TINEXTA CYBER

Panorama delle Minacce Finanziarie

Infostealer

2024

www.tinextacyber.com

Indice

INFOSTEALER

Questo studio si è concentrato su un gruppo di 30 banche precedentemente esaminate, suddivise equamente tra categorie "significative" e "meno significative"21. Il nostro obiettivo principale era identificare i dispositivi compromessi dal malware Infostealer e valutare i rischi associati alle violazioni dei dati. Le discrepanze osservate dall'ultima analisi22 sono preoccupanti.

In questa indagine, abbiamo approfondito le potenziali minacce poste da Infostealer, un tipo di malware progettato per raccogliere informazioni sensibili da sistemi infetti. Tali violazioni possono avere conseguenze molto gravi, potenzialmente causando perdite finanziarie sostanziali e danni alla reputazione per le banche interessate. I nostri risultati evidenziano le crescenti sfide di sicurezza informatica affrontate dalle istituzioni finanziarie e sottolineano l'urgente necessità di misure di protezione migliorate.

Abbiamo anche analizzato l'evoluzione di queste minacce nel tempo e confrontato i dati attuali con i risultati precedenti. L'aumento dei dispositivi compromessi e la gravità delle violazioni indicano una tendenza preoccupante che richiede un'attenzione immediata. Questa analisi mira a fornire una panoramica completa dell'attuale panorama della sicurezza informatica per queste banche e offre raccomandazioni attuabili per mitigare i rischi futuri.

Ulteriori informazioni rilevanti sono disponibili nelle sottosezioni “Extra” di seguito, che includono un’analisi dei vettori iniziali più utilizzati nel primo semestre del 2024.

Approfondimenti degni di nota

Gli Infostealer continuano a essere tra le minacce più significative che le organizzazioni dovranno affrontare nel 2024. Il modello di business dannoso Malware-as-a-Service rende questa categoria di software dannoso uno dei problemi più pervasivi.

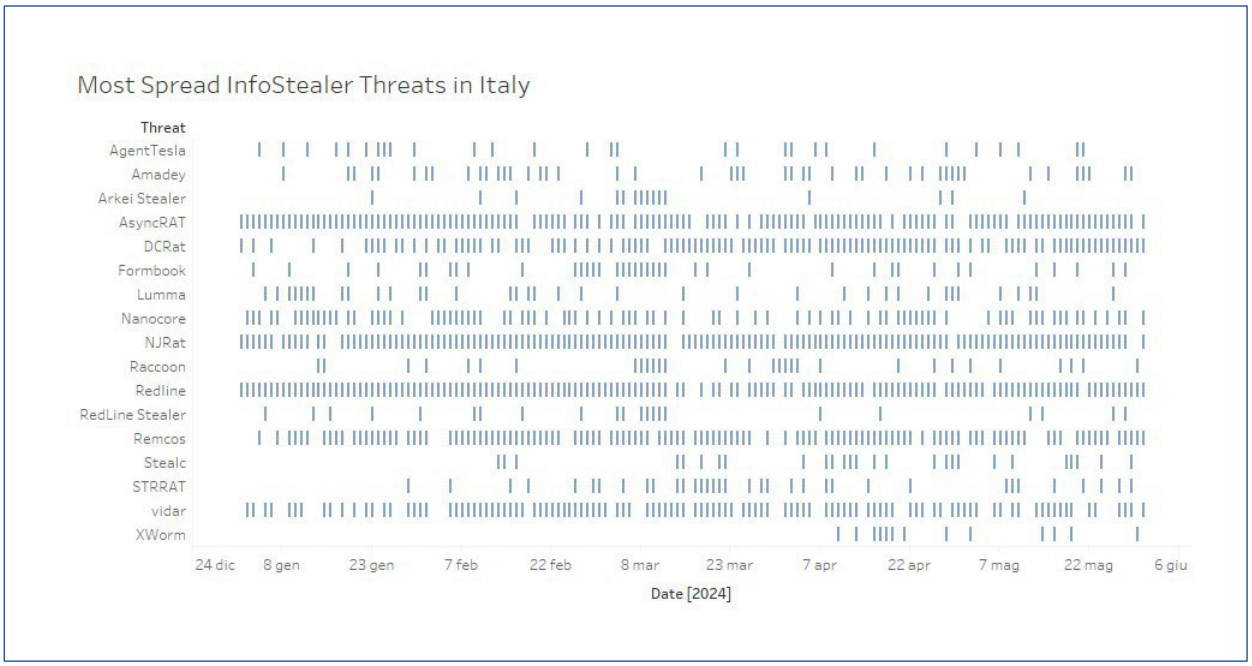

Figura 1: Minacce InfoStealer più diffuse in Italia – dati telemetrici raccolti nel primo semestre del 2024

La figura sopra mostra la telemetria infostealer di Tinexta Cyber, raccolta nella prima metà del 2024. Minacce come AsyncRAT, RedLine Stealer e Vidar sono le più persistenti nel periodo di sei mesi.

Nel corso dei primi tre trimestri del 2023, si è verificata una notevole fluttuazione nel panorama della sicurezza informatica sia per le banche meno significative che per quelle significative: il numero di dispositivi compromessi inizialmente ha mostrato un promettente trend al ribasso, suggerendo misure di sicurezza informatica migliorate o una tregua temporanea dagli attacchi informatici. Tuttavia, questa tendenza si è invertita bruscamente nel quarto trimestre del 2023, indicando un'allarmante impennata di attacchi informatici mirati a queste istituzioni. Questo preoccupante schema è continuato nel primo trimestre del 2024, con dispositivi compromessi che hanno raggiunto un numero sbalorditivo, evidenziando una minaccia persistente e in aumento.

Nel primo trimestre del 2023, le banche "meno significative" hanno segnalato 751 dispositivi compromessi. Il conteggio è sceso a 696 nel secondo trimestre del 2023 e ulteriormente ridotto a 550 nel terzo trimestre del 2023. Tuttavia, la tendenza si è invertita bruscamente nel quarto trimestre del 2023, con il numero di dispositivi compromessi salito a 1676. Il balzo da 550 nel terzo trimestre del 2023 a 1676 nel quarto trimestre del 2023 (un aumento del 205%) è preoccupante e la situazione è peggiorata nel primo trimestre del 2024, con i dispositivi compromessi che hanno raggiunto quota 2200. Ciò rappresenta un aumento del 193% rispetto al primo trimestre del 2023, evidenziando una minaccia continua e crescente alla sicurezza delle banche meno significative. Il costante aumento dei dispositivi compromessi nel quarto trimestre del 2023 e nel primo trimestre del 2024 sottolinea l'aumento dell'utilizzo di InfoStealer da parte degli attori delle minacce.

Durante i primi tre trimestri del 2023, anche le banche "significative" hanno registrato un trend in calo nel numero di dispositivi compromessi. A partire da 7714 dispositivi compromessi nel primo trimestre del 2023, il numero è sceso a 7215 nel secondo trimestre del 2023, per poi scendere bruscamente a 3712 nel terzo trimestre del 2023. Tuttavia, questa tendenza al miglioramento si è invertita nel quarto trimestre del 2023, dove il numero di dispositivi compromessi è salito a 11876. Si tratta di un aumento sostanziale, che ha più che triplicato le cifre del terzo trimestre del 2023, segnando un aumento del 220%. Ciò evidenzia lacune critiche nei protocolli di sicurezza che potrebbero essere state precedentemente trascurate o sottovalutate.

Il numero di dispositivi compromessi è aumentato ulteriormente nel primo trimestre del 2024, raggiungendo un allarmante numero di 24.240. Ciò rappresenta un aumento del 214% rispetto al primo trimestre del 2023 e un aumento del 104% rispetto al quarto trimestre del 2023.

Un aumento così ripido indica la persistenza e la sofisticatezza di questa minaccia informatica. La grande portata dei dispositivi compromessi sottolinea un'urgente necessità di aggiornamenti significativi alle misure di sicurezza informatica esistenti.urgente necessità di aggiornamenti significativi alle misure di sicurezza informatica esistenti.

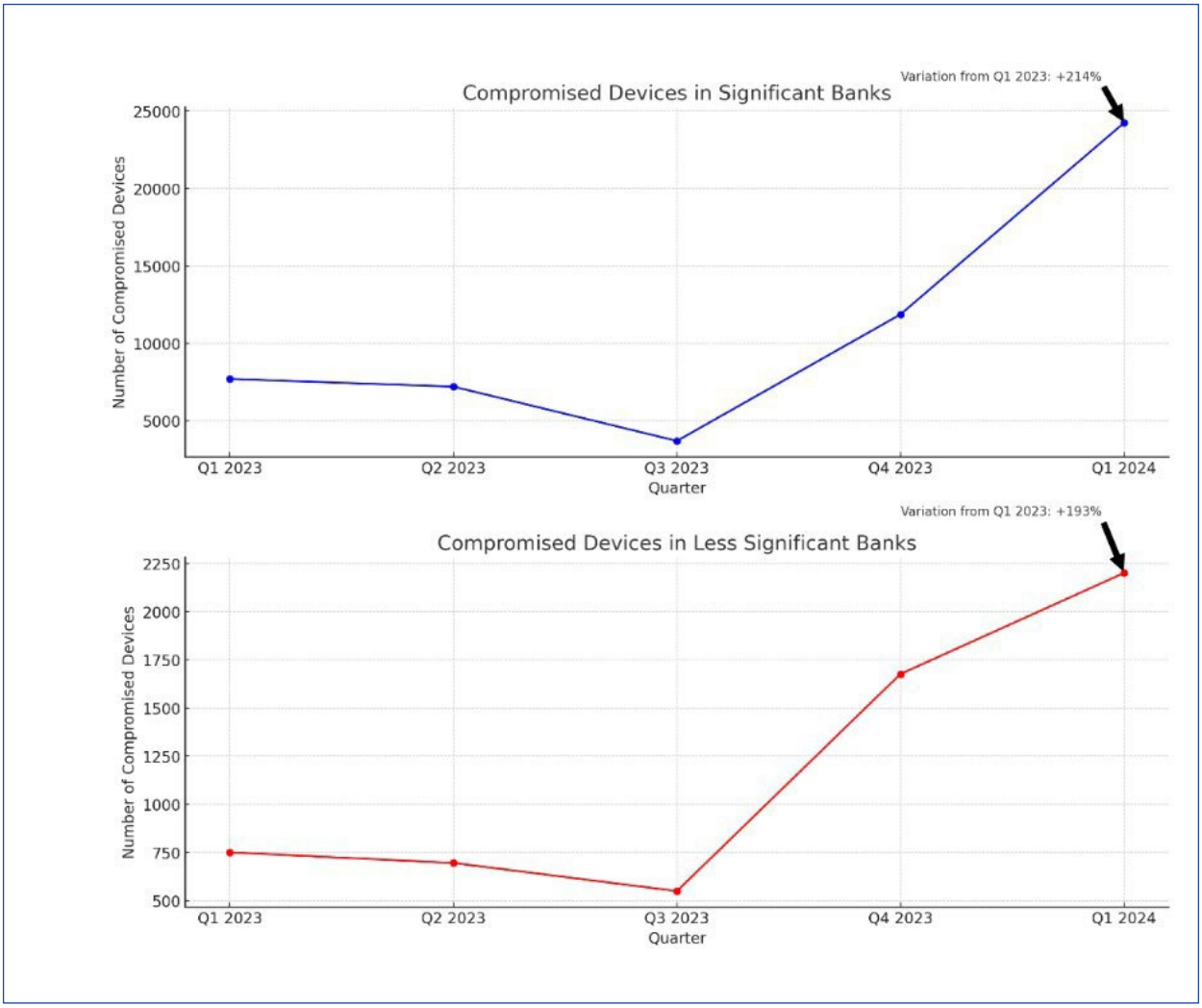

Figura 2: Andamento dei dispositivi compromessi per trimestre (banche significative e meno significative)

Poiché il secondo trimestre del 2024 non si è ancora concluso, ci si è concentrati specificatamente su aprile e maggio. Ad aprile 2023, gli eventi meno significativi erano 143, mentre gli eventi significativi erano 735. Passando a maggio 2023, il numero di eventi meno significativi è aumentato a 297, mentre anche gli eventi significativi hanno registrato un aumento, raggiungendo quota 1391. Entrambe le categorie hanno registrato una crescita, con gli eventi significativi che hanno mantenuto una presenza dominante.

Passando ad aprile 2024, gli eventi meno significativi sono saliti a 275, indicando un leggero aumento rispetto all'aprile precedente. Tuttavia, gli eventi significativi sono saliti alle stelle a 3087, segnando un aumento sostanziale di eventi degni di nota.

Infine, a maggio 2024, gli eventi meno significativi sono scesi a 106, mentre gli eventi significativi sono rimasti relativamente alti, attestandosi a 1114.

Sia le banche più importanti che quelle meno importanti hanno registrato un aumento sostanziale dei dispositivi compromessi, in particolare verso il quarto trimestre del 2023 e il primo trimestre del 2024. Il drammatico aumento dei dispositivi compromessi per le banche più importanti suggerisce una minaccia grave e crescente, che richiede misure di sicurezza informatica immediate e migliorate.

I dati dettagliati sulle tendenze delle 30 banche analizzate rivelano diversi rischi critici:

1. Elevata suscettibilità agli attacchi informatici su larga scala: i drammatici aumenti dei dispositivi compromessi nel Q4 2023 e nel Q1 2024 indicano una vulnerabilità significativa agli attacchi informatici su larga scala. Ciò suggerisce che le misure di sicurezza informatica esistenti potrebbero non essere sufficientemente robuste per gestire minacce sofisticate e persistenti.

2. Impatto operativo e finanziario: ripetute e gravi violazioni possono interrompere le operazioni bancarie, portare a significative perdite finanziarie e minare la fiducia dei clienti. Il risultato potrebbe essere un danno reputazionale a lungo termine, che incide sulla posizione di mercato della banca e sulla fedeltà dei clienti.

3. Sfide di conformità normativa: data la crescente attenzione normativa sulla protezione dei dati, la mancata protezione delle informazioni dei clienti potrebbe comportare sanzioni sostanziali, conseguenze legali e un maggiore controllo da parte degli enti normativi

TECNICHE DI DISTRIBUZIONE PIÙ UTILIZZATE NEL 2024

Piattaforme di social media

Snake InfoStealer, un nuovo malware basato su Python, si sta diffondendo tramite messaggi di Facebook. Sfrutta tattiche di ingegneria sociale, inviando link dannosi tramite chat che, se cliccati, scaricano il malware sul sistema della vittima. Questo metodo sfrutta la fiducia che gli utenti ripongono nei loro contatti sui social media, rendendolo un efficace vettore di distribuzione.

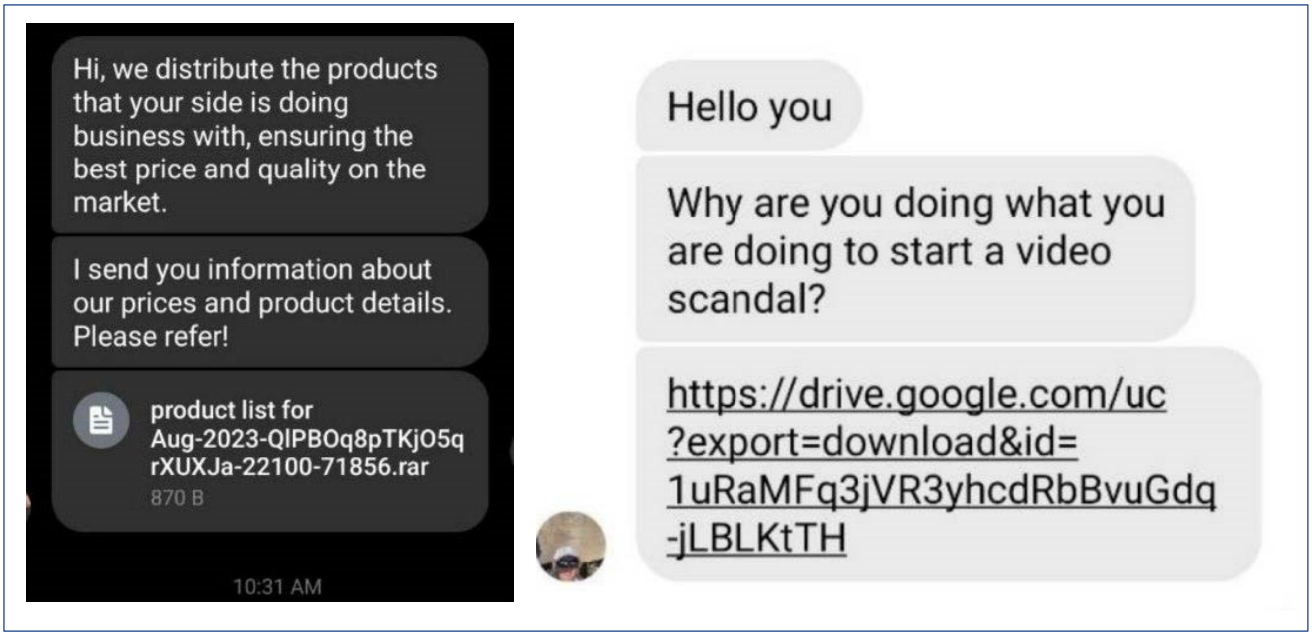

Figura 3: Malware distribuito tramite chat di Facebook

Repository di pacchetti dannosi

Negli ultimi sviluppi della sicurezza informatica, gli autori delle minacce hanno adottato un approccio nuovo e insidioso per distribuire malware, fingendosi collaboratori utili su Stack Overflow. Questo metodo sfrutta la fiducia e la credibilità della piattaforma della community degli sviluppatori per propagare codice dannoso. I criminali informatici si infiltrano nelle discussioni in cui gli utenti cercano consigli di programmazione, offrendo soluzioni apparentemente legittime che contengono payload dannosi incorporati. Questa tattica è particolarmente preoccupante in quanto prende di mira direttamente sviluppatori e ambienti aziendali, espandendo la portata delle minacce infostealer oltre la tipica base di utenti finali.

Figura 4: Distribuzione del malware tramite Stack Overflow

Il processo inizia solitamente quando un utente posta una domanda relativa a problemi di programmazione. Gli attori malevoli rispondono con frammenti di codice o link a repository, che sembrano essere soluzioni pratiche. Tuttavia, queste risposte sono sapientemente concepite per includere pacchetti dannosi. Una volta che uno sviluppatore incorpora questi suggerimenti nei propri progetti, il codice malevolo viene eseguito, spesso senza essere rilevato, portando all'installazione di infostealer come il malware Whitesnake.

Prendendo di mira gli sviluppatori, gli aggressori mirano a compromettere i sistemi che contengono codice critico e segreti aziendali, rappresentando una minaccia significativa per la sicurezza aziendale. Questa tendenza sottolinea l'evoluzione

panorama delle minacce in cui gli infostealer non si limitano più a colpire singoli utenti finali, ma si concentrano sempre più su obiettivi di alto valore all'interno di reti aziendali e ambienti di sviluppo.

Le implicazioni di questo cambiamento sono profonde e richiedono una maggiore vigilanza e misure di sicurezza avanzate all'interno degli ecosistemi aziendali e di sviluppo. Gli sviluppatori devono prestare attenzione quando integrano codice esterno e le organizzazioni devono implementare protocolli di sicurezza robusti per rilevare e mitigare tali minacce. La natura ingannevole di questi attacchi evidenzia la necessità di formazione e consapevolezza continue per proteggersi dai metodi sofisticati impiegati dai criminali informatici.

Ad esempio, WhiteSnake InfoStealer è stato distribuito tramite pacchetti dannosi caricati sul Python Package Index (PyPI). Questi pacchetti sono camuffati da librerie software legittime, ma contengono malware nascosti che infettano i sistemi al momento dell'installazione.

Di seguito un esempio del contenuto di un pacchetto PyPI dannoso in cui vengono recuperati i portafogli crittografici:

```
BTC = 'bc1qfy6lzwj8jcsl3x8kxccdvxzu0tmadmqshtqrxq' # Bitcoin
ETH = '0x985e5bb5BED55522DAc8Dae842b6647cD004149B' # Ethereum
ETHBEP2 = '' # Ethereum BEP-2
LTC = 'LdpfjshytTLYGynXxPvW73UyzMdMsBt1zf' # Litecoin
DASH = 'Xn5AMJ3jdz6ujgdveAWhDs5A5xwqSFupmg' # Dash
DOGE = 'DLeNR8mFCRnUW1riwSFSRs148cEsv1VmZE' # Dogecoin
RIPPLE = 'rwkw8TGegyDXT3KzkymitPCK54cbXiht9f' # Ripple
TRON = 'TGUoQnZi5SS2ZQuZwAeaU86wpYhqm2TcYB' # Tron
BTCCASH = 'bitcoincash:qql9le2pdg0szwgrslacf454fanvkwqj9vre3upt3g' # Bitcoincash
```

Figura 5: Esempio di pacchetto PyPI dannoso in cui vengono recuperati i portafogli crittografici

Malvertising e avvelenamento SEO

I criminali informatici hanno sempre più sfruttato l'avvelenamento SEO e Google Ads per distribuire infostealer, sfruttando la fiducia che gli utenti ripongono nei risultati di ricerca principali e nelle pubblicità dall'aspetto legittimo. Manipolando le classifiche dei motori di ricerca e inserendo annunci dannosi, indirizzano gli utenti verso siti Web ingannevoli progettati per assomigliare a siti di download di software autentici. Questa tattica è particolarmente insidiosa perché si integra perfettamente in una normale esperienza di navigazione Web, rendendo difficile per gli utenti discernere la minaccia. Per mitigare queste minacce, gli utenti devono essere vigili e le organizzazioni dovrebbero migliorare le loro misure di sicurezza informatica per rilevare e bloccare tali attività dannose.

Di seguito un esempio di un sito web antivirus falso che sfruttava questa tecnica per diffondere il malware InfoStealer.

Figura 6: Sito Web antivirus falso sfruttato per distribuire InfoStealer

Software craccato e YouTube

RisePro Info Stealer viene distribuito tramite software craccato disponibile su GitHub. Gli utenti che cercano di scaricare software senza pagarlo sono allettati dalla promessa di software gratuito, seppur illegale, che a sua volta infetta i loro sistemi con malware.

I criminali informatici usano YouTube anche per promuovere software craccato, incorporando link a download dannosi nelle descrizioni dei video. Questo metodo prende di mira gli utenti che cercano soluzioni software gratuite, portandoli a installare inavvertitamente InfoStealer come Lumma Stealer.

Fonti

• https://x.com/idclickthat/status/1692210489663905972?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1692210489663905972%7Ctwgr%5E954f3f8835db331294a-40aae7a%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fsecurityaffairs.com%2F160131%2Fmalware%2Fsnake-info-stealer.html&mx=2

• https://swascan.com

• https://yoroi.company

• https://www.fortinet.com/blog/threat-research/info-stealing-packages-hidden-in-pypi

• https://www.sonatype.com/blog/pypi-crypto-stealer-targets-windows-users-revives-malware-campaign

• https://www.trellix.com/blogs/research/a-catalog-of-hazardous-av-sites-a-tale-of-malware-hosting/

CREDITI

Collaboratori:

Riccardo Michetti
Riccardo D'Ambrosio
Fabrizio Rendina
Martina Fonzo
Luigi Martire

Editing e grafica:

Federico Giberti
Melissa Keysomi

Informazioni di contatto

www.tinextacyber.com
info@tinextacyber.com

Milano
Edificio Vetra, Via Fernanda Wittgens, 2, 20123
+ 39 02 6666 1442