COME VENGONO INTERCETTATI E BLOCCATI I RANSOMWARE

MÜSA
FORMAZIONE E LAVORO

19 Gennaio
05:00pm

Massimo Chirivì

Coordinatore Area IT Security | Senior Trainer Musa Formazione

Enrico Tonello

IT Security Researcher & Co-Autore di Vir.IT eXplorer, co-fondatore di TG Soft

MÜSA
FORMAZIONE E LAVORO

PARTNER

TG Soft
Cyber Security Specialist
www.tgsoft.it

Vir.IT
explorer PRO
AntiVirus, AntiSpyware, AntiMalware, AntiRansomware

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

RANSOMWARE

«… *come attaccano e come ci si può difendere…*»

Docenti:

Ing. Enrico TONELLO
IT Security Researcher, Cyber Security Evangelist
Socio e co-fondatore di TG Soft Cyber Security Specialist

Michele ZUIN
IT Security Researcher, Malware Analyst
Coordinatore Supporto Tecnico Clienti TG Soft Cyber Security Specialist

Vir.IT explorer PRO
AntiVirus, AntiSpyware, AntiMalware, AntiRansomware

TG Soft
Cyber Security Specialist
www.tgsoft.it

MUSA FORMAZIONE E LAVORO

COME VENGONO INTERCETTATI E BLOCCATI I RANSOMWARE

19 Gennaio 05:00pm

LABORATORIO IT SECURITY

Massimo Chirivì — Coordinatore Area IT Security | Senior Trainer Musa Formazione

Enrico Tonello — IT Security Researcher, Co-Autore di Vir.IT eXplorer, co-fondatore di TG Soft Cyber Security Specialist

PARTNER TG Soft, Vir.IT, aipsi

RANSOMWARE… Ma quante se ne leggono in giro 1/2

VirIT explorer PRO — AntiVirus, AntiSpyware, AntiMalware, AntiRansomware

TG Soft — Cyber Security Specialist — www.tgsoft.it

MUSA FORMAZIONE E LAVORO

COME VENGONO INTERCETTATI E BLOCCATI I RANSOMWARE
19 Gennaio 05:00pm
LABORATORIO IT SECURITY
Massimo Chirivì — Coordinatore Area IT Security | Senior Trainer Musa Formazione
Enrico Tonello — IT Security Researcher, Co-Autore di Vir.IT eXplorer, co-fondatore di TG Soft Cyber Security Specialist
PARTNER: TG Soft, Vir.IT, aipsi

RANSOMWARE… Ma quante se ne leggono in giro 2/2

R.it Sicurezza
Home | News | Speciali | Mobile | Social Network | Sicurezza

"WannaCry e le aziende? La disattenzione alla sicurezza è paradossale"

Intervista a Carlo Mauceli, CTO e CISO di Microsoft Italia. Che analizza i motivi del grande attacco di ransomware e dice: "Ci vuole più informazione e occorre maggiore collaborazione tra aziende, clienti e governi"

I CONSIGLI DELLA POLIZIA | 15 maggio 2017

Attacco hacker, cosa fare (e non fare) per difendersi da Wannacry

Carola Frediani

IL SECOLO XIX

COMMENTI | LinkedIn | Pinterest | Email | ISCRIVITI Newsletter Il Secolo XIX

agi.it

Microsoft

Wannacry: "Già in 200 hanno pagato il riscatto"

CYBERSECURITY Martedì 16 maggio 2017 - 15:50

Ministero difesa Russia: respinti tutti i cyberattacchi WannaCry

"immediatamente identificati e bloccati rapidamente"

MONDO | «Ransomware» globale, nel giorno degli hacker colpiti anche..

«Ransomware» globale, nel giorno degli hacker colpiti anche ospedali inglesi

CRONACA

"Un attacco senza precedenti". Chi è stato colpito da Wannacry

Vir.IT explorer PRO
AntiVirus, AntiSpyware, AntiMalware, AntiRansomware

TG Soft
Cyber Security Specialist
www.tgsoft.it

Ransomware: cosa sono ?

Con il termine **Ransomware** definiamo tutti quei programmi o software che bloccano l'accesso al computer o ai file di documenti chiedendo un riscatto in denaro per riaverne l'accesso.

Ransomware di 1° Generazione

(chiamati anche **BLOCKER**)

Trojan.Win32.FakeGdF o simili. Sono dei malware che bloccano l'accesso ai PC/Server e richiedono un riscatto (2010-2011-2012)

Ransomware di 2° Generazione

(chiamati anche **CRYPTOR**)

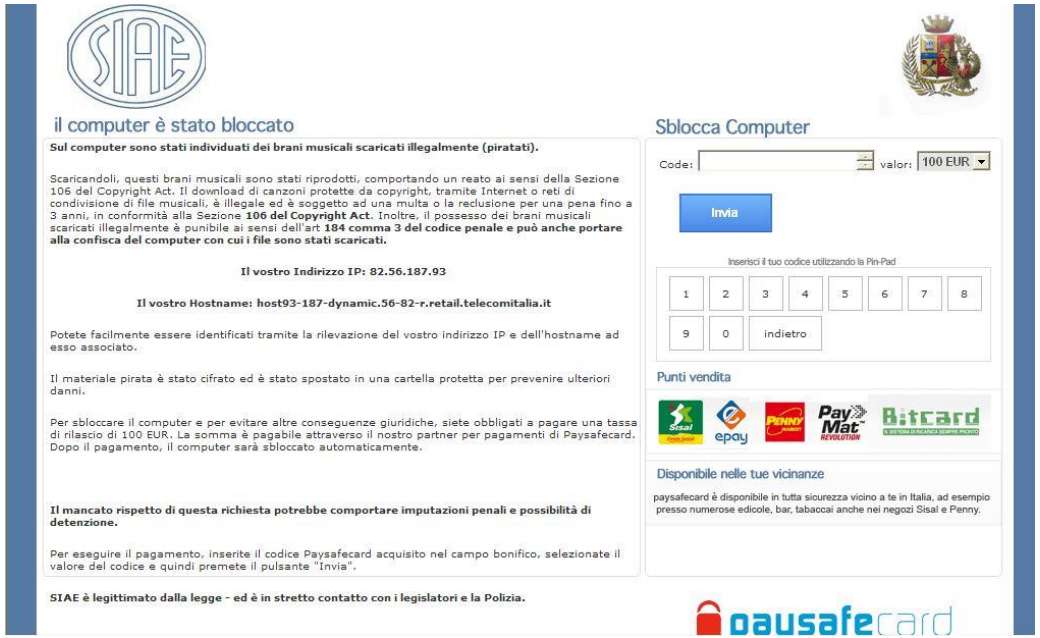
Crypto-Malware. Sono dei malware che cifrano i file di dati o altre parti vitali del disco fisso (es. MfT) e richiedono un riscatto (2012 ➔ 2023…)

Le numerose varianti di FakeGdF 1/2

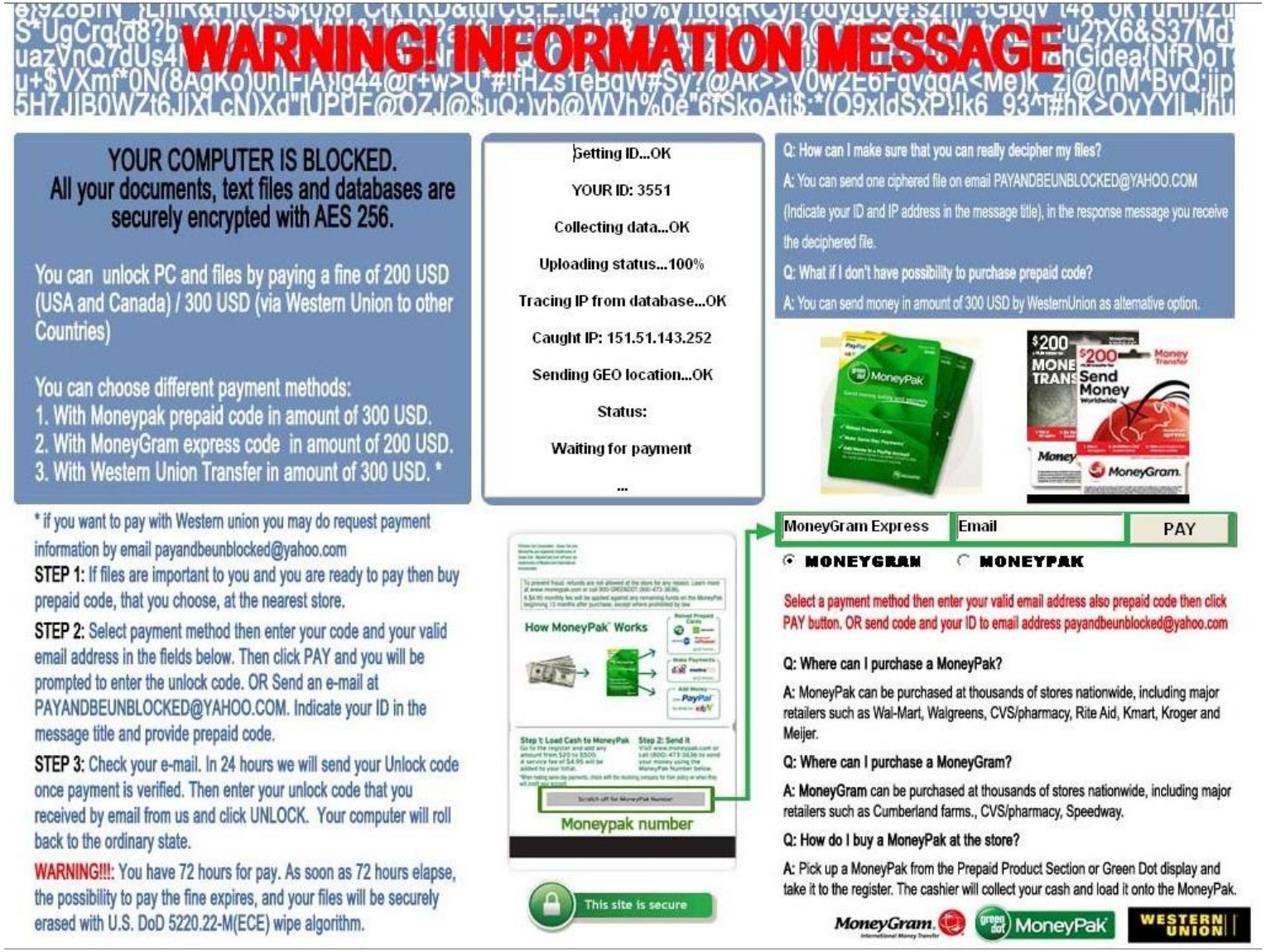
- Emulazione di siti pseudo istituzionali
- Panico nell'utente per accuse di reati gravi
- Facile guadagno
- Non rintracciabile

Le numerose varianti di FakeGdF 2/2

- Siae
- Polizia di Stato
- Altre istituzioni



Computer sotto ricatto: **DocEncrypter**



Ransomware di **2° Generazione** alias **Crypto-Malware**!

Malware che cifrano i file di dati di PC e SERVER e richiedono un riscatto in denaro per decifrarli.

Il riscatto richiesto è generalmente in cripto-valuta (come BITCOIN) da pagare attraverso il Dark/Deep WEB (rete Tor-Onion) su conti anonimi e difficilmente rintracciabili.

Alcuni esempi di ransomware:

Lockbit, HIVE, Conti, Everest, Quantum Locker, Stop / Djvu, BlackCat, BlackBasta, 54BB47H (Sabbath), Dharma, Ryuk, PETYA, Locky, TeslaCrypt, Cerber, CryptoLocker… etc.

Metodi di diffusione

- ✓ **via email** (ingegneria sociale)
- ✓ siti infettati (utilizzo di vulnerabilità)
- ✓ **altri malware**: SathurBot - HydraBot
- ✓ in bundle con altri software
- ✓ RDP/VPN


Da: Enel Spa <mcsrl@sicurezzapostale.it>
A: Carrozzeria Baggio
Cc:
Oggetto: Carrozzeria Baggio bolletta per la fornitura di energia elettrica

Enel
L'ENERGIA CHE TI ASCOLTA. Enel ENEL SERVIZIO ELETTRICO - Servizio di Maggior Tutela

DATI CLIENTE

Numero cliente: 59 369 524 Codice Fiscale: EPDZH02565QI

Carrozzeria Baggio

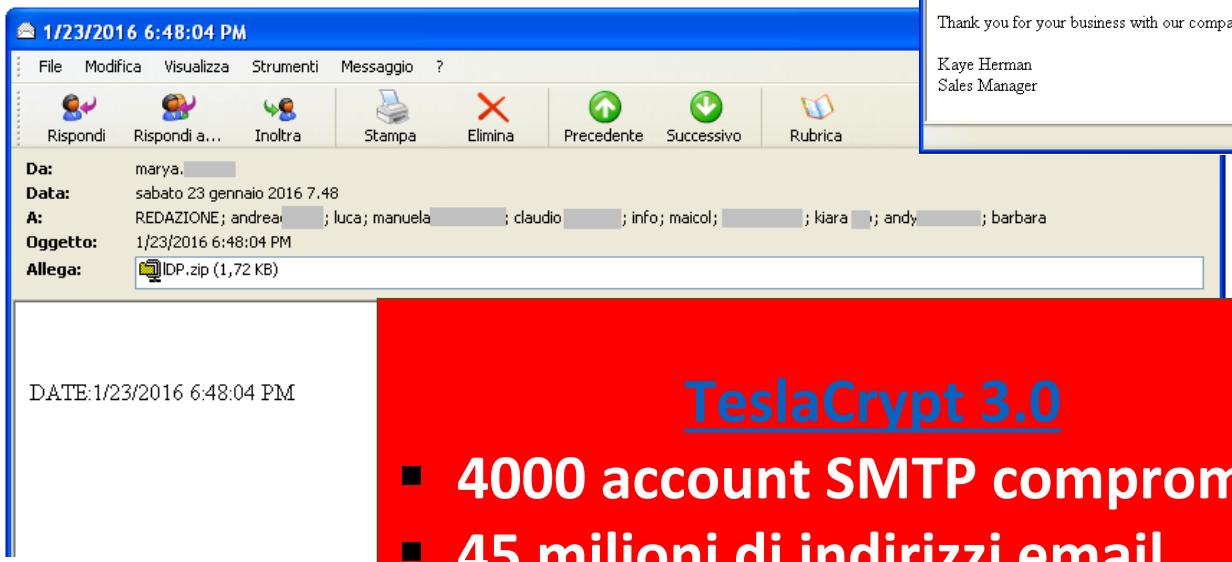
BOLLETTA PER LA FORNITURA DI ENERGIA ELETTRICA
N. fattura 499933859 del 1/03/2016 Bimestre gennaio - febbraio 2016
Totale da pagare entro il 31/03/2016: euro 336,10

Come da lei richiesto, sar`a addebitato nel giorno esatto della scadenza su conto corrente presso: 5330119521
Clicca qui per scaricare

DATI FORNITURARIEPILOGO IMPORTI FATTURATI

Politica sulla privacy

Enel adotta un apposito regolamento per la gestione ed il trattamento delle informazioni riservate, contenente anche le procedure per la comunicazione all'esterno di documenti ed informazioni concernenti Enel, con particolare riferimento alle informazioni privilegiate. Gli esponenti aziendali, i dipendenti e i collaboratori di Enel evitano comportamenti che possano dare luogo a fenomeni di insider trading e di manipolazione del mercato, anche da parte di terzi; al fine di garantire la massima trasparenza risultano adottate al riguardo procedure in materia di internal dealing rispettose della legge ed in linea con le best practice internazionali. Nel bilancio annuale sono pubblicate le azioni Enel possedute al termine

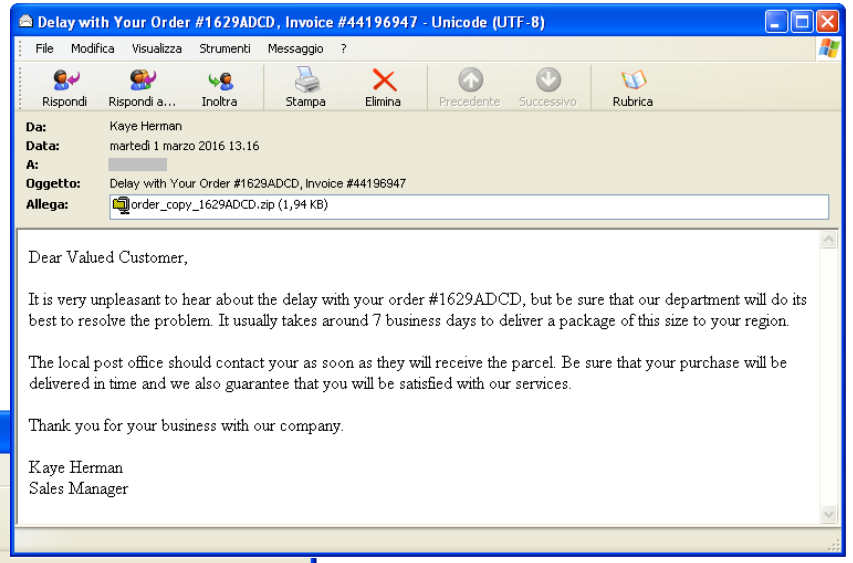

1/23/2016 6:48:04 PM

File Modifica Visualizza Strumenti Messaggio ?

Rispondi Rispondi a... Inoltra Stampa Elimina Precedente Successivo Rubrica

Da: marya.
Data: sabato 23 gennaio 2016 7.48
A: REDAZIONE; andrea; luca; manuela; claudio; info; maicol; ; kiara; andy; barbara
Oggetto: 1/23/2016 6:48:04 PM
Allega: IDP.zip (1,72 KB)

DATE:1/23/2016 6:48:04 PM


Delay with Your Order #1629ADCD, Invoice #44196947 - Unicode (UTF-8)

File Modifica Visualizza Strumenti Messaggio ?

Rispondi Rispondi a... Inoltra Stampa Elimina Precedente Successivo Rubrica

Da: Kaye Herman
Data: martedì 1 marzo 2016 13.16
A:
Oggetto: Delay with Your Order #1629ADCD, Invoice #44196947
Allega: order_copy_1629ADCD.zip (1,94 KB)

Dear Valued Customer,

It is very unpleasant to hear about the delay with your order #1629ADCD, but be sure that our department will do its best to resolve the problem. It usually takes around 7 business days to deliver a package of this size to your region.

The local post office should contact your as soon as they will receive the parcel. Be sure that your purchase will be delivered in time and we also guarantee that you will be satisfied with our services.

Thank you for your business with our company.

Kaye Herman
Sales Manager

TeslaCrypt 3.0

- **4000 account SMTP compromessi**
- **45 milioni di indirizzi email**

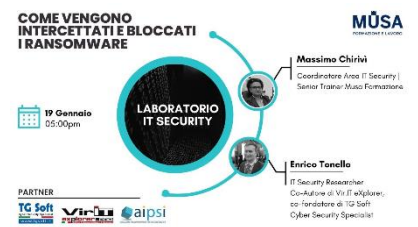
RDP Remote Desktop Protocol

- Violazione accesso RDP esposto sul web:
  - Furto di password / informazioni / dati.
  - Esecuzione di Ransomware/CryptoMalware.
  - Spostamento laterale.
  - Manomissione dei sistemi di sicurezza.

- Nel 2022 i principali Ransomware/CryptoMalware utilizzati sono stati:
  - **LockBit**;
  - HIVE;
  - **Conti**;
  - BlackCat;
  - BlackBasta;
  - Quantum Locker;
  - STOP / Djvu;
  - Makop;
  - ……;

Vir.IT explorer PRO
AntiVirus, AntiSpyware, AntiMalware, AntiRansomware

TG Soft
Cyber Security Specialist
www.tgsoft.it



Come difendersi dai ransomware

- Protezione multi-livello per difendersi dai ransomware:
  - ✓ Anti-virus attivo e sempre aggiornato
  - ✓ Windows, ma anche Java, Adobe Reader sempre aggiornati
  - ✓ Password degli utenti e dell'administrator complesse e non banali (L. 10)
  - ✓ Ove possibile attivare **SEMPRE** il controllo a 2 o più fattori MFA
  - ✓ **Protezione anti-ransomware ➔ mitigazione dell'attacco**
  - ✓ Backup offline

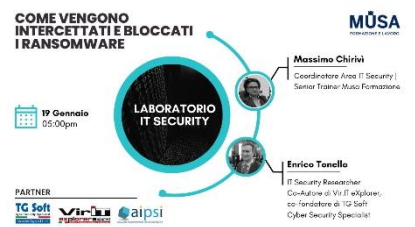
Protezione AntiRansomware ➔ Mitigazione dell'attacco

TG Soft Cyber Security Specialist dal 2013 ha sviluppato tutta una serie di tecnologie in grado di Salvare dalla cifratura i file di dati dell'utente integrando nell'ordine:

1. **2014-03 ➔ Sistema di Backup**, integrato nella suite Vir.IT eXplorer PRO, specificatamente progettato per proteggere dalla cifratura i dati dell'utente con dei contenitori di Backup ad accesso protetto così da escludere che:
   - un utente malintenzionato possa procedere sia volontariamente, cioè con intenti sabotatori, sia in «buona fede» a modificare tali file;
   - un agente informatico, come potrebbe essere un processo di cifratura in atto, sia in grado di modificare/cifrare questi dati…

   - I DATI SONO IN GRADO DI ESSERE PRESERVATI ANCHE DA UN PROCESSO DI CIFRATURA DERIVANTE DA UN RANSOMWARE DI NUOVA GENERAZIONE!!!

TG Soft
Cyber Security Specialist
www.tgsoft.it



2. **2015-05 ➔ Tecnologie EURISTICO-COMPORTAMENTALI,** sempre integrate nella suite **Vir.IT eXplorer PRO**, in grado di riconoscere nella fase iniziale dell'attacco un processo di cifratura da attacco simil-Ransomware in atto bloccando la cifratura nella fase iniziale dell'attacco con un tempo di reazione nell'ordine di 1/10° di secondo (cioè 100 millisecondi):

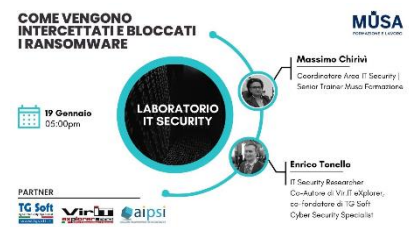
   - questo approccio **EURISTICO-COMPOSTAMENTALE** è in grado di salvaguardare dalla cifratura in attacchi reali, mediamente, non meno del **99,63%** dei file di dati che il ransomware avrebbe potuto cifrare;
   - inoltre vi sono dei **tool di recupero/ripristino** dei file che permettono il recupero dei file di dati cifrati nella fase iniziale dell'attacco con un'aspettativa asintotica al **100%**, se non del 100%, come accaduto in molte occasioni.

Protezione CryptoMalware

Protezione AntiRansomware ➔ Tool di ripristino / recupero

Per quei file che necessariamente verranno colpiti dal processo di cifratura nella fase iniziale dell'attacco **TG Soft** Cyber Security Specialist ha messo a punto 3 tool che permettono di recuperare come detto fino al 100% dei file cifrati senza perdere neanche una modifica ed il loro ripristino è realizzabile in, al più 5/10 minuti:

1. **Hacking della chiave di cifratura propria dell'attacco in atto ➔** possibile solo in quelle particolari situazioni ove la chiave di cifratura sia in «*chiaro*» e quindi su particolari tipologie di Ransomware (come accaduto nell'attacco mondiale da TeslaCrypt 3.0).
2. **Backup On-the-Fly (Backup al volo) ➔** non si tratta del Vir.IT Backup già citato ma di un sistema di **Backup automatico** presente nella suite **Vir.IT eXplorer PRO** che va a fare una copia di sicurezza in una cartella di servizio delle tipologie di file più comuni (.doc / .docx; .xls / .xlsx; .mdb; etc. etc.) da 3 kb a 3 Mb prima che questi siano cancellati da qualsiasi soggetto e possono essere ripristinato entro le 48 ore successive.
3. **Vir.IT Backup ➔** Si tratta dell'ultimo paracadute da dove ripristinare i file…



Come difendersi dai ransomware

- Protezione multi-livello per difendersi dai ransomware:
  - ✓ Anti-virus attivo e sempre aggiornato
  - ✓ Windows, ma anche Java, Adobe Reader sempre aggiornati
  - ✓ Password degli utenti e dell'administrator complesse e non banali (L. 10)
  - ✓ Ove possibile attivare **SEMPRE** il controllo a 2 o più fattori MFA
  - ✓ **Protezione anti-ransomware ➔ mitigazione dell'attacco**
  - ✓ Backup offline

Protezione AntiRansomware anche da attacchi «esterni»

- **Protezione Anti-Crypto Malware**: permette di bloccare cryptomalware anche di nuova generazione
- **Backup on-the-fly**: backup al volo di file documenti (da 2 KB a 3 MB) in fase di cancellazione, la copia dei file è mantenuta per 48 ore
- **Disattivazione automatica connessione di rete LAN**
- **Protezione da attacco esterno delle cartelle condivise**

Vir.IT explorer PRO
AntiVirus, AntiSpyware, AntiMalware, AntiRansomware

TG Soft
Cyber Security Specialist
www.tgsoft.it

RANSOMWARE Crypto-Malware… Attacco SENZA e CON PROTEZIONE Euristico-Comportamentale…

Simulazione su VM di attacco dal ransomware **STOP / Djvu** **su architettura SERVER-Client**

1 ➔ Senza alcuna protezione AntiRansomware Euristico-Comportamentale;

2 ➔ Con protezione AntiRansomware Euristico-Comportamentale solo sul SERVER;

3 ➔ Con protezione AntiRansomware Euristico-Comportamentale sia sul SERVER sia sui Client…

C.R.A.M.
CENTRO RICERCHE ANTI-MALWARE

Vir.IT explorer PRO
AntiVirus, AntiSpyware, AntiMalware, AntiRansomware

Vir.IT explorer PRO
AntiVirus, AntiSpyware, AntiMalware, AntiRansomware

TG Soft
Cyber Security Specialist
www.tgsoft.it

Conclusioni

Malware obiettivi:

- Economico
- Spionaggio
- Sabotaggio

Password Stealer:

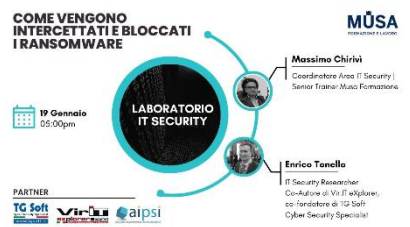
- Non memorizzare le password nel browser
- In caso di infezione -> cambiare la password
- Autentificazione multi-fattore

Ransomware come difendersi:

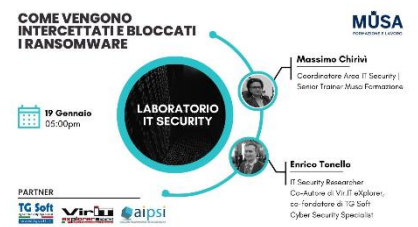
- AV con protezione anti-ransomware
- Backup offline (tempo di ripristino lungo)

Vir.IT explorer PRO
AntiVirus, AntiSpyware, AntiMalware, AntiRansomware

TG Soft
Cyber Security Specialist
www.tgsoft.it



Domande ?



GRAZIE dell'ATTENZIONE

Ing. Enrico TONELLO

IT Security Researcher, Cyber Security Evangelist
Socio e co-fondatore di TG Soft Cyber Security Specialist
E-mail: enrico.tonello@tgsoft.it - Tel. 049-8977432

Michele ZUIN

IT Security Researcher, Malware Analyst
Coordinatore Supporto Tecnico Clienti Vir.IT eXplorer PRO
E-mail: segreteria@tgsoft.it - Tel. 049-8977432

TG Soft
Cyber Security Specialist
www.tgsoft.it

Vir.IT explorer PRO
AntiVirus, AntiSpyware, AntiMalware, AntiRansomware

TG Soft
Cyber Security Specialist
www.tgsoft.it