

# COME VENGONO INTERCETTATI E BLOCCATI I RANSOMWARE

## 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

**MÜSA**  
FORMAZIONE E LAVORO



**19 Gennaio**  
05:00pm

**MÜSA**  
FORMAZIONE E LAVORO

PARTNER

**TG Soft**

Cyber Security Specialist

[www.tgsoft.it](http://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*



# RANSOMWARE... Ma quante se ne leggono in giro 1/2

**RaiNews**  
TECH  
ATTACCO SENZA PRECEDENTI VIA EMAIL  
**CRYPTOLOCKER SCATENATO: LA POLIZIA DÀ LA CACCIA AL VIRUS CHE BLOCCA I PC**  
Negli ultimi giorni la Polizia postale ha registrato una nuova ondata di attacchi contenenti il già noto virus Cryptolocker, che imperversa da tempo sul web. È un virus che infetta i computer con un allegato di una mail; di seguito arriva la richiesta di un "risatto" da pagare in bitcoin per liberare il pc

**Il Mattino**  
HOME NAPOLI AVELLINO BENEVENTO SALERNO CASERTA CALABRIA  
CASERTA  
Processo Eco 4, Cosentino: «Sostenni battaglia per Dda a non...  
CASERTA  
Maddaloni, arresti dopo la denuncia di Scialdone, ex presidente del Consorzio Unico di Bacino. Indagine...

**la tribuna**  
di Treviso  
COMUNI: TREVISO CONEGLIANO CASTELFRANCO MONTEBELLUNA VITTORIO VENETO ODERZO TUTTI I COMUNI  
HOME CRONACA SPORT VENETO NORDEST ECONOMIA ITALIA MONDO FOTO VIDEO RISTORANTI  
SI PARLA DI INCIDENTI STRADALI TYPAZ MENINGITE INCIDENTI PROFUGHI  
SOTTOCOSTO  
Sei in: TREVISO > CRONACA > CRYPTOLOCKER, NUOVA ONDATA DI DENUNCE  
**Cryptolocker, nuova ondata di denunce**  
Si moltiplicano i casi segnalati alla polizia del virus informatico che paralizza i computer e ruba i dati  
COMPUTER VIRUS AZIENDE  
23 febbraio 2016  
di RICCARDO LUNA

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

**VirIT explorer-PRO**  
AntiVirus, AntiSpyware, AntiMalware, AntiRansomware

**Il Fatto Quotidiano**  
TECNO  
KeRanger: il primo ransomware che attacca i Mac. Blocca tutto e chiede il riscatto

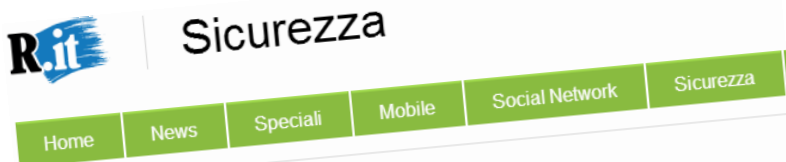
**Rai**  
Tecnologia  
Home News Speciali Mobile Social Network Sicurezza  
Vodafone Super ADSL. Parli e navighi da 25€ al mese + minuti illimitati

**"Paga o il virus distruggerà il pc": ora gli estorsori chiedono il riscatto**  
Da Cryptolocker a Cryptowall, privati e aziende sono sotto software che rubano documenti privati. Si infiltrano attraverso la trappola e chiedono di pagare in bitcoin per riavere il materiale

**Non aprite quella mail: attenzione al Cryptolocker**  
10 febbraio 2016  
Attenzione al Cryptolocker. È un virus che inganna gli utenti di posta elettronica in modo da ingannarli su presunte spie. Enti, gestori e fornitori di servizi (link o allegato a no... sul link o aprendo l'allegato in formato pdf o zip), viene immediatamente collegato al computer, anche di quelli eventualmente collegati a Internet. Gli informatici chiedono agli utenti, per riaprire i documenti, il pagamento di una somma di denaro, quale ricevere via e-mail un programma...



# RANSOMWARE... Ma quante se ne leggono in giro 2/2



## "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"



# 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



**Guardia di Finanza**  
*insieme per la legalità*

**Attenzione!!!**

È stata rivelata un'attività illegale. Il sistema operativo è stata bloccata per una violazione delle leggi della Repubblica Italiana!  
 È stata fissata una seguente violazione: Dal tuo indirizzo IP "95.236.187.73" era eseguito un accesso alle web-pagine contenenti la pornografia minorile, zo nonché la violenza dei bambini. Nel tuo computer sono stati trovati video-file contenenti la pornografia, elementi di violenza e la pornografia minorile.

**Dalla posta elettronica era effettuato anche la distribuzione dello spam con un senso recondito terroristico.  
 Il bloccaggio di computer serve per troncane l'attività illegale dalla parte tua.**

**I tuoi dati:** **IP:95.236.187.73**  
 Posizione: Italy, Padova  
 ISP: Telecom Italia S.p.a.

**Per togliere il bloccaggio devi pagare una multa di 100 euro.  
 Hai due seguenti varianti di pagamento:**

**1) Effettuare il pagamento tramite l'Ukash.**  
 Per questo inserisci il numero ricevuto nella colonna di pagamento, dopodiché premi OK (se hai più numeri, allora inseriscili uno dopo l'altro, dopodiché premi OK)

Se il sistema segnalerà un errore, allora dovrai mandare il numero per la posta elettronica [deposito@cyber-gdf.net](mailto:deposito@cyber-gdf.net).

**2) Effettuare il pagamento tramite il Paysafecard:**  
 Per questo inserisci per favore il numero ricevuto (nel caso di necessità insieme con la password) nella colonna di pagamento, dopodiché premi OK (se hai più numeri, allora inseriscili uno dopo l'altro, dopodiché premi OK).

Se il sistema segnalerà un errore, allora dovrai mandare il numero per la posta elettronica [deposito@cyber-gdf.net](mailto:deposito@cyber-gdf.net)

**Ukash Dove passo trovare Ukash?**  
 Puoi richiedere e ottenere Ukash presso migliaia di punti vendita, edicole, stazioni di servizio, bar e tabacchi e negozi di telefonia mobile dotati di terminale **Epay, Epipoli**.

Recati presso il punto vendita dotato di terminale **Epay, Epipoli** a te più vicino. Richiedi un voucher in contanti al negoziante. Il negoziante dovrà stampare e consegnarti un voucher Ukash con codice PIN da 19 cifre.

   
 epay relationship marketing group

  
 pay cash. pay safe.

## Le numerose varianti di FakeGdF 2/2

- Siae
- Polizia di Stato
- Altre istituzioni



**il computer è stato bloccato**

Sul computer sono stati individuati dei brani musicali scaricati illegalmente (piratati).

Scaricandoli, questi brani musicali sono stati riprodotti, comportando un reato ai sensi della Sezione 106 del Copyright Act. Il download di canzoni protette da copyright, tramite Internet o reti di condivisione di file musicali, è illegale ed è soggetto ad una multa o la reclusione per una pena fino a 3 anni, in conformità alla Sezione 106 del Copyright Act. Inoltre, il possesso dei brani musicali scaricati illegalmente è punibile ai sensi dell'art 184 comma 3 del codice penale e può anche portare alla confisca del computer con cui i file sono stati scaricati.

Il vostro Indirizzo IP: 82.56.187.93

Il vostro Hostname: host93-187-dynamic.56-82-r.retail.telecomitalia.it

Potete facilmente essere identificati tramite la rilevazione del vostro indirizzo IP e dell'hostname ad esso associato.

Il materiale pirata è stato cifrato ed è stato spostato in una cartella protetta per prevenire ulteriori danni.

Per sbloccare il computer e per evitare altre conseguenze giuridiche, siete obbligati a pagare una tassa di rilascio di 100 EUR. La somma è pagabile attraverso il nostro partner per pagamenti di Paysafecard. Dopo il pagamento, il computer sarà sbloccato automaticamente.

Il mancato rispetto di questa richiesta potrebbe comportare imputazioni penali e possibilità di detenzione.

Per eseguire il pagamento, inserite il codice Paysafecard acquisito nel campo bonifico, selezionate il valore del codice e quindi premete il pulsante "Invia".

SIAE è legittimato dalla legge - ed è in stretto contatto con i legislatori e la Polizia.



**Sblocca Computer**

Code:  valor: 100 EUR ▼


**Invia**

Inserisci il tuo codice utilizzando la Pin-Pad

1	2	3	4	5	6	7	8
9	0	indietro					

Punti vendita







Disponibile nelle tue vicinanze

paysafecard è disponibile in tutta sicurezza vicino a te in Italia, ad esempio presso numerose edicole, bar, tabaccai anche nei negozi Sisal e Penny.





**POLIZIA DI STATO**

**ATTENZIONE!**

Per motivi di sicurezza il suo sistema Windows è stato bloccato.

In seguito a visite a siti pornografici od infestati da virus, il computer è arrivato ad un livello critico oltre il quale potrebbe non funzionare più, e tutti i dati verranno persi. Per avere possibilità di recupero del sistema deve installare un programma aggiuntivo di sicurezza.

Questo programma a pagamento, studiato per i sistemi particolarmente infestati, protegge completamente il sistema dai virus e dai programmi malvagi, stabilizza il sistema del suo computer e previene la perdita dei dati.

Scelga la modalità di pagamento desiderata

 **DISPONIBILE** ✓

 **DISPONIBILE** ✓

Per migliorare (far guarire) il suo sistema, metta il codice per trasferire 100 Euro nei sistemi PaysafeCard o Ukash. Il codice può essere acquistato presso quasi tutti i fornitori di benzina oppure nelle tabaccherie. Tali codici si trovano in vendita anche presso qualsiasi locale dove si vendono le carte per ricaricare il cellulare.

Subito dopo la digitazione del codice e dopo la sua verifica, il suo computer sarà completamente aggiornato e protetto. Tutti i virus ed i cavalli di troia saranno eliminati.



# Computer sotto ricatto: DocEncrypter

**WARNING! INFORMATION MESSAGE**

**YOUR COMPUTER IS BLOCKED.**

All your documents, text files and databases are securely encrypted with AES 256.

You can unlock PC and files by paying a fine of 200 USD (USA and Canada) / 300 USD (via Western Union to other Countries)

You can choose different payment methods:

1. With Moneypak prepaid code in amount of 300 USD.
2. With MoneyGram express code in amount of 200 USD.
3. With Western Union Transfer in amount of 300 USD. \*

\* if you want to pay with Western union you may do request payment information by email [payandbeunblocked@yahoo.com](mailto:payandbeunblocked@yahoo.com)

**STEP 1:** If files are important to you and you are ready to pay then buy prepaid code, that you choose, at the nearest store.

**STEP 2:** Select payment method then enter your code and your valid email address in the fields below. Then click PAY and you will be prompted to enter the unlock code. OR Send an e-mail at [PAYANDBEUNBLOCKED@YAHOO.COM](mailto:PAYANDBEUNBLOCKED@YAHOO.COM). Indicate your ID in the message title and provide prepaid code.

**STEP 3:** Check your e-mail. In 24 hours we will send your Unlock code once payment is verified. Then enter your unlock code that you received by email from us and click UNLOCK. Your computer will roll back to the ordinary state.

**WARNING!!!!:** You have 72 hours for pay. As soon as 72 hours elapse, the possibility to pay the fine expires, and your files will be securely erased with U.S. DoD 5220.22-M(ECE) wipe algorithm.

Getting ID...OK

YOUR ID: 3551

Collecting data...OK

Uploading status...100%

Tracing IP from database...OK

Caught IP: 151.51.143.252

Sending GEO location...OK

Status:

Waiting for payment

...

Q: How can I make sure that you can really decipher my files?

A: You can send one ciphered file on email [PAYANDBEUNBLOCKED@YAHOO.COM](mailto:PAYANDBEUNBLOCKED@YAHOO.COM)

(Indicate your ID and IP address in the message title), in the response message you receive the deciphered file.

Q: What if I don't have possibility to purchase prepaid code?

A: You can send money in amount of 300 USD by WesternUnion as alternative option.



MoneyGram Express

Email

PAY

**MONEYGRAM**

**MONEYPAK**

Select a payment method then enter your valid email address also prepaid code then click PAY button. OR send code and your ID to email address [payandbeunblocked@yahoo.com](mailto:payandbeunblocked@yahoo.com)

Q: Where can I purchase a MoneyPak?

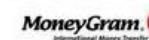
A: MoneyPak can be purchased at thousands of stores nationwide, including major retailers such as Wal-Mart, Walgreens, CVS/pharmacy, Rite Aid, Kmart, Kroger and Meijer.

Q: Where can I purchase a MoneyGram?

A: MoneyGram can be purchased at thousands of stores nationwide, including major retailers such as Cumberland farms., CVS/pharmacy, Speedway.

Q: How do I buy a MoneyPak at the store?

A: Pick up a MoneyPak from the Prepaid Product Section or Green Dot display and take it to the register. The cashier will collect your cash and load it onto the MoneyPak.





## 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.

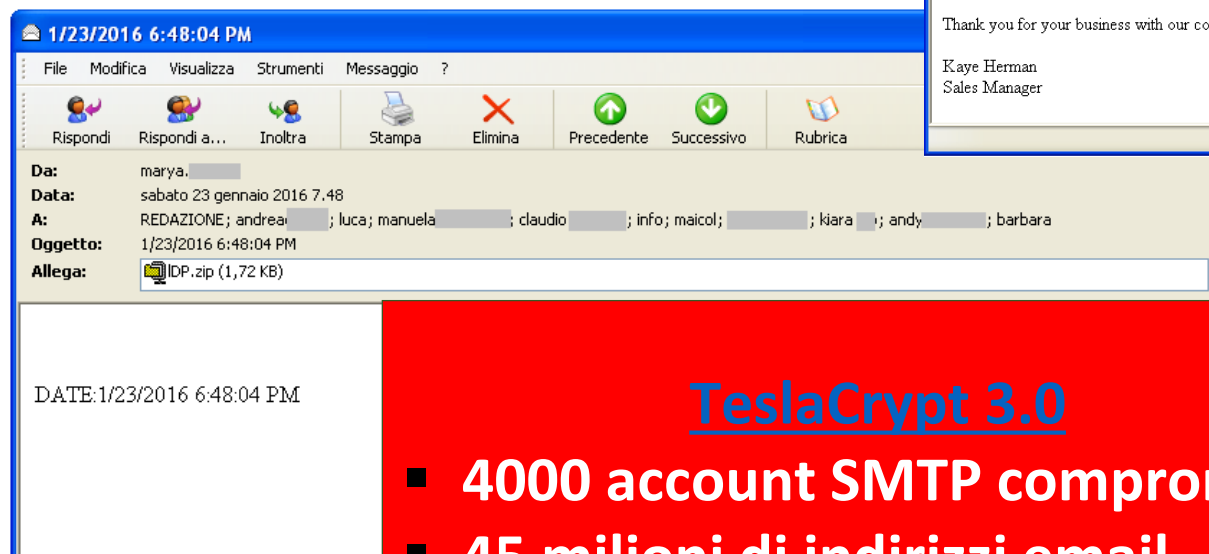
Il riscatto richiesto è generalmente in cripto-valuta (come BITCOIN) da pagare attraverso il Dark/Deep WEB (rete Tor-Onion) su conti anonimi e difficilmente rintracciabili.

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



## TeslaCrypt 3.0

- 4000 account SMTP compromessi
- 45 milioni di indirizzi email

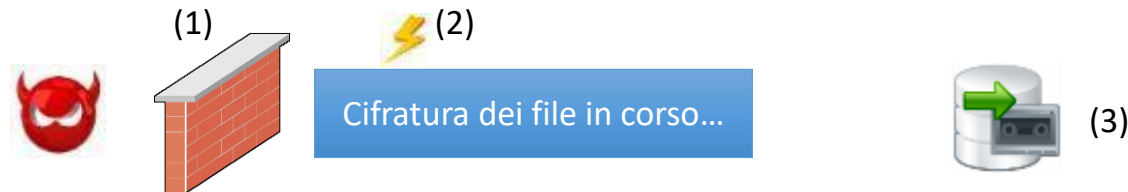


## RDP Remote Desktop Protocol

- 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**;
  - **BlackCat**;
  - **STOP / Djvu**;
  - **HIVE**;
  - **BlackBasta**;
  - **Makop**;
  - **Conti**;
  - **Quantum Locker**;
  - .....



# 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!!!

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  $1/10^{\circ}$  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



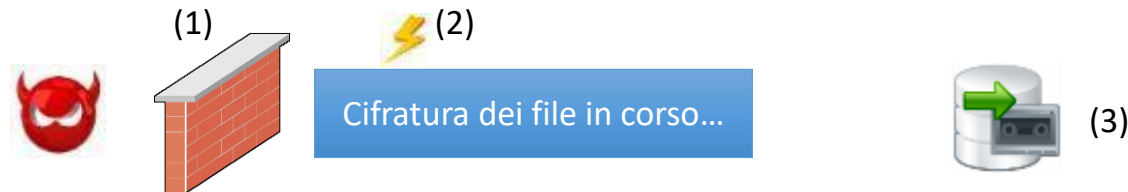


# Protezione AntiRansomware ➔ Tool di ripristino / recupero

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**



# 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...





# Conclusioni

## Malware obiettivi:

- Economico
- Spionaggio
- Sabotaggio

## Password Stealer:

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

## Ransomware come difendersi:

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



# 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](mailto:enrico.tonello@tgsoft.it) - Tel. 049-8977432*

## Michele ZUIN

*IT Security Researcher, Malware Analyst  
Coordinatore Supporto Tecnico Clienti Vir.IT e Explorer PRO  
E-mail: [segreteria@tgsoft.it](mailto:segreteria@tgsoft.it) - Tel. 049-8977432*

# TG Soft

Cyber Security Specialist

[www.tgsoft.it](http://www.tgsoft.it)



**TG Soft**  
Cyber Security Specialist  
[www.tgsoft.it](http://www.tgsoft.it)

