Virus e minacce informatiche

Introduzione

L'utilizzo quotidiano della rete Internet è ormai molto intenso e spesso irrinunciabile e riguarda milioni di utenti. La sempre maggiore diffusione della posta elettronica e della navigazione su internet hanno però portato con sé anche un aumento dei pericoli e dei rischi per gli utenti.
Per questo BNL ritiene che, oggi più che mai, sia importante saper affrontare le minacce informatiche che possono mettere a rischio la sicurezza dei dati dei propri clienti.

Dai Virus al Cybercrime

In passato i PC erano minacciati prevalentemente da virus e worm, che nella maggioranza dei casi avevano come intento quello di diffondersi il più possibile e danneggiare file e computer.
Con la nascita dei sistemi di home banking e di pagamento online, la minaccia più comune è diventata il crimeware, un software maligno che si presenta sotto forma di virus, worm, Trojan o altro malware con lo scopo di ottenere profitti illeciti.

Breve glossario delle minacce informatiche

➢ Virus e worm

Un **virus** informatico è un programma che si propaga di file in file all'interno di uno stesso PC e da un PC all'altro, e può essere programmato per cancellare o danneggiare dati. Spesso è mascherato dentro programmi che sembrano innocui.
I **worm** sono particolari tipi di virus che, per diffondersi, non infettano altri file ma utilizzano la rete: si installano in un computer per poi trovare il modo di diffondersi ad altri PC. In alcuni casi possono autoeseguirsi, ma più spesso hanno bisogno dell'intervento dell'utente per iniziare il ciclo di infezione.

➢ Malware

Con il termine **"malware"** ("malicious software", ovvero "software maligno") ci si riferisce a qualsiasi programma deliberatamente creato per **effettuare un'azione non autorizzata che può danneggiare il funzionamento e la sicurezza del sistema operativo**. Si trasmette via internet, tramite la posta elettronica o la semplice navigazione in internet. Tra le categorie di malware più diffuse si ricordano virus, trojan horse, keylogger, worm e backdoor.

➢ Trojan

Si definisce “Trojan” un malware nascosto in un programma che appare come software legittimo ma che, una volta lanciato, danneggia o compromette la sicurezza e il funzionamento del computer. Differisce da virus e worm perché non si diffonde da solo ma, **per lo più, viene inconsapevolmente installato dall’utente** che lo scarica da internet insieme al programma di cui necessita.
Esistono numerosi (e sempre nuovi) tipi di trojan, usati per accedere a informazioni riservate e dati sensibili. I più comuni sono i Trojan-Backdoor (spesso includono un keylogger), Trojan-Spy, Trojan che rubano password, Trojan-Proxy che trasformano il computer in una macchina distributrice di spam.

➢ Rootkit

Con questo termine si intende un programma che **permette di accedere a un computer senza l’autorizzazione dell’utente o dell’amministratore**. Si tratta di software finalizzati a nascondere l'attività svolta dai Trojan. Una volta installati sono invisibili agli utenti e riescono ad eludere anche i software di sicurezza.

➢ Phishing

Il phishing è una **frode informatica finalizzata a ottenere dati personali sensibili** come password, informazioni relative ai conti bancari o alle carte di credito. Si attua attraverso l’invio di una grande quantità di email a nome di istituti di credito, finanziari, assicurativi, in cui si invita l’utente a collegarsi tramite un link a un sito web fasullo (apparentemente uguale a quello vero) dove gli viene richiesto di inserire informazioni riservate.

➢ Keylogger

Si tratta di programmi che **registrano tutto ciò che l’utente digita sulla tastiera**: nella maggior parte dei casi sono quindi progettati per rubare dati sensibili quali login e codici bancari.

➢ Spyware

Con questa parola si indica un software che **monitora ciò che viene digitato sulla tastiera** ("keyloggers'"), **raccoglie informazioni confidenziali** (password, numeri di carte di credito, PIN etc.)

e indirizzi email, traccia le abitudini di navigazione dell'utente. I dati raccolti vengono inviati a terze persone, naturalmente senza che gli utenti interessati se ne accorgano.

➢ Botnet

Un botnet è una **rete di computer** collegati ad internet, **infettati** con un Trojan o dell'altro malware, e **controllati a distanza** dai criminali informatici.

➢ Adware

Si tratta di software che **generano la presentazione di messaggi pubblicitari** (spesso tramite banner pop-up) o reindirizzano a siti promozionali non richiesti. Spesso sono contenuti all'interno di programmi gratuiti, oppure possono essere scaricati e installati da un Trojan. L'Adware può anche modificare le impostazioni del browser e reindirizzare la navigazione verso un sito specifico.

Crimeware

➢ Crimeware: cos'è, come difendersi

Con crimeware si intende il **software maligno installato di nascosto sui computer degli utenti**, con lo scopo principale di "rubarne" informazioni riservate (ad es. password, PIN, OTP) e procedere quindi a una frode online. La maggior parte del crimeware è composta da Trojan.

Per proteggere il computer dalle minacce informatiche, si devono seguire delle **semplici regole**:

- Proteggi il computer installando un **software di Internet security**.
- Installa gli **aggiornamenti di sicurezza** per il sistema operativo e per le applicazioni. Se utilizzi Windows®, esegui semplicemente gli Aggiornamenti Automatici, anche per applicazioni come Microsoft® Office.
- Se ricevi una **email con allegato** un file (Word, Excel, .EXE etc.) non aprirla se non conosci il mittente. Mai aprire un file allegato a una mail non richiesta (spam). Lo stesso vale per i messaggi email e di chat (Instant Messaging) contenenti link.
- Se hai necessità di **scaricare software da internet**, la principale precauzione da adottare per non incombere in minacce informatiche (infezioni da malware, installazione di plug-in malevoli, ecc.) è quella di **preferire il download da siti conosciuti, la cui fonte sia certa ed attendibile**. Se ti imbatti in siti poco noti, che possono presentare messaggi che invitano a installare un plug-in o scaricare un programma per proseguire nella navigazione, **chiudi tutte**

le finestre di dialogo senza proseguire con il download oppure, se possibile, **esegui una scansione con l'antivirus** del file/programma che vuoi scaricare prima di aprirlo.

- **Aggiorna regolarmente il software di protezione** (almeno una volta al giorno).
- **Mantieni aggiornate anche le applicazioni** installate nel tuo sistema operativo.
- Usa l'**account dell'Amministratore** del computer soltanto nel caso in cui sia necessario, ad esempio per installare un software o eseguire delle modifiche nel sistema. Per l'utilizzo di tutti i giorni, crea un account separato con diritti di accesso limitati (puoi farlo a partire dalla voce "Account utente" nel "Pannello di controllo"). In questo modo limiterai l'accesso del malware ai dati sensibili del sistema.
- Esegui regolarmente delle **copie di backup dei dati** su CD, DVD, o supporti USB. Se i file dovessero subire danneggiamenti o criptaggio a causa dell'azione di un programma nocivo, potrai recuperarli dalla copia di backup.

➢ Hacker: chi sono, come difendersi dai loro attacchi

Con il termine "hacker" si indica chi entra in un computer altrui per installare malware, rubare dati confidenziali o usare il computer compromesso per distribuire spam.

Ci si può difendere da questi rischi usando un **firewall**, vale a dire un programma che rende il PC invisibile agli hacker e lo protegge rilevando potenziali intrusioni. Spesso il firewall è integrato nei software anti-virus.

E' necessario quindi:

- Installare un software di Internet security.
- Installare gli aggiornamenti di protezione.
- Fare attenzione alle email indesiderate e ai messaggi di Instant Messaging.
- Fare attenzione quando ci si registra con i diritti di Amministratore.
- Fare una copia di backup dei dati archiviati sul PC.

➢ Cos'è un attacco di phishing e come ci si può difendere

Un attacco di phishing è una forma di cybercrime. Il criminale informatico crea, ad esempio, un sito quasi identico a quello di un'istituzione finanziaria, per ingannare l'utente e fare in modo che questi inserisca le proprie credenziali – codice utente, password, PIN etc. – in un modulo presente sul sito fasullo; in tal modo **il criminale può appropriarsi delle credenziali dell'utente, accedere al suo conto corrente e sottrargli delle somme di denaro**.

Tra le numerose tecniche per attirare gli utenti su questi siti fasulli la più comune è senz'altro l'invio di **email** il cui mittente è apparentemente la stessa istituzione finanziaria della quale è stato

“clonato” il sito. Queste email contengono il logo della banca in questione, presentano un buon layout e hanno un oggetto verosimile come comunicazione di una banca. All’interno, generalmente con un pretesto qualunque ma credibile, si chiede a tutti i clienti di confermare i propri dati. Quando l'ignaro utente clicca sul link contenuto nella email, viene indirizzato ad un sito web fasullo, attraverso il quale molto probabilmente divulgherà la propria identità digitale ai cybercriminali.

Ecco le semplici regole per difendersi dal phishing:

- E’ impossibile che una Banca chieda di fornire informazioni personali via email. Non dare mai seguito a richieste di questo genere che provengono da tale canale.
- Non compilare moduli presenti nelle email dove si chiede di inserire informazioni personali. Fornire tali dati esclusivamente tramite siti web sicuri. Controllare che la URL inizi con "https://", piuttosto che "http://". Cercare il simbolo del lucchetto nell'angolo in basso a destra del browser e cliccarlo due volte per verificare la validità del certificato digitale. Oppure, in alternativa, in caso di dubbi utilizzare il telefono per le operazioni bancarie a distanza.
- Segnalare immediatamente alla Banca qualsiasi azione o situazione che sembri sospetta.
- Non usare link contenuti nei messaggi email per caricare una pagina web, ma digitarne la URL nel browser.
- Verificare che l'antivirus blocchi i siti di phishing, o prendere in considerazione l'installazione di una barra degli strumenti del browser che segnali eventuali attacchi di phishing.
- Controllare regolarmente i movimenti bancari (carte di debito e credito incluse, estratti conto etc.) per assicurarsi che le transazioni eseguite siano legittime.
- Assicurarsi di usare l'ultima versione del browser e che tutti gli aggiornamenti di sicurezza siano stati installati.

➢ Come si fa a capire che un computer è infetto?

Non è immediato capire se un computer è stato compromesso. Per questo è fondamentale installare un software di protezione completo, installare gli aggiornamenti di sicurezza del sistema operativo e delle applicazioni, ed eseguire regolarmente delle copie di backup dei dati.

Non è facile fornire una lista di sintomi caratteristici di un computer compromesso perché gli stessi sintomi posso essere provocati anche da problemi di hardware e/o software. Comunque, ecco alcuni esempi:

- Il computer si comporta in maniera strana e inusuale.
- Compaiono immagini o messaggi inaspettati.
- Emette dei suoni strani, a caso.
- I programmi si aprono da soli.

- Il firewall comunica che un'applicazione ha cercato di connettersi a Internet (e l'applicazione non è uno dei programmi che utilizzi).
- Gli amici segnalano di aver ricevuto dei messaggi email dal tuo indirizzo di posta elettronica, ma non li hai né scritti né inviati.
- Il computer si blocca spesso, o i programmi impiegano molto tempo ad aprirsi.
- Ricevi molti messaggi di "errore di sistema".
- Il sistema operativo non si carica correttamente all'avvio del computer.
- Alcuni file o cartelle sono stati modificati.
- Viene segnalato un accesso all'hard disk quando non ti risulta che ci sia alcun programma aperto.
- Il browser si comporta in maniera imprevedibile, ad esempio non riesci a chiudere o aprire una finestra.

➢ Cosa si può fare?

Se riscontri qualcuno dei sintomi sopra descritti, non farti prendere dal panico. Potresti semplicemente avere un problema dell'hardware o a livello di software, e non necessariamente si tratta di un virus, un worm o un Trojan.

Ecco, in ogni caso, cosa fare:

- Sconnetti il computer da Internet.
- Se il sistema operativo non carica, avvia il computer in Modalità di Sicurezza (quando si accende il computer, premi per qualche secondo il tasto F8, e poi seleziona la Modalita di Sicurezza dal menu che apparirà), oppure esegui l'avvio da un CD di soccorso.
- Assicurati che le firme antivirus siano aggiornate. Se possibile, non scaricare gli aggiornamenti usando il computer che temi sia infetto, ma un altro (ad esempio quello di un amico): se ci si collega a Internet tramite un computer infetto, un programma maligno potrebbe inviare informazioni importanti e confidenziali ad un hacker remoto, o propagarsi auto-inviandosi a quegli indirizzi email che sono archiviati sul computer stesso.
- Se non riesci a rimuovere il malware, controlla il sito web del tuo antivirus per avere maggiori informazioni o per scaricare eventuali utility dedicate per rimuovere singoli programmi maligni.
- Se il computer è connesso ad una rete locale, disconnettilo da tale rete.
- Esegui una scansione di tutto il computer.
- Se dovesse venire rilevato un programma nocivo, segui i suggerimenti del fornitore del software di Internet security. Un buon programma di sicurezza prevede l'opzione di disinfezione degli oggetti compromessi, la possibilità di metterli in quarantena e di eliminare worm e Trojan. Tali soluzioni sono in grado di creare un file di notifica che elenca i nomi dei file infetti e dei programmi malware trovati sul computer.
- Se il software di protezione non trova nulla, è molto probabile che il computer sia sano. Controlla l'hardware e i software installati sul computer (è bene rimuovere i software privi

di licenza e qualsiasi file spazzatura) e assicurati di avere installata l'ultima versione di sistema operativo e gli aggiornamenti di sicurezza delle applicazioni.

- Se necessario, contatta l'assistenza tecnica del produttore del tuo antivirus per ulteriori indicazioni. Potrai anche chiedere di sottoporre ad analisi un file campione.