Presentato da

Trellix ADVANCED RESEARCH CENTER

REPORT SULLE MINACCE

Febbraio 2023

INDICE DEI CONTENUTI

PANORAMICA SULLE MINACCE DEL 4° TRIMESTRE 2022

I criminali informatici si sono confermati avversari temibili durante gli ultimi mesi del 2022. Trellix Advanced Research Center ha risposto integrando ancora più risorse di intelligence sulle minacce al nostro team di centinaia di analisti e ricercatori esperti in sicurezza.

"Abbiamo ottimizzato la nostra intelligence sulle minacce. Elimina lo stress dei team SecOps con una sicurezza più semplice. Rafforza il tuo livello di sicurezza sicurezza con la massima tranquillità. Le minacce continuano a evolversi. Fai lo stesso."

Questo report prende in esame i criminali informatici, le famiglie di minacce, campagne e tecniche che hanno dominato nel corso dell'ultimo trimestre. E non è tutto. Abbiamo anche ampliato le nostre fonti per raccogliere dati provenienti dai siti di divulgazione dei ransomware e dai vari report pubblicati dal settore della sicurezza. L'aumento delle risorse di Trellix si traduce in nuove categorie di informazioni sulle minacce, tra cui contenuti sulla sicurezza di rete, sugli incidenti cloud, sugli incidenti relativi agli endpoint e sulle operazioni di sicurezza.

Dal nostro ultimo report sulle minacce, il Trellix Advanced Research Center ha condotto ricerche e osservazioni in tutto il mondo. In particolare il nostro team ha messo in luce il collegamento tra Gamaredon e l'aumento degli attacchi informatici che hanno preso di mira l'Ucraina nel quarto trimestre, corretto 61.000 progetti open source vulnerabili e pubblicato le sue previsioni sulle minacce per il 2023.

La panoramica seguente illustra l'ampia varietà di informazioni raccolta dal Trellix Advanced Research Center per supportare i clienti e il settore della sicurezza nella lotta contro le minacce:

Ransomware

- LockBit 3.0 è stato il gruppo di ransomware più attivo nel quarto trimestre.
- Il ransomware ha continuato a diffondersi in tutto il mondo, specialmente negli Stati Uniti.
- Il ransomware ha preso di mira settori come i beni e i servizi industriali.

Attacchi Nation-State

- Questi attacchi hanno preso di mira settori come quello della pubblica amministrazione e dei trasporti e della logistica.
- Le aziende con sede negli Stati Uniti sono state le più colpite.

Sfruttamento delle risorse locali (LOLBIN)

- La metodologia di ricerca di Trellix Advanced Research Center ha fornito indicazioni sull'uso di Cobalt Strike in ambienti reali.
- Un numero elevato di server Cobalt Strike è ospitato presso fornitori di cloud cinesi.
- Windows Command Shell rappresenta quasi la metà dei 10 principali file binari di sistemi operativi più diffusi utilizzati nelle campagne identificate.

Criminali informatici

- Cina, Corea del Nord e Russia sono in cima all'elenco dei paesi d'origine dei criminali informatici.

Tendenze in materia di sicurezza dell'email

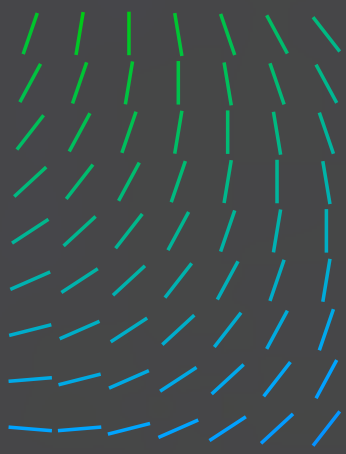
- Forte crescita del volume di email dannose nei Paesi arabi durante la Coppa del mondo di calcio
- Informazioni sulle campagne di phishing e vishing, incluse le tecniche di furto d'identità e i principali temi utilizzati dal vishing

Sicurezza della rete

- Attacchi, Webshell, strumenti e tecniche più efficaci, significativi e rilevanti del trimestre

Dati di telemetria sulle operazioni di sicurezza raccolti da Trellix XDR

- Avvisi di sicurezza, exploit, fonti di registri e tecniche MITRE ATT&CK prevalenti
- Incidenti cloud
- Tecniche e rilevamenti per Azure, AWS e GCP
- Principali tecniche e rilevamenti



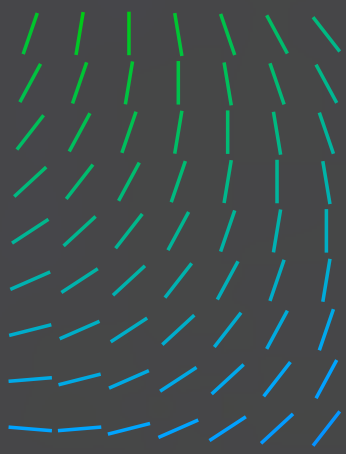
LETTERA DEL NOSTRO DIRETTORE DELL'INTELLIGENCE SULLE MINACCE

Il team Trellix Advanced Research Center è lieto di condividere i primi dati del report sulle minacce del 4° trimestre del 2022. Questo report combina nuovi dati provenienti dalla nostro serie di sensori di prodotto con le informazioni provenienti da altre fonti, come i siti di divulgazione del ransomware e il nostro monitoraggio delle infrastrutture in ambienti reali. In Trellix rimaniamo impegnati a proteggere i nostri clienti dalle minacce poste da criminali informatici tenaci e motivati, che si reinventano continuamente. In un contesto geopolitico ed economico complesso e di grande incertezza, un'intelligence sulle minacce globale è sempre più fondamentale.

A livello globale, l'incertezza economica generata dalla guerra in Ucraina ha portato al più elevato aumento dei prezzi dell'energia dagli anni '70, che sta avendo un pesante impatto sull'economia mondiale. Il ritorno della guerra in Europa è servito anche come campanello d'allarme per coloro che mettevano in discussione l'approccio dell'UE alla sicurezza e alla difesa e la sua capacità di difendere i propri interessi, in particolare nel cyberspazio. Negli Stati Uniti, invece i governi hanno riconosciuto la necessità di rispondere alla competizione geostrategica, di proteggere le infrastrutture critiche e di combattere la manipolazione delle informazioni e l'interferenza da parte di potenze straniere. La violazione SolarWinds, l'attacco Hafnium, la guerra in Ucraina e altri eventi hanno spinto l'amministrazione e il Congresso degli Stati Uniti ad agire in modo bipartisan su nuovi standard di sicurezza e politiche di finanziamento della sicurezza che si basano fortemente sugli impegni della nazione e sul lavoro delle amministrazioni precedenti. Qual è quindi l'impatto di questa incertezza sulla sicurezza informatica delle nostre aziende, delle nostre istituzioni pubbliche e private e dei nostri valori democratici?

Nell'ultimo trimestre, il nostro team ha osservato l'uso attivo di attacchi informatici a fini di spionaggio, guerra informatica e disinformazione al servizio di ambizioni politiche, economiche e territoriali. La guerra in Ucraina ha portato anche all'emergere di nuove forme di attacchi informatici e gli attivisti informatici sono diventati più abili e audaci nelle loro azioni: danneggiamento di siti web, divulgazione di informazioni e attacchi DDoS. Nel frattempo, le forme tradizionali di attacchi informatici continuano. Gli schemi di social engineering per ingannare e manipolare le persone e indurle a divulgare informazioni riservate o personali, come il phishing, rimangono prevalenti.

Il ransomware ha continuato ad affliggere molte aziende in tutto il mondo. Proprio come abbiamo osservato durante la pandemia di COVID 19, i criminali informatici cercano di trarre profitto da questo momento di crisi ed incertezza. La nostra attività di ricerca segue l'evoluzione del panorama delle minacce. Rimaniamo focalizzati sul



miglioramento costante dell'efficacia dei nostri prodotti e sul fornire informazioni utili ai nostri interlocutori, in modo che possano proteggere le loro risorse più preziose. In questo report, scoprirai l'importanza del nostro lavoro per tutti i membri del Trellix Advanced Research Center. I nostri ricercatori ed esperti affrontano ogni singolo progetto con motivazione e passione.

Sentiti libero di condividere con noi le tue opinioni su questo report dettagliato. Se desideri che il nostro team si addentrasse su temi specifici, contatta me o il nostro team @TrellixARC su Twitter. Ci auguriamo di incontrarti all'evento RSA che si terrà a San Francisco in aprile.

John Fokker
Direttore dell'intelligence sulle minacce

METODOLOGIA

I sistemi principali di Trellix forniscono i dati di telemetria che utilizziamo per preparare i nostri report trimestrali sul panorama delle minacce. Combiniamo i nostri dati di telemetria con quelli di varie fonti di dati pubbliche, nonché le nostre indagini sulle minacce prevalenti come ransomware, campagne di gruppi statali, ecc.

Per telemetria intendiamo i dati relativi ai rilevamenti, non alle infezioni. Un rilevamento viene registrato quando un file, URL, indirizzo IP o altri indicatori viene rilevato da uno dei nostri prodotti e ci viene poi segnalato.

Per esempio, sappiamo che un numero crescente di aziende utilizza strutture di test dell'efficacia che distribuiscono campioni di malware reali. Questo utilizzo apparirà come un rilevamento, ma non si tratta assolutamente di un'infezione.

Il processo di analisi e filtraggio dei falsi positivi nei dati di telemetria è in costante sviluppo, il che può portare all'apparizione di nuove categorie di minacce rispetto alle edizioni precedenti.

Verranno inoltre aggiunte nuove categorie di minacce man mano che altri team di Trellix contribuiscono a questo report trimestrale.

La riservatezza delle informazioni dei nostri clienti è essenziale. Viene rispettata durante la raccolta dei dati di telemetria e la loro mappatura in base ai settori e ai paesi dei nostri clienti. Poiché la nostra base di clienti varia in base al paese, le evoluzioni vengono analizzate in modo approfondito per identificare i fattori che entrano in gioco. A titolo d'esempio, il settore delle telecomunicazioni spesso mostra punteggi elevati. Ciò non significa necessariamente che questo settore sia preso

di mira in modo particolare. Il settore delle telecomunicazioni include anche ISP che possiedono uno spazio di indirizzi IP che viene venduto alle aziende. Cosa significa? Gli invii provenienti dallo spazio degli indirizzi IP dell'ISP sono attribuiti al settore delle telecomunicazioni, ma in realtà possono provenire dai suoi clienti, che operano in un altro settore.

RANSOMWARE: 4° TRIMESTRE 2022

Questa sezione raggruppa le informazioni che abbiamo raccolto sull'attività dei gruppi di ransomware. Queste informazioni provengono da più fonti e ci permettono di avere un quadro più completo del panorama delle minacce, di ridurre gli errori nell'osservazione e di stabilire la famiglia di ransomware più significativa nel 4° trimestre del 2022. La prima fonte è quantitativa e illustra le statistiche delle campagne ransomware derivate dalla correlazione degli indicatori di compromissione (IOC) del ransomware e dei dati di telemetria dei clienti Trellix. La seconda fonte è qualitativa e mostra l'analisi dei vari report pubblicati dal settore della sicurezza, vagliati e convalidati dal gruppo di Intelligence sulle minacce. Infine, la terza fonte è una nuova categoria che riunisce le informazioni sulle vittime di ransomware provenienti dai vari "siti di divulgazione" (leak sites) dei gruppi di autori di ransomware; tali informazioni vengono normalizzate, arricchite e infine analizzate per fornire una versione anonimizzata dei risultati.

Fornendo questi diversi punti di vista, speriamo di fornirti le chiavi di lettura dell'attuale panorama delle minacce. Nessuno di essi è sufficiente, perché ciascuno ha i propri limiti. Nessuno ha accesso a tutti i registri di tutti i sistemi connessi a Internet, non tutti gli incidenti di sicurezza vengono segnalati e non tutte le vittime vengono ricattate e pubblicati sui siti di divulgazione. Tuttavia, la combinazione dei diversi punti di vista può portare a una migliore comprensione del panorama delle minacce, riducendo al contempo i nostri punti ciechi.

Una combinazione di dati quantitativi e qualitativi provenienti da diverse fonti ci permette di formulare un giudizio informato, tenendo conto dei potenziali inconvenienti e punti ciechi.

Notizie sul ransomware: 4° trimestre 2022

Gruppo ransomware con il maggior impatto nel 4° trimestre: LockBit 3.0

Grazie alle osservazioni delle varie fonti Trellix, possiamo concludere che LockBit 3.0 è stato il gruppo ransomware con il maggior impatto nel 4° trimestre 2022. La reputazione di LockBit 3.0 si basa sulle seguenti caratteristiche:

3° LockBit 3.0 si è classificato al terzo posto tra i gruppi di ransomware più diffusi nel trimestre, secondo l'analisi dei dati di telemetria dei ransomware raccolti dai sensori Trellix distribuiti in tutto il mondo.

2° LockBit 3.0 è stato il secondo gruppo di ransomware più segnalato dal settore della sicurezza insieme a Cuba, in base alle analisi delle diverse campagne identificate dal gruppo di Intelligence sulle minacce.

1° Il sito di divulgazione di LockBit 3.0 ha riportato il maggior numero di vittime tra i gruppi ransomware nel trimestre. Questo rende LockBit il più propenso a usare la divulgazione pubblica come leva.

Ecco altre categorie e osservazioni relative a LockBit nel 4° trimestre 2022:

SETTORI COLPITI DA LOCKBIT 3.0: 4° TRIMESTRE 2022

29%

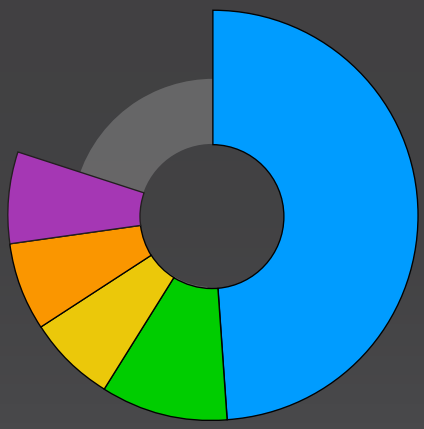
Secondo il sito di divulgazione di LockBit 3.0, il settore dei beni e servizi industriali è stato il più colpito da LockBit 3.0 nel 4° trimestre del 2022.

- Beni e servizi industriali
- Retail
- Tecnologia
- Sanità
- Costruzioni e materiali
- Beni personali e domestici
- Pubblica Amministrazione

PAESI DELLE AZIENDE COLPITE DA LOCKBIT 3.0: 4° TRIMESTRE 2022

49%

Secondo il sito di divulgazione di LockBit 3.0, le aziende statunitensi sono state le più colpite (49%) da LockBit 3.0 nel 4° trimestre 2022, seguite dalle aziende britanniche.



- Stati Uniti
- Regno Unito
- Canada
- Francia
- Brasile

Strumenti ed exploit LockBit 3.0

VULNERABILITÀ NOTE PER ESSERE SFRUTTATE DA LOCKBIT 3.0

CVE-2018-13379
CVE-2020-0787
CVE-2021-20028
CVE-2021-34473
CVE-2021-34523

STRUMENTI DANNOSI UTILIZZATI DA LOCKBIT 3.0

Amadey	Hakops
Blister	Neshta
BloodHound	SocGholish
Cobalt Strike	StealBit
Grabff	WinPEAS

STRUMENTI NON DANNOSI UTILIZZATI DA LOCKBIT 3.0

BCDEdit	MiniDump	NSIS	Schtasks.exe
Cmd	MpCmdRun.exe	PCHunter	VSSAdmin
Fltmc.exe	Mshta	PowerShell	wevtutil
Fsutil	Mstsc	Process Monitor	WMIC
GMER	Netsh	Rundll32	RCLONE
MEGASYNC	Nltest		

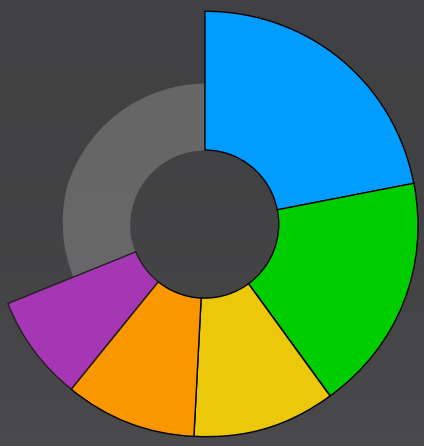
Il ransomware attraverso le lenti dei nostri dati di telemetria

Le seguenti statistiche si basano sulle correlazioni tra i nostri dati di telemetria e la nostra base di conoscenze di intelligence sulle minacce. Dopo una fase di analisi, identifichiamo una serie di campagne a partire dai dati raccolti nel periodo di tempo selezionato e ricaviamo le loro caratteristiche. Le statistiche visualizzate sono quelle delle campagne, non dei rilevamenti stessi. I nostri dati di telemetria globali hanno mostrato indicatori di compromissione (IOC) che appartengono a diverse campagne lanciate da vari gruppi di criminali informatici. Le seguenti famiglie di ransomware, con i rispettivi strumenti e tecniche, rappresentano le più diffuse nelle campagne identificate. Allo stesso modo, i paesi e i settori che seguono rappresentano i più colpiti dalle campagne identificate.

FAMIGLIE DI RANSOMWARE PIÙ DIFFUSE: 4° TRIMESTRE 2022

22%

Cuba è stata la famiglia di ransomware più diffusa nel 4° trimestre 2022 Zeppelin è stato spesso utilizzato da Vice Society. Scopri di più sulle fuoriuscite di comunicazioni di Yanluowang.



- Cuba
- Hive
- LockBit
- Zeppelin
- Yanluowang

STRUMENTI DANNOSI PIÙ DIFFUSI UTILIZZATI DAI GRUPPI RANSOMWARE: 4° TRIMESTRE 2022

41%

Cobalt Strike è stato lo strumento dannoso più diffuso utilizzato dai gruppi ransomware nel 4° trimestre 2022.

1.	Cobalt Strike	41%
2.	Mimikatz	23%
3.	BURNTCIGAR	13%
4.	VMProtect	12%
5.	POORTRY	11%

TECNICHE MITRE-ATT&CK PIÙ UTILIZZATE DAI GRUPPI RANSOMWARE: 4° TRIMESTRE 2022

1.	Crittografia dei dati per l'impatto	17%
2.	Rilevamento delle informazioni di sistema	11%
3.	PowerShell	10%
4.	Trasferimento di strumenti all'ingresso	10%
5.	Windows Command Shell	9%

STRUMENTI NON DANNOSI PIÙ DIFFUSI UTILIZZATI DAI GRUPPI RANSOMWARE: 4° TRIMESTRE 2022

21%

CMD è stato lo strumento non dannoso più diffuso utilizzato dai gruppi ransomware nel 4° trimestre 2022.

1.	Cmd	21%
2.	PowerShell	14%
3.	Net	10%
4.	Reg	8%
5.	PsExec	8%

PAESI PIÙ COLPITI DAI GRUPPI DI RANSOMWARE: 4° TRIMESTRE 2022

29%

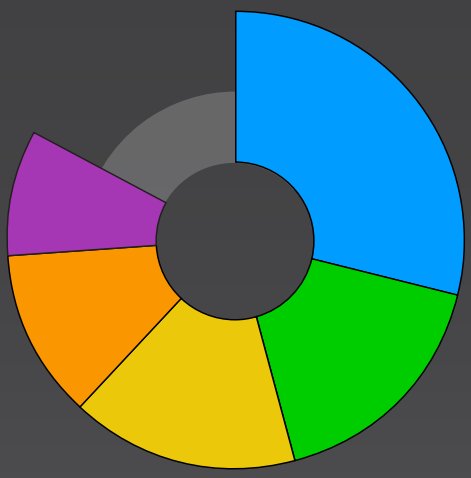
Gli Stati Uniti sono stati il paese più colpito dai gruppi ransomware nel 4° trimestre 2022 in base ai dati di telemetria di Trellix.

- Stati Uniti
- Cina
- Qatar
- Giappone
- Indonesia

SETTORI PIÙ COLPITI DAI GRUPPI RANSOMWARE: 4° TRIMESTRE 2022

29%

Esternalizzazione e hosting sono stati i settori più colpiti dai gruppi ransomware nel 4° trimestre 2022 in base ai dati di telemetria di Trellix. Questo dato è in linea con le dimensioni medie delle aziende delle vittime elencate nei siti di divulgazione di ransomware. Queste aziende spesso non hanno un proprio blocco IP assegnato e si affidano a fornitori di servizi in hosting terzi.



- Esternalizzazione e hosting
- Banche/Finanza/ Gestione patrimoniale
- Pubblica Amministrazione
- Vendita all'ingrosso
- Farmaceutico

Ransomware identificati dal settore della sicurezza

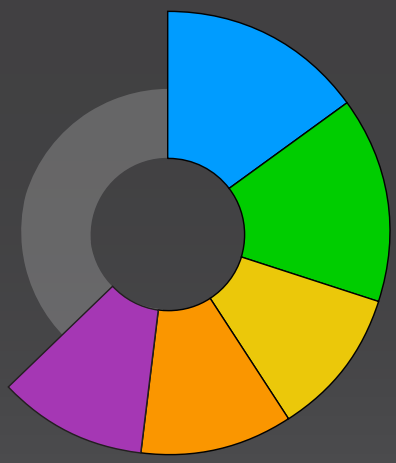
Le seguenti statistiche si basano su report pubblici e su ricerche interne. Si noti che non tutti gli incidenti ransomware vengono segnalati. Molte famiglie di ransomware sono attive da tempo e, naturalmente, sono meno degne di nota rispetto alle nuove famiglie nel corso di trimestri specifici. Sulla base di questi criteri, tali metriche sono un indicatore delle famiglie di ransomware che il settore della sicurezza ritiene più impattanti e rilevanti nel trimestre.

FAMIGLIE DI RANSOMWARE PIÙ SEGNALATE: 4° TRIMESTRE 2022

15%

In base ai report pubblicati dal settore della sicurezza, le famiglie di ransomware Black Basta e Magniber sono state le più segnalate nel 4° trimestre 2022.

- Black Basta
- Magniber
- Cuba
- LockBit
- Quantum



PRINCIPALI TECNICHE DI ATTACCO DELLE FAMIGLIE DI RANSOMWARE: 4° TRIMESTRE 2022

19%

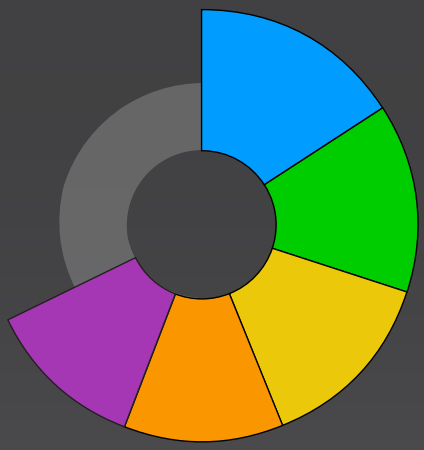
Secondo i report pubblicati dal settore della sicurezza, la crittografia dei dati per impatto è stata la tecnica di attacco più utilizzata dalle famiglie ransomware nel 4° trimestre del 2022.

1.	Crittografia dei dati per l'impatto	19%
2.	Windows Command Shell	11%
3.	Rilevamento delle informazioni di sistema	10%
4.	Trasferimento di strumenti all'ingresso	10%
5.	PowerShell	10%

PRINCIPALI SETTORI COLPITI DALLE FAMIGLIE DI RANSOMWARE: 4° TRIMESTRE 2022

16%

In base ai report pubblicati dal settore della sicurezza, il settore della sanità è stato il più colpito dalle famiglie di ransomware nel 4° trimestre 2022.



- Sanità
- Finanza
- Pubblica Amministrazione
- Industria manifatturiera
- Trasporto

PAESI PIÙ COLPITI PER FAMIGLIA DI RANSOMWARE: 4° TRIMESTRE 2022

19%

In base ai report pubblicati dal settore della sicurezza, gli Stati Uniti sono stati il paese più colpito dalle famiglie di ransomware nel 4° trimestre 2022.

- Stati Uniti
- Germania
- Brasile
- Argentina
- Canada
- India
- Paesi Bassi
- Corea del Sud
- Svizzera
- Regno Unito

CVE UTILIZZATI DALLE FAMIGLIE DI RANSOMWARE: 4° TRIMESTRE 2022

1.	CVE-2021-31207	16%
	CVE-2021-34474	16%
	CVE-2021-34523	16%
2.	CVE-2021-34527	13%
3.	CVE-2021-26855	9%
	CVE-2021-27065	9%

STRUMENTI DANNOSI UTILIZZATI DALLE FAMIGLIE DI RANSOMWARE: 4° TRIMESTRE 2022

44%

In base ai report pubblicati dal settore della sicurezza, Cobalt Strike è stato lo strumento dannoso più usato dalle famiglie di ransomware segnalate nel 4° trimestre 2022.

1.	Cobalt Strike	44%
2.	QakBot	13%
3.	IcedID	9%
4.	BURNTCIGAR	7%
5.	Carbanak SystemBC	7% 7%

STRUMENTI NON DANNOSI UTILIZZATI DALLE FAMIGLIE DI RANSOMWARE: 4° TRIMESTRE 2022

21%

In base ai report pubblicati dal settore della sicurezza, PowerShell è stato lo strumento non dannoso più utilizzato dalle famiglie di ransomware segnalate nel 4° trimestre 2022.

1.	PowerShell	21%
2.	Cmd	18%
3.	Rundll32	11%
4.	VSSAdmin	10%
5.	WMIC	9%

Vittime elencate nei "siti di divulgazione" del ransomware: 4° trimestre 2022

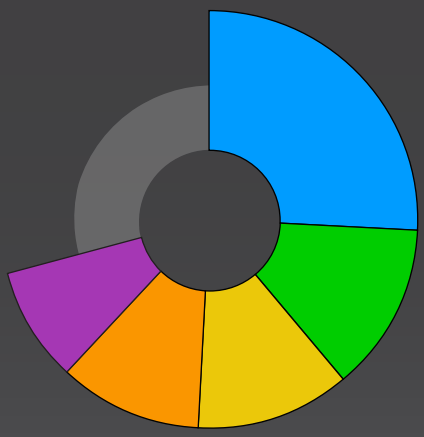
I dati presenti in questa sezione sono stati compilati esaminando i l"siti di divulgazione" (leak sites) dei diversi gruppi ransomware. Tali gruppi ricattano le loro vittime pubblicando informazioni su di loro su questi siti web. Quando le trattative si arenano o le vittime si rifiutano di pagare il riscatto entro la scadenza fissata, il gruppo ransomware fa trapelare le informazioni sottratte. Utilizziamo lo strumento open source RansomLook per raccogliere le varie divulgazioni e poi elaboriamo internamente i dati per normalizzare e arricchire i risultati e fornire una versione anonimizzata dell'analisi della vittimologia.

È importante sottolineare che non tutte le vittime vengono segnalate sui rispettivi siti di divulgazione. Molte vittime pagano il riscatto e non vengono conteggiate. Queste metriche sono un indicatore delle vittime che i gruppi ransomware hanno ricattato e non devono essere confuse con il numero complessivo di vittime.

GRUPPI DI RANSOMWARE CON IL MAGGIOR NUMERO DI VITTIME: 4° TRIMESTRE 2022

26%

LockBit 3.0 rappresenta il 26% dei 10 principali gruppi di ransomware che hanno riportato il maggior numero di vittime sui rispettivi siti di divulgazione nel 4° trimestre del 2022.

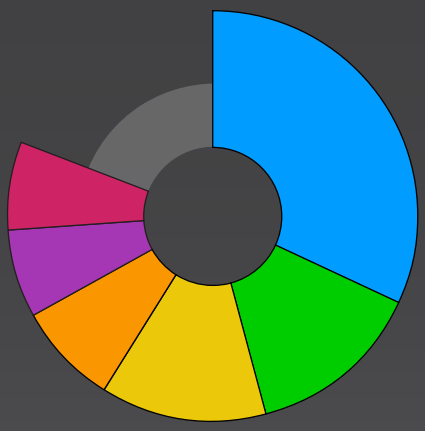


- LockBit 3.0
- ALPHV
- Royal
- Black Basta
- Cuba

SETTORI COLPITI DAI GRUPPI DI RANSOMWARE IN BASE AI LORO SITI DI DIVULGAZIONE: 4° TRIMESTRE 2022

32%

Il settore dei beni e servizi industriali è stato il più colpito dai gruppi di ransomware secondo i loro siti di divulgazione nel 4° trimestre del 2022. I beni e servizi industriali comprendono tutti i prodotti materiali e i servizi intangibili utilizzati principalmente per la costruzione e la produzione.

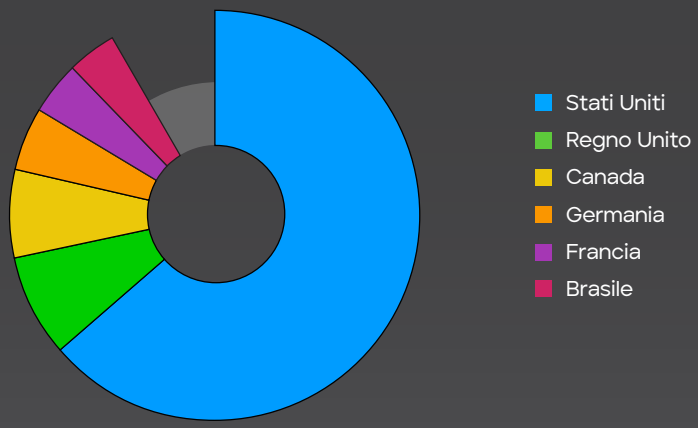


- Beni e servizi industriali
- Retail
- Tecnologia
- Costruzioni e materiali
- Sanità
- Pubblica Amministrazione

PAESI DELLE AZIENDE COLPITE DAI GRUPPI DI RANSOMWARE IN BASE AI LORO SITI DI DIVULGAZIONE: 4° TRIMESTRE 2022

63%

delle prime 10 aziende segnalate da diversi gruppi di ransomware nei rispettivi siti di divulgazione nel 4° trimestre del 2022 avevano sede negli Stati Uniti, seguiti da Regno Unito (8%) e Canada (7%).



STATISTICHE SUGLI ATTACCHI NATION-STATE: 4° TRIMESTRE 2022

Questa sezione presente le informazioni che abbiamo raccolto sull'attività dei gruppi Nation-State. Queste informazioni sono raccolte da più fonti per creare un quadro più completo del panorama delle minacce e ridurre gli errori di osservazione. In primo luogo, utilizziamo le statistiche estratte dalla correlazione tra gli indicatori di compromissione (IOC) dei gruppi Nation-State e i dati di telemetria dei clienti di Trellix. In secondo luogo, forniamo informazioni tratte da vari rapporti pubblicati dal settore della sicurezza, vagliati e convalidati dal gruppo di Intelligence sulle minacce.

Novità degli attacchi Nation-State: 4° trimestre 2022

- Stati Uniti e Germania hanno registrato un aumento significativo del numero di attacchi Nation-State.
- Cina e Vietnam entrano nella classifica dei paesi più colpiti da questo tipo di attacchi nel 4° trimestre.

Statistiche sugli attacchi Nation-State attraverso le lenti dei nostri dati di telemetria a livello globale

Queste statistiche si basano sulle correlazioni tra i nostri dati di telemetria e la nostra base di conoscenze di intelligence sulle minacce. Dopo una fase di analisi, identifichiamo una serie di campagne a partire dai dati raccolti nel periodo di tempo selezionato e ricaviamo

le loro caratteristiche. Le statistiche visualizzate sono quelle delle campagne, non dei rilevamenti stessi. A causa dell'aggregazione di vari registri, dell'uso da parte dei nostri clienti di framework di simulazione delle minacce e di correlazioni di alto livello con la base di conoscenza di intelligence sulle minacce, i dati vengono filtrati manualmente per soddisfare i criteri desiderati.

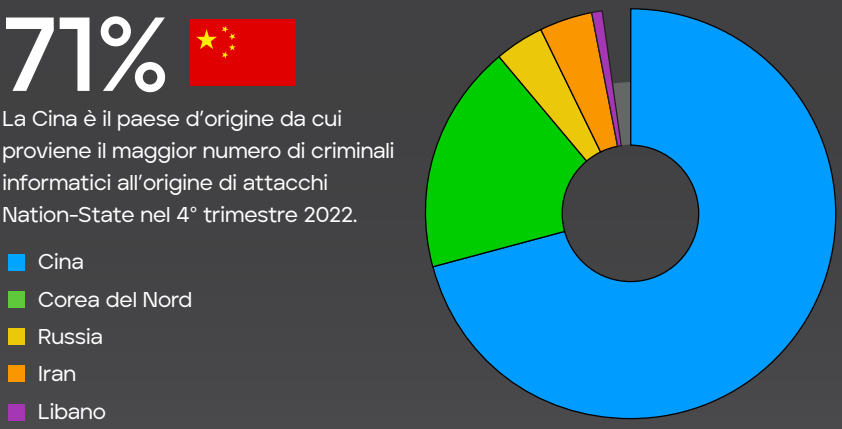
I nostri dati di telemetria globale hanno mostrato indicatori di compromissione (IOC) appartenenti a diverse campagne lanciate da gruppi APT. I seguenti paesi e criminali informatici, insieme ai loro strumenti e alle loro tecniche, rappresentano i più diffusi nelle campagne identificate. Analogamente, i dati relativi ai paesi e ai settori rappresentano i più colpiti dalle campagne identificate.

Dati di telemetria sugli attacchi Nation-State

PAESI D'ORIGINE PIÙ PREVALENTI DEI CRIMINALI INFORMATICI COINVOLTI IN ATTACCHI NATION-STATE: 4° TRIMESTRE 2022

71%

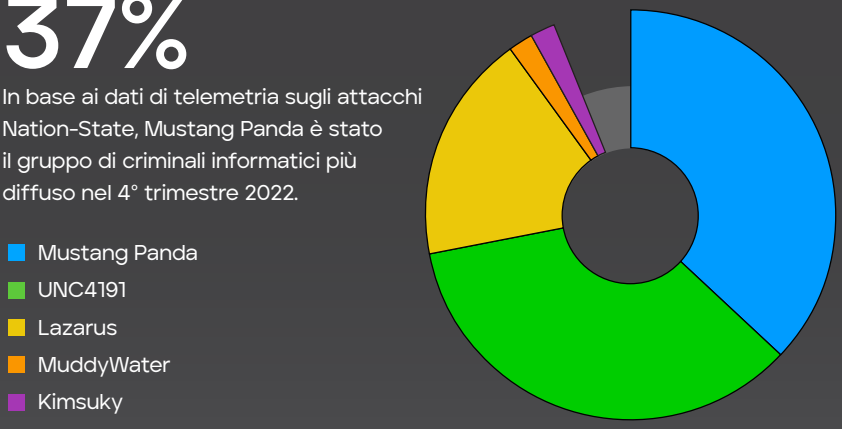
La Cina è il paese d'origine da cui proviene il maggior numero di criminali informatici all'origine di attacchi Nation-State nel 4° trimestre 2022.



GRUPPI DI CRIMINALI INFORMATICI PIÙ DIFFUSI: 4° TRIMESTRE 2022

37%

In base ai dati di telemetria sugli attacchi Nation-State, Mustang Panda è stato il gruppo di criminali informatici più diffuso nel 4° trimestre 2022.



TECNICHE MITRE ATT&CK PIÙ DIFFUSE UTILIZZATE NEGLI ATTACCHI NATION-STATE: 4° TRIMESTRE 2022

1.	DLL side loading	14%
2.	Rundll32	13%
3.	Offuscamento di file o informazioni	12%
4.	Windows Command Shell	11%
5.	Chiavi di esecuzione del registro/Cartella di avvio	10%

STRUMENTI DANNOSI PIÙ DIFFUSI UTILIZZATI NEGLI ATTACCHI NATION-STATE: 4° TRIMESTRE 2022

1.	PlugX	24%
2.	BLUEHAZE	23%
3.	DARKDEW	23%
4.	MISTCLOAK	23%
5.	JSX (trojan di accesso remoto)	2%

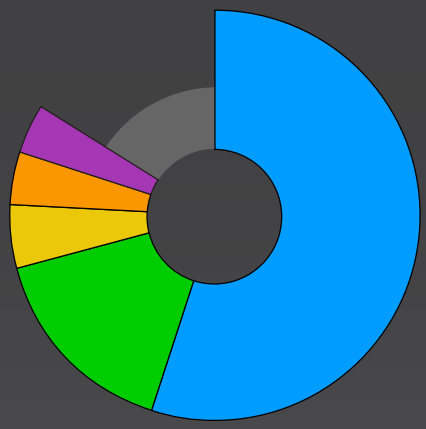
STRUMENTI NON DANNOSI PIÙ DIFFUSI UTILIZZATI NEGLI ATTACCHI NATION-STATE: 4° TRIMESTRE 2022

1.	Rundll32	22%
2.	Cmd	19%
3.	Reg	17%
4.	Ncat	12%
5.	Regsvr32	6%

PAESI PIÙ COLPITI DAGLI ATTACCHI NATION-STATE: 4° TRIMESTRE 2022

55%

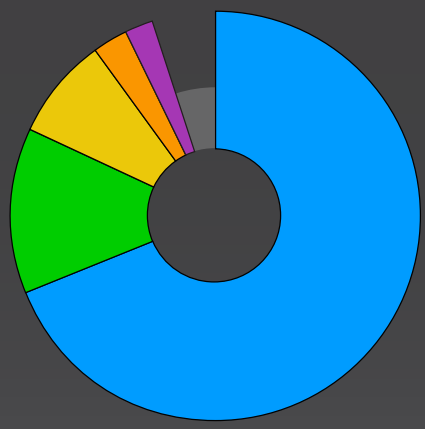
Gli Stati Uniti sono stati il paese più colpito dagli attacchi Nation-State nel 4° trimestre 2022.



SETTORI PIÙ COLPITI DAGLI ATTACCHI NATION-STATE: 4° TRIMESTRE 2022

69%

Il settore dei trasporti e della logistica è stato il più colpito dagli attacchi Nation-State nel 4° trimestre 2022.



Incidenti di attacchi Nation-State in base ai report pubblici: 4° trimestre 2022

Queste statistiche si basano su report pubblici e su ricerche interne e non su i dati di telemetria provenienti dai registri dei clienti. Si noti che non tutti gli incidenti Nation-State vengono segnalati. Molte campagne seguono tattiche, tecniche e procedure (TTP) che sono già note e meno interessanti da analizzare. Il settore tende a concentrarsi su campagne più recenti in cui un criminale informatico ha introdotto qualcosa di nuovo o ha commesso un errore. Tali metriche indicano ciò che il settore della sicurezza ha considerato più utile e rilevante nel 4° trimestre 2022.

PAESI CON IL MAGGIOR NUMERO DI CAMPAGNE DI ATTACCHI NATION-STATE SEGNALATI: 4° TRIMESTRE 2022

37%

delle campagne Nation-State segnalate pubblicamente nel 4°trimestre 2022 sono state lanciate dalla Cina.

1.	Cina	37%
2.	Corea del Nord	24%
3.	Iran	1%
4.	Russia	1%
5.	India	1%

CRIMINALI INFORMATICI PIÙ PREVALENTI ALL'ORIGINE DEGLI ATTACCHI NATION-STATE SEGNALATI: 4° TRIMESTRE 2022

33%

Lazarus è l'autore di attacchi Nation-State segnalati più diffuso nel 4° trimestre 2022.

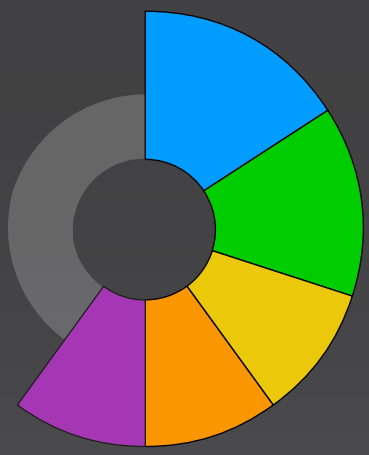
1.	Lazarus	33%
2.	Mustang Panda	17%
3.	APT34 APT37 APT41 COLDRIVER Patchwork Polonium SideWinder Winnti Group	1% ciascuno

PAESI PIÙ COLPITI DALLE CAMPAGNE NATION-STATE SEGNALATE: 4° TRIMESTRE 2022

16%

Gli Stati Uniti sono stati il paese più colpito dalle campagne Nation-State segnalate nel 4° trimestre 2022.

- Stati Uniti
- Regno Unito
- Pakistan
- Russia
- Ucraina

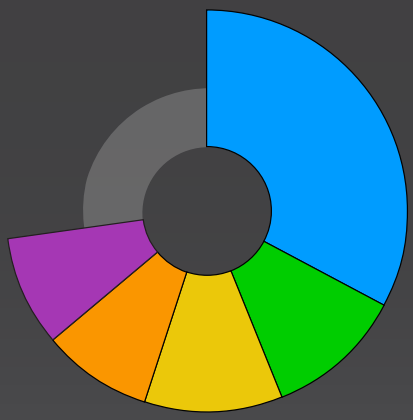


SETTORI PIÙ COLPITI DALLE CAMPAGNE NATION-STATE SEGNALATE: 4° TRIMESTRE 2022

33%

Il settore della pubblica amministrazione è stato il settore più colpito dalle campagne Nation-State segnalate nel 4° trimestre 2022, seguito dal settore delle forze armate (11%) e dalle telecomunicazioni (11%).

- Pubblica Amministrazione
- Forze Armate
- Telecomunicazioni
- Energia
- Finanza



STRUMENTI DANNOSI PIÙ UTILIZZATI NELLE CAMPAGNE NATION-STATE SEGNALATE: 4° TRIMESTRE 2022

1.	PlugX	22%
2.	Cobalt Strike	17%
3.	Metasploit	13%
4.	BlindingCan	9%
5.	Scanbox ShadowPad ZeroCleare	9% ciascuno

STRUMENTI NON DANNOSI PIÙ DIFFUSI UTILIZZATI NELLE CAMPAGNE NATION-STATE SEGNALATE: 4° TRIMESTRE 2022

1.	Cmd	32%
2.	Rundll32	20%
3.	PowerShell	14%
4.	Reg	8%
5.	Schtasks.exe	7%

TECNICHE MITRE ATT&CK PIÙ UTILIZZATE NELLE CAMPAGNE NATION-STATE SEGNALATE: 4° TRIMESTRE 2022

1.	Trasferimento di strumenti all'ingresso	13%
2.	Rilevamento delle informazioni di sistema	13%
3.	Offuscamento di file o informazioni	12%
4.	Protocolli web	11%
5.	Deoffuscamento/Decodifica di file o informazioni	11%

VULNERABILITÀ SFRUTTATE DALLE CAMPAGNE NATION-STATE SEGNALATE: 4° TRIMESTRE 2022

CVE-2017-11882
CVE-2021-44228
CVE-2018-0802
CVE-2021-26855
CVE-2021-27065
CVE-2021-34473
CVE-2021-34523
CVE-2015-2545
CVE-2017-0144
CVE-2018-0798
CVE-2018-8581
CVE-2019-0604
CVE-2019-0708
CVE-2019-16098
CVE-2020-0688
CVE-2020-1380
CVE-2020-1472
CVE-2020-17141
CVE-2020-17143
CVE-2021-21551
CVE-2021-26606
CVE-2021-26857
CVE-2021-26858
CVE-2021-28480
CVE-2021-28481
CVE-2021-28482
CVE-2021-28483
CVE-2021-31196
CVE-2021-31207
CVE-2021-40444
CVE-2021-45046
CVE-2021-45105
CVE-2022-1040
CVE-2022-30190
CVE-2022-41128

SFRUTTAMENTO DELLE RISORSE LOCALI E STRUMENTI DI TERZE PARTI: 4° TRIMESTRE 2022

Le osservazioni e il monitoraggio attraverso la piattaforma Global Threat Intelligence di Trellix Insights hanno permesso di ottenere la visibilità e le informazioni seguenti sul panorama delle minacce del 4° trimestre 2022.

NOTIZIE SULLO SFRUTTAMENTO DELLE RISORSE LOCALI: 4° TRIMESTRE 2022

- Lo sfruttamento delle risorse locali continua a giocare un ruolo in tutte le fasi di un attacco: accesso iniziale, esecuzione, scoperta, persistenza e impatto.

- In base ai dati raccolti nel 4° trimestre 2022, l'esecuzione dei comandi e degli script tramite Windows Command Shell e PowerShell è risultata la tecnica utilizzata più di frequente.
- L'uso dello sfruttamento delle risorse locali è prevalente tra i criminali informatici, compresi i gruppi APT esperti, i gruppi finanziariamente motivati e gli attivisti informatici.

Anche i nuovi arrivati, i criminali informatici occasionali e gli hacker dilettanti che si stanno facendo strada nel panorama delle minacce si avvalgono anche di binari già in uso negli exploit, nel tentativo di passare inosservati e di violare un sistema o sfruttare una vulnerabilità.

Le tecniche di sfruttamento delle risorse locali continuano a essere utilizzate per eseguire attività dannose in tute le fasi di un attacco: accesso iniziale, esecuzione, scoperta, persistenza e impatto. In base ai dati raccolti nel 4° trimestre 2022, l'esecuzione dei comandi e degli script tramite Windows Command Shell e PowerShell è risultata la tecnica più comunemente utilizzata.

FILE BINARI DEI SISTEMI OPERATIVI PIÙ DIFFUSI: 4° TRIMESTRE 2022

47%

Windows Command Shell rappresenta quasi la metà (47%) dei 10 file binari dei sistemi operativi più diffusi nel 4° trimestre del 22, seguito da PowerShell (32%) e Rundl32 (27%).

1.	Windows Command Shell	47%
2.	PowerShell	32%
3.	Rundl32	27%
4.	Schtasks	23%
5.	WMI	21%

L'uso dello sfruttamento delle risorse locali è prevalente tra i criminali informatici, compresi i gruppi APT esperti, i gruppi finanziariamente motivati e gli attivisti informatici.

Gli eventi elaborati attraverso la piattaforma Trellix Insights in cui i criminali informatici hanno utilizzato i file binari di Windows hanno portato alla distribuzione di malware aggiuntivo come strumenti di esfiltrazione di informazioni, un trojan di accesso remoto o un ransomware. File binari come MSHTA, WMI o WScript potrebbero essere stati eseguiti per recuperare ulteriori payload da risorse controllate dai criminali informatici.

PRINCIPALI STRUMENTI DI TERZE PARTI: 4° TRIMESTRE 2022

1.	Strumenti di accesso remoto	58%
2.	Trasferimento di file	22%
3.	Strumenti di post-sfruttamento	20%
4.	Rilevamento della rete	16%
5.	Rilevamento di Active Directory	10%

Gli strumenti di accesso e controllo remoto sono sempre tra i più utilizzati dai criminali informatici. Analogamente, gli strumenti utilizzati dai professionisti della sicurezza continuano a essere sfruttati per scopi dannosi. I criminali informatici possono utilizzarli per avviare beacon di connessione attiva, automatizzare l'esfiltrazione o raccogliere e comprimere informazioni mirate.

Tra gli strumenti gratuiti e open source, i programmi di compressione software sono utilizzati dai criminali informatici per ricompattare un software legittimo includendovi contenuti dannosi o per comprimere il malware nella speranza di eludere i rilevamenti e impedire le analisi.

INFORMAZIONI SU COBALT STRIKE: 4° TRIMESTRE 2022

Il gruppo Threat Intelligence dell'Advanced Research Center monitora l'utilizzo dei server Cobalt Strike (C2 Cobalt Strike) in ambienti reali combinando metodologie di tracciamento dei payload e delle infrastrutture. In questa sezione, presentiamo le nostre osservazioni derivanti dall'analisi dei beacon Cobalt Strike raccolti:

15%
LICENZE DI VALUTAZIONE DI COBALT STRIKE

Solo il 15% dei beacon Cobalt Strike identificati in un ambiente reale aveva una licenza di valutazione di Cobalt Strike. Questa versione di Cobalt Strike include la maggior parte delle funzionalità note di questo framework di post-sfruttamento. Tuttavia, aggiunge dei "segnali" e disabilita la crittografia dei dati in transito per rendere il payload facilmente rilevabile dai prodotti di sicurezza.

87%
RUNDLL32.EXE

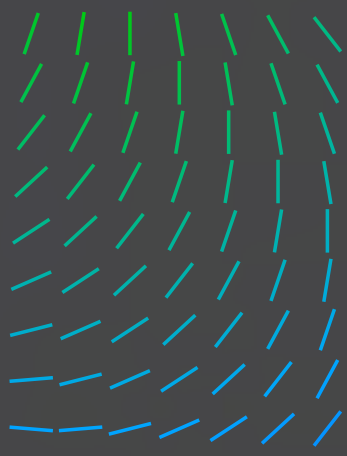
Rundll32.exe, il processo di default utilizzato per generare delle sessioni ed eseguire attività di post-sfruttamento, è stato rilevato nell'87% dei beacon identificati.

5% INTESTAZIONE HTTP HOST

Almeno il 5% dei beacon Cobalt Strike identificati utilizzava l'intestazione HTTP Host, un'opzione che facilita il domain fronting con Cobalt Strike. Il domain fronting è una tecnica che sfrutta le reti di distribuzione dei contenuti (CDN) che ospitano più domini. I criminali informatici nascondono una richiesta HTTPS inviata a un sito web dannoso sotto una connessione TLS a un sito web legittimo.

22% BEACON DNS

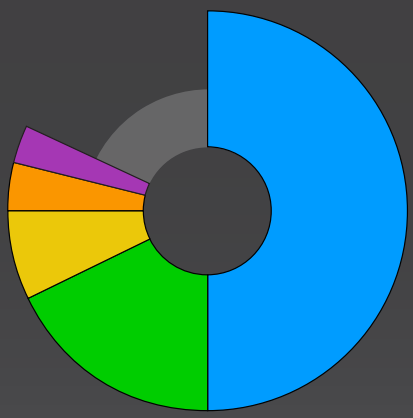
I beacon DNS rappresentano il 22% dei beacon Cobalt Strike identificati. Questo tipo di payload comunica con il server Cobalt Strike dell'aggressore, che è il server di riferimento del dominio, tramite delle query DNS per dissimulare la tua attività.



PRINCIPALI PAESI CHE OSPITANO SERVER COBALT STRIKE: 4° TRIMESTRE 2022

50%

La metà dei server Cobalt Strike rilevati nel 4° trimestre erano ospitati in Cina, in gran parte grazie alla capacità di hosting cloud disponibile in quel paese.



GOOTLOADER: 4° TRIMESTRE 2022

Gootloader è un malware modulare che a volte può essere indicato come "GootKit" o "GootKit Loader". Attualmente, le caratteristiche modulari del malware Gootloader vengono utilizzate per distribuire altri payload attivi, tra cui REvil, Kronos, Cobalt Strike e Icedid.

Negli ultimi eventi, Gootloader ha utilizzato l'ottimizzazione dei motori di ricerca (SEO) per attirare utenti inconsapevoli verso siti compromessi o fraudolenti utilizzati per ospitare un file di archivio contenente un payload JavaScript. Questa tecnica richiede tuttavia che l'utente troppo fiducioso apra l'archivio ed esegua il contenuto che a sua volta esegue il codice JavaScript dannoso tramite Windows Scripting Host. Una volta eseguito, Gootloader avvia le comunicazioni C2 e recupera ulteriore malware.

Si suppone che Gootloader sia un servizio MaaS (Malware as a Service) che consente ai criminali informatici di caricare diversi payload aggiuntivi. Pertanto, Gootloader rappresenta una minaccia significativa per gli ambienti aziendali.

Attraverso il nostro strumento di tracciamento interno di Gootloader abbiamo identificato una variante recente, rilevata in un ambiente reale il 18 novembre 2022, oltre a varianti più vecchie silenziose a partire dal 13 novembre 2022. Le modifiche dell'ultima variante sono le seguenti:

- Rimozione della funzionalità di manipolazione del registro
- Aumento delle richieste di rete remote a 10 URL anziché a tre

- Capacità di invocare direttamente script PowerShell tramite CScript
- Persistenza per ogni accesso dell'utente.

Il nostro processo di tracciamento di Gootloader

La nuova variante di Gootloader utilizza più livelli di offuscamento. Ogni fase annidata dopo la decompressione utilizza variabili caricate in una fase precedente che rendono l'analisi più complessa. I campioni raccolti grazie ai nostri sforzi di tracciamento YARA vengono inseriti in un analizzatore JavaScript e PowerShell statico per estrarre indicatori di compromissione (IOC) come i server di comando e controllo (C&C, C2) e le firme di identificazione uniche. Questi indicatori permettono di identificare e tracciare istanze specifiche di Gootloader in ambienti reali.

Gli indicatori estratti vengono quindi elaborati interrogando il database del team Trellix responsabile della reputazione degli URL per identificare gli URL dannosi, quelli legittimi potenzialmente compromessi e quelli legittimi utilizzati come esche per ostacolare l'analisi.

Dati di telemetria relativi a Gootloader

Le statistiche visualizzate sono quelle delle campagne identificate dalla correlazione degli indicatori di compromissione (IOC) estratti e dei registri dei nostri clienti, non i rilevamenti stessi. Nel caso di Gootloader, la maggior parte dei rilevamenti si basa sugli accessi ai domini. Poiché Gootloader utilizza domini esca, le statistiche mostrate devono essere interpretate come malevole con un livello di confidenza medio.

PAESI PIÙ COLPITI DA GOOTLOADER: 4° TRIMESTRE 2022

37% 

Gli Stati Uniti sono stati il paese più colpita da Gootloader nel 4° trimestre 2022.

1.	Stati Uniti	37%
2.	Italia	19%
3.	India	11%
4.	Indonesia	9%
5.	Francia	5%

TECNICHE MITRE ATT&CK PIÙ UTILIZZATE DA GOOTLOADER: 4° TRIMESTRE 2022

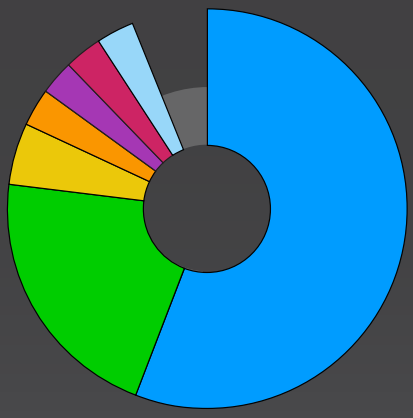
1. Deoffuscamento/ Decodifica di file o informazioni
2. JavaScript
3. Offuscamento di file o informazioni
4. PowerShell
5. Svuotamento del processo

SETTORI PIÙ COLPITI DA GOOTLOADER: 4° TRIMESTRE 2022

56%

Il settore delle telecomunicazioni è stato il più colpito da Gootloader nel 4° trimestre 2022.

- Telecomunicazioni
- Media e comunicazioni
- Finanza
- Istruzione
- Tecnologia
- Pubblica Amministrazione
- Grande distribuzione



Tecniche MITRE ATT&CK più utilizzate da Gootloader: 4° trimestre 2022

Deoffuscamento/Decodifica di file o informazioni
JavaScript
Offuscamento di file o informazioni
PowerShell
Svuotamento del processo
Caricamento riflessivo di codice
Chiavi di esecuzione del registro/Cartella di avvio
Rundll32
Attività pianificata

INFORMAZIONI SULLE VULNERABILITÀ: 4° TRIMESTRE 2022

La nostra dashnoard delle vulnerabilità raccoglie l'analisi delle ultime vulnerabilità ad alto impatto. L'analisi e il triage sono eseguiti dagli esperti di vulnerabilità del Trellix Advanced Research Center. Questi ricercatori, specializzati in reverse engineering e analisi delle vulnerabilità, monitorano costantemente le vulnerabilità più recenti e il modo in cui i criminali informatici le utilizzano nei loro attacchi per fornire consigli per correggerle. Questa consulenza concisa e altamente tecnica ti permette di filtrare i segnali di disturbo e di concentrarti sulle vulnerabilità più pericolose per la tua azienda, permettendoti di reagire rapidamente.

INFORMAZIONI SULLE VULNERABILITÀ: 4° TRIMESTRE 2022

41% Lanner ha rappresentato il 41% dei prodotti e dei fornitori vulnerabili impattati da CVE unici nel 4° trimestre del 2022.

29% La versione 1.10.0 del firmware IAC-AST2500A è stato il CVE più segnalato utilizzato dai prodotti nel 4° trimestre 2022

PRODOTTI VULNERABILI, FORNITORI E CVE CON IL MAGGIOR IMPATTO: 4° TRIMESTRE 2022

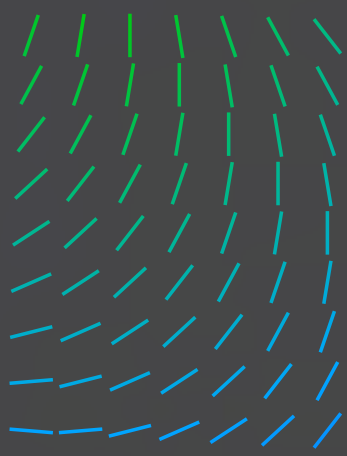
1.	Lanner	41%
2.	Microsoft	19%
3.	BOA	15%
4.	Oracle	8%
5.	Apple Chrome Citrix Fortinet Linux	5% ognuno

CVE SEGNALATI PER PRODOTTO: 4° TRIMESTRE 2022

29%

La versione 1.10.0 del firmware IAC-AST2500A è stata il CVE più segnalato utilizzato dai prodotti nel 4° trimestre 2022, seguita dal server Boa (10%), IAC-AST2500A (6%) e Exchange (6%).

Prodotti con CVE segnalati	CVE unici
IAC-AST2500A, versione 1.10.0 del firmware	9
Server Boa	3
Exchange	3
IAC-AST2500A	2
tvOS	1
iPadOS	1
iOS	1
Windows	1
Safari	1
SQLite versione 3.40.0 e precedenti	1
Oracle Access Manager, 11.1.2.3.0, 12.2.1.3.0, 12.2.1.4.0	1
MacOS	1
Kernel Linux antecedente la versione 5.15.61	1
Internet Explorer	1



Prodotti con CVE segnalati	CVE unici
FortiOS (sslvpnd)	1
Citrix ADC/Citrix Gateway	1
Chrome, antecedente la versione 108.0.5359.94/.95	1
Server Boa , Boa 0.94.13	1

CVE SEGNALATI: 4° TRIMESTRE 2022

CVE-2022-1786
CVE-2022-26134
CVE-2022-27510
CVE-2022-27518
CVE-2022-31685
CVE-2022-32917
CVE-2022-32932
CVE-2022-33679
CVE-2022-34718
CVE-2022-35737
CVE-2022-3602
CVE-2022-3786
CVE-2022-37958
CVE-2022-40684
CVE-2022-41040
CVE-2022-41080
CVE-2022-41082
CVE-2022-41128
CVE-2022-41352
CVE-2022-42468
CVE-2022-42475
CVE-2022-4262
CVE-2022-42856
CVE-2022-42889
CVE-2022-43995
CVE-2022-46908
CVE-2022-47939

TENDENZE IN MATERIA DI SICUREZZA DELL'EMAIL: 4° TRIMESTRE 2022

Queste statistiche si basano sui dati di telemetria generati dalle diverse appliance di sicurezza dell'email implementate nelle reti dei nostri clienti in tutto il mondo. I registri di rilevamento vengono aggregati e analizzati per produrre le seguenti informazioni:

INFORMAZIONI SULLE TENDENZE IN MATERIA DI SICUREZZA DELL'EMAIL: 4° TRIMESTRE 2022

100% Il volume delle email dannose nei Paesi arabi è aumentato del 100% nel mese di ottobre rispetto ad agosto e settembre.

40% Qakbot è stata la tattica malware più utilizzata, con il 40% delle campagne rivolte ai Paesi arabi.

42% Le telecomunicazioni sono state il settore più colpito dalle email dannose nel 4° trimestre del 2022, con il 42% delle campagne email dannose contro tutti i settori.

87% Le email di phishing che utilizzano URL dannosi sono state di gran lunga il vettore di attacco più diffuso nel 4° trimestre del 2022.

64% Gli attacchi di furto d'identità sono aumentati del 64% dal 3° al 4° trimestre del 2022.

82% di tutte le email di frode dei CEO sono state inviate utilizzando servizi email gratuiti.

78% di tutti gli attacchi di violazione dell'email aziendale (BEC) hanno utilizzato frasi comunemente utilizzate dai CEO.

142% Gli attacchi di vishing sono aumentati del 142% tra il 3° e il 4° trimestre del 2022.

TATTICHE DI DISTRIBUZIONE DI MALWARE TRAMITE EMAIL PIÙ DIFFUSE: 4° TRIMESTRE 2022

40%

Qakbot è stata la tattica di distribuzione di malware tramite email più diffusa utilizzata nel 4° trimestre 2022.

1.	Qakbot	40%
2.	Emotet	26%
3.	Formbook	26%
4.	Remcos	4%
5.	QuadAgent	4%

PRODOTTI E MARCHI PIÙ COLPITI DALLE EMAIL DI PHISHING: 4° TRIMESTRE 2022

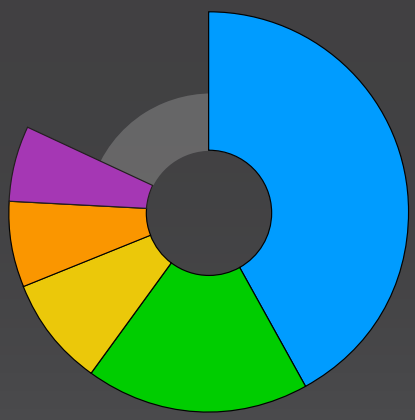
1.	Generico	62%
2.	Outlook	13%
3.	Microsoft	11%
4.	Ekinet	8%
5.	Cloudfare	3%

SETTORI PIÙ COLPITI DA EMAIL DANNOSE: 4° TRIMESTRE 2022

42%

Il settore delle telecomunicazioni è stato il più colpito dalle email dannose nel 4° trimestre 2022.

- Telecomunicazioni
- Pubblica Amministrazione
- Istruzione
- Finanza
- Servizi/consulenza



TENDENZE IN MATERIA DI FURTO DELL'IDENTITÀ TRAMITE L'EMAIL: 4° TRIMESTRE 2022

82% di tutte le email fraudolente dei CEO sono state inviate utilizzando servizi email gratuiti.

78% di tutti gli attacchi di violazione dell'email aziendale (BEC) hanno utilizzato frasi comunemente utilizzate dai CEO.

64% aumento del numero di email dannose che violano l'identità del CEO e altri leader aziendali dal 3° al 4° trimestre 2022.

Frasi dei CEO utilizzate negli attacchi BEC nel 4° trimestre del 2022

"Ho bisogno che tu svolga un compito per me immediatamente".

"Ho bisogno che tu porti a termine un compito, quindi gentilmente inviami il tuo numero di cellulare".

"Mandami il tuo numero di telefono, devi fare qualcosa per me immediatamente".

"Mandami il tuo numero di cellulare e tieni d'occhio i miei messaggi. Ho bisogno che sia portata a termine un'attività".

"Per favore, rivedi e conferma il tuo numero di cellulare e tieni d'occhio il mio messaggio per le istruzioni".

"Hai ricevuto la mia email precedente? Ho un deal redditizio da proporti".

EVOLUZIONE DEI FURTI D'IDENTITÀ: 4° TRIMESTRE 2022

64% Gli attacchi di furto d'identità sono aumentati del 64% dal 3° al 4° trimestre del 2022

INFORMAZIONI SULLE CAMPAGNE DI PHISHING: 4° TRIMESTRE 2022

I fornitori di servizi di web in hosting sono sempre più sfruttati per truffe e furti

Nel quarto trimestre abbiamo osservato un aumento dell'utilizzo di provider di servizi web in hosting legittimi per truffare gli utenti e sottrarre le credenziali d'accesso. I service provider più colpiti sono tre: dweb.link, ipfs.link e translate.goog. Abbiamo notato anche volumi significativi provenienti dai domini di altri service provider come ekinet, storageapi_fleek e selcdn.ru. I criminali informatici utilizzano continuamente nuovi e popolari servizi di hosting per ospitare pagine di phishing ed eludere i motori antiphishing. Questi servizi non possono essere inseriti in blacklist da alcun sistema di rilevamento poiché il loro obiettivo principale è di ospitare file legittimi e condividere contenuti. Questo è uno dei motivi per cui i criminali informatici sono sempre più interessati ai provider di servizi web in hosting.

VETTORI DI ATTACCO PIÙ UTILIZZATI NELLE EMAIL DI PHISHING

87%

Le email di phishing che utilizzano URL dannosi sono stati di gran lunga il vettore d'attacco più diffuso nel 4° trimestre 2022.

1.	URL	87%
2.	Allegato	7%
3.	Intestazione	6%

FORNITORI DI SERVIZI WEB IN HOSTING ALTAMENTE ABUSATI: 4° TRIMESTRE 2022

154%

Se Dweb è stato il provider di servizi in hosting più sfruttato nel 4° trimestre 2022, Google Traduttore ha registrato l'incremento maggiore (154%) tra il 3° e il 4° trimestre 2022.

1.	Dweb	81%
2.	Ipfs	17%
3.	Google Traduttore	10%

TECNICHE DI ELUSIONE PIÙ UTILIZZATE NEGLI ATTACCHI DI PHISHING: 4° TRIMESTRE 2022

63%

Gli attacchi di elusione basati sul reindirizzamento 302 sono stati i più numerosi nel 4° trimestre 2022.

- Gli attacchi di phishing di elusione basati sulla geolocalizzazione sono aumentati notevolmente nel 4° trimestre.
- Anche gli attacchi basati su Captcha sono aumentati nel 4° trimestre.

Il vishing è una forma di phishing progettata per indurre le vittime a interagire con i criminali informatici, principalmente tramite email, messaggi di testo, telefonate o messaggi diretti in chat.

142%

Gli attacchi di vishing sono aumentati del 142% tra il 3° e il 4° trimestre del 2022.

85%

I servizi email gratuiti sono diventati i preferiti dagli autori di attacchi di vishing. Un'elevata percentuale di attacchi di vishing rilevati nel 4° trimestre del 2022 (85%) è stata inviata utilizzando un servizio email gratuito.

Norton, McAfee, Geek Squad, Amazon e PayPal sono stati i temi più utilizzati dalle campagne di vishing nel 4° trimestre.

SICUREZZA DELLA RETE: 4° TRIMESTRE 2022

Il team di ricerca sulle reti di Trellix Advanced Research Center si concentra sul rilevamento e sul blocco degli attacchi di rete che minacciano i nostri clienti. Ispezioniamo diverse aree della catena d'attacco: ricognizione, violazione iniziale, comunicazione con il server C&C e TTP di spostamento laterale. La nostra capacità di sfruttare i punti di forza delle nostre tecnologie ci permette di avere visibilità per individuare meglio le minacce sconosciute.

Tecniche MITRE ATT&CK più utilizzate per eludere la sicurezza della rete: 4° trimestre 2022

- T1083 - Rilevamento di file e directory
- T1573 - Canale canale crittografato
- T1020 - Esfiltrazione automatica
- T1210 - Sfruttamento dei servizi remoti
- T1569 - Servizi di sistema
- T1059 - Interprete di comandi e script: Windows Command Shell
- T1047 - Strumentazione gestione Windows (WMI)
- T1087 - Rilevamento dell'account
- T1059 - Interprete di comandi e script
- T1190 - Sfruttamento di applicazioni per il pubblico

Attacchi con il maggior impatto contro servizi esterni: 4° trimestre 2022

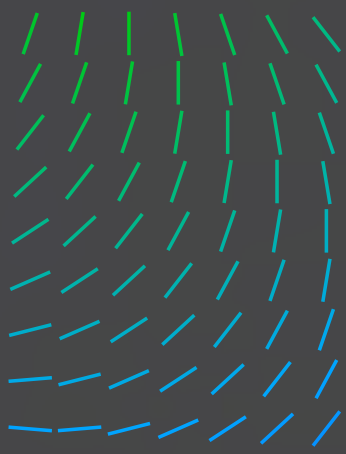
Ogni giorno vengono eseguite numerose analisi di rete per sondare le macchine con accesso esterno alla ricerca di un potenziale punto di accesso all'ambiente di un cliente. I vecchi exploit sono costantemente alla ricerca di sistemi privi di patch.

- Rilevamento di un tentativo di accesso al file/etc/passwd
- Possibile attacco di tipo di esecuzione di script tra siti
- Analizzatore di sicurezza SIPVicious
- Traffico dell'analizzatore Nmap rilevato
- Attività di analisi - Shellshock, sondaggio del server web
- Esecuzione di codice remoto Bash (Shellshock) CGI HTTP (CVE-2014-6278)
- Vulnerabilità di esecuzione di codice remoto CVE-2020-14882 Oracle WebLogic
- Tentativo di attraversamento di directory
- Iniezione di script OGNL ConversionErrorInterceptor Apache Struts 2
- Esecuzione di codice remoto CVE-2021-44228 Apache Log4j

Principali WebShell utilizzate per l'insediamento nella rete: 4° trimestre 2022

Le seguenti WebShell sono tipicamente utilizzate per tentare di controllare un server web vulnerabile.

- WebShell China Chopper
- WebShell JFolder
- WebShell ASPXSpy
- WebShell C99
- WebShell Tux
- WebShell B374K / Famiglia RootShell



Strumenti, tecniche e procedure più rilevanti una volta all'interno della rete: 4° trimestre 2022

Le seguenti WebShell sono tipicamente utilizzate per tentare di controllare un server web vulnerabile.

Abbiamo osservato un elevato volume di TTP utilizzati per gli attacchi durante lo spostamento laterale, comprese vecchie vulnerabilità come SCShell e PSExec.

- SCshell: spostamento laterale senza file tramite il Gestore di servizi
- Chiamata di processo remoto Windows WMI
- Invocazione della shell CMD con WMIEXEC tramite SMB
- Exploit EternalBlue rilevato
- Tentativo CVE-2020-0796 Microsoft SMBv3
- RCE CVE-2021-44228 Apache Log4j
- Enumerazione remota di account di amministrazione aziendale/di dominio
- Esecuzione remota di script PowerShell sospetti
- Ricognizione di reti sospette con WMIC
- Comando di enumerazione rilevato nel file batch
- Attività PSEXEC SMB

DATI DI TELEMETRIA SULLE OPERAZIONI DI SICUREZZA RACCOLTI DA TRELLIX XDR

Queste statistiche si basano sui dati di telemetria generati da diversi sensori implementati dai nostri clienti. I registri di rilevamento vengono aggregati e analizzati per produrre le seguenti informazioni:

Incidenti di sicurezza con il maggior impatto: 4° trimestre 2022

La sezione seguente mostra gli avvisi di sicurezza più diffusi nel 4° trimestre del 2022:

EXPLOIT - LOG4J [CVE-2021-44228]

OFFICE 365 ANALYTICS [Connessione anormale]

OFFICE 365 [Phishing autorizzato]

EXPLOIT - FORTINET [CVE-2022-40684]

EXPLOIT - APACHE SERVER [Tentativo CVE-2021-41773]

WINDOWS ANALYTICS [Attacco di forza bruta riuscito]

EXPLOIT - ATLASSIAN CONFLUENCE [CVE-2022-26134]

EXPLOIT - F5 BIG-IP [Tentativo CVE-2022-1388]

TECNICHE MITRE ATT&CK PIÙ UTILIZZATE: 4° TRIMESTRE 2022

1.	Sfruttamento di applicazioni per il pubblico (T1190)	29%
2.	Protocollo per il livello Applicazione: DNS (T1071.004)	14%
	Phishing (T1566)	14%
3.	Manipolazione di account (T1098.001) Attacco di forza bruta (T1110) Violazione per download all'insaputa dell'utente (T1189) Esecuzione da parte dell'utente: File dannoso (T1204.002) Account validi: Account locali (T1078.003)	7% ciascuno

DISTRIBUZIONE DELLE PRINCIPALI ORIGINI DEI REGISTRI: 4° TRIMESTRE 2022

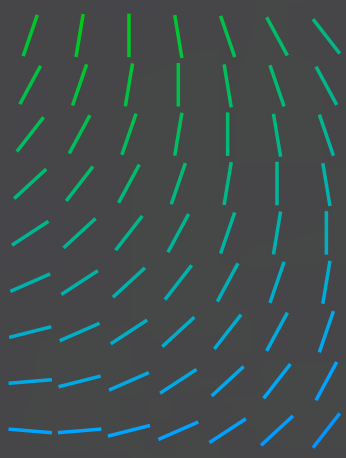
1.	Rete	40%
2.	Email	27%
3.	Endpoint	27%
4.	Firmware	6%

EXPLOIT IDENTIFICATI: 4° TRIMESTRE 2022

EXPLOIT PIÙ DIFFUSI OSSERVATI: 4° TRIMESTRE 2022

30% Log4j è stato l'exploit più diffuso identificato nel 4° trimestre 2022.

1.	Log4j (CVE-2021-44228)	30%
2.	Fortinet (CVE-2022-40684)	16%
3.	Apache Server (CVE-2021-41773)	15%
4.	Atlassian Confluence (CVE-2022-26134)	14%
5.	F5 Big-IP (tentativo CVE-2022-1388)	13%
6.	Microsoft Exchange (tentativo di exploit ProxyShell)	11%



INCIDENTI CLOUD: 4° TRIMESTRE 2022

Gli attacchi contro l'infrastruttura cloud continuano a crescere con il passaggio di molte aziende dall'infrastruttura on premise al cloud. Secondo gli analisti di Gartner, entro il 2025 oltre l'85% delle aziende adotterà un approccio basato sul cloud.

Analizzando i dati di telemetria raccolti nel 4° trimestre del 2022, abbiamo osservato quanto segue:

- I rilevamenti legati ad AWS sono stati i più numerosi, forse a causa della posizione di leader di AWS sul mercato del cloud.
- La maggior parte degli attacchi si è concentrata sull'accesso iniziale ad account validi tramite un attacco di forza bruta o passwordspray, suggerendo che il vettore d'infezione iniziale si trova a livello di superficie di attacco del cloud.
- Dato che la maggior parte degli account aziendali ha attivato l'autenticazione a più fattori (MFA), i criminali informatici all'origine degli attacchi di forza bruta riusciti hanno utilizzato piattaforme MFA, con un conseguente aumento dei rilevamenti associati.

Le sezioni seguenti descrivono brevemente i dati di telemetria degli attacchi cloud della nostra base clienti, suddivisi in base al fornitore di servizi cloud.

DISTRIBUZIONE DELLE TECNICHE MITRE ATT&CK PER AWS: 4° TRIMESTRE 2022

1.	Account validi (T1078)	18%
2.	Modifica dell'infrastruttura di servizio di elaborazione dell'account cloud (T1578)	12%
3.	Manipolazione di account (T1098)	9%
4.	Account cloud (T1078.004)	8%
5.	Attacco di forza bruta (T1110) Disabilitazione delle difese (T1562)	6% ciascuno

PRINCIPALI TECNICHE MITRE ATT&CK PER AZURE: 4° TRIMESTRE 2022

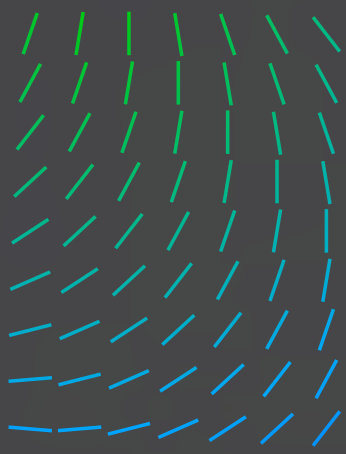
1.	Account validi (T1078)	23%
2.	Autenticazione a più fattori (T1111)	19%
3.	Attacco di forza bruta (T1110)	14%
4.	Proxy (T1090)	14%
5.	Manipolazione di account (T1098)	5%

PRINCIPALI RILEVAMENTI AWS DA PARTE DELLE TECNICHE MITRE ATT&CK: 4° TRIMESTRE 2022

Tecnica MITRE ATT&CK	Regola
Manipolazione di account (T1098)	Policy privilegiata AWS legata all'identità IAM AWS S3 - Cancellazione della policy di compartimentazione
Account validi (T1078)	AWS Analytics - Connessione anormale alla console AWS Analytics - Utilizzo anomale delle chiavi API AWS GuardDuty - Comportamento anomalo degli utenti AWS GuardDuty - Accesso anonimo garantito
Disabilitazione delle difese (T1562)	AWS CloudTrail - Modifiche alle policy AWS CloudTrail - Cancellazione del registro di monitoraggio
Credenziali nei file (T1552.001)	Avviso su un potenziale furto di chiavi segrete AWS
Modifica dell'infrastruttura di servizio di elaborazione dell'account cloud (T1578)	AWS CloudTrail - Cancellazione del bucket S3 AWS CloudTrail - Caricamento dell'ACL di un bucket S3 AWS CloudTrail - Caricamento dell'ACL di un oggetto

PRINCIPALI RILEVAMENTI AZURE DA PARTE DELLE TECNICHE MITRE ATT&CK: 4° TRIMESTRE 2022

Tecnica MITRE ATT&CK	Regola
Account validi (T1078)	Azure AD - Connessione a rischio Azure - Connessione da un luogo insolito Azure - Connessione da un conto inattivo da 60 giorni
Attacco di forza bruta (T1110)	Azure - Diversi errori di autenticazione Graph - Attacco di forza bruta contro il portale Azure Graph - Tentativi di violazione delle password distribuiti
Autenticazione a più fattori (T1111)	Azure - Autenticazione a più fattori negata perché allarme di frode Azure - Autenticazione a più fattori negata perché utente bloccato Azure - Autenticazione a più fattori negata perché codice fraudolento Azure - Autenticazione a più fattori negata perché applicazione fraudolenta



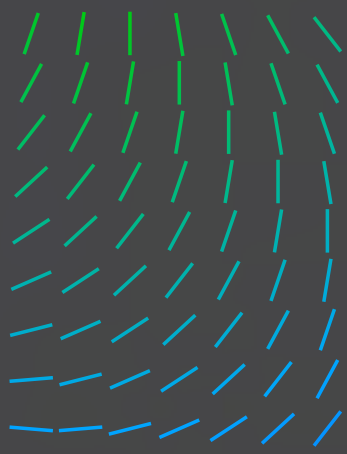
Servizi remoti esterni (T1133)	Azure - Connessione a partire dalla rete Tor
Manipolazione di account (T1098)	Azure - Reinizializzazione insolita di una password utente

DISTRIBUZIONE DELLE TECNICHE MITRE ATT&CK PER GCP: 4° TRIMESTRE 2022

1.	Account validi (T1078)	36%
2.	Esecuzione tramite API (T0871)	18%
3.	Rilevamento dell'account (T1087.001) Manipolazione di account (T1098) Disabilitazione delle difese (T1562) Modifica dell'infrastruttura di servizio di elaborazione dell'account cloud (T1578) Servizi remoti (T1021.004)	9% ciascuno

PRINCIPALI RILEVAMENTI GCP DA PARTE DELLE TECNICHE MITRE ATT&CK: 4° TRIMESTRE 2022

Tecnica MITRE ATT&CK	Regola
Account validi (T1078)	GCP - Creazione di un account di servizio GCP Analytics - Attività anormale GCP - Creazione della chiave dell'account di servizio
Servizi remoti (T1021.004)	GCP - Regola firewall I che autorizza tutto il traffico sulla porta SSH
Manipolazione degli account (T1098)	GCP - Modifica della policy IAM dell'azienda
Rilevamento dell'account (T1087.001)	Allarme [gcps net user]
Trasferimento dei dati verso un account cloud (T1527)	GCP - Modifica del sink dei registri
Modifica dell'infrastruttura di servizio di elaborazione dell'account cloud (T1578)	GCP - Disabilitazione della protezione contro l'eliminazione



REDAZIONE E RICERCA

Alfred Alvarado
Henry Bernabe
Adithya Chandra
Dr. Phuc Duy Pham
Sarah Erman
John Fokker
Lennard Galang
Sparsh Jain
Daksh Kapoor
Maulik Maheta
João Marques
Tim Polzer
Srini Seethapathy
Rohan Shah
Vihar Shah
Swapnil Shashikantpa
Shyava Tripathi
Leandro Velasco

RISORSE

Per seguire l'evoluzione delle minacce più recenti e di maggior impatto identificate dal team Trellix Advanced Research Center consulta queste risorse:

TWITTER

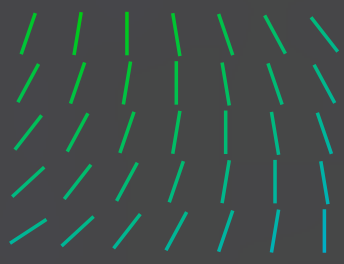
Trellix ARC

INFORMAZIONI SU TRELLIX ADVANCED RESEARCH CENTER

Trellix Advanced Research Center dispone dello statuto più esaustivo nel settore della sicurezza informatica ed è all'avanguardia nello studio di metodi, tendenze e gruppi di criminali informatici emergenti nel panorama delle minacce. Partner fondamentale dei team responsabili delle operazioni di sicurezza in tutto il mondo, il Trellix Advanced Research Center fornisce intelligence sulle minacce agli analisti di sicurezza e contenuti di prim'ordine, alimentando al contempo la nostra avanzata piattaforma XDR.

A PROPOSITO DI TRELLIX

Trellix è un'azienda internazionale che ridefinisce il futuro della cyber security. La piattaforma XDR (eXtended Detection and Response) aperta e nativa di Trellix aiuta le aziende a proteggersi dalle minacce sempre più sofisticate che ogni giorno si trovano ad affrontare, e a gestire le proprie attività di business in modo sicuro e con resilienza. Gli esperti di sicurezza di Trellix, insieme all'ampio ecosistema di partner, accelerano l'innovazione tecnologica attraverso la data science e l'automazione per supportare oltre 40.000 clienti in ambito privato e pubblico. Per maggiori informazioni visita il sito www.trellix.com.



Per saperne di più, visita il sito Trellix.com/it.

Trellix

A proposito di Trellix

Trellix è un'azienda internazionale che ridefinisce il futuro della cyber security. La piattaforma XDR (eXtended Detection and Response) aperta e nativa di Trellix aiuta le aziende a proteggersi dalle minacce sempre più sofisticate che ogni giorno si trovano ad affrontare, e a gestire le proprie attività di business in modo sicuro e con resilienza. Gli esperti di sicurezza di Trellix, insieme all'ampio ecosistema di partner, accelerano l'innovazione tecnologica attraverso la data science e l'automazione per supportare oltre 40.000 clienti in ambito privato e pubblico.

072022-05