zscaler™ | ThreatLabz

ThreatLabz: Report del 2022 Ultimi dati sui ransomware

Contenuti

Introduzione

Se sembra che i ransomware siano sempre al centro delle notizie, non è solo perché i media hanno deciso di interessarsene di più: ThreatLabz, il team di ricerca di Zscaler, ha scoperto che, rispetto all'anno precedente, gli attacchi ransomware sono aumentati di un ulteriore 80% tra febbraio 2021 e marzo 2022, stabilendo così nuovi record, sia per il volume degli attacchi che per il costo dei danni causati.

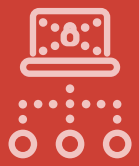
L'interesse degli utenti malintenzionati per i ransomware continua a crescere, perché questi strumenti dannosi consentono loro di condurre campagne sempre più redditizie sfruttando tre tendenze principali:

Gli attacchi alla catena di approvvigionamento

che sfruttano le relazioni con i fornitori di fiducia per violare le organizzazioni, moltiplicare i danni degli attacchi e colpire più vittime (a volte centinaia o migliaia) contemporaneamente.

I ransomware as a service

che utilizzano le reti di affiliati per distribuire ransomware su vasta scala. In questo modo, gli hacker esperti di violazione delle reti possono condividere i profitti con i gruppi di ransomware più avanzati.



Gli attacchi a estorsione multipla

che utilizzano il furto di dati, gli attacchi DDoS (Distributed Denial of Service), comunicazioni con i clienti e altro come tattiche di estorsione stratificate per incrementare gli introiti dei riscatti.

Queste tattiche possono essere molto dannose. Gli esperti del settore prevedono che nel 2022 i ransomware rappresenteranno la principale strategia impiegata nelle violazioni che coinvolgono terze parti e negli attacchi alla catena di approvvigionamento, e che il costo globale dei danni che causeranno salirà a 42 miliardi di dollari entro il 2024.

Queste tendenze hanno reso i ransomware un problema di sicurezza informatica ancora più prioritario per le organizzazioni di tutti i settori. Il report dei CISO di Aimpoint del 2022 ha riscontrato che i ransomware rappresentano la minaccia più preoccupante per i CISO in tutto il mondo.

Come identificare e difendersi dalle più recenti varianti di ransomware? Questo report ti aiuterà a scoprirlo.

ThreatLabz analizza i dati di oltre 200 miliardi di transazioni giornaliere, 150 milioni di attacchi bloccati ogni giorno attraverso Zero Trust Exchange di Zscaler, e delle informazioni sulle minacce raccolte da Zscaler ThreatLabz, per monitorare le principali famiglie di minacce, identificare le tendenze emergenti e migliorare le protezioni per i clienti di Zscaler. In questo report, ThreatLabz ha esaminato i dati sui ransomware raccolti dal 1° febbraio 2021 al 31 marzo 2022 per identificare le famiglie di ransomware più prolifiche e le tattiche che utilizzano. Condivideremo i nostri risultati, le nostre previsioni e le nostre indicazioni su come è meglio agire per definire delle strategie di difesa dai ransomware.

Risultati principali

Gli attacchi ransomware sono aumentati dell'80% dall'anno precedente, e rappresentano tutti i carichi utili di ransomware osservati nel cloud Zscaler.

I ransomware a doppia estorsione sono aumentati del 117%. Questo indica che un numero sempre maggiore di attacchi include il furto dei dati. Alcuni settori hanno registrato una crescita particolarmente elevata di questi attacchi, tra cui l'assistenza sanitaria (643%), la ristorazione (460%), l'estrazione mineraria (229%), l'istruzione (225%), i media (200%) e il settore manifatturiero (190%).

Il settore manifatturiero ha subito quasi il 20% del totale degli attacchi ransomware a doppia estorsione, ed è stato il settore più colpito per il secondo anno consecutivo.

Gli attacchi ransomware alla catena di approvvigionamento sono in aumento, così come anche altri tipi di attacchi che prendono di mira questi obiettivi. Sfruttando i fornitori di fiducia, gli aggressori sono in grado di violare contemporaneamente un gran numero di organizzazioni, comprese quelle che dispongono di protezioni solide contro gli attacchi esterni. Tra gli attacchi ransomware alla catena di approvvigionamento dell'anno scorso vi sono le campagne dannose contro Kaseya e Quanta e una serie di attacchi che hanno sfruttato la vulnerabilità Log4j.

I ransomware as a service contribuiscono all'aumento del numero di attacchi. I gruppi di ransomware continuano a fare proseliti attraverso forum criminali illegali. Questi affiliati compromettono le grandi organizzazioni e distribuiscono i ransomware del gruppo, generalmente in cambio di circa l'80% degli introiti ottenuti dai riscatti pagati dalle vittime. La maggior parte (8 su 11) delle principali famiglie di ransomware dell'ultimo anno si è diffusa sfruttando prevalentemente dei modelli ransomware-as-a-service.

Le autorità stanno inasprendo i controlli. Alcune delle principali famiglie di ransomware dello scorso anno, in particolare quelle che prendono di mira i servizi critici, hanno attirato l'attenzione delle autorità di tutto il mondo. REvil (responsabile del famoso attacco a Kaseya e JSB), DarkSide (responsabile dell'attacco a Colonial Pipeline) ed Egregor (il nuovo nome di Maze, la principale famiglia di ransomware dello scorso anno) hanno tutti subito il sequestro dei beni nel corso del 2021.

Le famiglie di ransomware non stanno scomparendo, stanno solo cambiando nome. A causa dell'aumento dei controlli delle autorità, molti gruppi di ransomware si sono sciolti e riformati sotto altri nomi, continuando a utilizzare le stesse tattiche (o molto simili). Il nuovo nome di DarkSide è BlackMatter, quello di DoppelPaymer è Grief, mentre Avaddon ha preso i nomi di Haron e Midas. Evil Corp, oggetto di sanzioni da parte delle autorità statunitensi, ha cambiato continuamente il nome delle proprie operazioni ransomware.

Il conflitto tra Russia e Ucraina ha messo in allerta il mondo. Ci sono stati diversi attacchi associati al conflitto tra Russia e Ucraina, tra cui vari wiper, come HermeticWiper e PartyTicket. Finora, la maggior parte di queste attività ha colpito l'Ucraina. Tuttavia, le agenzie governative hanno incoraggiato le organizzazioni e le aziende a prepararsi per attacchi più diffusi con il persistere del conflitto.

Lo zero trust rimane la migliore forma di difesa. Per ridurre al minimo la possibilità di una violazione e i danni che un attacco può causare, le organizzazioni devono utilizzare strategie difensive avanzate, che includono la riduzione della superficie di attacco, l'applicazione di un controllo degli accessi a privilegi minimi e il monitoraggio e l'ispezione continua dei dati in tutto l'ambiente.

L'evoluzione dei ransomware

Il ransomware è un tipo di malware che i criminali informatici utilizzano per bloccare le attività di un'organizzazione presa come target. Il ransomware cripta i file importanti di un'organizzazione in un formato illeggibile e richiede il pagamento di un riscatto per decriptarli. Le richieste di riscatto sono spesso proporzionali al numero di sistemi infetti e al valore dei dati criptati: più è alta la posta in gioco, più è alta la somma da pagare.

Alla fine del 2019 le tattiche degli aggressori si sono evolute, e hanno iniziato a includere l'esfiltrazione dei dati, dando origine a una forma di attacco ransomware comunemente nota come "doppia estorsione". In queste forme di attacco, nel caso in cui la vittima non volesse pagare il riscatto per decriptare i dati e cercasse invece di ripristinarli da un backup, gli aggressori minacceranno di divulgarli.

Alla fine del 2020, alcuni operatori di ransomware hanno aggiunto un ulteriore livello di attacco, con tattiche DDoS che bombardano il sito web o la rete della vittima, generando un'interruzione dell'attività persino più grave e inducendo la stessa a negoziare.

Nel 2021 e di nuovo nel 2022, gli attacchi ransomware più dannosi sono quelli che prendono di mira la catena di approvvigionamento. In questi attacchi, la violazione di un provider di servizi (in genere un software o un altro provider di soluzioni tecnologiche) consente di scagliare attacchi secondari alle organizzazioni che si affidano ai loro prodotti. Si stima che gli attacchi alla catena di approvvigionamento siano aumentati del 51% nella seconda metà del 2021. Gli aggressori hanno fatto notizia attaccando software popolari, come SolarWinds, Kaseya e Log4j, e prevediamo che questa tendenza si intensificherà nei prossimi anni.

La sequenza di attacco dei ransomware

Gli attacchi ransomware di oggi in genere prevedono le seguenti fasi:

1. **Compromissione iniziale:** gli aggressori utilizzano dei vettori di intrusione per ottenere l'accesso ai sistemi, tra cui le e-mail di phishing, lo sfruttamento delle vulnerabilità negli strumenti di amministrazione da remoto o nelle VPN e l'utilizzo di forza bruta o credenziali rubate per stabilire connessioni con protocollo RDP (Remote Desktop Protocol). Un altro metodo per infiltrarsi in un'organizzazione è quello di attaccare la catena di approvvigionamento.
2. **Movimento laterale:** dopo aver ottenuto l'accesso iniziale, gli aggressori raccolgono le informazioni sull'infrastruttura delle vittime e si spostano lateralmente tra i sistemi di rete, incrementando i privilegi e stabilendo meccanismi di persistenza secondo necessità, catalogando i dati più importanti da rubare o criptare e depositando i carichi utili dei ransomware per procedere con l'esecuzione in una fase successiva.
3. **Esfiltrazione dei dati:** nel caso di un attacco a doppia estorsione, gli aggressori proseguiranno rubando i dati sensibili da utilizzare per la tattica secondaria di estorsione, in modo che possano richiedere riscatti più elevati. In questo modo, riducono il potere di negoziazione delle vittime: anche se le organizzazioni sono in grado di recuperare i dati criptati attraverso i backup, devono comunque rispondere alla minaccia di divulgazione degli aggressori.
4. **Esecuzione del ransomware:** successivamente, gli aggressori distribuiscono ed eseguono il ransomware criptando i file target sui sistemi connessi alla rete. Di solito il ransomware termina i processi relativi a software di sicurezza e database per massimizzare il numero di file che può criptare. Anche le copie shadow di backup vengono solitamente eliminate dal sistema per ostacolare ulteriormente il recupero dei file. Alcune famiglie di ransomware, inoltre, riavviano il sistema compromesso nella modalità provvisoria di Windows per bypassare i software di sicurezza dell'endpoint prima di criptare i file. Dopo che i file sono stati criptati, le vittime ricevono una richiesta di riscatto, che fornisce loro le istruzioni per pagare e decriptare i file.
5. **DDoS:** se la vittima si rifiuta di negoziare, alcuni gruppi di hacker sferrano un attacco DDoS contro la rete o il sito web della stessa per interrompere le operazioni aziendali e ottenere un ulteriore margine di negoziazione.

La figura 1 mostra la tipica catena di attacco di un attacco ransomware con estorsione multipla

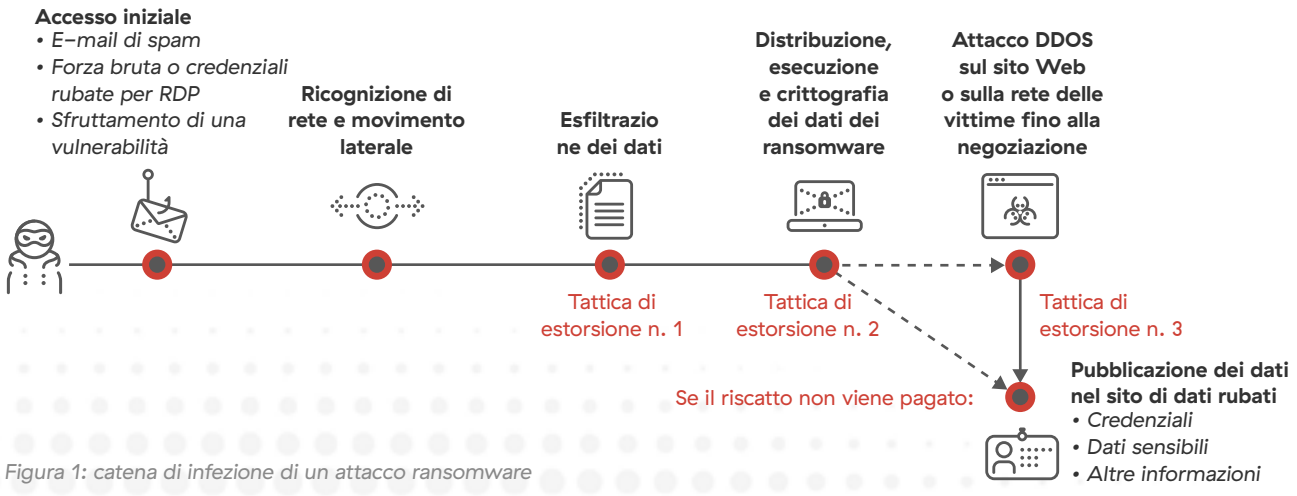


Figura 1: catena di infezione di un attacco ransomware

Le statistiche degli attacchi ransomware per il 2021–2022

L'elevato volume dei dati delle transazioni su Zero Trust Exchange di Zscaler fornisce una panoramica unica sulle tattiche e sulle vittime dei criminali informatici. Da febbraio 2021 a marzo 2022, ThreatLabz ha osservato un aumento dell'80% dei carichi utili di ransomware rispetto all'anno precedente. Inoltre, in base alla quantità di dati pubblicati sui siti di divulgazione degli aggressori, abbiamo osservato un aumento del 117% delle vittime dei ransomware a doppia estorsione.

I settori colpiti dai ransomware

Il settore manifatturiero è stato il settore più colpito già nel 2020, avendo subito il 12,7% del totale degli attacchi ransomware a doppia estorsione tra novembre 2019 e gennaio 2021. Quest'anno, gli attacchi contro le imprese manifatturiere sono aumentati ancora, raggiungendo il 19,5%. Seguono il settore dei servizi (9,7%), l'edilizia (8,1%), il commercio al dettaglio e all'ingrosso (7,5%) e il settore high tech (6,7%).

Infezioni ransomware per settore

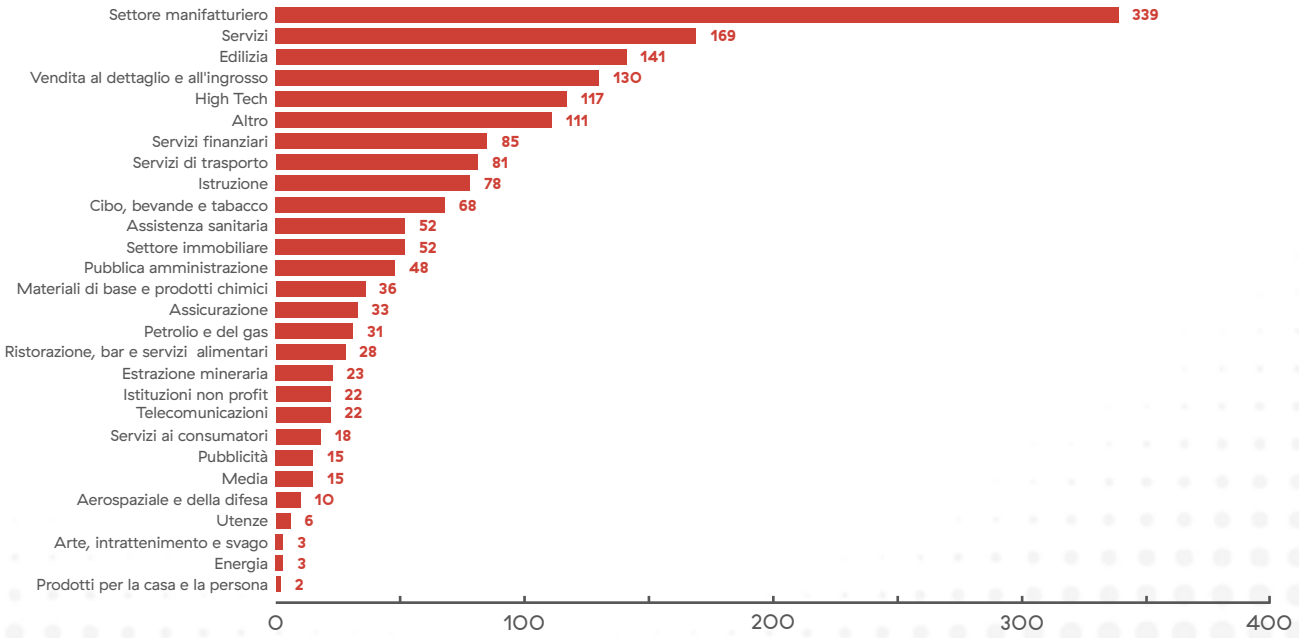


Figura 2: infezioni ransomware per settore

L'aumento degli attacchi ransomware a doppia estorsione varia ampiamente in base al settore. Nel report dell'anno scorso, abbiamo notato un numero particolarmente basso di attacchi contro le organizzazioni sanitarie, dovuto a un maggiore controllo da parte delle autorità e alla promessa da parte di diverse delle principali famiglie di ransomware di non prendere di mira il settore sanitario durante la pandemia di COVID-19.

I dati di quest'anno raccontano una storia diversa. Gli attacchi ransomware a doppia estorsione contro il settore sanitario sono cresciuti del 643% nel 2021, pur partendo da una baseline di attacchi molto bassa nel 2020. Anche molti altri settori con percentuali di partenza più elevate hanno registrato una crescita a tre cifre del numero di attacchi, tra cui l'istruzione (225%), il settore manifatturiero (190%), l'edilizia (161%), i servizi finanziari (130%) e i servizi (109%).

Variazione percentuale degli attacchi a doppia estorsione: confronto tra il 2021 e il 2020

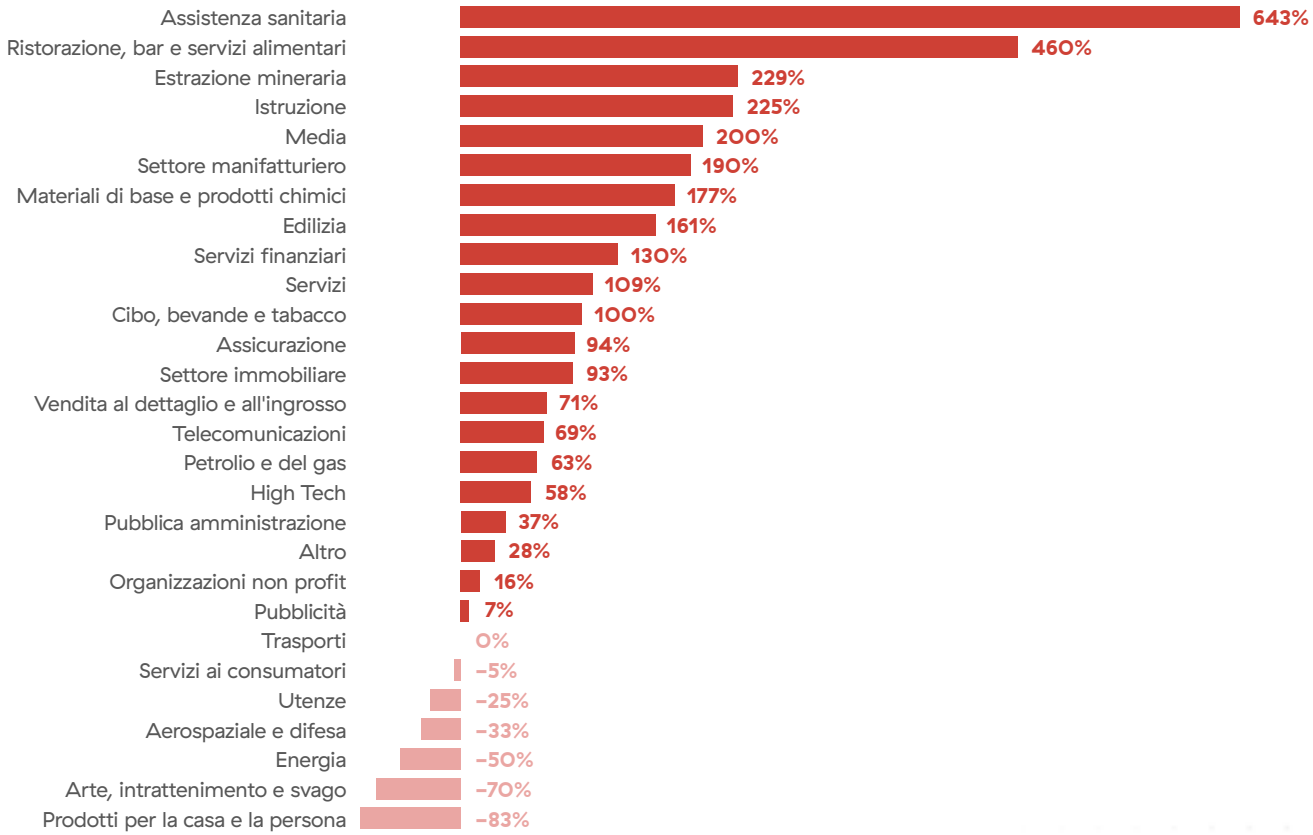


Figura 3: variazione percentuale degli attacchi a doppia estorsione per settore

Le principali famiglie di ransomware

Conti e LockBit sono state le famiglie di ransomware a doppia estorsione più diffuse nel 2021, insieme a una serie di nuove famiglie che sono emerse nel corso dell'anno.

La figura 4 mostra i momenti in cui le famiglie di ransomware più attive degli ultimi anni sono state scoperte per la prima volta e hanno iniziato a pubblicare dati sui siti web di divulgazione o su forum di hacking.

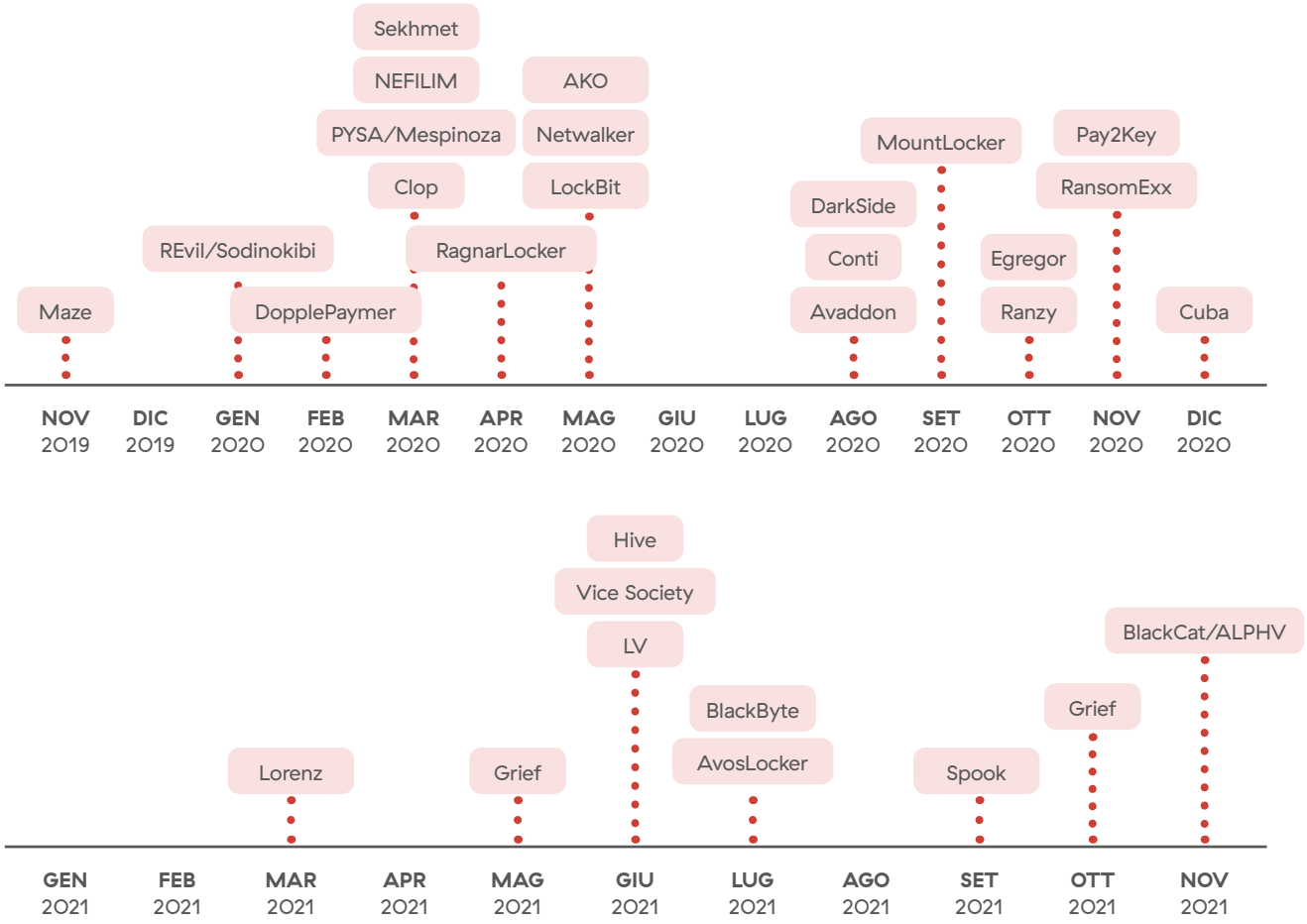


Figura 4: cronologia delle famiglie di ransomware che hanno pubblicato dati su siti di divulgazione o su forum di hacking

Molte delle famiglie di ransomware attive nel periodo 2021–2022 sfruttano modelli ransomware-as-a-service (RaaS) per aumentare la loro distribuzione attraverso le reti di affiliati. Nel 2021 abbiamo assistito inoltre al rebranding di diverse popolari famiglie di ransomware, come DoppelPaymer, che è stato ribattezzato Grief, DarkSide, diventato BlackMatter, e Avaddon, ribattezzato Haron e Midas (questi ultimi due utilizzano il generatore di ransomware Thanos).

Conti è stato il gruppo di ransomware più attivo degli ultimi due anni e il più dannoso di tutti i tempi in termini di riscatti pagati: l'FBI stima che, a partire da gennaio 2022, siano state più di 1000 le vittime di attacchi associati al ransomware Conti, con un totale degli introiti estorti che supera i 150 milioni di dollari (una cifra in cui non sono inclusi i danni correlati o i costi di correzione). Tra le vittime di Conti figurano diverse organizzazioni che offrono servizi critici nei settori finanziario, informatico, energetico e governativo, tra cui l'assistenza sanitaria pubblica irlandese e il Governo della Costa Rica. Nel maggio del 2022, il Dipartimento di Stato degli Stati Uniti ha offerto un premio di 10 milioni di dollari a chi fosse in grado di informazioni sui leader del gruppo.

LockBit, in precedenza noto come ransomware ABCD, tende ad attaccare le piccole e medie imprese, evitando così di finire nei titoli delle testate, fatta eccezione per l'attacco ad Accenture nell'agosto del 2021. LockBit è un RaaS ampiamente utilizzato, ed è molto interessante per gli aggressori per via della sua velocità e delle sue prestazioni.

La figura 5 mostra le famiglie di ransomware che hanno colpito il numero più elevato di organizzazioni con attacchi a doppia estorsione tra febbraio 2021 e marzo 2022, sulla base delle informazioni provenienti dai siti di divulgazione dei dati rubati.

Attacchi ransomware per famiglia

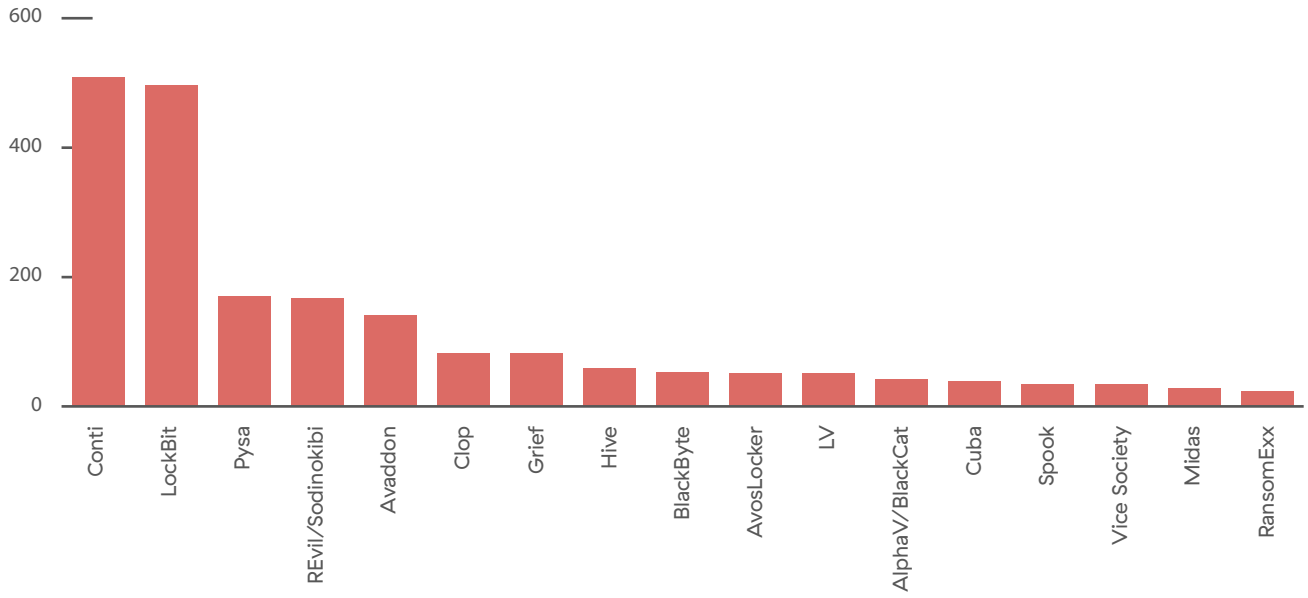


Figura 5: attacchi ransomware per famiglia tra febbraio 2021 e marzo 2022

Le previsioni per il 2022–2023

L'utilizzo dei ransomware come servizio (RaaS) continuerà ad aumentare

I RaaS si sono rivelati preziosi per tutte le parti coinvolte. I nuovi sviluppatori di ransomware e gli affiliati aumenteranno l'uso di questo modello per sferrare attacchi in grado di evolversi rapidamente contro le organizzazioni vulnerabili.

L'evoluzione dei modelli di ransomware porterà al cambiamento degli obiettivi

Con i generatori di ransomware e le informazioni sulle organizzazioni in vendita sul dark web, gli aggressori hanno il vantaggio di poter filtrare i profili aziendali per restringere il campo e individuare gli obiettivi più idonei per vulnerabilità specifiche, profitti e tipologie di ransomware. Di conseguenza, si prevede che ci sarà un passaggio verso obiettivi più semplici, tra cui le piccole e medie imprese con meno controlli di sicurezza e le organizzazioni con applicazioni visibili su Internet, che presentano vulnerabilità note e credenziali già esposte.

Il periodo di permanenza continuerà a diminuire

Ora che gli aggressori possono accedere in modo facile ed economico ai profili aziendali e alle credenziali compromesse in vendita sul dark web, i giorni in cui gli aggressori passavano mesi o addirittura anni a studiare i propri obiettivi stanno per volgere al termine. Un numero sempre maggiore di report disponibili pubblicamente indica che il tempo di osservazione degli aggressori si è ridotto a pochi giorni; questo significa che i criminali sono ormai esperti nelle tecniche di rilevamento più avanzate, e sanno che il tempo è un elemento fondamentale per il successo di un attacco. Di conseguenza, per evitare gravi violazioni nel 2022 e in futuro, i team di sicurezza devono rispondere a questa nuova tendenza e rendere più rapido il rilevamento, riducendolo a giorni, ore o addirittura minuti.

Gli attacchi alla catena di approvvigionamento aumenteranno, e gli aggressori comprometteranno gli ecosistemi dei partner e dei fornitori

Le aziende più importanti del mondo di solito dispongono di misure di sicurezza efficaci, ma questo potrebbe non essere vero per i loro fornitori e partner, i quali hanno accesso a reti, sistemi e informazioni importanti. Lo abbiamo visto nella recente compromissione di Okta da parte del gruppo di hacker Lapsus$ e nelle minacce di REvil a Apple attraverso Quanta Computer, un produttore dell'azienda di Cupertino. Questi gruppi e molti altri hanno utilizzato attacchi alla catena di approvvigionamento per accedere alle informazioni sensibili a monte, sfruttando l'accesso dei fornitori senza dover violare le misure di sicurezza più complesse dei loro obiettivi finali.

Il ransomware può essere utilizzato come un wiper o insieme ad esso per distruggere i dati

All'inizio del 2022, gli attacchi pubblicizzati verso l'Ucraina hanno fatto uso di diversi tipi di wiper, tra cui HermeticWiper insieme al ransomware esca PartyTicket. Non è la prima volta che un ransomware viene utilizzato per attacchi geopolitici: anche NotPetya e Bad Rabbit sono stati utilizzati nel 2017 per attaccare le organizzazioni ucraine. Le tensioni geopolitiche comportano la minaccia di ransomware mascherati, wiper e altre tattiche, che consentono agli aggressori un elevato grado di anonimato e la possibilità di smentire l'attacco in modo plausibile.

Le vulnerabilità vecchie (e nuove) continueranno a causare danni

Nel corso dell'ultimo anno sono state rilevate alcune importanti vulnerabilità (ad es. Log4j, PrintNightmare, ProxyShell/ProxyLogon), che terranno impegnate le organizzazioni per anni a venire. Gli aggressori continueranno a cercare e a sfruttare software e server non aggiornati e senza le dovute patch per bypassare i controlli di sicurezza.

Le famiglie di ransomware continueranno a cambiare nome

Abbiamo assistito a questo copione nel 2021: un gruppo di ransomware sferra un attacco devastante, ottiene l'attenzione delle autorità, riceve sanzioni dalle stesse e poi scompare per riprendere forma in un secondo momento con un nuovo nome. I ransomware sono nel mirino delle autorità, e questo ciclo continuerà nel 2022 e in futuro.

Le organizzazioni dovranno rafforzare la sicurezza oltre alla semplice protezione degli endpoint

I gruppi di ransomware intensificheranno l'uso di tattiche per aggirare gli antivirus e gli altri controlli di sicurezza degli endpoint. Le aziende avranno bisogno di difese avanzate, e non dovranno affidarsi esclusivamente alla sicurezza degli endpoint per prevenire e rilevare le intrusioni.

Gli sviluppatori di ransomware utilizzeranno più tecniche di offuscamento dei malware

Gli autori di malware implementano tecniche di offuscamento per ostacolare il reverse engineering e bypassare il rilevamento statico delle firme. La complessità dell'offuscamento dei malware continuerà ad aumentare, grazie a tecniche avanzate come l'appiattimento del flusso di controllo, l'offuscamento delle stringhe polimorfiche e l'uso di packer basati su macchine virtuali.

La divulgazione del codice sorgente dei ransomware contribuirà alla loro proliferazione

Nel corso dell'ultimo anno sono stati divulgati numerosi codici sorgente di ransomware, tra cui due versioni di Conti e Babuk. ThreatLabz ha già osservato che il codice sorgente di entrambe le famiglie di ransomware è stato utilizzato da terzi in altri attacchi. La pubblicazione di codice sorgente porterà indubbiamente ad abusi da parte di altri gruppi criminali che non hanno le competenze necessarie per progettare e costruire il proprio ransomware da zero.

Guida alla prevenzione

Che si tratti di un semplice attacco ransomware, di un attacco a doppia o tripla estorsione, di una famiglia di minacce indipendente o di un attacco RaaS eseguito tramite una rete di affiliati, la strategia di difesa è la stessa: utilizzare i principi dello zero trust per limitare le vulnerabilità, prevenire e rilevare gli attacchi e limitare il raggio di azione delle violazioni che vanno a buon fine. Di seguito sono riportati alcuni consigli sulle best practice da adottare per proteggere le organizzazioni dai ransomware.

1 Elimina le applicazioni da Internet.

Gli aggressori avviano gli attacchi eseguendo una ricognizione dell'ambiente, cercando le vulnerabilità da sfruttare e adattando il loro approccio in base alle condizioni che incontrano. Le applicazioni pubbliche su Internet sono più facili da attaccare, ed è quindi necessario adottare un'architettura zero trust che sia in grado di proteggere le applicazioni interne rendendole invisibili agli aggressori.

2 Applica una policy di sicurezza uniforme per prevenire la compromissione iniziale.

Con una forza lavoro distribuita, è importante implementare un'architettura SSE (Security Service Edge) in grado di applicare policy di sicurezza uniformi, indipendentemente dalla posizione degli utenti (in ufficio o da remoto).

3 Utilizza sandbox per rilevare i carichi utili sconosciuti.

Il rilevamento basato sulla firma non è sufficiente di fronte alla rapida evoluzione delle varianti di ransomware e dei carichi utili. Per questo motivo, ti consigliamo di proteggerti contro gli attacchi sconosciuti ed elusivi adottando una sandbox inline che faccia uso di algoritmi di intelligenza artificiale e analizzi il comportamento dei file anziché il loro aspetto esterno.

4 Implementa un'architettura ZTNA (Zero Trust Network Access).

Implementa una segmentazione granulare da utente ad applicazione e da applicazione ad applicazione, effettuando il brokering dell'accesso con controlli di accesso dinamici a privilegi minimi per eliminare il movimento laterale. In questo modo, riduci al minimo i dati che possono essere criptati o rubati, e restringi il raggio di azione di un attacco.

5 Distribuisci la prevenzione della perdita di dati inline.

Impedisci l'esfiltrazione delle informazioni sensibili impiegando strumenti e policy di prevenzione della perdita dei dati basate sull'attendibilità e contrasta le tecniche a doppia estorsione.

6 Aggiorna i software e investi nella formazione continua del personale.

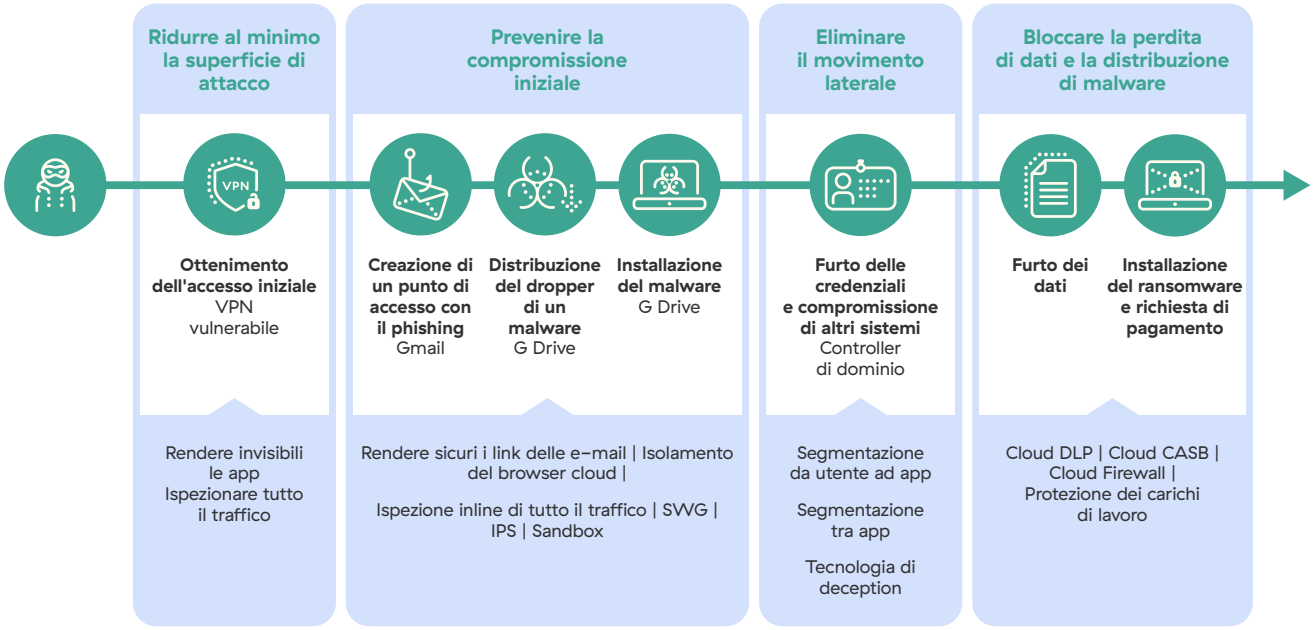
Applica patch di sicurezza ai software e accresci regolarmente la consapevolezza dei dipendenti sulle tematiche relative alla sicurezza attraverso programmi di formazione, riducendo così le vulnerabilità che possono essere sfruttate dai criminali informatici.

7 Prepara un piano di risposta.

Preparati al peggio stipulando un'assicurazione informatica e preparando un piano di backup dei dati e un piano di risposta che faranno parte del programma globale di continuità operativa e di ripristino di emergenza.

Per difenderti al meglio contro i ransomware, è bene adottare difese a strati in grado di interrompere l'attacco in ogni fase: dalla ricognizione alla compromissione iniziale, al movimento laterale, al furto di dati e all'esecuzione del ransomware.

Bloccare i ransomware grazie allo zero trust



Le principali tendenze dei ransomware

Attacchi alla catena di approvvigionamento

Che cos'è un attacco alla catena di approvvigionamento?
Gli attacchi alla catena di approvvigionamento (o supply chain), anche chiamati attacchi alla catena del valore o a terzi, sono attacchi che, per ottenere l'accesso a un'organizzazione, vengono sferrati contro i fornitori della stessa. La maggior parte delle grandi aziende dispone di controlli di sicurezza sofisticati che rendono difficile l'infiltrazione; gli aggressori hanno quindi trovato il modo di attaccare queste organizzazioni passando per i fornitori.

Gli attacchi alla catena di approvvigionamento sfruttano la fiducia tra organizzazioni legittime che intrattengono normali rapporti commerciali. Gli aggressori inseriscono una backdoor in un prodotto utilizzato dal loro obiettivo; questo consente loro di infiltrarsi nella rete senza essere individuati, tipicamente attraverso patch o aggiornamenti del software automatici in stile trojan. Una volta entrati, gli aggressori possono spiare, rubare dati, impiantare altre minacce informatiche e interrompere le operazioni.

Questi attacchi sono molto sofisticati e spesso pianificati nei minimi dettagli, e la compromissione originaria può portare a conseguenze devastanti per le aziende.

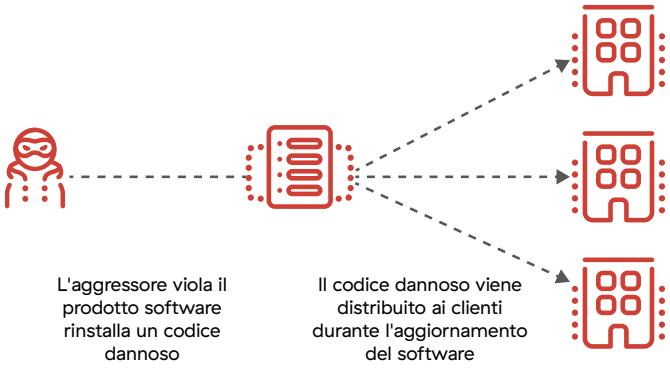


Figura 6: attacco alla catena di approvvigionamento

Il ransomware della catena di approvvigionamento di Kaseya
Il 2 luglio del 2021, la società di software per la gestione IT Kaseya ha divulgato informazioni in merito a un incidente di sicurezza che aveva colpito la versione on-premise del software Kaseya VSA, una piattaforma che consente ai provider di servizi gestiti (MSP) di eseguire la gestione delle patch, i backup e il monitoraggio dei client per i propri clienti. Si ritiene che durante questo attacco siano stati violati circa 70 MSP, e che le conseguenze secondarie abbiano interessato 1500 piccole e medie imprese.

L'aggressore responsabile di questo attacco ha identificato e sfruttato una vulnerabilità 0-day nel server Kaseya VSA, che gli ha permesso di inviare uno script dannoso a tutti i client gestiti da quel server. Questo script è stato utilizzato quindi per distribuire il ransomware REvil/Sodinokibi, che ha criptato i file sui sistemi colpiti.

La catena di approvvigionamento di Quanta Computer
Nell'aprile del 2021, REvil ha attaccato Quanta Computer, il più grande produttore di computer portatili al mondo e uno dei principali produttori di dispositivi Apple. Quanta si è rifiutata di pagare una richiesta di riscatto di 50 milioni di dollari e REvil ha quindi preso di mira Apple e altri clienti di Quanta per ottenere il riscatto. REvil ha pubblicato 21 schermate di schematiche MacBook e ha minacciato di pubblicare altri dati di Apple e di altre aziende se Apple o Quanta non avessero pagato il riscatto richiesto.

Il ransomware Log4j

A dicembre del 2021, l'Apache Software Foundation ha pubblicato un avviso di sicurezza relativo a una vulnerabilità all'esecuzione di codice da remoto (CVE-2021-44228) nella popolare libreria per la gestione dei log Log4j.

Questa vulnerabilità consente agli utenti malintenzionati di scaricare ed eseguire un carico utile dannoso inviando una richiesta appositamente creata al sistema vulnerabile. L'aggressore può quindi controllare i messaggi di log o i parametri dei messaggi di log per eseguire codice arbitrario caricato da server LDAP se la sostituzione dei messaggi di lookup è abilitata. Log4j è incorporato in molti siti web, applicazioni e framework popolari, e molti attacchi ransomware hanno eseguito l'exploit di questa vulnerabilità, portando a conseguenze molto diffuse:

Il ransomware NightSky
Il 4 gennaio 2021, gli aggressori hanno sfruttato la vulnerabilità Log4j in un sistema che si interfacciava con Internet e utilizzava VMware Horizon, rilasciando il ransomware NightSky.

Khonsari
Sono stati osservati diversi attacchi che hanno utilizzato exploit di Log4j su sistemi Windows per distribuire il ransomware Khonsari.

Conti
Anche il gruppo Conti ha sfruttato la vulnerabilità Log4j per lanciare attacchi ransomware. AdvIntel ha scoperto che il gruppo ha scansionato e colpito le versioni di VMware vCenter soggette alla vulnerabilità Log4j, spostandosi lateralmente dalle sessioni esistenti di Cobalt Strike alle reti vittime statunitensi ed europee.

TellYouThePass
Gli aggressori hanno sfruttato la vulnerabilità Log4j per distribuire ed eseguire il ransomware TellYouThePass nei sistemi Windows e Linux.

I ransomware as a service

Il dark web è diventato un luogo molto popolare per i gruppi di utenti malintenzionati che vendono la loro merce ai potenziali criminali. Abbiamo analizzato nel dettaglio l'impatto di questi mercati per la diffusione di altri tipi di attacchi, come il phishing as a service, nel report di ThreatLabz sugli attacchi di phishing del 2022.

I RaaS sono diventati incredibilmente popolari e ormai sono alla base della maggior parte degli attacchi ransomware moderni. Infatti, 8 delle 11 principali famiglie di ransomware attive nell'ultimo anno utilizzano gli ecosistemi RaaS.

Il modello RaaS richiede due parti: operatori e affiliati. Gli operatori sono i gruppi di hacker che sviluppano il ransomware. Gli affiliati prendono di mira le vittime, eseguono il ransomware ed effettuano le richieste.

Gli operatori reclutano gli affiliati e forniscono loro il ransomware e gli strumenti necessari per eseguirlo, l'accesso a un sito di divulgazione dei dati rubati, l'assistenza per la negoziazione e altro supporto, in cambio di circa il 70–80% dei profitti derivanti dagli attacchi.

Questo modello è vantaggioso per entrambe le parti. Gli affiliati ottengono tutto ciò di cui hanno bisogno per eseguire attacchi ransomware altamente efficaci senza dover sviluppare nulla. Si tratta di una soluzione interessante sia per i criminali esperti, che risparmiano tempo e risorse per lo sviluppo, sia per gli aggressori poco qualificati, che altrimenti non sarebbero in grado di eseguire un attacco di questo tipo. Gli operatori di ransomware possono aumentare esponenzialmente la portata delle loro operazioni e, di conseguenza, i loro profitti.

Il volume degli attacchi e i danni causati dai RaaS sono aumentati:

- **Aumento del volume di attacchi ransomware:** un numero maggiore di affiliati inizia a eseguire ransomware, perché ora richiedono meno tempo e competenze per essere sviluppati.
- **Aumento dell'importo dei riscatti a causa della doppia estorsione:** i RaaS includono la componente della doppia estorsione, in cui gli aggressori rubano i dati e minacciano di pubblicarli su un sito di divulgazione se il riscatto non viene pagato. In questo modo, si può aumentare l'importo del riscatto e la probabilità che questo venga pagato.

Gli attacchi geopolitici

I responsabili della sicurezza di tutto il mondo sono in allerta per l'aumento degli attacchi ransomware a seguito del conflitto tra Russia e Ucraina.

A marzo del 2022, il Presidente degli Stati Uniti Joe Biden ha pubblicato un avviso sulla possibilità che si verifichino comportamenti informatici dannosi nel territorio degli Stati Uniti in risposta alle sanzioni economiche contro la Russia. La sua dichiarazione ha indotto immediatamente le organizzazioni del settore pubblico e di quello privato a rafforzare le proprie difese informatiche.

8 delle 11 principali famiglie di ransomware attive nel 2021 utilizzano ecosistemi RaaS.

Al momento della stesura di questo report, si sono verificati diversi attacchi ransomware contro l'Ucraina e/o attacchi associati a questo conflitto:

1. **Il ransomware PartyTicket:** questo ransomware basato su Go è stato utilizzato in combinazione con il malware HermeticWiper per colpire le organizzazioni in Ucraina. PartyTicket non è sofisticato e il suo modo di criptare i file è difettoso, e può essere decriptato e invertito. Questo ci porta a sospettare che sia stato sviluppato come distrazione da HermeticWiper.
2. **Il ransomware Conti :** la CISA (Cybersecurity and Infrastructure Security Agency), l'FBI (Federal Bureau of Investigation), la NSA (National Security Agency) e i Servizi segreti degli Stati Uniti hanno pubblicato un avviso su Conti, un gruppo di ransomware legato alla Russia. L'avviso segnala che "gli aggressori responsabili della minaccia informatica Conti sono ancora operativi e gli attacchi ransomware di questo tipo contro organizzazioni statunitensi e internazionali hanno superato i 1000 casi". Alla fine di febbraio, Conti ha pubblicato due dichiarazioni sul suo sito di divulgazione di dati rubati in cui si è impegnato a sostenere il Governo russo in risposta all'"Occidente guerrafondaio e alle minacce americane di usare la guerra informatica contro i cittadini della Federazione Russa".

L'intervento delle autorità

Le autorità di tutto il mondo stanno prestando maggiore attenzione alle famiglie di ransomware, in particolare a quelle che causano danni diffusi. Le famiglie di ransomware dall'impatto elevato hanno registrato diversi successi durante il 2021 e all'inizio del 2022.

Lo sradicamento di REvil
REvil è una delle famiglie di ransomware più famigerate degli ultimi due anni, che ha fatto notizia dopo i principali attacchi contro Kaseya e JSB. Dopo l'attacco a Kaseya, l'FBI ha pianificato la rimozione dei server di REvil, ma senza riuscirci: poco dopo questo attacco critico, a luglio del 2021, REvil ha chiuso le sue operazioni e gli hacker sono scomparsi, ma la tregua è stata breve, e le operazioni sono ripartite a settembre del 2021.

A gennaio del 2022, il governo russo avrebbe smantellato il gruppo di hacker dietro a REvil, arrestando i membri su richiesta degli Stati Uniti. Il Federal Security Service (FSB) russo avrebbe perquisito 25 indirizzi, arrestato 14 membri del gruppo di REvil e sequestrato 426 milioni di rubli, 600.000 dollari americani, 500.000 euro, 20 auto di lusso e attrezzature informatiche. Tuttavia, REvil ha ripreso le attività ad aprile del 2022, e ha ricominciato ad attaccare le organizzazioni con una versione aggiornata del ransomware.

Lo sradicamento di DarkSide
Il 6 maggio 2021, il gruppo del ransomware DarkSide ha sferrato un attacco ransomware di alto profilo contro Colonial Pipeline, la più grande catena di oleodotti degli Stati Uniti. Le agenzie federali sono intervenute e, a due settimane dall'attacco, un aggressore noto come UNKN ha annunciato la chiusura di DarkSide a causa della perdita dell'accesso ai server e il trasferimento delle loro criptovalute su un conto sconosciuto. Il Dipartimento di Giustizia ha annunciato di aver sequestrato 63,7 bitcoin, per un valore di circa 2,3 milioni di dollari.

Lo sradicamento di Egregor
Il gruppo ransomware Egregor, in precedenza noto come Maze, è stato sconfitto il 9 febbraio del 2021 grazie alla cooperazione tra le autorità di vari paesi. Le agenzie di Ucraina, Francia e Stati Uniti hanno chiuso il sito web di divulgazione dei dati rubati di Egregor, arrestato i membri del gruppo e sequestrato i computer associati agli attacchi del ransomware. Egregor ha estorto circa 80 milioni di dollari da oltre 150 aziende vittime.

Il rebranding dei ransomware

Nell'ultimo anno gli operatori di ransomware hanno spesso cambiato nome. Questo rebranding è generalmente dovuto all'attenzione indesiderata da parte delle forze dell'ordine e dei media e alle sanzioni che limitano le capacità dei gruppi di riscuotere i pagamenti dei riscatti.

DoppelPaymer, ribattezzato Grief
All'inizio di maggio del 2021, l'attività del ransomware DoppelPaymer è diminuita in modo significativo. Sebbene il sito di divulgazione dei dati rubati di DoppelPaymer sia ancora online, dal 6 maggio del 2021 non sono stati pubblicati nuovi post sulle vittime. Inoltre, dalla fine di giugno non è stato aggiornato alcun post. Questa inattività è probabilmente una reazione all'attacco ransomware a Colonial Pipeline, avvenuto il 7 maggio del 2021. Tuttavia, l'apparente tregua è dovuta al fatto che il gruppo responsabile delle minacce DoppelPaymer ha ribattezzato il ransomware Grief. Entrambe le varianti del ransomware condividono il codice malware, e i siti di divulgazione dei dati rubati sono molto simili. Tuttavia, il portale per il riscatto di Grief presenta alcune differenze rispetto a quello di DoppelPaymer. In particolare, il metodo di pagamento del riscatto è in Monero (XMR) anziché in bitcoin (BTC). Questa modifica della criptovaluta potrebbe essere in risposta al recupero da parte dell'FBI di una porzione della somma pagata come riscatto da Colonial Pipeline.

I gruppi di ransomware cambiano nome per aggirare le sanzioni e i controlli delle autorità.

Darkside, ribattezzato BlackMatter
Dopo lo smantellamento di DarkSide a maggio del 2021, alla fine di luglio è emersa una nuova famiglia di ransomware chiamata BlackMatter. La routine di crittografia utilizzata dal ransomware e il testo nel sito di divulgazione dei dati rubati indicano che BlackMatter è il nuovo nome di DarkSide.

BlackMatter ha cessato le sue operazioni a novembre del 2021. Il gruppo ha pubblicato un messaggio di cessazione della sua attività sul portale del RaaS, in cui dichiarava che: "A causa di determinate circostanze non risolvibili associate alla pressione delle autorità (parte del team non è più disponibile dopo le ultime notizie), il progetto è stato chiuso".

Il rebranding dei ransomware Thanos
Pubblicizzato sul dark web come RaaS, il ransomware Thanos è stato identificato per la prima volta a febbraio del 2020. Il generatore di Thanos è stato divulgato e, nel corso dei due anni successivi, è stata sviluppata una serie di nuove varianti. La variante Prometheus del ransomware è emersa a febbraio del 2021. A settembre, Prometheus è stato rinominato Spook. Entrambi hanno richieste di riscatto analoghe e siti di divulgazione dei dati rubati simili, e contengono il Key Identifier di Thanos.

Nel luglio 2021 è stato individuato un altro ransomware derivato da Thanos, chiamato Haron. Il ransomware Haron presenta delle analogie rilevanti con il ransomware Avaddon. Le caratteristiche che Haron e Avaddon hanno in comune sono le richieste di riscatto, i siti di negoziazione e i siti di divulgazione dei dati rubati. Nel mese di ottobre del 2021 è stata scoperta un'altra variante chiamata Midas, una versione rinnovata del ransomware Haron.

Il rebranding di Evil Corp

Il gruppo Evil Corp, conosciuto anche come Indrik Spider, è noto per una serie di attività dannose e la creazione di trojan bancari come Dridex, che è stato utilizzato per distribuire il ransomware BitPaymer.

L'Office of Foreign Assets Control (OFAC) del Dipartimento del Tesoro statunitense ha sanzionato i membri di Evil Corp per i danni causati dal malware Dridex, che avrebbe fatto perdere più di 100 milioni di dollari a banche e istituzioni finanziarie in più di 40 Paesi. In seguito a queste sanzioni, le società di negoziazione si sono rifiutate di consentire i pagamenti dei riscatti a Evil Corp per paura di incorrere esse stesse in sanzioni o azioni legali da parte del Dipartimento del Tesoro statunitense. Per evitare pene, Evil Corp ha quindi individuato un semplice escamotage, ossia il rebranding del proprio ransomware.

Evil Corp ha distribuito il ransomware WastedLocker a giugno del 2020, il ransomware Hades a dicembre del 2020 e il ransomware Phoenix a marzo del 2021. A maggio del 2021 ha cambiato il nome del ransomware in PayloadBin, in modo da impersonare un aggressore non soggetto alle stesse sanzioni.

Il rebranding di Rook

Il ransomware Rook è stato individuato a novembre del 2021, in seguito alla divulgazione del codice sorgente del ransomware Babuk. A dicembre del 2021 una variante di Rook è stata ribattezzata Night Sky, ed è stata utilizzata dal gruppo di aggressori cinese DEV-0401 per colpire le reti aziendali con attacchi a doppia estorsione sfruttando la vulnerabilità Log4Shell. A gennaio del 2022 sia Rook che Night Sky hanno cessato le loro attività ed è emerso il ransomware Pandora. In base alle somiglianze nel codice, anche Pandora sembra essere una versione rinominata di Rook.

Le principali vulnerabilità sfruttate negli attacchi ransomware

Le vulnerabilità ProxyLogon

I ransomware BlackKingdom e DearCry hanno combinato quattro diversi exploit delle vulnerabilità ProxyLogon per accedere e criptare le reti delle loro vittime. Questa tattica è stata utilizzata per accedere ai server di Microsoft Exchange, rubare le e-mail e distribuire altre backdoor. Le vulnerabilità ProxyLogon includono CVE-2021-26855 (vulnerabilità SSRF [Server-Side Request Forgery, o falsificazione delle richieste lato server] di Exchange), CVE-2021-26857 (vulnerabilità di deserializzazione non sicura nel servizio di messaggistica unificata), CVE-2021-26858 (vulnerabilità di scrittura arbitraria di file post-autenticazione di Exchange) e CVE-2021-27065 (vulnerabilità di scrittura arbitraria di file post-autenticazione di Exchange). Microsoft ha risolto queste vulnerabilità distribuendo delle patch a marzo del 2021.

Una tipica catena di attacco che consente a un aggressore di eseguire codice da remoto sulla porta 443 esposta: gli aggressori utilizzano la vulnerabilità CVE-2021-26855 per bypassare l'autenticazione di Microsoft Exchange e impersonare un utente. L'aggressore invia una richiesta POST modificata per qualsiasi file nella directory che sia leggibile senza autenticazione dove il file nella directory non è richiesto. L'aggressore effettua l'autenticazione nel Pannello di controllo di Exchange (ECP) e sovrascrive tutti i file nel sistema di destinazione utilizzando le vulnerabilità CVE-2021-26858 o CVE-2021-27065. Dopo questi exploit, l'aggressore può quindi eseguire codice da remoto utilizzando la web shell sul server di Exchange.

La vulnerabilità ProxyShell di Exchange

Il ransomware Conti sfrutta la vulnerabilità di Microsoft Exchange Server per entrare nella

rete della vittima. Le vulnerabilità ProxyShell di Exchange sono una combinazione di CVE-2021-34473 (vulnerabilità di esecuzione di codice da remoto di Microsoft Exchange Server), CVE-2021-34523 (vulnerabilità di aumento dei privilegi di Microsoft Exchange Server) e CVE-2021-31207 (vulnerabilità di elusione delle funzionalità di sicurezza di Microsoft Exchange Server). Microsoft ha applicato le patch a queste vulnerabilità tra aprile e maggio 2021, ma Conti continua a colpire i server senza patch per eseguire codice da remoto. La catena di infezione di questo ransomware può essere consultata in questo report, nelle analisi dettagliate dei gruppi responsabili di BlackByte, AvosLocker e Hive. Anche il ransomware LockFile prende di mira queste vulnerabilità per distribuire il ransomware.

PrintNightmare
Gli attori di ransomware sfruttano le vulnerabilità PrintNightmare per colpire i sistemi Windows. Le vulnerabilità PrintNightmare sono una combinazione di CVE-2021-34527 e CVE-2021-34481, che sono vulnerabilità all'esecuzione di codice da remoto nel servizio spooler di stampa di Windows, il quale esegue in modo improprio operazioni privilegiate sui file e consente agli aggressori di eseguire codice da remoto con privilegi SYSTEM.

Questa vulnerabilità è presente nella funzionalità Point and print dei sistemi Windows, e consente agli utenti che non dispongono dei dovuti privilegi di aggiornare o installare stampanti in remoto. Microsoft ha reso disponibili gli aggiornamenti PrintNightmare che risolvono queste vulnerabilità a luglio e ad agosto del 2021.

Durante un attacco, un gruppo di ransomware ha sfruttato le vulnerabilità PrintNightmare e rilasciato il ransomware Vice Society. In un'altra campagna, gli aggressori hanno sfruttato PrintNightmare e il ransomware Magniber.

SonicWall SMA 100
A gennaio 2021, SonicWall ha confermato una vulnerabilità SQL injection nel proprio prodotto Secure Mobile Access SMA serie 100, che ha consentito agli aggressori di accedere alle credenziali di accesso, alle sessioni e ai dispositivi vulnerabili alla violazione utilizzando query non autenticate e appositamente create. SonicWall ha applicato le patch a febbraio del 2021.

La scoperta è avvenuta dopo che il gruppo responsabile di UNC2447 ha utilizzato questa falla per attaccare una rete e distribuire il ransomware a doppia estorsione FIVEHANDS nei sistemi delle vittime. Gli aggressori hanno utilizzato la vulnerabilità 0-day per ottenere l'accesso e rilasciare la backdoor SOMBRAT e strumenti aggiuntivi per ottenere un punto di accesso, eseguire la ricognizione ed esfiltrare i dati, tra cui i beacon Cobalt Strike, Adfind, BloodHound, Mimikatz, PC Hunter e Rclone. Al termine dell'attacco, UNC2447 ha lanciato ed eseguito il ransomware FIVEHANDS per criptare i dati del sistema colpito e ha quindi tentato di estorcere denaro con la minaccia di pubblicare i dati sui forum di hacking.

Dispositivo NAS di QNAP
Una nuova variante del ransomware eChOraix ha preso di mira i dispositivi NAS (Network Attached Storage) di QNAP (Quality Network Appliance Provider) e Synology. Nella catena di attacco, l'aggressore ha sfruttato la vulnerabilità CVE-2021-28799 nei dispositivi NAS di QNAP. Questa vulnerabilità all'autorizzazione impropria è stata segnalata nei dispositivi NAS di QNAP con sistema HBS 3 (Hybrid Backup Sync) e consente agli aggressori di accedere al dispositivo da remoto.

Le 11 famiglie di ransomware più diffuse

Di seguito è riportata una panoramica di 11 diverse famiglie di ransomware e delle loro sequenze di attacco. Queste sono le famiglie di ransomware che hanno colpito il maggior numero di vittime nel 2021 e nel 2022, e sono rappresentative della situazione attuale da cui le organizzazioni devono difendersi. Sono incluse informazioni sulla storia delle varie famiglie, un riepilogo delle tattiche impiegate (tra cui le mappature MITRE ATT&CK) e alcune statistiche relative ai settori che hanno colpito.

Conti

Il ransomware Conti è stato individuato per la prima volta a febbraio del 2020. Conti è talvolta classificato come RaaS, ma i suoi affiliati sono essenzialmente dipendenti, utilizzano un portale per gestire la pagina e ricevono una parte dei profitti. Conti e Ryuk condividono un codice simile, e questo suggerisce che Conti è probabilmente il successore di Ryuk. È stato il ransomware più diffuso nel 2021.

Catena di infezione:
Conti ha utilizzato meccanismi di accesso iniziale diversi nelle varie campagne:

1. È stato distribuito attraverso e-mail di spam contenenti allegati o link dannosi che scaricano in aggiunta anche TrickBot, IcedID, BazarLoader o Cobalt Strike per accedere nel sistema.
2. L'accesso iniziale è avvenuto anche sfruttando vulnerabilità note, come Log4j, ProxyShell, o utilizzando credenziali RDP (Remote Desktop Protocol) deboli.

Dopo la compromissione, Conti utilizza Cobalt Strike, Mimikatz e altri strumenti per rubare le credenziali e stabilire un punto di accesso alla rete. Il gruppo responsabile di Conti è noto per l'utilizzo di Metasploit, Netscan e altri strumenti utilizzati nelle simulazioni di attacco per ottenere informazioni sulla rete e sul controller di dominio. Dopo aver acquisito le informazioni necessarie, gli aggressori utilizzano AnyDesk, PsExec o altre utility remote per spostarsi lateralmente. Gli utenti malintenzionati associati a Conti esfiltrano i dati utilizzando Rclone o altri strumenti e, infine, distribuiscono ed eseguono il ransomware Conti per criptare i dati, come illustrato di seguito nella figura 7.

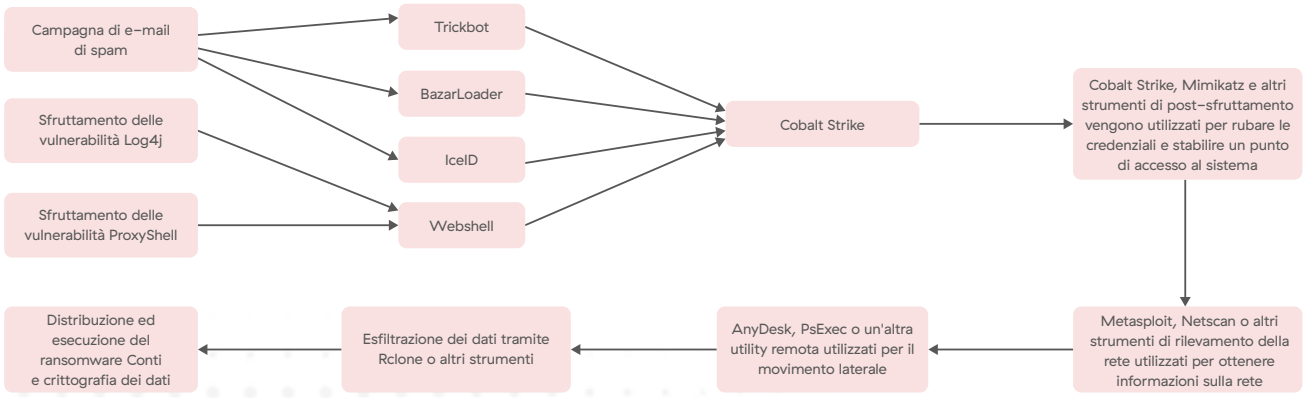


Figura 7: anatomia di un attacco del ransomware Conti

La prima versione di Conti impiegava gli algoritmi RSA e AES nel processo di crittografia. AES è stato in seguito sostituito con la crittografia ChaCha.

Alla fine di gennaio 2022, ThreatLabz ha identificato una versione aggiornata del ransomware Conti nell'ambito delle attività di monitoraggio dei ransomware a livello globale. Questo aggiornamento è stato rilasciato prima di una massiccia fuga del codice sorgente di Conti e dei log delle chat, pubblicati il 27 febbraio del 2022 da un ricercatore ucraino dopo l'invasione dell'Ucraina. La nuova versione di Conti presenta nuovi argomenti della riga di comando che consentono al ransomware di riavviare il sistema nella modalità provvisoria di Windows con la rete abilitata e quindi di avviare la crittografia. Avviando il sistema in modalità provvisoria, Conti è in grado di massimizzare il numero di file criptati, perché con tutta probabilità le applicazioni aziendali, come i database, non vengono eseguite. Conti ha anche aggiornato le estensioni dei file criptati, che ora includono caratteri maiuscoli, minuscoli e numeri. Inoltre, dopo aver criptato i file, cambia le impostazioni dello sfondo del desktop della vittima.

La figura 8 mostra i settori presi di mira dagli attacchi a doppia estorsione che utilizzano Conti.

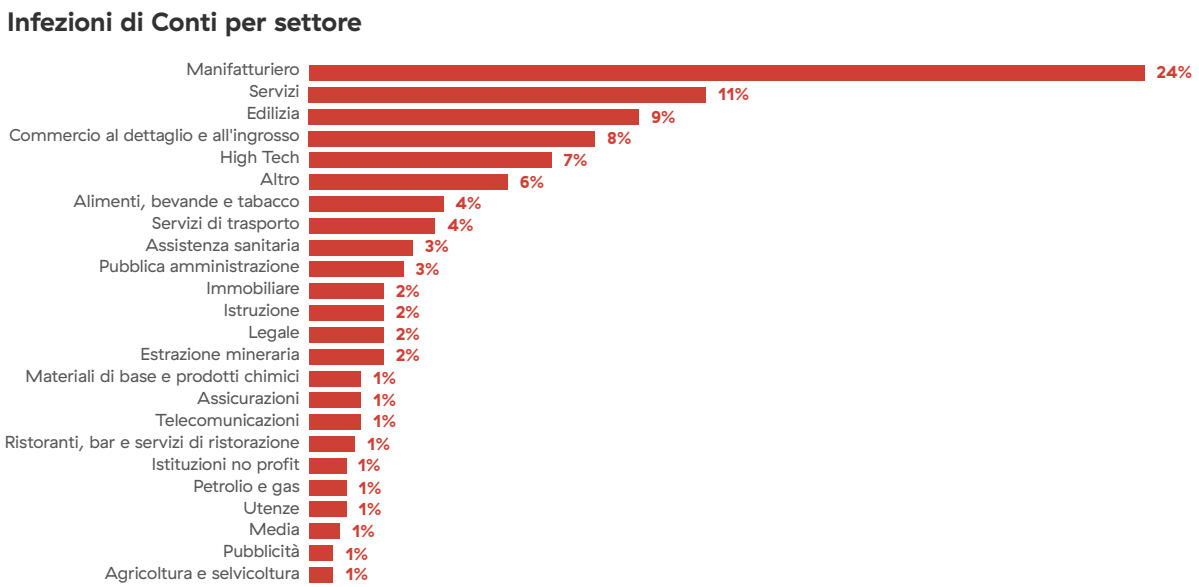


Figura 8: infezioni di Conti per settore

Conti ha creato un proprio sito di divulgazione dei dati rubati ad agosto del 2020; se un'azienda si rifiuta di pagare il riscatto, Conti procede alla pubblicazione dei dati rubati.

Figura 9: sito di divulgazione dei dati rubati di Conti

Conti: tattiche e tecniche MITRE ATT&CK

Accesso iniziale	Esecuzione	Persistenza	Escalation dei privilegi	Evasione della difesa	reciproca	Movimento laterale	Raccolta	Esfiltrazione	Impatto
Link di spear phishing	Interfaccia della riga di comando	Esecuzione automatica all'avvio o all'accesso	Manipolazione token di accesso	Deoffuscamento/decodifica di file o informazioni	Rilevamento della configurazione di rete del sistema	Trasferimento laterale dello strumento	Archiviazione dei dati raccolti	Esfiltrazione automatica	Dati criptati
Allegato di spear phishing	Esecuzione tramite caricamento del modulo		Sfruttamento per aumentare i privilegi	Compromissione delle difese	Rilevamento dei sistemi in remoto	Servizi da remoto	Dati dal sistema locale	Esfiltrazione tramite servizio web	Inibizione del ripristino di sistema
Exploit dell'applicazione rivolta al pubblico	Moduli condivisi			Iniezione nel processo	Rilevamento di file e directory				Arresto/riavvio del sistema
Account validi	Esecuzione utente				Rilevamento dei software di sicurezza				Deturpamento
Compromissione della catena di approvvigionamento					Ricerca nel registro				

LockBit

Il ransomware LockBit è emerso per la prima volta a settembre del 2019 come ransomware ABCD, il cui nome derivava dalla sua estensione ".abcd". All'inizio del 2020 è uscita una nuova versione che aggiunge l'estensione ".lockbit" ai file criptati. Nel 2020, LockBit si è unito al cartello di Maze e ha iniziato a pubblicare i dati delle vittime sul sito di divulgazione dei dati rubati di quest'ultimo. A settembre del 2020, quando Maze ha cessato le sue operazioni, LockBit ha aperto il proprio sito di divulgazione, come mostrato nella figura 10.

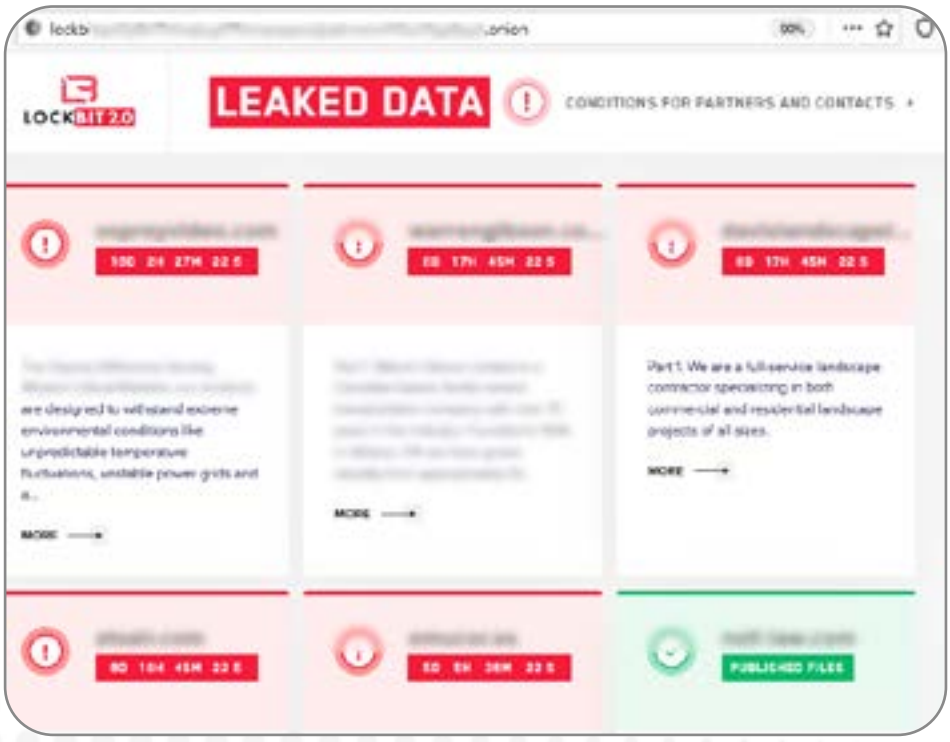


Figura 10: sito di divulgazione dei dati rubati di LockBit

A giugno del 2021 LockBit ha rilasciato una nuova versione chiamata LockBit 2.0, e a luglio del 2021 ha iniziato a pubblicare i dati delle vittime sul proprio sito di divulgazione. LockBit 2.0 utilizza il modello RaaS e ha operato reclutando affiliati impiegati nelle aziende target e con un accesso legittimo alla rete. Questo ransomware è stato distribuito tramite campagne di e-mail di spam contenenti allegati o link dannosi.

Per ottenere l'accesso, Lockbit ha anche adottato altre strategie, come la forza bruta per il furto di credenziali RDP o VPN tramite account RDP compromessi e sfruttando la vulnerabilità CVE-2018-13379 di Fortinet VPN.

Catena di infezione:
nel primo attacco di LockBit 2.0 che è stato osservato, gli aggressori hanno utilizzato un account RDP violato per accedere al sistema target. In seguito, hanno usato uno scanner di rete per recuperare informazioni sulla rete e individuare i controller di dominio. Gli aggressori hanno quindi usato StealBit per esfiltrare i dati e Process Hacker e PC Hunter per terminare i processi e i servizi del database e di altri strumenti. È stato utilizzato un file batch per disinstallare i prodotti di sicurezza e disattivare i log degli eventi di Windows e le funzionalità di Windows Defender. Infine, LockBit ha usato le policy di gruppo di Windows per distribuire ed eseguire il ransomware LockBit 2.0.

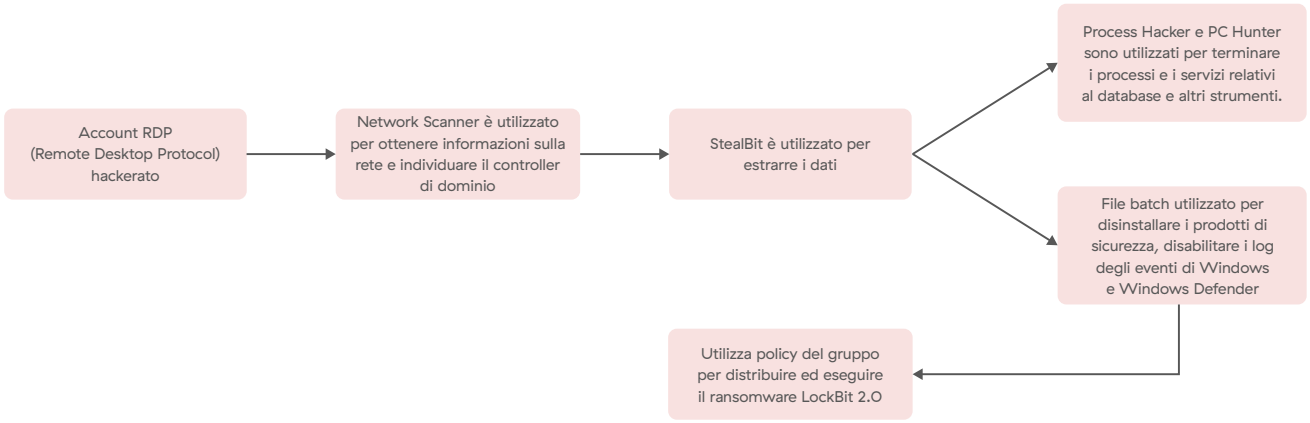


Figura 11: anatomia di un attacco del ransomware LockBit

Parte di ciò che rende LockBit così popolare è la sua efficienza: questo ransomware dispone del metodo di crittografia più veloce perché utilizza un approccio a più "thread" e cripta solo 4 KB di dati per ogni file; inoltre, utilizza una combinazione di algoritmi RSA e AES. LockBit ha rilasciato una variante per Linux e VMware ESXi a ottobre del 2021. Quest'ultima utilizza una combinazione di algoritmi AES (Advanced Encryption Standard) ed ECC (Elliptic-Curve Cryptography) per criptare i dati.

La figura 12 mostra i settori presi di mira dagli attacchi a doppia estorsione che utilizzano LockBit.

Infezioni di Lockbit per settore

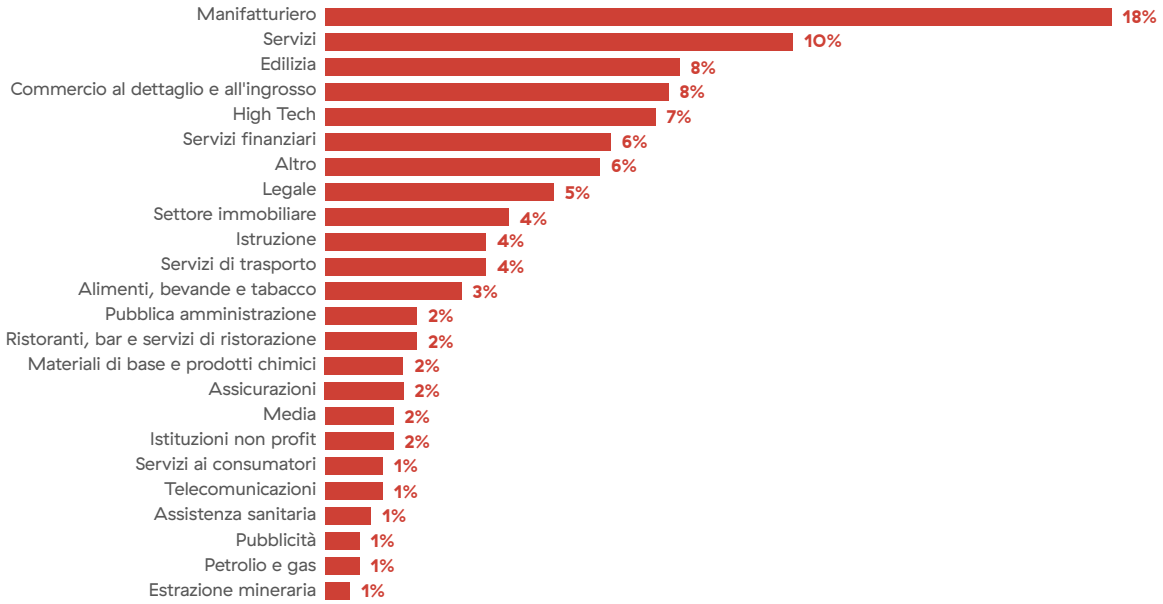


Figura 12: infezioni di LockBit per settore

LockBit: tattiche e tecniche MITRE ATT&CK

Accesso iniziale	Esecuzione	Persistenza	Escalation dei privilegi	Evasione della difesa	reciproca	Movimento laterale	Raccolta	Esfiltrazione	Impatto
Link di spear phishing	Interfaccia della riga di comando	Esecuzione automatica all'avvio o all'accesso	Abuso del meccanismo di controllo dell'aumento dei privilegi: elusione del controllo degli account utente	Deoffusca-mento/ decodifica di file o informazioni	Rilevamento della configurazione di rete del sistema	Trasferimento laterale dello strumento	Archiviazione dei dati raccolti	Esfiltrazione tramite servizio web	Dati criptati
Allegato di spear phishing				Danneggia-mento delle difese: disabilitazione o modifica degli strumenti	Rilevamento dei sistemi in remoto	Servizi da remoto	Dati dal sistema locale		Inibizione del ripristino di sistema
Account validi				Rimozione dell'indicatore sull'host: cancellazione dei log degli eventi di Windows	Rilevamento di file e directory				Deturpamento
Exploit dell'applica-zione rivolta al pubblico				Modifica delle policy del dominio: modifica delle policy di gruppo	Rilevamento dei software di sicurezza				
Compromissio-ne della catena di approvvigio-namento									

PYSA/Mespinoza

Il ransomware PYSA, noto anche come Mespinoza, è stato rilevato per la prima volta a ottobre del 2019. Questo ransomware attacca un'ampia varietà di settori in tutto il mondo, ma è noto in particolare per gli attacchi contro "bersagli deboli", come l'istruzione e gli ospedali.

Catena di infezione

PYSA effettua la compromissione iniziale tramite e-mail di spam o credenziali RDP compromesse. Successivamente, gli aggressori raccolgono le informazioni sulla rete tramite strumenti di scansione, come Port Scanner e Advanced IP Scanner, sviluppati da Famatech Corp. Utilizzano quindi strumenti di post-sfruttamento, come Mimikatz, PowerShell Empire, Koadic e PsExec, per rubare le credenziali e spostarsi lateralmente. I dati delle vittime vengono esfiltrati utilizzando lo strumento WinSCP. Uno script PowerShell disattiva il software di sicurezza ed elimina le copie shadow e i punti di ripristino del sistema, impedendo così alle vittime di ripristinare i dati. Infine, l'aggressore implementa ed esegue il ransomware PYSA e avvia la crittografia dei dati delle vittime.

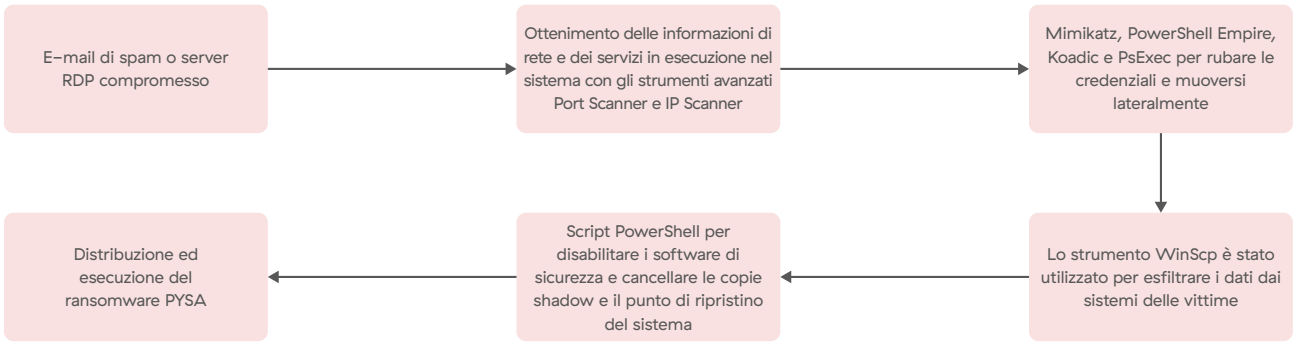


Figura 13: anatomia di un attacco del ransomware PYSA

Il 18% degli attacchi di PYSA ha preso di mira gli istituti d'istruzione.

PYSA utilizza una combinazione di algoritmi RSA e AES-CBC per criptare i file.

La figura 14 mostra i settori presi di mira dagli attacchi a doppia estorsione che utilizzano PYSA/Mespinoza.

Infezioni di PYSA/Mespinoza per settore

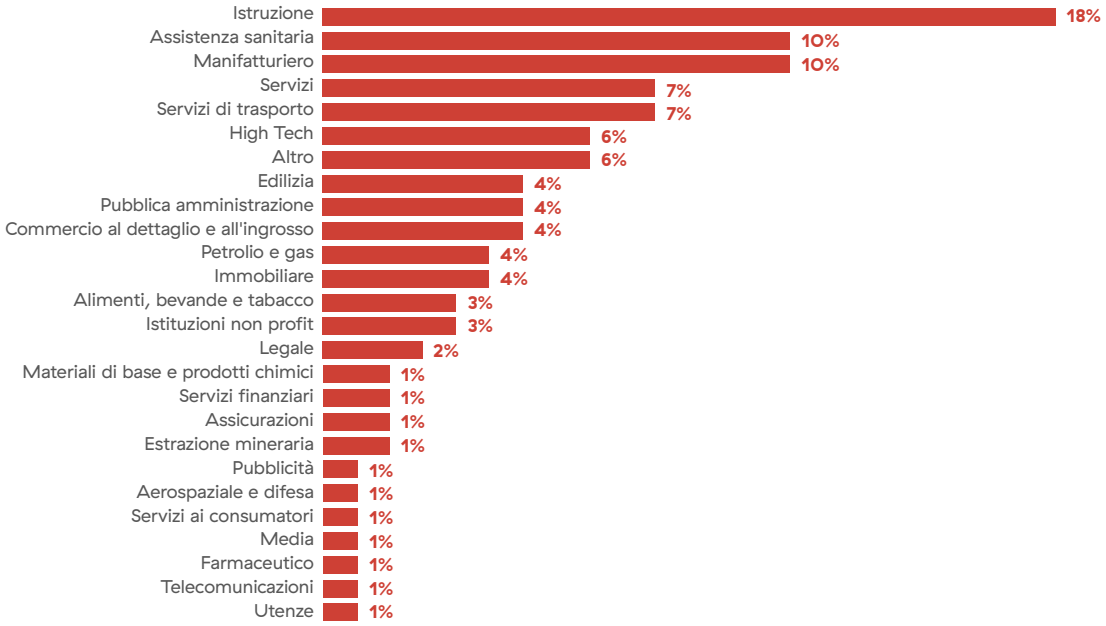


Figura 14: attacchi di PYSA/Mespinoza per settore

Se una vittima non paga il riscatto, PYSA pubblica i dati rubati sul suo sito di divulgazione (mostrato nella figura 15).

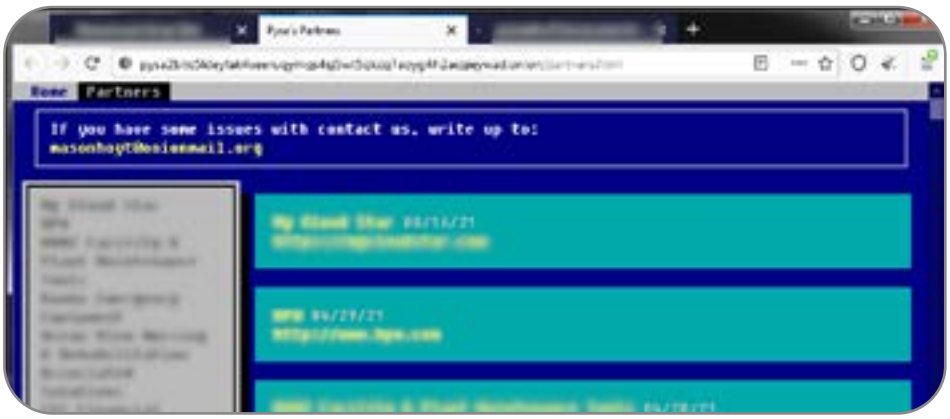


Figura 15: sito di divulgazione dei dati rubati di PYSA/Mespinoza

PYSA/Mespinoza: tattiche e tecniche MITRE ATT&CK

Accesso iniziale	Esecuzione	Persistenza	Escalation dei privilegi	Evasione della difesa	reciproca	Movimento laterale	Raccolta	Esfiltrazione	Impatto
Link di spear phishing	Interfaccia della riga di comando	Esecuzione automatica all'avvio o all'accesso	Manipolazione token di accesso	Deoffusca-mento/deco-difica di file o informazioni	Rilevamento della configu-razione di rete del sistema	Trasferimento laterale dello strumento	Archiviazione dei dati raccolti	Esfiltrazione tramite protocollo alternativo	Dati criptati
Allegato di spear phishing	Esecuzione tramite caricamento del modulo	Attività/ processo pianificati		Compromis-sione delle difese	Rilevamento dei sistemi in remoto		Dati dal sistema locale	Esfiltrazione tramite servizio web	Inibizione del ripristino di sistema
Account validi	Esecuzione utente			Modifica delle policy del dominio: modifica delle policy di gruppo	Rilevamento di file e directory				
					Rilevamento dei software di sicurezza				
					Ricerca nel registro				

REvil/Sodinokibi

Il ransomware REvil (o Sodinokibi) è stato individuato per la prima volta ad aprile del 2019, ed è stato uno dei ransomware più utilizzati negli ultimi anni. Anche REvil utilizza un ecosistema RaaS, e ha iniziato a praticare la doppia estorsione a gennaio del 2020, quando per la prima volta ha pubblicato i dati su un forum di hacking. A febbraio del 2020, gli aggressori responsabili di Sodinokibi hanno lanciato il proprio sito di divulgazione dei dati rubati, come mostrato nella figura 16.

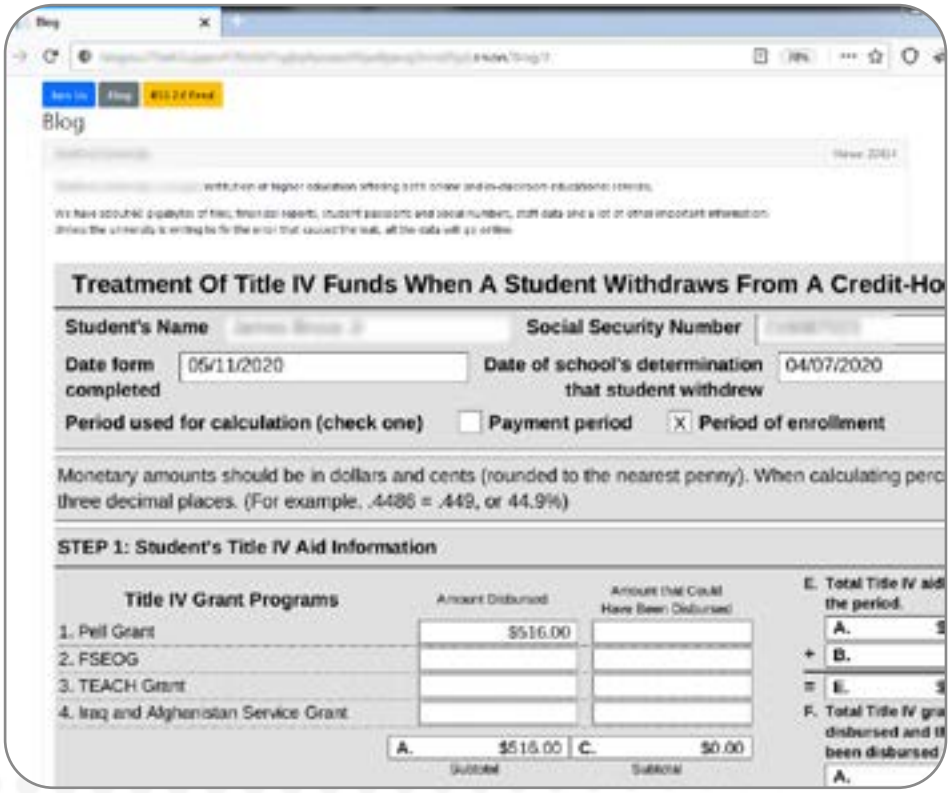


Figura 16: sito di divulgazione dei dati rubati di REvil/Sodinokibi

Inoltre, i dati rubati sul loro sito sono stati venduti all'asta, ma questa attività si è rivelata fallimentare.

Il gruppo responsabile di REvil è noto per aver sfruttato una vulnerabilità 0-day nel server di Kaseya VSA a luglio del 2021. Il server di Kaseya VSA compromesso è stato utilizzato per inviare uno script dannoso a tutti i client gestiti da quello specifico server.

Come già osservato in precedenza, sembrerebbe che i membri di REvil siano stati arrestati dalle autorità russe a gennaio del 2022. Tuttavia, il ransomware è stato aggiornato e l'infrastruttura è tornata online ad aprile dello stesso anno, quando gli attacchi di REvil sono ripresi.

Catena di infezione

Gli affiliati di REvil utilizzano diversi meccanismi di accesso iniziale, tra cui e-mail di spam, kit di exploit, account RDP compromessi ed exploit delle vulnerabilità. Una tipica campagna inizia con un'e-mail di spam contenente un allegato dannoso. Quest'ultimo, una volta aperto, scarica un trojan, come ad esempio IcedID, che serve per il movimento laterale. Come mostrato nella figura 17, gli affiliati di REvil utilizzano una serie di strumenti diversi, come Cobalt Strike, SharpSploit, Mimikatz e altri strumenti di post-sfruttamento per rubare le credenziali. Inoltre, raccolgono informazioni sulla rete utilizzando Netscan, BloodHound, AdFind e altri strumenti di rilevamento della rete. Gli aggressori si muovono lateralmente utilizzando PsExec o l'accesso RDP. L'esfiltrazione dei dati viene eseguita utilizzando FileZilla, Rclone, MEGAsync o FreeFileSync. Prima di distribuire il ransomware, gli affiliati di REvil utilizzano PC Hunter, Process Hacker, KillAV e/o altri script per terminare i processi e i servizi dei software di sicurezza. Infine, gli aggressori distribuiscono il ransomware REvil e criptano i dati.

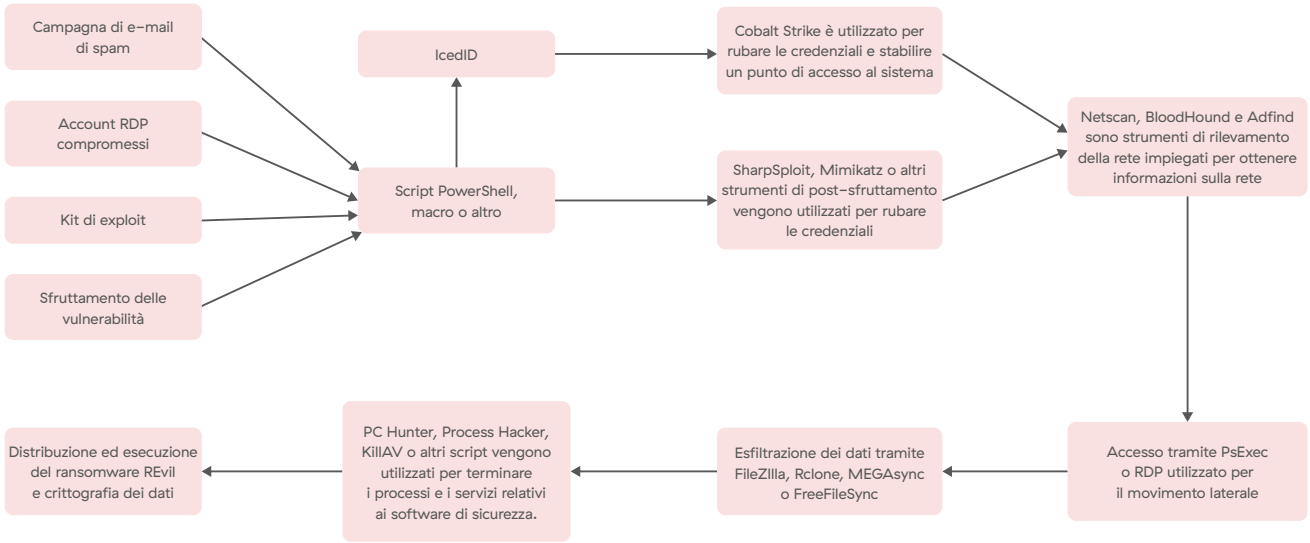


Figura 17: catena di attacco di REvil/Sodinokibi

REvil utilizza la crittografia ECC e usa una combinazione di Curve25519 e Salsa20 per criptare i file.

La figura 18 mostra i settori presi di mira dagli attacchi a doppia estorsione che utilizzano REvil.

Infezioni di REvil/Sodinokibi per settore

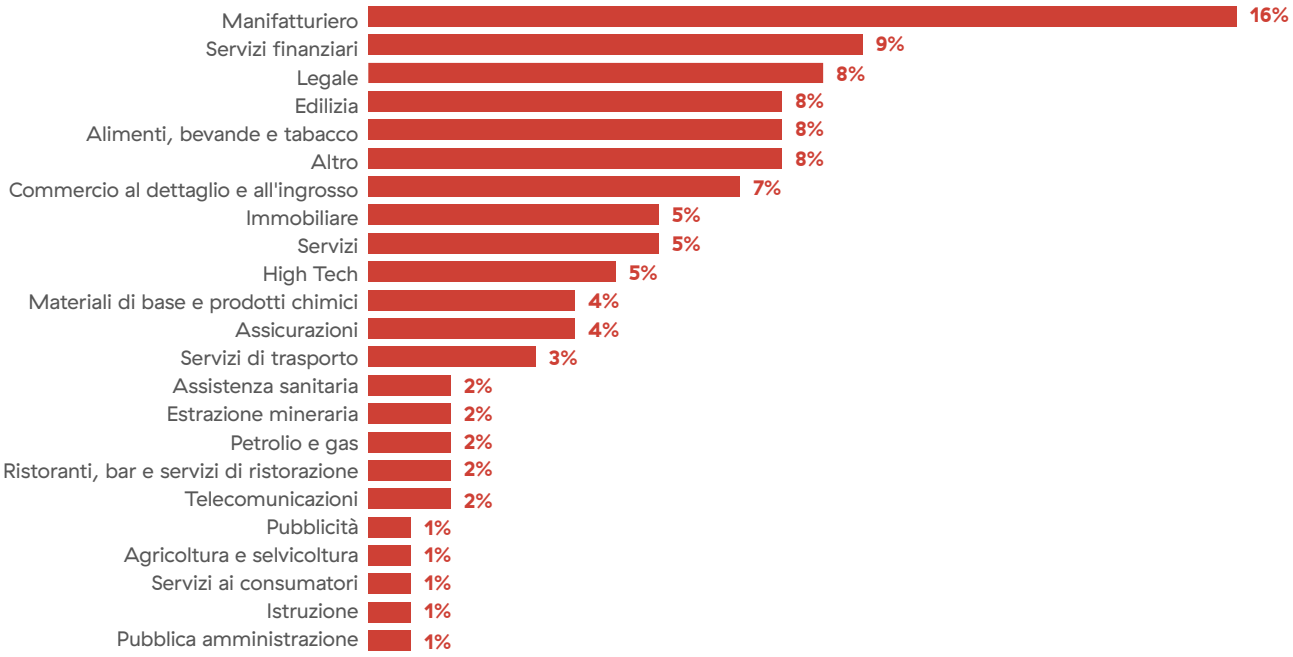


Figura 18: infezioni di REvil/Sodinokibi per settore

REvil/Sodinokibi: tattiche e tecniche MITRE ATT&CK

Accesso iniziale	Esecuzione	Persistenza	Escalation dei privilegi	Evasione della difesa	reciproca	Movimento laterale	Raccolta	Esfiltrazione	Impatto
Link di spear phishing	Interfaccia della riga di comando	Esecuzione automatica all'avvio o all'accesso	Manipolazione token di accesso	Deoffusca-mento/deco-difica di file o informazioni	Rilevamento della configu-razione di rete del sistema	Trasferimento laterale dello strumento	Archiviazione dei dati raccolti	Esfiltrazione automatica	Dati criptati
Allegato di spear phishing	Esecuzione tramite caricamento del modulo	Dirottamento del flusso di esecuzione	Dirottamento del flusso di esecuzione	Compromis-sione delle difese	Rilevamento dei sistemi in remoto	Servizi da remoto	Dati dal sistema locale	Esfiltrazione tramite servizio web	Inibizione del ripristino di sistema
Exploit dell'applica-zione rivolta al pubblico	Moduli condivisi		Sfruttamento per aumentare i privilegi		Rilevamento di file e directory				Arresto/riavvio del sistema
Compromesso drive-by	Esecuzione utente				Rilevamento dei software di sicurezza				Deturpamento
Account validi					Ricerca nel registro				
Compromis-sione della catena di approvvi-gionamento									

Avaddon

Il ransomware Avaddon è stato individuato per la prima volta a giugno del 2020, periodo in cui era molto attivo. Si tratta di un'altra famiglia di ransomware che utilizzava l'ecosistema RaaS. A gennaio del 2021, Avaddon ha aggiunto i DDoS alla sua attività per mettere in atto tattiche a tripla estorsione. Questo ransomware lanciava attacchi DDoS sul sito web o sulla rete delle vittime per spingerle a negoziare con gli operatori, richiedendo riscatti dalle somme più elevate.

Catena di infezione
Avaddon otteneva l'accesso tramite diversi affiliati che utilizzavano una varietà di vettori per la compromissione iniziale. È stato ampiamente distribuito tramite campagne spam e kit di exploit, ma alcuni affiliati hanno utilizzato attacchi di forza bruta o compromesso le credenziali RDP e VPN per ottenere l'accesso alle reti.

In una tipica catena di attacco, Avaddon otteneva l'accesso a un broker inizialmente infettato tramite credenziali compromesse e, per entrare nei sistemi target, utilizzava malware personalizzati, come le web shell BlackCrow e DarkRaven. Avaddon utilizzava SystemBC per ottenere l'accesso agli host compromessi, quindi Mimikatz e SharpDump per rubare le credenziali. In seguito, eseguiva la scansione della rete utilizzando SoftPerfect Network Scanner, PowerSploit ed Empire. Per gli spostamenti laterali, gli affiliati di Avaddon utilizzavano RDP e le Attività pianificate di Windows per la persistenza. Prima di rilasciare il carico utile principale del ransomware, gli aggressori esfiltravano i dati utilizzando MEGAsync e terminavano i processi e i servizi dei software di sicurezza. Infine, scaricavano ed eseguivano il carico utile di Avaddon e criptavano i sistemi target.

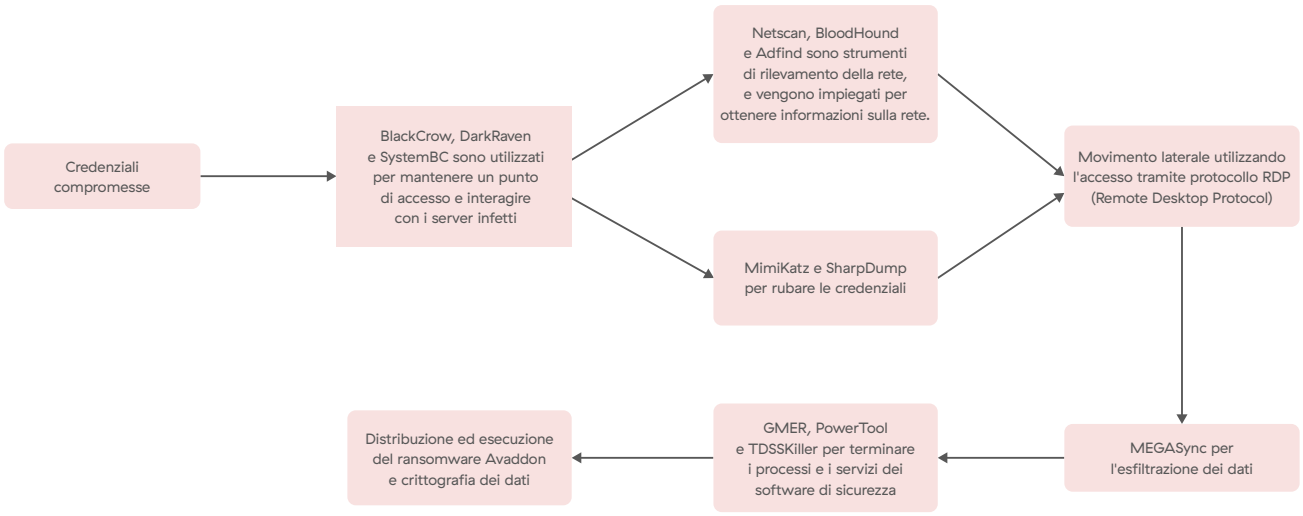


Figura 19: anatomia di un attacco del ransomware Avaddon

Avaddon impiegava una combinazione di algoritmi RSA e AES per criptare i file. Nel mese di febbraio, un ricercatore ha rilasciato un decrypter gratuito dopo aver scoperto un difetto, che Avaddon ha poi risolto. A giugno del 2021, Avaddon ha cessato le proprie operazioni e ha reso disponibili le chiavi di decriptazione delle vittime, consentendo a Emsisoft di creare un decrypter per questo ransomware.

In modo analogo alle altre famiglie di ransomware già discusse, Avaddon ha lanciato un sito web per la divulgazione dei dati rubati ad agosto del 2020, come mostrato nella figura 20.

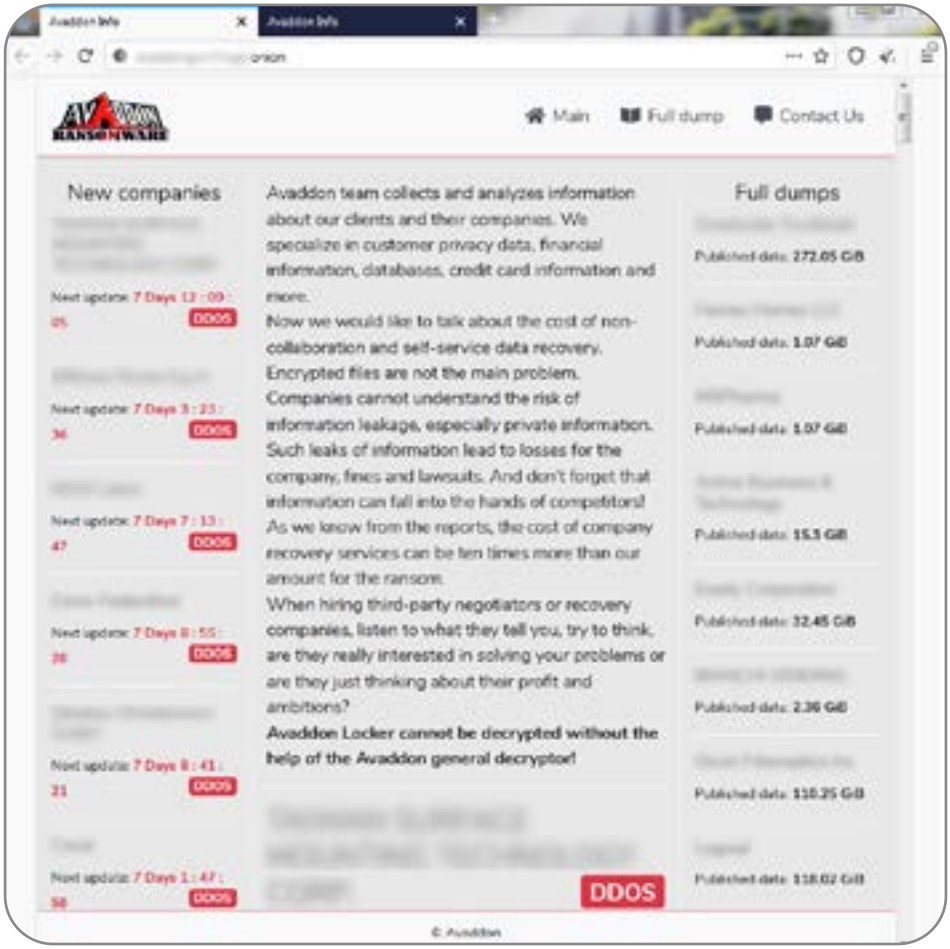


Figura 15: sito di divulgazione dei dati rubati di Avaddon

Dopo la cessazione delle attività di Avaddon, a giugno del 2021, il gruppo ha ripreso gli attacchi utilizzando il generatore di ransomware Thanos, ribattezzando Avaddon con il nome di Haron e cambiando nuovamente il nome del ransomware in Midas nel 2021.

La figura 21 mostra i settori presi di mira dagli attacchi a doppia estorsione che utilizzano Avaddon.

Infezioni Avaddon per settore

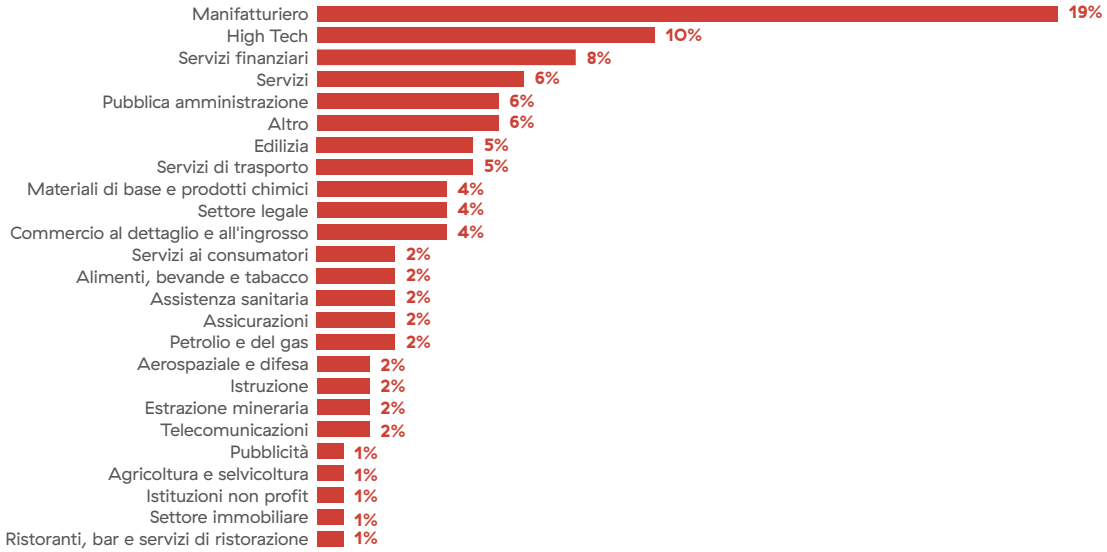


Figura 21: infezioni di Avaddon per settore

Avaddon: tattiche e tecniche MITRE ATT&CK

Accesso iniziale	Esecuzione	Persistenza	Escalation dei privilegi	Evasione della difesa	reciproca	Movimento laterale	Raccolta	Esfiltrazione	Impatto
Link di spear phishing	Interfaccia della riga di comando	Esecuzione automatica all'avvio o all'accesso	Account validi	Deoffusca-mento/ decodifica di file o infor-mazioni	Rilevamento della configu-razione di rete del sistema	Trasferimento laterale dello strumento	Archiviazione dei dati raccolti	Esfiltrazione tramite protocollo alternativo	Dati criptati
Allegato di spear phishing	Attività/ processo pianificati	Account validi		Compromis-sione delle difese	Rilevamento dei sistemi in remoto	Servizi da remoto: protocollo RDP	Dati dal sistema locale		Inibizione del ripristino di sistema
Exploit dell'applica-zione rivolta al pubblico	Esecuzione utente			Iniezione nel processo	Rilevamento di file e directory				
Compromesso drive-by				Rimozione dell'indicatore sull'host	Rilevamento dei software di sicurezza				
Account validi				Rimozione dell'indicatore sull'host	Rilevamento dei software di sicurezza				

Clop

Il ransomware Clop è stato individuato per la prima volta a febbraio del 2019. A marzo del 2020, Clop ha iniziato a utilizzare la doppia estorsione, divulgando i dati rubati delle organizzazioni compromesse che non pagavano il riscatto sul proprio sito web, come mostrato nella figura 22.

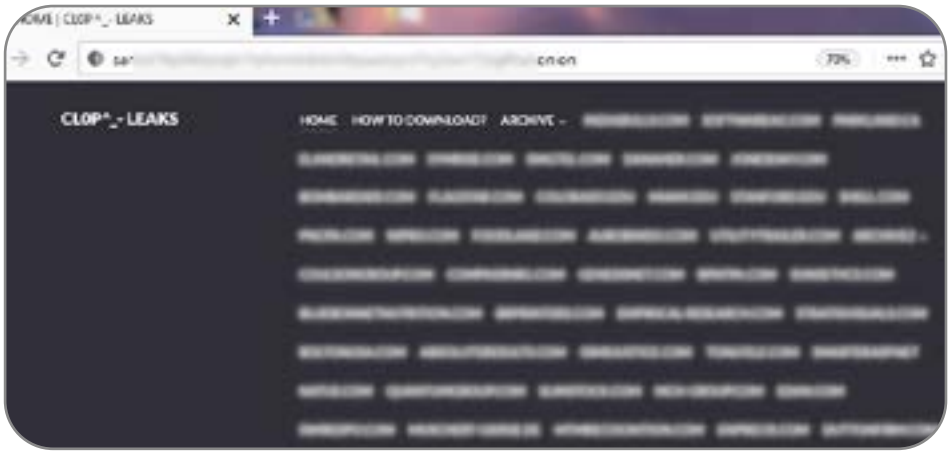


Figura 22: sito di divulgazione dei dati rubati di Clop

Il gruppo di Clop prende di mira soprattutto le grandi organizzazioni. ThreatLabz ha scoperto che questo gruppo richiede riscatti a otto cifre e rifiuta persino offerte di pagamento di vari milioni di dollari.

Clop è stato inizialmente diffuso dai gruppi TA505 e FIN11. Questo ransomware è stato ampiamente distribuito tramite le campagne di spam condotte dal gruppo TA505. ThreatLabz ha osservato che, per l'accesso iniziale, diversi attacchi di Clop hanno sfruttato la vulnerabilità di SolarWinds Serv-U, CVE-2021-35211, che consente l'esecuzione di codice da remoto con privilegi elevati. Il gruppo di FIN11 sfruttava diverse vulnerabilità di Accellion FTA (File Transfer Appliance) come CVE-2021-27101, CVE-2021-27102, CVE-2021-27103 e CVE-2021-27104. FIN11 rilascia quindi la web shell DEWMODE, che esfiltra i dati prima di rilasciare ed eseguire il ransomware Clop.

Clop è stato responsabile di attacchi di alto profilo e, a partire da novembre del 2021, ha causato danni per un ammontare stimato di 500 milioni di dollari.

Catena di infezione

Un attacco tipico di TA505 prevede una compromissione attraverso un'e-mail di spam contenente un allegato HTML. L'allegato reindirizza a un file di documento XLS che rilascia in aggiunta anche il loader Get2. Quest'ultimo scarica ulteriori carichi utili, come SdBot, FlawedAmmy, FlawedGrace e Cobalt Strike. Dopo aver ottenuto un punto di accesso alla rete, e aver rubato ed esfiltrato i dati, il gruppo distribuisce ed esegue il ransomware Clop, come illustrato nella figura 23.

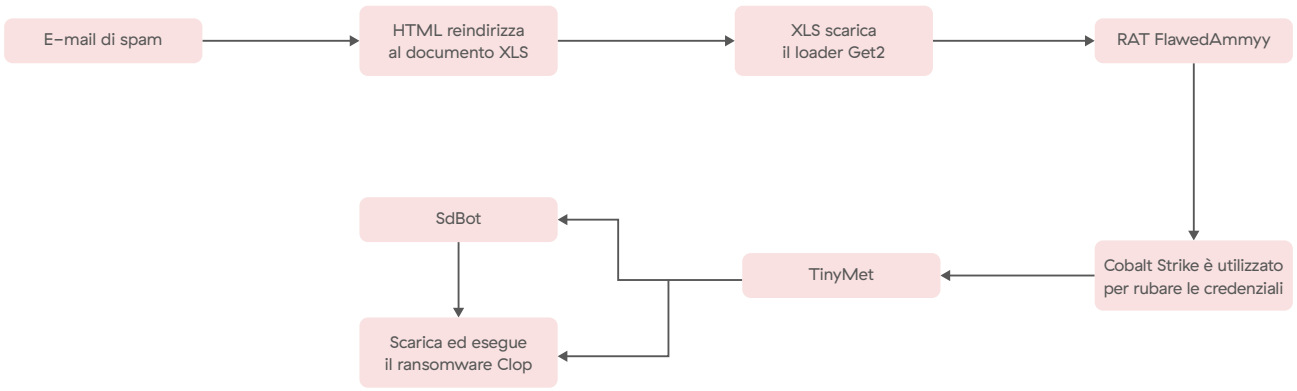


Figura 23: anatomia di un attacco del ransomware Clop

Clop utilizza una combinazione di algoritmi RSA e AES per crittografare i file.

La figura 24 mostra i settori presi di mira dagli attacchi a doppia estorsione che utilizzano Clop.

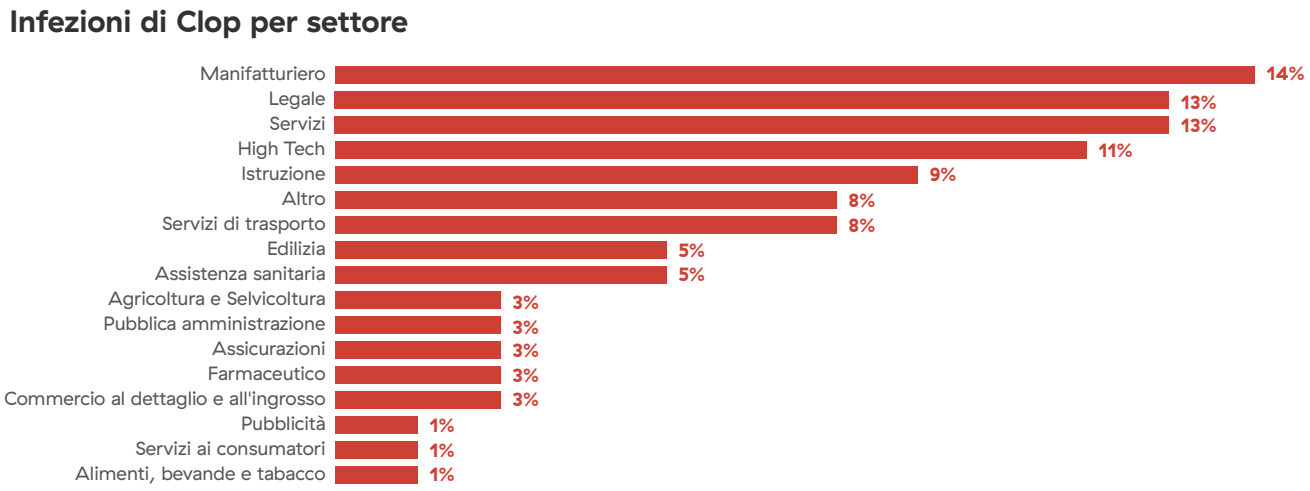


Figura 24: infezioni di Clop per settore

Clop: tattiche e tecniche MITRE ATT&CK

Accesso iniziale	Esecuzione	Persistenza	Escalation dei privilegi	Evasione della difesa	reciproca	Movimento laterale	Esfiltrazione	Impatto
Account validi	Interfaccia della riga di comando	Esecuzione automatica all'avvio o all'accesso	Manipolazione token di accesso	Mascheramento: invalidamento della firma del codice	Rilevamento della configurazione di rete del sistema	Trasferimento laterale dello strumento	Esfiltrazione automatica	Dati criptati
Allegato di spear phishing	Esecuzione utente	Creazione o modifica di un processo di sistema: servizio di Windows	Bypass del con-trollo dell'account utente	Compromissione delle difese: disabilitazione o modifica degli strumenti	Rilevamento dei sistemi in remoto	Servizi da remoto	Esfiltrazione tramite servizio web	Inibizione del ripristino di sistema
Exploit dell'applicazione rivolta al pubblico	API nativa		Sfruttamento per aumentare i privilegi	Deoffuscamento/ decodifica di file o informazioni	Rilevamento di file e directory			
Compromissione della catena di approvvigiona-mento				Iniezione nel processo: iniezione DLL	Ricerca nel registro			
				Esecuzione indiretta dei comandi	Rilevamento dei software di sicurezza			

Grief

Grief è un rebranding del ransomware DoppelPaymer, la cui attività è diminuita significativamente a maggio del 2021, in seguito all'attacco a Colonial Pipeline. Questo ransomware presenta molte somiglianze con DoppelPaymer, tra cui il codice del ransomware e i siti web di divulgazione dei dati. Una schermata esemplificativa del sito di divulgazione di Grief è mostrata nella figura 25.

Figura 25: sito di divulgazione dei dati rubati di Grief

Il portale per la richiesta dei riscatti di questo ransomware presenta alcune differenze rispetto al portale di DoppelPaymer. In particolare, il metodo di pagamento della richiesta di riscatto è in Monero anziché in bitcoin. La criptovaluta potrebbe essere cambiata in risposta al recupero da parte dell'FBI di una porzione del riscatto di Colonial Pipeline, che era stato pagato in bitcoin.

Catena di infezione

Il ransomware Grief viene distribuito su sistemi precedentemente infettati con Dridex, che l'aggressore utilizza prima di impiegare Cobalt Strike e distribuire ed eseguire il carico utile di Grief. Quest'ultimo utilizza una combinazione di algoritmi RSA a 2048 bit e AES a 256 bit per criptare i file.

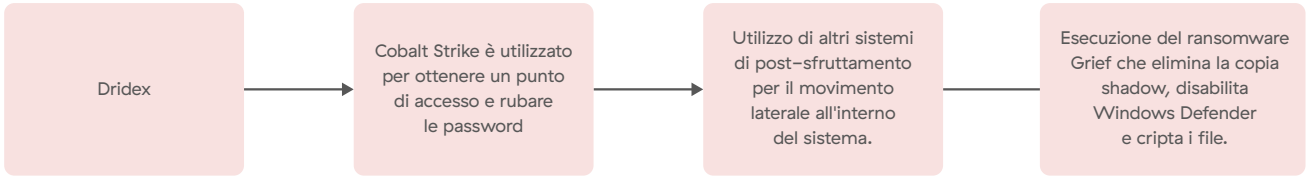


Figura 26: anatomia di un attacco del ransomware Grief

La figura 27 mostra i settori presi di mira dagli attacchi a doppia estorsione che utilizzano Grief.

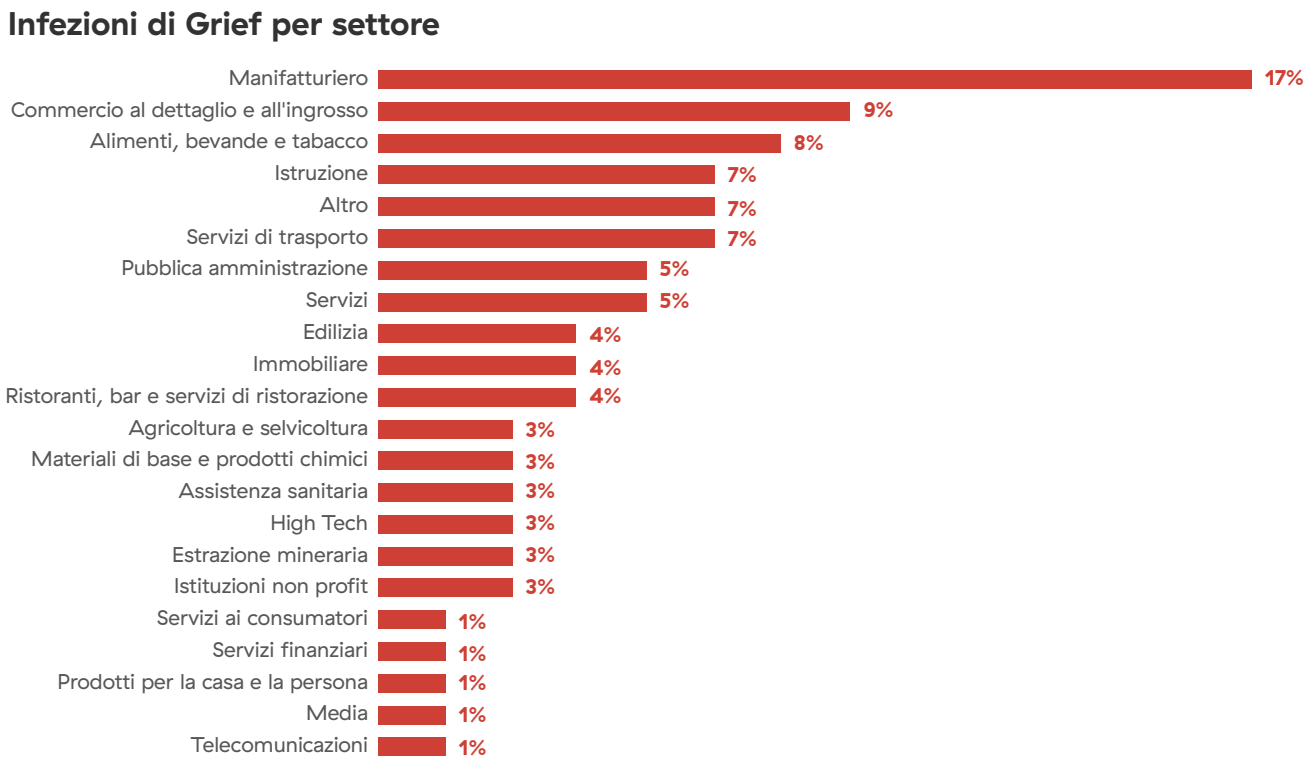


Figura 24: infezioni di Grief per settore

Grief: tattiche e tecniche MITRE ATT&CK

Accesso iniziale	Esecuzione	Persistenza	Escalation dei privilegi	Evasione della difesa	reciproca	Movimento laterale	Esfiltrazione	Impatto
Account validi	Interfaccia della riga di comando	Esecuzione automatica all'avvio o all'accesso: chiavi di esecuzione del registro/ cartella di avvio	Iniezione nel processo	Dirottamento del flusso di esecuzione: dirottamento dell'ordine di ricerca delle DLL	Rilevamento della configurazione di rete del sistema	Trasferimento laterale dello strumento	Trasferimento programmato	Dati criptati
Allegato di spear phishing	Esecuzione utente	Attività/ processo pianificati		Deoffuscamento/ decodifica di file o informazioni	Rilevamento dei sistemi in remoto			Inibizione del ripristino di sistema
	Moduli condivisi			Compromissione delle difese: disabilitazione o modifica degli strumenti	Rilevamento di file e directory			Arresto/riavvio del sistema
				Mascheramento: corrispondenza con un nome o una posizione legittima	Rilevamento dei software di sicurezza			

Hive

Il ransomware Hive è stato individuato per la prima volta a giugno del 2021, e sfrutta un modello RaaS. Questo ransomware utilizza più meccanismi per ottenere l'accesso iniziale, tra cui le e-mail di spam dannose, le credenziali VPN divulgate e gli exploit delle vulnerabilità nelle risorse che si interfacciano con l'esterno. L'infezione iniziale inizia con lo sfruttamento delle vulnerabilità ProxyShell presenti in Microsoft Exchange Server. Le vulnerabilità ProxyShell di Exchange sono una combinazione di CVE-2021-34473 (vulnerabilità all'esecuzione di codice da remoto di Microsoft Exchange Server), CVE-2021-34523 (vulnerabilità all'aumento dei privilegi di Microsoft Exchange Server) e CVE-2021-31207 (vulnerabilità all'elusione delle funzionalità di sicurezza di Microsoft Exchange Server).

Catena di infezione

L'aggressore crea un'e-mail bozza all'interno di una casella di posta elettronica con un allegato che contiene la web shell codificata. L'aggressore esporta quindi l'intera casella di posta (inclusa l'e-mail in bozza dannosa) in formato PST con estensione ASPX. Ciò consente agli aggressori di rilasciare la web shell sui server vulnerabili.La web shell scarica lo script PowerShell, che contiene il carico utile Cobalt Strike codificato. Scarica inoltre ulteriori stager e stabilisce un punto di accesso al sistema della vittima. Utilizza quindi Mimikatz per rubare gli hash NTLM e sfrutta una tattica "pass the hash" per accedere all'account di controllo del dominio. Hive esegue un ulteriore movimento laterale sull'RDP, utilizzando le credenziali rubate, esegue una scansione della rete e ottiene ulteriori informazioni utilizzando lo scanner SoftPerfect Network. Infine, distribuisce ed esegue il ransomware e cripta i dati.

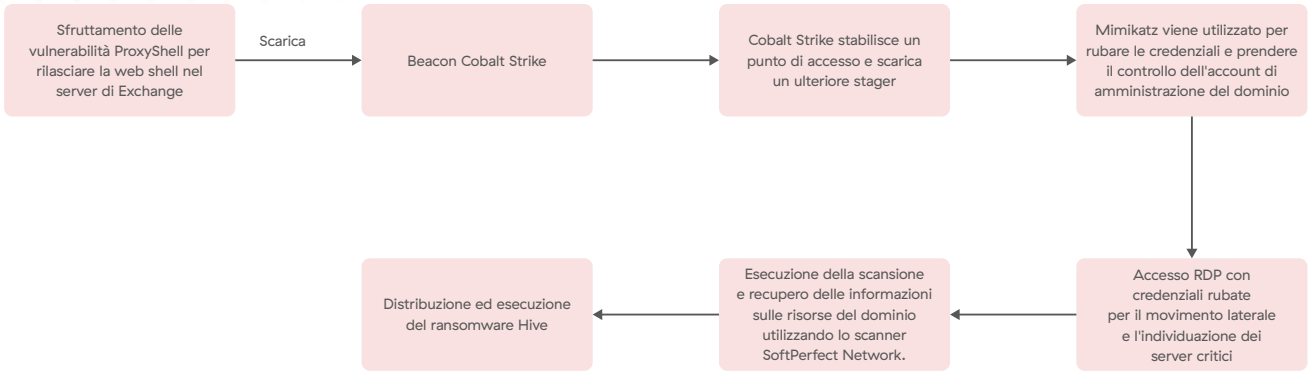


Figura 28: catena di attacco di Hive

Le versioni precedenti del carico utile del ransomware Hive erano scritte nel linguaggio di programmazione Go, e utilizzavano una combinazione di algoritmi RSA e AES per criptare i file. Le versioni più recenti, invece, sono scritte nel linguaggio di programmazione Rust e utilizzano Curve25519 e ChaCha20 per criptare i file.

Gli affiliati di Hive esfiltrano i dati delle vittime anche prima di criptare i file. La figura 29 mostra una schermata del sito di Hive di divulgazione dei dati rubati.

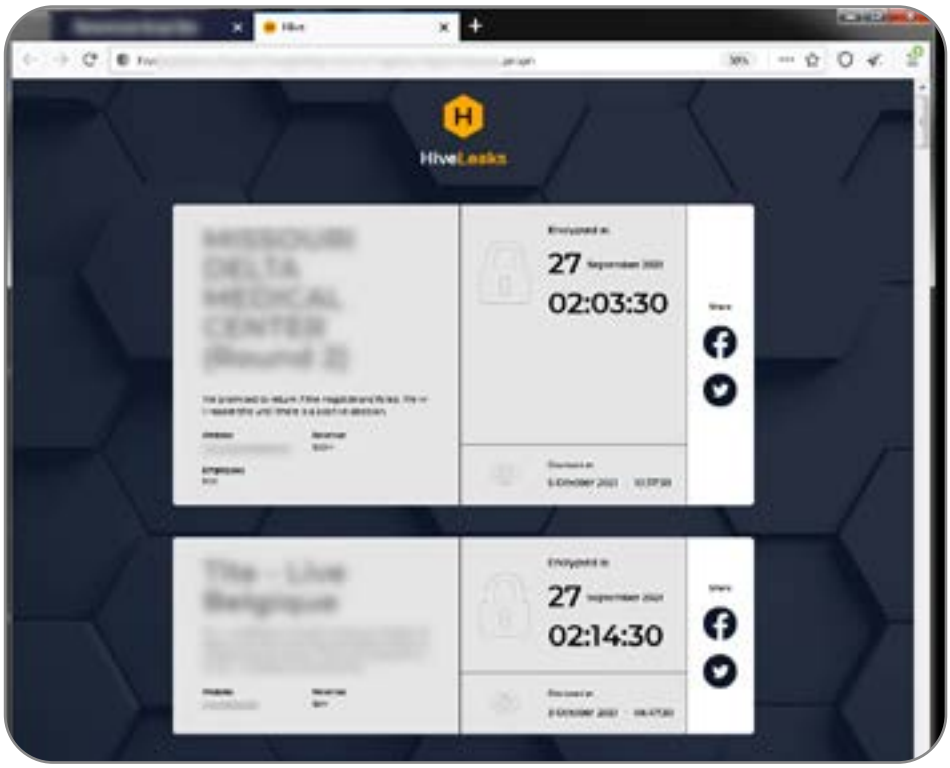


Figura 29: sito di divulgazione dei dati rubati di Hive

La figura 30 mostra i settori presi di mira dagli attacchi a doppia estorsione che utilizzano Hive.

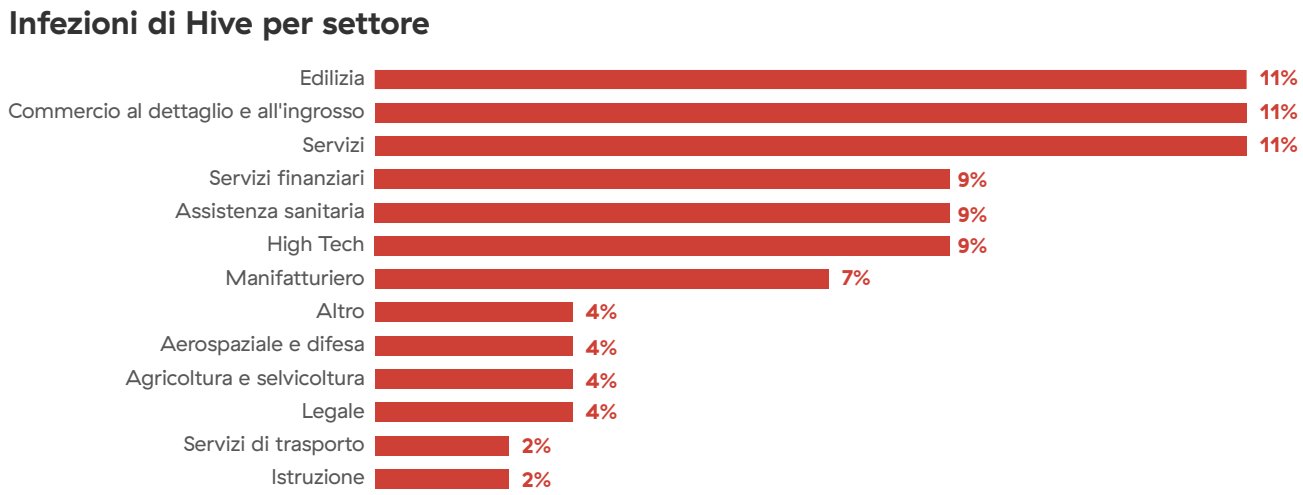


Figura 30: infezioni di Hive per settore

Hive: tattiche e tecniche MITRE ATT&CK

Accesso iniziale	Esecuzione	Persistenza	Escalation dei privilegi	Evasione della difesa	reciproca	Movimento laterale	Esfiltrazione	Impatto
Servizi da remoto esterni	Interfaccia della riga di comando	Account validi: account di dominio	Account validi	Cancellazione dei log degli eventi di Windows	Rilevamento della configurazione di rete del sistema	Protocollo RDP	Trasferimento programmato	Dati criptati
Allegato di spear phishing	Esecuzione utente	Creazione di un account: account di dominio	Account di dominio	Compromissione delle difese: disabilitazione o modifica degli strumenti	Rilevamento dei sistemi in remoto	Servizi da remoto		Inibizione del ripristino di sistema
Exploit dell'applicazione rivolta al pubblico			Sfruttamento per aumentare i privilegi	Deoffuscamento/ decodifica di file o informazioni	Rilevamento di file e directory			
					Ricerca nel registro			
					Rilevamento dei software di sicurezza			

BlackByte

BlackByte è un altro gruppo RaaS apparso a luglio del 2021. Originariamente era scritto in C#, e successivamente è stato riprogettato con il linguaggio di programmazione Go, intorno a settembre del 2021. La versione basata su Go condivide molte somiglianze con la versione C#, inclusi i comandi eseguiti per effettuare la propagazione laterale, l'escalation dei privilegi e la crittografia dei file.

Le campagne BlackByte iniziano sfruttando le vulnerabilità ProxyShell presenti in Microsoft Exchange Server.

Catena di infezione
L'aggressore crea un'e-mail in bozza all'interno di una casella di posta elettronica. Questa e-mail contiene un allegato con la web shell codificata. L'aggressore esporta quindi l'intera casella di posta (inclusa l'e-mail in bozza dannosa) in formato PST con un'estensione ASPX. Ciò consente agli aggressori di spostare le web shell sui server vulnerabili.

Successivamente, la web shell viene utilizzata per rilasciare un beacon Cobalt Strike sul server di Exchange preso di mira. Cobalt Strike viene utilizzato insieme ad altri strumenti di post-sfruttamento per rubare le credenziali, ottenere l'accesso agli account di servizio e un punto di accesso al sistema. Inoltre, BlackByte installa lo strumento AnyDesk RDP. Quest'ultimo viene utilizzato per il movimento laterale e per rilasciare Cobalt Strike nel controller di dominio infetto. Infine, Cobalt Strike distribuisce ed esegue il ransomware BlackByte.

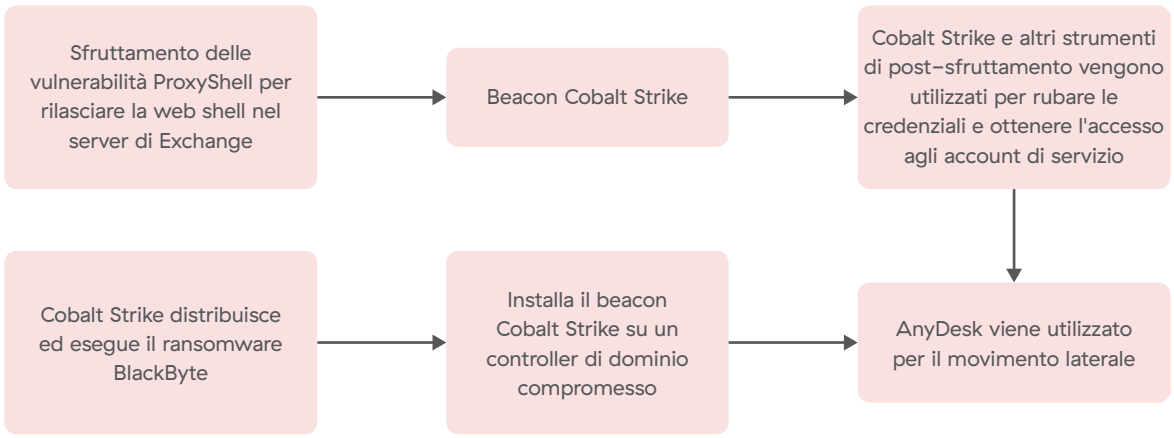


Figura 31: anatomia di un attacco del ransomware BlackByte

L'accesso iniziale avviene sfruttando le vulnerabilità ProxyShell per il rilascio di una web shell sul server di Exchange. Quest'ultima scarica quindi il beacon Cobalt Strike, che ruba le credenziali e installa lo strumento AnyDesk RDP. AnyDesk viene utilizzato per il movimento laterale e rilascia Cobalt Strike nel controller di dominio infetto. Quest'ultimo viene infine utilizzato per distribuire ed eseguire il ransomware BlackByte.

BlackByte utilizza una combinazione di algoritmi RSA e AES per criptare i file. Le versioni più recenti del ransomware utilizzano Curve25519 ECC per la crittografia asimmetrica e ChaCha20 per la crittografia simmetrica dei file.

Gli aggressori che utilizzano BlackByte esfiltrano i dati delle vittime anche prima di criptare i file. La figura 32 mostra una schermata del sito di divulgazione dei dati rubati di BlackByte.

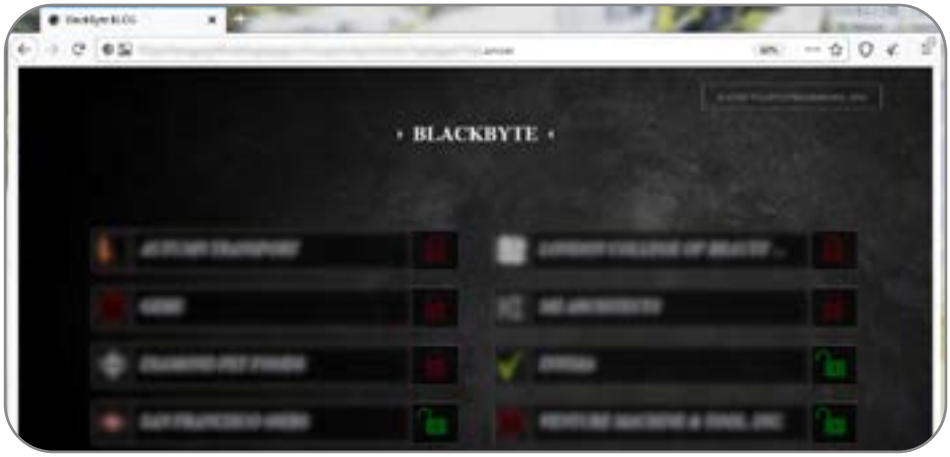


Figura 32: sito di divulgazione dei dati rubati di BlackByte

La figura 33 mostra i settori presi di mira dagli attacchi a doppia estorsione che utilizzano BlackByte.

Infezioni di BlackByte per settore

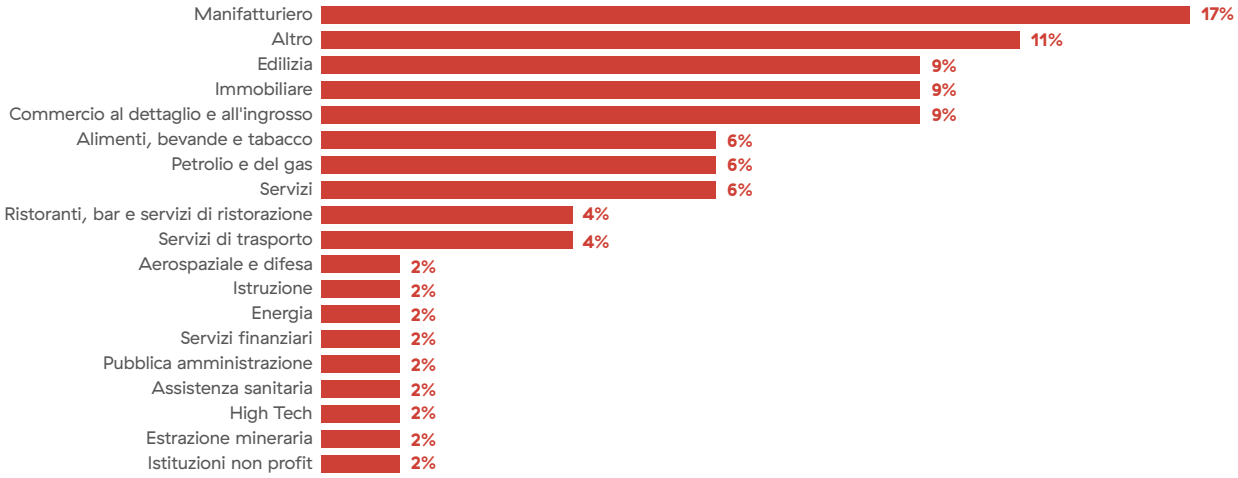


Figura 33: infezioni di BlackByte per settore

BlackByte: tattiche e tecniche MITRE ATT&CK

Accesso iniziale	Esecuzione	Persistenza	Escalation dei privilegi	Evasione della difesa	reciproca	Movimento laterale	Esfiltrazione	Impatto
Allegato di spear phishing	Interprete di comandi e scripting	Creazione o modifica di un processo di sistema: servizio di Windows	Account di dominio	Compromissione delle difese: disabilitazione o modifica degli strumenti	Rilevamento della configurazione di rete del sistema	Trasferimento laterale dello strumento	Trasferimento programmato	Dati criptati
Exploit dell'applicazione rivolta al pubblico	API nativa		Sfruttamento per aumentare i privilegi	Deoffuscamento/ decodifica di file o informazioni	Rilevamento dei sistemi in remoto			Inibizione del ripristino di sistema
	Esecuzione utente			Modifica registro	Rilevamento di file e directory			
					Ricerca nel registro			
					Rilevamento dei software di sicurezza			

AvosLocker

Il ransomware AvosLocker è un gruppo RaaS apparso a luglio del 2021. In modo analogo a Hive e BlackByte, l'infezione iniziale inizia con l'exploit delle vulnerabilità ProxyShell CVE-2021-34473, CVE-2021-34523 e CVE-2021-31207 presenti nel server di Microsoft Exchange.

Catena di infezione

L'aggressore crea un'e-mail in bozza all'interno di una casella di posta elettronica. Questa e-mail contiene un allegato co la web shell codificata. L'aggressore esporta quindi l'intera casella di posta (inclusa l'e-mail in bozza dannosa) in formato PST con un'estensione ASPX. Ciò consente agli aggressori di spostare le web shell sui server vulnerabili.

In seguito, vengono utilizzate delle web shell per il rilascio di Cobalt Strike sul server di Exchange infetto. Cobalt Strike e Rclone vengono utilizzati per rubare le credenziali ed esfiltrare i dati su server in remoto.

L'aggressore installa AnyDesk RDP per accedere a più sistemi, spostandosi lateralmente. Rilascia inoltre diversi script batch per modificare ed eliminare le chiavi di registro dei software di sicurezza. Inoltre, disabilita Windows Update e Windows Defender.

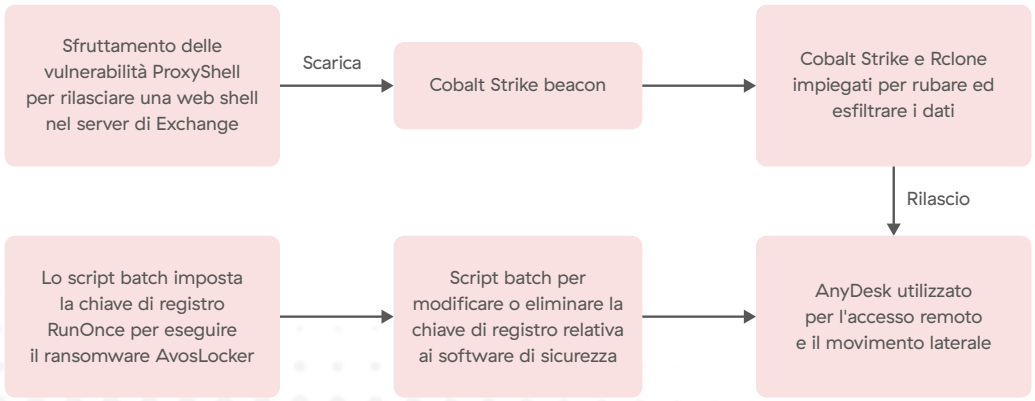


Figura 34: anatomia di un attacco del ransomware AvosLocker

Dopodiché, AvosLocker riavvia il sistema nella modalità provvisoria di Windows e inizia a criptare i file. Avviando il sistema in modalità provvisoria, AvosLocker è in grado di massimizzare il numero di file criptati, perché con tutta probabilità le applicazioni aziendali, come i database, non vengono eseguite. Queste applicazioni non avranno quindi handle di file aperti che potrebbero impedire la crittografia. Inoltre, molte applicazioni di sicurezza (come i programmi antivirus) non vengono caricate automaticamente quando il sistema è in modalità provvisoria. Quella di criptare i file nella modalità provvisoria di Windows è una caratteristica osservata anche in altre famiglie di ransomware, tra cui Conti, REvil e BlackMatter.

AvosLocker utilizza una combinazione di algoritmi RSA e AES per criptare i file, e ha creato una versione Linux del ransomware che colpisce VMware ESXi.

Dopo l'attacco, l'aggressore minaccia di pubblicare i dati rubati su un sito di divulgazione e, in alcuni casi, durante la negoziazione, minaccia di eseguire e lancia un attacco DDoS sulla rete della vittima. La figura 35 mostra una schermata del sito di divulgazione dei dati rubati di AvosLocker.

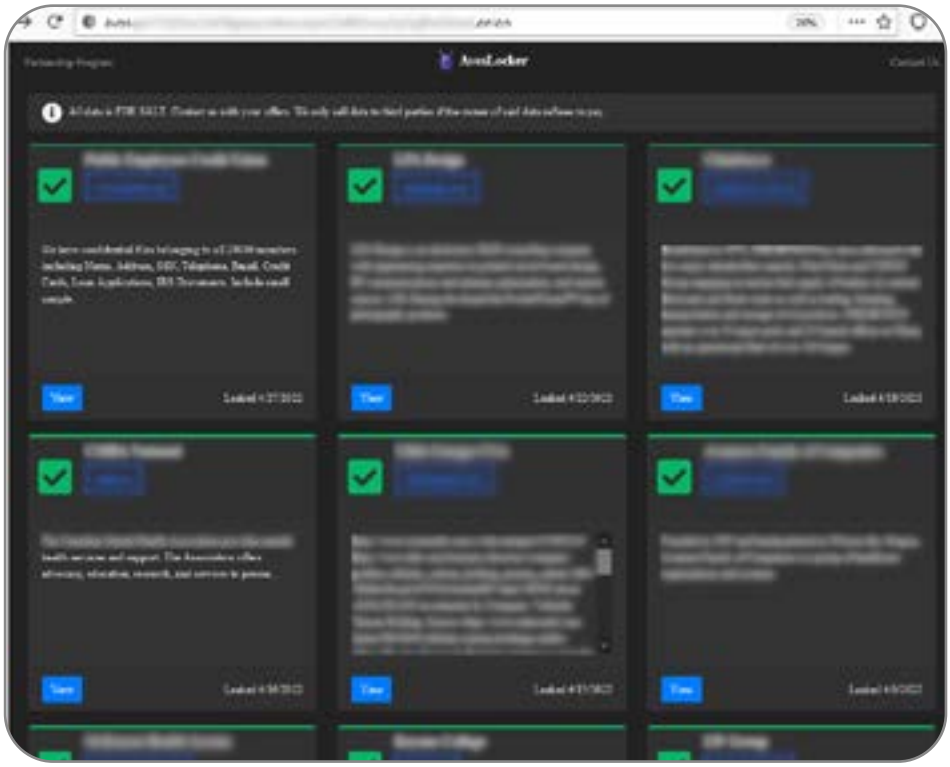


Figura 35: sito di divulgazione dei dati rubati di AvosLocker

La figura 21 mostra i settori presi di mira dagli attacchi a doppia estorsione che utilizzano AvosLocker.

Infezioni di AvosLocker per settore

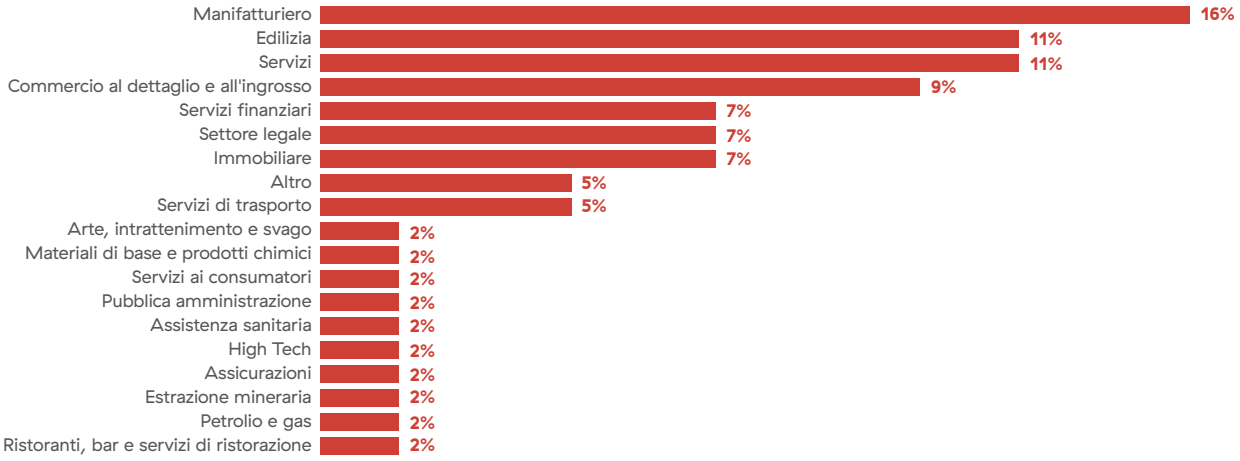


Figura 36: infezioni di AvosLocker per settore

AvosLocker: tattiche e tecniche MITRE ATT&CK

Accesso iniziale	Esecuzione	Persistenza	Escalation dei privilegi	Evasione della difesa	reciproca	Movimento laterale	Esfiltrazione	Impatto
Allegato di spear phishing	Interfaccia della riga di comando	Esecuzione automatica all'avvio o all'accesso: chiavi di esecuzione del registro/ cartella di avvio	Account di dominio	Compromissione delle difese: disabilitazione o modifica degli strumenti	Rilevamento della configurazione di rete del sistema	Trasferimento laterale dello strumento	Trasferimento programmato	Dati criptati
Exploit dell'applicazione rivolta al pubblico	Esecuzione utente	Attività/processo pianificati	Sfruttamento per aumentare i privilegi	Deoffuscamento/ decodifica di file o informazioni	Rilevamento dei sistemi in remoto			Inibizione del ripristino di sistema
					Rilevamento di file e directory			Arresto/riavvio del sistema
					Rilevamento dei software di sicurezza			

BlackCat/ALPHV

BlackCat, anche conosciuta come ALPHV, è un'operazione RaaS individuata per la prima volta a novembre del 2021. BlackCat utilizzava il linguaggio di programmazione RUST, che aiuta a migliorare le prestazioni e l'affidabilità dell'elaborazione simultanea.

Catena di infezione

L'infezione inizia con l'uso di credenziali compromesse per ottenere l'accesso ai sistemi di rete delle vittime. Inizialmente, per farsi strada nella rete della vittima vengono utilizzati Cobalt Strike, script PowerShell e script batch. Una volta ottenuto l'accesso, gli account di amministrazione in Active Directory vengono compromessi. Sono inoltre utilizzati GPO (Group Policy Object) dannosi per distribuire ed eseguire il ransomware. Durante l'attacco, vengono utilizzati anche Microsoft Sysinternals e altri strumenti amministrativi.

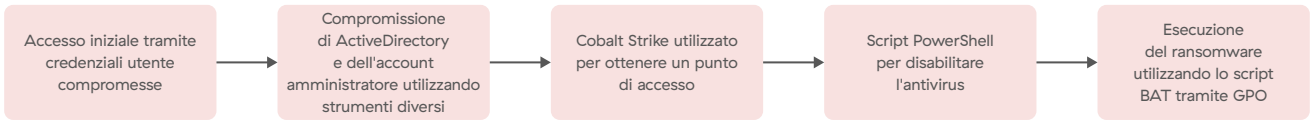


Figura 37: anatomia di un attacco del ransomware BlackCat/ALPHV

BlackCat fa anche uso di tattiche DDoS: sul sito web o sulla rete delle vittime vengono lanciati attacchi di questo tipo per fare in modo che negozino con gli operatori e per costringerle a pagare riscatti più elevati. La figura 38 mostra una schermata del sito di divulgazione dei dati rubati di BlackCat.

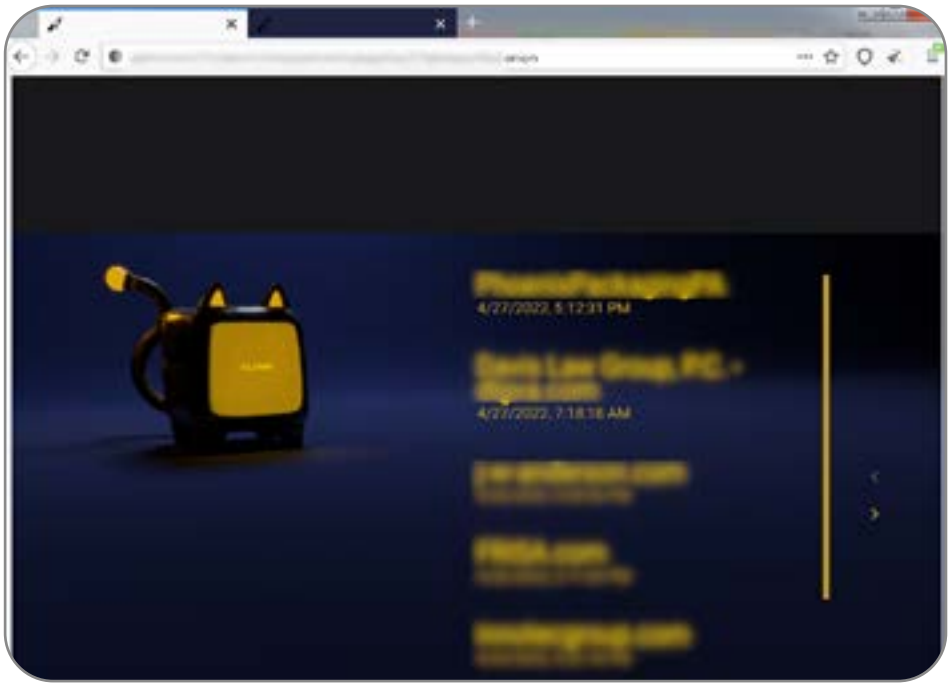


Figura 38: sito di divulgazione dei dati rubati di BlackCat/ALPHV

La figura 39 mostra i settori presi di mira dagli attacchi a doppia estorsione che utilizzano BlackCat/ALPHV.

Infezioni di BlackCat/ALPHV per settore

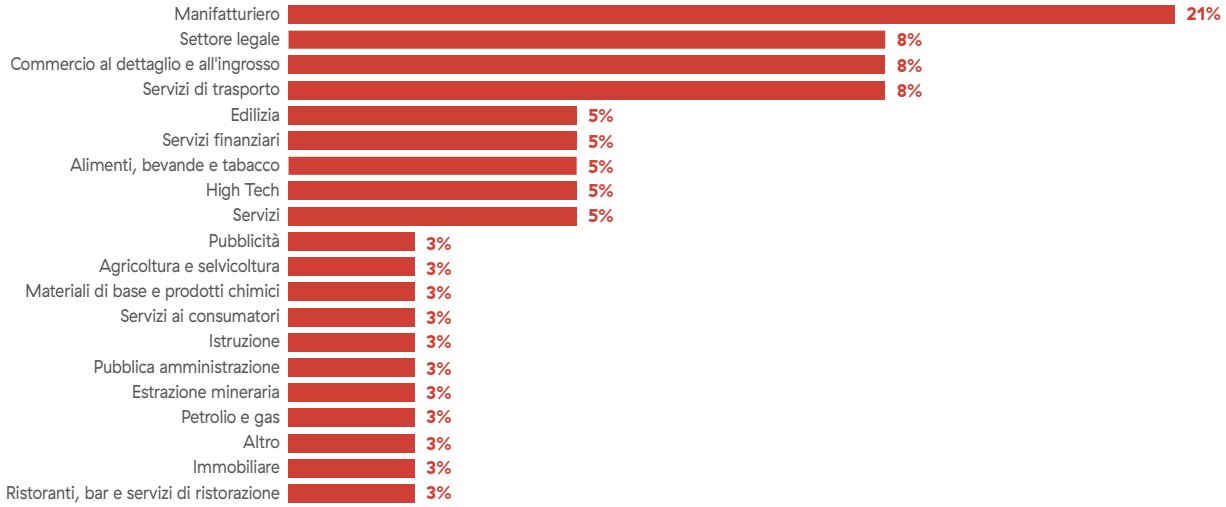


Figura 39: infezioni di BlackCat/ALPHV per settore

BlackCat: tattiche e tecniche MITRE ATT&CK

Accesso iniziale	Esecuzione	Persistenza	Escalation dei privilegi	Evasione della difesa	reciproca	Movimento laterale	Esfiltrazione	Impatto
Account validi	Interprete di comandi e scripting	Esecuzione automatica all'avvio o all'accesso: chiavi di esecuzione del registro/ cartella di avvio	Account di dominio	Compromissione delle difese: disabilitazione o modifica degli strumenti	Rilevamento della configurazione di rete del sistema	Trasferimento laterale dello strumento	Trasferimento programmato	Dati criptati
	Esecuzione utente	Attività/processo pianificati	Sfruttamento per aumentare i privilegi	Deoffuscamento/ decodifica di file o informazioni	Rilevamento dei sistemi in remoto			Inibizione del ripristino di sistema
				Modifica delle policy del dominio: modifica delle policy di gruppo	Rilevamento di file e directory			
					Rilevamento dei software di sicurezza			

Informazioni su ThreatLabz

ThreatLabz è il team di ricerca sulla sicurezza di Zscaler. Questo team di esperti di alto livello è responsabile della ricerca di nuove minacce e della protezione costante delle migliaia di aziende che utilizzano la piattaforma globale di Zscaler. Oltre alla ricerca di malware e all'analisi del comportamento, i membri del team si occupano della ricerca e dello sviluppo di nuovi prototipi per la protezione contro le minacce avanzate sulla piattaforma Zscaler, e conducono regolarmente controlli di sicurezza interni per garantire che i prodotti e l'infrastruttura di Zscaler siano in linea con gli standard di conformità. Sul suo portale, ThreatLabz pubblica regolarmente analisi approfondite sulle minacce nuove ed emergenti: research.zscaler.it

Non perderti le ultime novità sulle ricerche di ThreatLabz. Iscriviti alla nostra newsletter Trust Issues oggi stesso.

Zero Trust Exchange di Zscaler è stato nominato da Gartner tra le piattaforme SSE (Security Service Edge) principali del settore, grazie alla protezione dai ransomware in ogni fase della catena di attacco e alla capacità di ridurre drasticamente la possibilità di essere attaccati e mitigare i potenziali danni.

Zscaler integra in modo nativo funzionalità all'avanguardia per:

Per ulteriori informazioni, visita la nostra pagina sulla protezione contro i ransomware di Zscaler.

zscaler™ | Experience your world, secured.™

Informazioni su Zscaler

Zscaler (NASDAQ: ZS) accelera la trasformazione digitale in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zero Trust Exchange di Zscaler protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati connettendo in modo sicuro utenti, dispositivi e applicazioni, in qualsiasi luogo. Distribuita in più di 150 data center a livello globale, Zero Trust Exchange, basata su SASE, è la più grande piattaforma di cloud security inline del mondo. Scopri di più su **zscaler.it** o seguici su Twitter su **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.it