SICUREZZA INFORMATICA

CIRCOLARE n° 55-20 – ES MARZO 2020

VIRUS INFORMATICI

INFORMAZIONE PER GLI SMART WORKERS

In considerazione del massiccio utilizzo di smart working nel periodo di emergenza Covid, e del possibile utilizzo da parte degli smart workers anche di pc personali, oltre che aziendali, trasmettiamo una breve sintesi delle principali tipologie di virus informatici, consigliando di diffondere l'informazione ai fini di prevenire eventuali "contagi" informatici.
Alleghiamo inoltre l'elenco delle segnalazioni ricevuti dalla Polizia postale relativamente ad attacchi informatici aggiornato a Marzo 2020, alcune delle quali riguardano il tema Coronavirus.

I VIRUS INFORMATICI: COSA SONO

Un virus, in informatica, è un software che, una volta eseguito, infetta dei file in modo da fare copie di se stesso, generalmente senza farsi rilevare dall'utente. Il termine viene usato per un programma che si integra in qualche codice eseguibile (incluso il sistema operativo) del sistema informatico vittima, in modo tale da diffondersi su altro codice eseguibile quando viene eseguito il codice che lo ospita, senza che l'utente ne sia a conoscenza.
In pratica i virus informatici sono così chiamati poiché possiedono la capacità di infettare un elaboratore propagandosi velocemente al suo interno; nel momento in cui i files infetti vengono mandati via e-mail o vengono trasportati dagli utenti attraverso supporti fisici (es. pendrive) oppure copiati all'interno di reti aziendali si diffondono rapidamente su altre macchine.

Un virus è composto da un insieme di istruzioni, come qualsiasi altro programma per computer. È solitamente composto da un numero molto ridotto di istruzioni, ed è specializzato per eseguire soltanto poche e semplici operazioni e ottimizzato per impiegare il minor numero di risorse, in modo da rendersi il più possibile invisibile.
Principalmente un virus esegue copie di sé stesso, ma può avere anche altri compiti molto più dannosi (cancellare o rovinare dei file, formattare l'hard disk, aprire delle backdoor, far apparire messaggi, disegni o modificare l'aspetto del video, installare altri malware), ed altre attività minacciose per un sistema informatico.

IL CICLO DI VITA DI UN VIRUS INFORMATICO

I virus informatici presentano numerose analogie con quelli biologici per quello che riguarda il ciclo di vita, che si articola nelle fasi seguenti:

- *creazione*: è la fase in cui lo sviluppatore progetta, programma e diffonde il virus. Di solito i cracker (pirati informatici) per la realizzazione di virus utilizzano linguaggi di programmazione a basso livello in modo da ottenere codice virale di pochi centinaia di byte.
- *incubazione*: il virus è presente sul computer da colpire ma non compie alcuna attività. Rimane inerte fino a quando non si verificano le condizioni per la sua attivazione

- *infezione*: il virus infetta il file e di conseguenza il sistema
- *attivazione*: al verificarsi delle condizioni prestabilite dal cracker, il virus inizia l'azione dannosa
- *propagazione*: il virus propaga l'infezione, riproducendosi e infettando sia file nella stessa macchina che altri sistemi
- *riconoscimento*: l'antivirus riconosce un certo file come infetto. Tale riconoscimento può avvenire in più modi, a seconda di com'è fatto il virus e di quali algoritmi l'antivirus utilizza per la scansione del sistema e dei file che contiene. In casi particolari, se ad esempio il virus non è abbastanza diffuso, può non avvenire affatto, e quindi il virus può proliferare infettando sempre più file, e quindi diffondersi verso ulteriori PC
- *eliminazione*: è l'ultima fase del ciclo vitale del virus. Il virus viene eliminato dal sistema: di solito questa fase non viene eseguita direttamente dall'utente, ma da un software antivirus che cerca di fermare in qualche modo l'infezione.

I SINTOMI PIÙ FREQUENTI DI INFEZIONE

- *Rallentamento del computer*: il computer lavora molto più lentamente del solito. Impiega molto tempo ad aprire applicazioni o programmi. Il sistema operativo impiega molto tempo ad eseguire semplici operazioni che solitamente non richiedono molto tempo, questo segnale è il più comune e si manifesta quasi ogni volta che viene eseguito
- *Impossibilità di eseguire un determinato programma o aprire uno specifico file*
- *Scomparsa di file e cartelle*: i file memorizzati in determinate cartelle (di solito quelle appartenenti al sistema operativo o a determinate applicazioni) vengono cancellati (totalmente o in parte) o resi inaccessibili all'utente
- *Impossibilità di accesso al contenuto di file*: all'apertura di un file, viene visualizzato un messaggio di errore o semplicemente risulta impossibile aprirlo
- *Messaggi di errore inattesi o insoliti*: visualizzazione di finestre di dialogo contenenti messaggi assurdi, buffi, o aggressivi
- *Riduzione di spazio nella memoria e nell'hard disk*: riduzione significativa dello spazio libero nell'hard disk; quando un programma è in esecuzione, viene visualizzato un messaggio indicante memoria insufficiente per farlo (sebbene questo non sia vero e ci siano altri programmi aperti)
- *Settori difettosi*: un messaggio informa della esistenza di errori nella parte di disco sulla quale si sta lavorando e avverte che il file non può essere salvato o che non è possibile eseguire una determinata operazione
- *Modifiche delle proprietà del file*: il virus modifica alcune o tutte le caratteristiche del file che infetta. Di conseguenza risultano non più corrette o modificate le proprietà associate al file infettato. Tra le proprietà più colpite: data/ora (di creazione o dell'ultima modifica), la dimensione
- *Errori del sistema operativo*: operazioni normalmente eseguite e supportate dal sistema operativo determinano messaggi di errore, l'esecuzione di operazioni non richieste o la mancata esecuzione dell'operazione richiesta; in certi casi, l'errore può causare un riavvio spontaneo del computer
- *Ridenominazione di file*: un virus può rinominare i file infettati e/o file specifici, ad esempio di sistema
- *Problemi di avvio del computer*: il computer non si avvia o non si avvia nella solita maniera, oppure impiega molto tempo per caricarsi
- *Interruzione del programma in esecuzione* senza che l'utente abbia eseguito operazioni inaspettate o fatto qualcosa che potrebbe aver provocato questo risultato

- *Tastiera e/o mouse non funzionanti correttamente*: la tastiera non scrive ciò che è digitato dall'utente o esegue operazioni non corrispondenti ai tasti premuti. Il puntatore del mouse si muove da solo o indipendentemente dal movimento richiesto dall'utente
- *Scomparsa di sezioni di finestre*: determinate sezioni (pulsanti, menu, testi etc...) che dovrebbero apparire in una particolare finestra sono scomparse o non vengono visualizzate, oppure appaiono icone strane o con contenuto insolito
- *Antivirus disattivato automaticamente*: Può capitare che un malware disattivi forzatamente un antivirus per poter essere eseguito senza correre il rischio di essere rilevato
- *Lentezza della connessione Internet*: il virus potrebbe usare la connessione per propagare l'infezione, o inviare dati a chi ha scritto il virus
- *Limitazioni nella visualizzazione di alcuni siti Internet*, soprattutto quelli dei produttori di antivirus: è un meccanismo di protezione da parte del virus, che in questo modo impedisce di adottare contromisure dopo l'infezione

LA TERMINOLOGIA

MALWARE

Il malware è l'unione dei termini malicious e software. E' il nome dato a qualsiasi tipo di software che potrebbe danneggiare un computer, interferire con i programmi e raccogliere i dati di un utente o fare in modo che il computer esegua azioni senza che l'utente lo sappia o dia la propria autorizzazione. Questo tipo di virus rappresenta una minaccia in costante crescita. Oltre ai classici sistemi operativi windows, oggi è anche il sistema "Android", presente nella totalità degli smartphone, ad essere nel mirino dei cybercriminali, in particolare per effetto delle scarse protezioni adottate dagli utilizzatori. Anche i sistemi Apple iOS non sono comunque immuni dal rischio.

TROJAN HORSE

Chiamato comunemente "Trojan" questo programma si nasconde pur essendo sotto gli occhi di tutti, mascherandosi da file legittimo o da software. Una volta scaricato e installato il trojan apporta dei cambiamenti al computer e conduce attività dannose, senza la consapevolezza o il consenso della vittima. Esso utilizza un codice per installare software che sembra autentico ma che in realtà crea delle "backdoor" in un sistema causando solitamente la perdita o il furto dei dati trasmettendoli ad una fonte esterna.

WORM

A differenza dei virus i worm non hanno bisogno dell'intervento umano per diffondersi: infettano una sola volta anche solo navigando con un normale browser e poi utilizzano le reti del computer per entrare in altre macchine senza l'aiuto degli utenti. Sfruttando la vulnerabilità della rete, come alcune falle nei programmi e-mail, i worm possono auto-propagarsi in migliaia di copie con l'obiettivo di infettare nuovi sistemi nei quali attuare lo stesso processo.

SPYWARE

Lo spyware spia le azioni dell'utente. Esso raccoglie dati quali i tasti premuti dall'utente, le abitudini di navigazione e persino informazioni di accesso e informazioni su carte di credito che vengono poi inviate a terze parti, generalmente criminali. Lo spyware potrebbe anche modificare impostazioni di sicurezza specifiche sul computer dell'utente o interferire con le connessioni di rete. Secondo alcune fonti, tipologie emergenti di spyware potrebbero permettere a società esterne di tracciare in incognito il comportamento degli utenti e senza il loro consenso.

ADWARE

L'adware è una delle infezioni in rete più comuni. I programmi consegnano automaticamente pubblicità per fornire un host ai computer. Tra i tipi conosciuti di adware vi sono: pubblicità pop-up su pagine Web e pubblicità in programmi le quali spesso accompagnano software "gratuiti". Mentre alcuni tipi di adware sono relativamente pericolosi, altre varianti usano strumenti di localizzazione per carpire informazioni riguardanti la posizione dell'utente o la cronologia del browser e per presentare pubblicità mirate sullo schermo della vittima. Poiché l'adware viene installato con la consapevolezza e il consenso dell'utente, questi programmi non possono essere chiamati malware ma generalmente vengono identificati dai sistemi antivirus come "programmi potenzialmente indesiderati".

Per quanto riguarda gli smartphone, gli adware sono presenti all'interno del codice delle applicazioni, soprattutto di quelle che si scaricano da store di terze parte che non garantiscono le stesse protezioni del Google Play Store o di Apple Store che invece vengono verificate preventivamente da un organismo di controllo prima di essere pubblicate.

BOT

I bot sono programmi progettati per portare a termine automaticamente determinate operazioni. Sono utili per molti scopi legittimi, tuttavia sono stati anche riutilizzati come malware. Una volta all'interno del computer, i bot possono permettere alla macchina di eseguire comandi specifici senza l'approvazione o la consapevolezza dell'utente. Gli hacker potrebbero tentare anche di infettare più computer con lo stesso bot per creare un "botnet" (abbreviazione di robot network) che può essere successivamente usato per gestire da remoto computer danneggiati al fine di sottrarre dati sensibili per spiare le attività delle vittime, per distribuire spam automaticamente o per lanciare devastanti attacchi DDoS sulle reti del computer.

ROOTKIT

Il rootkit permette un accesso remoto o il controllo di un computer a opera di terzi. Una volta installato sul computer il rootkit permette di prendere il completo controllo della macchina per rubare dati o installare altri pezzi di malware. Rintracciare questo tipo di codice dannoso richiede un monitoraggio manuale per comportamenti insoliti, insieme a un regolare aggiornamento al sistema operativo e al software per eliminare potenziali vie di trasmissione.

RANSOMWARE

Tra le minacce alla sicurezza informatica che hanno interessato in questi ultimi anni le aziende di tutte le dimensioni e settori, comprese quelle italiane, al primo posto troviamo sicuramente il ransomware (dal termine "ransom", in inglese riscatto, e "ware", diminutivo di malware): si tratta di una tipologia di malware che agisce "criptando" i dati del computer infettato che vengono poi "liberati" solo sotto pagamento di un riscatto agli hacker che lo hanno installato.
La variante più nota della vasta famiglia dei ransomware è stata quella dei cryptolocker, che bene o male tutti hanno avuto modo di conoscere

LA PREVENZIONE

Alcune regole base ci permettono di limitare la possibilità di cadere nelle trappole dei virus informatici:

- Aggiornare frequentemente il sistema operativo e le applicazioni (i virus spesso sfruttano le falle di sicurezza presenti nei software obsoleti)
- Utilizzare un buon software antivirus prediligendo soluzioni a pagamento, peraltro obbligatorie per gli utenti di aziende e studi che trattano dati in maniera elettronica
- Eseguire regolari backup dei propri dati, possibilmente utilizzando due metodologie congiunte: una con frequenza giornaliera ed una con frequenza mensile, trimestrale, semestrale, ecc. in base alle esigenze. In questo modo in caso di perdita dei dati più il backup è frequente più i dati recuperabili dal salvataggio saranno aggiornati
- Non scaricare e installare software da Internet, a meno che non sia certa la fonte di provenienza
- Non ritenere mai attendibile l'installazione di un software "non originale", in quanto spesso contiene Malware e Trojan
- Adottare una sensibilizzazione specifica quando si usa la posta elettronica non aprendo allegati o link sospetti anche se arrivano da mittenti conosciuti, poiché gli stessi potrebbero essere stati infettati da un virus e poi usati per diffondere l'infezione. Anche se si conosce il mittente è consigliabile non aprire ciò di cui si dubita
- Informare tempestivamente gli addetti all'assistenza IT in caso di mail con un contenuto dubbio o comportamenti sospetti dell'elaboratore

Gian Franco Camarota