Stop al virus sequestra PC

COMMENTI • TENDENZE • RETROSCENA

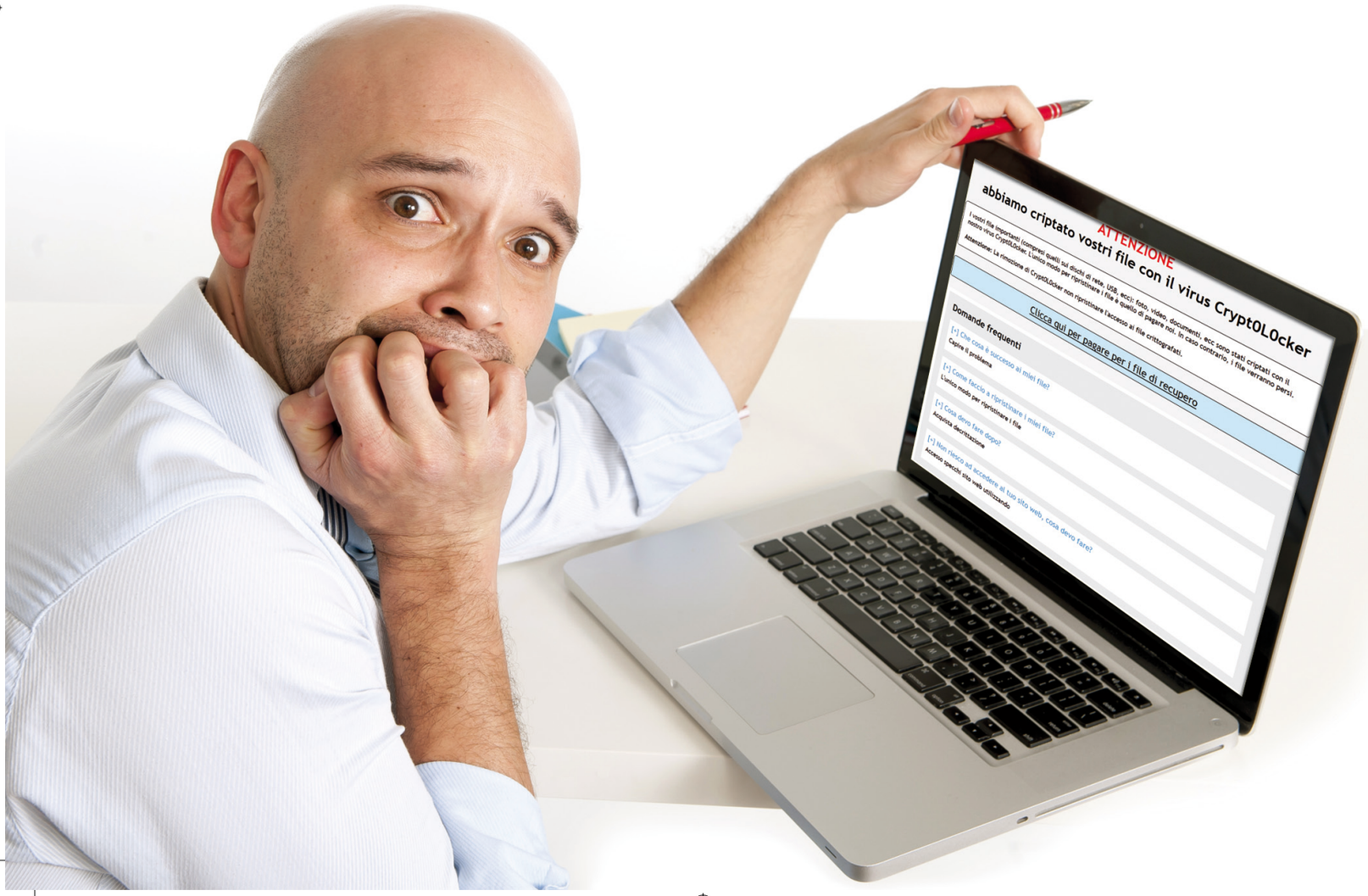
Enrico Tonello
Ricercatore Anti-Malware

Prende in ostaggio i nostri file e chiede un riscatto per sbloccarli. Ecco come non cedere al ricatto

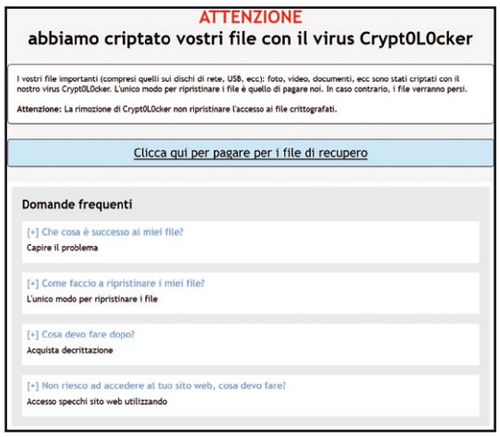
Era il dicembre del 2012 quando, sulla scena informatica, fece la sua comparsa il virus DocEncrypter, un malware di nuova generazione capace di rendere inaccessibili tutti i file DOC archiviati nell'hard disk della vittima. Da allora, questa nuova tipologia di malware venne classificata come ransomware (dall'inglese ransom, riscatto), ad indicare quei virus che, dopo aver infettato il sistema operativo, riescono a criptare tutti i file personali dell'utente bloccandone l'accesso fino a quando non viene pagato un riscatto richiesto dagli stessi cybercriminali creatori del virus.

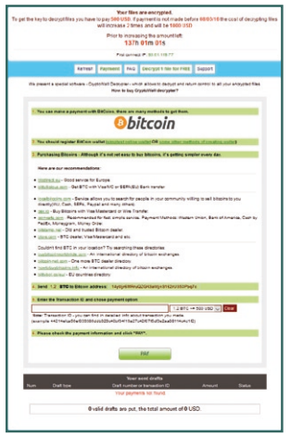
Come avviene l'infezione

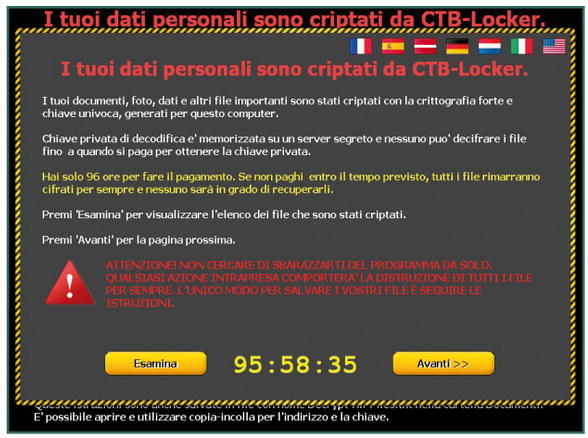
La diffusione dei cryptomalware, nella maggior parte dei casi, avviene attraverso e-mail fasulle (le più diffuse utilizzano i loghi di famosi corrieri come SDA e DHL, oppure quelli di Equitalia e TIM) che fungono da "cavallo di Troia" e invitano il destinatario a cliccare su un link o ad aprire un file allegato. Queste e-mail, come i file a queste allegati, sono generati e veicolati attraverso una botnet, cioè un insieme di server coordinati tra loro e dislocati in tutto il mondo che spediscono migliaia di messaggi simili ma con link e allegati diversificati. Di fatto, ogni e-mail ha in dotazione un file o un link da cui si attiva un altro file diversificato con frequenza temporale molto ridotta. Ad esempio, dallo stes-



ALCUNE DELLE SCHERMATE CHE ANNUNCIANO L'AVVENUTA INFEZIONE DA PARTE DI PERICOLOSI CRYPTOMALWARE







so link del medesimo messaggio che raggiunge un utente, con frequenza oraria o inferiore è possibile che il file che viene eseguito sul sito facente parte della botnet sia totalmente diverso. Solo in alcuni casi particolarmente fortunati, quindi, l'antivirus in uso sarà in grado di bloccare l'esecuzione di ogni specifico file generato dinamicamente sui server della botnet. Il più delle volte, invece, non essendo riconosciuto come una minaccia, il blocco dei file si scatenerà indisturbato. Ecco perché il metodo delle firme virali utilizzate dagli antivirus, in particolare per la protezione in tempo reale del computer, per queste tipologie di attacchi risulta in molti casi inefficace.

La nostra linea di difesa

Per evitare che un attacco di cryptomalware vada a "buon fine" con conseguente crittografazione dei dati del computer attaccato, la prima strategia di difesa per non cedere al ricatto non può che essere la prevenzione. Nella pratica quotidiana, avere attivo e correttamente configurato un sistema di backup è il primo passo per evitare di perdere completamente il proprio lavoro. Il vero problema è come garantirsi che i file di backup non vengano a loro volta crittografati dai cryptomalware che sono "ghiotti" non solo dei file di dati ma, se li trovano accessibili, anche delle copie dei file di backup che saranno anch'esse, senza alcuna pietà, crittografate. In questi casi, possono tornarci molto utili le tecnologie di protezione, recupero e decodifica dei file integrate in Vir.IT eXplorer Pro, un potente antivirus tutto italiano specializzato anche nella prevenzione da cryptomalware. Il programma, infatti, rende disponibile un sistema di backup integrato che, a patto di configurarlo correttamente, garantisce che almeno le copie di sicurezza dei file non vengano crittografati in caso di attacco. Tali file, inoltre, potranno essere conservati nello stesso computer in cui è operativa anche la protezione in tempo reale di Vir.IT eXplorer PRO, sebbene sia consigliabile che l'archiviazione dei file di backup avvenga su un disco USB collegato al PC locale di modo da preservare queste copie di sicurezza anche da possibili rotture hardware del disco rigido o del computer presidiato. Nella pratica, dunque, un sistema di backup avanzato con frequenza di aggiornamento giornaliera permette di effettuare il ripristino dei file di dati dalla copia di backup più recente in modo da minimizzare quantomeno la perdita dei dati ai soli nuovi file creati o modificati successivamente all'ultimo backup disponibile.

Tecnologie specializzate

Nell'ottica di arginare la diffusione dei cryptomalware, gli Autori di Vir.IT eXplorerPRO negli ultimi due anni hanno analizzato in modo approfondito le varie famiglie e tipologie ad oggi note di questi malware per cercare di trovare un metodo di intercettazione preventiva, o almeno nella fase iniziale dell'attacco, attraverso l'analisi euristico-comportamentale. Il

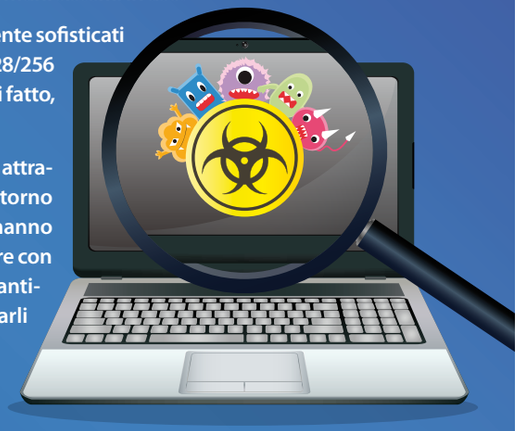
LE CARATTERISTICHE PECULIARI DEI CRYPTOMALWARE

✔ **Sono generalmente dei malware "mutanti". La loro mutazione si ottiene attraverso l'attivazione di file totalmente diversi dal medesimo link ad intervalli di tempo molto ravvicinati, anche nell'ordine del quarto d'ora. Da questi link vengono scaricati i file che potranno scatenare la crittografazione dei file di dati oppure, in alternativa, l'attacco di altre tipologie di virus quali dropper, rootkit eccetera. Di fatto, con una frequenza di mutazione e distribuzione così ravvicinata, nessun software basato su un approccio preventivo tradizionale (scudo residente in tempo reale basato sulle firme di identificazione), sarà ragionevolmente in grado di bloccare preventivamente.**

✔ **Hanno un periodo di incubazione praticamente nullo. L'attivazione del cryptomalware produce immediatamente i propri effetti malevoli e dannosi come la crittografazione dei file di uso più comune quali, ad esempio: DOC, XLS, MDB, JPG eccetera e in più di qualche occasione anche i file di backup di alcuni dei più comuni sistemi in uso.**

✔ **Crittografano i dati con algoritmi estremamente sofisticati come AES o RSA, con chiavi da un minimo di 128/256 bit fino ad arrivare ai 2.048 bit, o più, rendendoli, di fatto, praticamente irrecuperabili.**

✔ **Richiedono un riscatto, in molti casi in Bitcoin, attraverso la rete anonima Tor. Visto il notevole ritorno economico, quindi, i creatori del cryptomalware hanno tutto l'interesse a variare i file portatori del malware con la massima velocità di modo che alcun software antivirus, antispyware e antimalware possa intercettarli preventivamente.**



IL CRYPTOMALWARE SI AUTODISTRUGGE

Negli ultimi mesi è stato notato uno strano comportamento di alcuni cryptomalware che, dopo aver scandagliato il sistema, aver completato la crittografazione dei file e visualizzato le istruzioni di riscatto, si cancellano automaticamente. In poche parole, dopo aver raggiunto il suo scopo, il cryptomalware si autodistrugge per fornire meno informazioni possibili ai ricercatori di sicurezza che, non avendo il file portatore del malware da studiare, non sono nelle possibilità/condizioni di studiarne il comportamento ed estrarne l'eventuale firma di univoca identificazione.

risultato di questo lungo lavoro è stato il rilascio di Vir.IT Anti-CryptoMalware, un insieme di tecnologie integrate in Vir.IT eXplorer PRO in grado di bloccare nella fase iniziale dell'attacco la crittografazione dei file da parte di temibili ransomware quali CrytpoLocker, CTB-Locker, CryptoWall, Crypto.FF, CryptoEncoder, TeslaCrypt, CryptoLocky e altri, come anche le varianti di nuova generazione. Nelle migliori performance verificate, dopo la crittografazione dei primi 5 file il processo di crittografazione viene bloccato: la vittima, in questo caso, non deve fare altro che eseguire le semplici operazioni indicate nella videata di avviso che compare quando scatta la protezione di Vir.IT Anti-CryptoMalware (leggi il box Ecco cosa fare in caso di attacco da cryptomalware).

Un po' di buone notizie

È confortante sapere che le tecnologie di protezione anti-cryptomalware integrate in Vir.IT eXplorer PRO sono in grado di salvaguardare dalla crittografazione non meno del 99,63% dei file di dati archiviati nel computer. Lo 0,37% dei file che mediamente vengono crittografati nelle fasi iniziali dell'attacco, inoltre, possono essere sbloccati e recuperati mettendo in atto tre diverse tecnologie da utilizzare in cascata:

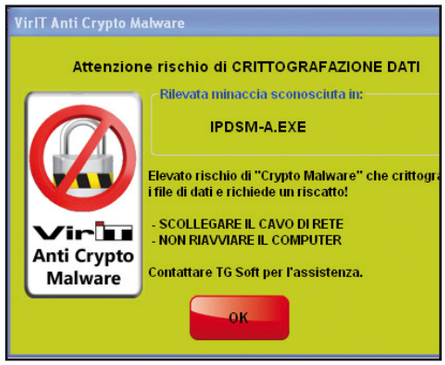
- nel caso di alcune tipologie/famiglie di cryptomalware (tra queste citiamo in particolare TeslaCrypt 3.0), possono essere sbloccati mediante le chiavi che Vir.IT eXplorer PRO è in grado di carpire durante l'attacco dal malware mentre è operativo in memoria. Questo permette di recuperare con ragionevole aspettativa il 100% dei file crittografati nella fase iniziale dell'attacco senza perdere neanche una virgola delle modifiche effettuate sui file fino al momento dell'attacco;
- per le tipologie di cryptomalware per le quali Vir.IT eXplorer PRO non è in grado di carpire le chiavi di crittografazione, vi è sempre e comunque la possibilità di recuperare i file attraverso il BackUp-On-The-Fly che è una tecnologia di backup automatico che procede ad effettuare copie di sicurezza "al volo" dei file di dati delle più comuni tipologie con dimensione fino a 3 MB in una cartella di sicurezza di Vir.IT eXplorer PRO. Il loro ripristino permetterà di recuperarne i contenuti senza perdere alcuna modifica;
- Come "ultima" opportunità, è possibile procedere al ripristino selettivo dei file di dati crittografati da Vir.IT BackUp (si tratta generalmente di copie dei file allo stato dell'arte del più recente backup disponibile, generalmente quello del giorno precedente).

Pagare o non pagare?

Nel caso in cui l'infezione da cryptomalware sia ormai completata, l'utente si trova a dover risolvere un atroce dilemma: cedere o non cedere al ricatto? Ovviamente, è sempre sconsigliato cedere al ricatto e pagare i cyber criminali nella speranza di ottenere la chiave di crittografazione dei file per due semplici motivi:

- non è sempre certo che dopo il pagamento, richiesto generalmente in Bitcoin, si ricevano le giuste istruzioni per sbloccare i propri file;
- pagando, indipendentemente dalla fornitura della chiave di decodifica, si darà ancora maggiore forza alle organizzazioni criminali che, con i "facili" guadagni ottenuti, sarà in grado di organizzare attacchi ancora più sofisticati e su scala ancora più vasta.

Quando si rimane vittima di un attacco da cryptomalware, inoltre, si diventa fortemente vulnerabili e può capitare che vagando su Internet alla spasmodica ricerca di una soluzione ci si imbatta in qualche pubblicità ingannevole o in qualche "guru" che promette il recupero della totalità dei file. Il consiglio, ovviamente, è quello di rivolgersi sempre a consulenti esperti in grado di dare una reale soluzione.



Vir.IT Anti CryptoMalware (www.tgsoft.it) è uno dei pochi tool capaci di identificare un cryptomalware. Quando appare questo alert significa che il processo di crittografazione è stato bloccato e l'antivirus lo sta "guidando" alla sua terminazione.

ECCO COSA FARE IN CASO DI ATTACCO DA CRYPTOMALWARE

✔ **È fondamentale agire repentinamente** scollegando innanzitutto il cavo di rete in modo che il virus rimanga confinato esclusivamente su quella macchina e non si diffonda su altre unità condivise in LAN.

✔ È importante, poi, **evitare di riavviare il computer**: questa raccomandazione, non immediatamente comprensibile dall'utente, è legata al fatto che, ad ogni riavvio del sistema, il cryptomalware prosegue nella sua attività di crittografazione dati prima che venga nuovamente individuato e bloccato da Vir.IT Anti-CryptoMalwawre. Si avrà quindi un numero di file crittografati progressivamente crescente. Inoltre, alcune tipologie di cryptomalware come TeslaCrypt 3.0, ad ogni riavvio del sistema procedono a crittografare i file con una chiave differente.

✔ **Mai riavviare in modalità provvisoria**. In passato, procedendo al riavvio dalla modalità provvisoria, molti virus e malware non si attivavano ed era possibile, sapendo quali fossero i loro file infetti (generalmente un file eseguibile o una libreria in formato .DLL), cancellarli e di fatto bonificare il sistema. Nel caso di alcune tipologie e famiglie di cryptomalware si è verificata anche la duplice infezione da parte di un Trojan.Dropper. Questo trojan è generalmente in grado di essere eseguito anche in modalità provvisoria, procedendo a scaricare ed eseguire altri cryptomalware cifrando i dati nuovamente (crittografazioni multiple).

✔ **Contattare TG Soft per assistenza**. Ai clienti di Vir.IT eXplorer PRO, TG Soft offre supporto e-mail, telefonico e assistenza remota proprio per gestire queste situazioni emergenziali che devono venire affrontate con più che ragionevole cognizione di causa con personale qualificato in grado non solo di tranquillizzare il cliente, ma anche di procedere alla disattivazione del cryptomalware ed il ripristino dei file attaccati e crittografati nella fase iniziale.