TG Soft di Tonello Gianfranco ed Enrico S.r.l.
Sede Legale ed operativa:
Via E. Fermi, 2 – 35030 Selvazzano Dentro (PD) - ITALIA
P. IVA/Cod. Fisc. IT03296130283
Tel. 049-4950030 - E-mail: segreteria@tgsoft.it
Sito Web: https://www.tgsoft.it

Proteggersi dai Ransomware bloccandoli entro i primi 100 millisecondi dalla loro esecuzione!

TG Soft Cyber Security Specialist protegge le PMI, e non solo, dagli attacchi informatici anche zero day… Una storia tutta italiana!

TG Soft dal 1992 sviluppa software antivirus VirIT per Ms-DOS che con l'avvento del Windows® trova la sua evoluzione nel 1998 nella suite Vir.IT eXplorer PRO come suite AntiVirus – AntiSpyware – AntiMalware e dal 2012 anche AntiRansomware protezione CryptoMalware.

I test internazionali a cui è sottoposto dal 2012 il motore di scansione di Vir.IT eXplorer PRO

Negli anni la suite Vir.IT eXplorer PRO è riuscita ad ottenere non solamente riconoscimenti a livello nazionale ma anche, e soprattutto, a superare test internazionali che ne hanno valutato l'efficacia e l'efficienza, tra i quali:

OPSWAT® (San Francisco US) ➔ Dal 2012 è stato inserito nella piattaforma Multimotore MetaDefender MAX in qualità di Partner tecnologia con certificazioni progressive:

- ✓ BRONZE (2012-10);
- ✓ SILVER (2016-05);
- ✓ GOLD (2020-06);
- ✓ PLATINUM (2020-09).

VB100® Virus Bulletin (London GB) ➔ Dal 2016 ha ottenuto oltre 40 certificazioni che hanno visto la suite Vir.IT eXplorer PRO ottenere nel 2025-07 la Certificazione VB100 Grade A. Il test VB100 è effettuato secondo rigidi protocolli standardizzati realizzato dalla società di Certificazione Indipendente inglese Virus Bulletin Ltd di Londra, raggiungendo risultati di eccellenza analogamente ai più noti software AntiVirus-Antispyware-AntiMalware internazionali.

ICSALabs (International Computer Security Association), una divisione indipendente di *Verizon Business* ➔ Che vede dal 2016-10 la suite Vir.IT eXplorer PRO essere "*Certified Anti-Virus Desktop/Server*" con il premio "**5-Year Excellence in Testing Security Award Winner for 2021**" accordato da **ICSALabs** a quei produttori software di sicurezza che testano con continuità i loro prodotti e mantengono le certificazioni di sicurezza anno dopo anno, aumentando l'elevato standard di qualità delle proprie tecnologie.

AppEsteem® (Seattle US) ➔ dal 2019-04 ottiene con continuità la Certificazione *AV DeceptorFighters* ad oggi 65 certificazioni periodiche superate con il massimo dei voti ottenibili.

Le partnership tecnologiche internazionali del motore di scansione di Vir.IT eXplorer PRO

OPSWAT® (San Francisco US) ➔ Dal 2012 il motore di Scansione di Vir.IT eXplorer è apprezzato partner tecnologico della piattaforma multimotore MetaScan prima e Meta Defender MAX poi.

MVI Microsoft Virus **Initiative** ➔ dal 2019 il motore di Vir.IT eXplorer PRO è testato periodicamente con prestazioni di efficacia ed efficienza apprezzate che gli permettono di essere riconosciuto dal Centro Sicurezza di Windows® nei vari S.O. per Client come anche per Server.

TG Soft di Tonello Gianfranco ed Enrico S.r.l.
Sede Legale ed operativa:
Via E. Fermi, 2 – 35030 Selvazzano Dentro (PD) - ITALIA
P. IVA/Cod. Fisc. IT03296130283
Tel. 049-4950030 - E-mail: segreteria@tgsoft.it
Sito Web: https://www.tgsoft.it

Virus TOTAL ➔ dal 2021 il motore di Vir.IT eXplorer PRO è stato riconosciuto come partner tecnologico ed inserito nella piattaforma Multimotore Virus TOTAL vedendosi riconosciute quelle caratteristiche di efficacia ed efficienza essendo un motore di scansione proprietario totalmente sviluppato e supportato in Italia.

Riconoscimenti internazionali dell'ing. Gianfranco Tonello CEO di TG Soft Cyber Security Specialist

Grazie all'attività di Ricerca & Sviluppo coordinate dall'ing. Tonello, riconosciute a livello internazionale, in rappresentanza di TG Soft è stato accreditato come membro di:

WILD List Organizzazione che si è occupata per decenni di catalogare i virus/malware realmente circolanti a livello mondiale dove Gianfranco Tonello, tra i pochi, se non unico italiano, ha avuto l'onore di essere accettato come Analista/reporter in rappresentanza della TG Soft, e di partecipare a questo gruppo di Ricercatori & Analisti con la maggior parte degli Analisti / Ricercatori dei team dei maggiori brand internazionali produttori di software AntiVirus / AntiMalware. Dopo un primo periodo di training, viste le ottimi analisi e considerazioni scambiate con gli altri analisti, è stato coinvolto nella catalogazione diventando parte del Team Core della WildList.

AMTSO Anti-Malware Testing Standars Organization (San Francisco CA United State) ➔ dal 2019 è stato accettato come membro stabile dal board di AMTSO, così da poter essere presente, in rappresentanza di TG Soft, ai più qualificati tavoli di discussione sulle modalità operative di esecuzione dei test effettuati sui software AntiVirus & AntiMalware e non solo.

C.A.R.O. Computer AntiVirus Research Organization ➔ che organizza eventi riservati ai soli ricercatori riconosciuti dal board come tra i più qualificati a livello internazionale dove:

- ✓ possono accedere tutti e solo i Ricercatori riconosciuti dal board;
- ✓ vengono presentati talk di altissimo livello tecnico ed è assolutamente vietato fotografare o fare video, come anche diffondere le informazioni che vengono presentate in questo ambito;
- ✓ non sono ammessi narratori fantasiosi proprio per preservare, il più possibile, la riservatezza di quanto viene presentato e discusso in questi incontri di altissimo livello tecnico e non solo.

Forse non è superfluo precisare che essere riconosciuti in tali ambiti è frutto di un lavoro di Ricerca & Sviluppo di valore assoluto e del riconoscimento di una più che buona reputazione internazionale.

Informative di sicurezza redatte periodicamente dal C.R.A.M. Centro Ricerche Anti Malware di TG Soft

L'enorme attività di Ricerca & Analisi di Virus & Malware informatici analizzati dal CRAM ci ha permesso di redigere dei bollettini di Cyber Security che riguardano:

- ✓ Le principali campagne di Phishing che hanno obiettivo l'Italia e non solo vengono monitorate ed illustrate in informative con cadenza mensile, ma vengono rese disponibili in libera e gratuita consultazione alla generalità dal sito ufficiale della TG Soft.
- ✓ Le principali campagne di Malspam che hanno obiettivo l'Italia e non solo vengono monitorate ed illustrate in informative standardizzate con cadenza settimanale e rese disponibili anch'esse in libera e gratuita consultazione alla generalità dal sito ufficiale.

Si tratta di attività utili a creare consapevolezza / awareness sulle campagne di Phishing come anche sulle campagne di Malspam che, forse, non è superfluo precisare che, ai non addetti ai lavori possono sembrare simili, ma che, vedono le campagne di **Malspam / Password Stealer** essere ben più insidiose e pericolose e possono essere foriere di attacchi informatici persistenti ed estremamente pericolosi.


In foto da sinistra a destra
ingg. Gianfranco ed Enrico Tonello

I fondatori della TG Soft (ingg. Gianfranco ed Enrico Tonello) nel 2021-05 sono stati indicati tra le <<*50 persone della cybersecurity italiana da seguire… secondo criteri generali tipo "la capacità di costruire qualcosa che resta", come imprese, enti, associazioni, e quello di "essere capace di modellare le idee, la cultura"… in una sorta di Who's Who del settore…*>> in un articolo redatto da Arturo di Corinto per La Repubblica

TG Soft di Tonello Gianfranco ed Enrico S.r.l.
Sede Legale ed operativa:
Via E. Fermi, 2 – 35030 Selvazzano Dentro (PD) - ITALIA
P. IVA/Cod. Fisc. IT03296130283
Tel. 049-4950030 - E-mail: segreteria@tgsoft.it
Sito Web: https://www.tgsoft.it

Gli attacchi RANSOMWARE un flagello che può essere evitato grazie al giusto approccio tecnologico

Tra un riconoscimento e l'altro la suite Vir.IT eXplorer PRO, e di conseguenza il nostro team di Ricerca & Sviluppo, ha dovuto suo malgrado, confrontarsi con tante nuove tipologie di minacce dove la più insidiosa e pericolosa sono i Ransomware cioè quei Malware che sono in grado di cifrare i dati degli utenti e richiedere un riscatto in denaro (generalmente in Crypto Valute di non facile tracciabilità BitCoin ma non solo…) per la loro de-cifratura e ha dovuto, suo malgrado, cercare un sistema progressivamente sempre più efficace ed efficiente per proteggere da questi attacchi estremamente insidiosi.

Vir.IT Backup un sistema di backup specificatamente progettato per resistere agli attacchi RANSOMWARE…

Il Team di Ricerca & Sviluppo che realizza la suite Vir.IT eXplorer PRO nel 2013 ha iniziato a sviluppare un sistema di Backup specificatamente progettato per blindare i file di dati dell'utente dalla cifratura. Si tratta di **Vir.IT Backup** che è stato integrato nella suite Vir.IT eXplorer PRO, presentato a vari eventi fieristici a partire dal 2014-04. Le tecnologie che stanno alla base di Vir.IT Backup permettono di proteggere i volumi di Backup dei file di dati dell'utilizzatore da qualsiasi attacco di cifratura grazie alla tecnologia proprietaria che è stata realizzata con la possibilità di ridondare le copie di sicurezza dei file di dati su servizi in Cloud e poter procedere alla loro cifratura di modo che la copia dei file salvata in remoto non siano facilmente consultabili da occhi indiscreti, forse, non è superfluo ricordare, in modo semplicistico, che il CLOUD è comunque, sempre, il/i computer di qualcun altro.

Oltre il "semplice" ripristino dei dati dai volumi di Backup…

Completata e rilasciata questa miglioria integrata nella suite Vir.IT eXplorer PRO il nostro team di Ricerca & Sviluppo si è fatto una domanda "retorica", ed ora che abbiamo messo il "*fieno in cascina e chiuso bene le porte*" possiamo fare qualcos'altro per proteggere i nostri clienti dai Ransomware ?

Naturalmente la risposta è Sì o almeno ci dobbiamo provare… Il nostro team di ingegneri & ricercatori dopo uno studio "*matto e disperatissimo…*" ci ha portato ad analizzare in modo sempre più accurato alcune delle principali famiglie di Ransomware in circolazione per individuarne i comportamenti comuni e provare a costruire un algoritmo / automa in grado di riconoscere i processi di cifratura in atto e quindi permetterci di bloccarli evitando che possano procedere alla cifratura dei file di dati dei nostri clienti, tutto ciò nel più breve tempo possibile dall'individuazione di un processo di sospetta cifratura in atto… Senza entrare nel dettaglio di come siamo riusciti ad ottenere tutto ciò siamo riusciti a stabilizzare un sistema di **riconoscimento** di un **processo di cifratura / attacco Ransomware** di cifratura dei file di dati **nell'intorno dei primi 100 millisecondi**, cioè 1/10° di secondo (di fatto un battito di ciglia…), **dall'attivazione** di questo/i processo/i malevolo/i e salvaguardare dalla cifratura, dagli ultimi test effettuati su attacchi Ransomware reali presenti in natura anche, e soprattutto, Zero Day, mediamente, non meno del **99,87%** dei file di dati dell'insieme dei computer presidiati con la nostra suite configurata secondo le specifiche tecniche e raccomandazioni del nostro team.

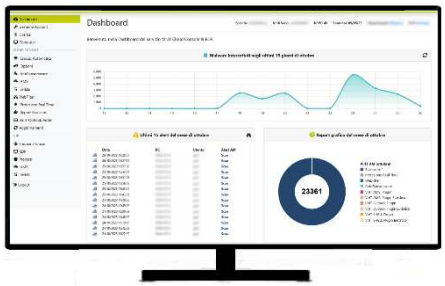
Recuperare i file cifrati nella fase iniziale dell'attacco

Per i file che dovessero essere stati cifrati nella fase iniziale dell'attacco, cioè quello **0,13%** sono state integrate delle tecnologie di recupero/ripristino che possono arrivare a recuperare quei pochi file cifrati nella fase iniziale dell'attacco, fino al 100%, si tratta di:

- ⇨ un sistema automatico di **recupero della chiave di cifratura** così da poter decifrare i file dopo la conclusione dell'attacco.
- ⇨ **Backup On-The-Fly** un sistema, anch'esso automatico, che permette di/ripristinare le tipologie di file di dati più comuni e farne il ripristino senza perdere nessuna modifica effettuata fino al momento dell'attacco Ransomware di cifratura dei file di dati.
- ⇨ Ultimo, ma non ultimo, andare a recuperare i file di dati cifrati nella fase iniziale dell'attacco dai "**volumi di file**" generati e protetti dalle tecnologie rese disponibili da **Vir.IT Backup.**

TG Soft di Tonello Gianfranco ed Enrico S.r.l.
Sede Legale ed operativa:
Via E. Fermi, 2 – 35030 Selvazzano Dentro (PD) - ITALIA
P. IVA/Cod. Fisc. IT03296130283
Tel. 049-4950030 - E-mail: segreteria@tgsoft.it
Sito Web: https://www.tgsoft.it

Tutte queste tecnologie sono integrate nelle suite Vir.IT eXplorer PRO AntiVirus + AntiSpyware + AntiMalware + AntiRansomware protezione CryptoMalware che si basa su tecnologie Euristico-Comportamentali.
Quanto descritto è solo una parte delle tecnologie che la TG Soft Cyber Security Specialist può offrire poiché abbiamo realizzato e sono già disponibili dal 2023:



⇨ un sistema di **gestione centralizzata** della suite **Vir.IT eXplorer PRO** denominato **CLOUD Console** molto utile per la gestione centralizzata della situazione in rete LAN come anche dei computer "dispersi" o che si aggiornano in modalità Stand-Alone.

⇨ **Vir.IT CLOUD Console + EDR** (Endpoint Detection & Response) che vi mette a disposizione una piattaforma Web per avere sotto controllo in modo centralizzato tutta una serie di informazioni sulle anomalie dei processi e quant'altro per permettervi di rilevare situazioni anomale e intervenire in via preventiva per prevenire attacchi informatici di varia natura e sventarli prima che possano accadere.

⇨ Vista la consolidata esperienza del nostro Team di ingegneri, analisti e ricercatori di Virus & Malware informatici un **servizio** di **supporto SOC remotizzato** per aiutarvi a disambiguare le situazioni anomale che vengono segnalate in modo automatizzato o eventuali dubbi e/o necessità di supporto da parte del personale del vostro SOC (Security Operation Center).

Potersi avvalere di un'azienda italiana i cui fondatori dal 1990 analizzano virus & malware e continuano a farlo oramai da 35 anni con un consolidato team di Analisti che, nel tempo è stato aggregato e che, tutti i giorni, si trova a fronteggiare minacce informatiche di nuova generazione è un plus da non sottovalutare poiché l'esperienza non si costruisce certo dall'oggi al domani.


repubblica.it

Scienze e Tecnologia

▲ Enrico e Gianfranco Tonello

LA STORIA

Gli artigiani italiani che ci difendono dai cybercriminali

Enrico e Gianfranco Tonello soci co-fondatori di TG Soft Cyber Security Specialist di Padova.

Per approfondimenti sulle nostre tecnologie 100 x 100% sviluppate e supportate in Italia non esitate a contattarci chiamando gli uffici della TG Soft Cyber Security Specialist.
https://ww.tgsoft.it