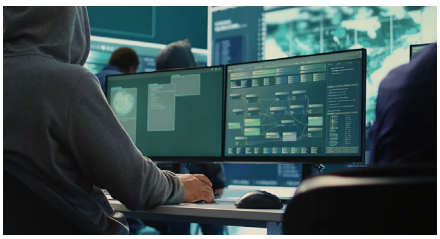
CyberGrant
SECURITY MADE EASY

WHITE PAPER

Ransomware, Spyware e Backdoor: minacce esterne da monitorare

Sommario

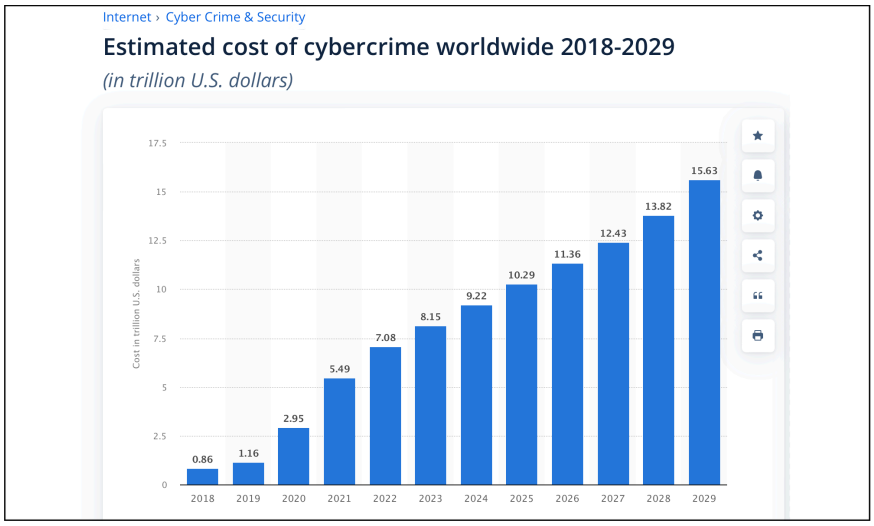
Scenario di cybersecurity



La criminalità informatica è in aumento e gli attacchi stanno diventando sempre più sofisticati e costosi per chi li subisce, mettendo sempre più in difficoltà le aziende.

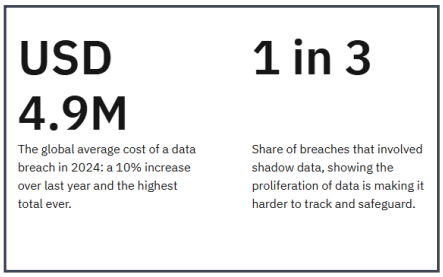
Di seguito alcune statistiche che evidenziano lo scenario 2025 degli attacchi con cui le aziende si stanno confrontando.

Scenario Globale



Fonte immagine: Statista “Technology Market Insight 2024”

- Il crimine informatico è destinato a costare alle aziende fino a 11,36 trilioni di dollari entro la fine del 2025 e potrebbe raggiungere i 15,63 trilioni di dollari entro il 2029. (Statista)
- Il costo medio di una violazione dei dati a livello globale è cresciuto fino a raggiungere circa 4,9 milioni di dollari nel 2024, con un aumento del 10% rispetto all’anno precedente. Con 1 su 3 violazioni che hanno coinvolto dati ombra. (IBM)
- Il ransomware costa alle vittime una media di 1,85 milioni di dollari per incidente, con un aumento degli attacchi del 13% negli ultimi cinque anni. (IBM)
- Il furto di credenziali continua a essere un problema, con un aumento del 71% su base annua degli attacchi che utilizzano credenziali compromesse. (IBM)
- Un aumento del 17% delle richieste di risarcimento per attacchi ransomware nel 2024, con un picco nel quarto



trimestre con il 57% in più rispetto al quarto trimestre del 2023. (Deloitte)

- Il 60% dei destinatari cade vittima di attacchi di phishing basati su GenAI, paragonabile ai numeri degli attacchi tradizionali. (Harward Business Review)
- In media, in tutti i settori, le aziende impiegano 204 giorni per individuare una violazione dei dati e 73 giorni per contenerla. (IBM)
- Le aziende che rilevano e contengono le violazioni dei dati entro 200 giorni registrano, complessivamente, un risparmio di 1 milione di dollari, rispetto a quelle che non lo fanno. (IBM)

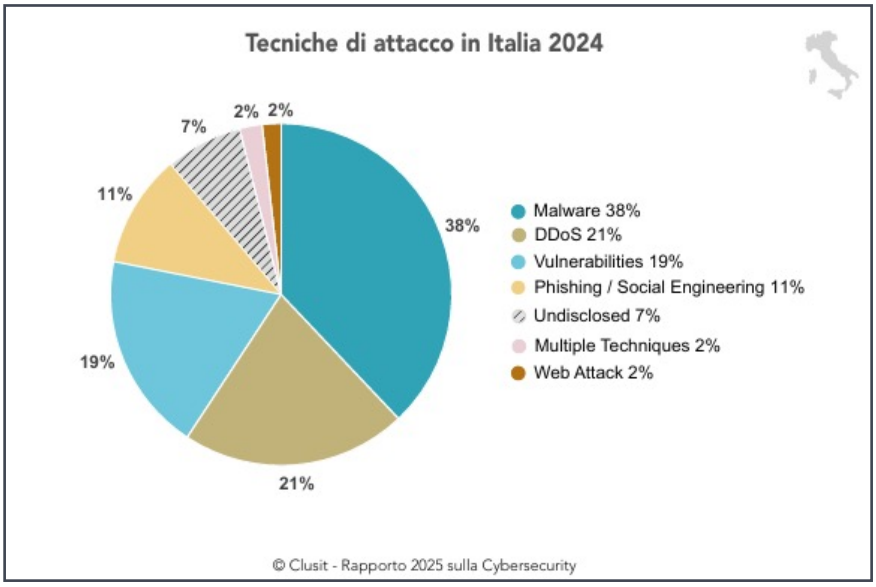
Scenario Italiano

Di seguito i dati più rilavanti resi noti.

Report ACN – Operational Summary Aprile 2025

Il report rivela che sono stati registrati:

- 118 ransomware, in **aumento del 64%** rispetto ai 72 dei primi 4 mesi del 2024;
- 73 rivendicazioni di ransomware da parte di gruppi criminali, in aumento rispetto alle 51 rivendicazioni dei primi 4 mesi del 2024.
- 24 attacchi ransomware sono stati rilevati, con un aumento del 30% rispetto ad aprile 2024.
- I maggiori vettori di attacco ad aprile 2025 risultano essere:
  - campagne malevole veicolate tramite e-mail,
  - utilizzo di credenziali valide precedentemente compromesse
  - sfruttamento di vulnerabilità note.
- 16.957 asset potenzialmente vulnerabili, pari ad un aumento del 443% rispetto ai 3.120 del primo quadrimestre del 2024



Fonte Immagine – CLUSIT Cybersecurity report 2025 -Distribuzione delle tecniche d'attacco in Italia

Clusit – Cybersecurity Report (marzo 2025)

Anche lo scenario presentato dall'ultimo Cybersecurity Report del Clusit non è incoraggiante. Di fatto dal report si evince che:

- L'Italia ha subito il 10% degli attacchi registrati a livello globale nel 2024
- Registrati **3577 incidenti noti di particolare gravità nel 2024 in Italia**
- Un +15% degli incidenti subiti

in Italia nel 2024 rispetto al 2023

- In Italia le tecniche di attacco risultano così distribuite: 38% malware; 28% DDoS; 19% vulnerabilità; 11%Phishing/ Social Engineering; 7%Tecniche non classificate; 2%Multiple Techniques; 2%Web Attacks.

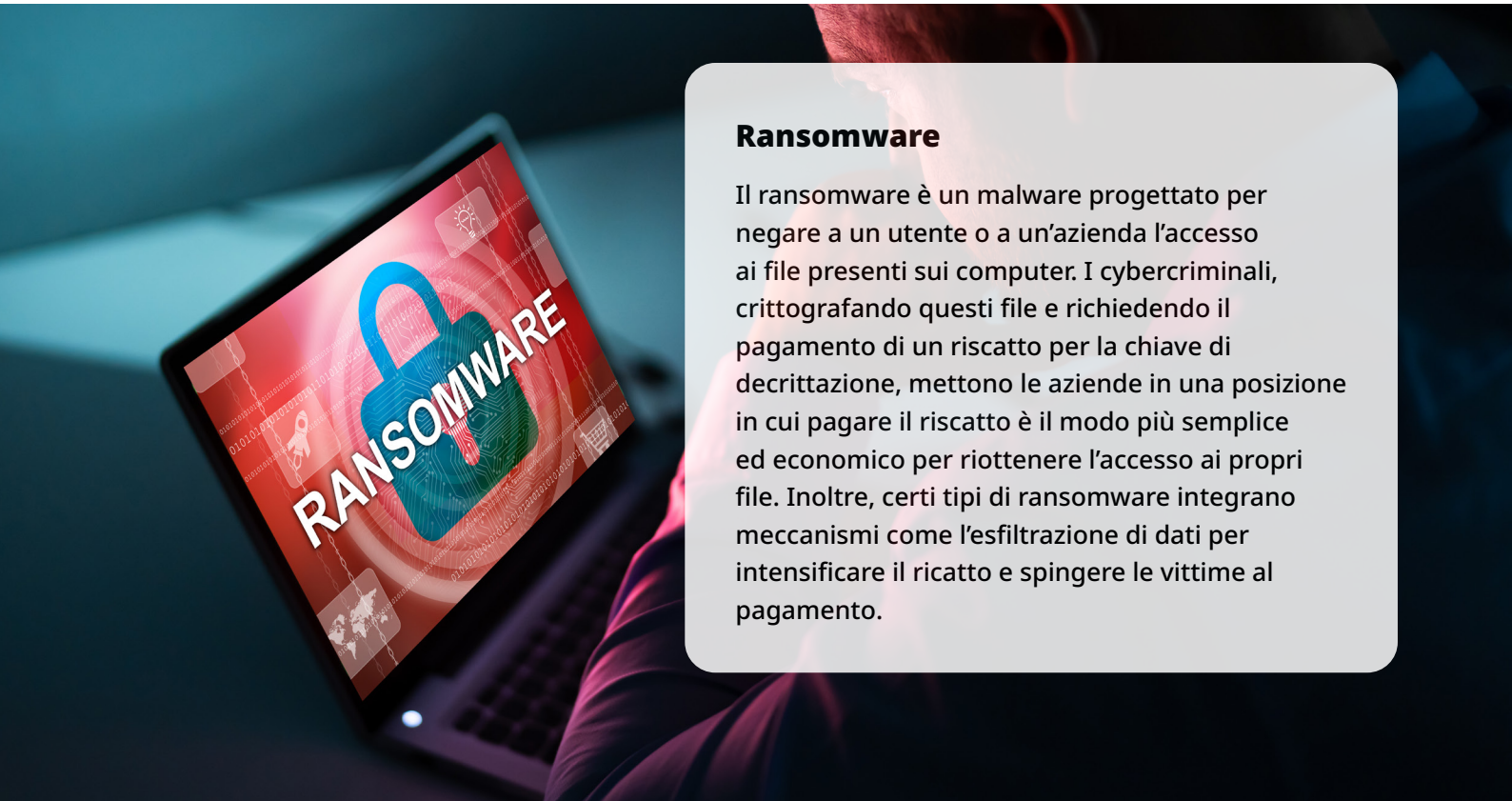
È interessante osservare come il Cybercrime non sia l'unico attore in crescita:

- **Hacktivism** segna un aumento del 16% rispetto all'anno precedente, evidenziando un ritorno di attività su questo fronte.
- Le operazioni di **Information Warfare** registrano un incremento ancora più marcato, quasi raddoppiando rispetto all'anno precedente.

In controtendenza, gli incidenti legati a **Espionage / Sabotage sono in calo**, con una riduzione del 20%, rappresentando l'unica categoria in diminuzione nel panorama delle minacce.

Ransomware, Spyware e backdoor: cosa sono, come si manifestano

Di seguito un focus su ransomware, spyware e backdoor.



Ransomware

Il ransomware è un malware progettato per negare a un utente o a un'azienda l'accesso ai file presenti sui computer. I cybercriminali, crittografando questi file e richiedendo il pagamento di un riscatto per la chiave di decrittazione, mettono le aziende in una posizione in cui pagare il riscatto è il modo più semplice ed economico per riottenere l'accesso ai propri file. Inoltre, certi tipi di ransomware integrano meccanismi come l'esfiltrazione di dati per intensificare il ricatto e spingere le vittime al pagamento.

È doveroso evidenziare che il ransomware è, negli ultimi anni, rapidamente diventato **la tipologia di malware più diffusa e visibile.** Basti pensare ai recenti attacchi ransomware che hanno compromesso la capacità degli ospedali di fornire servizi essenziali, paralizzato i servizi pubblici nelle città e causato danni significativi a diverse aziende.

Tipi di ransomware

Tipologie di attacchi ransomware - Il ransomware si è evoluto notevolmente negli ultimi anni. Tra i principali tipi di ransomware e minacce correlate figurano:

- **Ransomware a doppia estorsione** – Si caratterizza per il combinare la crittografia dei dati con il furto di dati. Tale tecnica è stata sviluppata in risposta alle aziende che si rifiutano di pagare i riscatti e preferiscono ripristinare i dati dai backup. Di fatto, i cyber criminali, rubando anche i dati di un'azienda, potrebbero minacciare di divulgarli se la vittima non paga.
- **Ransomware a tripla estorsione** – Si caratterizza per l'aggiunta di una terza tecnica di estorsione, includendo la richiesta di un riscatto ai clienti o ai partner della vittima o l'esecuzione di un attacco DDoS (Distributed Denial of Service) contro l'azienda.
- **Locker ransomware** – È un ransomware che non crittografa i file sul computer della vittima, bensì, blocca il computer, rendendolo inutilizzabile per la vittima, fino al pagamento del riscatto.
- **Crypto ransomware** – È un altro nome per il ransomware, a sottolineare il fatto che i pagamenti per i ransomware vengono comunemente effettuati in criptovalute, dato che sono valute digitali più difficili da tracciare, poiché non sono gestite dal sistema finanziario tradizionale.
- **Wiper** - Si tratta di una forma di malware correlata, ma distinta dai ransomware. Sebbene utilizzino le stesse tecniche di crittografia, l'obiettivo è negare definitivamente l'accesso ai file crittografati, il che può includere l'eliminazione dell'unica copia della chiave di crittografia.
- **Ransomware as a Service (RaaS)** - È un modello di distribuzione del malware in cui le bande di ransomware forniscono l'accesso al loro malware ad "affiliati". Questi affiliati infettano i bersagli con il malware e suddividono il pagamento del riscatto con gli sviluppatori del ransomware.

Cosa fare quando si subisce un attacco ransomware

È doveroso evidenziare che molti attacchi ransomware andati a buon fine vengono rilevati solo dopo il completamento della crittografia dei dati e la visualizzazione di una richiesta di riscatto sullo schermo del computer infetto. Ne consegue che i file crittografati sono probabilmente irrecuperabili; tuttavia, si consiglia di adottare, appena possibile, le seguenti attività:

- Mettere in quarantena il computer - Alcune varianti di ransomware cercheranno di diffondersi su unità connesse e ad altri computer. Pertanto, si consiglia di limitare la diffusione del malware impedendo l'accesso ad altri potenziali bersagli.
- Lasciare il computer acceso - La crittografia dei file può compromettere la stabilità del sistema e lo spegnimento del computer potrebbe comportare la perdita di dati in memoria volatile.. Pertanto, si consiglia di tenere il computer acceso per massimizzare le probabilità di ripristino.
- Creare un backup - Alcune varianti di ransomware permettono la decrittazione dei file senza necessità di pagamento. Pertanto, si consiglia di creare una copia dei file crittografati su un supporto rimovibile nel caso in cui una soluzione diventi disponibile in futuro o un tentativo di decrittazione non riuscito danneggi i file.
- Verificare la presenza di decryptor - Si consiglia di consultare il sito web "No More Ransom" – i.e. un'iniziativa intrapresa dal National High Tech Crime Unit della polizia olandese, dall' European Cybercrime Centre dell'Europol, dal Kaspersky e McAfee, con l'obiettivo di aiutare le vittime del ransomware a recuperare i loro dati criptati, senza dover pagare i criminali - per verificare se è disponibile un decryptor gratuito ed eseguirlo su una copia dei dati crittografati per verificare se è in grado di ripristinare i file.
- Chiedere supporto - A volte i computer archiviano copie di backup dei file in essi contenuti. Si consiglia di contattare un esperto di informatica forense per verificare la possibilità di recuperare queste copie, qualora non siano state eliminate dal malware.
- Cancellare e ripristinare – Si consiglia di effettuare il ripristino del computer utilizzando un backup pulito o un'installazione pulita del sistema operativo per garantire la completa rimozione del malware dal dispositivo.

Inasprimento della legislazione vs. ransomware

Un'azienda, **dopo un attacco** ransomware, ha tre opzioni principali:

- **Segnalare pubblicamente l'incidente** e ripristinare le operazioni e i dati senza comunicare con i criminali informatici.
- **Segnalare l'incidente, ma pagare un riscatto** per ripristinare i dati e impedirne la pubblicazione.
- **Nascondere l'accaduto pagando un riscatto** per il silenzio.

Molti Paesi, per arginare il pagamento del riscatto stanno **approvando leggi che rendono illegali tali azioni**. Ad esempio:

- L'UE con la **direttiva NIS2** e il DORA (Digital Operational Resilience Act) impone alle aziende di molti settori, nonché alle entità critiche, di segnalare tempestivamente gli incidenti informatici e richiedono il rispetto di significativi requisiti di resilienza informatica.
- Nel Regno Unito è in discussione una legge che impedirebbe alle aziende governative e ai gestori di infrastrutture critiche di pagare riscatti e imporrebbe inoltre a tutte le aziende di segnalare tempestivamente gli incidenti di ransomware.
- Negli Stati Uniti è già stato parzialmente adottato, un pacchetto di direttive federali e leggi statali che proibiscono pagamenti di importo elevato (oltre 100.000 dollari) ai criminali informatici e impongono la tempestiva segnalazione degli incidenti.
- In Italia la legislazione per contrastare gli attacchi ransomware si sta evolvendo. Recentemente, la Legge 90/2024 ha introdotto disposizioni specifiche per la Pubblica Amministrazione e il settore privato, con particolare attenzione alla gestione degli incidenti informatici. Inoltre, si sta valutando di vietare il pagamento dei riscatti, soprattutto per soggetti critici, con l'obiettivo di disincentivare questi attacchi.

Inoltre, lo scorso marzo 2025 è stata depositata alla Camera dei deputati una proposta di legge che punta a dotare il Paese di una strategia nazionale strutturata per contrastare questo fenomeno sempre più pervasivo e pericoloso.

Spyware

Lo spyware è un tipo di **software dannoso** (malware) che viene installato su un dispositivo informatico senza l'autorizzazione dell'utente finale ed è appositamente progettato per **accedere a un computer e registrarne l'attività**. Esso può tracciare e registrare le abitudini di navigazione di un utente, le credenziali di accesso, le password, ecc... Di fatto, l'autore dello spyware utilizza le informazioni ottenute durante la violazione dei dati per

Gli spyware si diffondono, normalmente, tramite: e-mail di phishing, download dannosi, app false o siti web compromessi e, una volta installati, **possono essere eseguiti in background, registrando le sequenze di tasti premuti, catturando screenshot o trasmettendo dati sensibili**.

Lo spyware ha come obiettivo principale lo **spionaggio**, spesso finalizzato a ottenere vantaggi economici, personali o politici

Tipi di spyware

Di seguito alcune delle tipologie più comuni di spyware a cui prestare attenzione:

- **Keylogger** – Il Keylogger tiene traccia e registra le sequenze di tasti durante la digitazione. Carpisce le informazioni e le invia a un hacker utilizzando un Command & Control (C&C) server. L'hacker analizza, quindi, le sequenze di tasti per individuare nomi utente e password e li utilizza per hackerare sistemi altrimenti sicuri.
- **Spyware Trojan** - Si maschera da programmi legittimi ed entra nei dispositivi tramite malware Trojan, che distribuisce il programma spyware.
- **Stalkerware** -È usato per controllare una persona a distanza e si basa su vari strumenti di monitoraggio impiegati per sorvegliare le attività online.
- **Adware** - Genera entrate per i suoi sviluppatori, creando automaticamente annunci pubblicitari sullo schermo, di solito all'interno di un browser web. L'adware viene in genere creato per i computer, ma può essere trovato anche su dispositivi mobili. È doveroso evidenziare che alcune forme di adware sono altamente manipolative e creano una porta aperta per programmi dannosi.
- **Rootkit** - I programmatori possono accedere e controllare un PC tramite un rootkit, i.e. una sorta di spyware. Nonostante la maggior parte dei rootkit si concentri sul framework e sui programmi installati, alcuni riescono a monitorare il framework, attaccando il firmware e il design del PC.

Computer, Mac, dispositivi iOS e Android, inclusi smartphone e tablet, possono essere generalmente infettati da spyware. Ovvero, uno **spyware può contaminare qualsiasi dispositivo in grado di connettersi a Internet**.

Ecco alcune strategie per rilevare lo spyware:

- Non fare nulla quando appare un pop-up o altro, senza prima capire di cosa si tratta.
- Evitare di aprire connessioni nei messaggi inviati da account sconosciuti.
- Evitare di scegliere connessioni che rimandano a siti malevoli.
- Evitare di scaricare software gratuiti introdotti come strumento di supporto o incluso in un collegamento e-mail che sembra reale.
- Evitare di scaricare app o file da fonti non attendibili, in particolare siti Web di terze parti.
- Fare attenzione alle e-mail di phishing e agli allegati, soprattutto se contengono messaggi urgenti o allarmanti.

Backdoor

Le backdoor rappresentano **punti di accesso non autorizzati** introdotti in un sistema informatico, progettati per aggirare i normali meccanismi di sicurezza. Tale tipo di minaccia consente agli aggressori di **ottenere un accesso continuo e invisibile ai sistemi**, spesso senza dover superare ulteriori controlli di autenticazione.

Gli attacchi backdoor si basano sull'**individuazione e lo sfruttamento di vulnerabilità presenti nel software, nell'hardware o nell'infrastruttura di rete**. Nella maggior parte dei casi, tali porte d'accesso vengono installate tramite malware, campagne di phishing o l'utilizzo di software non aggiornato, rendendole particolarmente insidiose e difficili da rilevare e, **se rimangono attive, passano completamente inosservate per mesi o anni,** permettendo agli hacker una via più facile per continuare le proprie attività senza essere individuati, causando effetti dirompenti sulle aziende.

Modalità di diffusione degli attacchi backdoor

Gli attacchi backdoor possono sfruttare diversi vettori, scelti in base alle vulnerabilità del sistema per garantire all'aggressore un accesso profondo e prolungato. In particolare, attraverso:

- **Installazione di malware** – Gli aggressori utilizzano trojan o altri malware camuffati da applicazioni legittime che, una volta eseguiti sul dispositivo della vittima, installano backdoor che consentono accessi non autorizzati. Il phishing è un canale d'attacco comune, in cui gli utenti vengono indotti a scaricare file infetti credendoli provenienti da fonti affidabili.
- **Exploit di rete** - Le backdoor possono essere installate su dispositivi di rete come router e firewall, consentendo agli attaccanti di monitorare, manipolare e deviare il traffico di rete aziendale. Inoltre, l'accesso ottenuto può estendersi a un'intera infrastruttura, compromettendo più sistemi contemporaneamente.
- **Ingegneria sociale** – Si tratta di tecniche – quali il phishing - che spingono gli utenti a rivelare credenziali o ad attivare involontariamente software malevoli. Gli aggressori si presentano spesso come contatti fidati o utilizzano siti web contraffatti per ottenere l'accesso e, dopo aver raccolto le credenziali, installano backdoor senza che l'utente se ne accorga.
- **Compromissione della catena di approvvigionamento** - Le backdoor possono essere inserite direttamente in componenti software o hardware durante la fase di produzione; successivamente, questi elementi compromessi vengono distribuiti e installati, attivando la backdoor. Si tratta di u tipo di attacco particolarmente difficile da rilevare, poiché sfrutta canali apparentemente legittimi dell'infrastruttura aziendale.

Come rilevare un attacco backdoor

È fondamentale prestare attenzione a determinati segnali che possono indicare una violazione in corso. Gli aggressori, infatti, mirano a restare il più a lungo possibile nei sistemi compromessi senza essere rilevati, cercando di coprire ogni traccia delle proprie attività. Pertanto, individuare tempestivamente comportamenti sospetti consente alle aziende di reagire con rapidità e limitare i danni, quali:

- **Rallentamento inspiegabile del sistema** - Una diminuzione improvvisa delle prestazioni può essere il sintomo della presenza di una backdoor. Questi rallentamenti sono spesso causati da processi nascosti in esecuzione che consumano risorse di sistema, quali il caricamento di dati o la registrazione delle attività degli utenti. Pertanto, se le operazioni abituali iniziano a richiedere più tempo del previsto, è possibile che un malware agisca silenziosamente in background.
- **Traffico di rete anomalo** - Un flusso insolito di dati, soprattutto verso indirizzi IP sconosciuti, può segnalare un'esfiltrazione di informazioni tramite una backdoor. In alcuni casi, gli attaccanti utilizzano tunnel crittografati per trasferire dati all'esterno,

rendendo l'attività difficile da rilevare. Picchi di traffico ricorrenti in orari inusuali rappresentano un chiaro indizio di un accesso non autorizzato in corso.

- **Modifiche sospette alla configurazione** - Cambiamenti imprevisti nelle impostazioni di sistema o nei privilegi utente sono spesso effettuati dagli attaccanti per indebolire le difese o garantirsi un accesso continuo. Un esempio tipico è l'alterazione delle regole del firewall per permettere connessioni in entrata attraverso una backdoor, facilitando così il controllo remoto del sistema compromesso.
- **Arresti anomali e instabilità del sistema** - Crash frequenti, errori improvvisi o comportamenti instabili possono essere il risultato dell'interferenza di una backdoor con le normali operazioni del sistema. In alcuni casi, questi problemi sono provocati intenzionalmente dagli aggressori per mascherare le proprie azioni o interrompere i processi aziendali, creando confusione e ritardando l'identificazione della minaccia.

Tipologie di attacchi Backdoor

Di seguito i principali tipi di attacchi backdoor:

- **Rootkit** - Un rootkit è una raccolta di strumenti progettata per nascondere la presenza di un utente malintenzionato. Esso può agire a livello di kernel, rendendo invisibili le attività malevole e difficilissimo il rilevamento. È spesso impiegato in attacchi persistenti avanzati (APT – Advanced Persistent Attack), sfuggendo ai software antivirus tradizionali.
- **Trojan Horse** - I trojan si camuffano da software legittimi e inducono l'utente a installarli e, una volta attivi, creano accessi nascosti per permettere ai cyber criminali di accedere. Sono comuni nei phishing, in cui link o allegati ingannevoli avviano l'infezione.
- **Attacchi a livello di applicazione** – Si tratta di backdoor che sfruttano le vulnerabilità in software specifici (es. file sharing o messaggistica), oltre ad operare all'interno di applicazioni affidabili, rendendo difficile sospettare attività malevole.
- **Backdoor basate su hardware** – Si tratta di backdoor incorporate nei componenti fisici, già in fase di produzione. Esse sono particolarmente insidiose e possono persistere a lungo nei dispositivi, intercettare dati e monitorare le attività senza essere rilevate.
- **Backdoor basate sulla rete** – Si tratta di backdoor inserite in dispositivi come router o firewall., permettendo agli attaccanti di monitorare, deviare o manipolare il traffico di rete, oltre ad esporre l'intera azienda a rischi estesi.
- **Cryptojacking** –Gli attaccanti, attraverso una backdoor, sfruttano le risorse IT della vittima per minare criptovalute, impattando negativamente su performance e costi aziendali, oltre a consumare risorse per fini illeciti.

Conseguenze degli attacchi ransomware, spyware e backdoor

Di seguito le conseguenze che le aziende normalmente si trovano a gestire quando colpite da ransomware, spyware e backdoor:

Conseguenze dirette

- **Furto di dati** - Gli attacchi ransomware, spyware e backdoor possono consentire ai criminali informatici di accedere a dati altamente sensibili, quali: proprietà intellettuale, registri finanziari e informazioni personali o aziendali dei clienti. Tali dati, dopo essere stati sottratti, possono essere crittografati (nel caso del ransomware) o silenziosamente trasmessi agli attaccanti (come con spyware o backdoor). Le informazioni rubate possono essere poi utilizzate per estorsioni, per spionaggio industriale, per furti di identità o per altre attività dannose, generando gravi perdite economiche e potenziali responsabilità legali per l'azienda colpita.
- **Interruzione del business**- Il ransomware può bloccare completamente l'accesso ai sistemi aziendali; mentre le backdoor permettono agli aggressori di infiltrarsi nei sistemi chiave e manipolarne il funzionamento. Ciò può comportare l'arresto forzato di applicazioni critiche, blackout informatici e l'impossibilità di accedere ai dati necessari per le

operazioni quotidiane. Tali interruzioni si traducono in: mancati ricavi, ritardi nelle consegne, paralisi delle attività produttive e compromissione dei rapporti con i clienti.

- **Perdita finanziaria** - Gli impatti economici diretti di un attacco ransomware, spyware o backdoor includono i costi per la gestione dell'incidente, il pagamento di eventuali riscatti, le sanzioni da parte delle autorità e le perdite di fatturato dovute all'interruzione delle attività. A questi si aggiungono i costi per le indagini forensi, il ripristino dei sistemi, la bonifica dell'infrastruttura IT e i risarcimenti per i clienti coinvolti. Le conseguenze finanziarie possono estendersi nel tempo e raggiungere cifre molto elevate, anche nell'ordine dei milioni di euro, come evidenziato anche dal report di IBM – Data breach cost 2024.
- **Danni alla reputazione** - Una violazione causata da ransomware, spyware o l'esistenza di una backdoor può generare una forte ondata di sfiducia da parte di clienti, partner e investitori, dato che l'esposizione pubblica dell'incidente e la percezione di vulnerabilità compromettono l'immagine aziendale, con effetti duraturi sulla redditività e sulle relazioni commerciali. Inoltre, ricostruire la reputazione richiede anni, mentre l'impatto negativo può portare alla perdita di clienti strategici e a un calo della competitività sul mercato.
- **Questioni legali e di conformità** - Le violazioni derivanti da questi tipi di attacchi possono comportare il mancato rispetto di normative come il GDPR, NIS2, DORA, ecc., esponendo l'azienda a sanzioni legali e amministrative. Inoltre, le autorità di regolamentazione ed i clienti possono intraprendere azioni legali, mentre l'azienda è spesso costretta a adottare, dopo l'incidente, onerose misure di adeguamento normativo. Ancora, la gestione legale post-attacco rappresenta un ulteriore aggravio economico e operativo. Senza dimenticare che gli hacker possono anche utilizzare le backdoor per compromettere i sistemi e rindirizzarli come parte di una botnet. Inoltre, il sistema compromesso può essere utilizzato per eseguire un attacco DDoS. Ovvero, la rete di un'azienda può essere utilizzata per attaccare altre aziende, portando a problemi di responsabilità e altri tipi di danni con conseguente compromissione dell'azienda.

Come prevenire gli attacchi ransomware, spyware e backdoor

Di seguito alcune delle best practice per prevenire gli attacchi ransomware, spyware e backdoor.

Controlli di sicurezza regolari

- **Eseguire audit frequenti** su sistemi e reti per individuare modifiche non autorizzate o configurazioni sospette che potrebbero indicare una backdoor.
- **Monitorare costantemente** per identificare precocemente **comportamenti anomali** e intervenire prima che una minaccia si concretizzi tramite implementazione di piattaforme SIEM e SOAR.

Rilevamento delle intrusioni e monitoraggio continuo delle minacce

- **Implementare sistemi IDS/IPS e soluzioni EDR** capaci di rilevare comportamenti fuori norma, quali trasferimenti anomali di dati o accessi da dispositivi sconosciuti.
- **Installare soluzioni di monitoraggio comportamentale** che possano identificare movimenti laterali tipici del ransomware o del traffico di spyware.

Protezione avanzata degli endpoint

- **Adottare soluzioni antivirus e antispyware affidabili**, arricchite da tecnologie di intelligenza artificiale e machine learning per intercettare malware noti e zero-day, per bloccare l'installazione di ransomware, rilevare spyware nascosti e impedire l'inserimento di backdoor a livello di sistema.

Formazione continua del personale

- **Educare i dipendenti a: riconoscere le email di phishing; gestire password in modo sicuro; segnalare comportamenti sospetti**. La consapevolezza è cruciale per evitare l'attivazione involontaria di spyware o il download di allegati contenenti ransomware o backdoor.

Aggiornamento costante di software e di hardware

- **Applicare le patch regolarmente** per correggere vulnerabilità sfruttate da attacchi ransomware e backdoor.
- **Abilitare gli aggiornamenti automatici**, ove possibile, dando priorità alle patch critiche e sostituendo sistemi obsoleti o non più supportati.

Controllo dei privilegi e gestione degli accessi

- **Implementare un modello di controllo basato sui ruoli** (RBAC – Role Based Access Control) per limitare l'accesso a dati sensibili.
- **Utilizzare MFA** (Multifactor Authentication) per gli account critici.
- **Implementare un'architettura Zero Trust (ZTA)** che presuppone che nessuna connessione, utente o risorsa sia affidabile finché non viene verificato.
- **Adottare soluzioni DLP** (Data Loss Prevention) per monitorare i privilegi e prevenire accessi impropri da parte di malware o utenti compromessi.

Backup regolari e isolati

- **Effettuare backup giornalieri** dei sistemi critici, memorizzandoli offline o su reti segmentate per proteggerli dal ransomware.
- **Verificare periodicamente l'integrità dei backup** e testarli, per assicurarsi che siano realmente ripristinabili in caso di emergenza.

Protezione contro lo spyware su dispositivi mobili e desktop

- **Controllare le autorizzazioni richieste dalle applicazioni**, soprattutto quelle che accedono a contatti, fotocamera o posizione.
- Installare strumenti per il **blocco dei pop-up**.
- **Limitare l'installazione di app** a fonti ufficiali e verificate.

Rilevamento proattivo delle minacce avanzate

- Valutare soluzioni di **threat detection in tempo reale e il supporto di un MSSP** (Managed Security Service Provider) per il monitoraggio h24, ove necessario, considerando che l'identificazione precoce di comportamenti sospetti consente di fermare ransomware e spyware prima che causino danni irreversibili.

CyberGrant a fianco delle aziende con la soluzione RemoteGrant

La società americana **CyberGrant**, attraverso la propria soluzione **RemoteGrant**, è a fianco delle aziende per supportarle nella prevenzione di attacchi ransomware, spyware e backdoor.

Di fatto, la **soluzione RemoteGrant** si converte in una leva strategica di cybersecurity per la protezione dei dati, essendo in grado di offrire e seguenti funzionalità:

RemoteGrant

RemoteGrant
ENDPOINT SECURITY

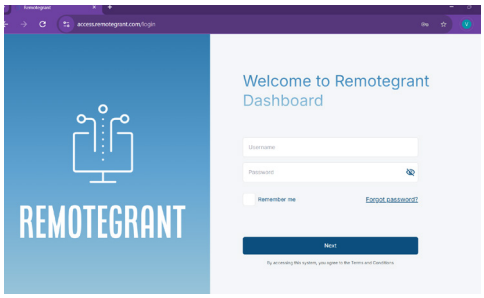
- **Monitorare e rilevare attività** sospette sui dispositivi.
- **Applicare automaticamente la cifratura** ai file aziendali, limitandone l'accesso esclusivamente alle applicazioni e dispositivi autorizzati e dotati di agenti di sicurezza approvati dall'organizzazione
- **Inviare avvisi** in caso di rilevamento di attività anomale non autorizzate.
- **Bloccare ransomware**, spyware, backdoor e le altre minacce.
- Fornire **protezione in tempo reale** contro exploit e vulnerabilità.
- **Monitorare e controllare** l'accesso remoto agli endpoint.
- **Registrare e monitorare tutti gli eventi** e le attività sugli endpoint.
- **Fornire log dettagliati** che possono essere analizzati per identificare e rispondere a incidenti di sicurezza.
- **Fornire autenticazione a più fattori (MFA)**.

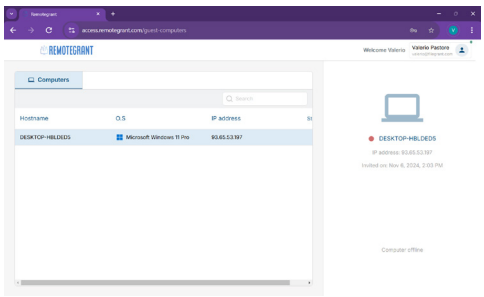
Le funzionalità di RemoteGrant sono di supporto alle aziende per la conformità alle maggiori vigenti regolamentazioni e normative - quali GDPR, NIS2, DORA, ecc – dato che soddisfano i rigorosi requisiti normativi in termini di protezione dei dati e di privacy.

Plus di RemoteGrant

Inoltre, RemoteGrant permette di:

- **Controllare quali applicazioni possono operare sui dati** sensibili e limitare azioni come copia, incolla o esportazione, mentre la crittografia assicura che le informazioni rimangano protette anche in caso di accesso non autorizzato.
- Selezionare le applicazioni con cui operare sui dati sensibili, **utilizzando le eccezioni per escludere eventuali processi non desiderat**i.
- **Indica le estensioni dei file da proteggere**, in modo che possano essere letti esclusivamente dalle applicazioni scelte.
- **Scegliere i computer sui quali applicare questa protezione**.
- **Impedire la copia di dati da macchine remote in RDP,** limitando altresì la possibilità di trasferire o duplicare file da percorsi remoti non autorizzati.
- **Vietare la scrittura di file in zone riservate**, impedendo la creazione o modifica di file in cartelle protette, oltre a ridurre il rischio di alterazioni accidentali o malevoli.





Conclusione

L’aumento degli attacchi informatici e la loro continua evoluzione e sofisticazione – in particolare ransomware, spyware e backdoor – impongono alle aziende un **cambio di paradigma: non è più sufficiente reagire, è necessario anticipare**.

La comprensione approfondita del proprio perimetro aziendale, delle vulnerabilità strutturali e dei punti di cedimento rappresenta il primo passo verso una strategia di difesa efficace. È proprio dalla **conoscenza dell’azienda** che si sviluppa la **consapevolezza necessaria per costruire una postura di cyber resilienza che sia al tempo stesso preventiva, reattiva e proattiva**.

Inoltre, fondamentale in questo contesto è l’investimento continuo in formazione e in esercitazioni, utili a rafforzare il “muscolo” della resilienza organizzativa e a testare la prontezza operativa in scenari critici.

Parallelamente, l’adozione e l’integrazione dei principi di **cybersecurity, business continuity e risk management, all’interno di un approccio risk-based e resilience-based** – come richiesto dalle normative vigenti – diventa non solo un obbligo, ma una leva strategica per garantire la continuità operativa, la protezione del valore aziendale e la fiducia degli stakeholder.

Ovvero, i**n un contesto di minacce sempre più sofisticate e pervasive, la resilienza non è un’opzione: è una necessità**.

A cura di **Federica Maria Rita Livelli**

www.cybergrant.net