Report del 2024 di ThreatLabz sui ransomware

Indice

Riepilogo

Gli attacchi ransomware hanno raggiunto livelli di ambizione e audacia senza precedenti nel corso dell'ultimo anno, contrassegnati da un notevole aumento degli attacchi di estorsione. In aggiunta all'incremento degli attacchi ransomware, la ricerca condotta da ThreatLabz ha svelato un **riscatto senza precedenti dell'ammontare di 75 milioni di dollari**: la somma più elevata mai pagata da un'azienda. Questo importo è quasi il doppio rispetto al riscatto più alto pubblicamente noto.[1] Solo nel 2023, i pagamenti correlati ai ransomware hanno superato 1 miliardo di dollari, evidenziando il crescente impatto finanziario di questi crimini informatici.

Le tattiche degli autori delle minacce ransomware sono diventate sempre più sofisticate e subdole. In particolare, hanno superato i confini tradizionali delle aziende che attaccano, arrivando addirittura a prendere di mira i bambini dei dirigenti per indurre a pagamenti dei riscatti più rapidi e più ingenti.[2] Dalle infrastrutture critiche[3] alle grandi aziende[4] alle piccole e medie imprese, nessuna organizzazione è immune dal trovarsi nel mirino della prossima campagna o dall'evoluzione di questi attacchi.

Nonostante la neutralizzazione da parte delle forze dell'ordine di numerosi broker di accesso iniziale, nell'ambito delle operazioni speciali "Operation Endgame" e "Operation Duck Hunt", molte delle più grandi famiglie di ransomware attive continuano a riorganizzarsi rapidamente e a lanciare nuovi attacchi senza fare una piega. Sfortunatamente, molti autori dei ransomware non sono raggiungibili dalle forze dell'ordine, il che li rende praticamente immuni ai procedimenti penali. Come dettagliato in questo report, le forze dell'ordine hanno potenziato le loro tattiche, facendo pressione attraverso ricompense in denaro, sanzioni, trolling e denunciando gli individui dietro ai ransomware, utilizzando varie tipologie di tecniche psicologiche.

Dato che gli autori dei ransomware evolvono continuamente le loro strategie, è fondamentale rimanere sempre aggiornati su come sta cambiando il panorama delle minacce.

Il Report del 2024 di Zscaler ThreatLabz sui ransomware offre una panoramica sulle minacce ransomware, a partire da aprile 2023 fino ad aprile 2024, descrivendo in dettaglio le ultime tendenze, gli obiettivi, le famiglie di ransomware e le strategie di difesa efficaci.

Analizzando i tentativi bloccati sul cloud Zscaler, ThreatLabz ha rilevato che gli attacchi ransomware sono aumentati del 17,8% su base annua, mentre quelli identificati attraverso l'analisi dei siti di data leak sono cresciuti del 57,8%. Gli obiettivi più comuni sono state le aziende operanti nei settori manifatturiero, sanitario e tecnologico, il che significa che nel mirino si trovano le operazioni e le infrastrutture critiche.

I risultati presentati in questo report sottolineano la necessità per le organizzazioni di dare priorità alle misure di protezione contro questa incessante ondata di ransomware. Gli approfondimenti e le strategie presenti nel report costituiscono una guida molto importante per migliorare le difese contro i ransomware. Imparando a conosce le ultime tendenze e le vulnerabilità e implementando le best practice consigliate, è possibile ridurre significativamente il rischio di cadere vittima dei ransomware e riuscire a proteggere al meglio le risorse e i dati critici dell'organizzazione.

[1] Bloomberg, **CNA Financial Paid $40 Million in Ransom After March Cyberattack**, 20 maggio 2021.
[2] Business Insider, **Hackers are now targeting the children of corporate executives in ransomware attacks**, 12 maggio 2024.
[3] Dark Reading, **Ascension Healthcare Suffers Major Cyberattack**, 10 maggio 2024.
[4] CyberScoop, **Boeing confirms attempted $200 million ransomware extortion attempt**, 8 maggio 2024.

I risultati chiave

La ricerca condotta da Zscaler ThreatLabz ha scoperto un riscatto da record pari a 75 milioni di dollari Si tratta del riscatto più elevato mai pagato da un'azienda nella storia dei ransomware, pari a quasi il doppio della somma più alta nota al pubblico.

Gli attacchi ransomware bloccati dal cloud Zscaler sono aumentati del 17,8%, e il numero di aziende vittime di estorsioni su siti di data leak è cresciuto del 57,8% nello stesso periodo, anno dopo anno, nonostante le numerose operazioni delle forze dell'ordine che hanno incluso il sequestro delle infrastrutture insieme ad arresti, rinvii a giudizio e sanzioni.

I settori manifatturiero, sanitario e tecnologico sono stati i principali obiettivi degli attacchi ransomware, mentre il settore dell'energia ha registrato un picco del 500% su base annua, poiché le infrastrutture critiche e la suscettibilità alle interruzioni operative lo rendono particolarmente interessante per i criminali informatici.

Gli Stati Uniti rimangono il principale obiettivo dei ransomware, registrando il 49,95% degli attacchi complessivi. Seguono Regno Unito, Germania, Canada e Francia.

ThreatLabz ha identificato 19 nuove famiglie di ransomware durante il periodo in analisi, portando il numero totale a 391 dall'inizio del nostro monitoraggio.

Le famiglie di ransomware più attive sono state **LockBit (22,1%)**, **BlackCat (alias ALPHV) (9,2%)** ed **8Base (7,9%)**.

Le vulnerabilità rimangono il vettore di attacco ransomware più comune, sottolineando l'importanza dell'applicazione tempestiva delle patch e della gestione unificata delle vulnerabilità, il tutto rafforzato da un'architettura zero trust, per fornire la massima protezione anche quando le patch non sono disponibili.

Gli attacchi di ingegneria sociale basati sulla voce sono sempre più utilizzati per ottenere l'accesso alle reti aziendali, una tecnica impiegata da Scattered Spider e dal gruppo di minacce Qakbot.

Il panorama dei ransomware: le principali tendenze e gli obiettivi presi di mira

La natura dinamica dei ransomware li ha portati in cima alla lista delle preoccupazioni correlate alla sicurezza nel corso degli ultimi anni. Gli autori delle minacce evolvono costantemente i loro metodi di attacco ed estorsione, sfruttando i progressi nella tecnologia dell'intelligenza artificiale (IA), la fuga di codice sorgente e la crittografia avanzata per massimizzare il loro impatto e i profitti.

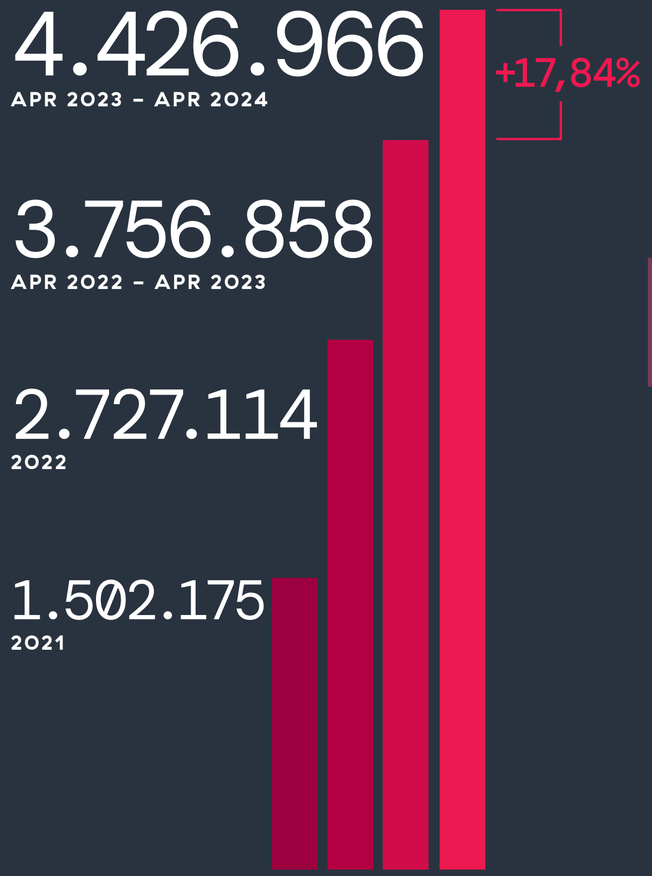
Questo report esamina le seguenti tendenze degli attacchi ransomware da aprile 2023 ad aprile 2024:

- L'aumento complessivo degli attacchi ransomware
- I settori più colpiti dai ransomware
- Distribuzione geografica delle organizzazioni colpite
- Il rafforzamento delle operazioni delle forze dell'ordine contro i gruppi ransomware e i broker di accesso iniziale
- Principali minacce ransomware e riscatti da record

L'aumento complessivo degli attacchi ransomware

L'ultima analisi condotta da ThreatLabz sui tentativi bloccati osservati nel cloud Zscaler rivela una tendenza preoccupante, con un aumento del 17,84% su base annua degli attacchi ransomware. L'incremento dell'attività dei ransomware si traduce in interruzioni dirompenti e ripercussioni finanziarie per le organizzazioni colpite, indipendentemente dalle dimensioni. Questi attacchi spesso interrompono le operazioni aziendali, causando periodi di inattività prolungati, perdita sostanziale di dati e ingenti costi di ripristino. L'onere finanziario è considerevole: non solo è in gioco una richiesta di riscatto, ma il ripristino del sistema e le operazioni per limitare i danni possono avere un costo estremamente elevato. Alla luce di queste crescenti minacce, la presenza di **solide misure di difesa contro i ransomware** non è mai stata così determinante.

NUMERO DI TENTATIVI BLOCCATI NEL CLOUD ZSCALER



I settori più colpiti dai ransomware

Gli attacchi ransomware comportano rischi significativi per le aziende di ogni dimensione e settore. Questi attacchi possono compromettere i dati sensibili, portare a pesanti perdite finanziarie, interrompere la continuità delle operazioni aziendali e danneggiare la reputazione. I vari settori si trovano poi ad affrontare sfide specifiche in relazione ai ransomware, sulla base del modo in cui operano, dei dati che gestiscono e della loro infrastruttura tecnologica.

Nonostante le variabili interessate, gli attacchi di estorsione ransomware sono aumentati costantemente, con il numero di aziende colpite riportate nei siti di data leak che è aumentato del 57,81%, rispetto al report di ThreatLabz sulle tendenze del ransomware dello scorso anno. Il settore manifatturiero è stato di gran lunga il settore più preso di mira, con 653 attacchi, più del doppio rispetto agli altri settori.

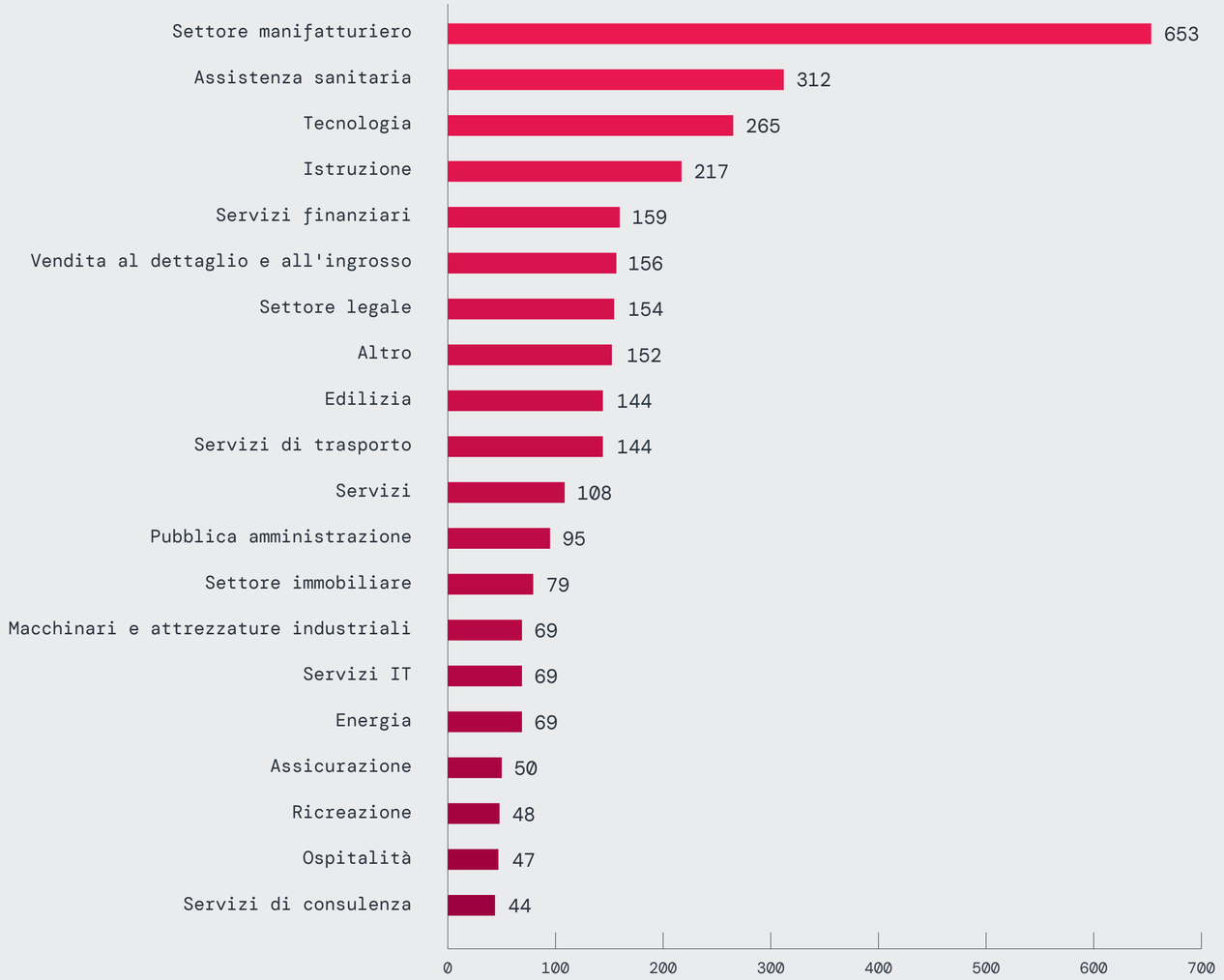


Figura1: attacchi ransomware per settore sulla base dei siti di data leak (solo i primi 20 settori).

Tendenze su base annua

Il settore dell'energia ha registrato un aumento degli attacchi ransomware del 527,27% su base annua, probabilmente a causa della sua natura critica e dell'elevato potenziale di riscatto che offre agli aggressori.

Allo stesso modo, la ristorazione, i bar e i servizi alimentari nel loro complesso hanno registrato un aumento degli attacchi del 333,33%. Ciò può essere attribuito alla rapida digitalizzazione del settore, guidata dall'adozione di sistemi avanzati PoS e piattaforme per l'ordinazione online. Sebbene queste tecnologie possano semplificare le operazioni e migliorare l'esperienza dei clienti, possono al contempo introdurre potenziali vulnerabilità.

Se da un lato questo aumento evidenzia la prevalenza degli attacchi ransomware, dall'altro potrebbe però non cogliere l'intera portata degli incidenti ransomware. Molti attacchi infatti, o non vengono denunciati, o vengono risolti privatamente, tramite il pagamento di un riscatto, senza essere resi pubblici. Pertanto, queste cifre dovrebbero essere considerate indicative di tendenze più estese dei ransomware e non come una rappresentazione esaustiva dell'intero panorama delle minacce.

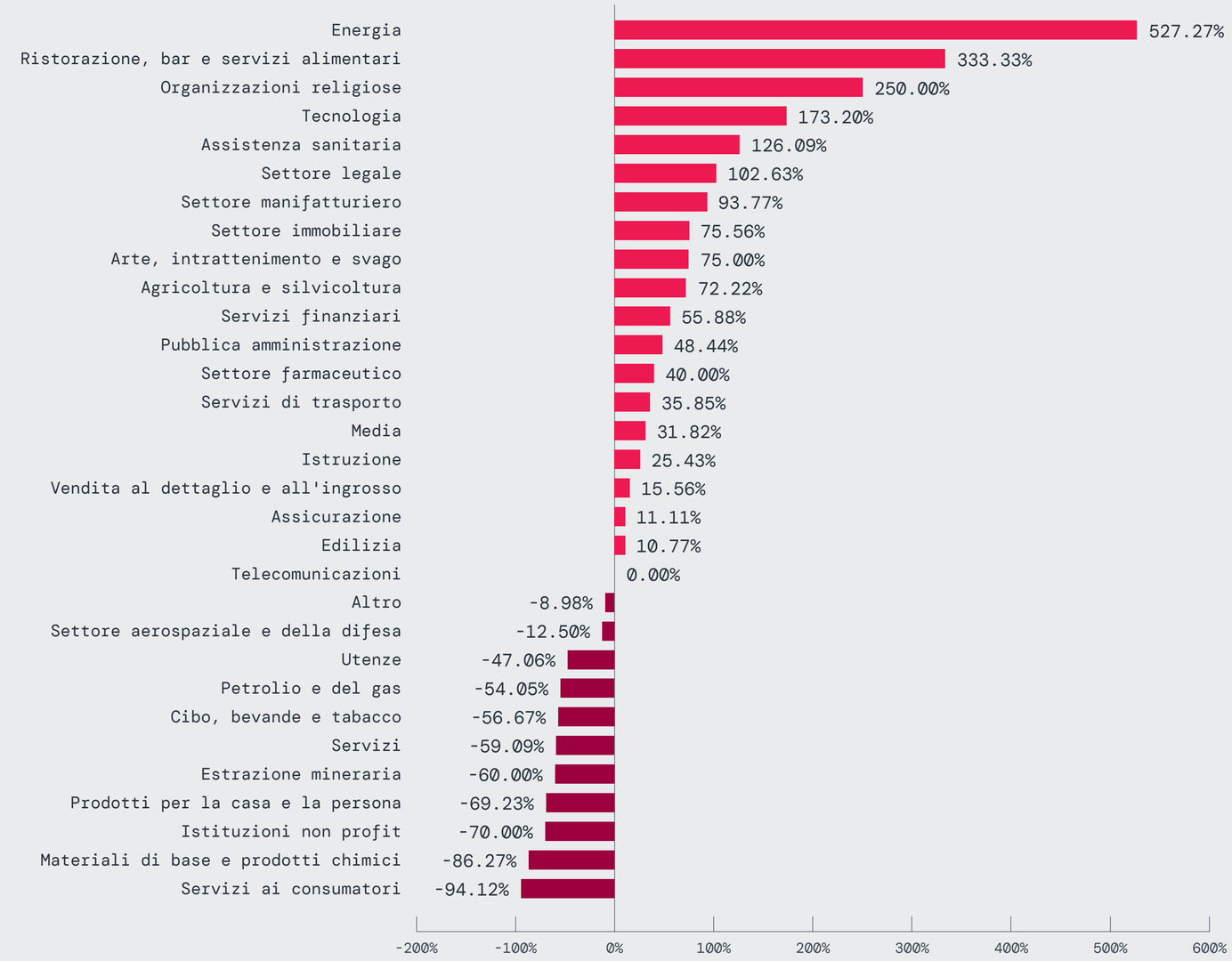


Figura 2: variazione percentuale su base annua degli attacchi di estorsione ransomware per settore. Si noti che alcuni settori presentavano una base di attacchi relativamente bassa nel report dello scorso anno, il che fa apparire la loro crescita più significativa.

Distribuzione geografica delle organizzazioni colpite

Gli Stati Uniti hanno dovuto affrontare un volume di attacchi ransomware decisamente più elevato rispetto a qualsiasi altro Paese, registrando circa il 50% di tutti gli incidenti a livello globale. A confronto, il Regno Unito è stata la seconda nazione più colpita, sfiorando il 6% di attacchi ransomware, seguita dalla Germania (4,09%), dal Canada (3,51%) e dalla Francia (3,26%). La Figura 3 mostra una mappa di calore che illustra i Paesi colpiti dalle estorsioni tra aprile 2023 e aprile 2024.

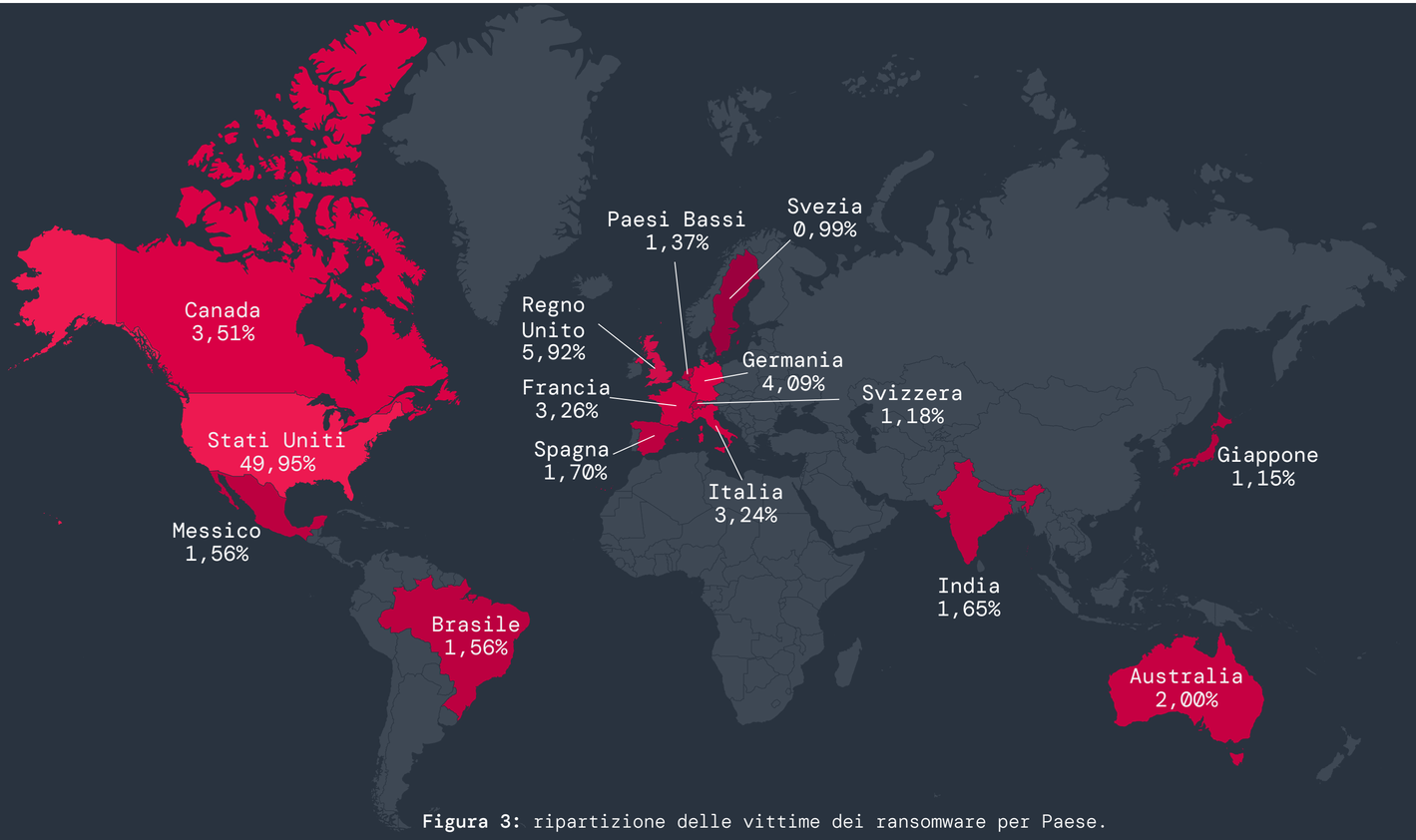


Figura 3: ripartizione delle vittime dei ransomware per Paese.

Comprendere la distribuzione degli attacchi ransomware è essenziale per valutare il rischio, allocare le risorse, sviluppare le politiche, cooperare a livello internazionale e accrescere gli sforzi di sensibilizzazione del pubblico nella lotta alle minacce ransomware.

Valutazione del rischio

L'analisi delle regioni fortemente colpite aiuta le organizzazioni presenti in quelle aree a valutare i propri livelli di rischio e a implementare una sicurezza informatica più efficiente. Nella ricerca condotta da ThreatLabz, gli Stati Uniti registrano il 50% degli attacchi ransomware globali, un dato che serve da monito alle organizzazioni all'interno del Paese per dare priorità all'adozione di rigorosi protocolli di sicurezza.

Sviluppo delle politiche

I governi possono utilizzare le informazioni derivanti dagli attacchi ransomware a livello regionale per prendere decisioni informate in ambito legislativo, migliorare gli standard di sicurezza, promuovere la cooperazione internazionale e facilitare la condivisione delle informazioni tra settore pubblico e privato. Un esempio recente e degno di nota sono le nuove regole di sicurezza informatica della SEC, che segnano un passo importante nel miglioramento della trasparenza e della responsabilità sullo sfondo delle crescenti minacce.

Sensibilizzazione del pubblico

Evidenziare i Paesi presi più frequentemente di mira può spingere individui, organizzazioni e governi ad adottare misure più proattive negli ambiti della formazione sulla sicurezza informatica, della pianificazione della risposta agli incidenti e degli investimenti nelle tecnologie di difesa.

Allocazione delle risorse

I dati presi di mira consentono ai governi e alle organizzazioni di allocare strategicamente le risorse, migliorando il loro profilo di sicurezza dando priorità al supporto, ai finanziamenti e alle competenze nelle aree più colpite dalle minacce.

Cooperazione internazionale

L'identificazione dei Paesi più colpiti consente di coordinare gli sforzi tra le forze dell'ordine, le organizzazioni e i governi, per combattere i ransomware a livello nazionale e internazionale. Le operazioni Duck Hunt ed Endgame esemplificano come la cooperazione internazionale sia davvero in grado di fermare le attività dei criminali informatici.

Tendenze su base annua

ThreatLabz ha confrontato gli attacchi ransomware del report di quest'anno con il Report del 2023 di ThreatLabz sui ransomware per valutare le variazioni. Tra i primi 15 Paesi più colpiti, gli Stati Uniti hanno registrato un notevole aumento, pari al 101,88% su base annua, mentre la Svezia ha registrato un incremento sbalorditivo, pari al 350%, sebbene abbia registrato una quota significativamente inferiore degli attacchi totali.

Sebbene l'analisi delle tendenze dei ransomware a livello globale sia di estremo valore, è anche importante esaminare gli sviluppi specifici nelle diverse regioni del mondo. Lo studio degli spaccati regionali aiuta le organizzazioni a creare piani di sicurezza su misura e i governi a sviluppare delle politiche di sicurezza informatica più efficaci.

CAMBIAMENTI NEGLI ATTACCHI RANSOMWARE NEI 15 PRINCIPALI PAESI PRESI DI MIRA

Paese	Attacchi ransomware per Paese (2023)	Attacchi ransomware per Paese (2024)	Variazione percentuale
Stati Uniti d'America	902	1.821	101,88%
Regno Unito	144	216	50%
Germania	110	149	35,45%
Canada	151	128	-15,23%
Francia	87	119	36,78%
Italia	63	118	87,30%
Australia	69	73	5,80%
Brasile	38	57	50%
Spagna	36	62	72,22%
Messico	31	57	83,87%
Paesi Bassi	17	50	194,12%
India	62	60	-3,23%
Svizzera	32	43	34,38%
Giappone	44	42	-4,55%
Svezia	8	36	350%

Figura 5: confronto su base annua degli attacchi ransomware per Paese.

VARIAZIONI NELLE PERCENTUALI DEGLI ATTACCHI RANSOMWARE NELL'AREA EMEA

Paese	Aziende colpite dagli attacchi ransomware (2023)	Aziende colpite dagli attacchi ransomware (2024)	Variazione percentuale
Regno Unito	144	216	50%
Germania	110	149	35,45%
Francia	87	119	36,78%
Italia	63	118	87,30%
Spagna	36	62	72,22%
Paesi Bassi	17	50	194,12%
Svizzera	32	43	34,38%
Svezia	8	36	350%
Belgio	16	34	112,50%
Sudafrica	13	24	84,62%
Austria	15	24	60%
Emirati Arabi Uniti	12	21	75%

Figura 6: confronto su base annua degli attacchi ransomware per Paese nella regione EMEA.

VARIAZIONI NELLE PERCENTUALI DEGLI ATTACCHI RANSOMWARE NELL'AREA APAC

Paese	Aziende colpite dagli attacchi ransomware (2023)	Aziende colpite dagli attacchi ransomware (2024)	Variazione percentuale
Australia	69	73	5,80%
India	62	60	-3,23%
Giappone	44	42	-4,55%
Thailandia	13	25	92,31%
Indonesia	15	23	53,33%
Malesia	14	20	42,86%
Taiwan	23	17	-26,09%
Filippine	7	16	128,57%
Singapore	8	16	100%
Cina	21	15	-28,57%
Corea del Sud	12	10	-16,67%
Vietnam	10	10	0%

Figura 7: confronto su base annua degli attacchi ransomware per Paese nella regione APAC.

I gruppi ransomware più attivi nel 2023-2024

LockBit (22,1%), BlackCat (9,2%) ed 8Base (7,9%) sono stati i gruppi di estorsione ransomware più attivi nell'ultimo anno, ciascuno responsabile di un numero significativo di attacchi. La Figura 8 mostra il numero di vittime di data leak per famiglia di ransomware durante questo periodo.

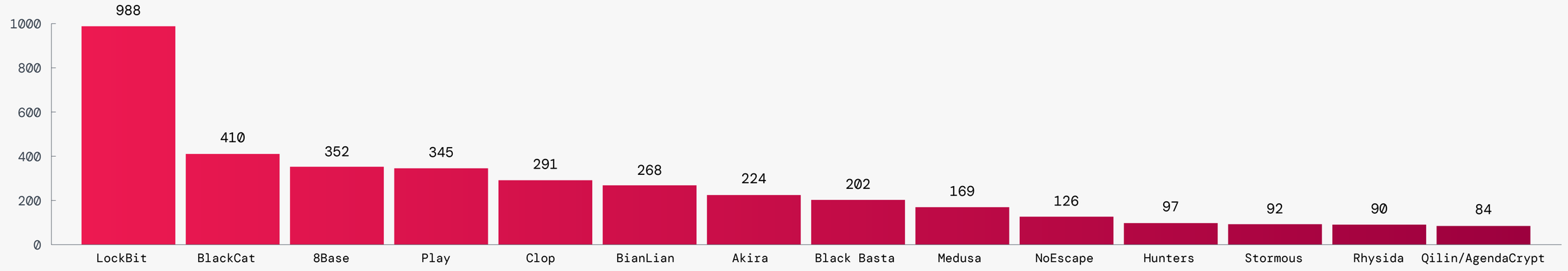


Figura 8: attacchi ransomware rilevati su siti dolosi di data leak.

Gli ultimi gruppi ransomware apparsi sulle scene

La Figura 9 mostra su una linea temporale i nuovi gruppi ransomware che hanno iniziato a pubblicare dati sui siti di data leak come parte della loro strategia di estorsione.

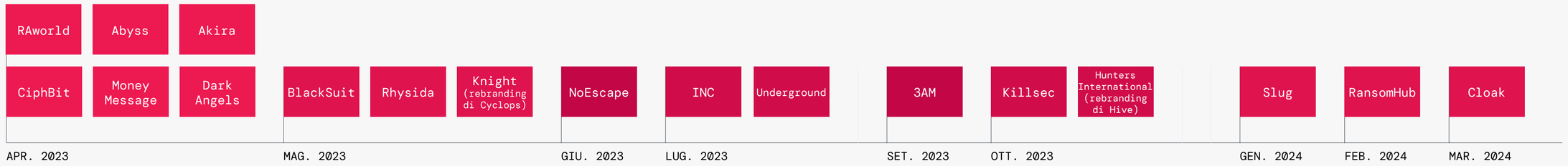


Figura 9: nuovi gruppi ransomware con siti di data leak.

Le principali vulnerabilità sfruttate negli attacchi ransomware

Le vulnerabilità nei software, nei sistemi e nell'infrastruttura digitale generale possono fungere da punti di ingresso critici per gli attacchi ransomware. Le organizzazioni devono essere consapevoli di queste vulnerabilità e adottare misure proattive per risolverle.

La Cybersecurity & Infrastructure Security Agency (CISA) ha stilato un elenco completo e sempre aggiornato delle vulnerabilità,[5] comprese quelle sfruttate attivamente dai gruppi ransomware. Le organizzazioni sono caldamente invitate a monitorare attentamente questo elenco e a dare la priorità alla mitigazione delle vulnerabilità che riporta. La gestione proattiva delle vulnerabilità è essenziale per rafforzare la strategia di sicurezza informatica complessiva di un'organizzazione.

In molti casi, le vulnerabilità sfruttate dai gruppi ransomware incidono sulle risorse connesse a Internet nella superficie di attacco esterna delle organizzazioni, come gateway, VPN e altre tecnologie per la connettività da remoto. Dato che si interfacciano con Internet, queste vulnerabilità sono molto più facili da scansionare e sfruttare per gli autori delle minacce. Le ultime linee guida della CISA[6] evidenziano ancora una volta le vulnerabilità presenti nelle VPN e nelle soluzioni per la connettività da remoto, indicandole come punti critici da risolvere e consigliando l'adozione di approcci più attuali, come l'architettura zero trust, l'SSE e il SASE, che si basano sulle policy per il controllo granulare dell'accesso.

Nell'ultimo anno, importanti famiglie di ransomware hanno preso di mira e sfruttato le vulnerabilità mostrate nella Figura 10, colpendo in modo significativo un'ampia varietà di sistemi.

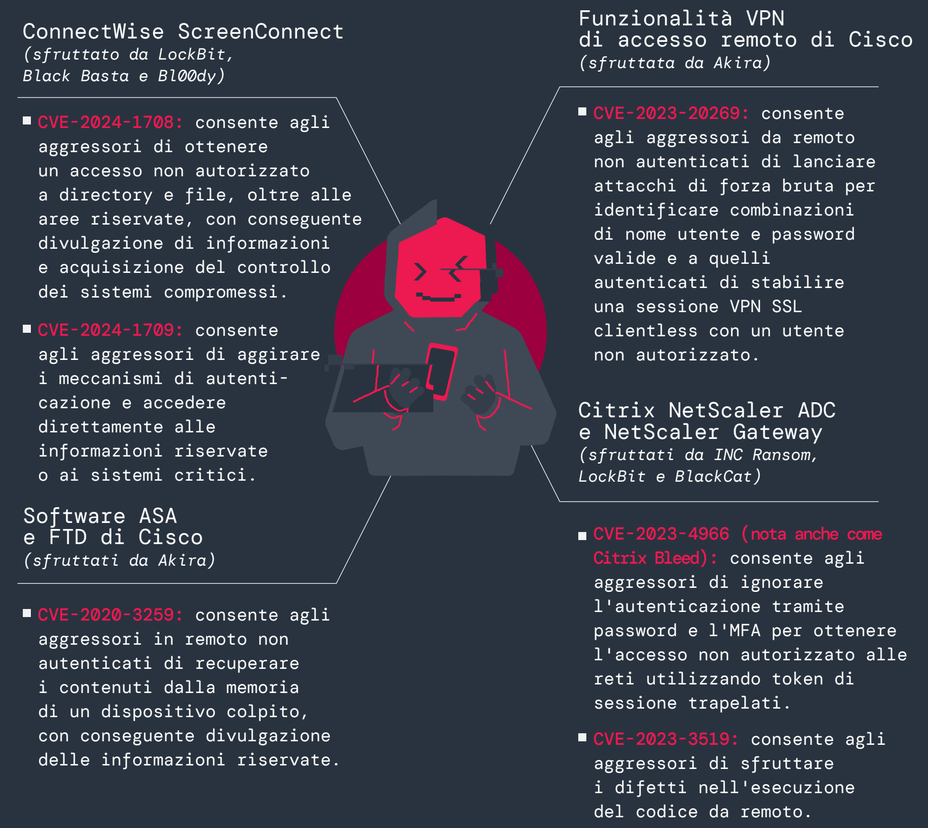


Figura 10: vulnerabilità prevalenti da aprile 2023 ad aprile 2024.

Le patch disponibili per queste vulnerabilità dovrebbero essere applicate il prima possibile, insieme alle seguenti misure di mitigazione:

- Disabilitare l'accesso remoto ai server
- Utilizzare password complesse e l'autenticazione a più fattori
- Monitorare i server per individuare le attività sospette

[5] Cybersecurity & Infrastructure Security Agency, **Known Exploited Vulnerabilities Catalog**, accesso effettuato il 25 giugno 2024.
[6] Cybersecurity & Infrastructure Security Agency, **Modern Approaches to Network Access Security**, 18 giugno 2024.

Riepilogo sui ransomware: cosa sta facendo notizia

Il ransomware è pervasivo e trascende i settori e quando un gruppo viene neutralizzato, un altro rinasce o emerge di nuovo. Ecco alcune storie recenti che evidenziano il panorama in continua evoluzione dei ransomware.

La piaga dei ransomware nel settore sanitario

Il settore sanitario ha dovuto affrontare sfide molto significative nel corso del 2023 e del 2024, in quanto è stato preso pesantemente di mira dai gruppi ransomware. Le ripercussioni dell'interruzione delle operazioni sanitarie sono gravi: le ambulanze vengono deviate, le prescrizioni vengono ritardate e le procedure mediche essenziali devono essere rinviate. Inoltre, il furto dei dati sanitari sensibili può avere conseguenze di vasta portata, tra cui il furto di identità e le frodi sanitarie, esacerbando ulteriormente le vulnerabilità dell'ecosistema sanitario.

CONSEGUENZE IMPREVISTE LEGATE AL PAGAMENTO DI UN RISCATTO

Un fornitore di tecnologia per il settore sanitario, che fornisce soluzioni di pagamento, è stato vittima di un attacco ransomware orchestrato dal gruppo BlackCat. Nonostante abbia accolto le richieste degli aggressori e pagato un riscatto da capogiro, pari a 22 milioni di dollari, la vicenda ha preso una piega inaspettata. BlackCat non ha rispettato la promessa di condividere una parte del riscatto con l'autore affiliato dell'attacco (la cosiddetta "exit scam"), spingendo quest'ultimo a minacciare l'operatore sanitario di rilasciare i dati sensibili.

Quanto accaduto ci ricorda chiaramente che il vecchio detto "tra ladri non c'è onore" è perfettamente riconducibile agli attacchi ransomware. Anche se vengono pagati i riscatti, non vi è alcuna garanzia che il gruppo hacker non pubblichi o elimini comunque i dati rubati. Inoltre, alcuni strumenti di decrittazione ransomware contengono bug che impediscono il corretto ripristino dei dati e potrebbero richiedere più tempo rispetto a un backup.

DOPPIA ESTORSIONE, DOPPIA VITTIMIZZAZIONE

A febbraio del 2023, un importante distributore farmaceutico statunitense ha confermato che i suoi sistemi IT erano stati compromessi. La violazione ha colpito una delle filiali del distributore e i file rubati sono poi stati divulgati dal gruppo ransomware Lorenz.[7] Dopodiché, a febbraio del 2024, lo stesso distributore ha dovuto affrontare un altro attacco ransomware.[8] Ciò sembra rientrare in una tendenza in crescita osservata da ThreatLabz, che vede le aziende cadere in numerosi incidenti ransomware nell'arco di un solo anno.

[7] BleepingComputer, **Drug distributor AmerisourceBergen confirms security breach**, 8 febbraio 2023.
[8] BleepingComputer, **Pharmaceutical giant Cencora says data was stolen in a cyberattack**, 27 febbraio 2024.

L'impatto della decisione della SEC in materia di sicurezza informatica

Nel 2023, la SEC ha introdotto nuove regole sulla divulgazione nell'ambito della sicurezza informatica, per accrescere la trasparenza e la responsabilità delle società quotate in borsa. A partire dal 15 dicembre 2023, queste regole impongono la segnalazione tempestiva degli incidenti materiali di sicurezza informatica e richiedono informazioni dettagliate sulla gestione, la strategia e la governance del rischio di sicurezza informatica dell'azienda. Gli elementi chiave delle decisioni della SEC includono l'aggiunta della voce 1.05 all'articolo 8-K, che richiede la segnalazione degli incidenti materiali di sicurezza informatica entro quattro giorni lavorativi dalla determinazione della materialità da parte della società. Inoltre, il Modulo 10-K ora richiede una rendicontazione annuale sulla gestione e sulla strategia del rischio di sicurezza informatica, a partire dagli anni fiscali che terminano dal 15 dicembre 2023 in avanti. Anche le società quotate private straniere devono rispettare specifici obblighi di divulgazione comparabili utilizzando il Modulo 6-K e il Modulo 20-K.

Queste decisioni rappresentano una nuova sfida per gli autori dei ransomware che offrono alle società quotate servizi confidenziali per la gestione dei pagamenti del riscatto, in quanto le stesso sono comunque tenute a divulgare integralmente l'attacco. L'aspetto positivo è che il nuovo obbligo indebolisce gli attacchi di estorsione senza crittografia, una tendenza emergente che vede gli autori dei ransomware fare affidamento esclusivamente sulla minaccia di divulgare i dati rubati per chiedere dei riscatti.

L'IMPATTO DELLE NUOVE REGOLE PER LE IMPRESE

Le decisioni della SEC in materia di sicurezza informatica possono rappresentare serie sfide per le imprese, in termini di conformità e gestione del rischio. Sebbene intese a migliorare la trasparenza e la protezione degli investitori, queste regole richiedono alle società di destreggiarsi tra complessi requisiti di rendicontazione e di fornire una divulgazione tempestiva degli incidenti materiali.

Uno dei principali effetti è la maggiore pressione esercitata sulle imprese, affinché quantifichino e valutino accuratamente gli incidenti informatici. Determinare la materialità e il potenziale impatto degli incidenti informatici richiede un'analisi attenta, che può essere costosa e potrebbe richiedere alle società (grandi e piccole) di riconsiderare i propri protocolli di risposta agli incidenti e aggiornare le proprie informative per soddisfare i requisiti della SEC.

Inoltre, le tempistiche per uniformarsi variano in base alle dimensioni e allo stato della rendicontazione delle imprese, aggiungendo un ulteriore livello di complessità. Le società più piccole soggette all'obbligo di rendicontazione, spesso, hanno scadenze di conformità diverse e, in genere, più lunghe, rispetto alle società più grandi. Inoltre, sebbene queste ultime debbano rispettare scadenze più ravvicinate, le loro dimensioni gli consentono però di disporre di più risorse per analizzare la materialità di un incidente di sicurezza informatica.

I nuovi requisiti di divulgazione eliminano inoltre la possibilità per le società quotate di pagare i riscatti in via confidenziale, senza incorrere ai danni alla reputazione e alla reazione negativa che seguirebbe dopo aver condiviso apertamente le informazioni su una violazione.

ALCUNE SOCIETÀ STANNO GIÀ VIOLANDO LE REGOLE DELLA SEC

Nonostante le chiare linee guida della SEC, alcune imprese già non risultano conformi alle nuove regole di sicurezza informatica. Recenti divulgazioni da parte di note imprese hanno sollevato preoccupazioni circa la non conformità e l'inadeguatezza della loro segnalazione degli incidenti.[9] Molte di queste divulgazioni mancano di dati quantitativi e valutazioni dettagliate delle implicazioni finanziarie e operative degli incidenti informatici, che rientrano invece nei requisiti oggi imposti dalla SEC. Questa tendenza, secondo la quale le società forniscono informazioni inadeguate sugli incidenti informatici nonostante la decisione della SEC, potrebbe indicare la necessità di redigere un guida migliore e di una supervisione da parte di autorità regolatorie per garantire una conformità coerente ed efficace.

Le decisioni della SEC sulla sicurezza informatica rappresentano un cambiamento normativo significativo, volto a migliorare la trasparenza e la responsabilità nella segnalazione degli incidenti. L'adesione a queste nuove regole in modo coerente e in buona fede richiederà una collaborazione continua tra enti regolatori, aziende e stakeholder del settore.

[9] Forbes, **Companies Are Already Not Complying With The New SEC Cybersecurity Incident Disclosure Rules**, 4 marzo 2024.

L'impatto delle azioni delle forze dell'ordine

Qakbot neutralizzato dalla "Operation Duck Hunt"

Il 29 agosto 2023, nell'ambito di uno sforzo multinazionale coordinato, l'FBI (Federal Bureau of Investigation) e il Dipartimento di Giustizia (DOJ) degli Stati Uniti hanno annunciato l'operazione Duck Hunt. Zscaler ThreatLabz ha fornito un'importante assistenza tecnica alle forze dell'ordine per supportare questa operazione.[10] L'infrastruttura di Qakbot era stata progettata per resistere ai tentativi di rimozione attraverso un'infrastruttura a più livelli, come mostrato nella Figura 11.

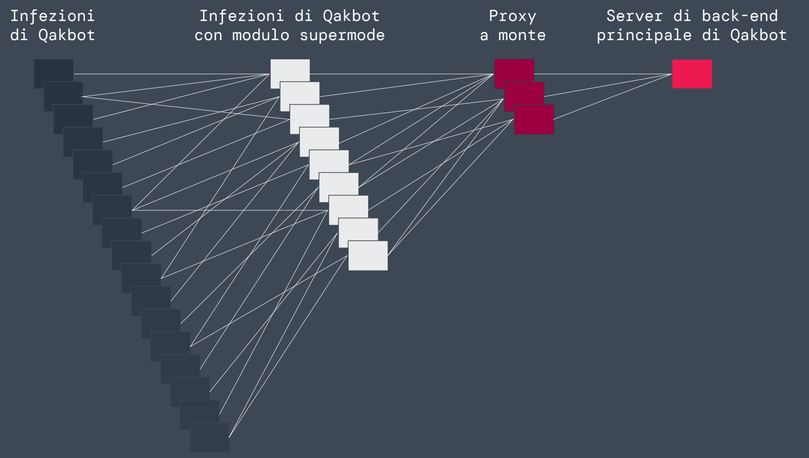


Figura 11: infrastruttura multilivello di Qakbot.

Questa infrastruttura forniva diversi livelli di resilienza, ciascuno dei quali richiedeva uno sforzo coordinato per essere smantellato. Il primo livello dell'infrastruttura di Qakbot includeva sistemi infetti che eseguivano un plugin supernodo che inoltrava il traffico a monte a diversi proxy progettati per nascondere il server di backend principale di Qakbot.

L'operazione Duck Hunt ha reindirizzato i server proxy a monte del supernodo su una serie di server sinkhole per prendere immediatamente il controllo dell'infrastruttura di Qakbot, come mostrato nella Figura 12.

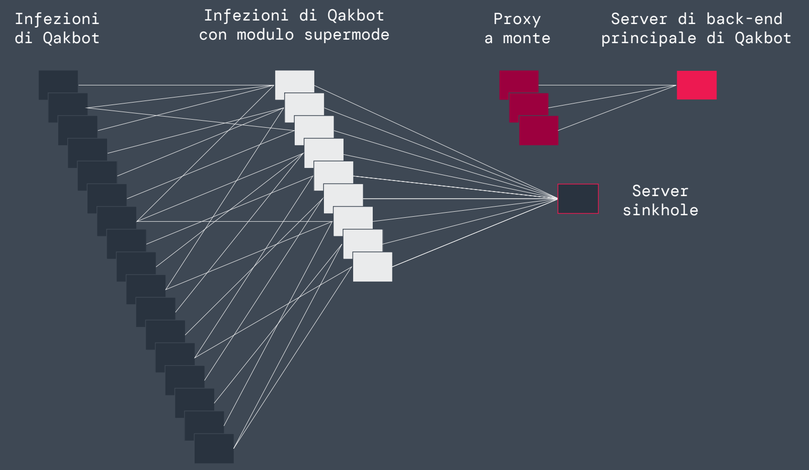


Figura 12: architettura di Qakbot dopo il reindirizzamento dei proxy a monte di ciascun supernodo.

Una volta che l'FBI ha preso il controllo dei supernodi, i server sinkhole hanno richiesto ai computer delle vittime di scaricare lo shellcode che caricava di riflesso una DLL che neutralizzava il malware. Ciò ha consentito di risanare con successo i computer delle vittime, impedendo ulteriori attacchi.

Al momento della rimozione, Qakbot aveva infettato più di 700.000 computer in tutto il mondo, di cui oltre 200.000 solo negli Stati Uniti.[11] Prima di questa operazione, **Qakbot era attivo da quasi 15 anni**; originariamente nato per facilitare le frodi basate su carte di credito e trasferimenti bancari, nel 2019, il gruppo è passato a fungere da broker di accesso iniziale per gruppi ransomware tra cui Conti, ProLock, Egregor, REvil, MegaCortex e Black Basta.

Il malware Qakbot veniva generalmente distribuito tramite e-mail di spam contenenti allegati o collegamenti dannosi. Dopo l'infezione, spesso veniva utilizzato Cobalt Strike per il movimento laterale e l'eventuale distribuzione di ransomware.

Sfortunatamente, non ci sono stati arresti o rinvii a giudizio desecretati contro gli autori della minaccia e Qakbot **è riemerso a dicembre del 2023**. Il gruppo ha aggiornato il malware per supportare le versioni a 64 bit di Windows, ha modificato il formato di configurazione interno e ha variato la comunicazione di rete per utilizzare la crittografia AES. Come discuteremo più avanti nel report, l'autore di Qakbot ha modificato in modo significativo le proprie TTP dai tempi dell'operazione Duck Hunt.

[10] Dipartimento di Giustizia degli Stai Uniti, **Qakbot Malware Disrupted in International Cyber Takedown**, 29 agosto 2023.
[11] TechCrunch, **How the FBI took down the notorious Qakbot botnet**, 1 settembre 2023.

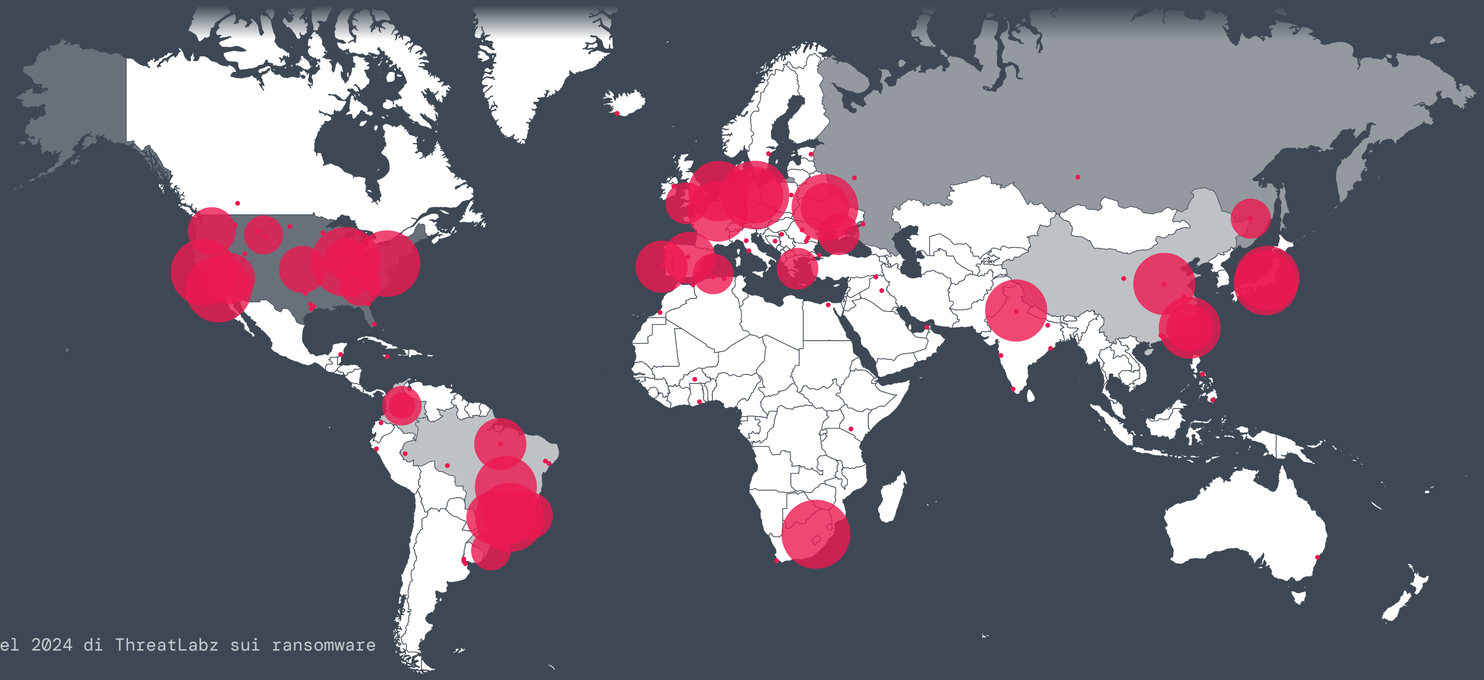
L'"Operazione Endgame" ha preso di mira contemporaneamente più broker di accesso iniziale

Il 28 maggio 2024, in collaborazione con numerose forze dell'ordine a livello internazionale, l'Europol ha annunciato l'Operation Endgame, che ha preso di mira contemporaneamente più broker di accesso iniziale. Ciò ha portato a più di una dozzina di perquisizioni globali, numerosi arresti e alla chiusura di oltre 100 server utilizzati per le attività criminali. Questi server erano parte integrante delle operazioni di vari downloader di malware (noti anche come "loader") che venivano utilizzati per infiltrarsi nei computer delle vittime, distribuendo software dannoso inclusi i ransomware.

Le famiglie di malware prese di mira da questa operazione sono state responsabili dell'infezione di milioni di computer in tutto il mondo, tra cui infrastrutture sanitarie e servizi infrastrutturali critici. Nell'ambito dell'operazione, sono stati presi provvedimenti contro SmokeLoader, Pikabot, Bumblebee e IcedID.

Zscaler ThreatLabz ha fornito assistenza tecnica per supportare la tecnica di sinkhole e le attività di bonifica contro SmokeLoader impiegate nell'operazione Endgame.

SmokeLoader, attivo dal 2011, è stato utilizzato da diversi broker di accesso iniziale per lanciare ransomware, tra cui Raspberry Robin e il gruppo di ransomware Stop (aka DJVU). L'operazione Endgame ha sequestrato più di 1.000 domini di SmokeLoader utilizzati da questi gruppi hacker. Questi domini venivano poi reindirizzati su un server sinkhole controllato dalle forze dell'ordine. La mappa riportata nella Figura 13 mostra i sistemi infetti che comunicavano con il sinkhole di SmokeLoader.



Questa mappa mostra l'impatto di vasta portata che SmokeLoader ha avuto in tutto il mondo, con infezioni significative in America Latina, Asia, Nord America ed Europa.

Figura 13: mappa delle infezioni di SmokeLoader che comunicano con il server sinkhole dell'operazione Endgame. (Fonte: Zscaler ThreatLabz)

Quando i sistemi infettati da SmokeLoader si connettevano al server sinkhole, ricevevano il comando di disinstallazione integrato del malware. Fino a oggi, sono stati ripuliti più di 40.000 sistemi infettati da SmokeLoader, come mostrato nella Figura 14.

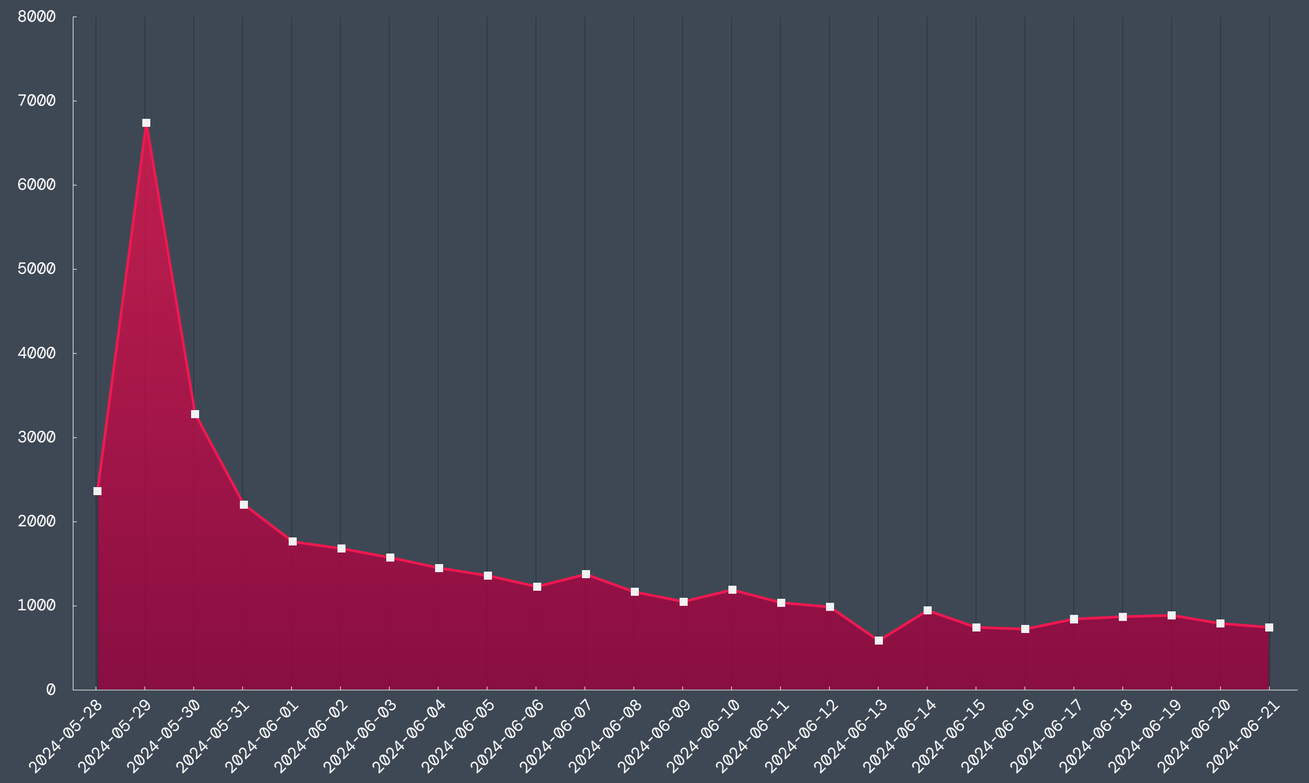


Figura 14: sistemi SmokeLoader risanati dall'operazione Endgame.

Pikabot è emerso originariamente all'inizio del 2023 e ha mostrato un'attività significativa nella seconda metà dell'anno. Questo aumento è riconducibile al fatto che il malware era diventato il broker di accesso iniziale preferito per il ransomware Black Basta dopo che l'operazione Duck Hunt aveva neutralizzato Qakbot. Nel febbraio 2024, **Pikabot è riemerso con cambiamenti significativi** a livello di base del codice e struttura. Pikabot è stato osservato da ThreatLabz utilizzare regolarmente **Cobalt Strike e Meterpreter** di Metasploit.

Bumblebee è stato introdotto a marzo del 2022 e aveva legami con l'ex gruppo ransomware Conti. Questo malware era il successore dello strumento malware BazarLoader del gruppo, utilizzato per l'accesso iniziale negli attacchi ransomware Conti e Diavol. ThreatLabz ha spesso osservato sia BazarLoader che Bumblebee distribuire payload di Cobalt Strike per il movimento laterale. Bumblebee è stato inoltre associato agli attacchi ransomware Akira e Black Basta.

In modo analogo a Qakbot, quando è apparso nel 2017, IcedID è stato originariamente concepito come trojan bancario. In seguito però il gruppo ha spostato il proprio focus per assumere il ruolo di broker di accesso iniziale per i ransomware. Nel corso degli anni, il codice malware di IcedID è stato modificato e riadattato per vari scopi. Inoltre, gli stessi sviluppatori hanno creato un nuovo loader di malware noto come Latrodectus, rilasciato a novembre del 2023, che probabilmente è stato utilizzato anche per distribuire ransomware.

Dopo l'operazione Endgame, l'attività per la maggior parte di questi broker di accesso iniziale si è ridotta, **fatta eccezione per Latrodectus**, che è riemerso in meno di un mese. Tuttavia, è probabile che questa tregua sarà di breve durata, perché gli autori delle minacce si riorganizzano costantemente.

Il ransomware Hive rinasce come Hunters International

A gennaio del 2023, l'infrastruttura del gruppo ransomware Hive è stata chiusa. Dopo un'operazione segreta, durata sette mesi, l'FBI riesce nell'intento di infiltrarsi nei server di Hive, recuperando più di 300 chiavi di decrittazione prevenendo così 130 milioni di dollari di riscatti. Operativo da giugno 2021, il collettivo Hive ha preso di mira e vittimizzato più di 1.500 organizzazioni in tutto il mondo, raccogliendo oltre 100 milioni di dollari in riscatti pagati.[12] Le vittime hanno incluso ospedali, distretti scolastici, istituti finanziari e varie altre realtà. Tuttavia, non è stato effettuato alcun arresto associato ad Hive e il gruppo è stato ribattezzato Hunters International a ottobre del 2023. I criminali informatici adottano spesso questa strategia di rebranding dopo un'interruzione importante.

Il gruppo ha modificato considerevolmente le proprie modalità operative e non offrirà più sconti, né negozierà con le vittime sulla richiesta di riscatto iniziale, come mostrato nella Figura 15.

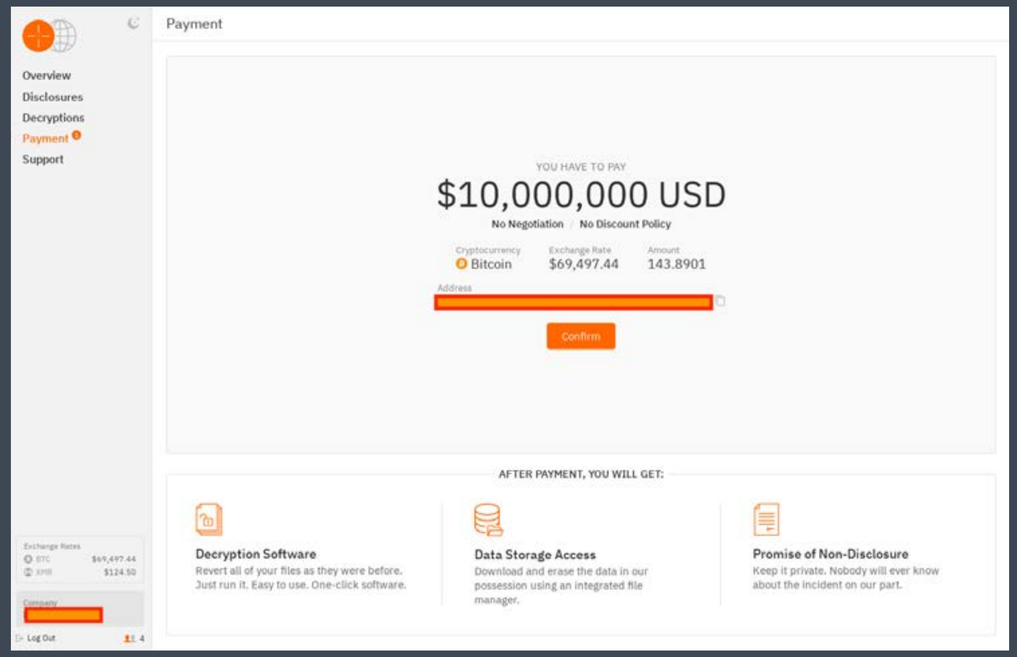


Figura 15: portale delle vittime di Hunters International senza sconti o negoziazioni sui prezzi.

La politica dei prezzi non negoziabili è **molto rara** tra i gruppi ransomware, che spesso offrono sconti significativi rispetto alla richiesta di riscatto originaria. Questa decisione del team di Hunters porterà probabilmente a un volume di pagamenti inferiore, ma a importi complessivi incassati molto più elevati.

Hunters International continua a lanciare nuovi attacchi ed è probabile che rimarrà una minaccia pervasiva, senza ulteriori arresti e rinvii a giudizio.

[12] Dipartimento di Giustizia degli Stati Uniti, **U.S. Department of Justice Disrupts Hive Ransomware Variant**, 26 gennaio 2023.

Le cinque principali famiglie di ransomware da tenere d'occhio nel 2024-2025

Con i ransomware e le altre minacce informatiche che continuano a evolversi a livello di complessità e sofisticatezza, rimanere informati sulle famiglie di ransomware più diffuse e pericolose è fondamentale per preservare l'efficacia del proprio approccio alla sicurezza. Questa sezione evidenzia cinque famiglie di ransomware che sono tra le più pericolose per le aziende, fornendo approfondimenti sulle loro tattiche, sul potenziale impatto e sulle attività recenti.

N.1 Dark Angels

Il gruppo ransomware Dark Angels, che gestisce il sito di data leak di Dunghill, è emerso intorno a maggio del 2022. Il gruppo ha condotto alcuni dei più significativi attacchi ransomware, ma è riuscito nell'intento di destare poca attenzione. All'inizio del 2024, ThreatLabz ha scoperto una vittima che ha pagato a Dark Angels 75 milioni di dollari, una somma che supera qualsiasi importo pubblicamente noto: un risultato destinato ad attirare l'interesse di altri aggressori che cercheranno di replicare tale successo adottando le medesime tattiche chiave (che descriveremo in seguito). Dark Angels si rivolge a vari settori, tra cui sanità, pubblica amministrazione, finanza e istruzione. Più di recente, ha lanciato attacchi contro grandi aziende industriali, tecnologiche e di telecomunicazione.

Il gruppo Dark Angels utilizza un approccio altamente mirato, attaccando in genere una singola grande azienda alla volta. Ciò è in netto contrasto con la maggior parte dei gruppi ransomware, che prendono di mira le vittime indiscriminatamente ed esternalizzano la maggior parte dell'attacco a reti affiliate di broker di accesso iniziale e a team di penetration testing. Una volta identificato e compromesso un obiettivo, Dark Angels decide selettivamente se cifrare i file dell'azienda. Nella maggior parte dei casi, il gruppo Dark Angels ruba una grande quantità di informazioni, in genere nell'ordine di 1–10 TB. Nelle grandi aziende, il gruppo ha esfiltrato tra 10 e 100 TB di dati, un trasferimento che può richiedere giorni o addirittura settimane.

L'attacco di più alto profilo condotto da Dark Angels è avvenuto a settembre del 2023, quando il gruppo ha violato un conglomerato internazionale che fornisce, tra gli altri servizi, soluzioni per sistemi di automazione degli edifici. Dark Angels ha chiesto un riscatto da 51 milioni di dollari, dichiarando di aver rubato oltre 27 TB di dati aziendali e di aver cifrato le macchine virtuali VMware ESXi dell'azienda. Durante l'attacco, è stata utilizzata una variante del ransomware RagnarLocker per cifrare i file dell'azienda. La relazione tra RagnarLocker e Dark Angels non è chiara, ma il gruppo utilizzava questo ransomware prima dell'azione delle forze dell'ordine contro RagnarLocker,[13] che portò all'arresto di un membro chiave a ottobre del 2023. Si noti che quando Dark Angels è apparso per la prima volta, ha distribuito una variante di Babuk prima di passare a RagnarLocker.

La strategia del gruppo ransomware Dark Angels, basata sul prendere di mira un ristretto numero di aziende di alto valore per ottenere pagamenti più elevati, è una tendenza che va sicuramente monitorata. Zscaler ThreatLabz prevede che altri gruppi ransomware prenderanno atto del successo di Dark Angels e potrebbero adottare tattiche analoghe, concentrandosi su obiettivi di alto valore e accrescendo la rilevanza del furto dei dati, per massimizzare i loro introiti finanziari.

[13] Europol, **Ragnar Locker ransomware gang taken down by international police swoop**, 20 ottobre 2023.

N.2 LockBit

LockBit è emerso per la prima volta a settembre del 2019 e ha acquisito notorietà molto rapidamente, grazie all'ampia rete di affiliazione ransomware del gruppo. LockBit sfrutta degli affiliati per condurre violazioni, esfiltrare i dati e distribuire il suo ransomware. L'infiltrazione inizia, in genere, attraverso delle e-mail di spam contenenti allegati o link dannosi. Altri metodi includono l'esecuzione di attacchi di forza bruta alle password, che prendono di mira le credenziali RDP (Remote Desktop Protocol) o VPN, l'acquisto di credenziali rubate compromesse tramite broker di accesso iniziale e lo sfruttamento delle applicazioni rivolte al pubblico. La rete criminale di LockBit ha preso di mira settori critici come l'industria manifatturiera, la sanità e la logistica. Il gruppo ha colpito complessivamente più di 2.000 sistemi in tutto il mondo e ha estorto oltre 120 milioni di dollari alle sue vittime.

Nell'ultimo anno, LockBit è rimasto in cima alla classifica, in termini di volume di attacchi. Utilizzando una strategia nettamente diversa da Dark Angels, il gruppo LockBit incoraggia gli affiliati ad attaccare quante più organizzazioni possibili, indipendentemente dal potenziale profitto. Questo elevato volume di attacchi spesso fa sì che le piccole imprese vengano prese di mira con richieste di riscatto relativamente basse.

Il ransomware LockBit viene distribuito su sistemi basati su Windows e Linux. Esistono tre versioni di LockBit per Windows: LockBit Red (l'originale), LockBit Black (basato sul codice sorgente di BlackMatter) e LockBit Green (basato sul codice sorgente trapelato di Conti). Come menzionato nel Report del 2023 di ThreatLabz sui ransomware, il builder di LockBit Black è trapelato e molti gruppi di criminali informatici non affiliati a LockBit lo hanno utilizzato per i propri attacchi ransomware. È interessante notare che LockBit Black è ancora la variante più comunemente utilizzata dal gruppo. La variante specifica del ransomware LockBit, utilizzata per cifrare i file di una vittima, viene ora indicata nella richiesta di riscatto accanto all'ID della vittima. Ciò consente all'autore della minaccia che conduce l'attacco di identificare facilmente la variante di LockBit distribuita, per aiutarlo a fornire lo strumento di decrittazione adeguato quando viene pagato un riscatto. Si veda la Figura 16 per un esempio di una recente richiesta di riscatto di LockBit Black.

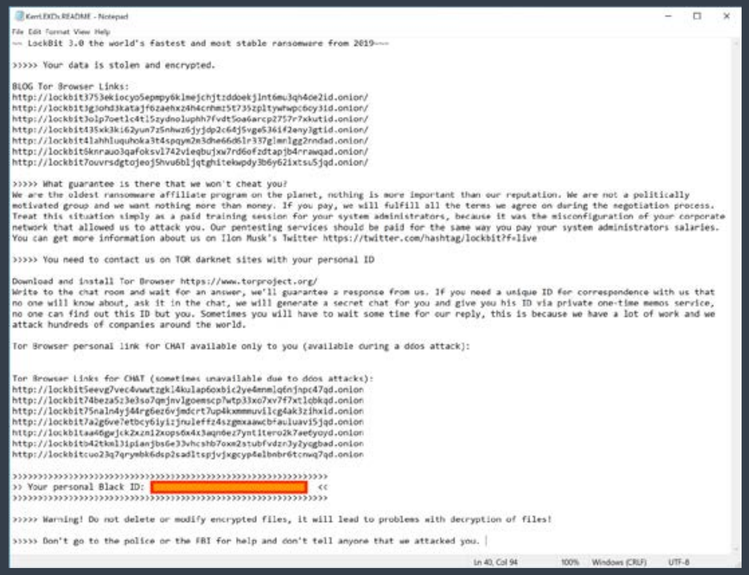


Figura 16: esempio di una recente richiesta di riscatto di LockBit Black.

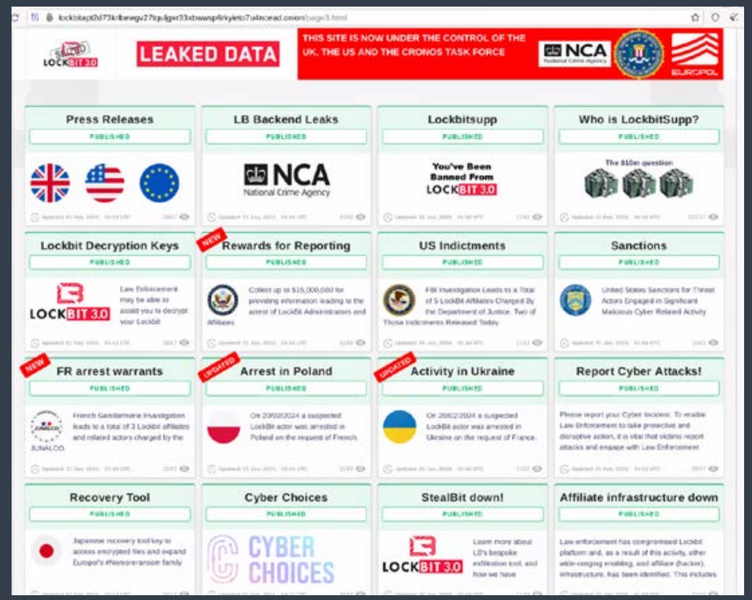


Figura 17: sequestro da parte delle forze dell'ordine del sito di data leak di LockBit.

Il 20 febbraio 2024, l'FBI e le forze dell'ordine del Regno Unito hanno sequestrato parti dell'infrastruttura di LockBit, che includevano circa 7.000 chiavi di decrittazione delle vittime. Dopo il sequestro, le forze dell'ordine hanno requisito il sito web di data leak di LockBit e hanno deriso i criminali informatici con una versione simile al sito precedente che mostrava vari articoli e timer per il conto alla rovescia fino al rilascio di nuove informazioni, come mostrato nella Figura 17 di seguito.

Sfortunatamente, pochi giorni dopo la rimozione, ThreatLabz ha identificato nuovi attacchi ransomware perpetrati da LockBit e un nuovo sito di data leak. Il gruppo è rimasto attivo e ha attaccato dozzine di nuove entità dopo l'azione delle forze dell'ordine.

Il 7 maggio 2024, l'FBI ha annunciato il rinvio a giudizio dello sviluppatore e operatore di LockBit, Dmitry Yuryevich Khoroshev. L'operatore di LockBit ha però subito dichiarato di non essere la persona che l'FBI stava cercando. Senza ulteriori arresti, gli attacchi di LockBit probabilmente continueranno nel prossimo futuro, anche se a un certo punto ThreatLabz prevede che il marchio LockBit verrà ritirato e l'operazione rinascerà con un altro nome, questo a causa del maggiore controllo.

N.3 BlackCat

BlackCat (alias ALPHV), introdotto a novembre del 2021, è stato tra le minacce più note fino alla sua chiusura a marzo del 2024. In modo analogo a LockBit, BlackCat ha sfruttato una rete di affiliazione per lanciare attacchi e condividere una percentuale dei pagamenti del riscatto.

Verosimilmente, l'affiliato più famigerato di BlackCat è un gruppo noto come Scattered Spider[14] (alias Star Fraud). Composto da membri anglofoni, questo gruppo è molto efficace negli attacchi di ingegneria sociale, impersonando spesso il personale IT o dell'assistenza tecnica nelle chiamate vocali ed effettuando attacchi di SIM swapping per eludere l'autenticazione a più fattori. Il 15 giugno 2024, il presunto boss[15] di Scattered Spider, un cittadino britannico di 22 anni, è stato arrestato. È però troppo presto per dire quale impatto avrà questo arresto sulla capacità del gruppo di continuare i suoi attacchi.

BlackCat è stata una delle famiglie di ransomware con la più elevata compatibilità multipiattaforma, in parte perché utilizza il linguaggio di programmazione Rust. La Figura 18 mostra gli strumenti di decrittazione disponibili per tutte le piattaforme supportate dal ransomware BlackCat poco prima che il gruppo interrompesse le operazioni. Le piattaforme includevano Windows, ESXi, FreeBSD e numerose varianti di sistemi operativi e architetture Linux, come ARM, x86/x64, e PowerPC.

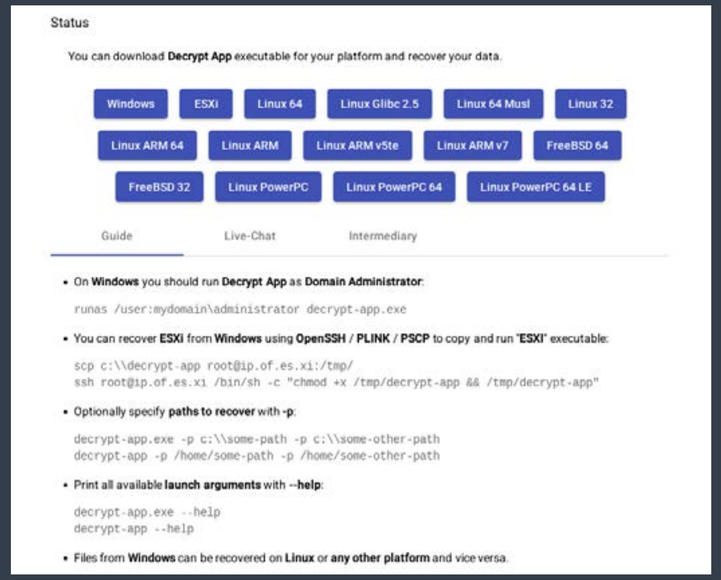


Figura 18: gli strumenti di decrittazione di BlackCat erano forniti per 15 diversi sistemi operativi, architetture e piattaforme.

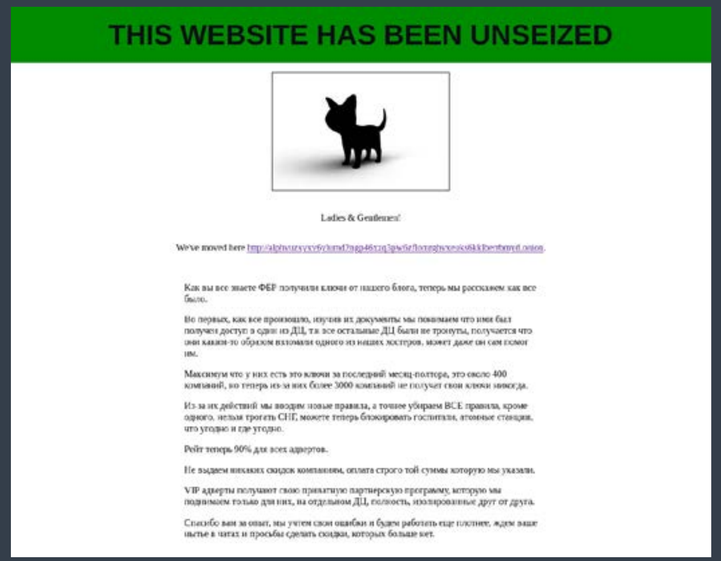


Figura 19: sito di data leak di BlackCat dopo che il gruppo ha ripreso il controllo a seguito dell'intervento delle forze dell'ordine.

Questo livello di compilazione multipiattaforma è insolito, se comparato ad altre famiglie di ransomware, che in genere supportano solo Windows, ESXi e un numero limitato di piattaforme basate su Linux. Ciò indica che gli affiliati di BlackCat potrebbero aver richiesto un supporto per più piattaforme al fine di cifrare i file sul maggior numero di sistemi possibile.

Nel dicembre del 2023, l'FBI ha ottenuto l'accesso ad alcune infrastrutture di BlackCat. Ha quindi tentato di sequestrare i siti web basati su Tor del gruppo, inclusi i portali per la negoziazione del riscatto e i siti di data leak. Tuttavia, in una rapida svolta degli eventi, BlackCat ha pubblicato un messaggio in cui informava di essere riuscito a riprendere il controllo dopo il sequestro del sito web di data leak e forniva un collegamento a un nuovo sito web di data leak che l'FBI non era in grado di manipolare, come mostrato nella Figura 19 di seguito.

Questo continuo andirivieni tra l'FBI e BlackCat è durato pochi giorni, fino a quando BlackCat non ha avuto la certezza che il nuovo sito di data leak fosse stato sufficientemente pubblicizzato. Va notato che "sequestrare" un sito web basato su Tor non è un'operazione banale, come nel caso di un sito web tradizionale basato su DNS, perché si basa su segreti crittografici anziché che su un'autorità centrale soggetta alle ordinanze del tribunale.

A marzo del 2024, il gruppo BlackCat ha annunciato il proprio scioglimento, citando la compromissione della propria infrastruttura da parte dell'FBI, che presumibilmente li avrebbe resi incapaci di continuare le loro operazioni. Tuttavia, sono sorti sospetti a causa della tempistica della loro chiusura avvenuta immediatamente dopo aver ricevuto un riscatto di 22 milioni di dollari, per poi truffare con una scam exit un affiliato che aveva assistito il gruppo a violare un fornitore di servizi per il settore sanitario (come discusso in precedenza in questo report).

Sebbene il ransomware BlackCat non sia più attivo, gli affiliati dietro agli attacchi del gruppo sono verosimilmente migrati su altre reti ransomware-as-a-service come RansomHub (dove sono divulgati i dati rubati all'operatore sanitario che ha pagato i 22 milioni di dollari). Inoltre, è improbabile che il gruppo ransomware BlackCat stesso abbia realmente cessato le proprie attività e probabilmente riemergerà sotto un nuovo nome.

[14] Cybersecurity & Infrastructure Security Agency, **Cybersecurity Advisory: Scattered Spider**, 16 novembre 2023.
[15] Krebs on Security, **Alleged Boss of 'Scattered Spider' Hacking Group Arrested**, 15 giugno 2024.

N.4 Akira

Il ransomware Akira ha fatto il suo ingresso in scena ad aprile del 2023, guadagnandosi rapidamente notorietà per il volume degli attacchi condotti dagli affiliati. Il gruppo Akira è probabilmente un altro ramo del defunto gruppo Conti. Infatti il codice del ransomware di Akira condivideva originariamente molte somiglianze con il codice sorgente di Conti trapelato. Tuttavia, il gruppo ha recentemente sviluppato un ransomware basato su Rust che contiene riferimenti a personaggi dei Power Rangers, come Megazord.

Gli affiliati del ransomware Akira hanno utilizzato vari meccanismi per l'accesso iniziale, anche attraverso lo sfruttamento della CVE-2023-20269.[16] Anche il gruppo hacker che gestisce Bumblebee, che ha legami con il ransomware Conti, è noto per essere un broker di accesso iniziale per Akira. Come accennato in precedenza nel report, l'operazione Endgame ha smantellato Bumblebee, ma ha avuto un impatto minimo sulle operazioni di Akira.

Per comprendere meglio gli attacchi di Akira possiamo sfruttare direttamente le informazioni che Akira fornisce alle vittime che pagano un riscatto. ThreatLabz è entrato in possesso del seguente messaggio di chat di Akira, che contiene dettagli su come hanno inizialmente ottenuto l'accesso alla rete dell'azienda tramite un broker di accesso iniziale e offre anche suggerimenti per prevenire attacchi ransomware in futuro:

L'accesso iniziale alla tua rete è stato acquistato sul dark web. Abbiamo quindi lanciato un attacco di kerberoasting e abbiamo ottenuto gli hash delle password. Dopodiché, ci è bastato usare la forza bruta per ottenere la password dell'amministratore del dominio. Dopo aver trascorso settimane all'interno della tua rete, siamo riusciti a rilevare alcuni errori che ti consigliamo vivamente di eliminare:

1. Nessuno dei tuoi dipendenti dovrebbe aprire e-mail sospette, collegamenti sospetti o scaricare file, tanto meno eseguirli sul proprio computer.

2. Utilizza password complesse, cambiale il più spesso possibile (almeno 1-2 volte al mese). Le password non devono corrispondere o essere riutilizzate per risorse diverse.

3. Installa la 2FA ove possibile.

4. Utilizza le versioni più recenti dei sistemi operativi, in quanto sono meno vulnerabili agli attacchi.

5. Aggiorna tutte le versioni dei software.

6. Utilizza soluzioni antivirus e strumenti di monitoraggio del traffico.

7. Crea un jump host per la tua VPN. Utilizza credenziali specifiche per quest'ultimo, diverse dal dominio uno.

8. Utilizza un software di backup con archiviazione sul cloud che supporti una chiave token.

9. Occupati dalla formazione dei tuoi dipendenti, istruendoli il più frequentemente possibile sulle precauzioni da adottare nell'ambito della sicurezza online. Il punto più vulnerabile è il fattore umano e l'irresponsabilità dei tuoi dipendenti, amministratori di sistema, ecc. Ti auguriamo un futuro di sicurezza, serenità e ricco di opportunità. Grazie per aver collaborato con noi e per il tua attenzione per la sicurezza.

Sebbene questi consigli provengano direttamente da Akira, le raccomandazioni sono valide e forniscono una base per imparare a riconoscere e contrastare tali attacchi.

Akira è uno dei pochi grandi gruppi ransomware che non è stato direttamente interessato dalle interruzioni legate alle attività delle forze dell'ordine. Di conseguenza, è attualmente uno dei gruppi ransomware più attivi che probabilmente continuerà a lanciare nuovi attacchi nel corso del prossimo anno.

[16] https://nvd.nist.gov/vuln/detail/CVE-2023-20269

N.5 Black Basta

Il ransomware Black Basta, identificato per la prima volta ad aprile del 2022, è un altro successore del gruppo ransomware Conti. Gli affiliati di Black Basta hanno utilizzato diversi metodi per ottenere l'accesso alle reti aziendali. Prima dell'operazione Duck Hunt (agosto 2023), Qakbot era uno dei principali broker di accesso iniziale per Black Basta. Come accennato in precedenza, dopo lo smantellamento, il vuoto è stato riempito dall'ingresso in scena di Pikabot. Tuttavia, quest'ultimo è stato chiuso dopo l'operazione Endgame a maggio del 2024.

Da allora, ThreatLabz ha monitorato le nuove attività del gruppo di minacce Qakbot, rilevando che quest'ultimo ha cambiato radicalmente le sue TTP. Invece di utilizzare e-mail di spam per infettare i sistemi con Qakbot, il gruppo ora utilizza una combinazione di tecniche di ingegneria sociale. Invece di inviare e-mail di spam a milioni di indirizzi, ora esegue attacchi mirati. Questi attacchi iniziano con l'invio di e-mail di spam da parte del gruppo criminale a un numero limitato di aziende prese di mira. Il gruppo chiama quindi a un dipendente di queste aziende fingendo di appartenere al reparto IT. Chi chiama ordina alla vittima di partecipare a una sessione di condivisione dello schermo, utilizzando un software di desktop remoto come Quick Assist di Microsoft, per "aggiornare i filtri antispam dell'azienda" per il dipendente. Una volta che il dipendente ha concesso l'accesso all'autore della minaccia, viene eseguito uno script batch di Windows per lanciare la ricognizione, rubare le credenziali e installare una backdoor sul sistema della vittima. La backdoor continua a cambiare, ma ha incluso Qakbot, Cobalt Strike e uno strumento proxy SOCKS. Lo script batch contiene un'interfaccia della riga di comando simile a quella mostrata nella Figura 20.

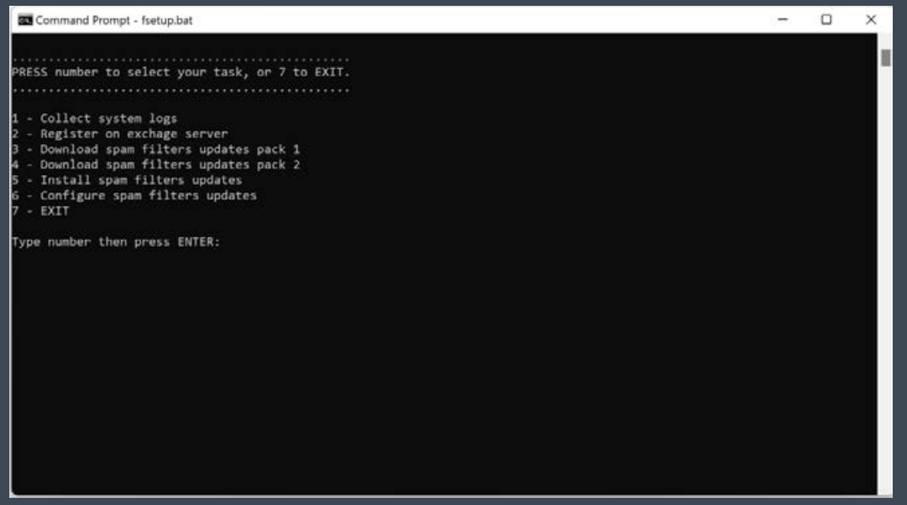


Figura 20: interfaccia dello script batch dannoso di Windows utilizzato per creare una backdoor sul sistema di una vittima come precursore di un attacco ransomware Black Basta.

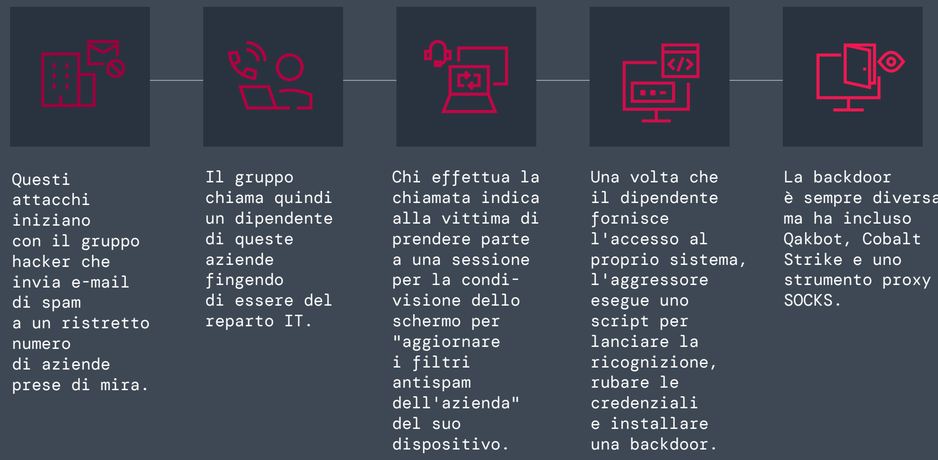


Figura 21: catena di attacco del ransomware Black Basta con accesso iniziale mediato dal gruppo hacker Qakbot.

Una volta instaurato l'accesso tramite backdoor, il gruppo Qakbot lo trasferisce a un team di penetration testing responsabile del movimento laterale e dell'implementazione finale del ransomware Black Basta.

Sebbene l'operazione Duck Hunt abbia avuto un impatto significativo a breve termine, questo gruppo di minacce è ancora attivo e continua a innovarsi e sperimentare nuove tecniche per compromettere le organizzazioni. Nel corso del prossimo anno, il gruppo Qakbot rimarrà probabilmente un importante broker di accesso iniziale per gli attacchi ransomware come Black Basta.

Archivio di ThreatLabz delle richieste di riscatto dei ransomware

Zscaler ThreatLabz gestisce un repository pubblico su GitHub che, al momento della stesura di questo documento, tiene traccia di 391 famiglie di ransomware e contiene un totale di 945 richieste di riscatto, e ha aggiunto 19 famiglie e 55 richieste di riscatto tra aprile 2023 e aprile 2024. Questo archivio può essere utile per monitorare i gruppi ransomware nel tempo, compresi i siti web di data leak e le tattiche di negoziazione, e per ricollegare i gruppi che cambiano nome, utilizzando l'analisi stilometrica.

La Figura 22 mostra un confronto stilometrico tra una chat per il riscatto di Conti (in alto) e una chat di Black Basta (in basso). Ciò dimostra che i membri di Black Basta sono quasi certamente ex membri di Conti, come risulta evidente dalle somiglianze nella struttura delle frasi, nella scelta delle parole e persino nelle istruzioni specifiche.

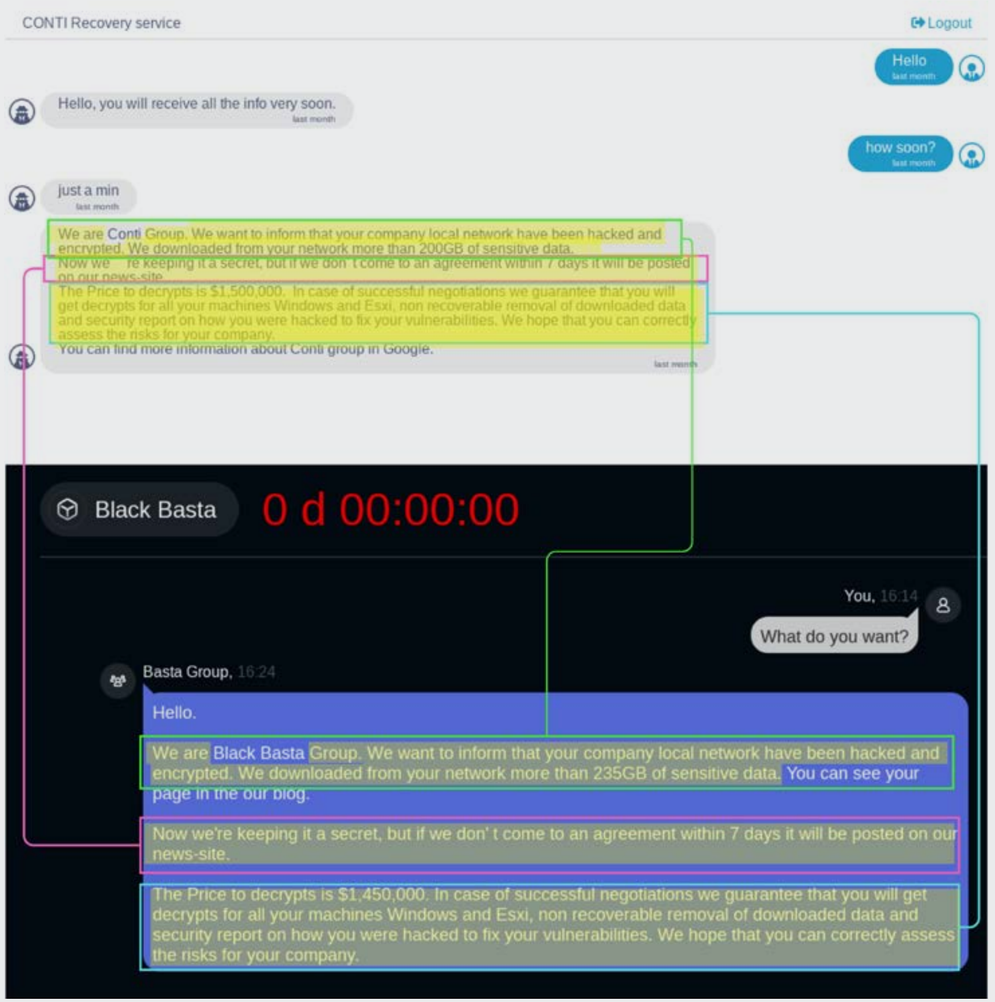


Figura 22: confronto stilometrico tra le chat per il riscatto di Conti (in alto) e Black Basta (in basso).

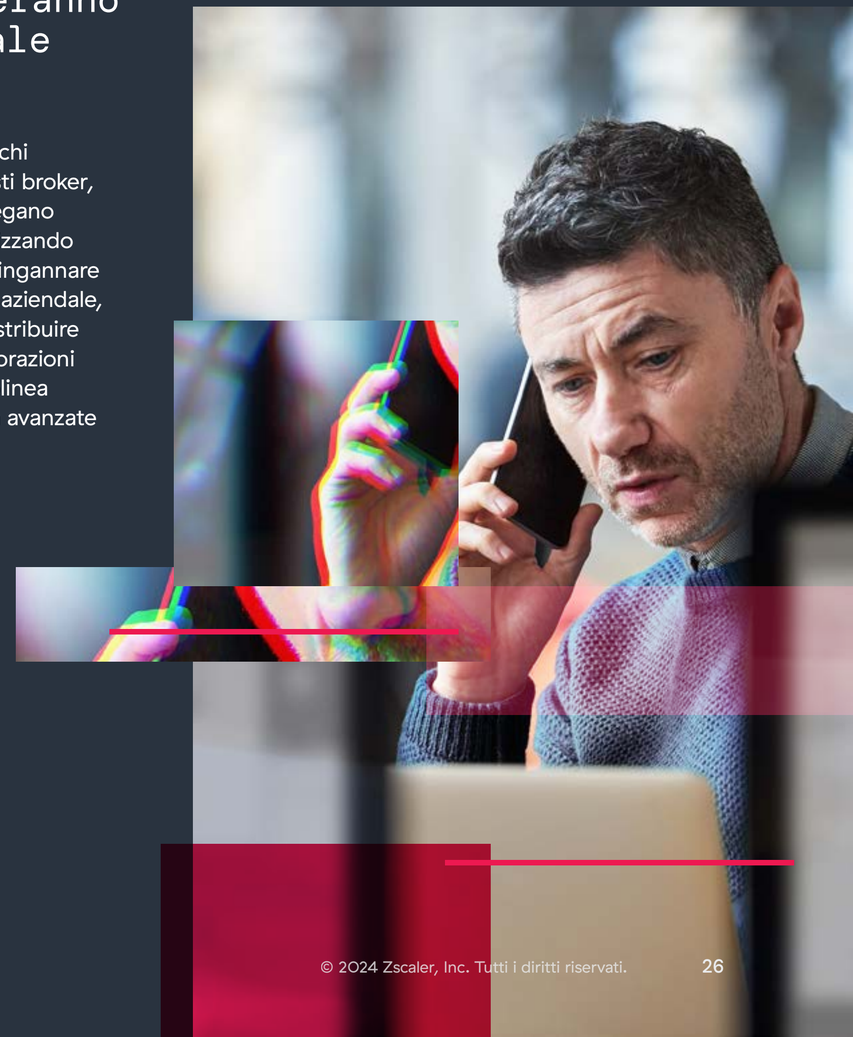
Previsioni per il 2024-2025

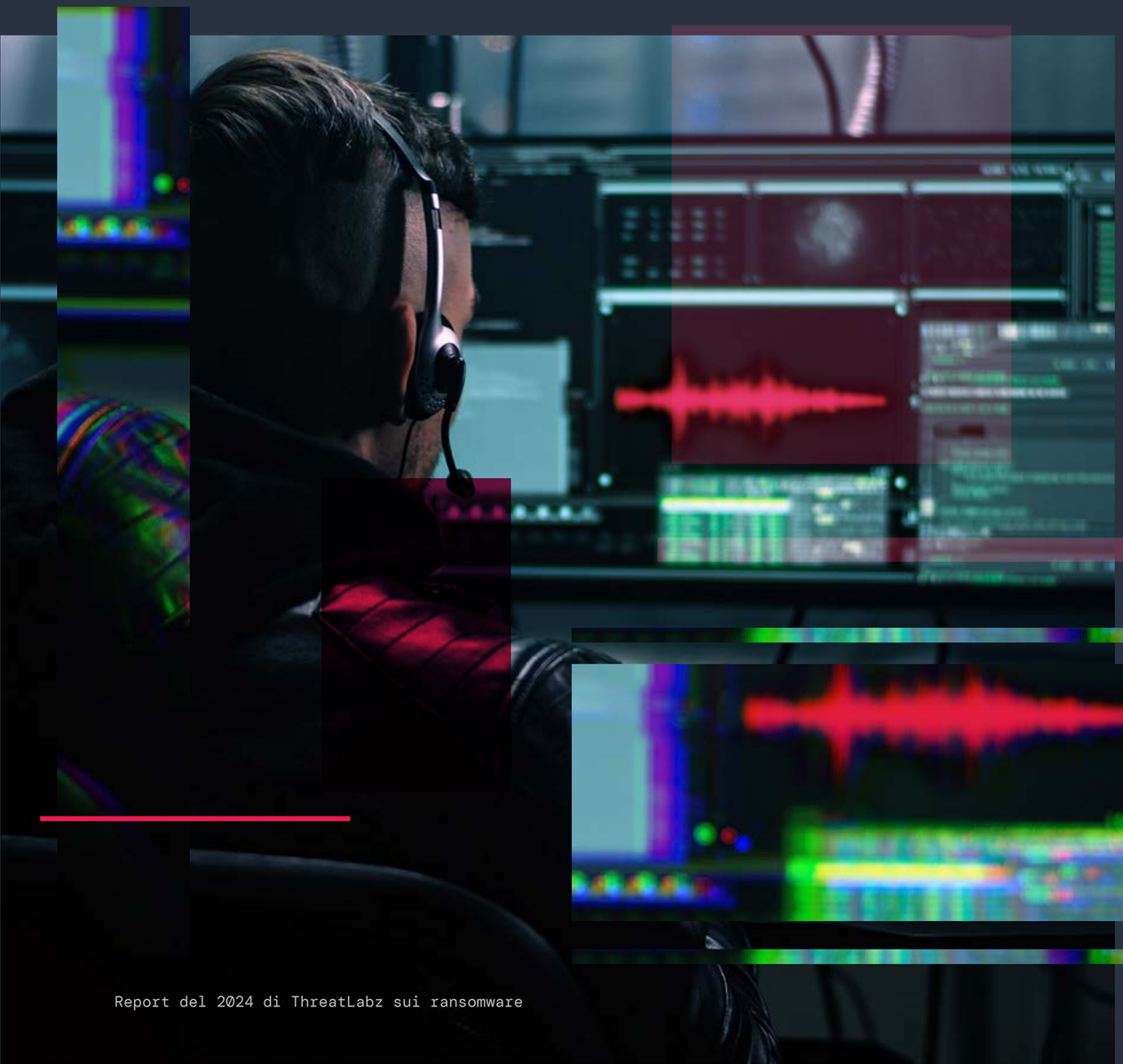
1. Gli autori delle minacce ransomware adotteranno strategie di attacco altamente mirate.

Nel corso dell'ultimo anno, Dark Angels è stato uno dei gruppi ransomware di maggior successo e meno conosciuti, caratterizzato da una strategia molto particolare volta a prendere di mira un ristretto numero di aziende multimiliardarie ed estorcere riscatti ingenti. Questa strategia ha un duplice scopo: approfittare di un controllo ridotto da parte delle forze dell'ordine e del settore della sicurezza, spendendo allo stesso tempo più risorse per infiltrarsi in grandi aziende disposte a pagare riscatti molto elevati pur di proteggere enormi volumi di dati rubati. Ciò ha portato il gruppo a ricevere il più grande riscatto della storia dei ransomware, pari a 75 milioni di dollari, che è destinato ad attirare l'interesse di altri autori di minacce ransomware nel 2025, che potrebbero voler replicare questo successo.

2. Gli attacchi mirati coinvolgeranno sempre più l'ingegneria sociale basata sulla voce.

Nel 2025, prevediamo di registrare un incremento degli attacchi mirati facilitati da broker di accesso iniziale specializzati. Questi broker, esemplificati dalle attività di Qakbot e Scattered Spider, impiegano tecniche sofisticate per assicurare l'accesso, in particolare utilizzando attacchi di ingegneria sociale basati sulla voce ("vishing") per ingannare gli individui inducendoli a concedere l'accesso a un ambiente aziendale, che viene poi utilizzato in ultima analisi per esfiltrare dati e distribuire ransomware. Questa tendenza emergente evidenzia le collaborazioni all'interno dell'ecosistema della criminalità informatica e sottolinea la necessità di una maggiore vigilanza e di misure di sicurezza avanzate per contrastare queste minacce in evoluzione.





3. Gli aggressori che lanciano ransomware adotteranno sempre più l'IA generativa, o GenAI, per creare campagne più efficaci, personalizzate e localizzate.

L'adozione dell'IA generativa crescerà nel 2025 e in futuro e consentirà agli autori delle minacce di creare e-mail di spam con grammatica e ortografia accurate, nonché di utilizzare la clonazione vocale per impersonare i dipendenti dell'azienda al fine di ottenere un accesso privilegiato. Nei prossimi anni, le voci generate dall'IA potrebbero essere personalizzate con accenti e dialetti locali, per migliorarne la credibilità e accrescere le probabilità di successo, e ciò è un ottimo esempio di come gli autori delle minacce ransomware riusciranno a rendere gli attacchi ancora più convincenti e difficili da rilevare.

4. Verranno segnalati sempre più incidenti di sicurezza informatica in linea con le nuove regole della SEC.

A seguito della decisione della SEC, che impone una segnalazione più rigorosa degli incidenti di sicurezza informatica, il 2025 continuerà a vedere un aumento delle organizzazioni che divulgheranno gli incidenti subiti legati ai ransomware. La speranza è che ciò si traduca in una maggiore trasparenza e promuova una cultura di responsabilità e difese proattive, guidando miglioramenti nelle pratiche di sicurezza informatica.

5. Gli attacchi ransomware con esfiltrazione di grandi volumi di dati saranno in aumento.

Gli attacchi basati dull'esfiltrazione grandi quantitativi di dati, compresi gli incidenti senza crittografia, aumenteranno in modo smisurato nel corso del prossimo anno. Questa tendenza, che ha iniziato a prendere slancio nel 2022, vede gli autori delle minacce concentrarsi esclusivamente sull'esfiltrazione dei dati, senza cifrare i sistemi. Questo approccio consente operazioni più rapide e opportunistiche e sfrutta la paura che i dati sensibili vengano divulgati per costringere le vittime a pagare un riscatto. Ciò sottolinea un continuo spostamento delle strategie ransomware verso metodi più efficienti e ad alto impatto.

6. Le aziende del settore sanitario, in particolare, continueranno a registrare attacchi persistenti da parte dei gruppi ransomware.

L'elevato valore dei dati sanitari continuerà ad attirare l'attenzione anche nel 2025. Molte aziende sanitarie faticano a sostituire i sistemi legacy con misure di sicurezza moderne e avanzate, il che le rende particolarmente vulnerabili. Di conseguenza, queste organizzazioni rischiano di dover affrontare ripetute violazioni e tentativi di estorsione. Le realtà che non riusciranno a intraprendere le azioni necessarie per dare priorità alle strategie di difesa zero trust potrebbero ritrovarsi prese di mira dai gruppi ransomware.

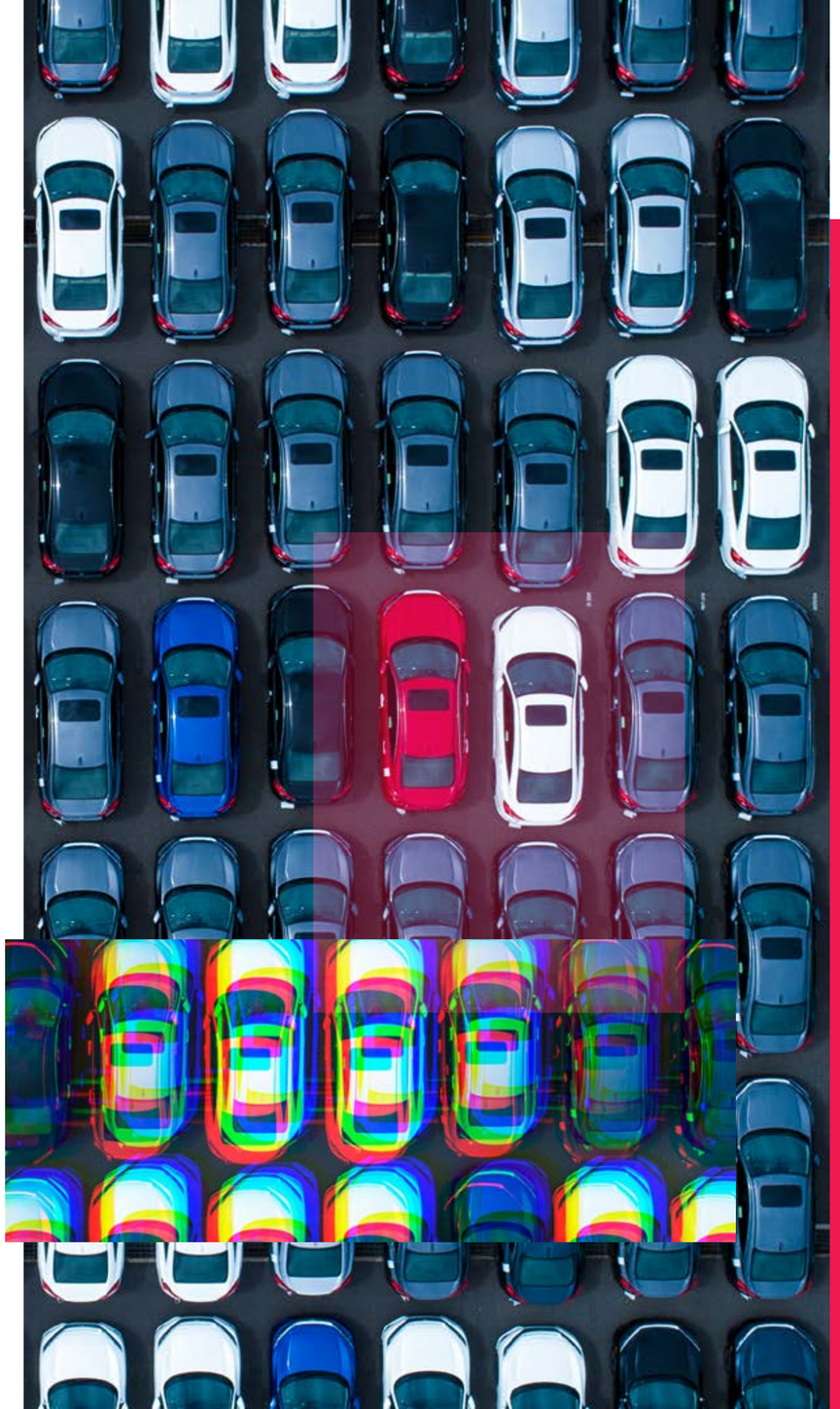
7. La collaborazione internazionale contro le organizzazioni criminali informatiche si baserà sugli sforzi già esistenti.

Le forze dell'ordine e il settore privato continueranno a collaborare attivamente per combattere gli attacchi ransomware, ad esempio interrompendo i principali broker di accesso iniziale e gruppi ransomware. La collaborazione internazionale diventerà sempre più vitale, data la crescente l'interconnessione globale che rende più semplice per i criminali informatici operare a livello transnazionale. Condividendo informazioni e competenze, queste azioni coordinate riusciranno a interrompere in modo più efficace le reti ransomware globali. Zscaler ThreatLabz è sempre stato in prima linea e determinante nel fornire assistenza tecnica per molte di queste operazioni nel corso dell'ultimo anno.

In che modo Zscaler semplifica la protezione dai ransomware

La crescente complessità e il costo in costante aumento degli attacchi ransomware sottolineano la necessità di adottare difese zero trust complete. La piattaforma Zscaler Zero Trust Exchange™ semplifica questa sfida, offrendo un approccio olistico per fermare i ransomware.

Zero Trust Exchange consente alle aziende di implementare difese più intelligenti ed efficaci contro tutte le fasi di un attacco. Tutto ciò inizia con impedire agli aggressori di rilevare o sfruttare gli utenti e le applicazioni, rendendo tali utenti e app invisibili e concedendo l'accesso solo agli utenti o ai dispositivi autorizzati. Questa soluzione ispeziona tutto il traffico in entrata e in uscita inline, cifrato o meno. Gli utenti e i dispositivi autenticati si connettono direttamente alle applicazioni di cui hanno bisogno, mai alla rete; in questo modo, anche se un aggressore riesce ad autenticarsi, non è in grado di muoversi lateralmente per rubare o cifrare i dati.



PERCHÉ LO ZERO TRUST È FONDAMENTALE PER PROTEGGERSI DAI RANSOMWARE
Le architetture di sicurezza legacy sono inefficaci nel fermare gli attacchi ransomware.

DIAMO UN TAGLIO AL PASSATO: le misure di sicurezza tradizionali e le soluzioni indipendenti, inclusi firewall di "nuova generazione" e VPN, spesso introducono punti ciechi, complessità e costi significativi. Questi approcci legacy non sono in grado di ispezionare in modo economicamente vantaggioso il traffico e i file cifrati, rendendo così le organizzazioni vulnerabili al movimento laterale e agli attacchi ransomware che sfruttano le lacune nella visibilità e nel controllo, spesso con conseguenze devastanti.

AVANTI CON LO ZERO TRUST:
un'architettura zero trust presuppone che ogni singolo utente, connessione o dispositivo sia potenzialmente compromesso. Questo approccio impone una verifica continua e un controllo rigoroso degli accessi. Verificando costantemente le identità e ispezionando tutto il traffico, compresi i dati cifrati, lo zero trust riduce significativamente il rischio di subire attacchi e che essi si diffondano all'interno della rete, neutralizzando le minacce ransomware prima che possano causare danni.

ZSCALER BLOCCA OGNI FASE DEL CICLO DI ATTACCO DEI RANSOMWARE: dalla ricognizione iniziale e dalla compromissione al movimento laterale, al furto di dati e all'esecuzione del payload.

Riduzione della superficie di attacco: Zero Trust Exchange è una soluzione basata su un'architettura zero trust, che sostituisce le architetture VPN e i firewall legacy sfruttabili, che espandono la superficie di attacco. Zscaler riduce efficacemente al minimo la superficie di attacco, nascondendo utenti, applicazioni e dispositivi dietro un proxy cloud, facendo in modo non risultino visibili o rilevabili da Internet. In modo analogo a un centralino che instrada le chiamate verso le destinazioni autorizzate, Zscaler collega l'utente o il dispositivo giusto e autorizzato a un'applicazione specifica.

Prevenzione della compromissione iniziale: Zero Trust Exchange impiega l'ispezione TLS/SSL, l'isolamento del browser, il sandboxing avanzato inline e i controlli dell'accesso basati su policy per impedire agli utenti di accedere a siti web dannosi e per rilevare le minacce sconosciute prima che raggiungano la rete. Ciò riduce al minimo il rischio di subire una compromissione.

Eliminazione del movimento laterale: sfruttando la segmentazione da utente ad app o da app ad app, gli utenti si connettono direttamente alle applicazioni (e le app ad altre app), non alla rete, eliminando così il rischio di incorrere al movimento laterale. Centralizzando la gestione delle policy per il controllo dell'accesso, Zscaler agisce da checkpoint di sicurezza per il traffico Internet, eliminando i percorsi che consentono il movimento laterale. Zscaler è inoltre in grado di identificare e impedire ai potenziali aggressori di muoversi lateralmente, siano essi minacce esterne o utenti interni malintenzionati, attraversol'ITDR (Identity Threat Detection and Response) e le funzionalità di deception.

Blocco della perdita dei dati: le misure di prevenzione della perdita dei dati inline, combinate con l'ispezione TLS/SSL completa, contrastano efficacemente i tentativi di furto dei dati. Inoltre, Zscaler assicura che i dati siano sempre protetti, sia quando sono in transito che quando sono inattivi.

COMBATTERE LE MINACCE GUIDATE DALL'IA CON L'IA + L'INNOVAZIONE ZERO TRUST

Queste funzionalità basate sull'IA consentono a Zscaler di offrire una solida protezione contro i ransomware, garantendo una sicurezza completa per le aziende che si trovano a contrastare un panorama di minacce in continua evoluzione:

- ***Il rilevamento di attacchi di phishing e C2 basato sull'IA*** utilizza il rilevamento inline basato sull'IA di Zscaler Secure Web Gateway per identificare e bloccare i siti di phishing e le infrastrutture di comando e controllo (C2) sconosciute.
- ***Il sandboxing basato sull'IA*** offre una prevenzione completa dei malware e delle minacce 0-day, analizzando i file sospetti in un ambiente controllato.
- ***La segmentazione basata sull'IA*** fornisce delle raccomandazioni automatizzate sulle policy di accesso per ridurre al minimo la superficie di attacco e prevenire il movimento laterale, utilizzando fattori come il contesto, il comportamento, la posizione e la telemetria delle app private relativi all'utente.
- ***Una policy dinamica e basata sul rischio*** analizza costantemente il rischio correlato a utenti, dispositivi e applicazioni per applicare delle policy dinamiche di sicurezza e di accesso.
- ***L'isolamento del browser basato sull'IA*** crea un gap sicuro tra gli utenti e i contenuti web dannosi, effettuando il rendering delle pagine sotto forma di immagini pixel, prevenendo così le fughe di dati e la diffusione delle minacce attive.
- ***Il rilevamento e la classificazione dei dati basati sull'IA*** forniscono visibilità istantanea e classificazione immediata dei dati su endpoint, inline e cloud, rendendo più difficile per i ransomware prendere di mira e cifrare i dati sensibili.

Prevenzione olistica contro ogni fase della catena di attacco

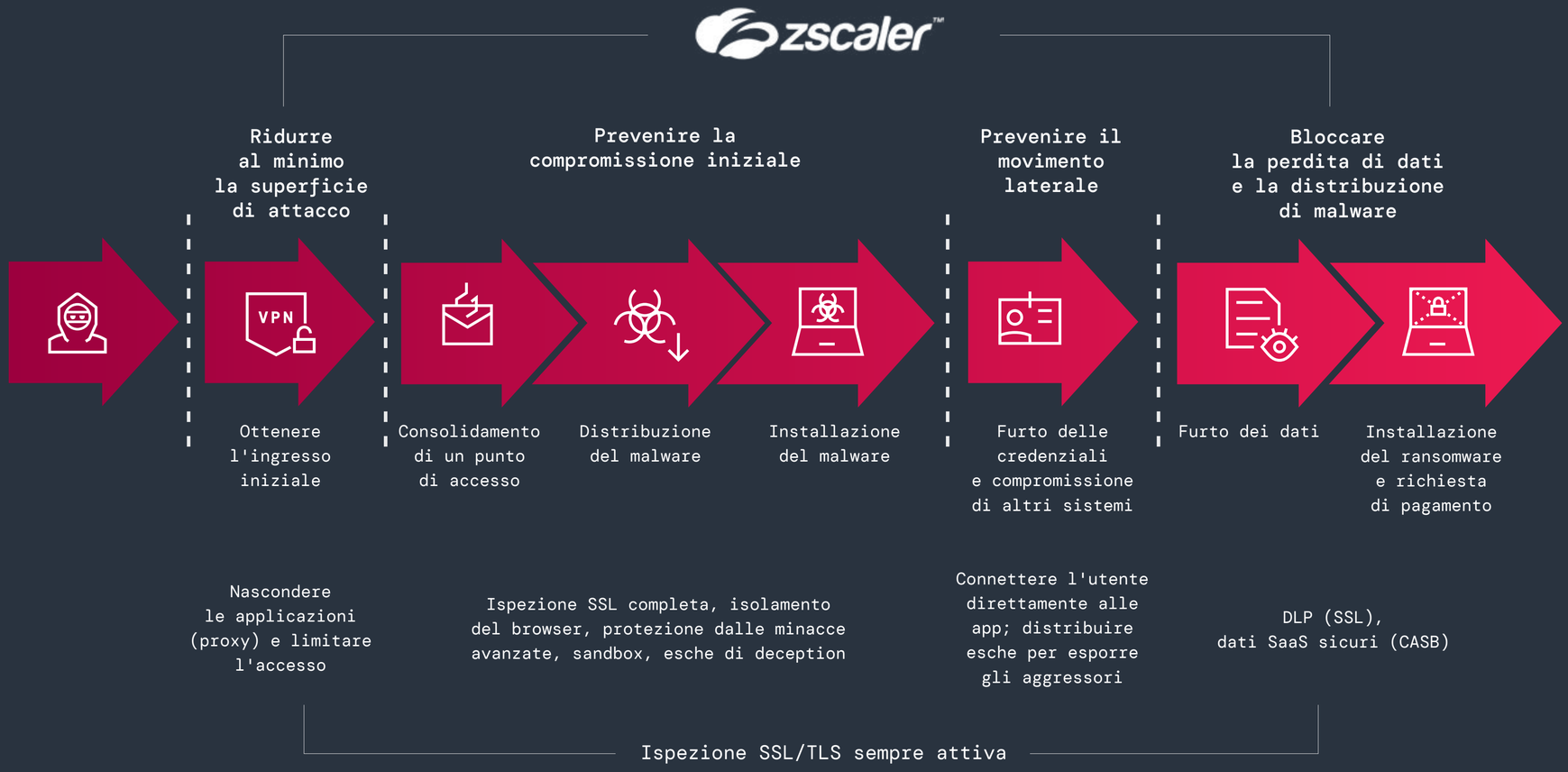


Figura 23: mappa della risposta dell'architettura zero trust alla catena di un attacco ransomware.

Prodotti correlati di Zscaler

Zscaler Internet Access™ (ZIA™) fornisce un accesso sicuro e diretto a Internet, offrendo una protezione inline dalle minacce. Le funzionalità avanzate di prevenzione delle minacce e di sandboxing di ZIA aiutano a contrastare lo scaricamento dei ransomware e le comunicazioni di comando e controllo (C2), prevenendo l'infiltrazione dei ransomware.

Zscaler Private Access™ (ZPA™) consente un accesso sicuro alle applicazioni interne, senza incorrere all'esposizione a Internet, questo grazie all'impiego di un modello zero trust. ZPA garantisce che solo gli utenti e i dispositivi autorizzati possano accedere alle applicazioni critiche, riducendo così la superficie di attacco e prevenendo tentativi di attacco ransomware.

Zscaler Zero Trust Firewall intercetta e ispeziona il traffico TLS/SSL per rilevare i malware nascosti nel traffico cifrato, impedendone l'infiltrazione nella rete.

Zscaler Deception rileva e blocca gli aggressori che tentano di muoversi lateralmente o di accrescere i propri privilegi, attirandoli con server, applicazioni, directory e account utente esca.

Zscaler Sandbox analizza i file e gli eseguibili sospetti in un ambiente virtuale controllato, aiutando a identificare e bloccare il codice dannoso e consentendo alle organizzazioni di essere sempre un passo avanti rispetto ai ransomware basati su file e agli attacchi O-day.

Zscaler Cloud Browser isola le sessioni web e trasmette solo i pixel ai dispositivi, per eliminare in modo efficace il rischio di download drive-by e di exploit O-day che potrebbero essere utilizzati dagli operatori dei ransomware.

Zscaler ITDR (Identity Threat Detection and Response) rileva e difende dagli attacchi diretti alle identità, come il furto delle credenziali, l'abuso dei privilegi, gli attacchi ad Active Directory e le autorizzazioni rischiose.

Zscaler Data Protection fornisce una sicurezza uniforme e unificata per i dati in movimento e inattivi nelle applicazioni SaaS e sul cloud pubblico, riducendo la probabilità di incorrere all'esfiltrazione dei dati e mitigando al tempo stesso il potenziale impatto degli attacchi ransomware.

Guida alla prevenzione dei ransomware

Una strategia di difesa basata su un'architettura zero trust è una misura di sicurezza testata per fermare i ransomware, ma affrontare questa minaccia multiforme richiede una pianificazione proattiva, una collaborazione continua e investimenti strategici.

Gli esperti di ThreatLabz hanno stilato le best practice più recenti per aiutarti a mitigare il rischio di subire attacchi ransomware e salvaguardare l'organizzazione dalle minacce esistenti ed emergenti.

- **Implementa backup periodici e sicuri dei dati.** Assicurati che vengano eseguiti dei backup sicuri e periodici di tutti i dati, inclusi dei backup offline. Inoltre, adatta le strategie di backup in base all'evoluzione delle minacce.
- **Mantieni i software aggiornati.** Applica tempestivamente le patch di sicurezza più recenti per risolvere le vulnerabilità note. Utilizza piattaforme di intelligence sulle minacce basate sull'IA per stabilire le priorità e gestire le patch di sicurezza in modo efficace.
- **Abilita l'autenticazione a più fattori (MFA).** Aggiungi un ulteriore livello di sicurezza agli account utente con l'MFA, per mitigare il rischio di accesso non autorizzato. Inoltre, integra soluzioni MFA per rilevare e prevenire efficacemente le violazioni degli account.
- **Definisci una policy di sicurezza informatica coerente a livello aziendale.** Assicurati che tutti gli utenti seguano delle procedure di sicurezza coerenti, che includono MFA e aggiornamenti periodici di sicurezza, per aiutare a prevenire le compromissioni iniziali. In presenza di una forza lavoro distribuita, risulta ancora più importante implementare un'architettura SSE (Security Service Edge) per proteggere gli utenti ovunque si trovino.
- **Rafforza la sicurezza delle applicazioni.** Rimuovi le applicazioni dalla rete Internet pubblica per impedire agli autori dei ransomware di sfruttarne le vulnerabilità. Inoltre, implementa un'architettura zero trust per le applicazioni interne per proteggerle dai tentativi di attacco ransomware.
- **Implementa l'accesso a privilegi minimi.** Implementa policy basate sul principio dei privilegi minimi per limitare l'accesso degli utenti solo alle risorse necessarie per i loro ruoli. Utilizza soluzioni basate sull'IA per analizzare dinamicamente il comportamento degli utenti e adattare di conseguenza i privilegi di accesso.
- **Rafforza la protezione delle identità.** Utilizza degli strumenti di ITDR per ottenere la massima visibilità sugli errori di configurazione delle identità, correggere le vulnerabilità in Active Directory, sfruttate dagli aggressori per accrescere i privilegi e muoversi lateralmente, e rilevare le minacce nascoste dirette alle identità.
- **Ispeziona tutto il traffico.** Attualmente, l'86% delle minacce viene trasmesso tramite i canali cifrati, che spesso non vengono ispezionati, consentendo anche agli aggressori moderatamente sofisticati di aggirare con facilità i controlli di sicurezza. È pertanto essenziale ispezionare tutto il traffico, cifrato o meno, per evitare le compromissioni.
- **Implementa lo ZTNA (Zero Trust Network Access).** Distribuisci la segmentazione granulare da utente ad applicazione e da applicazione ad applicazione, intermediando l'accesso tramite controlli dell'accesso con privilegi minimi, per eliminare il movimento laterale, ridurre al minimo l'esposizione dei dati e migliorare il tuo profilo di sicurezza generale.

- **Utilizza l'isolamento del browser basato sull'IA.** Proteggi gli utenti dalle minacce web con l'isolamento basato sull'IA dei contenuti Internet sospetti e degli utenti ad alto rischio. Isolando l'esperienza del browser e limitando le azioni potenzialmente dannose (come l'inserimento delle credenziali), gli utenti possono accedere in modo sicuro a URL e file sospetti, senza mettere a rischio la sicurezza del proprio sistema.
- **Utilizza il sandboxing avanzato basato sull'IA.** Blocca i malware elusivi e mai visti prima con una sandbox in grado di rilevare e mettere in quarantena in automatico le minacce sconosciute e i file sospetti, sfruttando l'analisi basata su IA/ML.
- **Implementa la prevenzione della perdita dei dati inline (DLP).** Proteggiti dall'esfiltrazione e dall'esposizione dei dati implementando misure di DLP inline.
- **Sfrutta la tecnologia di deception.** Utilizza strumenti di deception e honeypot per ingannare gli aggressori e dirottarli, rafforzando così le tue difese e impedendo l'infiltrazione nel sistema.
- **Utilizza un CASB (Cloud Access Security Broker).** Controlla e monitora l'utilizzo delle applicazioni cloud con un CASB per prevenire le attività dannose, come lo scaricamento dei file e l'esfiltrazione di dati.
- **Fornisci una formazione continua ai dipendenti.** Organizza periodicamente dei corsi per accrescere la sensibilizzazione sul tema della sicurezza informatica e istruire i dipendenti sulle minacce ransomware. Utilizza delle simulazioni di scenari ransomware reali per migliorare la preparazione dei dipendenti.
- **Sviluppa un piano completo di risposta ai ransomware.** Delinea un piano di risposta che comprenda il recupero dei dati, la risposta agli incidenti e i protocolli di comunicazione per agire in modo rapido ed efficace in caso di attacco ransomware.

Segui gli approfondimenti di Zscaler ThreatLabz per ricevere aggiornamenti periodici sulle minacce informatiche e sugli sviluppi più recenti, inclusi gli indicatori di compromissione (IOC) pubblicati e le mappature di MITRE ATT&CK. Queste informazioni possono essere utilizzate per istruire i team, migliorare il profilo di sicurezza e contribuire a prevenire gli attacchi ransomware.

ThreatLabz gestisce inoltre un repository su GitHub che include IOC, strumenti (tra cui gli strumenti di decrittazione ransomware proof-of-concept) e un archivio delle richieste di riscatto di tutti i principali gruppi ransomware.

X @ThreatLabz | Blog delle attività di ricerca sulla sicurezza di ThreatLabz

Metodologia del report

La metodologia di ricerca impiagata in questo report è caratterizzata da un processo completo che ha attinto da diverse fonti di dati per identificare e monitorare le tendenze dei ransomware. Il team che ha lavorato al report ha raccolto i dati da una varietà di fonti tra aprile 2023 e marzo 2024, tra cui:

- **Il security cloud globale di Zscaler,** che elabora più di 500 trilioni di segnali ogni giorno, blocca oltre 9 miliardi di minacce e violazioni delle policy al giorno e fornisce oltre 250.000 aggiornamenti di sicurezza al giorno ai clienti di Zscaler. Abbiamo analizzato questi dati, che includono informazioni sugli indirizzi IP di origine, gli indirizzi IP di destinazione e i tipi di file associati agli attacchi ransomware, per identificare l'attività dei ransomware.

- **Fonti di intelligence esterne.** Abbiamo inoltre raccolto dati da fonti di intelligence esterne, come feed di intelligence sulle minacce, ricerche open source e rapporti delle forze dell'ordine, che hanno contribuito a fornire informazioni aggiuntive sugli aggressori che sfruttano i ransomware, sui loro obiettivi e sui loro metodi.

- **L'analisi del team di ThreatLabz condotta sui campioni di ransomware e i dati sugli attacchi.** Il team di Threat Intelligence di ThreatLabz tiene traccia delle famiglie di ransomware su larga scala attraverso il reverse engineering e l'automazione dell'analisi dei malware per sviluppare strategie di risposta efficaci. ThreatLabz lavora inoltre a stretto contatto con le forze dell'ordine a livello internazionale e ha svolto un ruolo significativo in azioni recenti, tra cui l'operazione Duck Hunt e l'operazione Endgame.

Informazioni su ThreatLabz

ThreatLabz è il team di ricerca sulla sicurezza di Zscaler. Questo team di esperti 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 sui malware e all'analisi del loro comportamento, i membri del team si occupano delle attività di ricerca e sviluppo di nuovi prototipi per la protezione contro le minacce avanzate sulla piattaforma Zscaler. Inoltre, 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.com**.

Informazioni su Zscaler

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

Experience your world, secured.™