

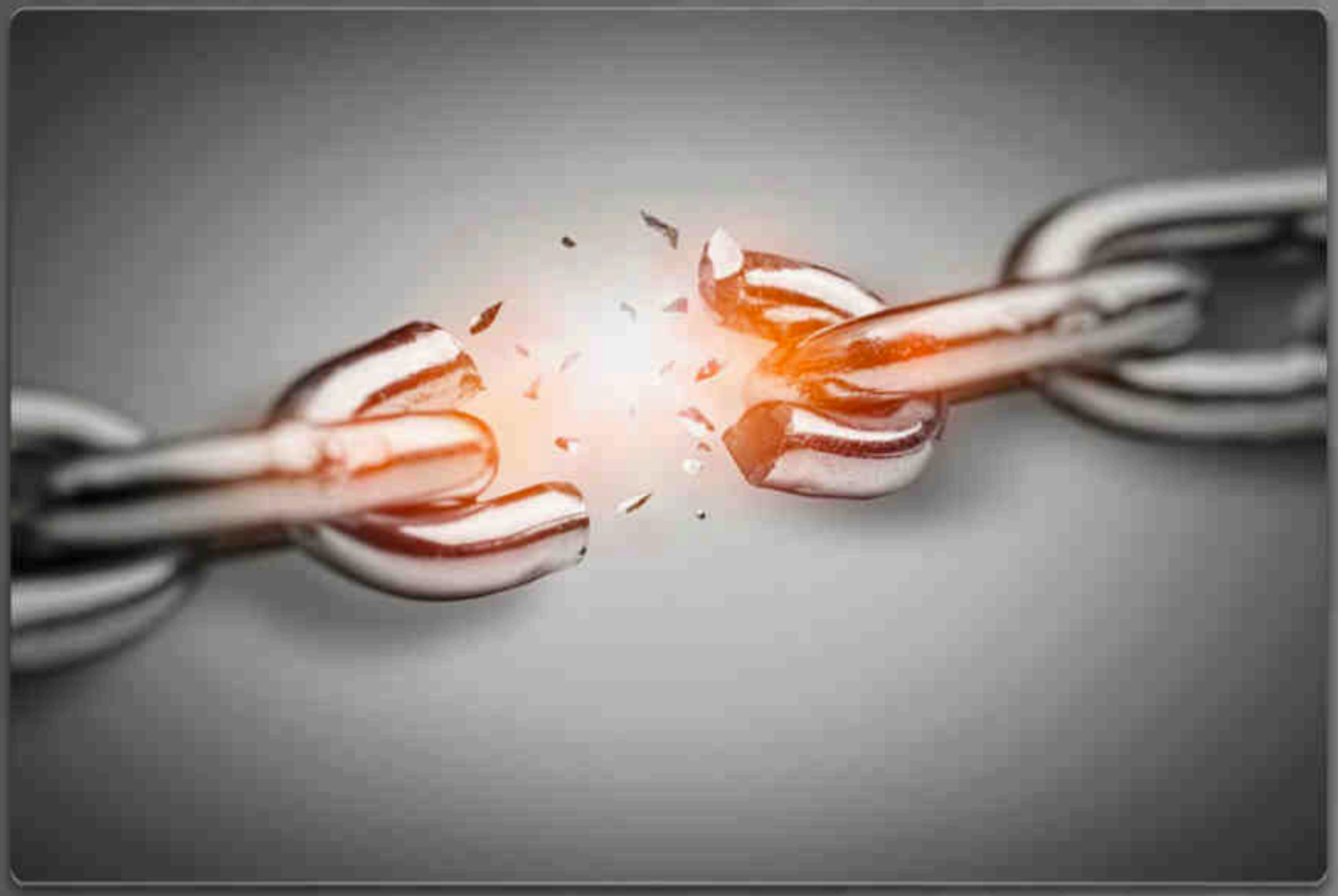
Introduzione | Capitolo 2

Capitolo 2: Gli attacchi: concetti e tecniche

In questo capitolo vengono spiegate le modalità con cui i professionisti della cybersecurity analizzano gli effetti di un attacco informatico. Illustra le vulnerabilità di protezione di natura hardware e software suddivise per categorie.

Vengono analizzate le varie tipologie di software dannoso (noto come malware) e i sintomi generati dal malware. Vengono trattati i vari metodi utilizzati dagli autori degli attacchi per penetrare in un sistema nonché gli attacchi di tipo denial of service.

Gli attacchi informatici più recenti sono considerati perlopiù attacchi misti. Gli attacchi misti impiegano varie tecniche per penetrare nei sistemi e attaccarli. Quando è impossibile evitare un attacco, è compito dei professionisti della cybersecurity ridurne l'impatto.

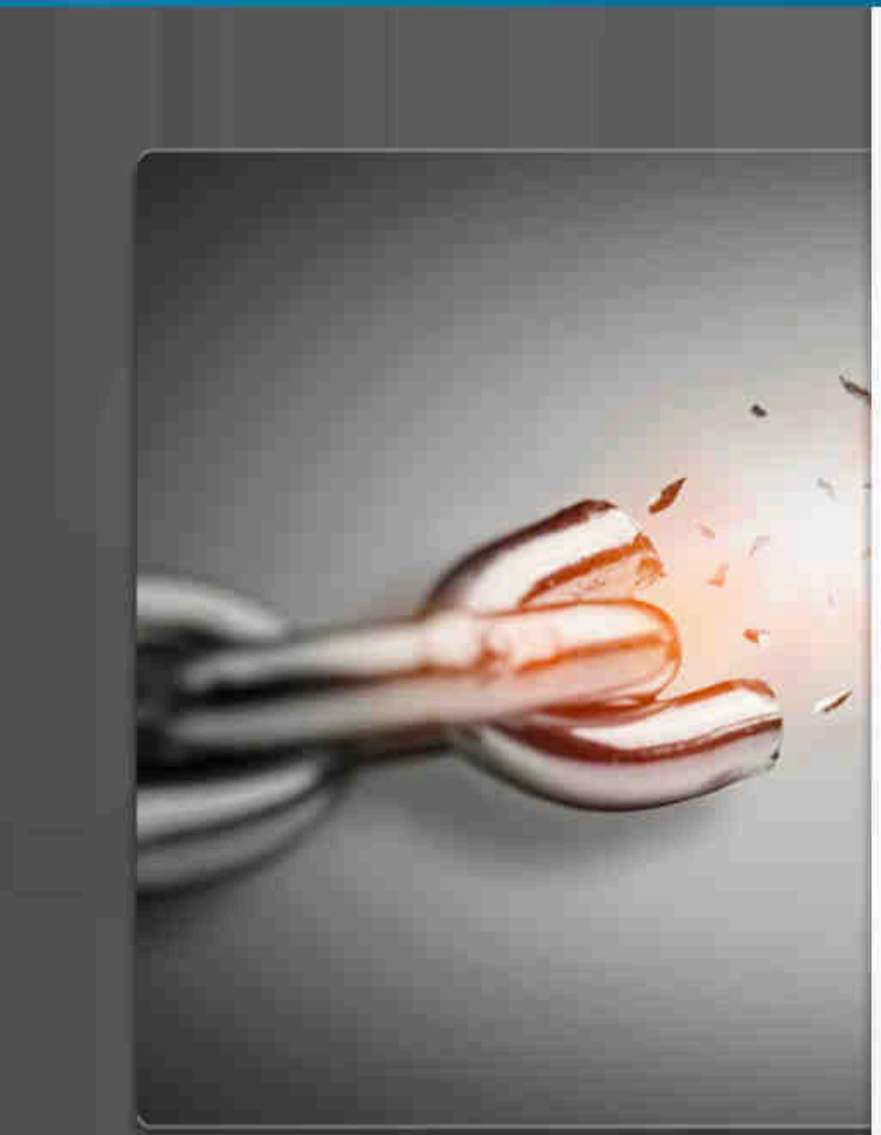


Individuazione delle vulnerabilità di protezione

Per vulnerabilità di protezione si intende qualsiasi tipo di difetto software o hardware. Dopo avere individuato una vulnerabilità, gli utenti malintenzionati tentano di sfruttarla. Exploit *è il* termine utilizzato per descrivere un programma scritto allo scopo di sfruttare una vulnerabilità nota. L'atto di utilizzare un exploit contro una vulnerabilità è definito "attacco". L'obiettivo di un attacco è ottenere l'accesso a un sistema, ai dati al suo interno o a una risorsa specifica.

Vulnerabilità software

Le vulnerabilità software sono solitamente introdotte da errori nel sistema operativo o nel codice delle applicazioni e malgrado tutto l'impegno posto dalle aziende nell'individuazione e nel patching di tali vulnerabilità, spesso ne emergono di nuove. Microsoft, Apple e altri produttori di sistemi operativi rilasciano patch e



Individuazione delle vulnerabilità di protezione

Per vulnerabilità di protezione si intende qualsiasi tipo di difetto software o hardware. Dopo avere individuato una vulnerabilità, gli utenti malintenzionati tentano di sfruttarla. Exploit *è il* termine utilizzato per descrivere un programma scritto allo scopo di sfruttare una vulnerabilità nota. L'atto di utilizzare un exploit contro una vulnerabilità è definito "attacco". L'obiettivo di un attacco è ottenere l'accesso a un sistema, ai dati al suo interno o a una risorsa specifica.

Vulnerabilità software

Le vulnerabilità software sono solitamente introdotte da errori nel sistema operativo o nel codice delle applicazioni e malgrado tutto l'impegno posto dalle aziende nell'individuazione e nel patching di tali vulnerabilità, spesso ne emergono di nuove. Microsoft, Apple e altri produttori di sistemi operativi rilasciano patch e aggiornamenti quasi ogni giorno. È frequente anche l'utilizzo di aggiornamenti delle applicazioni. Applicazioni quali browser Web, app per dispositivi mobili e server Web vengono spesso aggiornate dalle aziende o dalle organizzazioni che ne sono responsabili.

Nel 2015 una vulnerabilità importante, denominata SYNful Knock, è stata individuata in Cisco IOS. Questa vulnerabilità ha consentito agli autori degli attacchi di ottenere il controllo di router di livello enterprise, quali Cisco 1841, 2811 e 3825. In questo modo gli autori degli attacchi potevano monitorare tutta la comunicazione di rete e infettare altri dispositivi. Questa vulnerabilità è stata introdotta nel sistema a seguito dell'installazione di una versione IOS alterata nei router. Per evitare una simile situazione, è importante verificare sempre l'integrità dell'immagine IOS scaricata e limitare l'accesso fisico all'attrezzatura solo al personale autorizzato.



Suddivisione in categorie delle vulnerabilità di protezione

La maggior parte delle vulnerabilità di protezione software rientra in una delle seguenti categorie:

Overflow del buffer: questa vulnerabilità è dovuta alla scrittura di dati oltre i limiti del buffer. I buffer sono aree di memoria allocate a un'applicazione. Modificando i dati oltre i limiti di un buffer, l'applicazione accede alla memoria allocata ad altri processi. Questa condizione può portare a un arresto anomalo del sistema, alla compromissione dei dati o all'esecuzione dell'escalation dei privilegi.

Input non validato: i programmi spesso operano con input di dati. Tali dati immessi nel programma possono avere contenuto dannoso, progettato per forzare un comportamento non intenzionale del programma. Si pensi a un programma che riceve un'immagine per l'elaborazione. Un utente malintenzionato può creare un file di immagine con



Suddivisione in categorie delle vulnerabilità di protezione

La maggior parte delle vulnerabilità di protezione software rientra in una delle seguenti categorie:

Overflow del buffer: questa vulnerabilità è dovuta alla scrittura di dati oltre i limiti del buffer. I buffer sono aree di memoria allocate a un'applicazione. Modificando i dati oltre i limiti di un buffer, l'applicazione accede alla memoria allocata ad altri processi. Questa condizione può portare a un arresto anomalo del sistema, alla compromissione dei dati o all'esecuzione dell'escalation dei privilegi.

Input non validato: i programmi spesso operano con input di dati. Tali dati immessi nel programma possono avere contenuto dannoso, progettato per forzare un comportamento non intenzionale del programma. Si pensi a un programma che riceve un'immagine per l'elaborazione. Un utente malintenzionato può creare un file di immagine con dimensioni dell'immagine non valide. Le dimensioni create per fini dannosi potrebbero forzare il programma ad allocare buffer di dimensioni non corrette e impreviste.

Race condition: questa vulnerabilità si ha quando l'output di un evento dipende da output ordinati o temporizzati. Un condition rate diventa fonte di vulnerabilità quando gli eventi ordinati o temporizzati richiesti non si verificano nell'ordine o nei tempi corretti.

Punti deboli nelle procedure di sicurezza: sistemi e dati sensibili possono essere protetti con tecniche quali autenticazione, autorizzazione e crittografia. Gli sviluppatori non devono tentare di creare i propri algoritmi di protezione, perché potrebbero introdurre vulnerabilità. È di gran lunga preferibile che gli sviluppatori utilizzino librerie di protezione già create, collaudate e verificate.

Problemi di controllo degli accessi: il processo di controllo degli accessi consente di verificare l'autore di



Input non validato: i programmi spesso operano con input di dati. Tali dati immessi nel programma possono avere contenuto dannoso, progettato per forzare un comportamento non intenzionale del programma. Si pensi a un programma che riceve un'immagine per l'elaborazione. Un utente malintenzionato può creare un file di immagine con dimensioni dell'immagine non valide. Le dimensioni create per fini dannosi potrebbero forzare il programma ad allocare buffer di dimensioni non corrette e impreviste.

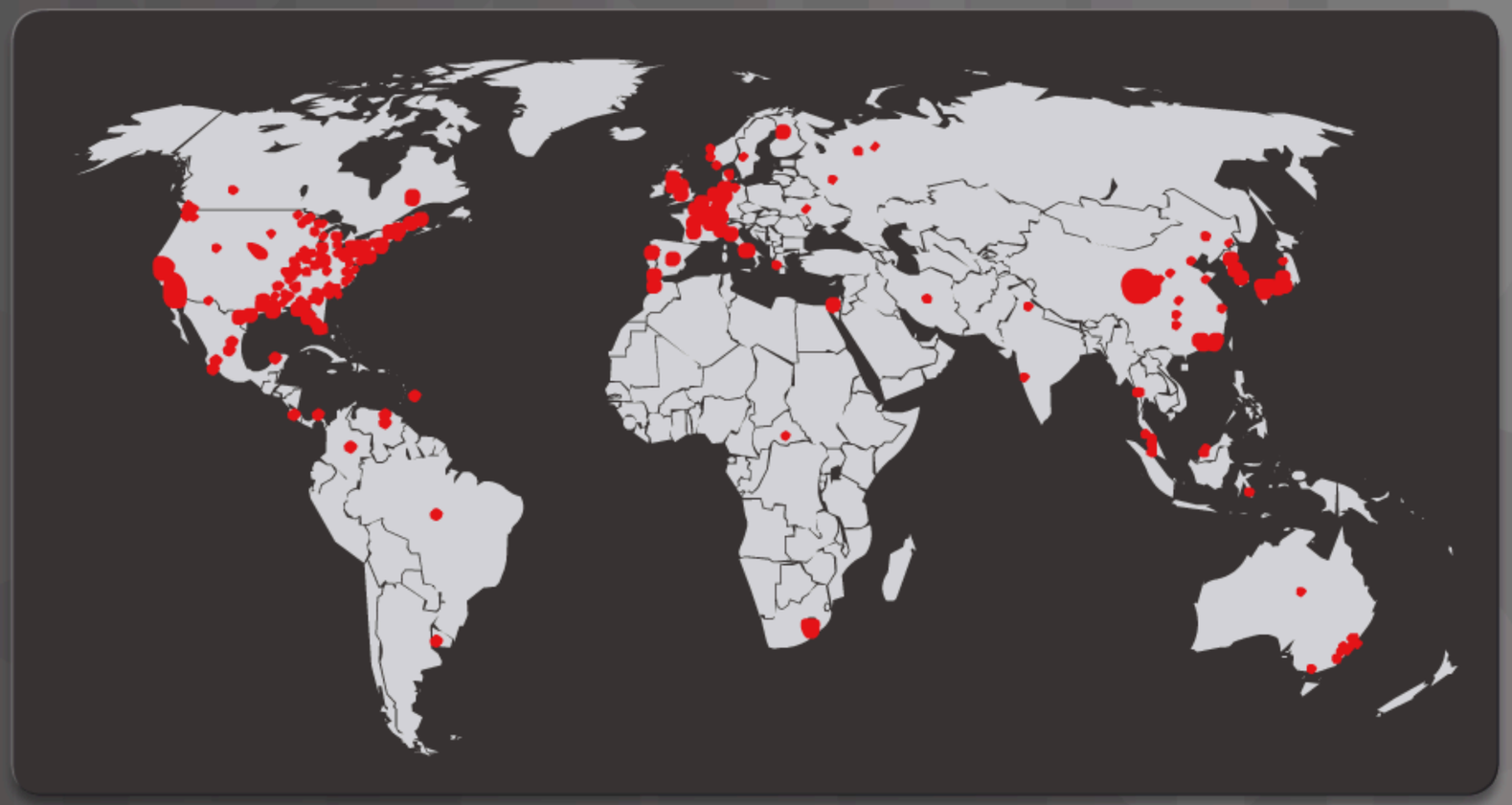
Race condition: questa vulnerabilità si ha quando l'output di un evento dipende da output ordinati o temporizzati. Un condition rate diventa fonte di vulnerabilità quando gli eventi ordinati o temporizzati richiesti non si verificano nell'ordine o nei tempi corretti.

Punti deboli nelle procedure di sicurezza: sistemi e dati sensibili possono essere protetti con tecniche quali autenticazione, autorizzazione e crittografia. Gli sviluppatori non devono tentare di creare i propri algoritmi di protezione, perché potrebbero introdurre vulnerabilità. È di gran lunga preferibile che gli sviluppatori utilizzino librerie di protezione già create, collaudate e verificate.

Problemi di controllo degli accessi: il processo di controllo degli accessi consente di verificare l'autore di un'operazione e spazia dalla gestione dell'accesso fisico alle apparecchiature all'assegnazione delle autorizzazioni e dei diritti di accesso a una risorsa, ad esempio di lettura o modifica del file. Molte vulnerabilità di protezione vengono create dall'utilizzo non corretto del controllo degli accessi.

Quasi tutti i sistemi di controllo degli accessi e le procedure di sicurezza possono essere elusi quando l'autore degli attacchi ha accesso fisico all'apparecchiatura obiettivo. Ad esempio, a prescindere dalle autorizzazioni impostate per un file, il sistema operativo non può impedire a un utente di aggirarlo e leggere i dati direttamente dal disco. Per proteggere il computer e i dati in esso contenuti, occorre limitare l'accesso fisico e utilizzare tecniche di crittografia per proteggere i dati da tentativi di furto o danneggiamento.

Infezione iniziale da worm Code Red

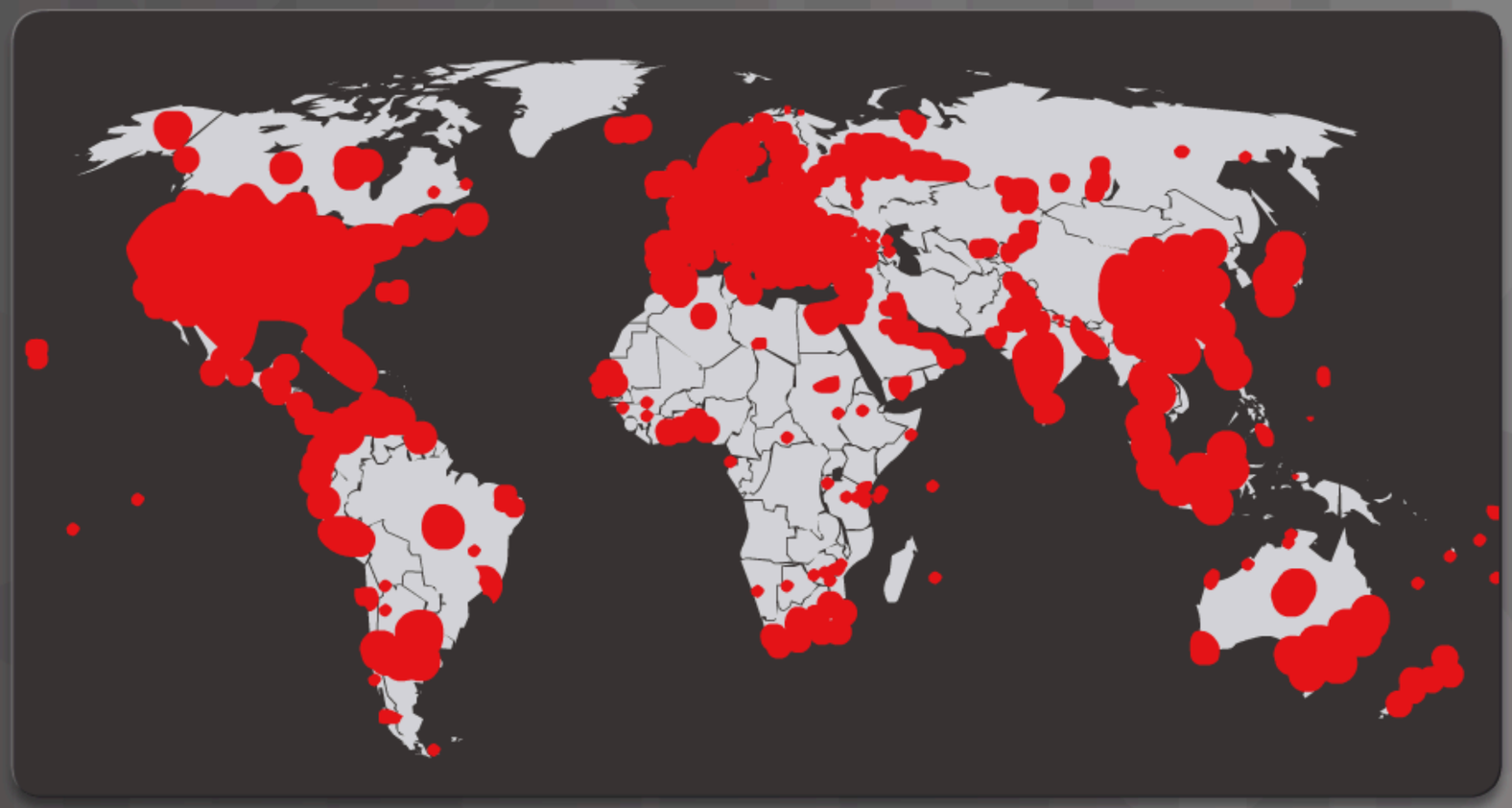


Tipologie di malware

Il malware, abbreviazione di software dannoso (Malicious Software), è qualsiasi codice utilizzabile per il furto dei dati, il bypass del controllo degli accessi oppure il danneggiamento o la compromissione di un sistema. Di seguito sono riportate alcune tipologie comuni di malware:

Spyware: questo malware è progettato per tracciare e spiare l'utente. Lo spyware spesso comprende activity tracker, sequenze di tasti e acquisizione di dati. In un tentativo di eludere le misure di sicurezza, lo spyware spesso modifica le impostazioni di protezione. Lo spyware è di frequente associato a software legittimo o Trojan horse.

Adware: l'Advertising supported software è progettato per recapitare automaticamente pubblicità. L'adware è spesso installato con alcune versioni software. Alcuni adware sono progettati per recapitare solo pubblicità ma è frequente che



Tipologie di malware

Il malware, abbreviazione di software dannoso (Malicious Software), è qualsiasi codice utilizzabile per il furto dei dati, il bypass del controllo degli accessi oppure il danneggiamento o la compromissione di un sistema. Di seguito sono riportate alcune tipologie comuni di malware:

Spyware: questo malware è progettato per tracciare e spiare l'utente. Lo spyware spesso comprende activity tracker, sequenze di tasti e acquisizione di dati. In un tentativo di eludere le misure di sicurezza, lo spyware spesso modifica le impostazioni di protezione. Lo spyware è di frequente associato a software legittimo o Trojan horse.

Adware: l'Advertising supported software è progettato per recapitare automaticamente pubblicità. L'adware è spesso installato con alcune versioni software. Alcuni adware sono progettati per recapitare solo pubblicità ma è frequente che



Tipologie di malware

Il malware, abbreviazione di software dannoso (Malicious Software), è qualsiasi codice utilizzabile per il furto dei dati, il bypass del controllo degli accessi oppure il danneggiamento o la compromissione di un sistema. Di seguito sono riportate alcune tipologie comuni di malware:

Spyware: questo malware è progettato per tracciare e spiare l'utente. Lo spyware spesso comprende activity tracker, sequenze di tasti e acquisizione di dati. In un tentativo di eludere le misure di sicurezza, lo spyware spesso modifica le impostazioni di protezione. Lo spyware è di frequente associato a software legittimo o Trojan horse.

Adware: l'Advertising supported software è progettato per recapitare automaticamente pubblicità. L'adware è spesso installato con alcune versioni software. Alcuni adware sono progettati per recapitare solo pubblicità ma è frequente che contengano spyware.

Bot: derivante dalla parola robot, un bot è un malware progettato per eseguire automaticamente azioni, solitamente online. Sebbene la maggior parte dei bot sia innocua, un utilizzo crescente di bot dannosi è rappresentato dai botnet. Molti computer sono infetti da bot programmati per restare in attesa dei comandi dell'autore degli attacchi.

Ransomware: questo malware è progettato per tenere bloccato un sistema informatico o i dati in esso contenuti fino al pagamento di una somma. Il ransomware solitamente agisce crittografando i dati nel computer con una chiave sconosciuta all'utente. Altre versioni del ransomware possono sfruttare vulnerabilità specifiche del sistema per bloccare il sistema. Il ransomware viene diffuso nel sistema da un file scaricato o mediante una



Scareware: è un tipo di malware progettato per indurre l'utente a eseguire un'azione specifica facendo leva sulla paura. Lo scareware crea finestre pop-up simili alle finestre di dialogo del sistema operativo. Queste finestre visualizzano messaggi creati per informare l'utente che il sistema è a rischio o che necessita dell'esecuzione di un programma specifico per tornare allo stato normale di funzionamento. In realtà, non è stato accertato o rilevato alcun problema e se l'utente accetta e approva l'esecuzione del programma indicato, il sistema viene infettato da malware.

Rootkit: questo malware è progettato per modificare il sistema operativo al fine di creare una backdoor. Gli autori degli attacchi utilizzano poi la backdoor per accedere al computer in remoto. La maggior parte dei rootkit sfrutta le vulnerabilità software per eseguire l'escalation dei privilegi e modificare i file di sistema. È inoltre frequente che i rootkit modifichino gli strumenti di monitoraggio e le analisi forensi del sistema, rendendone estremamente difficile il rilevamento. Spesso, per un computer infetto da rootkit occorre procedere alla cancellazione e reinstallazione dei dati del sistema.

Virus: un virus è un codice eseguibile dannoso collegato ad altri file eseguibili, spesso programmi legittimi. La maggior parte dei virus richiede attivazione da parte dell'utente finale e può attivarsi a un'ora o una data specifica. I virus possono essere innocui e visualizzare semplicemente un'immagine o distruttivi, ad esempio quelli progettati per modificare o eliminare i dati. Possono inoltre essere programmati per mutare ed evitare il rilevamento. La diffusione della maggior parte dei virus ora avviene per mezzo di unità USB, dischi ottici, condivisioni di rete o e-mail.

Trojan horse: un Trojan horse è un tipo di malware che esegue operazioni dannose sotto forma di un'operazione desiderata. Questo codice dannoso procede all'exploit dei privilegi dell'utente che lo esegue. I trojan sono spesso presenti in file di immagini, file audio o giochi. Un Trojan horse differisce da un virus perché si associa a file non eseguibili.

Infezione da worm Code Red 19 ore dopo



spesso presenti in file di immagini, file audio o giochi. Un Trojan horse differisce da un virus perché si associa a file non eseguibili.

Worm: i worm sono costituiti da codice dannoso che si replica in modo autonomo sfruttando le vulnerabilità nelle reti. Solitamente i worm rallentano le reti. Mentre per l'esecuzione di un virus occorre un programma host, i worm possono attivarsi autonomamente. Dopo l'infezione iniziale, non necessitano più di alcuna interazione da parte dell'utente. Quando l'host è infettato, il worm è in grado di diffondersi molto rapidamente in rete. I worm condividono pattern analoghi. Tutti hanno una vulnerabilità abilitante, un modo per propagarsi e contengono un payload.

I worm sono responsabili di alcuni degli attacchi più devastanti di Internet. Come illustrato nella Figura 1, nel 2001 il worm Code Red aveva infettato 658 server. Dopo 19 ore, il worm aveva infettato 300.000 server come indicato nella Figura 2.

Man-In-The-Middle (MitM): il MitM consente all'autore dell'attacco di prendere il controllo su un dispositivo senza che l'utente ne sia a conoscenza. Con questo livello di accesso, l'autore dell'attacco può intercettare e acquisire informazioni dell'utente prima del loro trasferimento nella destinazione prevista. Gli attacchi di tipo MitM sono ampiamente utilizzati per il furto di informazioni di natura finanziaria. Esistono molte tecniche e tipologie di malware che forniscono agli autori degli attacchi funzionalità MitM.

Man-In-The-Mobile (MitMo): variazione di man-in-middle, il MitMo è un tipo di attacco impiegato per acquisire il controllo su un dispositivo mobile. Una volta infettato, al dispositivo mobile può essere richiesto di esfiltrare informazioni sensibili dell'utente e inviarle agli autori degli attacchi. ZeuS, un esempio di exploit con funzionalità MitMo, consente agli autori degli attacchi di acquisire silenziosamente i messaggi SMS di verifica in 2 fasi inviati agli utenti.

Sintomi del malware

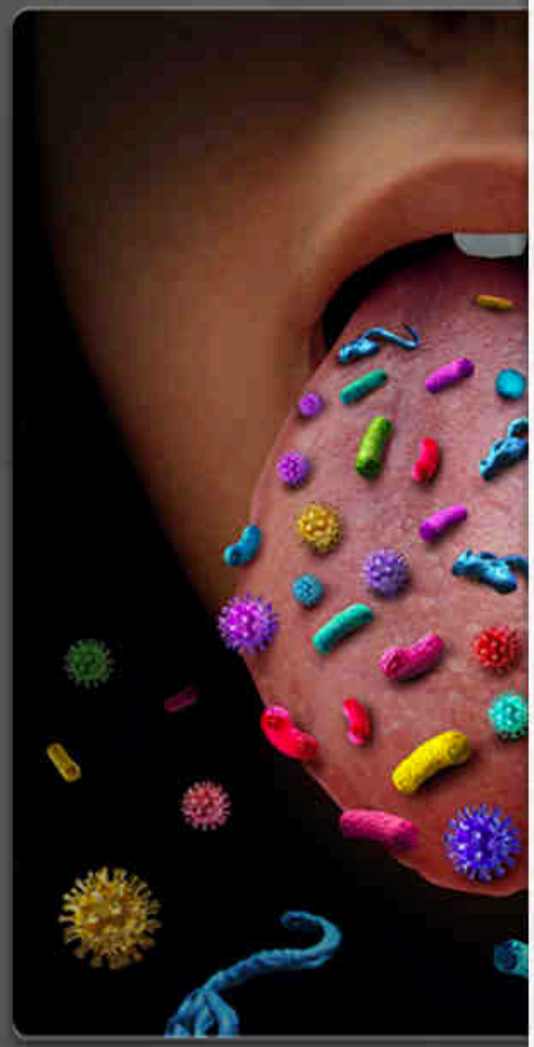


Sintomi del malware

Di seguito sono riportati sintomi di infezione da malware comuni a prescindere dal tipo di malware con cui è stato infettato un sistema:

- Aumento nell'utilizzo di CPU.
- Riduzione nella velocità del computer.
- Il computer spesso si blocca o si arresta in modo anomalo.
- Riduzione nella velocità di navigazione nel Web.
- Problemi inspiegabili con le connessioni di rete.
- File modificati.
- File eliminati.
- Presenza di file, programmi o icone desktop sconosciuti.

Sintomi de



Sintomi del malware

Di seguito sono riportati sintomi di infezione da malware comuni a prescindere dal tipo di malware con cui è stato infettato un sistema:

- Aumento nell'utilizzo di CPU.
- Riduzione nella velocità del computer.
- Il computer spesso si blocca o si arresta in modo anomalo.
- Riduzione nella velocità di navigazione nel Web.
- Problemi inspiegabili con le connessioni di rete.
- File modificati.
- File eliminati.
- Presenza di file, programmi o icone desktop sconosciuti.
- Processi sconosciuti in esecuzione.
- I programmi si disattivano o riconfigurano autonomamente.
- Invio di e-mail senza che l'utente ne sia a conoscenza o abbia acconsentito.

Social engineering



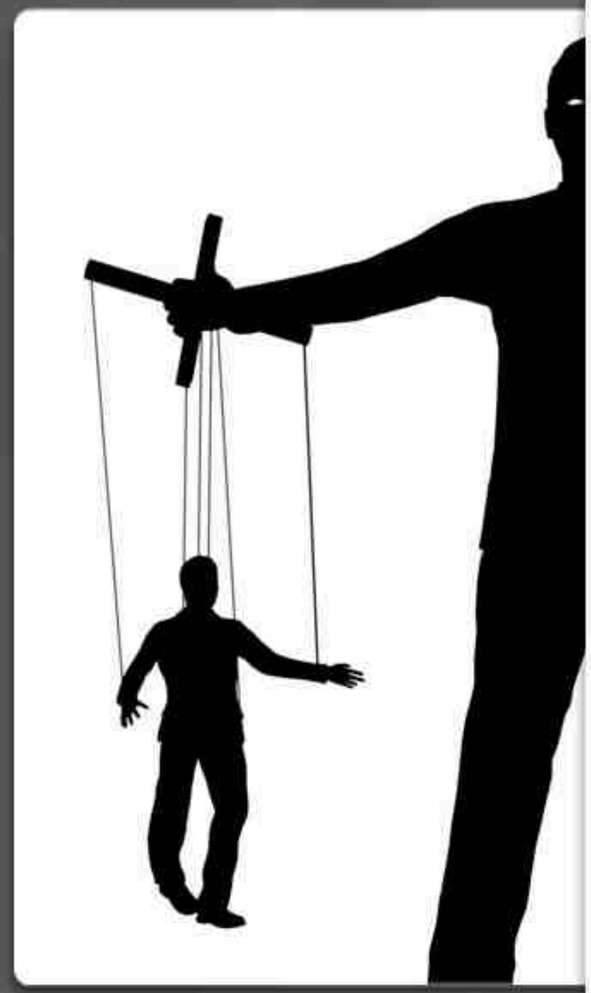
Social engineering

Il social engineering è un attacco di accesso in cui si tenta di manipolare gli utenti nell'esecuzione di azioni o nella divulgazione di informazioni riservate. I social engineer spesso contano sulla disponibilità delle persone a rendersi utili oltre ad approfittare delle loro debolezze. L'autore degli attacchi, ad esempio, potrebbe contattare un dipendente autorizzato con un problema urgente che richiede accesso immediato alla rete. Potrebbe far leva sulla vanità del dipendente, evocare autorità con tecniche di name-dropping o fare ricorso alla cupidigia del dipendente.

Di seguito sono riportati alcuni tipi di attacchi di social engineering:

- Pretexting: si ha quando l'autore degli attacchi si rivolge a un individuo mentendogli nel tentativo di ottenere l'accesso a dati con privilegi. Ne è un esempio un autore di attacchi che finge di avere necessità di dati di

Social engineering



Social engineering

Il social engineering è un attacco di accesso in cui si tenta di manipolare gli utenti nell'esecuzione di azioni o nella divulgazione di informazioni riservate. I social engineer spesso contano sulla disponibilità delle persone a rendersi utili oltre ad approfittare delle loro debolezze. L'autore degli attacchi, ad esempio, potrebbe contattare un dipendente autorizzato con un problema urgente che richiede accesso immediato alla rete. Potrebbe far leva sulla vanità del dipendente, evocare autorità con tecniche di name-dropping o fare ricorso alla cupidigia del dipendente.

Di seguito sono riportati alcuni tipi di attacchi di social engineering:

- Pretexting: si ha quando l'autore degli attacchi si rivolge a un individuo mentendogli nel tentativo di ottenere l'accesso a dati con privilegi. Ne è un esempio un autore di attacchi che finge di avere necessità di dati di natura personale o finanziaria per poter verificare l'identità del destinatario.
- Tailgating: si ha quando l'autore degli attacchi segue rapidamente una persona autorizzata in un luogo sicuro.
- Something for Something (Quid pro quo): si ha quando l'autore degli attacchi chiede dati personali a un interlocutore in cambio di qualcosa, ad esempio un regalo.

Violazione delle password Wi-Fi



Violazione delle password Wi-Fi

Per violazione delle password Wi-Fi si intende il processo di individuazione delle password utilizzate per proteggere una rete wireless. Di seguito sono riportate alcune tecniche utilizzate nella violazione delle password:

Social engineering: l'autore degli attacchi manipola una persona per farsi comunicare la password di cui è a conoscenza.

Attacchi " brute-force" : l'autore degli attacchi prova varie password nel tentativo di indovinare quella giusta. Se la password è un numero di 4 cifre, ad esempio, l'autore degli attacchi dovrebbe provare tutte e 10.000 le combinazioni. Gli attacchi " brute-force" si avvalgono solitamente di un file elenco di parole. Si tratta di un file di testo contenente un elenco di parole estratte da un dizionario. Un programma prova ogni parola e le combinazioni più comuni. Dato che gli attacchi

Violazione delle password Wi-Fi



Violazione delle password Wi-Fi

Per violazione delle password Wi-Fi si intende il processo di individuazione delle password utilizzate per proteggere una rete wireless. Di seguito sono riportate alcune tecniche utilizzate nella violazione delle password:

Social engineering: l'autore degli attacchi manipola una persona per farsi comunicare la password di cui è a conoscenza.

Attacchi "brute-force": l'autore degli attacchi prova varie password nel tentativo di indovinare quella giusta. Se la password è un numero di 4 cifre, ad esempio, l'autore degli attacchi dovrebbe provare tutte e 10.000 le combinazioni. Gli attacchi "brute-force" si avvalgono solitamente di un file elenco di parole. Si tratta di un file di testo contenente un elenco di parole estratte da un dizionario. Un programma prova ogni parola e le combinazioni più comuni. Dato che gli attacchi "brute-force" richiedono tempo, per indovinare password complesse ne occorre molto di più. Alcuni degli strumenti di attacco "brute-force" per le password sono Ophcrack, L0phtCrack, THC Hydra, RainbowCrack e Medusa.

Network sniffing: restando in ascolto dei pacchetti inviati sulla rete e acquisendoli, l'autore degli attacchi potrebbe riuscire a scoprire la password se questa è stata inviata in forma non crittografata. Quando la password è crittografata, l'autore degli attacchi può riuscire comunque a identificarla utilizzando uno strumento di violazione delle password.

Phishing



Phishing

Il phishing consiste nell'invio da parte di un utente malintenzionato, di un'e-mail fraudolenta dissimulata come proveniente da una fonte legittima e attendibile. L'intento del messaggio è convincere con l'inganno il destinatario a installare il malware sul dispositivo o a condividere dati di natura personale o finanziaria. Un esempio di phishing è un'e-mail creata per sembrare inviata da un negozio al dettaglio, in cui si chiede all'utente di selezionare un collegamento per ottenere un premio. Il collegamento potrebbe accedere a un finto sito in cui si richiedono dati personali oppure installare un virus.

Lo spear phishing è un attacco di tipo phishing altamente mirato. Sebbene sia il phishing che lo spear phishing utilizzino e-mail per raggiungere le vittime, le e-mail inviate da quest'ultimo sono personalizzate per un individuo specifico. L'autore degli attacchi prima di inviare l'e-mail esegue una ricerca sugli interessi dell'obiettivo. Ad esempio,

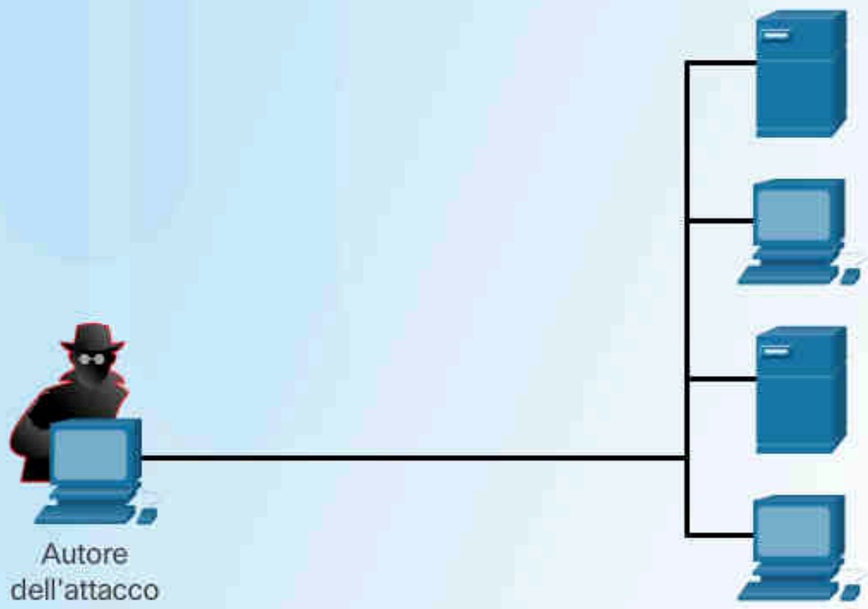


Phishing

Il phishing consiste nell'invio da parte di un utente malintenzionato, di un'e-mail fraudolenta dissimulata come proveniente da una fonte legittima e attendibile. L'intento del messaggio è convincere con l'inganno il destinatario a installare il malware sul dispositivo o a condividere dati di natura personale o finanziaria. Un esempio di phishing è un'e-mail creata per sembrare inviata da un negozio al dettaglio, in cui si chiede all'utente di selezionare un collegamento per ottenere un premio. Il collegamento potrebbe accedere a un finto sito in cui si richiedono dati personali oppure installare un virus.

Lo spear phishing è un attacco di tipo phishing altamente mirato. Sebbene sia il phishing che lo spear phishing utilizzino e-mail per raggiungere le vittime, le e-mail inviate da quest'ultimo sono personalizzate per un individuo specifico. L'autore degli attacchi prima di inviare l'e-mail esegue una ricerca sugli interessi dell'obiettivo. Ad esempio, l'autore degli attacchi scopre che l'obiettivo è interessato alle auto e sta valutando di acquistare un modello specifico. L'autore degli attacchi si collega allo stesso forum di discussione sulle auto di cui è membro l'obiettivo, crea un'offerta di vendita di auto e invia l'e-mail all'obiettivo. L'e-mail contiene un collegamento per accedere alle immagini dell'auto. Quando l'obiettivo seleziona il collegamento, il malware viene installato sul computer dell'obiettivo.

Strumento WHOIS



Exploit delle vulnerabilità

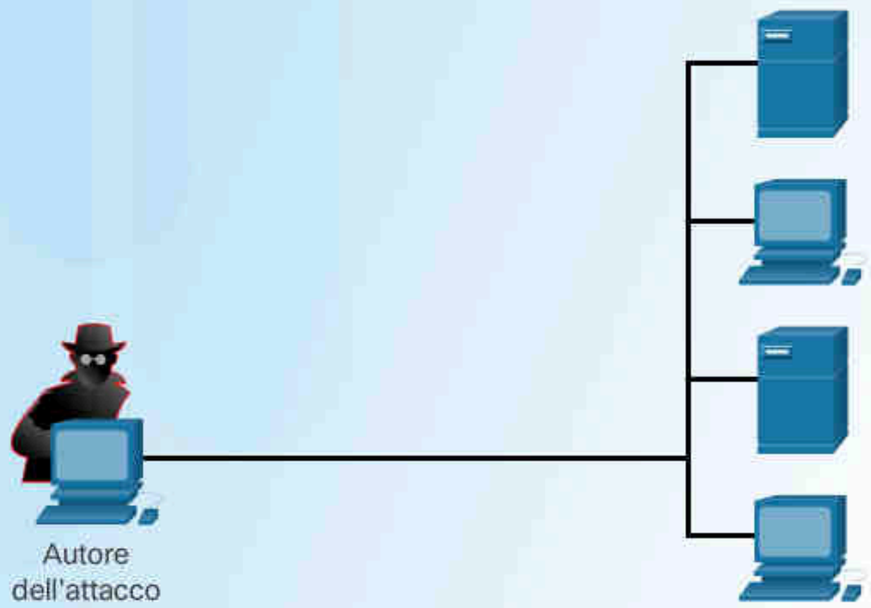
L'exploit delle vulnerabilità è un altro metodo diffuso di infiltrazione. Gli autori degli attacchi analizzano i computer per ottenerne le informazioni. Di seguito è riportato un metodo diffuso di exploit delle vulnerabilità:

Fase 1. Raccolta di informazioni sul sistema obiettivo. Questa operazione è eseguibile in molti modi differenti, ad esempio mediante scanner di porte o social engineering. L'intento è apprendere quanto più possibile sul computer obiettivo.

Fase 2. Una parte delle informazioni pertinenti ottenute nella fase 1, potrebbe riguardare il sistema operativo, la relativa versione e un elenco dei servizi in esecuzione su di esso.

Fase 3. Una volta conosciuti sistema operativo e versione dell'obiettivo, l'autore degli attacchi cerca vulnerabilità note specifiche di tale versione di sistema operativo o di altri servizi del sistema operativo.

Scanner porte (NMAP)



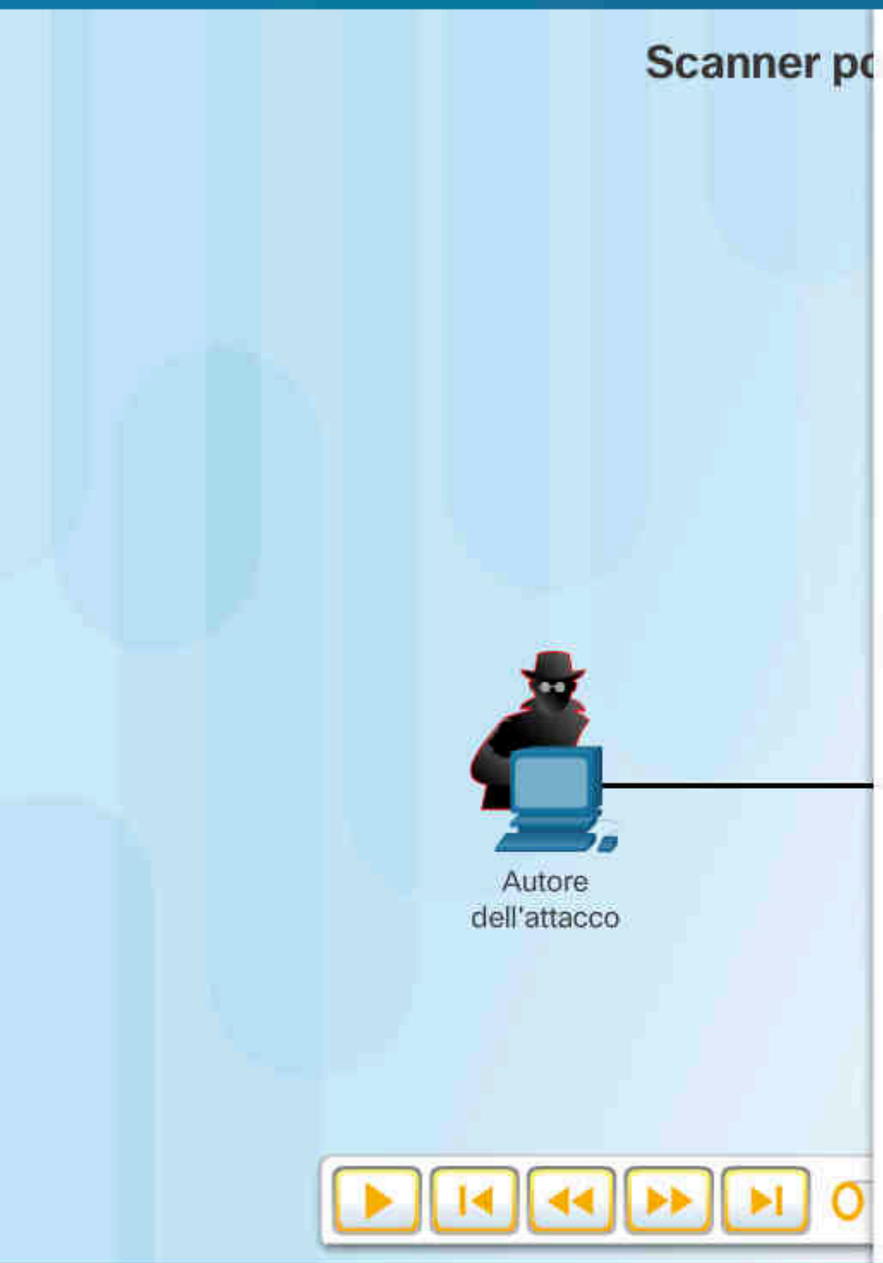
Exploit delle vulnerabilità

L'exploit delle vulnerabilità è un altro metodo diffuso di infiltrazione. Gli autori degli attacchi analizzano i computer per ottenerne le informazioni. Di seguito è riportato un metodo diffuso di exploit delle vulnerabilità:

Fase 1. Raccolta di informazioni sul sistema obiettivo. Questa operazione è eseguibile in molti modi differenti, ad esempio mediante scanner di porte o social engineering. L'intento è apprendere quanto più possibile sul computer obiettivo.

Fase 2. Una parte delle informazioni pertinenti ottenute nella fase 1, potrebbe riguardare il sistema operativo, la relativa versione e un elenco dei servizi in esecuzione su di esso.

Fase 3. Una volta conosciuti sistema operativo e versione dell'obiettivo, l'autore degli attacchi cerca vulnerabilità note specifiche di tale versione di sistema operativo o di altri servizi del sistema operativo.



Exploit delle vulnerabilità

L'exploit delle vulnerabilità è un altro metodo diffuso di infiltrazione. Gli autori degli attacchi analizzano i computer per ottenerne le informazioni. Di seguito è riportato un metodo diffuso di exploit delle vulnerabilità:

Fase 1. Raccolta di informazioni sul sistema obiettivo. Questa operazione è eseguibile in molti modi differenti, ad esempio mediante scanner di porte o social engineering. L'intento è apprendere quanto più possibile sul computer obiettivo.

Fase 2. Una parte delle informazioni pertinenti ottenute nella fase 1, potrebbe riguardare il sistema operativo, la relativa versione e un elenco dei servizi in esecuzione su di esso.

Fase 3. Una volta conosciuti sistema operativo e versione dell'obiettivo, l'autore degli attacchi cerca vulnerabilità note specifiche di tale versione di sistema operativo o di altri servizi del sistema operativo.

Fase 4. Individuata una vulnerabilità, l'autore degli attacchi cerca un exploit scritto in precedenza da utilizzare. Se non è stato scritto alcun exploit, l'autore degli attacchi può considerare di scriverne uno.

Nella Figura 1 è raffigurato un autore di attacchi che utilizza whois, un database Internet pubblico contenente informazioni sui nomi di dominio e i relativi registranti. Nella Figura 2 è raffigurato un autore di attacchi che utilizza lo strumento nmap, uno scanner di porte molto diffuso. Con uno scanner di porte, l'autore degli attacchi può sondare le porte di un computer obiettivo per conoscere quali servizi sono in esecuzione su tale computer.

Minacce persistenti avanzate

Scanner po



Autore dell'attacco

Fase 2. Una parte delle informazioni pertinenti ottenute nella fase 1, potrebbe riguardare il sistema operativo, la relativa versione e un elenco dei servizi in esecuzione su di esso.

Fase 3. Una volta conosciuti sistema operativo e versione dell'obiettivo, l'autore degli attacchi cerca vulnerabilità note specifiche di tale versione di sistema operativo o di altri servizi del sistema operativo.

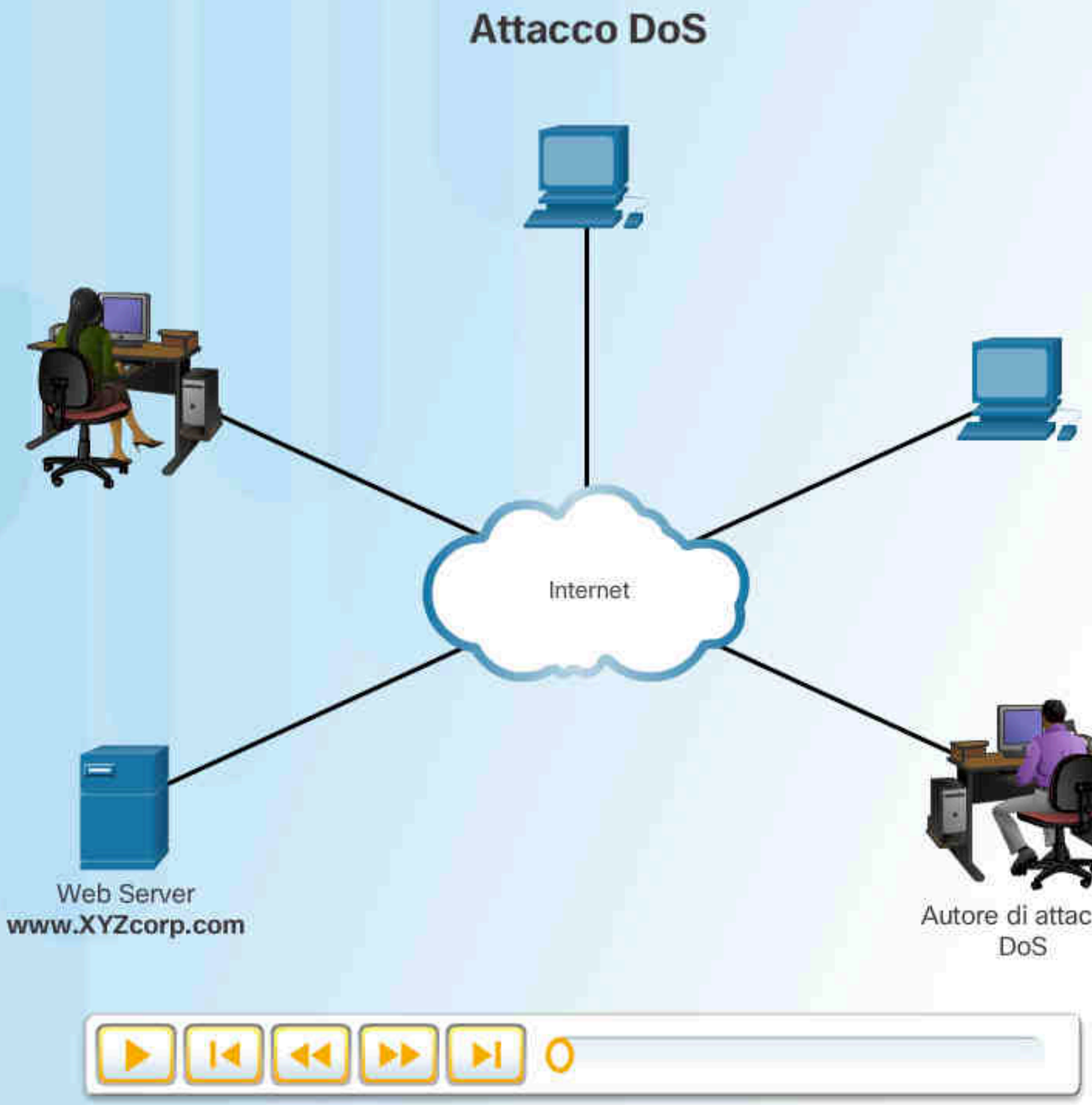
Fase 4. Individuata una vulnerabilità, l'autore degli attacchi cerca un exploit scritto in precedenza da utilizzare. Se non è stato scritto alcun exploit, l'autore degli attacchi può considerare di scriverne uno.

Nella Figura 1 è raffigurato un autore di attacchi che utilizza whois, un database Internet pubblico contenente informazioni sui nomi di dominio e i relativi registranti. Nella Figura 2 è raffigurato un autore di attacchi che utilizza lo strumento nmap, uno scanner di porte molto diffuso. Con uno scanner di porte, l'autore degli attacchi può sondare le porte di un computer obiettivo per conoscere quali servizi sono in esecuzione su tale computer.

Minacce persistenti avanzate

Uno dei metodi utilizzati per penetrare in un sistema sono le minacce avanzate persistenti (APT). Si tratta di un'operazione multi fase avanzata e dissimulata a lungo termine posta in essere contro un obiettivo specifico. Data la sua complessità e il livello di competenza richiesto, un APT è ben finanziato. Un APT è mirato a organizzazioni o nazioni per motivi commerciali o politici.

Generalmente collegato allo spionaggio basato sulla rete, lo scopo dell'APT è implementare malware personalizzato su uno o più dei sistemi obiettivo senza essere rilevato. Essendo caratterizzato da un'operazione multi fase e da vari tipi personalizzati di malware che interessano dispositivi differenti ed eseguono funzioni diverse, un singolo autore di attacchi manca spesso della serie di competenze, delle risorse o della perseveranza necessarie per un attacco di tipo APT.

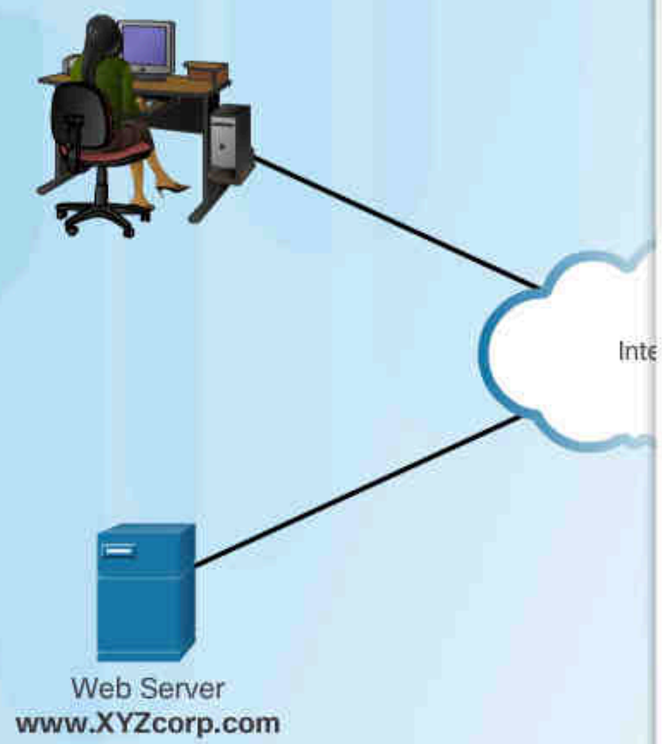


DoS

Gli attacchi Denial-of-Service (DoS) sono un tipo di attacchi alla rete. Un attacco DoS genera una sorta di interruzione del servizio di rete a utenti, dispositivi o applicazioni. Esistono due tipi principali di attacchi DoS:

Overwhelming Quantity of Traffic: in questo tipo di attacco un enorme volume di dati viene inviato a una rete, un host o un'applicazione a una velocità ingestibile. Ciò causa un rallentamento nella trasmissione o nella risposta oppure l'arresto anomalo di un dispositivo o di un servizio.

Maliciously Formatted Packets: in questo tipo di attacco un pacchetto formattato con intento dannoso viene inviato a un host o a un'applicazione e il ricevente non è in grado di gestirlo. Ad esempio, l'autore degli attacchi invia pacchetti contenenti errori non identificabili dall'applicazione oppure inoltra pacchetti non correttamente formattati. In tal modo, il dispositivo



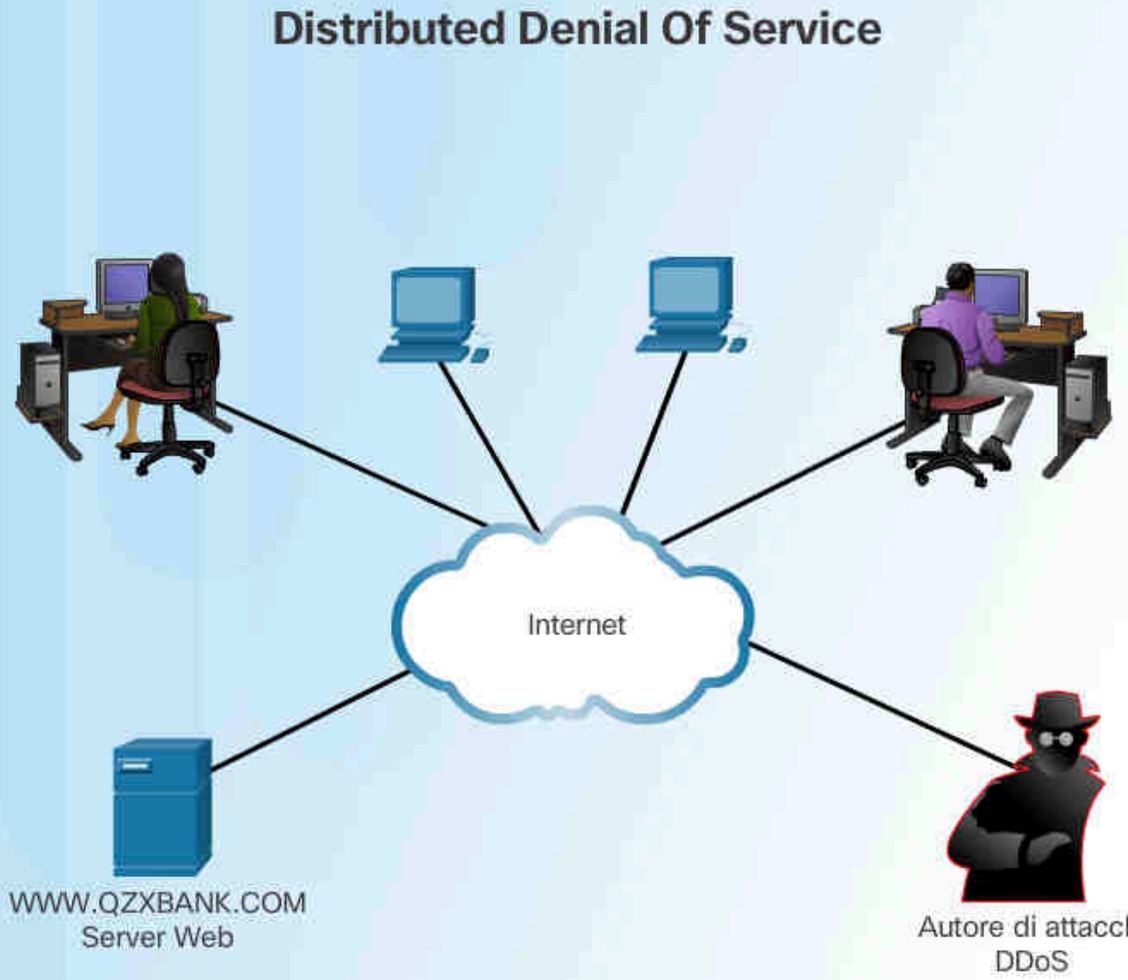
DoS

Gli attacchi Denial-of-Service (DoS) sono un tipo di attacchi alla rete. Un attacco DoS genera una sorta di interruzione del servizio di rete a utenti, dispositivi o applicazioni. Esistono due tipi principali di attacchi DoS:

Overwhelming Quantity of Traffic: in questo tipo di attacco un enorme volume di dati viene inviato a una rete, un host o un'applicazione a una velocità ingestibile. Ciò causa un rallentamento nella trasmissione o nella risposta oppure l'arresto anomalo di un dispositivo o di un servizio.

Maliciously Formatted Packets: in questo tipo di attacco un pacchetto formattato con intento dannoso viene inviato a un host o a un'applicazione e il ricevente non è in grado di gestirlo. Ad esempio, l'autore degli attacchi invia pacchetti contenenti errori non identificabili dall'applicazione oppure inoltra pacchetti non correttamente formattati. In tal modo, il dispositivo ricevente risulta estremamente lento oppure si arresta in modo anomalo.

Gli attacchi DoS sono considerati un grave rischio in quanto possono facilmente interrompere la comunicazione e causare significative perdite di tempo e denaro. Questi attacchi sono relativamente semplici da attuare, anche da un autore di attacchi inesperto.



DDoS

Un attacco Distributed DoS (DDoS) è simile al DoS ma originato da più sorgenti coordinate. Ad esempio, un attacco DDoS potrebbe procedere nel seguente modo:

L'autore degli attacchi crea una rete di host infetti denominata botnet. Gli host infetti sono detti zombie. Gli zombie sono controllati da sistemi gestori.

I computer zombie analizzano e infettano costantemente altri host, creando nuovi zombie. Una volta pronto, l'hacker ordina ai sistemi gestori di far eseguire ai botnet di zombie un attacco DDoS.

Fare clic su Play nella figura per visualizzare le animazioni di un attacco DDoS.

Alterazione SEO



Alterazione SEO

I motori di ricerca come Google operano classificando le pagine e presentando risultati pertinenti basati sulle query di ricerca degli utenti. A seconda della pertinenza del contenuto del sito Web, possono comparire ai livelli più alti o più bassi dell'elenco dei risultati di ricerca. Con l'acronimo SEO, Search Engine Optimization ovvero ottimizzazione dei motori di ricerca, sono identificate una serie di tecniche utilizzate per migliorare la classificazione di un sito Web da parte del motore di ricerca. Anche se molte aziende legittime sono specializzate nell'ottimizzazione dei siti Web per migliorarne la posizione di visualizzazione, un utente malintenzionato potrebbe utilizzare tecniche SEO per fare in modo che un sito Web dannoso compaia nelle prime posizioni dei risultati di ricerca. Questa tecnica è detta SEO poisoning.

L'obiettivo più comune del SEO poisoning è aumentare il traffico verso siti dannosi che

Alterazione SEO

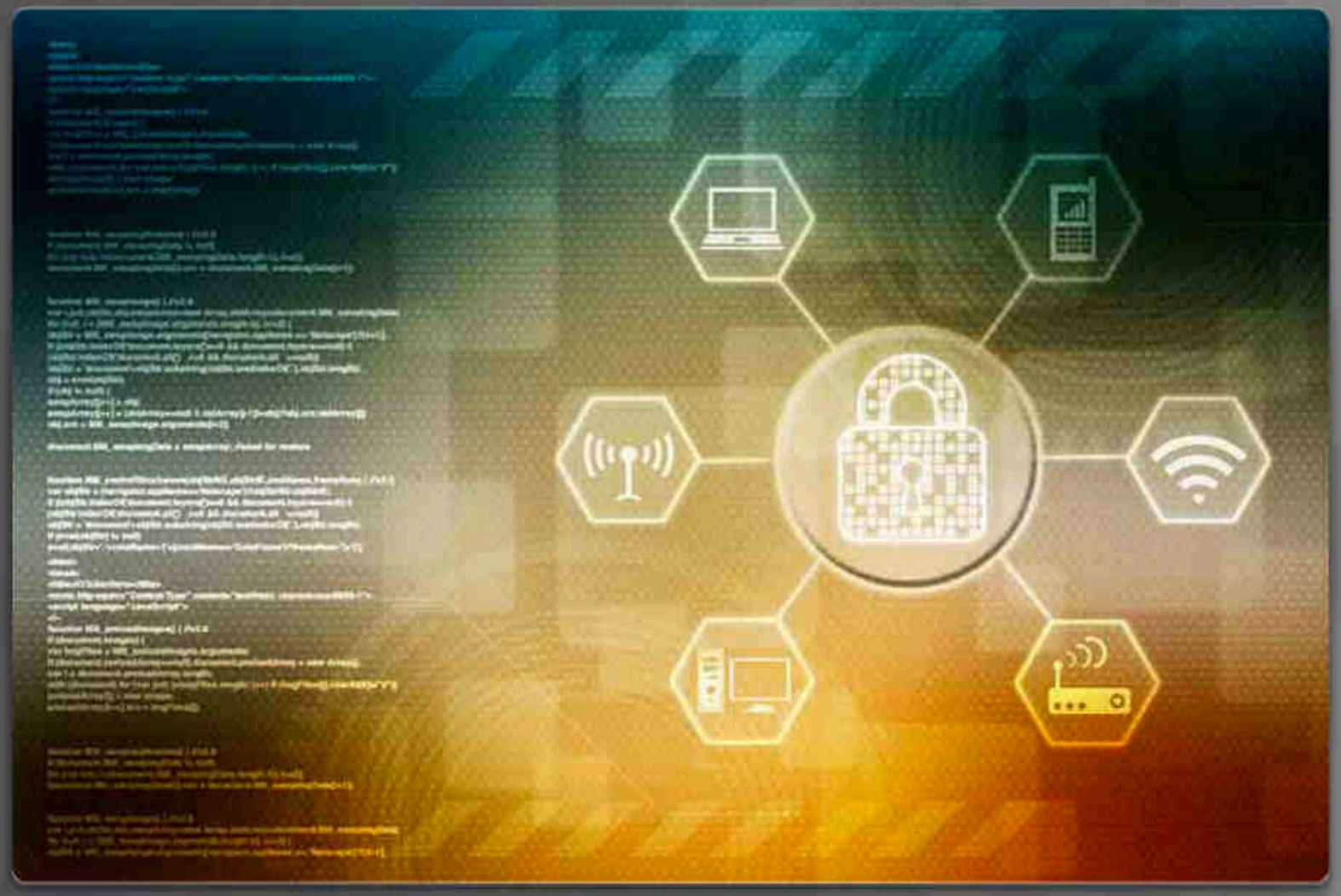


Alterazione SEO

I motori di ricerca come Google operano classificando le pagine e presentando risultati pertinenti basati sulle query di ricerca degli utenti. A seconda della pertinenza del contenuto del sito Web, possono comparire ai livelli più alti o più bassi dell'elenco dei risultati di ricerca. Con l'acronimo SEO, Search Engine Optimization ovvero ottimizzazione dei motori di ricerca, sono identificate una serie di tecniche utilizzate per migliorare la classificazione di un sito Web da parte del motore di ricerca. Anche se molte aziende legittime sono specializzate nell'ottimizzazione dei siti Web per migliorarne la posizione di visualizzazione, un utente malintenzionato potrebbe utilizzare tecniche SEO per fare in modo che un sito Web dannoso compaia nelle prime posizioni dei risultati di ricerca. Questa tecnica è detta SEO poisoning.

L'obiettivo più comune del SEO poisoning è aumentare il traffico verso siti dannosi che potrebbero contenere malware o eseguire il social engineering. Per forzare il posizionamento di un sito dannoso ai livelli più alti dei risultati di ricerca, gli autori degli attacchi si avvalgono dei termini di ricerca più diffusi.

Attacchi misti



Che cos'è un attacco misto?

Gli attacchi misti utilizzano varie tecniche per compromettere un obiettivo. Impiegando contemporaneamente più tecniche di tipo diverso, gli autori degli attacchi ottengono malware che sono un ibrido degli schemi di worm, Trojan horse, spyware, keylogger, spam e phishing. Il trend degli attacchi misti è rivelatore di malware più complessi ed espone i dati degli utenti a un grande rischio.

La tipologia più comune di attacco misto si avvale di messaggi e-mail spam, messaggistica istantanea o siti Web legittimi per distribuire collegamenti da cui vengono scaricati segretamente malware o spyware sul computer. Un altro attacco misto molto diffuso impiega il DDoS in combinazione con e-mail di phishing. Inizialmente, il DDoS viene utilizzato per disattivare il sito Web di una Banca conosciuta e inviare e-mail ai clienti della banca per scusarsi dell'inconveniente. L'e-mail indirizza inoltre gli utenti su un falso sito di emergenza che consente



Che cos'è un attacco misto?

Gli attacchi misti utilizzano varie tecniche per compromettere un obiettivo. Impiegando contemporaneamente più tecniche di tipo diverso, gli autori degli attacchi ottengono malware che sono un ibrido degli schemi di worm, Trojan horse, spyware, keylogger, spam e phishing. Il trend degli attacchi misti è rivelatore di malware più complessi ed espone i dati degli utenti a un grande rischio.

La tipologia più comune di attacco misto si avvale di messaggi e-mail spam, messaggistica istantanea o siti Web legittimi per distribuire collegamenti da cui vengono scaricati segretamente malware o spyware sul computer. Un altro attacco misto molto diffuso impiega il DDoS in combinazione con e-mail di phishing. Inizialmente, il DDoS viene utilizzato per disattivare il sito Web di una Banca conosciuta e inviare e-mail ai clienti della banca per scusarsi dell'inconveniente. L'e-mail indirizza inoltre gli utenti su un falso sito di emergenza che consente il furto dei loro dati di accesso reali.

Molti dei worm più dannosi per i computer come Nimbda, CodeRed, BugBear, Klez e Slammer sono classificati più specificatamente come attacchi misti, come indicato di seguito:

- Alcune varianti di Nimbda utilizzavano allegati e-mail, download di file da un server Web violato e il file sharing (condivisione di file) Microsoft (ad es. condivisioni anonime) come metodi di propagazione.
- Altre varianti di Nimbda erano in grado di modificare gli account guest del sistema per fornire privilegi amministrativi all'autore degli attacchi o al codice dannoso.

Anche i recenti worm Conficker e ZeuS/LICAT sono stati classificati come attacchi misti. Conficker faceva ricorso a tutti i metodi di propagazione tradizionali.

Riduzione dell'impatto



Cosa si intende per riduzione dell'impatto?

Sebbene la maggior parte delle odierne aziende di successo sia a conoscenza dei problemi di sicurezza più comuni e dedichi notevole impegno alla loro prevenzione, nessuna procedura di sicurezza è efficiente al 100%. Poiché una violazione è probabile che si verifichi quando la ricompensa è alta, le aziende e le organizzazioni devono essere preparate anche a contenere i danni.

È importante capire che l'impatto di una violazione non è connesso esclusivamente all'aspetto tecnico di essa, ad esempio furto di dati, danneggiamento di database o danni alla proprietà intellettuale, ma i danni si estendono anche alla reputazione dell'azienda. Rispondere a una violazione dei dati è un processo estremamente dinamico.

Di seguito sono riportate alcune importanti misure che un'azienda dovrebbe adottare, secondo molti

Riduzione dell'impatto



Cosa si intende per riduzione dell'impatto?

Sebbene la maggior parte delle odierne aziende di successo sia a conoscenza dei problemi di sicurezza più comuni e dedichi notevole impegno alla loro prevenzione, nessuna procedura di sicurezza è efficiente al 100%. Poiché una violazione è probabile che si verifichi quando la ricompensa è alta, le aziende e le organizzazioni devono essere preparate anche a contenere i danni.

È importante capire che l'impatto di una violazione non è connesso esclusivamente all'aspetto tecnico di essa, ad esempio furto di dati, danneggiamento di database o danni alla proprietà intellettuale, ma i danni si estendono anche alla reputazione dell'azienda. Rispondere a una violazione dei dati è un processo estremamente dinamico.

Di seguito sono riportate alcune importanti misure che un'azienda dovrebbe adottare, secondo molti esperti di sicurezza, quando viene identificata una violazione della sicurezza:

- Comunicare il problema. Internamente i dipendenti devono essere informati del problema e invitati a intraprendere azioni adeguate. Esternamente, i clienti devono essere informati tramite comunicazione diretta e annunci ufficiali. La comunicazione crea trasparenza, fattore essenziale in questo tipo di situazione.
- È importante essere sinceri e responsabili in caso di colpa dell'azienda.
- Fornire dettagli. Spiegare a cosa è dovuta la situazione e cosa è stato compromesso. Si presume inoltre che l'azienda si faccia carico dei costi relativi ai servizi di protezione dal furto di identità per i clienti interessati.
- Capire cosa ha causato e facilitato la violazione. Se necessario rivolgersi a esperti in analisi forense per

Riduzione dell'impatto



anche alla reputazione dell'azienda. Rispondere a una violazione dei dati è un processo estremamente dinamico.

Di seguito sono riportate alcune importanti misure che un'azienda dovrebbe adottare, secondo molti esperti di sicurezza, quando viene identificata una violazione della sicurezza:

- Comunicare il problema. Internamente i dipendenti devono essere informati del problema e invitati a intraprendere azioni adeguate. Esternamente, i clienti devono essere informati tramite comunicazione diretta e annunci ufficiali. La comunicazione crea trasparenza, fattore essenziale in questo tipo di situazione.
- È importante essere sinceri e responsabili in caso di colpa dell'azienda.
- Fornire dettagli. Spiegare a cosa è dovuta la situazione e cosa è stato compromesso. Si presume inoltre che l'azienda si faccia carico dei costi relativi ai servizi di protezione dal furto di identità per i clienti interessati.
- Capire cosa ha causato e facilitato la violazione. Se necessario rivolgersi a esperti in analisi forense per cercare e scoprire i dettagli.
- Utilizzare quanto scoperto dall'indagine forense per fare in modo che simili violazioni non si ripetano in futuro.
- Verificare che tutti i sistemi siano puliti, non sia stata installata alcuna backdoor e nient'altro sia stato compromesso. Gli autori degli attacchi spesso tentano di lasciare una backdoor per agevolare future violazioni. Verificare che questa situazione non si verifichi.
- Istruire dipendenti, partner e clienti su come evitare future violazioni.