

I malware dalla A alla Z

Obiettivo	Approfondire la conoscenza dei malware
Strumenti	<ul style="list-style-type: none">• Software di videoscrittura
Attività	<ul style="list-style-type: none">• Formatta il testo seguente, utilizzando gli strumenti di videoscrittura conosciuti e che ritieni adatti, es. elenchi, tabelle, formattazione del carattere e del paragrafo, bordi, sfondi ecc.• Inserisci le immagini per le diverse slide, che sono disponibili nel DVD nella cartella Immagini.• Al termine dell'attività, salva il file in formato .pdf.• Carica il file in Google Drive.• Condividi il file con il tuo insegnante.

1. I MALWARE, dalla A alla Z

2. Adware: È un programma che mostra messaggi pubblicitari sul monitor del computer. Non si tratta di un'azione dannosa in quanto tali azioni possono finanziare programmi utili che vengono distribuiti gratuitamente (es. il browser Opera). Questi virus possono rallentare il PC, così come la navigazione, a causa dell'intasamento dovuto ai messaggi pubblicitari.
3. Brute Force: È un attacco in cui gli hacker provano un gran numero di combinazioni di dati o password per riuscire ad accedere a un sistema o file non autorizzato.
4. Backdoor Trojan: È un programma che consente di prendere il controllo del computer di un utente senza il suo consenso, tramite una connessione Internet.
5. Boot sector malware: Questo virus si diffonde modificando il programma di avvio del computer (Boot). All'accensione del PC, l'hardware cerca il boot sector, o settore di avvio, sul disco rigido (ma può trattarsi anche di un floppy o CD) ed esegue il programma di avvio del sistema. Il boot sector malware sostituisce il boot sector con danni evidenti.
6. Botnet: Serie di computer infettati da un virus che sono controllati in remoto via Internet da un hacker. Da quel momento il PC diventa uno "zombie" sottostando ai voleri dell'hacker, anche se il proprietario del PC non ne è a conoscenza. L'hacker può vendere l'accesso al PC per scopi malevoli.
7. Browser hijacker: Questo virus modifica la pagina iniziale e le pagine di ricerca del programma di navigazione, il browser appunto (Internet Explorer, Mozilla Firefox, Chrome ecc.). Per l'utente è impossibile modificare la pagina iniziale e il "dirottamento" del browser viene fatto per incrementare gli introiti pubblicitari. Sono software difficili da eliminare.

8. Buffer overflow: Un buffer overflow si verifica quando un programma memorizza una quantità eccessiva di dati, sovrascrivendo altre parti della memoria del PC e provocando errori o blocchi del sistema. Il virus invia una quantità eccessiva di dati e il PC genera errori di sistema.

9. Catena di Sant'Antonio: Si tratta di email che esortano a inoltrare urgentemente copie del messaggio ad altri utenti. Scopo di questo virus non è danneggiare il PC ma causare spreco di tempo e diffusione di informazioni spesso non attendibili; generano inoltre traffico inutile nella rete.

10. Centro di comando e controllo: È il computer che comanda e controlla una botnet. Dal centro di comando e controllo, gli hacker possono invitare più computer a eseguire le attività da loro desiderate.

11. Cookie: Si tratta di file che permettono a un sito web di registrare le visite e memorizzare i dati dell'utente e di tenere traccia delle visite. Sono piccoli file di testo che non danneggiano il computer, tuttavia possono violare la privacy, poiché spesso si autoinstallano senza il consenso dell'utente.

12. Denial of Service: Un attacco DoS (*Denial of Service*, letteralmente negazione del servizio) impedisce agli utenti di accedere a un computer o sito Internet.

13. Documento malware: Questo virus sfrutta lo script incorporato o il contenuto delle macro nei file documento, in particolare quelli di Microsoft Office, ed è molto diffuso.

14. Download drive-by: Questo virus infetta un PC che visita un sito malevolo e spesso l'utente non se ne accorge, subito... Per proteggersi da questi virus è necessario utilizzare filtri di protezione per il Web e un efficace software antivirus, sempre aggiornato.

15. Email malware: Si tratta di malware distribuito tramite posta elettronica. La trasmissione di virus tramite messaggi o allegati ai messaggi è ormai stata sostituita dall'invio di email contenenti link a siti malware. L'educazione dell'utente contribuisce ad accrescere la consapevolezza delle truffe via email e la pericolosità di allegati dall'aspetto innocuo inviati da sconosciuti.

16. Exploit: Un exploit sfrutta una vulnerabilità o insicurezza di un computer per poi accedervi e infettarlo.

17. Furto di dati: Il furto di dati è un'azione volontaria, a differenza della perdita accidentale. Può avvenire a opera di persone che agiscono all'interno di un'organizzazione o di criminali esterni. Il malware accede al PC e ruba i dati. Questi ultimi possono essere sottratti anche rubando i dispositivi che li contengono (USB o altre memorie di massa).

18. Hoax: Gli Hoax sono falsi allarmi su virus inesistenti. Solitamente sono email che segnalano la presenza di un virus altamente distruttivo e che non può essere rilevato o fingono di scrivere per conto di grandi produttori di software ecc. La diffusione di tali allarmi provoca sovraccarico nei server di posta. Poiché non sono malware spetta solo all'utente essere accorto e non crederci.

19. Mobile phone malware: Questo malware è destinato all'esecuzione su dispositivi mobili, quali smartphone o PDA.

20. Rootkit: È un software in grado di nascondere i programmi o i processi in esecuzione sul computer. Viene solitamente utilizzato per sottrarre dati o eseguire operazioni illecite.

21. Spam: Lo spam è la posta commerciale non richiesta, l'equivalente elettronico dei volantini e dei cataloghi che intasano la cassetta della posta. Gli spammer (coloro che creano gli spam) "truccano" le proprie email affinché il software antispam non le intercetti e le elimini. Lo spam fa perdere tempo al personale di un'azienda che deve eliminarlo e inoltre intasa le mail-box.

22. Spear phishing: Si tratta di un tipo di phishing mirato, che usa email apparentemente autentiche ma in realtà false. Il phishing è una frode che induce un utente a comunicare proprie informazioni personali e credenziali sensibili (codice fiscale, password per la banca online, numero di conto corrente bancario o postale, numero della carta di credito).

23. Zombie: È un computer infettato e controllato in remoto, tramite la rete, da un hacker.