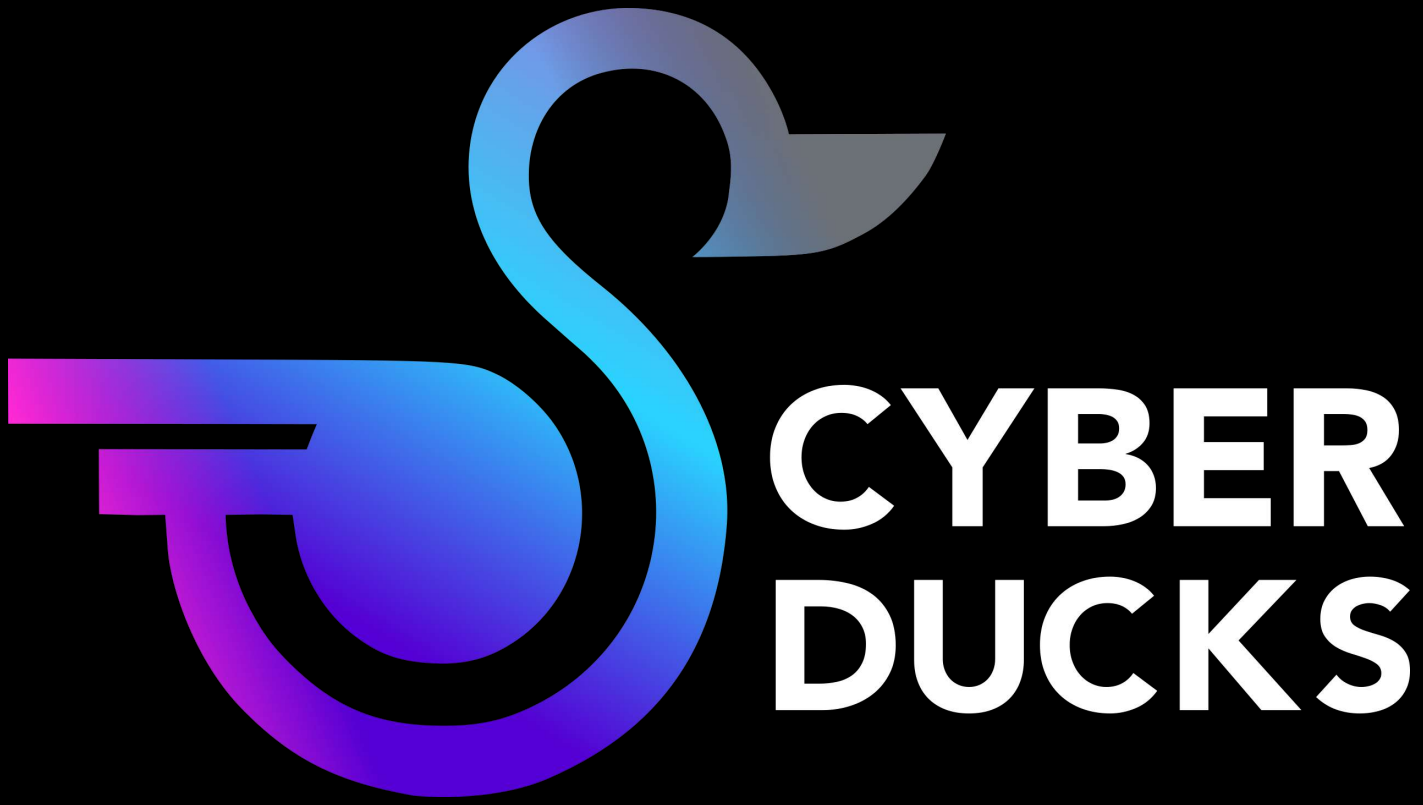

RANSOMWARE

Minacce cyber in evoluzione

RANSOMWARE

Sommario:

RANSOMWARE

Protagonista indiscusso

Sono molte le minacce informatiche che incombono su utenti troppo spesso distratti o inconsapevoli, che diventano così facili prede di criminali informatici, pronti a tutto per monetizzare i dati digitali di cui riescono a entrare in possesso.

Tra queste i *ransomware* si confermano essere la principale minaccia informatica degli ultimi anni. Una crescita esponenziale iniziata ben trent'anni fa, che ha visto di recente un vero e proprio boom, stimolando la nascita di varianti e sistemi di business. Attacchi che tendono a essere sempre meno generici e più mirati a obiettivi in grado di pagare somme anche importanti. Le aziende, infatti, hanno un potenziale economico maggiore rispetto ai singoli utenti. Che tuttavia rimangono il fattore chiave, perché un *ransomware* infetta la rete aziendale solo se qualcuno dall'interno gli apre la porta.

Protagonista indiscusso del 2021 è stato, ancora una volta, il *ransomware*: Il numero di casi è più che raddoppiato rispetto all'inizio 2020.

RANSOMWARE MIRATI

Sempre meno generici, sempre più specifici

Tra il 2019 e il 2020 i ransomware mirati hanno registrato una crescita del 767%. Perché mirati? Perché si tratta di attacchi destinati a obiettivi di alto profilo come aziende, agenzie governative, strutture sanitarie. Obiettivi dai quali risulta più facile ottenere un riscatto, sia per la disponibilità economica che per la necessità di dover ripristinare quanto prima i servizi compromessi. Allo stesso tempo calano gli utenti vittime di ransomware generici, quasi il 30% in meno. Si tratta di attacchi più sofisticati, che richiedono un maggior impegno nella preparazione per conoscere le infrastrutture di rete e le possibilità di accesso, incluse tattiche di social engineering per trovare l'anello debole. Le previsioni per il futuro vanno tutte in questa direzione: saranno sempre più le imprese a dover fronteggiare la minaccia dei ransomware, che dovranno quindi adottare tutte le misure idonee a proteggere i dati, a permettere un loro rapido recupero e il ripristino dell'operatività. Anche e soprattutto attraverso un'adeguata e instancabile opera di sensibilizzazione e formazione del personale. Inoltre, grazie ai nuovi business, i ransomware sono alla portata di tutti: criminali informatici trovano nel dark web kit già pronti per essere utilizzati e grazie a tecniche di social engineering o alle classiche e-mail di phishing è facile portare a termine un attacco con successo.

La doppia estorsione.

Se i primi ransomware chiedevano riscatti bassi, alla portata di tutti, facendo leva sul gran numero di pc da infettare e di vittime disposte a pagare, gli attacchi mirati si focalizzano al contrario su obiettivi ben selezionati, capaci di fronteggiare pagamenti consistenti pur di riottenere l'accesso ai dati violati. E per assicurarsi che ciò accada veramente, i criminali hanno pensato alla tecnica della ***doppia estorsione***. Il virus cripta i dati rendendoli illeggibili ma li esfiltra, così gli attaccanti ne entrano in possesso minacciandone la diffusione qualora l'azienda si rifiuti di pagare il riscatto. Attraverso questa doppia minaccia e la selezione dell'obiettivo, i criminali riescono a massimizzare i profitti .

NUOVI MODELLI DI BUSINESS

Ransomware as-a-service

Un nuovo ecosistema criminale si è venuto a creare attorno al business dei ransomware. E' il ***ransomware as-a-service o RaaS***.

In pratica il codice, o parti di esso, viene venduto attraverso appositi canali nel dark web permettendo anche ad hacker inesperti di effettuare un attacco ransomware con successo, con conoscenze informatiche minime. Chi crea il codice può, in questo modo, guadagnare sia dall'utilizzo diretto dello stesso che dalla sua vendita o noleggio. Al tempo stesso si moltiplicano gli attori in gioco, con il numero dei soggetti che tentano l'intrusione nelle reti informatiche aziendali, che cresce esponenzialmente. Si stima che nella prima metà dell'anno le organizzazioni americane potrebbero aver pagato ben 600 milioni di dollari a gruppi criminali informatici a causa di attacchi ransomware. Ciò che si trova in vendita sul dark web permette di effettuare attacchi forse non molto sofisticati e ben mirati ma sicuramente efficaci. Codici malevoli, accessi agli account, ma anche vere e proprie piattaforme organizzate per lanciare attacchi, monitorando l'andamento, la diffusione del ransomware e i guadagni ottenuti.

Come funziona.

I modelli di business più comuni sono quattro:

1. Abbonamento mensile per accedere al codice malevolo;
2. Affiliazione, simile all'abbonamento mensile ma con l'aggiunta di una percentuale sui profitti ottenuti per il gestore del Raas;
3. Pagamento una tantum di una licenza, senza nessuna partecipazione ai guadagni;
4. Partecipazione agli utili senza costi fissi.

I costi partono da 40 dollari fino a migliaia di dollari al mese, a seconda di quanto è sofisticata la piattaforma nella quale è inclusa, in molti casi, l'assistenza h24. Cifre che i criminali pagano volentieri visto il guadagno potenziale: un riscatto medio che è passato da 115.123 $ nel 2019 a **312.493 $ nel 2020** (+171%). Nel 2020 la richiesta più elevata , pari a 30 milioni di dollari .

COME DIFENDERSI

Conoscere il nemico

La debolezza umana: questo rimane il fattore principale per il successo dei ransomware così come di altre minacce informatiche. Contrastare efficacemente il rischio è possibile solo a partire da una ***maggior consapevolezza*** e dallo sviluppo di una sensibilità vigile ed attenta capace di valutare e prendere decisioni efficacemente.

La maggior parte degli attacchi infatti si basa sulla fiducia. Così il ransomware arriva da servizi che si utilizzano spesso o da software di aziende conosciute e quindi ritenute affidabili. Altre volte si nasconde in applicazioni che si scaricano da siti non ufficiali, magari per risparmiare il costo della licenza, con il rischio di trovarsi il pc inaccessibile. Sempre molto diffuse sono le e-mail di phishing, che imitando quasi alla perfezione comunicazioni ufficiali di siti e marchi conosciuti, inducono a scaricare un allegato o a cliccare su un link che apre la porta al ransomware.

Infine, altra mezzo di diffusione sono le chiavette USB, nelle quali ovviamente è stato inserito il codice malevolo o l'utilizzo di applicazioni come i desktop remoti. Tutto ciò, unito alla mancanza di un antivirus efficace e di una infrastrutture informatica ben protetta.

I VETTORI DI ATTACCO PIU' COMUNI.

67%

E-MAIL DI PHISHING

30%

CREDENZIALI RUBATE

16%

SITI WEB INFETTI

COME DIFENDERSI

Regole e buone pratiche

Dato che una volta che la cifratura dei dati è avvenuta è praticamente impossibile recuperarli, risulta fondamentale la prevenzione.

Prevenire l'attacco è l'unica arma a disposizione.

Ecco allora alcuni consigli utili:

1. Effettuare un **backup** completo dei dati, anche ogni giorno, e mantenerlo offline affinché non venga interessato da un eventuale attacco.

2. Controllare attentamente le e mail ricevute, verificando il mittente ed evitando di scaricare allegati non conosciuti e di cliccare sui link. Meglio utilizzare Google per cercare un link o raggiungerlo direttamente senza cliccare su quello contenuto nella e-mail.

3. Se si ricevono e-mail che invitano a modificare i propri dati di accesso ad account particolari, evitare di farlo seguendo le indicazioni contenute nel messaggio ma raggiungere il proprio account dal sito ufficiale e verificare se effettivamente il sistema richiede un aggiornamento dei dati.

4. Prestare attenzione ai siti web su cui si naviga, evitando quelli dubbi dai quali scaricare software gratuiti al limite della legalità e controllare sempre i domini per individuare eventuali siti fake.

5. Effettuare gli aggiornamenti periodici dei sistemi operativi per evitare rischi connessi alle vulnerabilità.

6. Utilizzare servizi Anti-Spam e Antivirus aggiornati. Questo vale ovviamente anche per i dispositivi mobili.

Il danno è rapissimo: in soli *4 minuti*, ben 30,000 file di un'azienda sono stati danneggiati.

PHISHING

Riconoscerlo ed evitarlo

Si tratta del metodo di infezione per eccellenza, non solo per i ransomware ma per molte altre minacce informatiche. Si tratta di e-mail truffa formulate appositamente per trarre in inganno gli utenti portandoli a condividere informazioni personali o a compiere azioni che permetteranno al virus di infettare il pc. E nel caso in cui il pc sia quello aziendale, a rischio è l'intera rete e tutti i dispositivi a essa connessi.

Come funzionano le email di phishing.

Queste comunicazioni hanno in genere toni allarmistici finalizzati a mettere fretta, ignorando le comuni e basilari regole di buon senso. Invitano a cliccare su un link o a scaricare allegati i quali conterranno il codice malevolo che infetterà il pc. Per meglio trarre in inganno i criminali simulano aziende o servizi noti, si pensi ad esempio alla bolletta telefonica da scaricare, così che l'utente provi un senso di fiducia verso un brand noto e allo stesso tempo si ritrovi curioso di capire che cosa l'azienda richieda.

Come difendersi.

1. Controllare sempre sia l'indirizzo email del mittente che il link prima di cliccarlo. I domini dei servizi o brand noti non possono essere copiati, pertanto avranno sempre qualche piccola differenza rispetto all'originale. Passando il mouse sopra al link si potrà visualizzare il collegamento effettivo e verificare che sia davvero quello indicato.
2. Verificare sempre il dominio quando si apre per controllare che sia quello effettivo, in ogni caso è sempre meglio evitare di cliccare qualunque cosa nella e-mail ma piuttosto utilizzare i normali motori di ricerca.
3. Spesso i criminali informatici utilizzano indirizzi e-mail di amici o colleghi (in precedenza violati); meglio diffidare di comunicazioni anomale con link o allegati che non erano attesi e controllare con il diretto interessato.
4. Utilizzare un Antivirus che offra una protezione adeguata.
5. Non aprire e-mail che finiscono dello SPAM.

IN CASO DI INFEZIONE

Cosa fare

In caso di attacco riuscito, non c'è molto in realtà da fare. Ma qualcosa è possibile tentare per non perdere definitivamente i propri dati.

1. Ripristinare i dati tramite il **backup.** Se si è provveduto ad effettuare backup periodici, dopo aver bonificato il pc infetto, si può procedere al ripristino dei file. Questa è ovviamente la soluzione migliore e auspicabile.

2. Cercare in rete un **decryptor**. Sono programmi realizzati dagli esperti informatici in grado di recuperare i file criptati. Infatti, data la grande proliferazione dei ransomware, molte aziende di sicurezza sono riuscite nel tempo a trovare la soluzione per alcuni particolari tipi di minacce. Attenzione però ai falsi decrypter. In rete sono disponibili anche false soluzioni che in realtà effettuano una doppia cifratura! Fidarsi solo dei canali ufficiali.

3. Accettare di **perdere i dati**. Se ciò che è andato perduto in fondo non è così importante in molti casi può anche essere la scelta migliore, per non perdere ulteriori risorse, aumentando il danno.

QUALUNQUE COSA SI DECIDA DI FARE SE SI E' STATI INFETTATI DA UN RANSOMWARE, PAGARE IL RISCATTO NON E' MAI LA SCELTA MIGLIORE.

Non sempre i dati vengono davvero recuperati, o non tutti, e si contribuisce ad alimentare il crimine informatico.