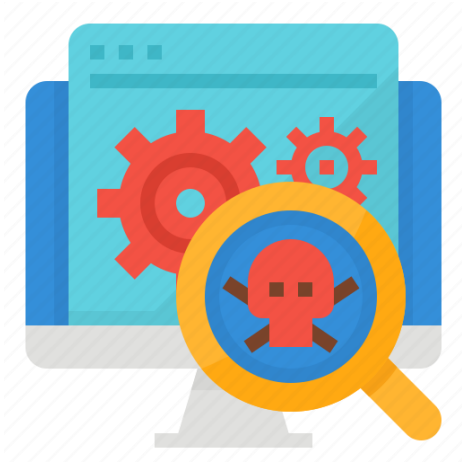
Malware

Security Awareness

Malware

«Malware» è un acronimo per **«MALicious softWARE»**, che si riferisce a qualsiasi script o codice binario che esegue qualche attività dannosa. Il malware può presentarsi in diversi formati, come eseguibili, codice binario di shell, script e firmware. In questo studio, quando ci riferiamo al malware, usiamo anche il termine "codice binario malevolo", ma sono accettabili anche i termini "script malevolo" o "eseguibile malevolo".



Tipologie di malware parte 1

Un **virus** inietta il suo codice maligno in altri file, diffondendosi così all'interno dell'host (e potenzialmente anche in altri host).

Un **trojan** è un tipo di software maligno che finge di essere innocuo mascherandosi da software benigno per rimanere in background ed eseguire i loro compiti maligni.

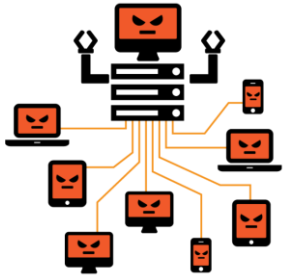
Gli **spyware** tracciano l'utente senza il suo consenso e riportano all'attaccante le attività dell'utente, i siti web visitati, la posizione geografica e così via.

Un **worm** è un programma che si duplica e si diffonde rapidamente attraverso le reti, intasandole. Una volta individuato, è spesso facile applicare una patch e impedire che si diffonda ulteriormente.

L'**adware** mostra automaticamente pubblicità all'utente.

Lo **scareware** presenta un'interfaccia che informa gli utenti che sono stati infettati da un malware. Dopo che la vittima acquista e installa il software, lo scareware viene rimosso dal software acquistato.

Tipologie di malware parte 2



Un **Bot** è un malware che esegue azioni senza il consenso dell'utente come parte di un esercito di "zombie". Tutti i bot ricevono le loro istruzioni da un server di comando e controllo (C&C), e il gruppo di host infetti viene definito botnet. Le botnet sono principalmente utilizzate per gli attacchi DDoS.

Il **ransomware** cripta i file dell'utente (documenti e foto) con una forte forma di crittografia e richiede un pagamento in cambio della chiave di decrittazione. Di solito, questo tipo di comportamento non impedisce di usare il computer, ma rende effettivamente inaccessibili tutte le informazioni. A peggiorare le cose, la maggior parte dei ransomware richiede il pagamento entro un breve periodo di tempo (di solito pochi giorni). I moderni ransomware richiedono il pagamento in Bitcoin o altre criptovalute, perché permettono all'attaccante di rimanere relativamente anonimo.

I **cryptominer** usano tutta la potenza di calcolo disponibile della vittima per minare criptovalute per l'attaccante. Le vittime sopportano il deterioramento delle prestazioni, mentre l'aggressore ottiene tutti i profitti. Si tratta di un attacco abbastanza nuovo che è in aumento dal 2017.

Malware moderni

- Eludono facilmente antivirus datati basati su signature e firewall di vecchia generazione.
- Sono in grado di mutare per colpire o evitare certi target.
- 0 Gli zero-day sono malware visti per la prima volta.

Esempio – Ramsonware – La regione Lazio

Regione Lazio ha confermato che l'attacco è partito da un computer di un dipendente LazioCrea in smart working (senza dare dettagli sulle cause principali, però).

Al momento la versione ufficiale è che il dipendente sia stato contagiato da malware (forse per aver cliccato su un link in mail phishing).

Fatto sta che ci sono stati **errori di gestione privilegi o di password** in Regione se è stato possibile per gli attaccanti passare dal computer del dipendente ad account con privilegi di admin con cui criptare il tutto.

Grazie a **vulnerabilità di sistema** è possibile fare elevation di privilegi, come avvenuto con bug print server Windows; ma su virtual machine sembra più difficile.

InnovaPuglia S.p.A.

CSIRT PUGLIA