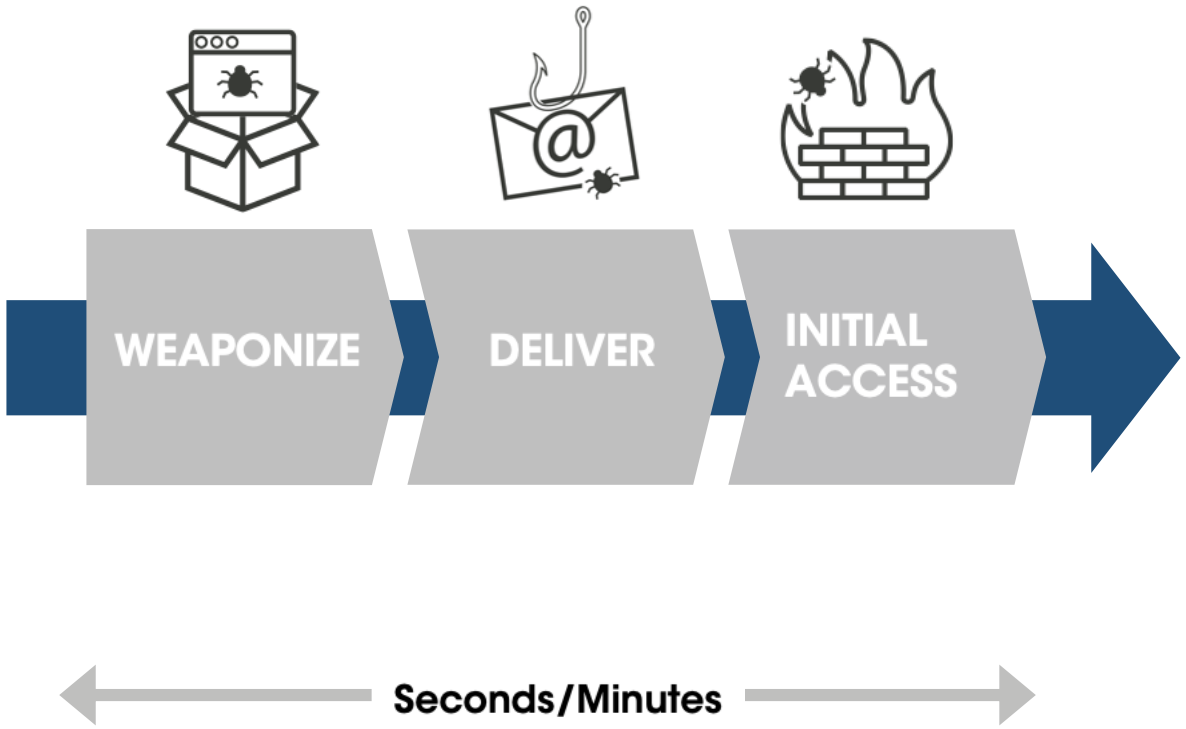
Source: Certego CSIRT

certego

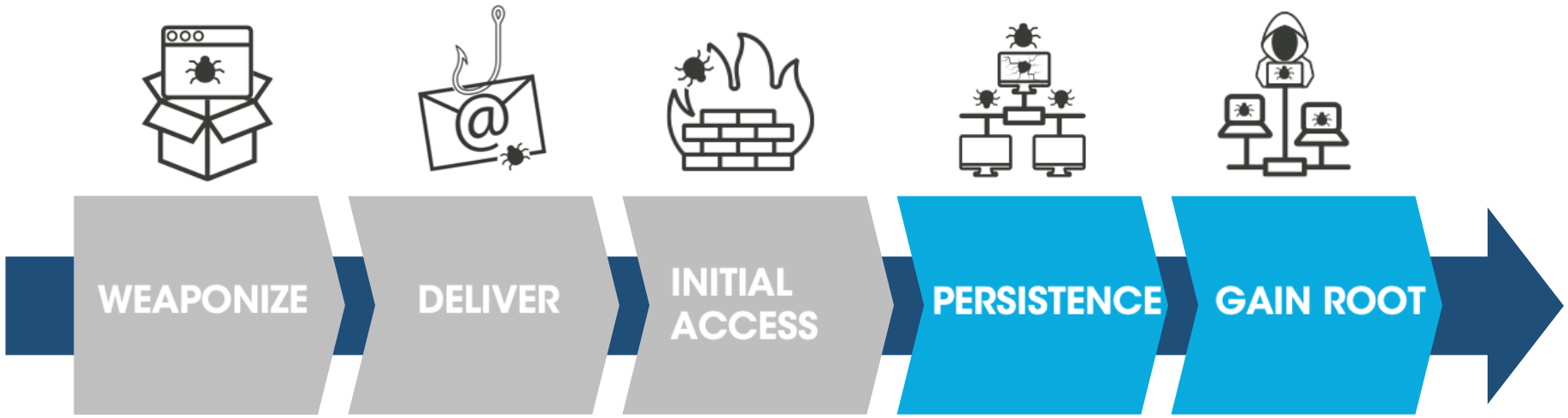
CORPORATE RANSOMWARE

- Minore frequenza, maggiori impatti
  - Obiettivo principale: **Blocco della produzione**
- **Aumento del valore** del riscatto
  - Da poche centinaia di Euro a milioni di Euro
- Capacità di **propagazione laterale**
- Spesso veicolato come **payload** attraverso altri vettori di infezione (i.e. Emotet, TrickBot, etc.)
- Utilizzato nelle **fasi successive alla compromissione iniziale** per monetizzare l'attacco

FASE 1: COMPROMISSIONE INIZIALE

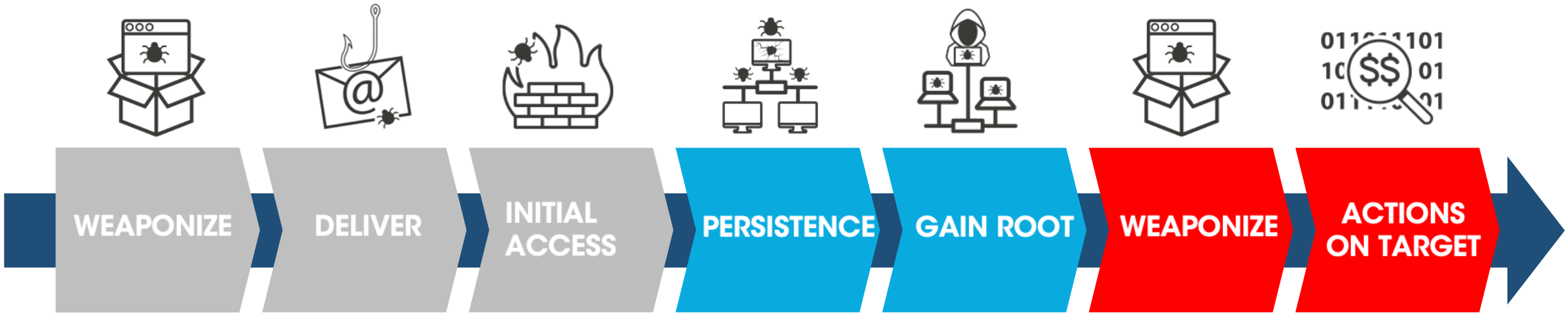


FASE 2: PERSISTENZA & PRIVILEGE ESCALATION



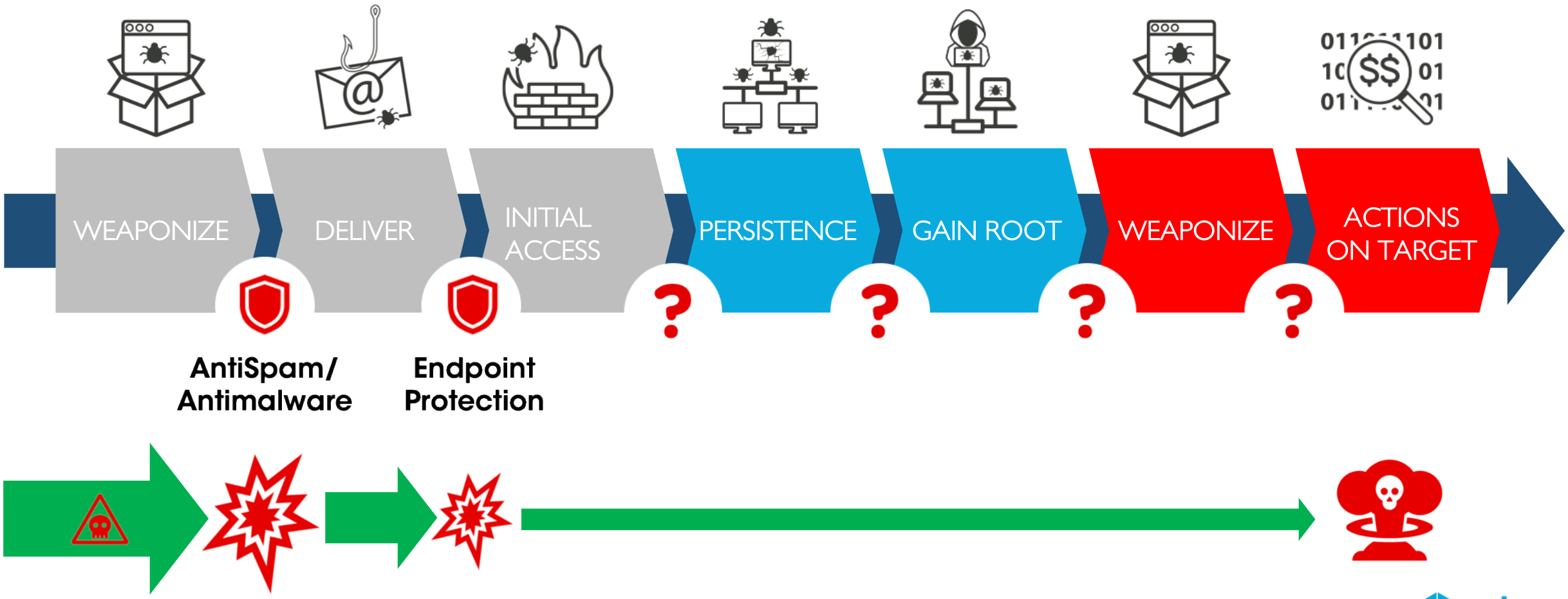
certego

FASE 3: AZIONI FINALI



certego

DIFESA: APPROCCIO TRADIZIONALE




Initial Access
Actions on Target

MITRE ATT&CK ENTERPRISE FRAMEWORK

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Actions on Target
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service

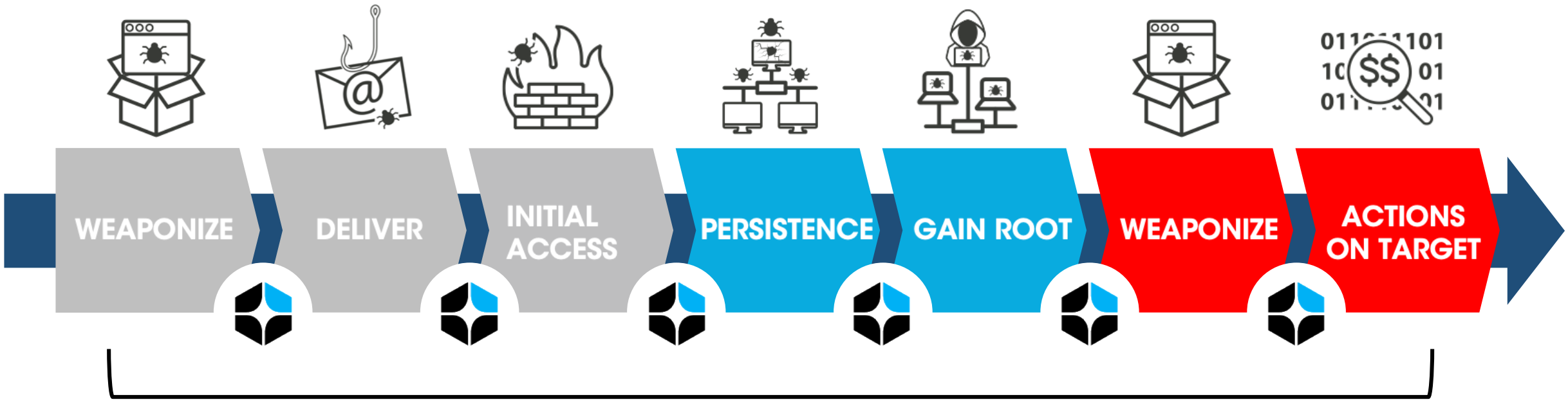
MITRE ATT&CK ENTERPRISE FRAMEWORK

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Actions on Target
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service

MITRE ATT&CK ENTERPRISE FRAMEWORK

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Actions on Target
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service

FULL KILL CHAIN DETECTION



Network Traffic

Event Logs

Process Activities

Vulnerabilities

File Analysis

certego

L'ATTACCO A IRIS CERAMICA

il Resto del Carlino MODENA

CRONACA SPORT COSA FARE EDIZIONI PIRATI TRAGEDIA BIMBI E45 METEO GRATTA E VINCI DIABETE

HOME › MODENA › CRONACA

Pubblicato il **28 dicembre 2018**

Gruppo Iris, attacco hacker. Chiesti 950mila euro di riscatto

Due settimane fa il sistema dell'azienda è stato 'tenuto in ostaggio' Federica Minozzi: "Non abbiamo ceduto, i nostri tecnici hanno risolto tutto"

Ultimo aggiornamento il **28 dicembre 2018 alle 11:51**

L'ATTACCO A IRIS CERAMICA

il Resto del Carlino MODENA

CRONACA SPORT COSA FARE EDIZIONI PIRATI TRAGEDIA BIMBI E45 METEO GRATTA E VINCI DIABETE

HOME › MODENA › CRONACA

Pubblicato il **28 dicembre 2018**

Gruppo Iris, attacco hacker. Chiesti 950mila euro di riscatto

Due settimane fa il sistema dell'azienda è stato 'tenuto in ostaggio' Federica Minozzi: "Non abbiamo ceduto, i nostri tecnici hanno risolto tutto"

Ultimo aggiornamento il **28 dicembre 2018 alle 11:51**

«Forse – spiega il ceo di Iris group, Federica Minozzi – **qualcuno dei nostri dipendenti ha aperto inavvertitamente una di queste mail** e nel giro di poche ore tutta la rete si è praticamente spenta. Fortunatamente noi abbiamo una squadra di 18 tecnici informatici che hanno lavorato 48 ore giorno e notte per ripristinare il funzionamento del sistema in tutte le fabbriche».

certego

L'ATTACCO A BONFIGLIOLI RIDUTTORI

il Resto del Carlino BOLOGNA

CRONACA SPORT COSA FARE EDIZIONI PIRATI TRAGEDIA BIMBI E45 METEO GRATTA E VINCI DIABETE

HOME › BOLOGNA › CRONACA

Pubblicato il 2 luglio 2019

Attacco hacker alla Bonfiglioli. "Chiesto riscatto di 2,4 milioni"

L'azienda decide di non pagare: "Abbiamo scelto di non assoggettarci al ricatto e non alimentare un meccanismo criminale"

Ultimo aggiornamento il 2 luglio 2019 alle 19:37

L'ATTACCO A BONFIGLIOLI

il Resto del

CRONACA SPORT COSA FARE EDIZIONI PIRATI

HOME › BOLOGN

Attac
milior

L'azienda de
criminale"

Ultimo aggiorname

ANSA.it Emilia-Romagna

Fai la ricerca

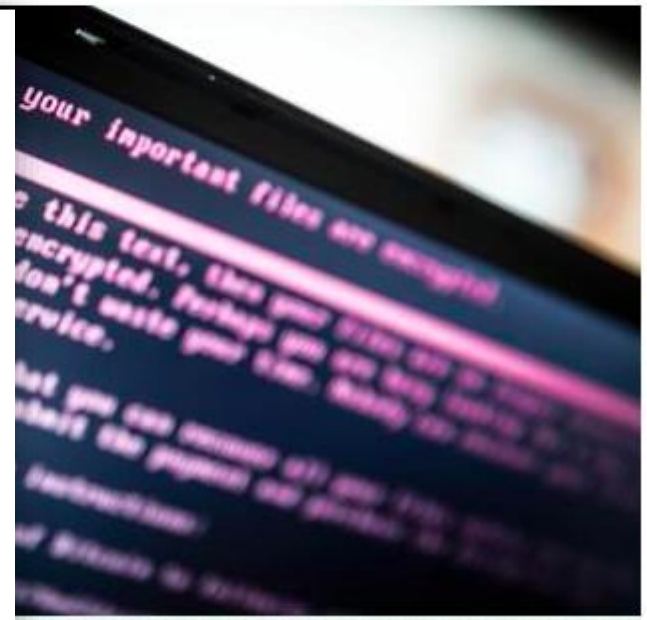
Galleria Fotografica Video

CRONACA • POLITICA • ECONOMIA • SPORT • SPETTACOLO • MADE IN E-R • ANSA VIAGGIART • EMILIA-ROMAG

ANSA.it › Emilia-Romagna › Cyber-attacco ad azienda bolognese

Cyber-attacco ad azienda bolognese

Nel mirino Bonfiglioli Riduttori a giugno, hacker fermati



CLICCA PER INGRANDIRE

MENU | CERCA

la Repubblica

HOME CRONACA SPORT FOTO RISTORANTI ANNUNCI LOCA

Cyberattacco a famosa azienda bolognese, riscatto da 2,4 milioni di euro

La Bonfiglioli rifiuta di pagare e denuncia. "Abbiamo subito rallentamenti nel lavoro"

certego

L'ATTACCO A BONFIGLIOLI

Un **malware** ha disattivato l'**antivirus**: i server hanno ceduto uno dopo l'altro sotto i colpi di uncryptolocker, Ryuk, che ha cifrato, rendendo indisponibile, una grande quantità di file. E' accaduto tra l'11 e il 13 giugno scorsi. All'azienda è giunta la richiesta di un **riscatto di 340 Bitcoin** (2,4 milioni di euro al valore del 12 giugno, 3,5 milioni dopo l'annuncio del varo di Libra, la criptovaluta di Facebook) per consegnare la 'chiave' digitale che avrebbe potuto disattivare il malware.

ANSA.it Emilia-Romagna

Fai la ricerca

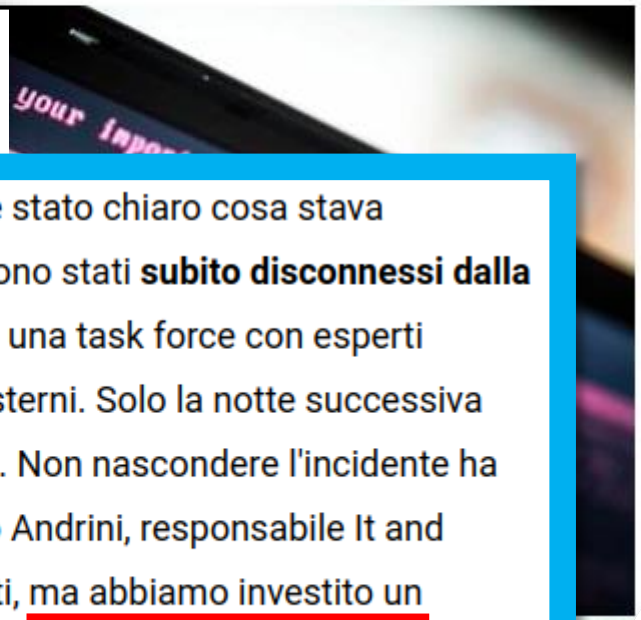
Galleria Fotografica | Video

SPORT • SPETTACOLO • MADE IN E-R • ANSA VIAGGIART • EMILIA-ROMAG

ber-attacco ad azienda bolognese

ad azienda bolognese

ttori a giugno, hacker fermati



Attac
milior

L'azienda de
criminale"

Ultimo aggiorname

HOME CRONACA SP

Cyberattacco
bolognese, ris
milioni di eur

La Bonfiglioli rifiuta di pagare e denuncia. "Abbiamo subito rallentamenti nel lavoro"

Anche perché, la mattina dell'11 giugno, quando è stato chiaro cosa stava accadendo, i server dal contenuto più 'prezioso' sono stati **subito disconnessi dalla rete**, per renderli irraggiungibili. "Abbiamo istituito una task force con esperti interni, agenti della Polizia postale e consulenti esterni. Solo la notte successiva siamo riusciti a domare la diffusione del malware. Non nascondere l'incidente ha comunque accelerato la soluzione", spiega Enrico Andrini, responsabile It and digital di Bonfiglioli Riduttori. "Eravamo già protetti, ma abbiamo investito un milione di euro per acquistare due antivirus e nuovi software", conclude Bonfiglioli.

certego

UN ESEMPIO PIÙ RECENTE

Manuel D'Alessandro @xMegaloma... · 3g

Battling against **Ryuk** **#Ransomware** for 8 Days & Nights in a Customer's multi-site company. @Sophos has been massively deployed and it's kicking hard. Big thanks to @Veeam for saving the day!

UN CASO REALE

- Contesto dell'attacco: Organizzazione di medie dimensioni operante nel settore dei servizi IT avanzati
- Tipologia di attacco: Inizialmente **Opportunistico,** successivamente **Targeted/Mirato**
- Vettore di attacco: Variante di **Malware Emotet**
  - Rilevabile soltanto dal **3%** di prodotti AV
  - **Sandbox-evading** malware
  - **Nessuna informazione di Intelligence disponibile** (i.e. Dropzone, C&C server, etc.)

certego

Alerts [redacted]

Summary | Raw Events | Query on Sensor | Threat Analysis | Open Tickets 49 | Customer Info

23 total

RAW | CONN | PAYLOAD | HTTP | SSL | DNS | CB | WFD

timestamp	source	watchlist name	feed name	process name	username	cmdline
2019-05-06 05:40:10 Z		[redacted]				
2019-05-06 05:40:11 Z		[redacted]				
2019-05-06 05:40:54 Z		[Certego Malware] Unsigned Process with MS-SCMR capabilities		xinputisve.exe	[redacted]	[xinputisve.exe,c:\\windows\\syswow64\\xinputisve.exe]
2019-05-06 05:40:54 Z		[redacted]				
2019-05-06 05:40:54 Z		[Certego Malware] Unsigned Process with MS-SCMR capabilities		xinputisve.exe	[redacted]	[xinputisve.exe,c:\\windows\\syswow64\\xinputisve.exe]

Certego s.r.l.

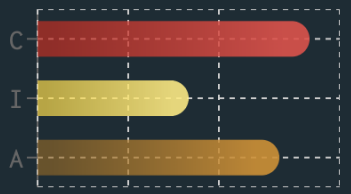
Ticket opened by Bernardino Grignaffini May 6, 2019 5:59 PM

5

Rilevamenti multipli di malware Emotet su host interni

Diversi host interni risultano essersi infettati con un malware noto come Emotet, appartenente alla categoria dei Trojan Dropper.

Suggeriamo di proseguire con la lettura del ticket per una descrizione più accurata di quanto rilevato e per alcune indicazioni su containment ed eradication di questa minaccia.



Incident Response Procedure

- Detection
- **Analysis**
- Info Gathering
- Containment 1
- Eradication 2
- Post Incident 1

A partire dalle 13:13, diversi host interni hanno iniziato ad effettuare connessioni malevole compatibili con le tecniche di propagazione laterale del malware noto come Emotet. Gli host interni coinvolti nell'infezione sono i seguenti:

172.16.10.23 (Utente: user01)
172.16.10.121 (Utente: user01)
172.16.10.148 (Utente: user02)
172.16.15.20 (Utente: user02)

Il malware Emotet si è recentemente evoluto in un malware modulare, capace di intraprendere diverse azioni sulla macchina infetta. Ha la capacità di effettuare furto di credenziali, di scaricare ulteriori malware tra cui ransomware e infostealer (Ursnif, Trickbot, etc), e, soprattutto, di diffondersi sulla rete compromessa fino ad infettare l'intera rete. Attualmente viene diffuso principalmente tramite e-mail di phishing contenenti documenti Word malevoli come allegato.

In questo caso, il malware scaricato dal Dropper è Ursnif, un Infostealer in grado di rubare, tra le altre cose, tutte le password salvate sulla postazione infetta e di mettersi in ascolto per intercettare tutte quelle digitate dall'utente. Lo stesso malware permette anche di effettuare in automatico bonifici fraudolenti su alcuni siti di home banking per i quali il malware possiede una specifica configurazione.

#PIEX9QIY

5 malware

Certego s.r.l.

Ticket opened by Bernardino Grignaffini May 6, 2019 5:59 PM

5

Rilevamenti multipli di malware Emotet su host interni

Diversi host interni risultano essersi infettati con un malware noto come Emotet, appartenente alla categoria dei Trojan Dropper.

Suggeriamo di proseguire con la lettura del ticket per una descrizione più accurata di quanto rilevato e per alcune indicazioni su containment ed eradication di questa minaccia.

Incident Response Procedure

- Detection
- Analysis
- Info Gathering
- **Containment** 1
- Eradication 2
- Post Incident 1

☐ 1

☐ 1

Block Command & Control Servers — CERTEGO

Bloccare i seguenti indirizzi IP sui firewall perimetrali:

```
91.218.127.160 -> utilizzato come "dropzone" del malware
80.211.41.213  e 185.197.74.123-> utilizzato come server di Comma
```

Acknowledge

Write a new message

Certego s.r.l.

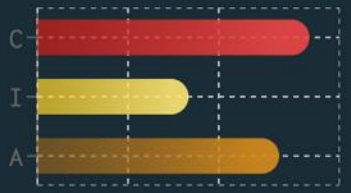
Ticket opened by Bernardino Grignaffini May 6, 2019 5:59 PM

5

Rilevamenti multipli di malware Emotet su host interni

Diversi host interni risultano essersi infettati con un malware noto come Emotet, appartenente alla categoria dei Trojan Dropper.

Suggeriamo di proseguire con la lettura del ticket per una descrizione più accurata di quanto rilevato e per alcune indicazioni su containment ed eradication di questa minaccia.



Incident Response Procedure

- Detection
- Analysis
- Info Gathering
- Containment
- **Eradication**
- Post Incident 1

☐ 1 ☐ 2

☐ 2

Manually remove persistence — CERTEGO

Se le scansioni antivirus non hanno rilevato nulla:

- Verificare che non esistano task schedulati chiamati `AppRunLog`, o con un nome formato dalle prime 5 o 6 cifre del codice UUID della macchina infetta, con la lettera `U` davanti (es. `U34792`). Se il task esiste, deve essere rimosso.
- Verificare che la cartella `%APPDATA%` non contenga una sottocartella chiamata con l'UUID dell'host infetto. Se tale cartella esiste, molto probabilmente contiene dei componenti del malware che devono essere rimossi manualmente.

Nel caso in cui uno o più di questi artefatti fosse presente, oltre a rimuoverlo suggeriamo di allegarlo o copiarlo in questo ticket, per approfondire le analisi.

Acknowledge

Write a new message

Certego s.r.l.

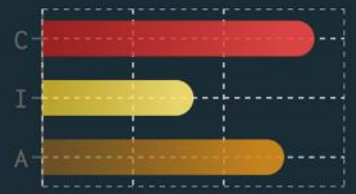
Ticket opened by Bernardino Grignaffini May 6, 2019 5:59 PM

5

Rilevamenti multipli di malware Emotet su host interni

Diversi host interni risultano essersi infettati con un malware noto come Emotet, appartenente alla categoria dei Trojan Dropper.

Suggeriamo di proseguire con la lettura del ticket per una descrizione più accurata di quanto rilevato e per alcune indicazioni su containment ed eradication di questa minaccia.



Incident Response Procedure

- Detection
- Analysis
- Info Gathering
- Containment
- Eradication
- **Post Incident**

1

1

BG

Block Bad Domain — CERTEGO

Bloccare per le prossime 48 ore i seguenti domini su firewall perimetrale:

```
asdijwensd.co
edfhsafuen.ru
ofinnsnelrzu.se
```

Add comment

a few seconds ago Done

Write a new message

People respond to incidents.

Certego S.R.L.
Via G. Perlasca, 25
41126 Modena, ITALY
+39 059 7353333
www.certego.net
info@certego.net