Lezione 1

Introduzione al malware

Analisi del Malware

28 settembre 2023

Marco Cesati

Dipartimento di Ingegneria Civile e Ingegneria Informatica
Università degli Studi di Roma Tor Vergata

Di cosa parliamo in questa lezione?

Il malware:

1. Cosa è
2. Chi lo crea
3. Perché esiste
4. Come si diffonde
5. Come ci si difende

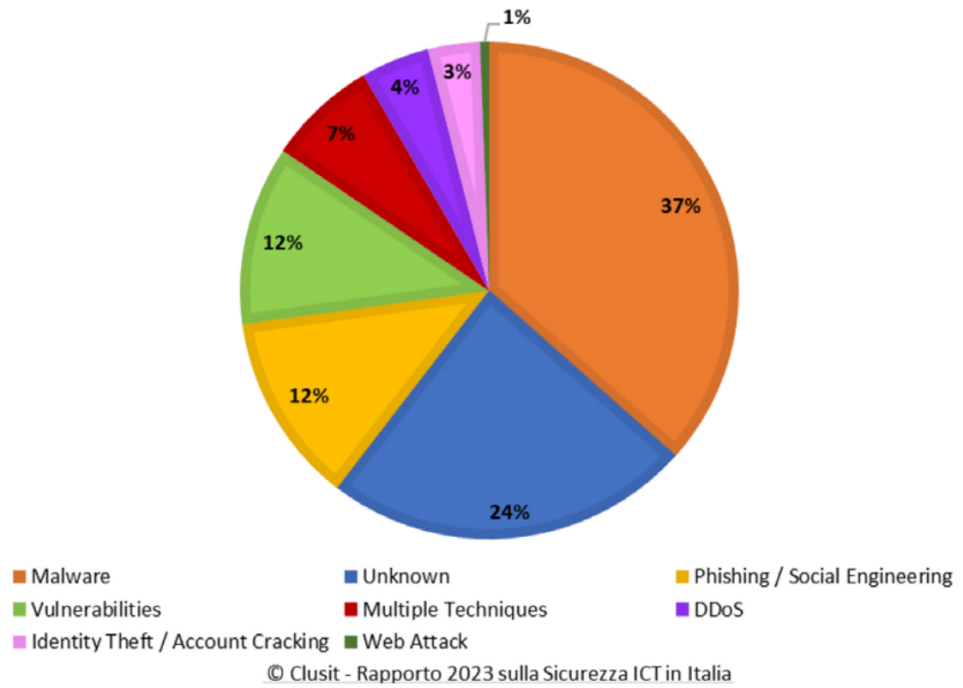
Cybersecurity

Difesa di infrastrutture critiche, calcolatori, dispositivi mobili, sistemi elettronici, reti e dati informatici da attacchi dannosi

- Sicurezza delle applicazioni
- Sicurezza di rete
- Sicurezza delle informazioni
- Sicurezza operativa
- Analisi e recupero degli incidenti
- Formazione degli utenti finali

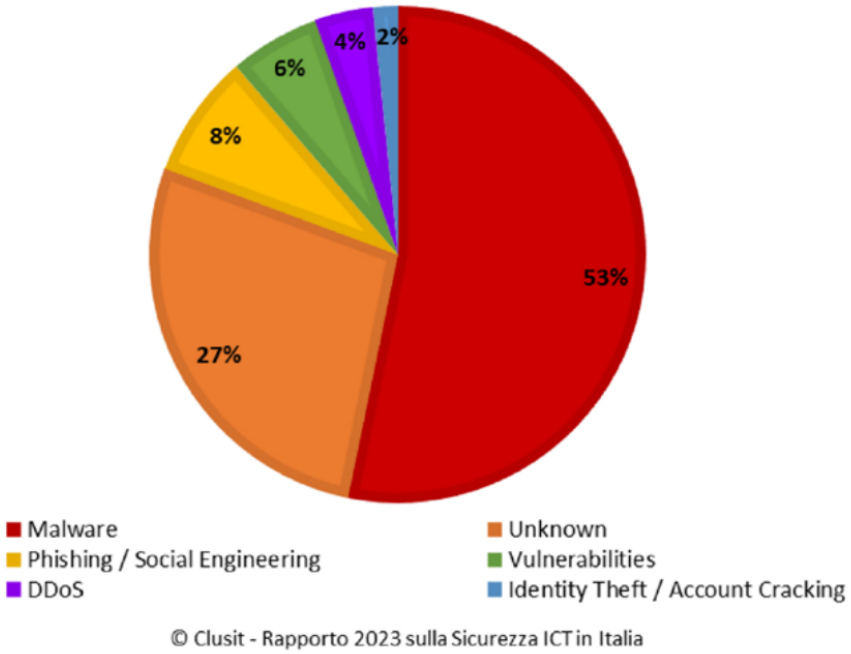
sicurezza che tocca aree diverse.

Incidenza dei metodi di attacco cyber nel mondo nel 2022



Malware è inteso come MALicious softWARE. Nel grafico molti tipi di attacchi non sono etichettati.

Incidenza dei metodi di attacco cyber in Italia nel 2022



© Clusit - Rapporto 2023 sulla Sicurezza ICT in Italia

Cosa è il malware

Il termine “**malware**” deriva dalla contrazione di “**mal**icious soft**ware**”

Un programma (o parte di un programma) che interferisce con il normale funzionamento di un calcolatore e/o permette l’esfiltrazione di dati dal calcolatore stesso

Ogni programma che viene eseguito all’insaputa, contro l’esplicita volontà, o contro gli interessi dell’utente del calcolatore può essere definito “malware”

Chi li scrive non è il ragazzo incappucciato che si vede nei film, bensì si tratta di vere e proprie organizzazioni criminali!

Perché esiste il malware?

Nella grande maggioranza dei casi:

Profitto illecito! Soldi facili!!

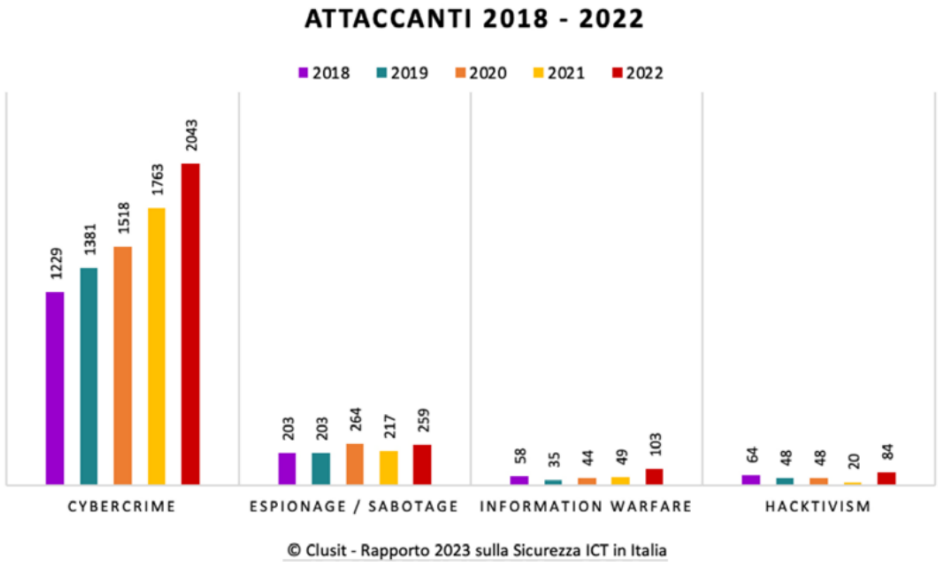
Oggi anche per sabotaggio, sopratutto in caso di elezioni.

Perché esiste il malware? (2)

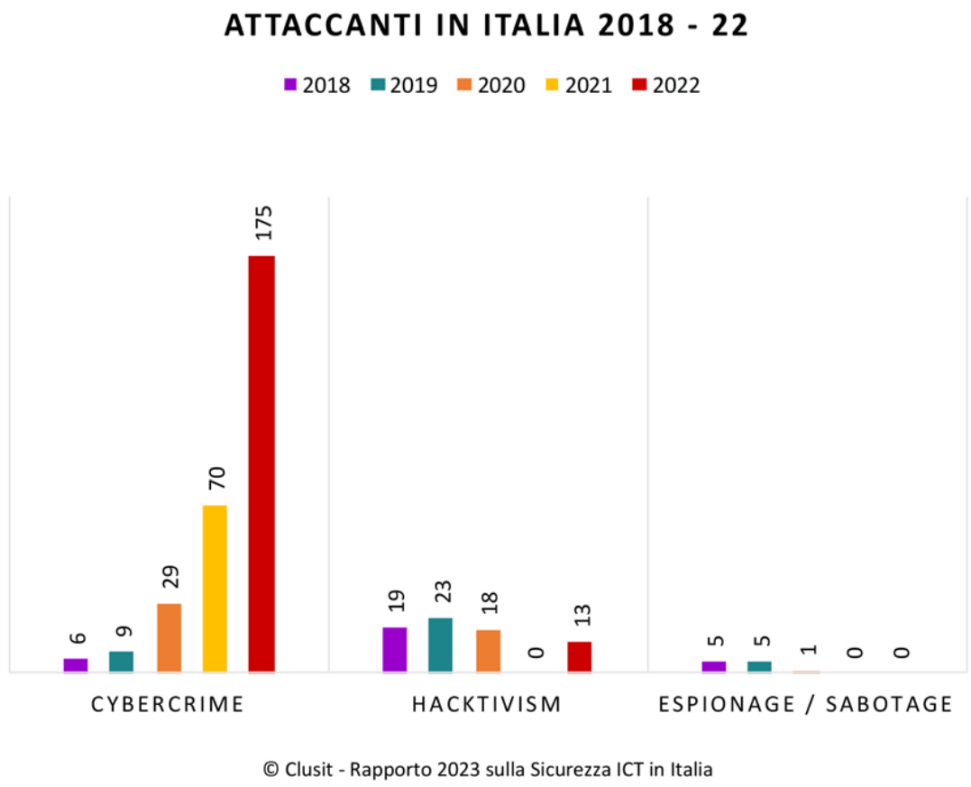
Sempre più spesso:

operazioni mirate di guerra, sabotaggio o spionaggio

Incidenza di vari tipi di attacchi cyber nel mondo



Incidenza di vari tipi di attacchi cyber in Italia



Chi scrive il malware?

Chi scrive il malware?

- In origine il malware era scritto da studenti e appassionati di informatica, soprattutto a scopo di studio o per divertimento
- Progressivamente lo sviluppatore del malware è divenuto una figura ambigua e/o malintenzionata
- Oggi esistono organizzazioni criminali internazionali che sviluppano, diffondono e/o rivendono malware a livello professionale
- Le nazioni più sviluppate possiedono laboratori e centri di formazione dedicati allo sviluppo di software “offensivo” (a tutti gli effetti pratici, malware)

Breve storia del malware — Le origini

1971 **Creeper** Primo worm sperimentale (ambito accademico)

1974 **Wabbit** Programma auto-replicante che bloccava il calcolatore

1982 **Elk Cloner** Scritto da un quindicenne, uno dei primi virus auto-replicanti che ha avuto grande diffusione

1986 **Brain Boot Sector Virus** Primo virus che attaccava MS-DOS

1986 **PC-Write Trojan** Primo esempio di malware che simulava un programma benigno

1988 **Morris Worm** Ha infettato una frazione significativa dei calcolatori connessi ad ARPANET, bloccandola in 24 ore. Robert Morris è stato il primo autore di malware condannato da un tribunale

1991 **Michelangelo Virus** Progettato per cancellare tutti i file il 6 marzo, ha creato grande clamore e panico, ma in realtà ha avuto diffusione limitata

1999 **Melissa Virus** Il primo virus ad ampia diffusione trasmesso tramite posta elettronica (spediva se stesso a 50 persone prese dalla rubrica di Outlook)

Breve storia del malware – La grande diffusione

2000 **ILOVEYOU Worm** Virus diffuso tramite posta elettronica a circa 50 milioni di calcolatori, con un danno stimato di quasi sei miliardi di dollari

2003 **SQL Slammer Worm** Uno dei più infestanti worm di tutti i tempi, ha infettato 75 000 calcolatori in 10 minuti. Ha causato un rallentamento totale del traffico di Internet

2004 **Cabir Virus** Primo virus che attaccava i telefoni cellulari

2005 **Koobface Virus** Uno dei primi virus che infettava i PC e poi si propagava tramite i social network Facebook, MySpace e Twitter

2008 **Conficker Worm** Malware molto sofisticato, è tra quelli che ha causato i maggiori danni a livello globale

Introduzione al malware
Marco Cesati

Schema della lezione
Cybersecurity
Cosa è il malware
Breve storia
Tipologie
Trasmissione
Diffusione
Nei sistemi industriali
Nei sistemi embedded
Strategia di difesa

Breve storia del malware – Malware come arma e come affare

2010 **Stuxnet Worm** Malware attribuito ad un gruppo di professionisti IT con lo scopo di attaccare alcuni dispositivi necessari per l'arricchimento dell'uranio in Iran

2011 **Zeus Trojan** La diffusione del codice sorgente di questo malware lo ha reso il più utilizzato programma per la creazione di botnet, con milioni di macchine infettate

2013 **Cryptolocker** Uno dei primi esempi di ransomware, con grande impatto sull'opinione pubblica

2014 **Backoff** Concepito per attaccare i sistemi POS (Point-of-Sale) per rubare i dati delle carte di credito

2016 **Cerber** Uno dei più diffusi, e remunerativi, ransomware sviluppati fino ad oggi

2017 **WannaCry** Un altro ransomware estremamente diffuso, sfruttante la vulnerabilità EternalBlue del protocollo Windows SMB scoperta, si dice, dalla National Security Agency

Quali sono i principali tipi di malware?

Quali sono i principali tipi di malware?

Adware e Malvertising Visualizzano pubblicità, corrompono le domande o le risposte sui motori di ricerca, intercettano i click sui banner pubblicitari

Spyware e Stealer Monitorano il traffico Web per catturare le preferenze dell'utente, esfiltrano informazioni critiche quali i dati degli account bancari, delle carte di credito e delle crittovalute

Loader Programmi semplici e di piccole dimensioni che consentono di scaricare dalla rete ed installare ogni altro tipo di malware

Backdoor e Remote Access Trojan (RAT) Consentono l'accesso remoto non autorizzato al calcolatore

Parlo di RAT se mi riferisco a tale attacco per un singolo calcolatore, o un gruppo ristretto, comunque "non generico".

Quali sono i principali tipi di malware? (2)

Bot Inseriscono il calcolatore in una grande rete (botnet) controllabile da un unico server centrale. Utilizzata per lanciare attacchi di tipo Distributed Denial of Service (DDoS) e per cryptomining (il comando è unico per tutti!)

Ransomware Cifrano alcuni file critici sul calcolatore per poi richiedere alla vittima il pagamento di un riscatto per decifrarli. Per il pagamento si utilizzano cryptovalute, minimizzando così le possibilità di rintracciare i responsabili soluzione: fare backup.

Clipper Attaccano le transizioni finanziarie basate su crittovalute: monitorano la clipboard di sistema e per qualunque pagamento sostituiscono l'indirizzo del ricevente il pagamento con un indirizzo appartenente all'autore del malware

Come si trasmette il malware?

It's perfectly OK to click on anything during my lunch break. I'm not in work mode.

Come si trasmette il malware?

Possiamo classificarli anche per come si trasmettono:
alcuni fanno leva sul comportamento errato degli utenti, altri no.

Virus Il malware si aggancia a file del calcolatore e si auto-replica infettando altri file in locale. Si diffonde tramite la condivisione dei file non è eseguibile, si aggancia a qualche cosa di eseguibile.

Worm Il malware è un programma a se stante che si auto-replica e si diffonde tramite rete (posta elettronica, WWW, condivisione P2P, social network, . . .)
è a se stante, si nasconde.

Trojan Il malware è un programma che si presenta come benigno e utile alla vittima si traveste da altro programma.

Come si trasmette il malware? (2)

Phishing Il malware non ha capacità di auto-replicazione e non viene trasmesso automaticamente tramite rete; al contrario, è la vittima stessa che è indotta a scaricare ed installare il malware per mezzo di tecniche di “ingegneria sociale”

ad esempio: premi per riscattare un premio

Spearphishing Una particolare forma di phishing avente come obiettivo un particolare individuo o gruppo di individui

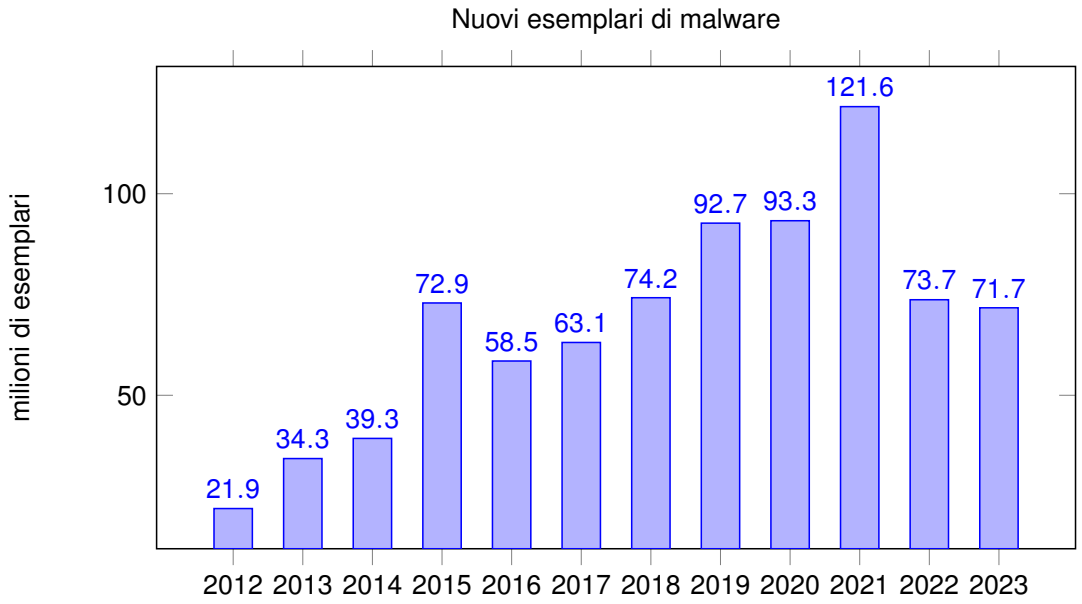
qui l'ingegneria sociale è più usata, perchè richiede più informazioni sulla vittima specifica.

Come si trasmette il malware?

Introduzione al malware
Marco Cesati

Schema della lezione
Cybersecurity
Cosa è il malware
Breve storia
Tipologie
Trasmissione
Diffusione
Nei sistemi industriali
Nei sistemi embedded
Strategia di difesa

Qual è la reale diffusione del malware?

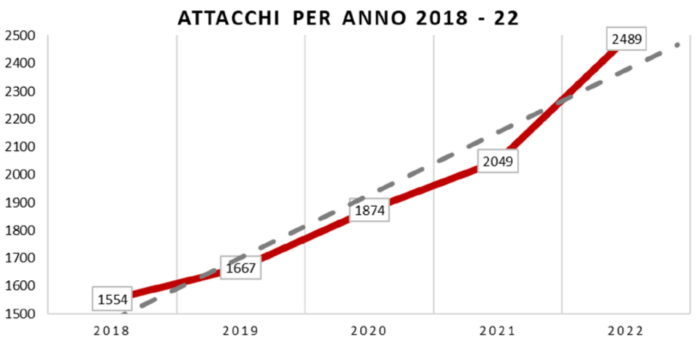


Fonte: https://portal.av-atlas.org/malware/statistics

Vengono diffusi centinaia di migliaia di **nuovi** esemplari di malware **ogni giorno**!

Qual è la reale diffusione del malware? (2)

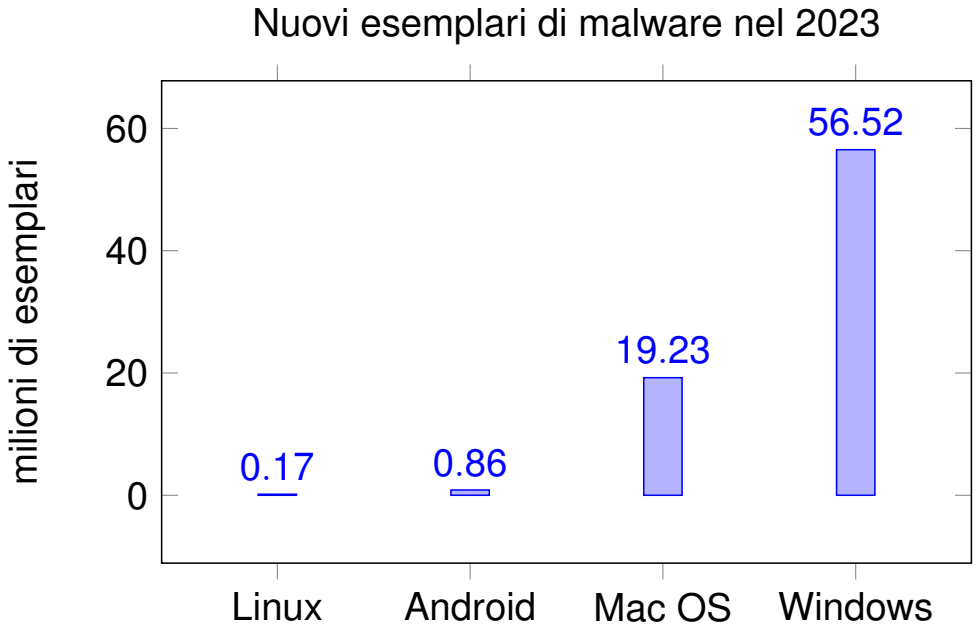
- Tra il 2018 ed il 2022 sono stati registrati 9633 incidenti gravi (di rilevanza internazionale)
- Nella maggioranza di questi incidenti il malware ha avuto un ruolo cruciale
- Nel solo anno 2021 i danni dovuti al malware in tutto il mondo ammontavano a circa 2500 miliardi di dollari (equivalenti all'intero PIL italiano)



Fonti: Rapporto CLUSIT 2023 sulla sicurezza ICT in Italia, Cybersecurity Ventures

In quale ambito si diffonde il malware?

La maggior diffusione del malware si verifica nei sistemi basati su Microsoft Windows



Fonte: https://www.av-test.org/en/statistics/malware/

I primi 10 malware per Windows in Q2 2023

(1) CoinMiner: miner di crittovalute basato essenzialmente su WMI (Windows Management Instrumentation)

(2) NanoCore: RAT che permette di accettare comandi da remoto per scaricare ed eseguire file, visitare siti web e aggiungere chiavi di registro

(3) ZeuS: anche se la versione originale è apparsa nel 2011, è ancora il più diffuso malware per rubare le credenziali di accesso ai siti di home banking

(4) ViperSoftX: stealer di crittovalute diffuso tramite siti di file sharing e torrent

(5) Agent Tesla: RAT in vendita su forum criminali come Malware-as-a-Service (MaaS)

Fonte: `https://www.cisecurity.org/insights/blog/top-10-malware-q2-2023`

I primi 10 malware per Windows in Q2 2023 (2)

(6) Ratenjai: un trojan scoperto nel 2022 con funzionalità RAT

(7) Gh0st: RAT che permette di ottenere il completo controllo della macchina infettata; originalmente era utilizzato per una operazione di spionaggio su scala mondiale scoperta nel 2009

(8) Laplas: clipper diffuso da SmokeLoader tramite email di phishing

(9) DarkVision: RAT scritto in C++ e venduto sul dark web

(10) Amadey: botnet venduto su forum criminali: utilizzato prevalentemente come information stealer e per scaricare altro malware

Fonte: `https://www.cisecurity.org/insights/blog/top-10-malware-q2-2023`

In quale ambito si diffonde il malware? (2)

È comunque un grave errore assumere che il malware sia diffuso soltanto nei sistemi desktop personali

Il rischio più grave in effetti è ignorare la minaccia che il malware può rappresentare in tanti diversi ambiti

Due esempi per tutti:

- Sistemi industriali
- Sistemi embedded

Malware nei sistemi industriali

I sistemi dedicati al controllo industriale (OT=Operation Technology, ICS=Industrial Control Systems) sono vulnerabili al malware esattamente come i calcolatori personali

In una indagine statistica rivolta a circa 500 imprese in tutto il mondo:

- Il 15% delle imprese afferma di aver avuto incidenti rilevanti nel 2021
- Il 12% afferma di non aver avuto incidenti rilevanti nel 2021
- **Almeno il 49% non sa rispondere con certezza**

Fonte: SANS 2021 Survey OT/ICS Cybersecurity

Malware nei sistemi industriali (2)

Tra le aziende che hanno rilevato incidenti nel 2021:

- il 57% ne ha contati più di 10
- il 90% ha avuto ripercussioni sulla produzione
- nel 54% dei casi si è trattato di **ransomware**

Fonte: SANS 2021 Survey OT/ICS Cybersecurity

Esempio: il caso Stuxnet

Esempio: il caso Stuxnet

- Nel 2010 è stata portata alla luce l'esistenza di un worm sviluppato per attaccare i PLC (controller logici programmabili) utilizzati per le centrifughe per la produzione di uranio arricchito in Iran
- Utilizzava 4 diverse vulnerabilità "zero-day" di Windows per scalare i privilegi e agganciarsi ad un programma di controllo della Siemens sulla macchina locale
- Installava anche un rootkit per nascondere l'esistenza del malware
- I suoi scopi erano:
  - collezionare informazioni sugli OT/ICS iraniani
  - provocare un malfunzionamento nelle centrifughe tali da portarle, progressivamente, alla rottura
- L'infezione iniziale è stata causata, probabilmente, da un trasferimento da dispositivo USB
- Dopo la prima infezione il worm si trasmetteva autonomamente agli altri calcolatori connessi nella rete locale

Esempio: il caso Stuxnet (2)

- Gli autori di Stuxnet non sono ufficialmente noti
- È molto probabile che sia il risultato di una operazione di guerra cibernetica messa in atto da USA e, probabilmente, Israele
- Certamente il livello di sofisticazione ed il valore intrinseco del malware sono al di sopra delle capacità di un singolo programmatore
- Si stima che Stuxnet abbia danneggiato circa 1/5 delle centrifughe iraniane
- Poiché il worm è progettato per diffondersi in modo indiscriminato, e solo successivamente installa un payload specifico per il sistema Siemens attaccato, è possibile riutilizzarlo per altri scopi
- In totale, in tutto il mondo, il worm ha infettato circa 200 000 sistemi e danneggiato un migliaio di dispositivi

Malware nei sistemi embedded

Malware nei sistemi embedded

- I sistemi embedded sono tutti i sistemi di calcolo integrati all'interno di dispositivi hardware
- Dal punto di vista dei progettisti dei dispositivi hardware, questi sistemi di calcolo sono a tutti gli effetti computer liberamente programmabili
- Ciò che l'utente finale definisce "firmware" è il software eseguito dal sistema di calcolo sul dispositivo
- Sebbene meno diffuso del malware per i calcolatori ad uso generale, è possibile trovare malware anche nel firmware
- In questo scenario l'utente non ha alcuna facile difesa!
  - Non può installare un software antivirus od eseguire un controllo
  - Non può disabilitare l'esecuzione del firmware
  - I meccanismi di aggiornamento del firmware possono essere sfruttati anche per installare nuovo malware
  - Non si aspetta realmente che un dispositivo elettronico possa essere "malevolo"!

Esempio: spyware in una videocamera di sorveglianza

Esempio: spyware in una videocamera di sorveglianza

- Una videocamera di sorveglianza di produzione cinese è dotata di una interfaccia WiFi per la connessione al server di monitoraggio
- Il firmware della videocamera è basato su Linux
- Lo abbiamo analizzato a fondo e trovato:
  - Un account di amministratore non documentato con password prefissata
  - Servizi di messaggistica aperti verso server cinesi
  - Decine di vulnerabilità che consentono a utenti remoti di eseguire qualunque comando con privilegi di root
- Non è un caso isolato! VStarcam, Loftek, Neo IP sono produttori cinesi che utilizzano tutti essenzialmente la stessa elettronica, lo stesso firmware ed hanno le stesse vulnerabilità
- Solo in questa classe di videocamere: circa 200 000 dispositivi nel mondo

Una strategia per la difesa

Una strategia per la difesa

- Il malware si presenta sotto tante forme e tanti diversi modi di operare

> Non esiste una soluzione definitiva!

- Dobbiamo considerare il problema del malware nel contesto di tutta la **cybersecurity**
- Siamo, a livello di nazione e continente, molto indietro: le minacce sono sempre crescenti e sempre più dannose
- Quale strategia possiamo adottare? Dobbiamo:
  - rendere consapevoli gli utenti finali
  - formare specialisti di cybersecurity

Una strategia per la difesa (2)

Possiamo fare un parallelo con il sistema sanitario nazionale:

- Tutti i cittadini ricevono una istruzione di base sui rischi sanitari e sulle regole igieniche da seguire
- Sul territorio operano figure professionali che assistono la popolazione
  (medici di base, pediatri, geriatri, odontoiatri,...)
- Operatori specializzati in varie patologie lavorano in cliniche ed ospedali per fare ricerca e risolvere i casi critici
- In alcuni centri nazionali operano professionisti ad altissima specializzazione per fare ricerca e trattare le patologie più rare, gravi o rischiose
- Tutti gli operatori sanitari sono formati dal sistema universitario

Una strategia per la difesa (3)

Dovremo arrivare ad avere un sistema equivalente per la cybersecurity!

- Tutti i cittadini ricevono una istruzione di base sui rischi connessi all'uso delle tecnologie digitali
- Sul territorio operano figure professionali che assistono le aziende ed i privati per le problematiche di cybersecurity
- Operatori specializzati in vari aspetti della cybersecurity lavorano in centri specializzati per studiare e trattare i casi più critici
- In alcuni centri nazionali operano professionisti ad altissima specializzazione per studiare e trattare gli incidenti di rilevanza per la sicurezza nazionale
- Tutti gli operatori di cybersecurity sono formati dal sistema universitario

Quale è la situazione attuale in Italia?

Quale è la situazione attuale in Italia?

- In base all'indice DESI della Commissione Europea, l'Italia è tra i 27 paesi della Unione Europea:
  - Ventesima per digitalizzazione complessiva
  - Terzultima per popolazione con competenze digitali almeno di base
  - Quartulima per popolazione con competenze digitali avanzate
  - Ultima per quota di laureati in ambito ICT sul totale della popolazione laureata
- L'Italia ha speso nel 2022 lo 0.1% del PIL in prodotti e servizi di sicurezza informatica
  - In valore assoluto è circa la metà di quanto spendono paesi come Germania, Francia, Canada, Giappone, e circa un terzo di quanto spendono USA e Gran Bretagna

Fonte: Rapporto CLUSIT 2023 sulla Sicurezza ICT in Italia

Quale è la situazione attuale in Italia? (2)

- Esistono alcuni progetti pilota per la formazione di studenti delle scuole secondarie, anche a livello nazionale
  - Molto bravi: ci siamo sempre classificati nei primi tre posti alle Olimpiadi di Cybersecurity
  - Comunque sono piccoli numeri: qualche centinaio di persone coinvolte al più
- Solo nelle aziende più grandi vi sono figure dedicate alla cybersecurity
- Esistono alcuni centri nazionali per trattare il cybercrime, primo fra tutti la Agenzia per la Cybersicurezza Nazionale (ACN), che però è stata istituita solo nel 2021 ed ha un ruolo di coordinamento e supervisione
- Non esistono centri di formazione specializzati
- Esistono alcuni corsi di laurea universitari focalizzati sugli aspetti di cybersecurity (ancora troppo pochi!)

Quale è la situazione attuale in Italia?

"WE COULDN'T HIRE THE CYBERSECURITY CANDIDATE YOU SENT US, HE WAS SAYING TOO MANY SCARY THINGS ABOUT OUR COMPUTERS."