Malware types

Iniziamo con la definizione di malware ed in particolar modo, abbiamo che il malware è essenzialmente un software malevole, che compie azioni che possono andare a compromettere le proprietà di sicurezza di base di un sistema informativo, ovverosia:

- disponibilità;
- integrità;
- riservatezza;
- safety (intesa come sicurezza delle persone).

Quali sono queste azioni malevole? Alcuni esempi sono i seguenti:

- rubare informazioni sensibili (quali ad esempio credenziali o dati di carte di credito);
- cifrare i dati;
- rendere un sito web non raggiungibile ai propri utenti.

Sorge un'altra domanda: "Come fanno i malware ad infettare il sistema o le reti?" Vi sono due macro-categorie, ovverosia:

1. La prima macro-tecnica coinvolge l'utilizzo di tecniche di ingegneria sociale → per quanto riguarda le tecniche di ingegneria sociale, abbiamo già detto, che si può infettare un sistema esistente:
    a. mandando delle email di phishing più o meno personalizzate;
    b. oppure utilizzare la tecnica del Drive-by-Compromise → ovverosia andare a compromettere un sito, che i dipendenti dell'azienda vanno a visitare continuamente, in cui viene installato uno script, il quale va a scaricare il malware nelle macchine delle vittime;
    c. oppure si possono utilizzare delle tecniche di ingegneria sociale, per andare a convincere le vittime ad utilizzare una chiavetta USB infetta da un malware.
2. La seconda macro-tecnica coinvolge lo sfruttamento di vulnerabilità, le quali possono essere presenti:
    a. nei dispositivi connessi alla rete dell'azienda o dell'organizzazione obiettivo dell'attacco;

b. nei servizi o nel sistema operativo delle macchine.

Diamo ora, una rapida panoramica delle **principali categorie di malware presenti**:

- Tra le prime tipologie di malware presenti in circolazione (intorno agli anni ‘90), vi erano i **Virus**. I virus erano un tipo di malware in grado di replicarsi solamente se l’utente svolgeva determinate azioni. Un esempio di virus era ILOVEYOU, il quale riusciva a propagarsi, inviando email a tutti i contatti della vittima, quando l’utente apriva l’email infettata dal virus. In circolazione, abbiamo tre principali categorie di virus, ovverosia:
  - **Macro** → virus implementati attraverso le macro. Abbiamo detto, che uno dei veicoli per l’installazione dei malware sono i documenti Office, i quali contengono del codice malevole, ovvero delle macro EPA. In questo caso, il virus è implementato dalla macro stessa, la quale quindi va a scaricare il malware nella macchina delle vittime;
  - **Polymorphic** → abbiamo virus polimorfici, ovverosia che possono adattare il proprio comportamento a seconda del sistema operativo o della piattaforma su cui vengono eseguiti, in maniera tale da evadere l’identificazione del software antivirus;
  - **Companion** → abbiamo, infine, i virus detti Companion, in quanto solitamente si mascherano ad un software legittimo, che tipicamente viene installato sulla macchina target (ovvero della vittima) → per esempio il classico aggiornamento di Windows.
- Un’altra tipologia di malware sono i **Worms** → I worms sono una variante più evoluta dei virus, in quanto i worms per diffondersi non hanno bisogno di un’azione compiuta dall’utente, bensì possono propagarsi ad altre macchine presenti sulla rete sfruttando vulnerabilità presenti nei dispositivi o nelle reti. Da notare, che i worms da soli, non sono più diffusi nelle campagne di distribuzione dei malware, bensì solitamente sono una componente di altri virus;
- Altra tipologia di malware sono i **Key loggers** → I Key loggers ci consentono di catturare qualsiasi carattere che viene digitato sulla tastiera delle vittime. I Key loggers, quindi, diventano molto utili nel momento in cui, l’attaccante vuole rubare l’username e la password, per successivamente ottenere l’accesso ad altri servizi utilizzati dall’utente. Nella versione basica (ovvero quella più semplice), i Key loggers salvano i caratteri digitati sulla tastiera dall’utente in un file di testo e periodicamente li manda, tramite email o altri canali di Command and Control (come ad esempio: servizi Cloud), all’attaccante;

- Una categoria molto diffusa ultimamente sono i **Remote Access Trojans (RATs)** → tipologia di malware utilizzata principalmente nella fase di Installation della Cyber Kill Chain, in quanto in questa fase, tipicamente l'attaccante vuole mantenere l'accesso che ha ottenuto alla macchina. Il RAT è stato progettato per consentire a un utente malintenzionato di controllare da remoto una macchina e per fare ciò, creerà un canale di Command and Control (C2) con il Server dell'attaccante, attraverso il quale sarà possibile inviare comandi al RAT e inviare dati in risposta. I RATs dispongono in genere di una serie di comandi integrati e di metodi per nascondere il loro traffico C2 al rilevamento. Infine, abbiamo che i RATs possono essere integrati con funzionalità aggiuntive o progettati in modo modulare per fornire capacità aggiuntive in base alle necessità.
- Un'altra categoria abbastanza diffusa negli ultimi anni sono i **Trojans** → i Trojans sono nati proprio per rubare informazioni confidenziali dalla macchina delle vittime. Inizialmente, in particolare, essi erano finalizzati a rubare solo informazioni di carattere finanziario (come per esempio credenziali per accedere a servizi di online banking o ai propri wallet). Con il tempo, anche i Trojans si sono sempre più evoluti e anch'essi sono diventati uno strumento organizzato in moduli, nel senso che forniscono diverse funzionalità (come per esempio: rubare credenziali, fare lateral movement o per installare altri malware). Spesso i Trojans vengono scaricati da siti web non ufficiali ed essi creano una backdoor, che consente agli hacker di controllare la macchina della vittima;
- Un'altra categoria è quella dei **Rootkits** → i Rootkits danno l'accesso di root alla macchina delle vittime. Essi possono essere implementati in diversi modi ed in particolare quello più insidioso è il cosiddetto kernel Rootkit, il quale è installato nel kernel del sistema operativo. Essendo nel SO, il kernel Rootkit non solo viene utilizzato come strumento per ottenere l'accesso di amministratore nella macchina, bensì viene utilizzato anche per nascondere la presenza di altri malware, i quali potrebbero aver infettato la macchina. Perchè i kernel Rootkit sono i più insidiosi? Perchè essendo installati nel kernel del SO, per eliminarli è necessario rimuovere ed installare nuovamente il SO (in realtà, a volte, nemmeno questo può essere sufficiente);
- Un'altra categoria è quella dei **Droppers** o dei **Downloaders** → i Droppers sono dei malware, che hanno come obiettivo di far arrivare sulla macchina delle vittime altre tipologie di malware, tra cui i Ransomware (categoria di malware che vedremo tra poco). La forma più comune dei Droppers è implementata tramite documenti Office o documenti PDF malevoli, che contengono codice JavaScript per:

    - connettersi ai Command and Control Server;
    - scaricare il file eseguibile;
    - lanciare l’eseguibile sulla macchina.

  Esistono anche altre forme di Droppers, che contengono l’eseguibile all’interno del processo stesso. Tipicamente, i Droppers nascondono i malware, che devono installare nella macchina delle vittime, all’interno delle risorse del file → vi sono, quindi, delle Windows API che consentono ai malware di recuperare il file contenuto nelle risorse ed installarlo sulla macchina della vittima e lanciarlo;

- Un’altra categoria sono i **Bots** (o **Botnet**) → i Bots sono una tipologia di malware, che trasforma le macchina che vengono infettate in macchine sotto il controllo dell’attacccante. Un po’ come abbiamo visto con i RATs, i Bots sono macchine che agiscono sulla base dei comandi che gli vengono inviati dai C2 Server diretti dagli attaccanti. Ad oggi, i Bots sono uno dei malware più diffusi e vengono utilizzati per costruire delle reti di macchine infette controllate dagli attaccanti. Vengono utilizzati per lanciare due tipologie di attacchi:
    - Distributed denial-of-service attack (DDoS attack) → l’attaccante attraverso i C2 Server invii ai vari bot la richiesta di eseguire il comando di **ping** verso l’obiettivo dell’attacco (come per esempio uno specifico sito web o un Server). L’elevato volume di traffico generato dai vari bot, va ad esaurire le risorse computazionali e di memoria della macchina su cui è ospitato il sito web o il Server, che è obiettivo dell’attacco;
    - Distribuzione di spam dannoso → ovverosia i bot vengono utilizzati come infrastruttura per distribuire altri malware, tra cui principalmente RATs e Ransomware.

  I bots sono una categoria di malware sempre più diffusa, in quanto uno dei trend in comune tra varie categorie di attaccanti, è quello di andare ad utilizzare come iniziale punto di accesso nella rete delle vittime dispositivi IoT → infatti, le principali categorie di botnet in circolazione, sono specializzate nell’attaccare dispositivi Iot;

- Un’altra categoria diffusa sono i **Cripto Miners** → la maggior parte dei Crypto Miner non sono altro, che software di mining di criptovalute open source riproposti. In particolare, abbiamo che i dispositivi infettati vengono utilizzati, o meglio dire le risorse computazioni della macchina infettata, vengono utilizzate per creare delle nuove crypto valute, le quali vengono inviate al wallet

dell’aggressore. Solitamente questa categoria di malware, si diffonde attraverso botnet o malspam;

- Infine abbiamo i **Ransomware** → i Ransomware sono la categoria di malware più diffusa e nella loro versione base, i Ransomware è una tipologia di malware, che non fa altro che rendere i file disponibili su una macchina non accessibili agli utenti, in quanto essi vengono cifrati e si chiede alle vittime di pagare un riscatto per ottenere la chiave di decrifratura.

Le principali tipologie di malware diffuse su macchine Windows sono:

- Botnet;
- Infostealer → ci consentono di rubare credenziali che possono essere utili per ottenere l’accesso iniziale alle macchine delle vittime;
- RATs;
- Ransomware.

Al giorno d’oggi, anche macchine Linux e MacOs sono obiettivi d’attacco.

Come prevenire un attacco malware

L’approccio che dobbiamo utilizzare è di **sicurezza in profondità** (Security in Depth), ovverosia dobbiamo applicare diversi livelli di misure di protezione. In particolare, il nostro obiettivo è quello di:

1. Tentare di bloccare l’attacco prima che arrivi sulla macchina, ovvero bloccare qualsiasi tecnica che favorisca l’installazione del malware sulla macchina;
2. Vogliamo prevenirne l’esecuzione sulla macchina, ovvero il malware è arrivato sulla macchina e di conseguenza ne vogliamo bloccare la sua esecuzione;
3. Vogliamo limitare i danni una volta che il malware è arrivato sulla macchina.

Procedendo in ordine, ci chiediamo: Come facciamo a bloccare un malware? Abbiamo detto, che la principale metodologia con cui un malware viene consegnato sulla macchina è il phishing. Il phishing ha due modalità per portare all’installazione del malware sulla macchina delle vittime, ovvero:

1. contiene un link, da cui viene scaricato il malware;
2. ha un allegato malevolo, che deve essere aperto.

Dobbiamo, quindi, impedire all’utente in un qualche modo di cliccare sul link o di aprire l’allegato. Per fare questo, dobbiamo fare in modo, che l’email non arrivi

proprio all’utente e quindi si può adottare l’utilizzo dei classici software di spam filtering. Possiamo, anche impedire la navigazione verso siti che sono considerati malevoli, quindi possiamo utilizzare proxy di intercettazione, che bloccano i siti web considerati pericolosi o non attendibili e utilizzare delle white list, ovvero degli elenchi di navigazione sicura all’interno dei browser web, che possono impedire l’accesso a siti che ospitano contenuti dannosi.

Come facciamo, invece, a prevenire l’esecuzione dei malware? Certamente un primo modo è quello di scaricare software solamente da siti certificati. Un’altra cosa che si può fare, è quella di andare a disabilitare la funzione di autorun per i supporti montati (quali ad esempio chiavette USB). Un’altra cosa è di disattivare o limitare gli ambienti di scripting e le macro, come Powershell e le macro di Microsoft Office. Infine, installare le ultime versioni dei SO e delle applicazioni, al fine di sfruttare le più recenti funzionalità di sicurezza e monitorare il traffico di rete e adottare un firewall.

Se, invece, vogliamo evitare che il malware si diffonda alle altre macchine della rete, una delle prime cose da fare è adottare l’autenticazione a più fattori, in quanto nelle fasi successive all’installazione, una delle tecniche che gli attaccanti possono usare, è quella di creare o rubare nuovi account presenti sulla macchina infetti o cercare account per accedere alle altre macchine presenti sulla rete. Altre azioni da compiere sono:

- garantire che le piattaforme obsolete (sistemi operativi e applicazioni) siano adeguatamente segregate dal resto della rete;
- rivedere regolarmente e rimuovere le autorizzazioni degli utenti non più necessarie, per limitare la capacità di diffusione del malware;
- assicurarsi che gli amministratori di sistema evitino di utilizzare i loro account per la posta elettronica e la navigazione web (per evitare che il malware possa essere eseguito con il loro elevato livello di privilegi di sistema);
- tenere traccia di quali versioni del software sono installate sui dispositivi, in modo da poter eseguire rapidamente gli aggiornamenti di sicurezza.

Soprattutto, **per prevenire ed evitare la diffusione dei malware, è necessario istruire i dipendenti dell’azienda su quali sono i principali attacchi** a cui l’azienda può essere soggetta in base al settore in cui opera e su cosa possono fare i dipendenti stessi per prevenire l’attacco ed eventualmente per bloccarlo.

Inoltre, un ulteriore aspetto per prevenire i malware ed in particolare i Ransomware, è quello che le aziende devono avere un meccanismo regolare di backup. In

particolare, l’azienda dovrebbe assicurarsi di:

- creare backup offline che siano tenuti separati, in un luogo diverso (idealmente fuori sede), dalla vostra rete e dai vostri sistemi, o in un servizio cloud progettato per questo scopo;
- eseguire più copie dei file utilizzando diverse soluzioni di backup e luoghi di archiviazione;
- assicurarsi che i dispositivi contenenti il backup (come dischi rigidi esterni e chiavette USB) non siano costantemente collegati alla rete;
- assicurarsi che i backup siano collegati solo a dispositivi noti e puliti prima di avviare il ripristino;
- eseguire la scansione dei backup alla ricerca di malware prima di ripristinare i file.

Infine, se il malware ha già infettato l’azienda i passaggi consigliati da svolgere sono i seguenti:

1. Scollegare immediatamente i dispositivi infetti;
2. Spegnete il vostro Wi-Fi, disabilitando tutte le connessioni di rete principali (compresi gli switch);
3. Reimpostare le credenziali, comprese le password (in particolare per gli account di amministratore e altri account di sistema);
4. Cancellare in modo sicuro i dispositivi infetti e reinstallare il sistema operativo;
5. Prima di ripristinare da un backup, verificare che sia privo di malware;
6. Collegare i dispositivi a una rete pulita per scaricare, installare e aggiornare il sistema operativo e tutti gli altri software;
7. Installare, aggiornare ed eseguire il software antivirus;
8. Riconnettersi alla rete;
9. Monitorare il traffico di rete ed eseguire scansioni antivirus per identificare eventuali infezioni.

Attacchi Ransomware

Abbiamo già dato una definizione base dei Ransomware, ovverosia un malware che va a cifrare i dati sulla macchina delle vittime e in cambio chiede un riscatto per dare

alle vittime la chiave di cifratura. Però, questa non è l'unica categoria di Ransomware, in quanto quest'ultimi si sono evoluti nel tempo.

In particolare, abbiamo:

- I **Lockers** → categoria di Ransomware che loggava fuori dal computer gli utenti, faceva visualizzare un messaggio e chiedeva un riscatto per ridare agli utenti accesso al proprio computer. I Lockers, quindi, andavano a compromettere il processo di login dell'utente alla propria macchina;
- I Ransomware che vanno a compromettere il **Master Boot Record** della macchina che viene infettata e andando a compromettere il Master Boot Record o cifrandolo o modificando il file, si rende la macchina non più riavviabile (ovvero non più boottabile).;
- I **Wipers** → l'obiettivo di questa tipologia di malware non è quello di andare a rendere i dati non disponibile agli utenti cifrandoli, bensì cancellandoli e quindi, anche se le organizzazioni colpite dovessero avere dei backup, quest'ultimi non servirebbero a nulla, in quanto i Wipers molto spesso vanno a cancellare anche i backup.

Nella loro forma base, i Ransomware hanno quattro moduli principali:

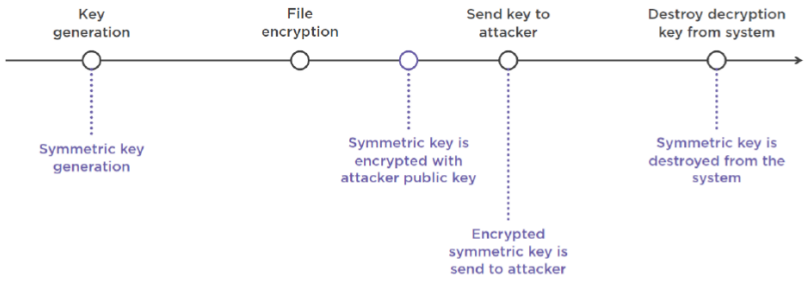
1. Un primo modulo, che implementa i meccanismi che consentono al Ransomware di arrivare sulla macchina delle vittime → tale modulo, quindi, implementa le tecniche di delivery e di conseguenza si occuperà di:
    a. **generare le email di phishing** con i relativi allegati malevoli, i quali (ovvero gli allegati malevoli) scaricano il malware sulla macchina;
    b. **implementare un exploit**, quindi del codice, che sfrutta le vulnerabilità del target;
    c. **compromettere siti web esistenti** per scaricare i ransomware sulla macchina delle vittime.

2. Poi abbiamo il meccanismo, ovverosia la routine, che si occupa della cifratura e della decifratura dei file → tale modulo utilizza le due principali tecniche di cifratura che abbiamo attualmente, ovvero:
    a. la cifratura a chiave simmetrica, per cifrare effettivamente i file sulla macchina delle vittime → la cifratura a chiave simmetrica utilizza la stessa chiave per cifrare e decifrare il file e conseguentemente è molto più veloce nella fase di cifratura del file, rispetto alla cifratura a chiave pubblica;
    b. la cifratura a chiave pubblica → viene utilizzata per proteggere la chiave simmetrica, che viene utilizzata per cifrare i file ed in particolare per distribuire agli attaccanti la chiave simmetrica utilizzata per la cifratura. In particolare, abbiamo che la chiave simmetrica viene cifrata con la chiave pubblica dell'attaccante e quest'ultimo riesce a decifrarla attraverso la sua chiave privata.

    Quindi, tutto il processo di cifratura (che avviene ovviamente sulla macchina delle vittime) è il seguente:

    1. inizia con la generazione della chiave di cifratura;
    2. dopodiché tutti i file oppure i file con una determinata estensione vengono cifrati sulla macchina delle vittime;
    3. la chiave viene cifrata con la chiave pubblica dell'attaccante e può essere distribuita all'attaccante tramite il C2 channel;
    4. la chiave cifrata, a questo punto, viene inviata agli attaccanti;
    5. infine la chiave generata viene distrutta, perchè se i security analists che lavorano per l'organizzazione colpita riescono a recuperare la chiave, l'organizzazione non ha la necessità di pagare il riscatto.

    Il seguente processo può essere osservato meglio nell'immagine riportata sotto:



3. Abbiamo il modulo, che si occupa della:

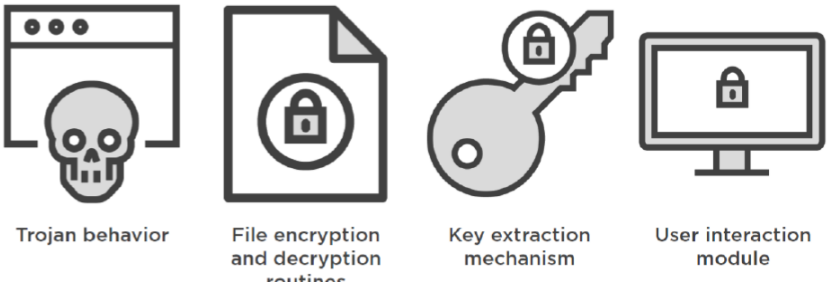
a. generazione della chiave che viene utilizzata per la cifratura;

b. e di dare la chiave di cifratura agli attaccanti.

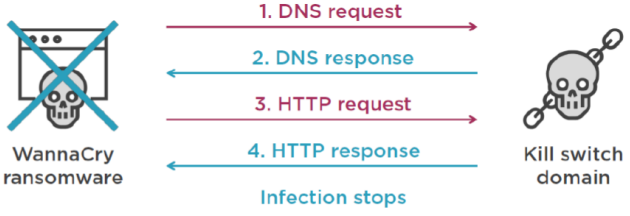
4. Abbiamo il modulo responsabile dell'interazione tra le vittime e gli attaccanti → tale modulo può essere:

   a. una semplice interfaccia, che mostra alle vittime le istruzioni per pagare il riscatto;

   b. un'interfaccia con delle funzionalità più complesse.

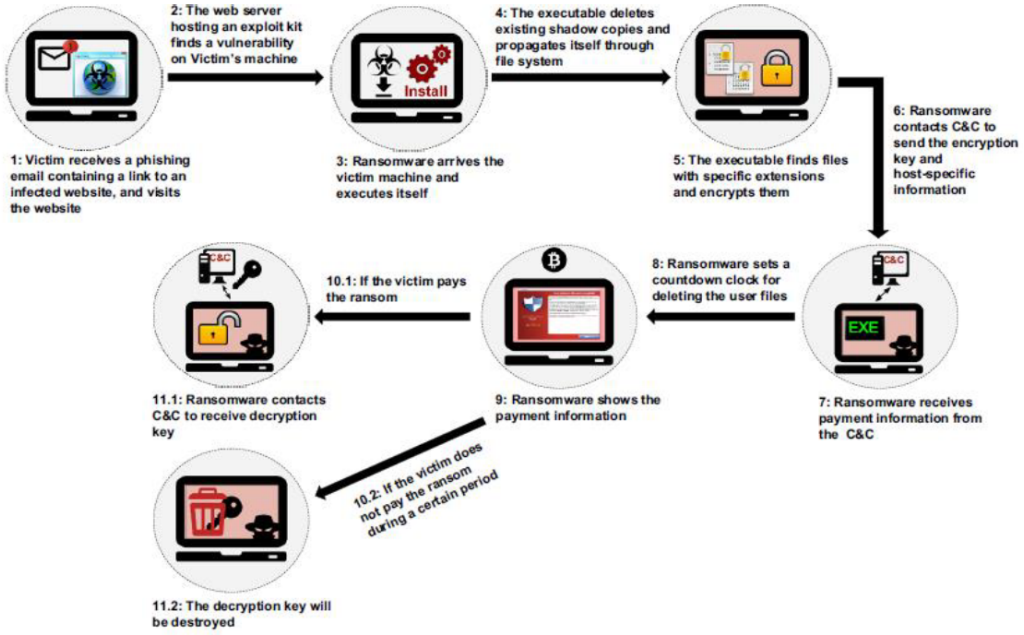


Un'altra componente fondamentale presente nei primi ransomware era il cosiddetto **Kill Switches**, ovverosia una funzionalità per impedire la propagazione dei ransomware e di conseguenza impedire l'infezione. Implementati dagli autori di malware per evitare di infettare la propria infrastruttura. Il Kill Switch più famoso era **WannaCry**, in quanto è andato a colpire target molto noti, quali ad esempio il servizio nazionale sanitario inglese. Tale Kill Switch è stato scoperto da un ricercatore della sicurezza inglese, il quale facendo reverse engineering del codice di WannaCry, si accorse che ad un certo punto il codice andava a fare un controllo, ovvero andava a verificare se esisteva un determinato dominio. In particolare, se il dominio esisteva e la richiesta HTTP fatta verso questo dominio aveva successo, WannaCry stoppava il suo funzionamento. Facendo questa scoperta, il ricercatore registrò il dominio a suo nome e di conseguenza ha bloccato tutte le infezioni di WannaCry.



Per quanto riguarda la Cyber Kill Chain, abbiamo detto che principalmente i Ransomware vengono consegnati mediante attacchi di ingegneria sociale, quindi presumibilmente nella fase di Recognize, possiamo immaginare che gli attaccanti vadano a raccogliere informazioni sugli indirizzi email delle vittime a cui inviare email di phishing. Supponendo, che poi si utilizzi la tecnica di Drive-by-Compromise, ovvero andare a compromettere un sito visitato dalle vittime, l'email conterrà un link a questo sito e nel momento in cui le vittime cliccano su tale link, esse vengono ridirette sul sito e il malware viene scaricato sulla macchina. Dopodichè, in alcuni casi, il Ransomware può tentare di eliminare la possibilità delle organizzazione di recuperare i dati, quindi il Ransomware tenta di trovare ed eliminare eventuali copie di backup dei file. Successivamente abbiamo la fase di cifratura vera e propria dei file e a questo punto, il Ransomware stabilisce un canale di comunicazione con il C&C Server da cui riceve le istruzioni per pagare il riscatto. A questo punto la cifratura è terminata, la nota di riscatto viene visualizzata sul computer delle vittime e da questo momento vi sono due strade possibili:

1. la vittima paga il riscatto e quindi la vittima ottiene la chiave di decifratura → in realtà si è scoperto, che se anche le vittime pagavano il riscatto, alcune volte non ricevevano la chiave di decifratura;
2. la vittima NON paga il riscatto e di conseguenza la chiave di decifratura viene eliminata e quindi le vittime non hanno più possibilità di recuperare i dati cifrati.



Questa era la classica Cyber Kill Chain fino a pochi anni fa. Diciamo ciò, perchè negli ultimi 3 anni la situazione si è complicata molto, in quanto:

- le vittime hanno capito che se hanno un meccanismo di backup ben funzionante, esse non sono obbligate a pagare il riscatto;
- le vittime hanno aumentato i meccanismi di difesa per identificare e prevenire queste tipologie di attacchi.

Questo ha portato a come conseguenza, che le vittime pagavano con sempre meno frequenza i riscatti. Di conseguenza gli attaccanti hanno dovuto trovare delle nuove modalità/tecniche di estorsione. Un primo esempio di queste nuove tecniche era che, oltre a cifrare i dati sulla macchina delle vittime, prima di cifrarli, abbiamo che una parte dei dati sensibili (quali ad esempio informazioni relative ai clienti o ai prodotti) venivano salvati sul C&C Server degli attaccanti e se dopo pochi giorni le vittime si rifiutavano di pagare, gli attaccanti minacciavano di rendere le informazioni pubbliche → questa tecnica prende il nome di **doppia estorsione**. Nell'ultimo anno, si è passati anche a tecniche di tripla o quadrupla estorsione, in cui gli attaccanti oltre a cifrare i dati, minacciare di rendere le informazioni pubbliche, gli attaccanti hanno iniziato a chiamare i clienti e/o i fornitori delle organizzazioni attaccate, dicendogli che i propri dati erano stati rubati e che sarebbero stato resi pubblici → il riscatto quindi veniva anche chiesto direttamente ai clienti e/o ai fornitori dell'organizzazione e se il riscatto non veniva pagato, gli attaccanti minacciavano di bloccare i servizi dell'organizzazione attaccata.

Inoltre, oltra a migliorare le tecniche di estorsione, sono state anche migliorate le tecniche di cifratura dei file., ovverosia si è adottata una **cifratura ad intermittenza**, attraverso la quale non viene cifrato l'intero file, bensì vengono cifrato solamente dei blocchi del file, in modo da renderlo comunque inutilizzabile → questo velocizza di molto la cifratura dei file. Un'altra tecnica che sta prendendo piede è quella di non cifrare più i file sulla macchina delle vittime, dato che i file vengono salvati C&C Server per minacciare le vittime di renderli pubblici, i file vengono cifrati direttamente sul Server e poi rimandati sulla macchina delle vittime.

Un'altra novità sta nel processo di negoziazione. Tipicamente i primi ransomware (come WannaCry) andavano semplicemente a visualizzare la nota del riscatto, dicendo che se volevano avere la chiave di decifratura, dovevano pagare un riscatto all'indirizzo specificato → con l'introduzione delle nuove tecniche di estorsione, anche il processo di negoziazione si è industrializzato. L'esempio cardine/principale di tale processo di industrializzazione è **Lockbit**, il quale ha realizzato un portale di negoziazione, ovverosia quando le vittime vengono infettate, nella nota di riscatto non vi è più l'indirizzo per pagare il riscatto, bensì vi è l'indirizzo ad una chat di messaggistica. Inoltre nel portale:

- vengono resi pubblici i dati rubati dalle macchine delle vittime;
- vengono forniti dei servizi di aste, in modo tale che altri cybercriminali possano acquistare i dati rubati.

Sta cambiando anche il **target**, perchè oltre ad avere come obiettivo i dispositivi IoT, si sta mirando a compromettere anche Server Cloud. In particolare, quest'anno molte campagne ransomware hanno sfruttato una vulnerabilità presente negli ESXi Server (in particolare era una vulnerabilità legata alla gestione della memoria), grazie alla quale gang cybercriminali sono riuscite ad installare ransomware su questi Server.

→ un'altra cosa interessante è legata a LockBit, in quanto quest'ultimo ha aperto un Bug Bounty Program, ovverosia un programma che paga ricercatori e sviluppatori per trovare vulnerabilità nel codice nel codice di un software delle aziende.

Tecniche utilizzate dai ransomware

Un'azienda olandese opeante nel settore della cybersecurity, ha analizzato le principali tecniche utilizzate dalle gang di cybercriminali operanti attualmente. In particolare, abbiamo che:

- Nella fase iniziale, quindi nell'Initial Access, i ransomware vengono deliberati mediante:
  - email di phishing → quindi, gli attaccanti inviano email di phishing con allegati dannosi o link a siti web che ospitano malware;
  - sfruttano vulnerabilità presenti in servizi, come per esempio Remote Desktop Protocol (RDP), presenti di default su tutte le macchine Windows;
  - sfruttare vulnerabilità nei servizi offerti su internet dalle organizzazioni.
- Passiamo poi alla fase di Execution, in cui i ransomware possono essere eseguiti in diverse modalità:
  - se l'attacco è iniziato attraverso una email di phishing, l'azione che deve essere eseguita è che l'utente clicca sul link presente nell'email, oppure apre l'allegato malevolo;
  - se, invece, l'accesso iniziale è stato tramite una vulnerabilità presente nella macchina delle vittime, allora il malware può essere eseguito attraverso tecniche che prevedono l'utilizzo di funzionalità presenti sulla macchina Windows. Le due principali modalità sono:

        - l’utilizzo della Windows Command Shell → consente di eseguire qualsiasi tipologia di comando;
        - l’utilizzo di PowerShell → consente di eseguire task e lanciare operazioni sulla macchina Windows.
- La fase successiva è quella di Persistence, la quale comprende tutte le tecniche che vengono adottate per mantenere l’accesso sulla macchina una volta che lo abbiamo ottenuto. Tra le tecniche più utilizzate dai ransowmare vi è:
    - la creazione di un task, il quale viene eseguito periodicamente sulla macchina delle vittime. Il task viene implementato dal codice del malware stesso;
    - la manipolazione dell’account → questa tecnica comprende azioni, quali la modifica delle credenziali dell'account o dei gruppi di autorizzazioni e il sovvertimento dei criteri di sicurezza, come l'aggiornamento ripetuto delle password per aggirare i criteri di durata delle password;
    - creare o modificare un processo di sistema → ovverosia andare a stabilire la persistenza creando o alterando processi a livello di sistema, che eseguono ripetutamente payload dannosi. Questi processi possono essere avviati dal sistema operativo durante l'avvio e sono noti come servizi in Windows e Linux;
    - esecuzione dell’avvio automatico di boot o logon → garantisce l’esecuzione continua del malware sulla macchina infetta, andando a modificare i registri (come per esempio i registri di Windows).
- Nella fase di Installation, oltre che alla persistenza, vogliamo anche elevare i privilegi (ovvero vogliamo ottenere i privilegi di root o di amministratore). I principali modi per fare ciò sono:
    - Exploitation for Privilege Escalation → ovverosia gli attaccanti possono utilizzare le vulnerabilità del software per ottenere l'escalation dei privilegi. Quando un attaccante sfrutta una vulnerabilità software, approfitta di un errore di programmazione in un programma, un servizio o un kernel del sistema operativo per eseguire il proprio codice;
    - riutilizzare software legittimo di Microsoft per eseguire il malware o comunque garantire l’esecuzione del malware;
    - adottare tecniche per nascondere che il ransomware è malevole, come ad esempio:

        - rinominare il file con il nome di un processo legittimo di Windows;
        - modificare i metadati associali al file (come ad esempio la data di creazione);
        - modificare le proprietà del file.
- Le tecniche più interessanti sono quelle che permettono al ransomware di non essere identificato sulla macchina delle vittime. Queste tecniche vanno a far sì, che il codice del malware venga eseguito nello spazio di memoria di un altro processo. Quando carichiamo un processo su una macchina Windows, gli viene allocato un'area di memoria, dove vengono copiate tutte le librerie (le cosiddette DLL), che implementano le funzionalità eseguite dal codice del ransomware. Vi sono diverse tecniche che permettono ciò:
    - DLL Injection → viene utilizzata per eseguire codice nello spazio degli indirizzi di un processo attivo. Ciò si ottiene scrivendo prima il percorso di una DLL nello spazio degli indirizzi virtuali del processo bersaglio e poi caricando la DLL invocando un nuovo thread;
    - Process hollowing → consiste nel creare un processo in stato di sospensione e successivamente disinstallare o svuotare la sua memoria, consentendo di sostituirla con codice dannoso;
    - Thread execution hijacking → viene utilizzato per eseguire codice arbitrario nello spazio degli indirizzi di un processo attivo. Per eseguire questa tecnica, un processo esistente viene dapprima sospeso e la sua memoria viene poi disassemblata, consentendo l'iniezione di codice dannoso o il percorso di una DLL;
    - altre tecniche riguardano di ostacolare le misure antivirus oppure di andare a cancellare i log o andare a cancellare direttamente i file.
- Per fare lateral movement, abbiamo poi bisogno di scoprire nuove credenziali di macchine collegate alla macchina infetta o collegate alla rete aziendale. Per scoprire nuove credenziali si può ricorrere a:
    - alla forza bruta → gli attaccanti possono utilizzare la forza bruta per ottenere l'accesso agli account indovinando iterativamente le password;
    - oppure vi sono tecniche che accedono ai file che memorizzano le password → ad esempio, il Security Account Manager (SAM) è un database di Windows che memorizza gli account utente.

- Infine, nella fase di Discovery, abbiamo che gli attaccanti raccolgono informazioni/credenziali per infettare altre macchine. Questo lo possono fare andando, ad esempio, a listare tutti gli utenti connessi alla macchina infetta, oppure listare tutti gli utenti che sono associati allo stesso dominio della macchina infetta. Conoscendo gli username è possibile, poi, utilizzare le stesse tecniche per ottenere le credenziali. Gli attaccanti, vogliono anche scoprire altre macchine sulla rete e di conseguenza adottano tecniche di Network Service Discovery.

Abbiamo, quindi, che i ransomware possono avere due principali conseguenze:

1. Gli attaccanti interrompono la disponibilità e compromettono l'integrità delle risorse di sistema e di rete crittografando i dati sui sistemi di destinazione, rendendoli inaccessibili agli utenti. Per ottenere l'accesso ai dati crittografati, gli avversari chiedono un riscatto in cambio della chiave di decrittazione;
2. Gli avversari possono rimuovere o eliminare i dati essenziali del sistema operativo e disattivare i servizi di ripristino progettati per aiutare a ripristinare un sistema compromesso.