

Protezione Crypto-Malware Anti-Ransomware

Vir.IT eXplorer PRO integra tecnologie in grado di salvaguardare dalla cifratura (crittografia), mediamente, non meno del 99,63% dei file di dati di uso quotidiano da attacchi Crypto-Malware anche di nuova generazione delle famiglie/tipologie ad oggi note: CryptoLocker; CryptoWall; CryptoEncoder/CrySis; TeslaCrypt; Locky; CryptoRokku; Cerber; HydraCrypt; Petya 1.0; CryptoFBI; Sage; CryptoShield; Spora; CryptoShade, CryptoXmas etc.



Fig. 11
Protezione euristico-comportamentale Anti-CryptoMalware
Videata di Alert che segnala il rilevamento di un attacco CryptoMalware in atto e indica le istruzioni necessarie a mitigare i possibili danni da questi derivanti.

Quei pochi file che dovessero venire cifrati nella fase iniziale dell'attacco potranno essere decrittografati/ripristinati attraverso:

- l'intercettazione in memoria della chiave di cifratura nella fase iniziale dell'attacco che permetterà di decodificare i file recuperandoli senza perdere alcuna modifica;
- Backup On-The-Fly che effettua automaticamente copie di sicurezza dei file di dati in via preventiva.

Tecnologie che permettono di ripristinare fino al 100% dei file di dati crittografati nella fase iniziale dell'attacco.

Eventuali altri file che non fosse possibile decodificare né con la chiave privata intercettata in memoria né attraverso Backup On-The-Fly potranno essere ripristinati selettivamente da Vir.IT BackUp se preventivamente configurato ed attivato.

VirIT Mobile Security

L'AntiMalware di TG Soft per Android™ dalla versione 4.0 alla 6.0 (Ice Cream, Sandwich, Jelly Bean, Kitkat, Lollipop e Marshmallow).



Per Smartphone e Tablet Android™ 4.0+



VirIT Mobile Security è una suite progettata specificamente per proteggere i dispositivi Android™.

In particolare, VirIT Mobile Security offre:

- Protezione dai malware per Android™, tramite il rilevamento automatico di app malevole alla loro installazione, e automaticamente ad ogni aggiornamento delle firme.
- Protezione in tempo reale delle SD Card.
- Protezione da SMS di spam, tramite il rilevamento automatico di URL malevoli.
- Navigazione web sicura, tramite l'analisi automatica degli URL delle pagine web quando si naviga con Android browser e/o Google Chrome.
- Monitoraggio del traffico di rete entrante ed uscente.
- Protezione della privacy.
- Gestione app ed invio di applicazioni sospette al C.R.A.M. per analisi e ricerca di malware.
- Gestione online dei Vostri dispositivi Android.
- Pianificazione delle scansioni delle app.
- Aggiornamenti automatici delle firme dei malware.
- Log delle attività dei moduli di VirIT Mobile Security.



Fig. 12 - La home screen di VirIT Mobile Security

Per maggior info sulle caratteristiche tecniche di VirIT Mobile Security PRO e provare la versione Lite collegatevi alla pagina dedicata del nostro sito:



Una soluzione completa ...

... per Windows Microsoft®



Individua virus e malware
noti e di nuova generazione grazie all'utilizzo di tecnologie Euristiche.



DEEP SCAN
tecnologia che identifica virus polimorfici.



INTRUSION DETECTION
tecnologia in grado di segnalare l'intrusione di virus e malware non riconosciuti e/o di nuova generazione.



MACRO VIRUS ANALYSER
rileva macro virus di nuova generazione.



Rimuove Virus e Malware
noti e di nuova generazione grazie alle funzioni speciali dei tools di riparazione.



Protegge con scudi residenti a 32 e 64 bit che bloccano in tempo reale i tentativi di infezione dai virus e dai malware riconosciuti.



Vir.IT SAFE Browser
segnala possibili tentativi di frode informatica come dirottamento bonifici, furto credenziali di accesso Home Banking, posta elettronica, social network etc.



Installazione centralizzata
in rete locale attraverso Active Directory.



PROTEZIONE Crypto-Malware
anche varianti di nuova generazione delle famiglie/tipologie ad oggi note: CryptoLocker; CryptoWall; CryptoEncoder/CrySis; TeslaCrypt; Locky; CryptoRokku; Cerber; HydraCrypt; Petya 1.0; CryptoFBI; Sage; CryptoShield; Spora; CryptoShade, CryptoXmas etc.

... e Android®

Microsoft, MS-DOS, Windows e i loghi MS-DOS e Windows sono marchi registrati della Microsoft Corporation. • Android e i loghi Android sono marchi registrati da Google Inc.



TG Soft S.a.s.

Sede Operativa:

Via Pitagora, 11/b
35030 Rubano (PD) - ITALIA

Segreteria generale:

Tel. 049.8977432 - Fax 049.8599020

E-mail: segreteria@tgsoft.it

E-mail: info@tgsoft.it

Ufficio commerciale:

Tel. 049.8977432 - Fax 049.8599020

E-mail: commerciale@viritpro.com



Vir.IT BACKUP crea copie di sicurezza dei tuoi dati per proteggerli dai malware che potrebbero tentare di cifrarli a scopo di riscatto (es. Crypto-Malware/Ransomware).



Vir.IT Controllo Genitori - Parental Control
rende più sicuro l'accesso al web ai tuoi figli.



Vir.IT SCAN MAIL
Scudo a 32 bit per Win 95/98/ME® e Win 2000/XP/Server 2003® per il blocco preventivo delle e-mail con allegati infetti.



Vir.IT Console SERVER Client
modulo per la gestione centralizzata degli aggiornamenti dei software in rete LAN.



Vir.IT Webfilter Protection
per il blocco preventivo delle pagine Web riconosciute dal C.R.A.M. come infette/compromesse così da evitare di accedervi o esservi dirottati.



Aggiornamento automatico
delle firme e dei software dell'intera suite via Internet.



Vir.IT PERSONAL FIREWALL
per Win 95/98/ME® e Win 2000/XP/Server 2003® 32 bit, protegge il computer dalle intrusioni indesiderate e dagli attacchi hacker.



Assistenza telefonica e on-line
diretta dal produttore in lingua italiana.



C.R.A.M. Centro Ricerche Anti-Malware
si occupa di analizzare virus e malware informatici per i S.O. Windows® Microsoft® e Android™ per comprenderne il funzionamento e aggiornare i software per l'univoca identificazione e corretta rimozione.



VirIT Mobile Security
per Android™ dalla versione 4.0 alla 6.0 (Ice Cream Sandwich, Jelly Bean, Kitkat, Lollipop e Marshmallow).

Rivenditore autorizzato

Grafica & Stampa: www.composervic.com



i ransomware
ti hanno cifrato i dati?

PROTEGGILI! con **Vir.IT**

integra tecnologie anti-ransomware contro i
malware che richiedono un riscatto!



Nuove Tecnologie
ancora più sicurezza



Windows 10 compatible ...e per tutti gli altri S.O. Windows Microsoft® sia Client che Server

Windows 8 / 8.1 Windows Server 2012

..e ora anche VirIT Mobile Security PRO per ANDROID®



TG Soft nasce nel 1992 come Team emergenziale per il circuito bancario nazionale per l'analisi di virus/malware informatici di nuova generazione, cioè non ancora identificati dai più noti brand internazionali di software AntiVirus, per comprenderne il funzionamento e realizzare software ad hoc per la loro univoca identificazione e rimozione. Dopo l'esperienza maturata nell'attività di supporto emergenziale TG Soft ha realizzato un software AntiVirus con motore proprietario non meno performante dei più noti brand internazionali di Software AV in uso, in particolare, negli ambiti bancari. Nel 1993 viene rilasciata la prima release di **Vir.IT** per DOS. L'obiettivo è quello di rendere disponibile un software antivirus costantemente aggiornato per l'identificazione e la rimozione dei virus e dei malware più diffusi, corredato da un servizio di assistenza e pronto intervento per la

soluzione di eventuali problematiche emergenziali generate dai virus/malware informatici di nuova generazione, che possono rappresentare i maggiori pericoli per il nostro prezioso patrimonio informatico/informativo. Con l'aumentare dei virus/malware circolanti, inviati al C.R.A.M. (Centro Ricerche Anti-Malware) di TG Soft dai maggiori gruppi bancari ed aziende italiane e soprattutto grazie alle collaborazioni con alcuni dei centri di ricerca più noti del panorama internazionale, dal 1997, TG Soft rende disponibile **Vir.IT eXplorer** aggiornato per proteggere e rimuovere le più diffuse minacce derivanti da virus e malware informatici realmente circolanti nel mondo. Oltre 2 milioni 300 mila installazioni di **Vir.IT eXplorer Lite** e **PRO** ne testimoniano l'apprezzamento non solo in Italia ma anche in oltre 30 paesi nel mondo.

Vir.IT eXplorer-PRO • AntiVirus - AntiSpyware - AntiMalware per Windows® Microsoft



Per PC e SERVER
Windows®
Microsoft



Fig. 1 - Vir.IT eXplorer modulo di scansione-rimozione dei virus/malware. Permette analisi e bonifica in ambiente Windows®, sia Client sia SERVER, su tutti i dischi locali e remoti, oppure attraverso la rete locale LAN. Include speciali tool diagnostici: Process Manager, Ads (Alternate data stream) Look, Vir.IT Agent System tecnologia per la rimozione dei rootkit.

Vir.IT eXplorer PRO è costituito da vari moduli e tecnologie:
• **Vir.IT eXplorer** per la ricerca e la rimozione di virus e malware informatici. Le scansioni possono essere effettuate sia manualmente sia automatizzate/pianificate tramite Scheduler.

- **Vir.IT Security Monitor** per la protezione in tempo reale dagli attacchi di virus/malware e per il blocco preventivo di file infetti. La tecnologia **Vir.IT Safe Browser** permette di segnalare eventuali tentativi di frodi informatiche. Le tecnologie euristico-comportamentali **Anti-CryptoMalware** sono in grado di bloccare nella fase iniziale la crittografia dei dati anche nel caso di varianti di nuova generazione.



Fig. 2 - Scheduler. Permette di impostare scansioni automatiche in giorni e orari prestabiliti.



Fig. 3 - Vir.IT Safe Browser. Tecnologia integrata in Vir.IT Security Monitor per evitare frodi informatiche.

- **Vir.IT Backup** per creare copie di sicurezza dei tuoi dati. Protegge i file di backup anche da attacchi Crypto-Malware di famiglie/topologie di nuova generazione.
- **Vir.IT Controllo Genitori** filtra l'accesso al web in ambito privato e aziendale con approccio BlackList o WhiteList anche per fasce orarie. **BlackList**: impedisce la navigazione sui siti non raccomandabili per categorie. **WhiteList**: permette la navigazione sui soli siti autorizzati dall'ente/impresa (Policy Aziendali).
- **Vir.IT Webfilter Protection** per il blocco preventivo delle pagine Web riconosciute dal C.R.A.M. come infette evitando di venire dirottati su siti malevoli.
- **Vir.IT Scan Mail** per il controllo preventivo della posta elettronica.

Caratteristiche principali di Vir.IT eXplorer:

- Identifica e rimuove virus, worm, trojan, keylogger, backdoor, BHO, LSP, hijacker, dialer, rootkit, adware, fraudtool, spyware, malware e crypto-malware.
- Identifica anche virus/malware sconosciuti e/o di nuova generazione grazie alle tecnologie euristico-comportamentali.

- Identifica MACRO VIRUS di nuova generazione.
- Identifica VIRUS POLIMORFICI e ROOTKIT GENERICI come Sinowal e TDL.
- Scansiona automaticamente le unità di archiviazione di massa (memory card, USB Drives etc.) all'inserimento.
- Aggiornamenti automatici Motore+Firme via internet.
- Tools di diagnosi dei processi attivi e dei device drivers.

Vir.IT Console SERVER-Client

Modulo centralizzato per la gestione e l'aggiornamento automatico della suite **Vir.IT eXplorer PRO** in una rete LAN. È costituito da due componenti:
a) **Vir.IT Console SERVER**
b) **Vir.IT Console Client**

Vir.IT Console SERVER, installato su un unico computer della rete LAN che abbia accesso ad internet, permette di scaricare e distribuire gli aggiornamenti della suite (motori e firme) su tutti i client.

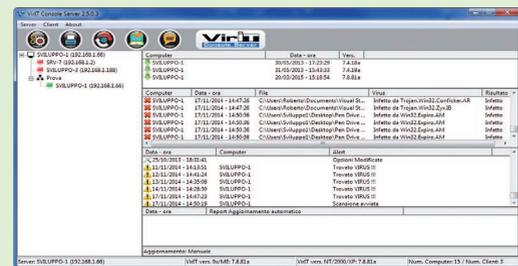


Fig. 4 - Vir.IT Console SERVER. Permette di aggiornare automaticamente la suite Vir.IT eXplorer-PRO attraverso la rete LAN. Permette all'amministratore di verificare lo stato di aggiornamento dell'antivirus su ogni computer, con reportistica centralizzata delle infezioni in corso.

Vir.IT Console SERVER può essere installato sui seguenti sistemi operativi: Windows NT/2000/XP/Vista, Windows Server 2003/2008/2012, Windows 7, Windows 8/8.1 e Windows 10, dando la possibilità all'amministratore della rete di gestire tutti i client che hanno Vir.IT Console Client operativo.

Il computer dove viene installato Vir.IT Console Server funge da Server antivirus e dovrà necessariamente essere collegato alla rete LAN ed a INTERNET.

La console di amministrazione permette di controllare lo stato di aggiornamento dell'antivirus installato su ogni client, inoltre segnala lo stato di aggiornamento e quindi di sicurezza dei principali software installati (Browser, Java, FlashPlayer etc.).



Vir.IT Console Client è il componente che interroga **Vir.IT Console SERVER**, provvedendo a prelevare l'ultima release delle firme e, se disponibile, anche del motore per il sistema operativo di competenza, aggiornando automaticamente i client.



Fig. 6 Vir.IT Console Client: Modulo di aggiornamento antivirus sui client.



Fig. 7 - Aggiornamento via internet. Aggiornamenti continui sono disponibili presso il sito web di Vir.IT eXplorer-PRO prelevabili direttamente, in modalità automatica o manuale, da Vir.IT Console Server.

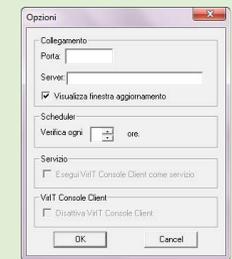


Fig. 8 Opzioni di Vir.IT Console Client

Vir.IT Backup => File di backup protetti anche dai Crypto-Malware di nuova generazione

È una tecnologia di backup avanzato per proteggere i dati dai virus/malware (anche di nuova generazione) che crittografano i file del computer al fine di richiederne il riscatto per decrittografarli. (es. CryptoLocker, CTB-Locker, CryptoWall, TeslaCrypt, CryptoLocky, CryptoCerber etc.).



Fig. 9 - Il menu a discesa di Vir.IT Backup accessibile dallo scudo residente in tempo reale Vir.IT Security Monitor.

Vir.IT Backup è una funzionalità integrata nello scudo residente in tempo reale Vir.IT Security Monitor che ne impedisce la modifica evitando che la loro integrità venga compromessa.



La creazione del Backup dei vostri dati più preziosi è impostabile in modo semplice e rapido e, dopo questa operazione preliminare, il backup viene effettuato in modo pianificato automaticamente.

Fig. 10 - La finestra di creazione di un nuovo backup.

Vir.IT Backup permette di proteggere i file di backup da questo generati ed aggiornati non solo dai crypto-malware già noti, ma anche (e soprattutto) da quelli di nuova generazione, non ancora intercettati da alcun software AntiVirus-AntiMalware. I file di backup non possono essere modificati da terzi, o da agenti ransomware, poiché presidiati da Vir.IT Security Monitor, che ne impedisce la modifica evitando che la loro integrità venga compromessa.