Proteggersi dai Ransomware

TG Soft Cyber Security Specialist protegge le Pmi, e non solo, dagli attacchi informatici anche zero day

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

I test internazionali a cui è sottoposta la suite Vir.IT eXplorer PRO

Negli anni Vir.IT eXplorer PRO è riuscito 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 tecnologico con certificazioni progressive: BRONZE (2012); SILVER (2016); GOLD (2020-06); PLATINUM (2020-09);
VB100® Virus Bulletin (London GB) dal 2016 ha ottenuto oltre 40 certificazioni, raggiungendo il Grado A nel luglio 2025;
ICSALabs (International Computer Security Association, divisione indipendente di Verizon®), Vir.IT eXplorer PRO ottiene il premio "5-Year Excellence in Testing Security Award Winner for 2021", in quanto ha superato con continuità dal 2016-10 i test "Certified Anti Virus Desktop/Server", aumentando l'elevato standard di qualità delle proprie tecnologie.

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

La prima collaborazione internazionale è nata nel 2012 con OPSWAT® che ha riconosciuto il motore di scansione di Vir.IT eXplorer partner tecnologico della piattaforma multimotore MetaScan prima e Meta Defender MAX poi.
Dal 2019 il motore di Vir.IT eXplorer PRO viene testato periodicamente per essere riconosciuto dal centro sicurezza di Windows® (MVI Microsoft Virus Initiative).
Nel 2021 ottiene il riconoscimento come partner tecnologico in Virus TOTAL, entrando come unico motore di scansione proprietario totalmente sviluppato in Italia.
Grazie all'attività di ricerca & sviluppo coordinate dall'ingegnere Gianfranco Tonello, 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.

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

Tra un riconoscimento e l'altro della suite Vir.IT eXplorer PRO, il team di ricerca e sviluppo ha dovuto, suo malgrado, confrontarsi con tante nuove tipologie di minacce, tra cui la più insidiosa e pericolosa è il Ransomware cioè quel Malware che è in grado di cifrare i dati degli utenti e richiedere un riscatto in denaro (generalmente in Crypto Valute, BitCoin ma non solo) per la loro decifratura, questo lo ha portato a cercare un sistema progressivamente sempre più efficace ed efficiente per proteggere da questi attacchi estremamente insidiosi.
Vir.IT Backup è un sistema di backup specificatamente progettato per resistere agli attacchi Ransomware. Il team di ricerca e sviluppo che realizza la suite Vir.IT eXplorer PRO, nel 2013 ha iniziato a sviluppare un sistema di backup in grado di proteggere i file di dati dell'utente dalla cifratura. Si tratta di Vir.IT Backup che è stato integrato nella suite Vir.IT eXplorer PRO e 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 e/o cancellazione.

Oltre il "semplice" ripristino dei dati dai volumi di backup

Il team di ingegneri e ricercatori di TG Soft ha analizzato in modo sempre più accurato alcune delle principali famiglie di Ransomware per individuarne i comportamenti comuni e provare a costruire un algoritmo in grado di riconoscere i processi di cifratura in atto e quindi bloccarli evitando che possano criptare i file di dati, tutto ciò nel più breve tempo possibile dall'individuazione di un processo di sospetta cifratura in atto.
Si è riusciti a stabilizzare un sistema di riconoscimento di un processo di cifratura / attacco Ransomware nell'intorno dei primi 100 millisecondi e salvaguardare la maggior parte dei file dalla cifratura. Dagli ultimi test effettuati su attacchi Ransomware reali presenti in natura, mediamente, vengono salvati non meno del 99,87 per cento dei file di dati ove sia presente la suite Vir.IT eXplorer PRO.

Servizi di cyber security avanzati per la protezione degli Endpoint

TG Soft dal 2023 ha sviluppato un sistema di monitoraggio degli EndPoint, attraverso una piattaforma in Cloud che permette di monitorare comodamente da un unico panello web tutti gli Endpoint ove è installato Vir.IT eXplorer PRO, denominato CLOUD Console.
Con Vir.IT CLOUD Console + EDR (Endpoint Detection & Response) sono inoltre disponibili una serie di informazioni sulle anomalie dei processi e quant'altro che permettono di rilevare situazioni sospette e intervenire per prevenire attacchi informatici di varia natura.
Inoltre rendiamo disponibile un servizio di supporto SOC remotizzato, da parte di un Team di ingegneri, analisti e ricercatori di Virus & Malware informatici, che vi affiancherà nella protezione della vostra rete IT.
Potersi avvalere di un'azienda italiana i cui fondatori dal 1990 analizzano virus & malware, con una consolidata esperienza oramai da 35 anni è un plus da non sottovalutare poiché l'esperienza non si costruisce dall'oggi al domani. •BG

Enrico e Gianfranco Tonello di TG Soft

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 per cento, 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 per cento. Si tratta di un sistema automatico di recupero così da poter decifrare i file dopo la conclusione dell'attacco.
Backup On-The-Fly è un sistema, anch'esso automatico, che permette di recuperare/ripristinare le tipologie di file più comuni e farne il ripristino senza perdere nessuna modifica effettuata fino al momento dell'attacco Ransomware di cifratura. Ultimo, ma non ultimo, permette di andare a recuperare i file di dati cifrati nella fase iniziale dell'attacco dai "volumi" protetti da Vir.IT Backup. Tutte queste tecnologie sono integrate nelle suite Vir.IT eXplorer PRO AntiVirus + AntiSpyware + AntiMalware + AntiRansomware basato su tecnologie euristico-comportamentali.