ICDL/ECDL
FULL STANDARD
IT – SECURITY
2 – MALWARE

A Cura di Enzo Exposyto

ICDL/ECDL

FULL STANDARD

IT – SECURITY

2 – MALWARE

2.1 – Tipi e Metodi

IT – SECURITY

Syllabus

Versione 2.0

IT – SECURITY

SEZIONE 1 - CONCETTI di SICUREZZA

- 1.1 Minacce ai Dati
- 1.2 Valore delle Informazioni
- 1.3 Sicurezza Personale
- 1.4 Sicurezza dei File

IT – SECURITY

SEZIONE 2 - MALWARE

- 2.1 Tipi e Metodi
- 2.2 Protezione dal MalWare
- 2.3 Risoluzione e Rimozione del MalWare

IT – SECURITY

SEZIONE 3 - SICUREZZA IN RETE

- 3.1 Reti e Connessioni

- 3.2 Sicurezza su Reti Wireless

IT – SECURITY

SEZIONE 4 - CONTROLLO di ACCESSO

- 4.1 Metodi per Impedire Accessi Non Autorizzati

- 4.2 Gestione delle Password

IT – SECURITY

SEZIONE 5 - USO SICURO DEL WEB

- 5.1 Impostazioni del Browser

- 5.2 Navigazione Sicura in Rete

IT – SECURITY

SEZIONE 6 - COMUNICAZIONI

- 6.1 Posta Elettronica
- 6.2 Reti Sociali
- 6.3 VoIP e Messaggistica Istantanea
- 6.4 Dispositivi Mobili

IT – SECURITY

SEZIONE 7 - GESTIONE SICURA dei DATI

- 7.1 Messa in Sicurezza e Salvataggio dei Dati

- 7.2 Cancellazione e Distruzione Sicura dei Dati

IT – SECURITY

Syllabus Versione 2.0

SEZIONE 2

MalWare

MalWare

2.1 Tipi e Metodi

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “MalWare”. Riconoscere diversi modi con cui il MalWare si può nascondere nei computer, quali: trojan, rootkit e backdoor.

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

- **Il termine ‘MALWARE’ deriva dall'unione di**
  - **‘MALICIOUS’ (maligno, malvagio, malizioso, cattivo, dannoso, …)**
    e
  - **‘SOFTWARE’**
- **Esso è usato per indicare i PROGRAMMI DANNOSI per COMPUTER e DISPOSITIVI MOBILI.**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

- **Tali programmi sono INSTALLATI SENZA il CONSENSO dell'UTENTE.**
- **Essi possono causare SPIACEVOLI CONSEGUENZE, quali:**
  - **il BLOCCO delle PRESTAZIONI del DEVICE AGGREDITO**
  - **il ‘MINING’ del SISTEMA per ottenere DATI PERSONALI:**
    (DATA MINING = ESTRAZIONE di DATI)
  - **la CANCELLAZIONE di DATI**
  - **…**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

- **Il ‘MalWare’ può, perfino, avere un IMPATTO NEGATIVO sulle OPERAZIONI dell'HARDWARE del DISPOSITIVO VITTIMA.**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

- **Infatti, i creatori di malware -probabilmente- non svolgono test accurati prima di lanciare il loro ultimo virus o programma trojan.**
- **Talvolta il MALWARE può essere semplicemente INCOMPATIBILE con il SOFTWARE e l’HARDWARE del sistema informatico vittima.**
- **Ciò può generare un GUASTO del COMPUTER o del SERVER,**
  oppure PROVOCARE un DRASTICO AUMENTO del TRAFFICO di SPAM,
  fino a PARALIZZARE totalmente il FUNZIONAMENTO di una RETE.

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

- Questo avviene piuttosto di frequente.
- Esistono molti esempi ben documentati di gravi problemi di funzionamento causati dal MalWare e dai relativi bug

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

- **Nel 1988, negli Stati Uniti, il WORM ‘MORRIS’ provocò una vera e propria epidemia su ARPANET, l’antenato di Internet.**
- **Furono infettati più di 6.000 computer, circa il 10% del numero complessivo di computer allora presenti su tale rete.**
- **In pratica, un bug nel codice nocivo consentiva al Worm di autoreplicarsi e diffondersi in Arpanet, causando il completo assorbimento delle risorse disponibili e la conseguente paralisi del sistema.**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

- **Il WORM SLAMMER, gennaio 2003, provocò un BlackOut di Internet**
  - negli USA
  - nella Corea del Sud
  - in Australia
  - in Nuova Zelanda
  con una specie di ‘rotazione geografica’.
- **Con la diffusione incontrollata del Worm, il TRAFFICO di RETE AUMENTÒ del 25%, causando anche gravi problemi all’operatività della stessa Bank of America.**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

- **Successivamente, enormi danni sono stati causati da**
  - **Lovesan (Blaster, MSBlast)**
  - **Mydoom**
  - **Sasser**
  - **altri Worm in grado di scatenare epidemie informatiche globali**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

- **La rapida diffusione di questi temibili software nocivi ha, anche, provocato**
  - **la cancellazione di numerosi voli da parte di alcune compagnie aeree**
  - **la temporanea sospensione dell’attività di alcune banche.**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

GUASTI HARDWARE

- **Raramente i virus informatici sono in grado di danneggiare i componenti hardware, visto che i moderni computer sono relativamente ben protetti nei confronti di eventuali danni provocati da errori del software.**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

GUASTI HARDWARE - VIRUS CIH (CHERNOBYL)

- **Tuttavia, nel 1999, il VIRUS CIH, noto anche come CHERNOBYL, colpì diverse centinaia di migliaia di computer, cancellando i dati nel BIOS FLASH di ogni computer.**
- **Ciò rese impossibile l’avvio delle macchine infette.**
- **Gli utenti vittima furono costretti a rivolgersi a centri di assistenza, per riscrivere il BIOS FLASH e ripristinare il funzionamento del device**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

GUASTI HARDWARE - VIRUS CIH (CHERNOBYL)

- **In molti laptop, il BIOS FLASH era saldato direttamente alla scheda madre, assieme al drive, alla scheda video e ad altro hardware.**
- **Nella maggior parte dei casi, quindi, il costo della riparazione superava, in pratica, quello relativo all’acquisto di un nuovo laptop.**
- **Tali computer danneggiati dalla ‘bomba’ CIH, di conseguenza, furono semplicemente gettati via.**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

wikipedia.org

GUASTI HARDWARE - VIRUS CIH (CHERNOBYL) - BIOS - BOOT

- **Il Basic Input-Output System (acronimo BIOS), in Informatica, è il primo software che viene eseguito dopo l'accensione, ed è, quindi, decisivo nella fase di avvio (fase di boot) del device.**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

wikipedia.org

GUASTI HARDWARE - VIRUS CIH (CHERNOBYL) - BIOS - BOOT

- **Il termine boot, bootstrap, booting, in Informatica, indica l'insieme dei processi che vengono eseguiti da un computer durante la fase di avvio, in particolare dall'accensione fino al completo caricamento del kernel (‘cuore’) del sistema operativo in memoria primaria (RAM) dalla memoria secondaria (esempio: Hard Disk)**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

wikipedia.org

GUASTI HARDWARE - VIRUS CIH (CHERNOBYL) - BIOS

- **Più precisamente, il BIOS è costituito da un insieme di routine software, generalmente scritte su**
  - memoria ROM
  - memoria FLASH
  - altra memoria non volatile
  che forniscono una serie di funzioni di base per accedere all'hardware del computer e alle sue periferiche

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

wikipedia.org

GUASTI HARDWARE - VIRUS CIH (CHERNOBYL) - BIOS - FIRMWARE

- **Tale insieme di routine software su memoria non volatile è definito FIRMWARE (unione di "firm" e "software", cioè componente logico permanente) che è, quindi, una sequenza di istruzioni integrate direttamente in un componente elettronico programmato (tipico esempio: BIOS su ROM).**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

wikipedia.org

GUASTI HARDWARE - VIRUS CIH (CHERNOBYL) - BIOS - POST

- **L'accesso al menu del BIOS avviene premendo un tasto o una combinazione di tasti, che dipende dai produttori e dai modelli, durante la fase di POST**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

wikipedia.org

GUASTI HARDWARE - VIRUS CIH (CHERNOBYL) - BIOS - POST

- **Il POST (Power-On Self-Test), in Informatica, indica la fase di AUTO DIAGNOSI di personal computer, di router, di stampanti, et cetera, avviata automaticamente dal BIOS, all'accensione, per testare il corretto funzionamento dell'hardware prima dell'avvio delle successive fasi del processo di bootstrap.**
- **Oltre al funzionamento della scheda madre, il POST può verificare anche il funzionamento delle periferiche più comuni, come mouse, tastiera, scheda video, …**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

wikipedia.org

GUASTI HARDWARE - VIRUS CIH (CHERNOBYL) - BIOS

Di seguito, alcuni produttori di computer, con i tasti da premere per accedere al menu del BIOS

- **Acer: Canc o F2**
- **Asus: F2**
- **HP: F1 o F2 o F10 o Esc o Canc**
- **Lenovo: F1 o F2**
- **Samsung: F2**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

wikipedia.org

GUASTI HARDWARE - VIRUS CIH (CHERNOBYL) - BIOS

- **Dal 2010, è in corso la sostituzione del BIOS con altra tecnologia**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

GUASTI HARDWARE

- **Si incontrano, talvolta, programmi Trojan in grado di eseguire azioni ripetitive: ad esempio aprire e chiudere periodicamente il vassoio CD-DVD.**
- **Anche se l’hardware attuale è, generalmente, molto affidabile,**

software nocivi del genere potrebbero causare, teoricamente,
dei danni a quei computer che vengono tenuti accesi
in maniera pressoché ininterrotta.

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

- **Poiché gli hacker sviluppano strategie sempre più sofisticate per infiltrarsi nei sistemi dell'utenza,**
  il mercato dei malware ha visto una crescita considerevole.

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

Vediamo, ora, alcuni tra i più comuni diffusi tipi di malware

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

VIRUS INFORMATICI

- **I virus informatici hanno questo nome poiché possiedono la capacità di infettare più file in un computer.**
- **Se i file infetti sono installati in altri devices -essendo stati, ad esempio, inviati via e-mail o trasportati dagli utenti su supporti fisici, quali chiavetta USB, memory card, floppy disk, et cetera- i virus si diffondono anche in questi altri computer.**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

VIRUS INFORMATICI

- **Secondo il NIST statunitense -Istituto Nazionale di Standard e Tecnologie- il primo virus informatico, detto ‘Brain’, venne sviluppato nel 1986.**
- **Stanchi dei clienti che creavano copie illegali di alcuni programmi nel loro negozio, due fratelli affermarono di aver progettato un virus per infettare il settore di avvio dei floppy disk dei ladri di software**
- **Quando i clienti caricavano sui loro dischetti copie illegali dei file nel negozio, con esse installavano il virus progettato che, così, si propagava.**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

WORM

- **A differenza dei virus, i Worm non hanno bisogno dell'intervento umano per diffondersi.**
- **Essi infettano una sola volta e poi utilizzano le reti del computer per entrare in altri devices, senza l’intervento degli utenti.**
- **Sfruttando, ad esempio, vulnerabilità delle reti o 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.**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

WORM

- **La maggior parte degli ATTUALI WORM contiene anche ‘payload’ (*) dannosi, progettati per rubare o cancellare file.**
- **(*) ‘Carico Utile’ … In sicurezza informatica, un payload è una routine presente in un Virus/Worm informatico che ne estende le funzioni oltre l'infezione del sistema.**
  Con altre parole, la routine contiene il codice per far eseguire al Virus/Worm le azioni successive all’infezione del sistema.

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

pandasecurity.com

WORM

- **I Worm sono una SOTTOCLASSE di VIRUS e ne condividono alcune caratteristiche.**
- **Essi sono programmi che creano copie di se stessi in diversi punti di un computer.**
- **L'obiettivo di questo tipo di MalWare è - *solitamente* - quello di SATURARE COMPUTER E RETI, IMPEDENDO CHE VENGANO UTILIZZATI.**
- **A differenza dei Virus, i Worm non infettano i file.**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

pandasecurity.com

WORM

- **L'obiettivo principale dei creatori di Worm è quello di diffondere e infettare quanti più computer possibile.**
- **I Worm creano -sui computer infetti- copie di se stessi, che poi si diffondono su altri devices, tramite canali quali e-mail, programmi Peer To Peer (P2P), et cetera.**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

pandasecurity.com

WORM

- **Anche i progettisti di Worm utilizzano, spesso, tecniche di INGEGNERIA SOCIALE**
- **I creatori di MalWare usano nomi attraenti per camuffare i loro file dannosi: la maggior parte di questi nomi si riferisce a sesso, personaggi famosi, software piratato.**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

ADWARE

- **L’AdWare è una delle ‘seccature’ più comuni in Internet.**
- **I programmi AdWare consegnano automaticamente pubblicità agli utenti.**
- **Tra i tipi conosciuti di AdWare vi sono:**
  - pubblicità in finestre pop-up su pagine Web
  - pubblicità in programmi ormai indispensabili (email, ad esempio)
  - pubblicità in altri software ‘gratuiti’ (calcolatrici, et cetera)

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

ADWARE

- **Accanto ai programmi di AdWare ‘tradizionali’,**
  vi sono varianti che usano
  - gli strumenti di localizzazione
  - la cronologia del browser
  per
  - carpire informazioni riguardanti la posizione dell'utente
  - presentare pubblicità mirate sullo schermo della vittima

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

ADWARE

- **Inoltre, come scrive BetaNews (sito web di notizie e analisi tecnologiche), è stata individuata una nuova forma di AdWare capace di METTERE FUORI USO il SOFTWARE ANTIVIRUS di un UTENTE**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

ADWARE

- **Poiché l’AdWare viene installato con la consapevolezza e il consenso dell'utente, QUESTI PROGRAMMI NON POSSONO ESSERE DEFINITI MALWARE in SENSO STRETTO.**
- **Tuttavia, essi -generalmente- sono identificati come ‘PROGRAMMI POTENZIALMENTE INDESIDERATI’**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

SPYWARE

- **Lo SpyWare è una spia di nome e di fatto: spia le azioni dell'utente che usa un computer.**
- **Esso raccoglie dati, quali**
  - i tasti premuti dall'utente
  - le abitudini di navigazione
  - le informazioni di accesso
- **I dati raccolti sono poi inviati - generalmente - a cybercriminali.**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

SPYWARE

- **Alcuni tipi di SpyWare possono anche**
  - modificare impostazioni di sicurezza specifiche sul computer dell'utente
  - interferire con le connessioni di rete

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

SPYWARE

- **Secondo TechEye.net (WP: sito web britannico di notizie e opinioni tecnologiche), tipi emergenti di SpyWare potrebbero permettere alle società di TRACCIARE il COMPORTAMENTO degli UTENTI ATTRAVERSO PIÙ DISPOSITIVI, SENZA il LORO CONSENSO.**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

RANSOMWARE

- **Il RansomWare infetta il computer**
- **Successivamente cripta i dati sensibili, quali documenti personali, foto, et cetera**
- **Chiede un riscatto per il loro rilascio**
- **Se la vittima rifiuta di pagare i dati vengono eliminati**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

RANSOMWARE

- **Alcuni tipi di ransomware bloccano completamente l'accesso al computer**
- **Potrebbero dichiarare**
  - di essere forze dell'ordine
  - che l'utente sia stato colto in un'azione irregolare

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

RANSOMWARE

- **Nel giugno del 2015, Internet Crime Complaint Center (IC3) dell'FBI ha ricevuto lamentele da parte di utenti che hanno denunciato una perdita di 18 milioni di dollari a causa di una comune minaccia RansomWare chiamata CryptoWall**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

wikipedia

RANSOMWARE

- **Un RansomWare è un tipo di MalWare che limita l'accesso del dispositivo che infetta, chiedendo un riscatto (*ransom*, in inglese) da pagare per rimuovere la limitazione**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

wikipedia

RANSOMWARE

- **Ad esempio,**
  - alcune forme di RansomWare
  bloccano il sistema e intimano all'utente di pagare per sbloccarlo,
  - altre, invece,
  cifrano i file dell'utente chiedendo di pagare per riportare i file cifrati in chiaro

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

wikipedia

RANSOMWARE

- **Inizialmente diffusi in Russia, gli attacchi con RansomWare sono ora perpetrati in tutto il mondo.**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

wikipedia

RANSOMWARE

- **Nel giugno 2013, la casa software McAfee, specializzata in software di sicurezza, ha rilasciato dei dati che mostravano che, nei primi tre mesi del 2013,**
  erano stati registrati 250 000 diversi tipi di RansomWare,
  più del doppio del numero ottenuto nei primi tre mesi dell'anno precedente

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

wikipedia

RANSOMWARE - CRYPTOLOCKER

- **CryptoLocker, un ransomware apparso alla fine del 2013, ha reso ai cybercriminali circa 3 milioni di dollari prima di essere reso innocuo dalle autorità**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

wikipedia

RANSOMWARE - CRYPTOLOCKER

- **CryptoLocker è stato perfezionato nel maggio 2017**
- **Vi è la versione CryptoLocker 2019**
- **Questa forma di RansomWare**
  - infetta i sistemi Windows,
  - cripta i dati della vittima
  - chiede un pagamento per la decriptazione

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

wikipedia

RANSOMWARE - CRYPTOLOCKER

- **Symantec (ora Norton) stima che circa il 3% di chi è colpito dal MalWare decide di pagare**
- **Alcune vittime dicono di aver pagato il riscatto ma di non aver visto i propri file decriptati.**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

BOT

- **I Bot sono programmi progettati per portare a termine *automaticamente* determinate operazioni.**
- **Sono utili per molti scopi legittimi, ma sono utilizzati anche come malware.**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

BOT

- **Una volta all'interno del computer, i Bot possono ordinare al device di eseguire comandi specifici senza la consapevolezza e/o l'approvazione dell'utente.**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

BOT

- **Gli hacker/cracker possono, in alcuni casi, infettare più computer con lo stesso Bot per creare una ‘BotNet’ (abbreviazione di RoBot NetWork)**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

BOT

- **Una BotNet può essere usata per gestire da remoto computer infettati, col fine di**
  - spiare l’attività delle vittime
  - sottrarre dati sensibili (password, ad esempio)
  - distribuire spam *automaticamente*
  - diffondere RansomWare
  - lanciare devastanti attacchi DDoS in Internet (vedi Trojan, pagine successive)

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

ROOTKIT

- **Il RootKit permette un accesso remoto o il controllo di un computer da parte di terzi.**
- **Questi programmi sono utili ai professionisti ICT per risolvere problemi informatici a distanza.**
- **Tuttavia, possono diventare -facilmente- dannosi**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

ROOTKIT

- **Una volta installato sul computer, il RootKit permette ai criminali di prendere il completo controllo del device per**
  - rubare dati
  - installare altri pezzi di malware.

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

ROOTKIT

- **Il RootKit è progettato per muoversi in maniera discreta e agire nell'ombra.**
- **Per rintracciare e contrastare questo tipo di codice dannoso, occorre**
  - un monitoraggio manuale se vi sono ‘comportamenti’ insoliti
  - una regolare applicazione di patch al sistema operativo
  - software specifico per eliminare potenziali vie di trasmissione.

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

TROJAN HORSE

- **Chiamato comunemente ‘Trojan’, questo programma si nasconde sotto gli occhi dell’utenza, mascherandosi da file legittimo o da software.**
- **Una volta scaricato e installato, il Trojan apporta cambiamenti al computer e opera con attività dannose, senza la consapevolezza e/o il consenso dell’utente (vedi pagine successive)**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

BUG

- **I Bug, errori generati da un programmatore in pezzi di codice software, NON sono un tipo di malware.**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

BUG

- **Tuttavia, possono avere effetti dannosi sul computer.**
  Ad esempio, possono provocare:
  - la riduzione delle prestazioni del device
  - il ‘congelamento’ del computer
  - il suo arresto

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it

BUG

- **Più specificamente, i Bug nella sicurezza facilitano gli accessi dei criminali informatici che possono, semplicemente, eludere le difese del computer e infettarlo.**

MalWare
2.1 Tipi e Metodi
2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

Comprendere il termine ‘MalWare’

kaspersky.it
BUG

- **Un maggiore e/o migliore controllo sulla programmazione, mirato -in particolare- alla sicurezza, aiuta a eliminare o a ridurre il numero di Bug**
- **Infatti, risulta evidente che è difficile applicare patch software che mirino all’eliminazione di Bug disseminati**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

Il MalWare si può nascondere nei computer in diversi modi; esempi:

- Trojan
- RootKit
- BackDoor

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

MalWare - Trojan

da wikipedia

- **Un Trojan, Trojan Horse, Cavallo di Troia, in Informatica, è un tipo di MalWare**
- **Il Trojan nasconde il suo funzionamento all'interno di un altro programma, apparentemente utile e innocuo**
- **Il Trojan non si diffonde autonomamente; occorre un'azione dell'aggressore per far giungere il software maligno all’utente**
- **Ad esempio, la vittima è indotta a scaricare un programma utile contenente il Trojan**
- **L'utente, installando o eseguendo il programma, attiva anche il codice del Trojan nascosto**
- **Tale codice contiene istruzioni dannose che vengono eseguite all'insaputa dell'utilizzatore**
- **Il Trojan non replica se stesso.**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

MalWare - Trojan

da kaspersky.it

- **Il Cavallo di Troia o Trojan è un tipo di malware spesso mascherato da software legittimo.**
- **Il Trojan può essere impiegato da cyberladri e hacker che cercano di accedere ai sistemi informatici degli utenti.**
- **Le vittime, in genere, sono ingannati da qualche forma di social engineering nel caricamento e nell'esecuzione di Trojan sui loro sistemi.**
- **Una volta attivato, il Trojan può consentire ai cybercriminali di**
  - spiare l'utente,
  - rubare dati sensibili
  - ottenere l'accesso backdoor al sistema.

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

MalWare - Trojan

da kaspersky.it

Inoltre, il Trojan può effettuare:

- **eliminazione di dati**
- **blocco di dati**
- **modifica di dati**
- **copia di dati**
- **compromissione delle prestazioni di computer**
- **compromissione delle prestazioni di reti**

A differenza dei Virus informatici e dei Worm, i Trojan non sono in grado di autoreplicarsi.

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

MalWare - Trojan

da kaspersky.it

POSSIBILI CONSEGUENZE dell’ATTIVITÀ dei TROJAN

I Trojan possono essere classificati in base al tipo di azioni dannose che compiono sul computer vittima

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

MalWare - Trojan

da kaspersky.it

BackDoor

Un Trojan Backdoor fornisce al malintenzionato il controllo remoto del dispositivo vittima.
Consente al criminale informatico di fare ciò che desidera sul computer infetto; ad esempio:
- inviare, ricevere, eseguire, eliminare file
- visualizzare dati
- riavviare il computer.
Spesso i Trojan BackDoor vengono utilizzati per unire un gruppo di computer vittime
per formare una BotNet o una Rete Zombie che può essere sfruttata a scopi criminali.

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

MalWare - Trojan

https://it.wikipedia.org/wiki/Backdoor

BackDoor

BackDoor deriva dal termine inglese che sta per ‘porta di servizio’, ‘porta sul retro’.
In Informatica è un metodo, spesso segreto, per passare oltre (aggirare, bypassare)
la normale autenticazione in un
- prodotto
- sistema informatico
- crittosistema
- un algoritmo

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

MalWare - Trojan

https://it.wikipedia.org/wiki/Backdoor

BackDoor

Le backdoor sono spesso scritte in diversi linguaggi di programmazione
e hanno la funzione principale di superare le difese imposte da un sistema,
come può essere un FireWall,
al fine di accedere in remoto a un personal computer,
ottenendo per mezzo di un sistema di crittografia un'autenticazione
che permetta di prendere il completo o parziale possesso del computer vittima.

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

MalWare - Trojan

https://it.wikipedia.org/wiki/Backdoor

BackDoor

Una backdoor può celarsi segretamente all'interno di un
- ignaro programma di sistema
- software separato

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

MalWare - Trojan

https://it.wikipedia.org/wiki/Backdoor

BackDoor

Può anche essere un componente HardWare malevolo come:
- apparati di rete
- sistemi di sorveglianza
- alcuni dispositivi di infrastruttura di comunicazione
che possono avere celate al loro interno BackDoor maligne
Permettendo, così, l'intrusione di un eventuale criminale informatico (cracker).

MalWare

2.1 Tipi e Metodi

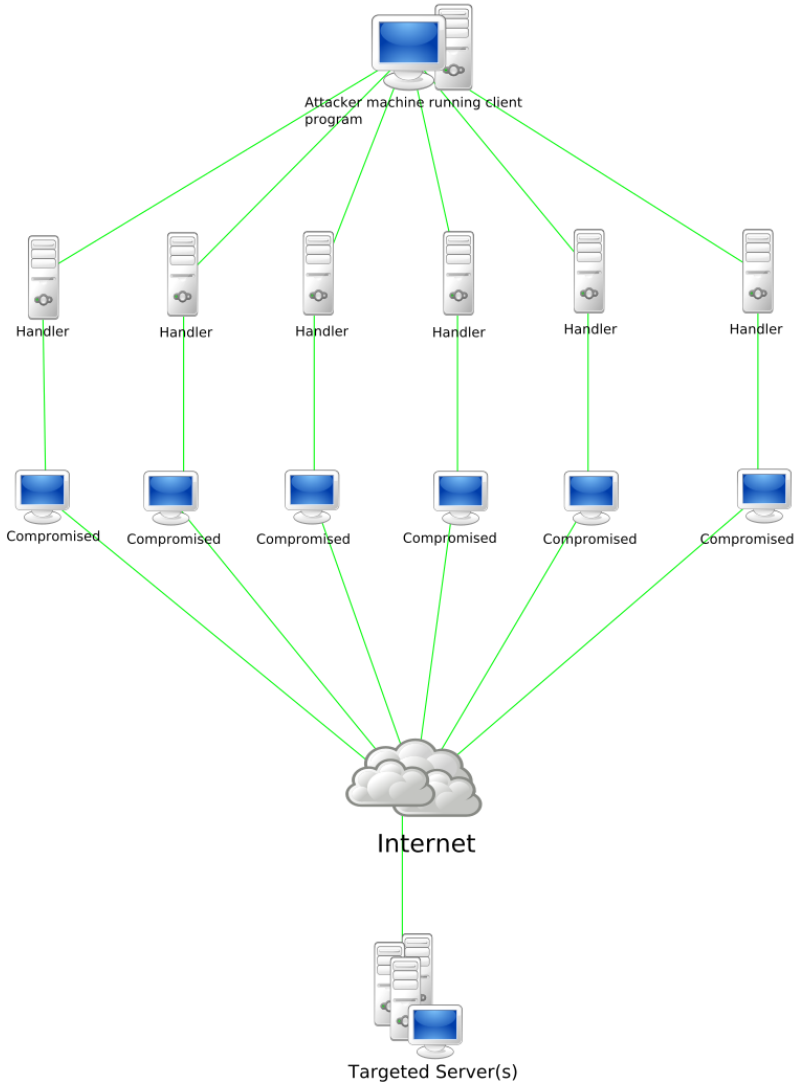
2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

MalWare - Trojan

https://it.wikipedia.org/wiki/Botnet

BotNet

Una BotNet è una rete di computer, solitamente PC, controllata da un BotMaster. Essa è composta da dispositivi infettati da malware specializzato. I computer infetti sono detti Bot o Zombie.



https://it.wikipedia.org/wiki/Botnet

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

MalWare - Trojan

https://it.wikipedia.org/wiki/Botnet

BotNet

- **I dispositivi connessi ad Internet, che hanno vulnerabilità nella loro struttura di sicurezza informatica, possono - talvolta - diventare parte di una BotNet.**
- **Se l'agente infettante è un Trojan, il BotMaster può controllare il sistema con accesso da remoto.**
- **I computer così infettati possono compiere attacchi,**
  chiamati Distributed Denial of Service (DDoS),
  contro altri sistemi
  e/o compiere altre operazioni illecite (inviare spam o virus, rubare dati personali, …)
  in alcuni casi persino su commissione di organizzazioni criminali.

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

MalWare - Trojan

https://it.wikipedia.org/wiki/Botnet

BotNet - Applicazioni Legali

- In generale, il termine BotNet viene usato per reti in grado di agire, con sincronia ed autonomia, per fini illegali.
- Tuttavia, esistono BotNet LEGALI usate per
  - calcoli distribuiti
  - studiare la diffusione del malware.

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

MalWare - Trojan

[da kaspersky.it]

Exploit

Gli exploit sono programmi che contengono dati o codice che sfruttano vulnerabilità presenti in un software in esecuzione sul computer.

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

MalWare - Trojan

da kaspersky.it

RootKit

I rootkit sono progettati per nascondere determinati oggetti o attività nel sistema.
Spesso il loro obiettivo principale è impedire il rilevamento di programmi nocivi,
per estendere il periodo di esecuzione dei programmi su un computer infetto.

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

MalWare - Trojan

https://it.wikipedia.org/wiki/Rootkit

RootKit

- **Il RootKit è un insieme di software, tipicamente malevoli, realizzati per ottenere l'accesso a un computer, o a una parte di esso, accesso che non sarebbe altrimenti possibile (ad esempio, da parte di un utente non autorizzato a effettuare l'autenticazione).**
- **Questi software, oltre a garantire tali accessi, si preoccupano di mascherare se stessi o altri programmi utili per raggiungere lo scopo.**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

MalWare - Trojan

https://it.wikipedia.org/wiki/Rootkit

RootKit

- **Il termine ROOT è il nome utente predefinito dell’Amministratore di sistema.**
- **Spesso vengono usati come sinonimi**
  - **Amministratore**
  - **SuperUtente**
  - **SuperUser**
- **ROOT significa RADICE, in quanto l’Amministratore è l'unico a poter modificare i file presenti nella DIRECTORY '/', detta ROOT.**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

MalWare - Trojan

https://it.wikipedia.org/wiki/Rootkit

RootKit

Il termine inglese ‘RootKit’ deriva, quindi, dalla concatenazione di due termini:

- **‘Root’, che indica -tradizionalmente- l'utente con i maggiori permessi in alcuni Sistemi Operativi**
- **‘Kit’, che si riferisce al software che riesce ad ‘ottenere’ tali permessi**

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

MalWare - Trojan

da kaspersky.it

Trojan Banker

I programmi Trojan Banker sono progettati per rubare i dati degli account
sui sistemi di banking online, di pagamento elettronico e delle carte di credito o di debito.

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

MalWare - Trojan

da kaspersky.it

Trojan DDoS

Questi programmi sferrano attacchi DoS (Denial of Service) contro un indirizzo Web ben preciso.
Inviando numerose richieste da svariati computer infetti,
l'attacco può sopraffare l'indirizzo web preso di mira,
generando un rifiuto del servizio.

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

MalWare - Trojan

da kaspersky.it

Trojan Downloader

Il trojan downloader può scaricare e installare nuove versioni di programmi nocivi sul computer, compresi trojan e adware.

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

MalWare - Trojan

da kaspersky.it

Trojan Dropper

Questi programmi vengono utilizzati dagli hacker per installare trojan e/o virus, oppure per impedire il rilevamento dei programmi nocivi.
Non tutti i programmi antivirus sono in grado di analizzare tutti i componenti di questo tipo di trojan.

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

MalWare - Trojan

da kaspersky.it

Trojan FakeAV

I programmi trojan Fake AV simulano l'attività del software antivirus.
Sono progettati per estorcere denaro agli utenti, in cambio del rilevamento e dell'eliminazione delle minacce,
anche se le minacce che notificano in realtà non esistono.

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

MalWare - Trojan

da kaspersky.it

Trojan GameThief

Questo tipo di programma ruba informazioni sull'account utente dai giocatori online.

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

MalWare - Trojan

da kaspersky.it

Trojan IM

I programmi trojan IM rubano le credenziali di accesso e le password dei programmi di messaggistica immediata, come ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype e molti altri.

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

MalWare - Trojan

da kaspersky.it

Trojan Ransom

Questo tipo di trojan può modificare i dati sul computer per danneggiarne il funzionamento e per impedire all'utente di utilizzare dati specifici.
Il criminale ripristinerà le prestazioni del computer oppure sbloccherà i dati solo dopo che l'utente avrà pagato il riscatto richiesto.

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

MalWare - Trojan

da kaspersky.it

Trojan SMS

Questi programmi possono costare soldi,
perché inviano messaggi di testo
dal dispositivo mobile a numeri telefonici a pagamento.

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

MalWare - Trojan

da kaspersky.it

Trojan Spy

I programmi Trojan Spy possono spiare tutto ciò che l'utente sta ricercando,
ad esempio tenendo traccia dei dati immessi con la tastiera,
catturando schermate del monitor
o procurandosi un elenco delle applicazioni in esecuzione.

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

MalWare - Trojan

da kaspersky.it

Trojan MailFinder

Questi programmi possono raccogliere gli indirizzi e-mail dai computer infetti.

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

MalWare - Trojan

da kaspersky.it

Altri tipi di Trojan:

- Trojan Arcbomb
- Trojan Clicker
- Trojan Notifier
- Trojan Proxy
- Trojan PSW

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

MalWare - Trojan

- **Nel 1985, uno dei primi trojan, ‘Gotcha’, creò molti danni**
  Il programma che lo conteneva era un visualizzatore grafico;
  il Trojan eliminava i dati presenti sul disco

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”.
Riconoscere diversi modi con cui il malware
si può nascondere nei computer,
quali: trojan, rootkit e backdoor.

MalWare - Trojan

- **Come riporta il www.dw.com, in un articolo datato 22 febbraio 2016,**
  «Il GOVERNO TEDESCO USA lo SPYWARE TROJAN per MONITORARE i CITTADINI
  Un portavoce del Ministero dell'Interno tedesco ha annunciato …
  che il governo ha approvato l'uso dei trojan per monitorare i cittadini sospetti.
  Le agenzie di intelligence in Germania possono ora utilizzare il malware
  per tracciare i computer delle persone sospettate.
  Il Trojan sarà in grado di tracciare le chat degli utenti e le conversazioni
  su smartphone e PC.»

MalWare

2.1 Tipi e Metodi

2.1.1 Comprendere il termine “malware”. Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

MalWare - Trojan

- **Altri Casi …**

Conoscere le minacce alla sicurezza provenienti da siti web, quali: virus, worm, cavalli di Troia, spyware.
Comprendere il termine “malware”.

Problemi derivanti da:

- **Scambio di File**
- **Collegamento in Rete con Altri Computer**
- **File Scaricati da Internet**
- **File Allegati di Posta Elettronica**
- **…**

Conoscere le minacce alla sicurezza provenienti da siti web, quali: virus, worm, cavalli di Troia, spyware.
Comprendere il termine "malware".

Malware (Malicious Software)

- Elenco0
- Elenco1
- Elenco2
- Elenco3
- Virus
- Worm
- Cavalli di Troia, Trojans
- BackDoor
- KeyLogger (HW o SW negativi e positivi)
- …

MalWare

2.1 Tipi e Metodi

2.1.2 Riconoscere i tipi di malware infettivo e comprendere come funzionano, ad esempio, virus e worm.

MalWare

2.1 Tipi e Metodi

2.1.3 Riconoscere i tipi di malware usati per furto di dati, profitto/estorsione e comprendere come operano, ad esempio:

- **adware** (proposta di pubblicità attraverso banner e popup),
- **ransomware** (blocco doloso di un programma con lo scopo di chiedere un riscatto per sbloccarlo),
- **spyware** (software che invia ad un server remoto i dati di navigazione),
- **botnet** (software capace di prendere il controllo di una rete di computer),
- **keylogger** (software capace di inviare ad un server remoto i caratteri digitati su una tastiera),
- **dialer** (software capace di cambiare la connessione del modem da un provider ad un altro).

MalWare

2.1 Tipi e Metodi

2.1.3 Riconoscere i tipi di malware usati per furto di dati, profitto/estorsione e comprendere come operano, ad esempio:

- phishing (…)

MalWare - Phishing

https://amalfinotizie.it/costiera-amalfitana-inviavano-sms-per-svuotare-i-conti-denunciate-tre-persone/

amalfinotizie

Territorio

Costiera Amalfitana, inviavano sms per svuotare i conti. Denunciate tre persone

Di **Redazione Web** - 17 Apr 2021

Il modus operandi ricorrente consiste nell'invio di sms o email di cosiddetto "phishing", costruiti ad arte per simulare una comunicazione ufficiale di un istituto di credito o di un fornitore di strumenti di pagamento elettronici relativi a problemi di autorizzazione: cliccandoci sopra viene richiesto l'inserimento delle proprie credenziali ed a quel punto il malvivente di turno è in grado di approfittare delle risorse finanziarie della vittima.

Nei tre casi oggetto di attenzione da parte dei Carabinieri sono stati effettuati acquisti online e bonifici per circa 2.000 euro ciascuno. L'attività dei militari, a seguito di denuncia, è consistita nel difficoltoso rintraccio degli "ip" di partenza dei "phishing", poi si è passati agli acquisti ed i bonifici effettuati, spesso a prestanome. Entrando a fondo negli accertamenti e grazie ad alcuni riscontri sul campo, la responsabilità è stata ricondotta a un 50enne napoletano, a un 35enne napoletano e a un 50enne residente a Torino.

I Carabinieri raccomandano sempre la **massima attenzione** nelle proprie transazioni telematiche, nonché alle mail ed sms truffa, invitando a contattare le Forze dell'Ordine in caso di dubbio o a far riferimento ai propri Istituti di Credito.

ICDL/ECDL
FULL STANDARD
IT – SECURITY
2 – MALWARE
2.2 – Protezione

MalWare

2.2 Protezione

MalWare

2.2 Protezione

2.2.1 Comprendere come funziona il software antivirus e quali limitazioni presenta.

MalWare

2.2 Protezione

2.2.2 Comprendere che il software antivirus dovrebbe essere installato su tutti i sistemi informatici.

MalWare

2.2 Protezione

2.2.3 Comprendere l'importanza di aggiornare regolarmente vari tipi di software, quali:

antivirus,

browser web,

plug-in,

applicazioni,

sistema operativo.

Comprendere che il software antivirus regolarmente aggiornato aiuta a proteggere il computer contro le minacce alla sicurezza.

- **>...**
- **>Antivirus gratuiti**

MalWare

2.2 Protezione

2.2.4 Eseguire scansioni di specifiche unità, cartelle, file usando un software antivirus.

Pianificare scansioni

usando un software antivirus.

MalWare

2.2 Protezione

2.2.5 Comprendere i rischi associati

all'uso di software obsoleto e non supportato, quali: maggiori minacce da parte del malware, incompatibilità.