Swascan
TINEXTA GROUP

Botnet e infostealer

Financial threat landscape 2023

www.swascan.com

Sommario

Botnet e infostealer

Le botnet rappresentano una minaccia significativa e insidiosa. La loro natura resistente agli sforzi di mitigazione le rende particolarmente pericolose. Attraverso le analisi svolte dal Cyber Security Team di Swascan non solo sono state individuate le botnet che hanno colpito direttamente gli asset del settore finanziario italiano ma anche quelle che potrebbero aver infettato dispositivi personali o utilizzati dai dipendenti in modalità di lavoro remoto.

Collegarsi alle applicazioni aziendali da dispositivi infetti può avere conseguenze devastanti. Malware come gli InfoStealer possono rubare credenziali di accesso, informazioni finanziarie, dati personali, informazioni di carte di credito e documenti riservati.

Nella sottosezione *Extra #1* sono rappresentati i risultati di un'analisi effettuata su un campione di 30 banche italiane, equamente divise tra "significant" e "less significant"[1] volta ad esaminare la presenza di dispositivi compromessi e i rischi derivanti da data breach considerando il periodo compreso tra il 2022 e il 2023.

Nel dettaglio, tra il 2022 e il 2023 sulle 30 banche analizzate, sono stati riscontrati un totale di 48.565 dispositivi infettati da InfoStealer; in particolar modo, si è passati da un totale di 19.806 nel 2022 a 28.759 credenziali esfiltrate da InfoStealer nel 2023 che hanno rubato le credenziali di accesso ai conti correnti ma allo stesso tempo informazioni finanziarie, dati personali, informazioni di carte di credito e documenti riservati, con un incremento pari a 45.2%.

Una delle principali osservazioni, quindi, è l'evidente crescita nell'utilizzo di malware di tipo InfoStealer per l'esfiltrazione di credenziali, coinvolgendo sia i dipendenti delle banche sia i clienti finali. Nel complesso, si sono riscontrate una quantità di 105.777 dispositivi infetti appartenenti ad utenti interni, esterni, clienti finali e dispositivi da cui sono stati esfiltrati cookie, autofill, cronologia e documenti.

Contrariamente a questa tendenza, l'uso delle combolist [2]è in diminuzione, evidenziando una transizione nelle tattiche degli attaccanti. Nel 2023, le combolist hanno raggiunto un totale di 1.148 rispetto alle 9.486 del 2022, segnalando una contrazione nell'approccio alla pubblicazione di elenchi di credenziali. Questo si traduce in una differenza percentuale

[1] Le banche selezionate per l'analisi sono state classificate come *significant* e *less-significant* in accordo alla classificazione realizzata della Banca Centrale Europea (BCE).

[2] Una combolist è una lista di combinazioni di nomi utente e password. Queste liste vengono spesso create da hacker o da individui che cercano di ottenere accesso non autorizzato a account online, come quelli su siti web, forum, servizi di posta elettronica e così via.
La logica dietro una combolist è quella di testare automaticamente diverse combinazioni di nomi utente e password in modo da individuare quelle che potrebbero consentire l'accesso a un account.

significativa del 87.9%, indicando una notevole diminuzione del numero di combolist pubblicate quest'anno rispetto al precedente.

Inoltre, nella sottosezione *Extra #2* viene fornita una panoramica dei principali InfoStealer identificati nel contesto dell'analisi condotta.

In fine, nella sottosezione *Extra #3* è stato realizzato un approfondimento relativo alle principali motivazioni dietro il sempre più crescente utilizzo di malware di tipo InfoStealer tramite l'esaminazione di alcuni forum underground dove tali malware sono messi in vendita.

Una sincronia pericolosa

Le botnet e gli infostealer spesso vengono utilizzati in combinazione per condurre attacchi informatici.

Una botnet può essere impiegata per distribuire e gestire malware, inclusi gli infostealer. I dispositivi infetti all'interno della botnet possono essere sfruttati per diffondere il malware in modo massiccio, aumentando così il numero di sistemi vulnerabili.

Gli infostealer, una volta installati sui dispositivi target, raccolgono informazioni sensibili e le inviano al comando e al controllo della botnet. Il botmaster può quindi utilizzare queste informazioni per scopi fraudolenti, come il furto di identità o la compromissione delle credenziali di accesso garantendo la persistenza all'interno del sistema bersaglio.

Questo permette al Criminal Hacker di ricevere informazioni sempre aggiornate dal dispositivo colpito anche nel caso di registrazione di nuovi servizi e/o credenziali

Volendo fare un breve sillogismo, la botnet fornisce l'infrastruttura di controllo e distribuzione, mentre gli infostealer sono progettati per raccogliere informazioni sensibili dai dispositivi infettati all'interno di questa rete. L'integrazione di queste due minacce consente agli attaccanti di orchestrare attacchi sofisticati e di ottenere un accesso più ampio a dati preziosi.

Notable Insights

Nella top 3 degli InfoStealer maggiormente rilevati e che hanno compromesso dispositivi associati alle 30 banche analizzate figurano Redline, Raccoon e Arkei.

I risultati delle analisi rappresentati rivelano una evidente **crescita** nell'utilizzo di malware di tipo **InfoStealer**; tali malware hanno interessato utenze sia di dipendenti delle banche che utenti esterni. Infatti, dai risultati delle analisi emerge un **notevole aumento**

(pari a 45.2%) **del numero di dispositivi compromessi** nel 2023 rispetto al 2022. Tale aumento potrebbe essere attribuito ad un sempre più crescente utilizzo di malware di tipo Infostealer da parte degli attaccanti. Tale dinamica evidenzia l'importanza di una difesa multi-livello e proattiva per affrontare un panorama di minacce in continua evoluzione.

Tale trend è ulteriormente confermato da un'analisi effettuata sui **forum underground** maggiormente frequentati dai cybercriminali. Il numero sempre più crescent di Threat Actors che sviluppano e mettono in vendita nuovi Infostealer con nuove funzionalità evidenzia un **ambiente sempre più dinamico e sofisticato**.

Allo stesso tempo, è stata notata una **diminuzione nell'uso di combolist**[3], indicando un cambiamento nelle tattiche degli attaccanti. Nel 2023, le combolist hanno raggiunto un totale di 1.148 rispetto alle 9.468 del 2022, segnalando una contrazione nell'approccio alla pubblicazione di elenchi di credenziali. La riduzione delle combolist pubblicate può essere interpretata come una variazione strategica da parte degli attaccanti che trova dimostrazione nel numero crescente di dispositivi infetti da InfoStealer.

Inoltre, dalle analisi emerge una marcata **diminuzione dei data breach** nel corso del 2023 rispetto all'anno precedente.

La presenza di mail aziendali all'interno di Data Breach e Combolist, solitamente derivante dall'utilizzo di account aziendali per l'iscrizione a servizi di terze parti, può portare a situazioni di rischio quali:

- Furto di account social;
- Attacchi di tipo Credential Stuffing;
- Attacchi di Phishing mirati.

L'efficacia delle combolist per un attaccante risiede nella consapevolezza che un dipendente ha utilizzato la propria mail aziendale su un sito terzo che ha subito una violazione dei dati. Questo scenario apre la strada a potenziali attacchi di phishing mirati in cui l'attaccante può cercare di indurre il dipendente a fornire ulteriori informazioni sensibili o ad eseguire azioni dannose all'interno dell'ambiente aziendale.

TIP Le implicazioni del confronto riportato nella presente analisi sono significative, richiamando l'attenzione sulle nuove sfide che il settore bancario deve affrontare nel proteggere le informazioni sensibili e le risorse critiche. In risposta a questa escalation delle minacce, diventa imperativo che le istituzioni finanziarie adottino misure di sicurezza avanzate,

implementando strategie proattive e soluzioni tecnologiche all'avanguardia per prevenire, rilevare e mitigare efficacemente le botnet e le violazioni di sicurezza.

#1 – Analysis of compromised devices and data breaches among “less-significant” and “significant” Italian financial institutions

L'obiettivo principale dell’analisi effettuata è quello di analizzare attentamente le minacce informatiche che possono compromettere l'integrità e la confidenzialità dei dati delle banche, concentrandosi specificamente su tre categorie di botnet:

- **Botnet-internal**: riguarda la presenza di dispositivi infetti dove sono state esfiltrate credenziali con indirizzi e-mail aziendali associate ai domini analizzati e credenziali di dominio per accesso a portali interni.
- **Botnet-external**: si concentra su dispositivi infetti esterni alle organizzazioni bancarie analizzate, che possono includere dunque clienti e utenti delle banche, o visitatori esterni al sito.
- **Botnet-other**: comprende cookie e autofill associati ai domini analizzati. Questa suddivisione mira a identificare eventuali tracce di dati sensibili o di accesso a informazioni critiche attraverso dispositivi connessi all'infrastruttura o esterni ad essa.

Parallelamente, un focus è stato rivolto alle numeriche relative ai dispositivi infetti responsabili della **sottrazione di accessi a portali** con mail aziendali, distinguendoli dai dispositivi infetti da cui sono state esfiltrate credenziali di dominio.

Significant institutions analysis

Nel corso dell'analisi condotta sul periodo compreso tra il 2022 e il 2023 è emerso un significativo **aumento nel numero complessivo di dispositivi infetti**, con conseguente esfiltrazione di credenziali sia di utenti interni che esterni alle organizzazioni bancarie analizzate.

Nel dettaglio, concentrandosi sui 51.971 dispositivi infetti da infostealer da cui sono state esfiltrate credenziali, solamente nel 2022 il totale dei dispositivi infetti è stato di 17.350, mentre nel 2023 tale cifra è salita a 26.308. Questo rappresenta un incremento del 51.63%%.

Sul totale dei dispositivi infetti risulta che 1243 (botnet-internal) di questi presentavano credenziali interne. In particolare, come affermato precedentemente, in 712 casi sono state esfiltrate credenziali con e-mail aziendale, mentre dai restanti 531 casi sono state esfiltrate credenziali di dominio Active Directory.

Questo è un dato cruciale, le credenziali di Active Directory sono fondamentali poiché consentono l'accesso e la gestione centralizzata degli utenti in reti aziendali Windows,

controllando l'autenticazione, la sicurezza e l'accesso alle risorse di rete. La loro protezione è fondamentale per prevenire accessi non autorizzati e garantire la sicurezza informatica.

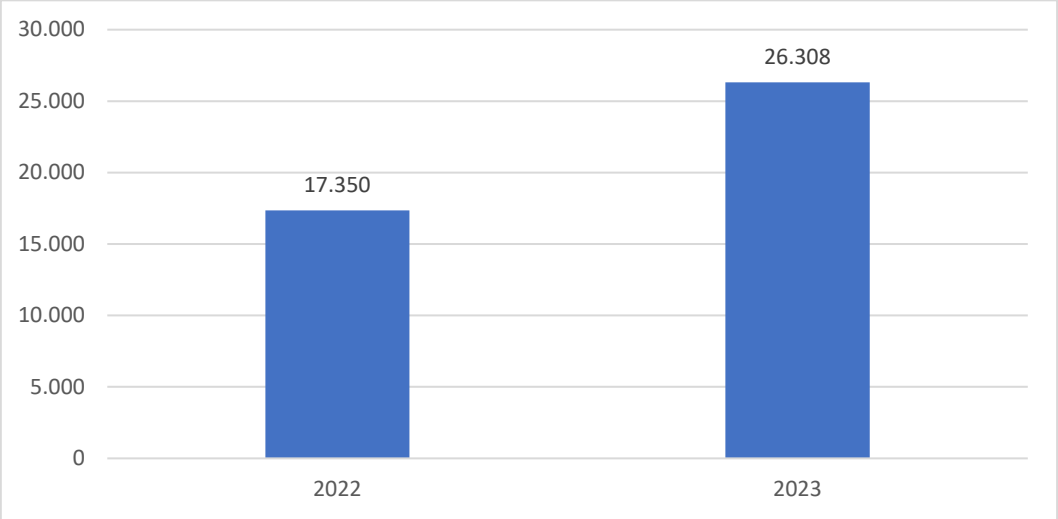

Figure 1: Dispositivi infetti da cui sono state esfiltrate credenziali (2022-2023) - cluster significant

Nel dettaglio, per le 15 *Significant Institution* (SI) analizzate:

- **Una SI non ha alcun dispositivo infetto** da cui sono state esfiltrate credenziali che includono accessi con e-mail aziendale;
- **6 SIs** hanno **tra 1 e 10** dispositivi infetti da cui sono state esfiltrate credenziali che includono accessi con e-mail aziendale;
- **5 SIs** hanno **tra 11 e 50** dispositivi infetti da cui sono state esfiltrate credenziali che includono accessi con e-mail aziendale;
- **3 SIs** hanno **più di 50** dispositivi infetti da cui sono state esfiltrate credenziali che includono accessi con mail aziendale.

Inoltre:

- **3 SIs non hanno dispositivi infetti** da cui sono state esfiltrate credenziali che includono accessi con credenziali di dominio;
- **6 SIs** hanno **tra 1 e 10** dispositivi da cui sono state esfiltrate credenziali che includono accessi con credenziali di dominio;
- **4 SIs** hanno **tra 11 e 50** dispositivi da cui sono state esfiltrate credenziali che includono accessi con credenziali di dominio;
- **2 SIs** hanno **più di 50** dispositivi da cui sono state esfiltrate credenziali che includono accessi con credenziali di dominio.

A seguire la distribuzione delle credenziali associate a diversi portal critici:

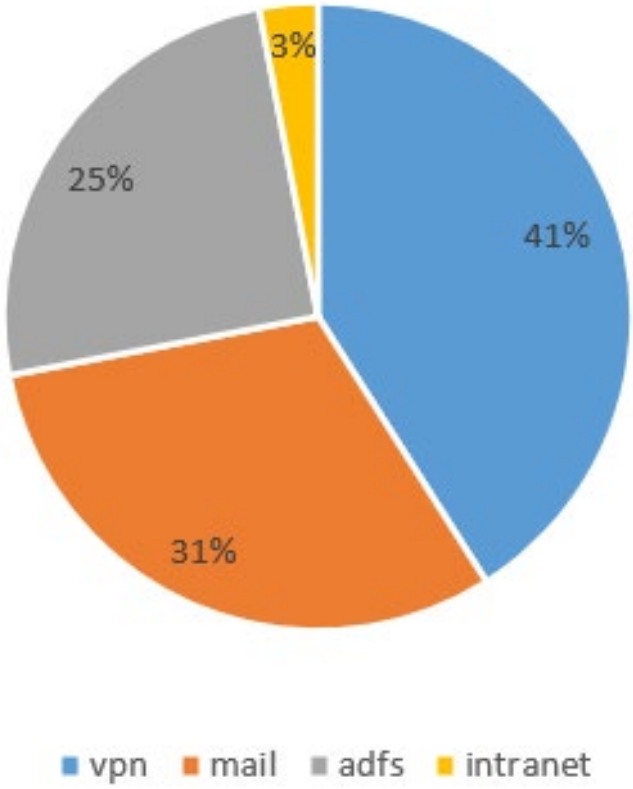

Figure 2: Distribuzione credenziali sottratti su portali critici - cluster significant

Less-significant institutions analysis

L'analisi rivela un totale di **14.184** dispositivi infetti, considerando sia dispositivi interni che esterni che hanno effettuato l'accesso ai portali bancari, nonché dispositivi da cui sono stati esfiltrati cookie e autofill. Affinando ulteriormente l'indagine e focalizzandoci esclusivamente sui dispositivi da cui sono state esfiltrate credenziali, includendo sia clienti che accedono ai portali bancari che dipendenti, il totale dei dispositivi infetti è di **6.539**. Di questi, 187 sono di natura interna (utenti con indirizzi e-mail e utenze di dominio esfiltrate) e **6.352** sono di provenienza esterna.

Di questi 187 casi, sono state esfiltrate 106 credenziali associate ad e-mail aziendali per accedere a portali interni ed esterni alle organizzazioni analizzate, ed 81 utenze di dominio Active Directory.

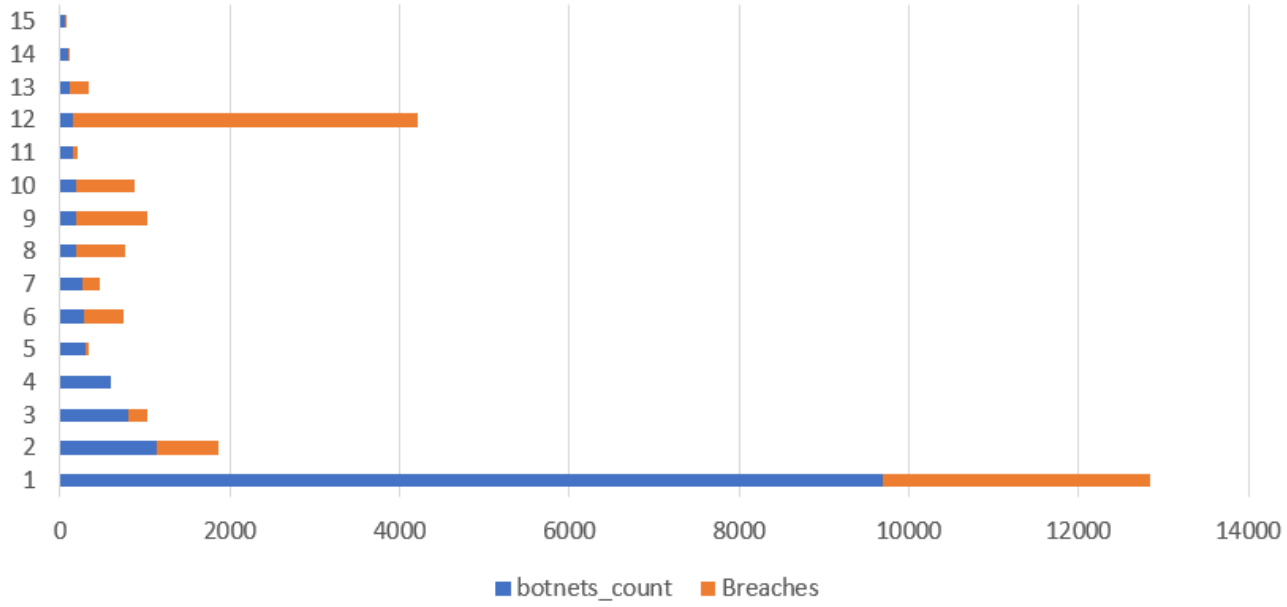

Figure 3: Dispositivi compromessi vs data breaches - cluster less-significant

Concentrandosi sui 6539 dispositivi infetti totali (botnet-internal + botnet external) da cui sono state esfiltrate credenziali, negli ultimi due anni il totale delle credenziali esfiltrate è di 4907 di cui, nel 2022 sono state esfiltrate 2456 crendeziali da InfoStealer mentre, nel 2023, il numero è di 2451.

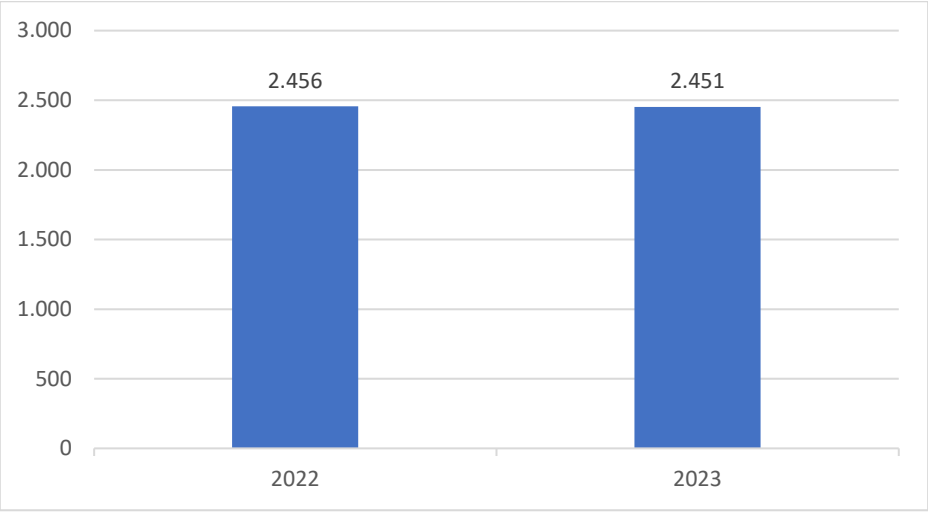

Figure 4: Dispositivi infetti da cui sono state esfiltrate credenziali (2022-2023) - cluster less-significant

Nel dettaglio, per le 15 *Less-Significant Institution* (LSI) analizzate:

- **Un LSI non ha alcun dispositivo infetto** da cui sono state esfiltrate credenziali che includono accessi con mail aziendale;

- **11** LSI hanno **tra 1 e 10** dispositivi da cui sono state esfiltrate credenziali che includono accessi con mail aziendale;
- **3** LSI hanno **tra 11 e 50** dispositivi da cui sono state esfiltrate credenziali che includono accessi con mail aziendale;
- **Nessun LSI ha più di 50** dispositivi da cui sono state esfiltrate credenziali che includono accessi con mail aziendale.

Inoltre:

- **4 LSI non hanno dispositivi infetti** da cui sono state esfiltrate credenziali che includono accessi con credenziali di dominio;
- **8 LSI** hanno **tra 1 e 10** dispositivi da cui sono state esfiltrate credenziali che includono accessi con credenziali di dominio;
- **3 LSI** hanno **tra 11 e 50** dispositivi da cui sono state esfiltrate credenziali che includono accessi con credenziali di dominio;
- **Nessun LSI ha più di 50** dispositivi da cui sono state esfiltrate credenziali che includono accessi con credenziali di dominio.

A seguire la distribuzione delle credenziali associate a diversi portal critici:

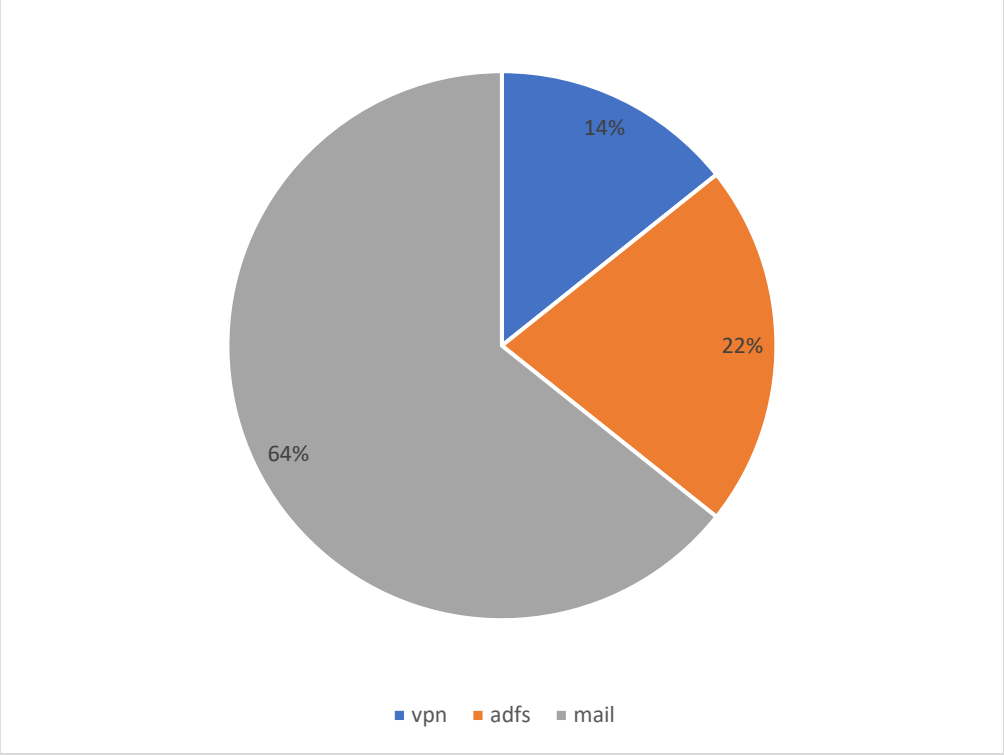

Figure 5: Distribuzione credenziali sottratte su portali critici - cluster less-significant

Breaches & infostealers

Il **totale dei data breach identificati** a partire dal 2016, per il cluster significant, relativi ad utenti interni ammonta a **38.174,** di cui **712** account e-mail compromessi da InfoStealer e **37.462** account e-mail presenti in combolist. È essenziale sottolineare che questo numero include sia gli account aziendali compromessi da infostealer sia la presenza di e-mail aziendali all'interno di combolist. È importante notare che, nel conteggio totale, se un singolo account è presente in più combolist, esso verrà contato più volte.

Nel quadro complessivo dei data breach identificati, emerge un dato interessante. Nel dettaglio, focalizzandoci negli ultimi due anni, sono stati riscontrati 2.042 data breach nel 2023, mentre nel 2022 il numero ammonta a 10.166. Questo si traduce in una differenza percentuale significativa del 79.8%, evidenziando una marcata **diminuzione dei data breach** nel corso del 2023 rispetto al 2022.

Approfondendo ulteriormente l'analisi, emerge che nel corso del 2023 sono state identificate 1.062 e-mail appartenenti ad utenti interni e/o a collaboratori esterni con e-mail aziendale associate ai domini delle banche analizzate all'interno delle combolist, rispetto a un totale di 8.945 nel 2022. Questo si traduce in una differenza percentuale significativa dell'88.1%, indicando una notevole diminuzione del numero di utenze associate a dipendenti e collaboratori all'interno di combolist pubblicate quest'anno rispetto al precedente. Questo porta a pensare che l'attenzione dei Threat Actor si stia spostando verso credenziali esfiltrate da InfoStealer.

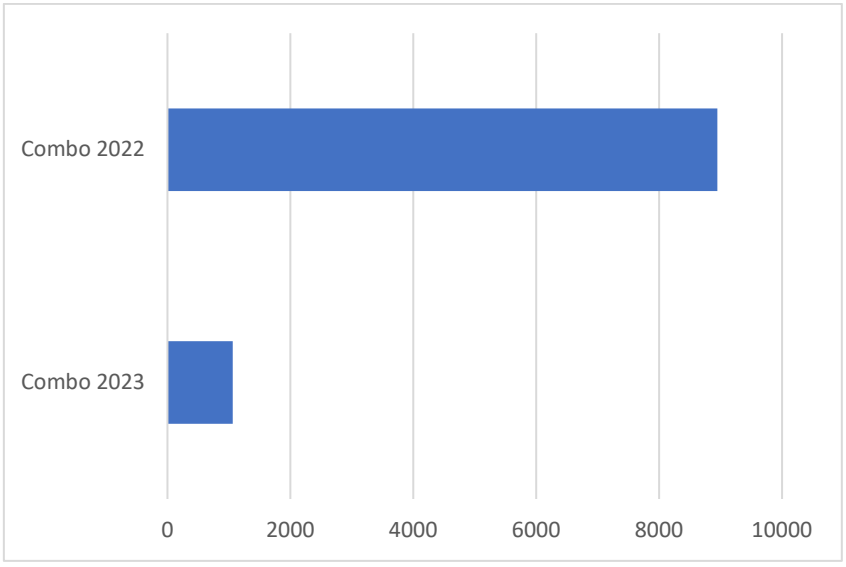

Figure 6: Comparazione presenza di e-mail aziendali delle banche italiane nelle combolist (2022-2023) - cluster significant

La riduzione delle combolist pubblicate può essere interpretata come una variazione strategica da parte degli attaccanti, che trova dimostrazione nel numero crescente di dispositivi infetti da InfoStealer. Infatti, l'analisi che si è focalizzata sulle 15 banche classificate come significant ha identificato un totale di **51.971** (in questo caso il dato si riferisce a *botnet-internal + botnet-external,* mentre precedentemente l'attenzione era stata rivolta al numero dei soli utenti interni) dispositivi infetti da botnet. Va notato che tale numero indica esclusivamente dispositivi infetti dove sono state esfiltrate credenziali escludendo volontariamente i dispositivi da cui sono stati esfiltrati cookie e autofill, per i quali il totale è di **39.622** (classificate dunque come *botnet-other)*, raggiungendo un numero di **91.593** dispositivi compromessi.

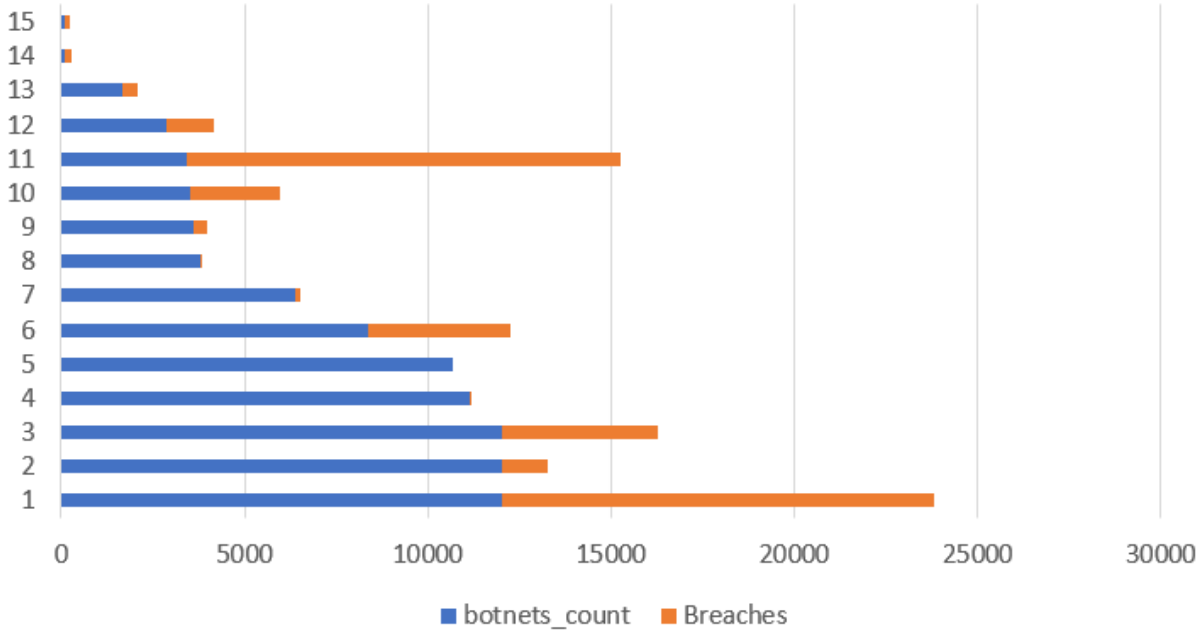

Figure 7: Dispositivi compromessi vs data breaches - cluster significant

Nel contesto dell'analisi delle banche classificate come less significant, emergono alcune dinamiche interessanti. Anche in questo caso l'approfondimento ha evidenziato un'**incidenza maggiore di dispositivi compromessi** da malware di tipo InfoStealer rispetto alla pubblicazione di **combolist**, fenomeno **in decrescita**.

Per le 15 banche analizzate, si è riscontrato un totale di **14.184** dispositivi compromessi che comprendono dunque botnet-internal, botnet-external e botnet-other e 11318 utenti interni inclusi in data breach, dove dunque è stata compromessa l'e-mail aziendale, a partire dal 2016. Un'analisi più dettagliata ha permesso di distinguere tra i dati del 2023 e quelli del 2022, rivelando che 132 di tali breaches appartengono al 2023, mentre 710 sono stati pubblicati nel 2022.

In particolare, anche in questo caso è degno di nota il cambiamento nella pubblicazione di combolist: nel 2023, sono state individuate 86 presenze di utenti interni in combolist, rispetto a 541 nel 2022. Questo rappresenta una significativa diminuzione dell'84.1% nella presenza di e-mail interne o di collaboratori con e-mail aziendali dei domini analizzati all'interno di combolist per il cluster preso in analisi.

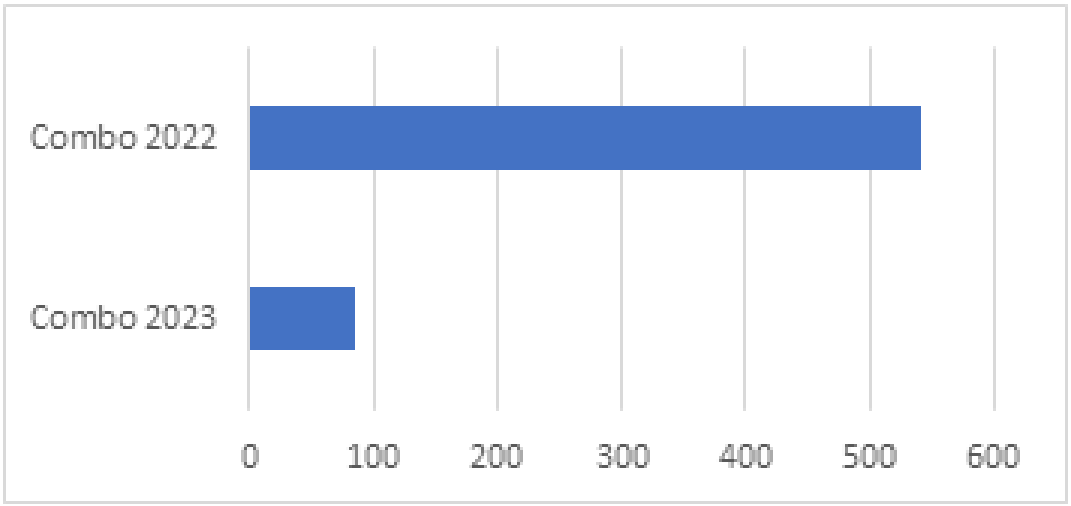

Figure 8: Comparazione presenza di e-mail aziendali delle banche italiane nelle combolist (2022-2023) - cluster less-significant

#2 – TOP 15 InfoStealer families

La seguente analisi fornisce una panoramica dei principali InfoStealer identificati nel contesto dell'analisi condotta. I primi 15 malware che sono stati identificati nel corso dell'analisi sono:

Anubis	Arkei	Azorult	DarkCrystal	Ficker
Krot	LummaC	Nexus	Oski	Predator
Raccoon	RedLine	StealC	Taurus	Vikro

Analizzando le **30** banche prese in considerazione, emerge un totale di **58.510** (tot botnet-internal e botnet-external di *significant* + tot botnet-internal e botnet-external di *less significant*) credenziali esfiltrate collegate ad attività bancarie. Tra questi, i 15 tipi di InfoStealer identificati sono responsabili dell'esfiltrazione di 52.326 credenziali (27.405 solo nel 2023), sia interne che esterne. Le restanti credenziali sono state esfiltrate da InfoStealer la cui famiglia non è stata identificata, riportate nel grafico di seguito come "Other[4]".

[4] "Other" rappresenta le famiglie di InfoStealer al momento non conosciute indefinita le utilizzate per esfiltrare credenziali successivamente pubblicate sul Deep e Dark Web.

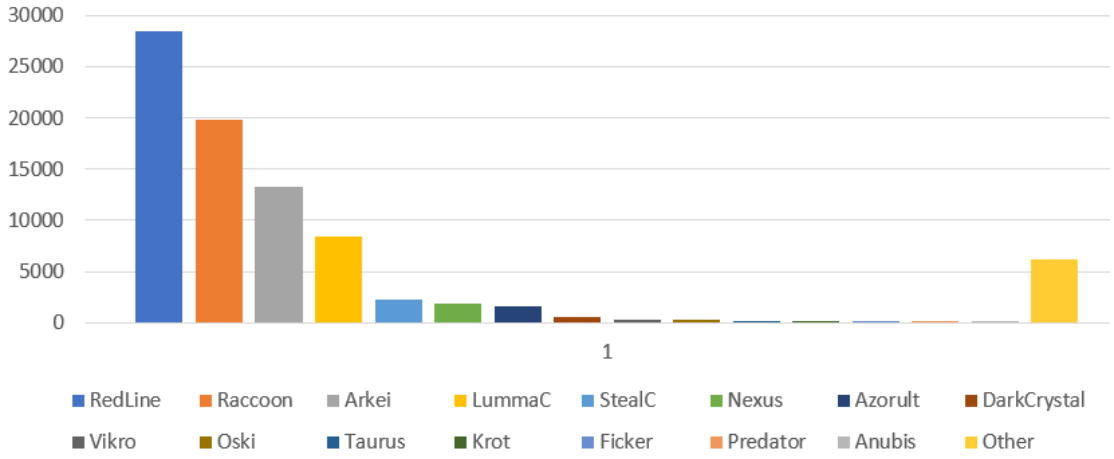

Figure 9: Top 15 identified InfoStealers over the 30 banks under analysis

Focalizzando l'attenzione sul cluster di 15 banche classificate come *significant*, emerge un quadro dettagliato delle esfiltrazioni di dati causate da 15 specifici InfoStealer. Complessivamente, questi malware sono responsabili di 46.692 compromissioni dei dati, di cui 25.054 si sono verificate nel solo anno del 2023.

Al vertice della lista si posiziona Redline, con un totale di 17.257 compromissioni, di cui 9.160 si sono verificate nel 2023. Al secondo posto troviamo Raccoon, con 11.463 compromissioni totali, di cui 7.128 riscontrate nel 2023. Al terzo posto c'è Arkei, con un totale di 9.537 compromissioni, di cui 2.367 nel 2023.

Un elemento interessante è il quarto posto occupato da LummaC nella classifica generale delle banche significant, salendo al terzo posto nel 2023. Un malware comparso quest'anno, che ha totalizzato 4.060 esfiltrazioni per il cluster oggetto dell'analisi. Questo suggerisce una veloce diffusione e un impatto significativo nel breve periodo di osservazione.

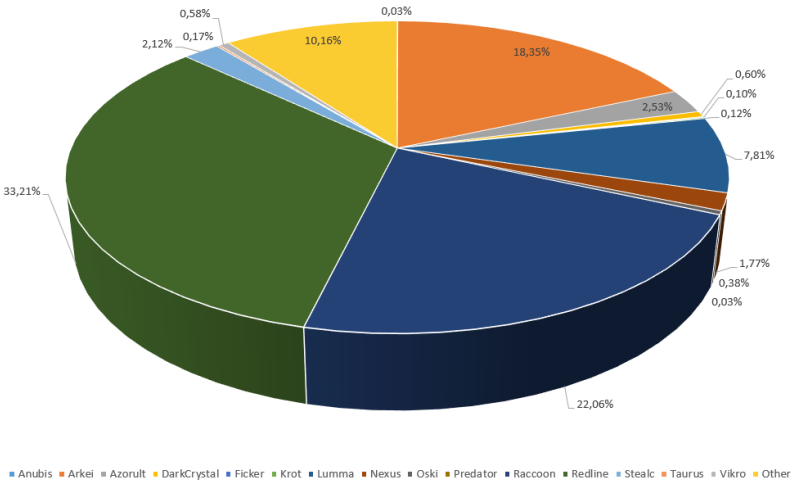

Figure 10: Top 15 identified InfoStealer - cluster significant

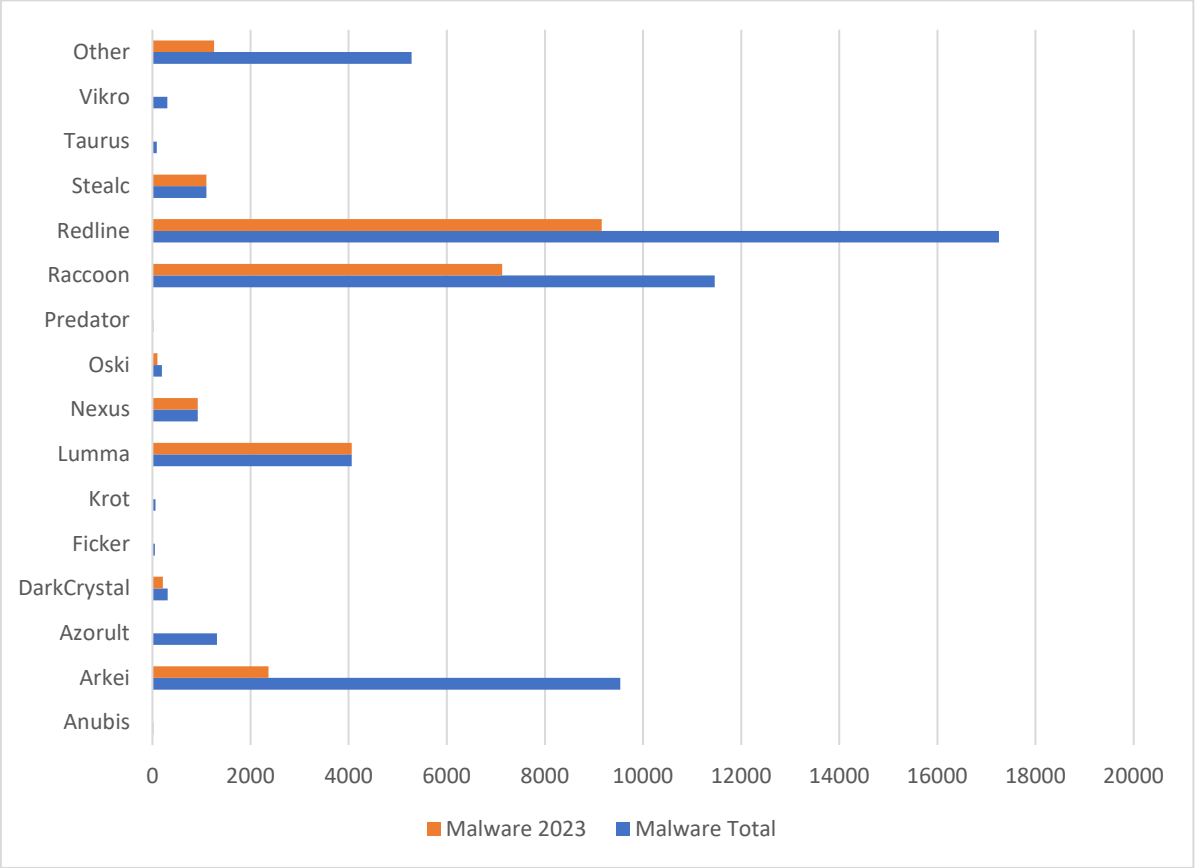

Figure 11: InfoStealer total vs 2023 - cluster significant

Estendendo l'analisi al cluster delle 15 banche classificate come less significant, emerge un quadro simile per quanto riguarda i 15 malware presi in considerazione. Redline mantiene la sua predominanza, occupando il primo posto e risultando responsabile del 37% delle esfiltrazioni totali. Nel dettaglio, Redline ha causato un totale di 2.089 esfiltrazioni, di cui 1.025 sono avvenute nel 2023.

Al secondo e terzo posto nella classifica generale troviamo rispettivamente Arkei (24%) e Raccoon (23%). Focalizzandoci esclusivamente sul 2023, il podio è occupato da Redline, Raccoon, e nuovamente LummaC, con un totale di 327 esfiltrazioni.

Complessivamente, i 15 malware analizzati per il cluster preso in analisi sono responsabili di 5634 compromissioni di cui, 2.351 avvenute nel 2023 (escludendo *botnet-other*) confermando una significativa incidenza delle minacce nel corso dell'ultimo anno.

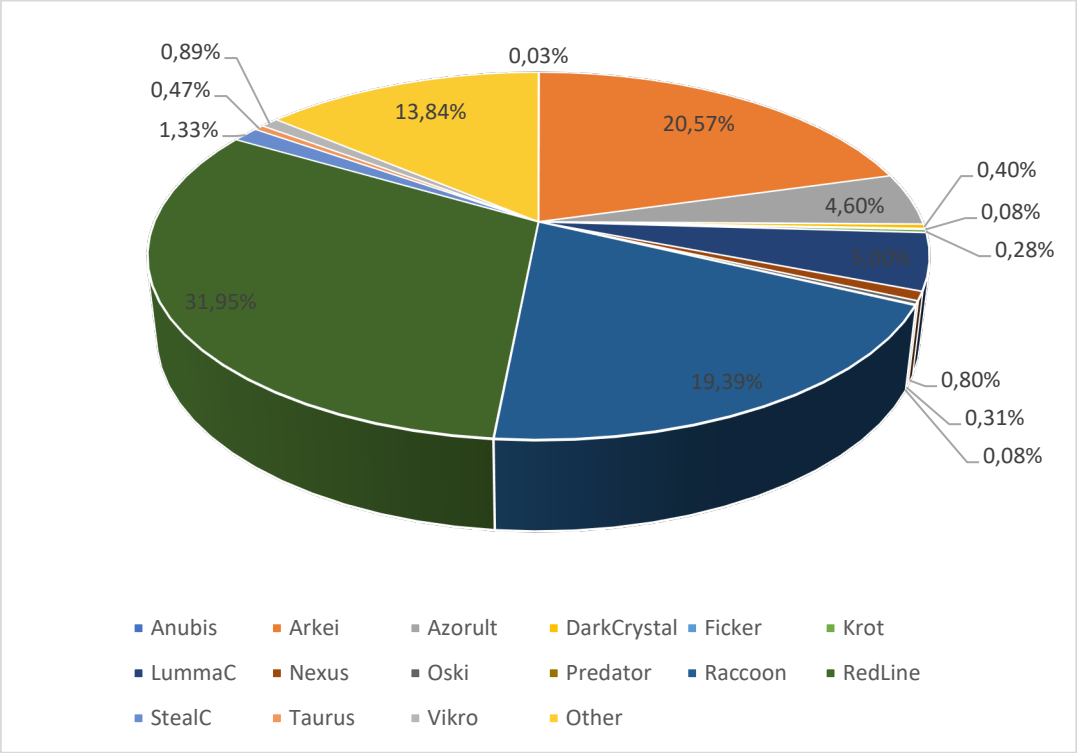

Figure 12: Top 15 identified InfoStealer - cluster less-significant

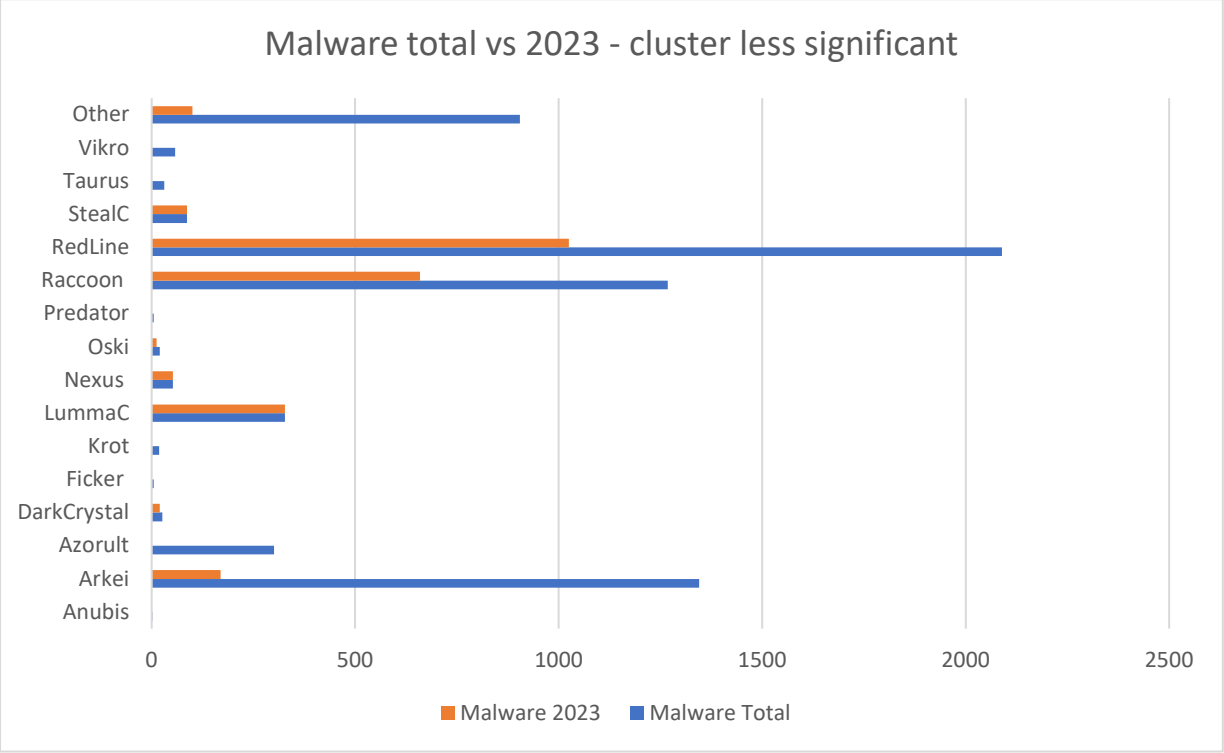

Figure 13: InfoStealer total vs 2023 - cluster less-significant

#3 – InfoStealer presence in the underground ecosystem

I forum underground sono diventati un terreno fertile per la distribuzione di malware, soprattutto gli Infostealer. Tali forum sono spesso frequentati da cybercriminali che cercano di acquistare o vendere malware e/o credenziali di accesso (Initial Access Broker). Difatti negli ultimi anni si è creato un vero e proprio ecosistema criminale basato sulla condivisione di conoscenze, competenze e informazioni.

Ci sono diversi fattori che contribuiscono alla crescente popolarità degli InfoStealer. Uno fra tutti è la facilità di reperire tali prodotti già pronti all'uso. Un altro fattore di rilievo è dovuto alla sofisticazione dei malware, difatti sono in grado di evadere totalmente gli AntiVirus più comuni che possono essere installati sui dispositivi personali facendo di fatto crescere il numero di dispositivi infetti globalmente. Inoltre, sono molteplici i programmatori esperti che offrono le loro competenze per lo sviluppo di InfoStealer custom per andare in contro a tutte le necessità del Threat Actor. Allo stesso tempo sono presenti figure che offrono supporto per tutto ciò che concerne installazione, manutenzione e fornitura di vere e proprie infrastrutture virtuali sui cosiddetti "BulletProof" Hosting Provider.

Malware as a Service: case study

Da quanto osservato nei vari forum underground gli InfoStealer vengono tipicamente venduti sotto forma di subscription, definendo un vero e proprio modello commerciale chiamato "**Malware-as-a-Service**" (MaaS).

Per esempio, per quanto concerne LummaStealer, uno degli InfoStealer più utilizzati nel 2023, sono presenti **diversi tipi di subscription** in base alle necessità dell'utilizzatore:

- Experienced: $250/month;
- Professional: $500/month;
- Corporate: $1000/month.

Il Threat Actor dietro il progetto Lumma fa notare come il malware sia "fully undetectable" e che sia funzionate sia su architetture ARM sia su quelle Intel ponendo quindi anche i nuovi MacOS che girano Windows su ambienti virtuali a rischio.

I thread relativi alla vendita di questi malware sono in continuo aggiornamento, difatti vengono **regolarmente postati gli update del prodotto** comunicando le nuove funzionalità dello stesso (see Figure 14) (e.g., funzionalità di evasion di Windows Defender, esfiltrazione dei cookie relativi agli account Google). Questo tipo di professionalità e livello di servizio può

essere quindi paragonato a quella di un vendor lecito di un qualsiasi prodotto commerciale e legale.

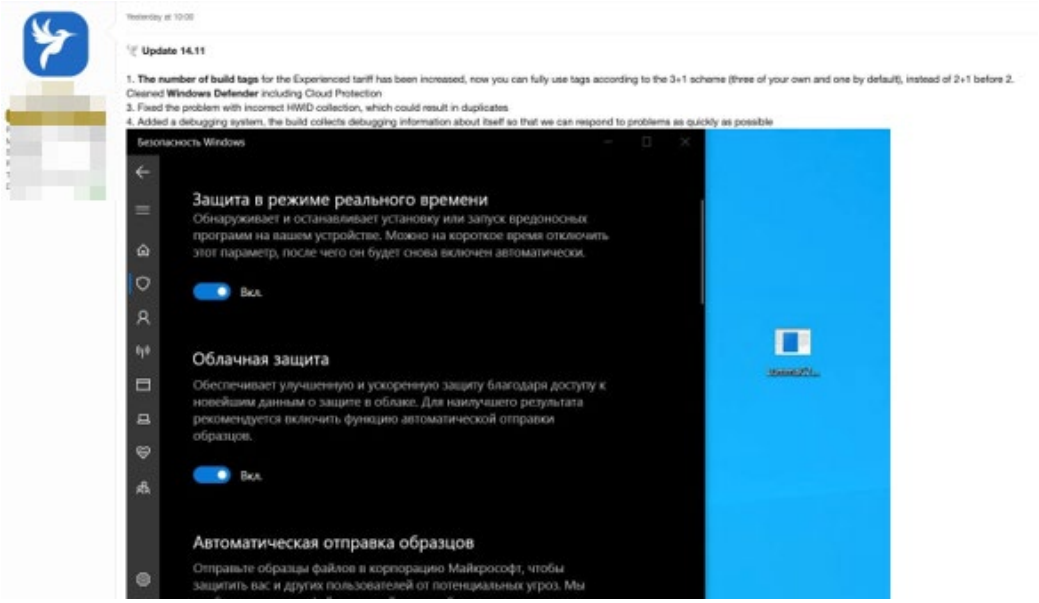

Figure 14: Example of LummaStealer's Windows Defender evasion feature

LummaStealer non è però l'unico InfoStealer di rilievo nel 2023; sono numerose le famiglie di malware che sono in circolazione nei vari forum frequentati da cybercriminali come ad esempio StealC, Meduza Stealer, DanaBot, Silver RAT, Continental Stealer, Se7en, Scarlet Project, Rhadamanthys.

Spesso tali malware vengono distribuiti anche in versioni gratuite e/o crackate. I rischi ovviamente in tali casi son molteplici. Il malware crackato potrebbe contenere un ulteriore malware o backdoor al suo interno infettando di fatto anche i dispositivi dei Threat Actor che lo utilizzano; inoltre, la disponibilità di questi programmi gratuiti mette uno strumento pericoloso in mano ad utenti più o meno esperti aumentando la mole di distribuzione del malware.

Come vere e proprie aziende, tali gruppi di cybercriminali pubblicano post per reclutare nuove leve indicando le skill necessarie per poter presentare la propria candidatura e viceversa. Infatti sono molteplici gli sviluppatori pronti ad offrire le proprie competenze e i propri servizi anche ad eventuali Threat Actor che necessitano di malware custom.

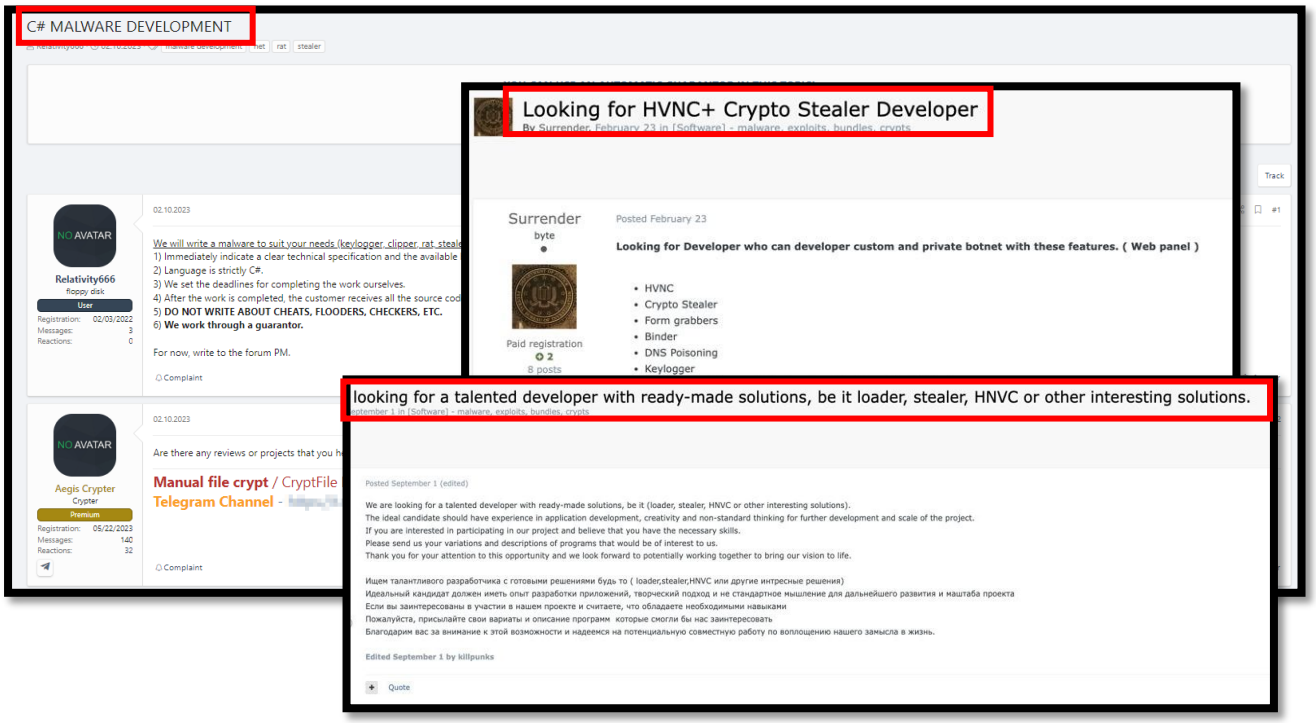

Figure 15: Esempi di post pubblicati su un noto forum underground dove sviluppatori mettono a disposizione le proprie competenze per lo sviluppo di malware

È quindi chiaro che quello dietro gli Infostealer è un vero e proprio ecosistema in continua evoluzione e che nei prossimi mesi è possibile prevedere un loro maggiore utilizzo e diffusione da parte dei Threat Actors.

Next steps

L'analisi del panorama del cyber crime rivela una trasformazione significativa, in cui questo sta diventando sempre più una "commodity". Questo fenomeno può essere attribuito alla sua crescente democratizzazione, resa possibile attraverso l'accesso facilitato a nuovi codici e competenze verticali. In particolare, l'aumento vertiginoso degli "InfoStealer as a service" rappresenta un'evidente manifestazione di questa tendenza. Tale democratizzazione si riflette anche nella sua accessibilità, con una varietà di attori, anche meno esperti, che possono sfruttare queste risorse cyber criminali.

In questo contesto, è prevedibile una possibile impennata nell'utilizzo degli InfoStealer accanto alle campagne di phishing. La combinazione di tecniche come l'ingegneria sociale e l'accesso semplificato a strumenti sofisticati favorirà un aumento nell'efficacia di attacchi mirati, minacciando la sicurezza delle informazioni sensibili.

In sintesi, l'analisi prospetta un futuro in cui i malware di tipo Information Stealer continueranno a proliferare, con una particolare attenzione al 2024.

La prospettiva è decisamente preoccupante, specialmente se guardiamo quanto trascorso con il fenomeno ransomware.

Come è stato possibile osservare, infatti, non sono solo gli InfoStealer as a service ad essere distribuiti, appannaggio dei Criminal Hacker con delle competenze decisamente più basse, ma anche lo stesso codice infrastrutturale degli stessi malware.

Rendere disponibile il codice, come accennato, è stato uno dei fattori scatenanti dell'epidemia ransomware nel triennio 2020/2023.

Un effetto idra, che consente ai threat actor più esperti e skillati di modificare a piacimento infrastrutture già presenti ed in vendita creandone varianti custom più efficaci e soprattutto difficili da tracciare.

Aumenteranno i prodotti in vendita, molto probabilmente, e di conseguenza gli attacchi tramite questo tipo di malware.

Ciò sarà accompagnato da un aumento delle competenze nel Deep e Dark Web, alimentando ulteriormente la diffusione di minacce informatiche. La transizione dalla pubblicazione di combolist alla diffusione di log di InfoStealer indica una mutazione nelle strategie degli attaccanti, richiedendo alle organizzazioni di rafforzare le loro difese. Le crescenti infezioni da InfoStealer, evidenziate nell'analisi, sottolineano l'urgenza di adottare misure di sicurezza avanzate.

Di conseguenza, solo attraverso un approccio olistico alla sicurezza informatica sarà possibile mitigare gli impatti potenzialmente devastanti delle minacce cyber emergenti.

About Us

Swascan è una Cyber Security Company nata da un'idea di Pierguido Iezzi e Raoul Chiesa.

La prima azienda di Cyber Security Italiana proprietaria di una piattaforma di **Cyber Security Testing e Threat Intelligence,** oltre ad un **Cyber Competence Center** premiato con numerosi riconoscimenti nazionali e internazionali dai più importanti player del mercato IT e non solo.

Da ottobre 2020, Swascan è parte integrante di Tinexta Cyber (Tinexta S.P.A), diventando protagonista attiva del primo polo nazionale di Cyber Security: non solo una azienda, ma un gruppo italiano, un nuovo hub nazionale specializzato nei servizi di idetità digitale e sicurezza digitale.

Credits

Analysis by:

Martina Fonzo
Riccardo Michetti

Technical Contributors:

Soc Team Swascan

Editing & Graphics:

Federico Giberti
Melissa Keysomi

Contact Info

Milano
+39 0278620700
www.swascan.com
info@swascan.com
Via Fabio Filzi, 2b, 20063, Cernusco sul Naviglio, MI