RedHot Cyber

WWW.REDHOTCYBER.COM

La cybersecurity è condivisione.
Riconosci il rischio, combattilo,
condividi le tue esperienze ed
incentiva gli altri a fare meglio di te.

Infostealer: un pacco da Babbo Natale… con dentro le tue password

Edited by DarkLab

DARKLAB
RHC INTELLIGENCE LABORATORY

DARKLAB E' UN SOTTO GRUPPO DELLA COMMUNITY DI RED HOT CYBER SPECIALIZZATO AL MONITORAGGIO DELLE MINACCE INFORMATICHE.

Dark Lab nasce con l'obiettivo principale di diffondere la conoscenza sulle minacce informatiche per migliorare la consapevolezza e le difese digitali del paese.

INTRODUZIONE

Babbo Natale è in sciopero. Quest'anno invece di portar regali, si prende il tuo Wi-Fi, la tua carta di credito e, già che c'è, anche le tue password. D'altronde perché limitarsi a regali tangibili quando si può rubare l'identità digitale con stile? Benvenuti nell'era degli infostealer, pronti a svuotarti la tua vita digitale mentre sei distratto a scegliere il maglione natalizio più kitsch.

Immagina la scena: una mail con l'offerta di un iPhone gratis. Lo clicchi (dai, ammettilo, chi non lo farebbe?), e puff: i tuoi dati finiscono su un server remoto pronti ad essere venduti al miglior offerente o, peggio, usati per devastare il tuo conto in banca. Il bello è che chi ti ha colpito potrebbe essere un criminale esperto... o un dilettante con un malware da quattro soldi acquistato su qualche oscuro angolo del dark web. Insomma, il crimine digitale non ha più bisogno del genio alla Mr. Robot: basta una connessione e un po' di faccia tosta.

E mentre noi ci destreggiamo tra regali e cene in famiglia, i cybercriminali affinano le loro tecniche trasformando ogni clic maldestro in una porta d'accesso ai nostri dati. Le conseguenze? Aziende in ginocchio, clienti che fuggono e un "Buon Natale" che suona più come una beffa.

Ma c'è speranza. Possiamo difenderci.

No, non parliamo di un antivirus dell'anteguerra o di sacrificare il panettone per risparmiare sui backup. Parliamo di strategia, consapevolezza e, perché no, un pizzico di astuzia. Perché se gli infostealer sono la minaccia delle feste noi possiamo diventare il loro peggior incubo. Preparati, dunque, a scoprire come trasformare la tua sicurezza digitale in un fortino inespugnabile. Dopo tutto, Natale è anche il momento perfetto per regalarsi un po' di serenità digitale.

INDICE DEI CONTENUTI

PREFAZIONE

Initial access brokers, malware as a service, trojans, spyware, credential theft, keyloggers, botnets, command and control servers, Social Engineering, Threats to data Denial of Service (DDoS) attacks, Information manipulation, Ransomware, Supply chain attacks, la famigerata darknet.

Tutte queste realtà, apparentemente eterogenee ma ugualmente affascinanti, condividono un elemento comune: il loro legame intrinseco con il furto di informazioni. Si tratta di minacce cibernetiche in continua evoluzione, sostenute da attori malevoli sempre più sofisticati, determinati a sfruttare ogni vulnerabilità disponibile.

Negli ultimi decenni, il panorama delle minacce cibernetiche si è evoluto rapidamente, diventando sempre più complesso e sofisticato. Dalle prime forme di malware *(Vedi appendice "Origine ed evoluzione delle minacce informatiche"),* create per scopi di ricerca o sperimentazione, siamo passati a strumenti malevoli utilizzati per obiettivi criminali, geopolitici e finanziari. Oggi, termini come ransomware, spyware, botnet e phishing sono entrati nel vocabolario comune, rappresentando una costante minaccia per individui, aziende e governi.

Questa evoluzione non riguarda solo la tecnologia, ma anche le strategie e i modelli di business dietro gli attacchi, dimostrando come il cybercrimine sia diventato una vera e propria industria globale.

Malware è una parola che deriva dalla combinazione di due parole, "malizioso" e "software". La semplice definizione che si può ricavare da questo è che qualsiasi software che esegue attività dannose può essere considerato malware. Esistono diversi tipi di malware in base al loro comportamento.

Quando sentiamo parlare di Virus e malware, spesso si usano le due parole in modo intercambiabile, ma non è così. I virus esistono da decenni ed hanno attirato una forte attenzione mediatica negli anni ‘90 quando internet è diventato commerciale ed il suo utilizzo nei PC domestici ha iniziato a farsi strada. Di fondamentale comprensione sono le definizioni, sappiamo che tutti i virus sono malware ma non tutti i malware sono virus. Dato l’enorme quantità di programmi indesiderati esistenti essi sono raggruppati in diverse categorie per facilitare e comprenderne la funzione e le caratteristiche.

Alcune di queste categorie includono:

- **adware**, progettato per fornire pubblicità
- **backdoor**, metodi per ottenere un accesso non autorizzato a un sistema
- **bot**, abbreviazione di robot , sono programmi che eseguono un compito specifico o operano in un modo che simula l'attività umana

- **browser hijacker,** chiamato anche virus di reindirizzamento del browser, è un malware che impatta sulle impostazioni del browser web di un utente e forza fraudolentemente il browser a reindirizzare a siti web che l'utente non intende visitare. Spesso, i siti web a cui un browser hijacker reindirizza gli utenti sono dannosi
- **exploit,** sono progettati per sfruttare le vulnerabilità del sistema, come una falla di sicurezza in un sistema operativo
- **password stealer e monitoring Tools,** sono utilizzati per monitorare il tuo sistema e registrare informazioni sulle tue attività
- **ransomware**, è un tipo di software dannoso che impedisce l'accesso o esegue altre azioni che bloccano il computer o i dispositivi o crittografano i dati, tenendo essenzialmente in ostaggio il computer/i dati finché non paghi il creatore del malware per liberarlo
- **rootkit/bootkit,** Il termine Rootkit è la combinazione delle parole Root, "Amministratore" e "Kit", che indica un pacchetto di strumenti software. Quindi un rootkit è un set di strumenti che fornisce a qualcuno i privilegi più elevati in un sistema. Un bootkit è un tipo di infezione dannosa che prende di mira il Master Boot Record situato sulla scheda madre fisica del computer. Le infezioni ad bootkit sono in calo grazie alla crescente adozione si S.O. e hardware che utilizzano tecnologie UEFI e Secure Boot
- **scareware**, è un malware progettato per spaventarti e farti visitare siti web che installeranno altri software dannosi, o cerca di convincerti ad acquistare software per rimuovere virus o altre minacce che in realtà non esistono sul tuo sistema;
- **spyware**, è un software progettato per monitorare le tue attività e segnalarle in qualche modo
- **trojan horse (o trojan),** è un software dannoso che si nasconde all'interno o si camuffa da programma, documento o altro file apparentemente innocuo
- **keylogger,** piccole applicazioni che risiedono su un computer per registrare i tasti premuti
- **worm,** sono un altro tipo comune di malware e possono causare seri problemi a computer e reti. Sono autoreplicanti e possono riempire la memoria del computer e/o consumare larghezza di banda su una rete, causando problemi di prestazioni ed errori.

Quindi Malware è una versione abbreviata del termine software dannoso. Il Free Online-Dictionary of Computing definisce il malware come "Qualsiasi software progettato per fare qualcosa che l'utente non vorrebbe che facesse, non gli

ha chiesto di fare e spesso non ne è a conoscenza fino a quando non è troppo tardi».

Pertanto, quando ci si pone la domanda "Cosa rende un software dannoso" sappiamo che il software diventa malware in base all'intento del creatore, se chi lo crea vuole che faccia qualcosa di buono o di cattivo. Il software che fa qualcosa di cattivo è noto come malware.

- **Ransomware:** questa minaccia continua a essere una delle più critiche. Gli attaccanti criptano i dati delle vittime e chiedono un riscatto per ripristinarne l'accesso. Le tecniche di estorsione si sono evolute, includendo la minaccia di divulgare pubblicamente i dati se il riscatto non viene pagato.
- **Malware:** il malware rimane una costante minaccia alla sicurezza dei dati. L'evoluzione del Malware-as-a-Service (MaaS) ha reso possibile anche ai criminali meno esperti di lanciare attacchi sofisticati. Questo modello di business permette di acquistare e distribuire malware personalizzati, aumentando la diffusione di attacchi.
- **Ingegneria sociale:** tecniche come il phishing e lo spear-phishing sfruttano la componente umana per indurre errori e violare sistemi altrimenti ben protetti. Questi attacchi sono sempre più sofisticati e difficili da rilevare.
- **Minacce ai dati:** le violazioni dei dati sono una delle maggiori preoccupazioni per le aziende. Errori umani, configurazioni errate e attacchi mirati sono tra le cause principali di queste violazioni.
- **Attacchi DDoS:** gli attacchi Denial of Service mirano a interrompere la disponibilità di servizi critici, causando interruzioni significative per le aziende.

L'evoluzione dei malware è particolarmente interessante. In passato, i malware erano spesso semplici virus o trojan progettati per danneggiare o rubare dati. Oggi, i malware sono diventati strumenti complessi e multifunzionali. Ad esempio, i ransomware non solo criptano i dati, ma possono anche rubare informazioni sensibili prima di bloccarle. Inoltre, il Malware-as-a-Service ha abbassato la barriera d'ingresso per i cybercriminali, permettendo a chiunque di lanciare attacchi sofisticati senza necessitare di competenze tecniche avanzate.

La crescente sofisticazione delle minacce richiede un approccio proattivo alla cybersecurity, con investimenti in tecnologie avanzate di rilevamento e formazione continua del personale per riconoscere e mitigare le minacce.

Gli infostealer sono una categoria di malware progettata per rubare informazioni sensibili dai dispositivi infetti. Questi malware possono sottrarre dati come credenziali di accesso, informazioni finanziarie, cookie di sessione e altri dati personali.

GLI INFOSTEALER

I VERI PREDATORI DIGITALI

Gli infostealer raccolgono ed esfiltrano i dati attraverso l'ausilio di una serie di tecniche

- **Keylogging:** registrano tutto ciò che digiti sulla tastiera, catturando password, numeri di carte di credito e altre informazioni sensibili.
- **Form Grabbing:** intercettano i dati che inserisci nei moduli web prima che vengano criptati e inviati al server, rubando così credenziali di accesso e dettagli di pagamento.
- **Cookie Theft:** rubano i cookie di sessione dai browser, permettendo agli attaccanti di accedere ai tuoi account senza bisogno di password e bypassando MFA tramite tecniche di hijacking.
- **Email:** gli attaccanti inviano i dati raccolti a indirizzi email controllati da loro, spesso usando tecniche di offuscamento per evitare il rilevamento.
- **Upload su Server Remoti:** i dati vengono caricati su server remoti controllati dagli attaccanti, spesso attraverso protocolli sicuri come HTTPS per evitare il rilevamento.

Anni 2010 e oltre: Raffinatezza tecnologica e professionalizzazione degli attacchi.

Gli infostealer sono particolarmente pericolosi perché operano in modo discreto e possono raccogliere una vasta gamma di informazioni sensibili.

La difficoltà nel rilevarli e la potenziale perdita di dati critici possono causare gravi danni economici e reputazionali alle vittime.

Nel corso dell'ultimo decennio gli infostealer hanno fatto una metamorfosi degna di un Pokémon: da semplici larve di malware a predatori ben strutturati e letali. Tra il 2013 e il 2016 erano i bravi scagnozzi dei trojan bancari come Zeus, impegnati a raccogliere credenziali finanziarie come un contabile zelante. All'epoca gli antivirus dormivano sonni tranquilli, facilmente aggirati con il vecchio trucco dell'offuscamento del codice: "Non mi vedi, non mi prendi!"

Poi è arrivato il 2017 e tutto è cambiato. Con il modello "Malware-as-a-Service" (MaaS), gli infostealer sono diventati l'equivalente digitale dei noodles istantanei: economici, pronti all'uso e disponibili per chiunque, anche per gli aspiranti hacker della domenica. Strumenti come Azorult e RedLine hanno ampliato il loro menù, prendendo di mira non solo i conti bancari ma anche i social, le email e persino i portafogli di criptovalute. È stata l'età d'oro dei ladri digitali, complice anche il boom delle criptovalute, con il Bitcoin che passava da 1.000 $ a 7.000 $ in pochi anni: come resistere?

.

Nel 2020-2021 la pandemia ha trasformato il lavoro da remoto in un parco giochi per i cyber criminali. Mentre noi imparavamo a usare Zoom loro perfezionavano strumenti come Raccoon e Vidar, progettati per aggirare i sistemi EDR e sfruttare la confusione generale. Phishing e software pirata? Sempre in voga. E così hanno continuato a mietere vittime tra un allegato malevolo e un plugin vulnerabile.

E dal 2022? Beh, qui entrano in scena i superpoteri dell'intelligenza artificiale. Gli infostealer di ultima generazione sono diventati dei veri trasformisti: possono usare l'AI per creare messaggi di phishing irresistibili o per mascherare meglio le loro attività. Nel frattempo, non si accontentano più di PC e laptop: ora puntano anche a dispositivi mobili e architetture ARM, ampliando il loro arsenale per diventare il terrore trasversale del panorama digitale

In sintesi gli infostealer non solo sono cresciuti ma si sono anche adattati con un tempismo perfetto, dimostrando che il crimine informatico, quando incontra l'innovazione, può essere davvero difficile da contrastare.

Distribuzione e Vettori di Infezione

Come a Natale trovi i regali sotto l'albero, anche gli infostealer ti fanno una sorpresa… ma di certo non di quelle che vorresti.

Come fanno ad arrivare? Beh, sono come quegli ospiti indesiderati che si autoinvitano: la loro facilità di distribuzione è incredibile ed è proprio questo che li ha resi così popolari negli ultimi anni.

Nel Dark Web sono praticamente in saldo, disponibili come "Malware-as-a-Service" (MaaS) pronti a finire nelle mani di chiunque, dai cyber criminali esperti ai temuti script kiddies con più ambizione che competenze.

A dargli una spintarella ci pensano poi le campagne di phishing, sempre più raffinate, che arrivano dritte nella tua inbox con link e allegati che sembrano innocui ma sono tutto tranne che un regalo. E la vittima? In preda alla fretta, magari sommersa di email e notifiche, clicca senza pensarci due volte: perché leggere con attenzione quando c'è da rispondere a tutto in tempo record? E così cade nella trappola.

E che dire degli exploit kit? Questi geni del male sfruttano ogni vulnerabilità lasciata scoperta, come chiudere tutte le finestre di casa ma dimenticare la porta spalancata. E per non farci mancare niente ci sono i crack dei software: perché pagare per l'originale quando puoi scaricare un malware in omaggio? Alla fine la gente cerca di risparmiare soldi e finisce per spendere i propri dati… letteralmente.

Una volta entrati questi piccoli fenomeni fanno tutto da soli: raccolgono i tuoi dati e li inviano direttamente ai server dei loro creatori, il tutto mentre tu ignori beatamente cosa sta succedendo. I loro metodi di infezione sono altrettanto variegati: download inconsapevoli, social engineering che ti manipola come una marionetta e app fasulle che sembrano troppo belle per essere vere.

Insomma gli infostealer sono i veri Grinch del digitale, sempre pronti a rovinarti la festa!

BOTNET E INFOSTEALER

COME FUNZIONANO, LE TIPOLOGIE, I BLACK FEED, I MARKET UNDERGROUND E I SISTEMI DI CYBER THREAT INTELLIGENCE

Una botnet è una rete di computer infettati da un malware, controllata da un individuo che prende il nome di **bot master.** Il **bot master** è la persona che gestisce l'infrastruttura botnet, che utilizza i computer compromessi per lanciare una serie di attacchi come *iniettare malware, raccogliere credenziali o eseguire attività ad alta intensità di CPU.* Ogni singolo dispositivo all'interno della rete botnet è chiamato bot.

La prima generazione di botnet operava su un'architettura client-server, in cui un server di comando e controllo (C&C) gestiva l'intera botnet. A causa della sua semplicità, lo svantaggio dell'utilizzo di un modello centralizzato rispetto a un modello P2P è che è suscettibile di un singolo point of faliure.

I due canali di comunicazione C&C più comuni sono IRC e HTTP:

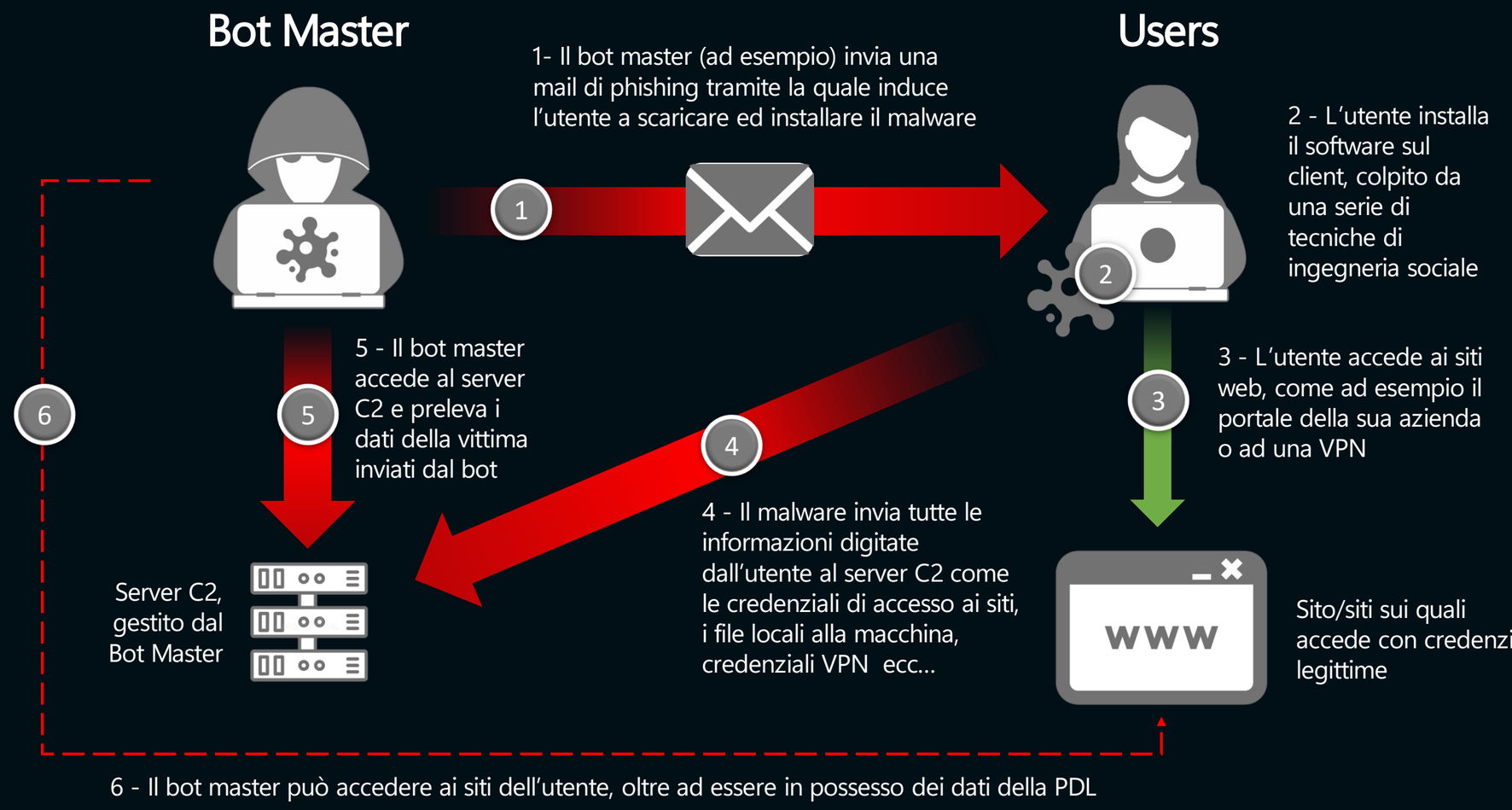
- **botnet IRC (Internet Relay Chat) :** Le botnet IRC sono tra i primi tipi di botnet e sono controllate da remoto con un server e un canale IRC preconfigurato. I bot si connettono al server IRC e attendono i comandi del bot master;
- **botnet HTTP :** Una botnet HTTP è una botnet basata sul Web attraverso la quale il bot master utilizza il protocollo HTTP per inviare comandi. I bot visiteranno periodicamente il server per ottenere aggiornamenti e nuovi comandi. L'utilizzo del protocollo HTTP consente di mascherare le proprie attività come un normalissimo traffico web.

Le tipologie di Botnet sono le seguenti:

- **Botnet DDoS:** I bot infetti vengono sfruttati per lanciare attacchi Distributed Denial of Service (DDoS) contro server o reti mirate. Questi attacchi saturano la larghezza di banda e le risorse di un sistema, rendendolo inaccessibile agli utenti legittimi. Le botnet DDoS vengono spesso affittate a pagamento da criminali informatici che desiderano interrompere l'attività di un sito web o di un servizio online, danneggiando la reputazione dell'obiettivo o estorcendo denaro attraverso il ricatto, minacciando attacchi più gravi se non vengono pagati.
- **Botnet per il rilevamento della rete**: I bot infetti sono programmati per esplorare la rete alla ricerca di altri dispositivi vulnerabili da infettare. Questi bot cercano obiettivi specifici, come server o dispositivi con vulnerabilità note, per ottenerne il controllo completo. Una volta infettato, il sistema diventa parte della botnet e può essere utilizzato per propagare malware o raccogliere dati sensibili. L'accesso completo ai sistemi permette agli attaccanti di utilizzare risorse hardware e software, rubare informazioni o controllare interamente le operazioni dei dispositivi compromessi.

- **Botnet backdoor:** Questi bot infettano altri dispositivi per aggiungerli alla botnet e dare agli attaccanti un controllo remoto continuo. Le botnet backdoor sono utilizzati per aprire **porte "segrete" sui dispositivi infetti**, permettendo agli hacker di eseguire comandi, caricare o scaricare file, e compromettere ulteriormente il sistema. Queste botnet possono essere utilizzate per scopi diversi, come il furto di informazioni, l'esecuzione di attacchi di ransomware, o il monitoraggio delle attività della vittima senza che quest'ultima se ne accorga.
- **Botnet per furto di informazioni (Info-stealer/Stealer):** I bot infetti da malware stealer sono progettati per *raccogliere informazioni sensibili dalle vittime, come credenziali di accesso, dati bancari,* informazioni personali e dettagli su account online. Questi malware possono utilizzare tecniche avanzate come **keylogging, screenshot grabber** e la registrazione delle attività della tastiera per rubare informazioni senza che l'utente se ne accorga. Una volta raccolti, i dati vengono inviati al server di comando e controllo *(come vedremo nella figura della pagina successiva),* dove vengono poi venduti sul mercato nero o utilizzati per attacchi futuri. Le botnet stealer sono molto pericolose, in quanto possono mettere a rischio dati bancari, identità online e altre informazioni vitali.
- **Botnet per spam:** Queste botnet sono progettate per inviare enormi quantità di messaggi di spam a indirizzi e-mail rubati, con lo scopo di *promuovere prodotti, servizi o attività fraudolente*. Anche se lo spam è spesso associato a messaggi promozionali indesiderati, le botnet per spam possono essere utilizzate anche per distribuire malware, truffe di phishing o altre minacce. I bot infetti raccolgono indirizzi e-mail da fonti pubbliche o infettano altri dispositivi per espandere la rete di invio. Questi attacchi possono provocare danni reputazionali alle vittime, aumentare il carico sui server di posta elettronica e contribuire alla diffusione di contenuti dannosi.

Schema del funzionamento di una Botnet



Una botnet, come abbiamo visto può essere utilizzata per molti scopi, ma per poterci addentrare in questa analisi, dobbiamo per prima cosa comprendere come funziona una infezione da botnet.

Nel disegno riportato sotto, viene mostrato uno schema di una classica infezione. La mail di phishing è un esempio, in quanto il vettore di attacco iniziale può essere diverso.

Sinteticamente possiamo suddividere l'infezione in 6 fasi che sono:

1. Il Bot master invia ad una vittima una mail di phishing, costringendola a cliccare sull'allegato utilizzando varie forme di ingegneria sociale. Per maggiori informazioni potete leggere il funzionamento di BazarCall/BazarLoader, un malware precursore molto utilizzato nelle attività ransomware, che spiega queste forme evolute di ingegneria sociale. Oltre al classico phishing, il malware che permette l'ingresso in una botnet viene spesso inserito all'interno di eseguibili (ad esempio i keygen) oppure software pirata;
2. Una volta eseguito dall'utente il software nella postazione di lavoro, tale software inizia a lavorare inviando informazioni al sistema di comando e controllo C2. Normalmente inizia ad inviare dati come i cookie di sessione dei siti visitati, dati sensibili dell'utente presenti
3. nel suo hard disk, schermate o filmati di quello che avviene sulla PDL e sequenze di tasti premuti, come un normale keylogger;
4. L'utente non accorgendosi del malware, continua le sue attività, come ad esempio andare sui siti dell'organizzazione per la quale lavora, effettuare transazioni bancarie, ecc…
5. Ovviamente, tutte queste preziose informazioni vengono inviate al sistema di comando e controllo controllato dall'attaccante;
6. Ora l'attaccante può accedere a questi dati, analizzarli e comprendere come beneficiare di queste informazioni;
7. A questo punto il bot master può rivendere queste informazioni ad altri criminali che potranno condurre attività illecite simulando ed impersonando l'utente finale, sul quale è stato installato il malware.

Sistemi di Intelligence e Market Underground

Il bot master, ovvero il possessore di una botnet, ha un'influenza significativa nel panorama della cybercriminalità, potendo sfruttare i **black feed** di dati raccolti dalle macchine infettate in modo vantaggioso su vari mercati. Da un lato, è possibile rivendere l'accesso ai bot ai **mercati underground**, dove gli hacker acquistano credenziali rubate per lanciare attacchi mirati. Questi feed contengono informazioni preziose,

come password, accessi a sistemi bancari, account di social media e altre credenziali sensibili, che, una volta nelle mani sbagliate, possono essere utilizzate per commettere frodi o rubare dati a livello industriale.

Al contempo, i bot master possono vendere questi stessi feed a un altro mercato, legato alla sicurezza informatica, dove le aziende che sviluppano **sistemi di cyber threat intelligence** integrano i dati nei loro strumenti per *monitorare e analizzare la compromissione di credenziali*. Questi "**black feeds**" forniscono alle aziende l'accesso a informazioni critiche che rivelano quali credenziali sono state compromesse e in quali contesti, consentendo così di adottare misure preventive. Le organizzazioni possono *monitorare la diffusione di queste credenziali compromesse e rilevare tempestivamente eventuali attacchi mirati.*

Un altro aspetto cruciale riguarda l'analisi dei dati exfiltrati dalle botnet, che può essere condotta non solo attraverso strumenti di cyber threat intelligence tradizionali, ma anche tramite piattaforme legate a mercati oscuri, come Genesis, un noto sito underground che fornisce accesso ai bot per altri criminali. Questi strumenti di intelligence non solo permettono di acquisire credenziali e informazioni compromesse, ma consentono anche di monitorare l'attività dei bot, correlando i feed con domini specifici e identificando vittime potenziali o già compromesse.

La capacità di monitorare i feed provenienti dalle botnet e integrarli in strumenti di intelligence offre alle aziende un doppio vantaggio: da un lato, possono proteggere i loro sistemi, rilevando accessi non autorizzati attraverso credenziali rubate; dall'altro, possono partecipare a una rete più ampia di rilevamento e prevenzione di attacchi, comprendendo meglio i trend delle minacce.

Analizzare i black feed consente anche di studiare i metodi utilizzati dai criminali per accedere alle risorse aziendali, permettendo alle aziende di migliorare le proprie difese.

Infine, la vendita di feed dalle botnet non è limitata solo alla comunità underground o alle aziende di intelligence, ma può coinvolgere anche *governi e agenzie di sicurezza, interessati a raccogliere informazioni per combattere attivamente la criminalità informatica*.

Questi enti, grazie all'accesso ai dati esfiltrati dalle botnet, possono acquisire una panoramica più completa sugli attacchi in corso, le vulnerabilità comuni e le tecniche utilizzate dai criminali. In questo modo, la comprensione delle botnet/infostealer diventa un'arma fondamentale non solo per la protezione delle singole aziende, ma anche per le operazioni di difesa su scala globale.

RedHot Cyber

DARKLAB
RHC INTELLIGENCE LABORATORY

Schema della rivendita dei black feed da parte dei Bot Master

Black Hacker

Bot Master

Intelligence User

3 – I criminali informatici acquistano le credenziali rivendute sui black market

1 - Il bot master rivende i feed prodotti dalla sua botnet a diverse entità

5 – Gli analisti di sicurezza informatica, accedono ai log degli infostealer venduti dal Bot Master

2 – I black Feed vengono venduti ai Black Market

4 – I black Feed vengono venduti ad aziende che rivendono sistemi di Cyber Threat intelligence

Server C2, gestito dal Bot Master

L’IMPATTO DEGLI INFOSTEALER

SETTORI PIU’ COLPITI E QUANTIFICAZIONE DEI DANNI PRODOTTI DAGLI INFOOSTEALER

L'impatto degli infostealer si estende a vari settori economici critici, tra cui il finanziario, il sanitario e il retail, generando conseguenze significative in termini di sicurezza, fiducia dei consumatori e costi economici.

Settore Finanziario

Il settore finanziario è uno dei principali bersagli degli infostealer. Le banche e altre istituzioni finanziarie gestiscono una grande quantità di dati sensibili, rendendole un obiettivo attraente per i cybercriminali. Gli attacchi degli infostealer possono portare a:

- *Furto di identità e frodi bancarie:* Gli infostealer rubano credenziali di accesso e informazioni finanziarie, utilizzate poi per commettere frodi bancarie. Secondo un'analisi a campione su trenta banche italiane, si è passati da quasi 20.000 credenziali esfiltrate nel 2022 a quasi 29.000 nel 2023. Si tratta di credenziali di accesso ai conti correnti ma allo stesso tempo informazioni finanziarie, dati personali, informazioni di carte di credito e documenti riservati. Nel complesso, si sono riscontrate una quantità di 105.777 dispositivi infetti.
- *Costi di gestione e riparazione:* Le banche devono investire notevoli risorse per gestire gli incidenti di sicurezza, riparare i sistemi compromessi e compensare i clienti colpiti.
- *Danno alla reputazione:* La fiducia dei clienti nelle istituzioni finanziarie può essere seriamente compromessa, influenzando negativamente le relazioni a lungo termine e la fiducia nel sistema.

Settore Sanitario

Il settore sanitario gestisce dati altamente sensibili, inclusi i dati medici dei pazienti. Gli infostealer possono avere conseguenze devastanti:

- Violazione della privacy dei pazienti: Gli infostealer possono rubare dati medici e personali, mettendo a rischio la privacy e la sicurezza dei pazienti. Le informazioni rubate possono essere utilizzate per frodi mediche o vendute nel mercato nero.
- Interruzione dei servizi: Gli attacchi possono causare interruzioni nei servizi sanitari, influenzando la qualità dell'assistenza ai pazienti e causando ritardi nel trattamento.
- Costi di conformità e sicurezza: Le organizzazioni sanitarie devono investire in misure di sicurezza aggiuntive per conformarsi alle normative sulla protezione dei dati, aumentando i costi operativi.

Settore Retail

Il settore retail, che include il commercio al dettaglio sia online che fisico, è anch'esso vulnerabile agli attacchi degli infostealer:

- Furto di dati dei clienti: Gli infostealer possono rubare informazioni personali e di pagamento dei clienti, portando a frodi e perdite finanziarie significative.
- Perdita di fiducia dei consumatori: Un attacco di grande portata può portare alla perdita di clienti e a danni a lungo termine alla reputazione aziendale.
- Costi di riparazione e gestione: Le aziende devono affrontare costi elevati per gestire gli incidenti di sicurezza, riparare i sistemi compromessi e implementare misure di sicurezza più robuste.

Secondo una ricerca di Deloitte, nel 2022, il 98% delle aziende italiane ha subìto almeno una violazione informatica (nella maggior parte dei casi manifestati con tecniche di phishing via e-mail, messaggi di testo, telefonate o siti web fraudolenti), con danni gravi o estremamente gravi in due casi su tre. Dal punto di vista delle imprese, le violazioni informatiche possono comportare, a livello economico, perdite di fatturato (per il 40% degli intervistati) e riduzione del valore di mercato (per il 36%). Ma sono percepiti anche rischi a livello normativo, con sanzioni per inadempienza (per il 52%), e di reputazione (44%).

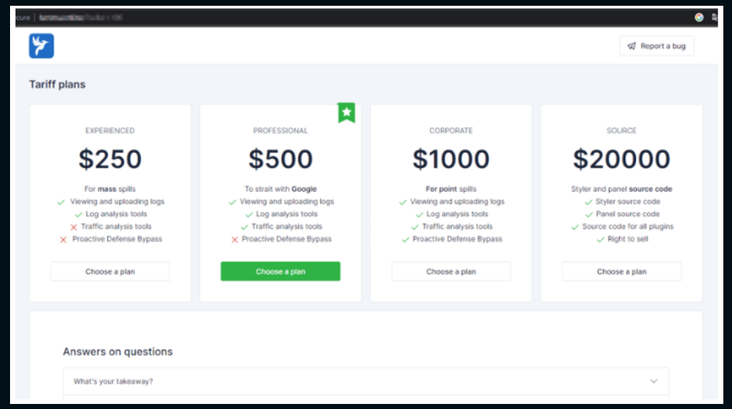
D: Su una scala da 1 (per nulla) a 4 (in larga misura), quanto la sua organizzazione ha subito conseguenze negative in ognuna delle seguenti aree riconducibili a violazioni della cybersecurity?
Deloitte, 2023.

Secondo il report, le questioni legate alla cybersecurity stanno diventando sempre più importanti per i dirigenti, in quanto una corretta strategia genera valore in termini di brand reputation, fiducia dei clienti, modello di business resiliente e agile. Sfruttare appieno tale potenziale, rendendo la cyber sicurezza un vero e proprio fattore abilitante per il raggiungimento degli obiettivi aziendali, è possibile solo se questa viene integrata nella più ampia strategia di business.

I dati rubati, come nomi, indirizzi e numeri di telefono, alimentano altre attività cybercriminali : possono essere utilizzati per creare identità false e commettere frodi finanziarie.

Le informazioni di pagamento rubate, come numeri di carta di credito e dettagli di conti bancari, vengono utilizzate per effettuare acquisti non autorizzati e trasferimenti di fondi (carding).

Le credenziali di accesso rubate possono essere utilizzate per ottenere accesso non autorizzato a sistemi e reti, permettendo ulteriori attacchi informatici, in particolare la diffusione dei temuti ransomware, con cui le organizzazioni vengono ricattate e messe sotto scacco.



LummaC2's official seller website

Il crimine informatico si sta specializzando in diversi ruoli all'interno dell'economia illecita e l'intero ecosistema del malware infostealer degli attori e delle loro operazioni può essere sintetizzato in questo modo:

1. gli sviluppatori di software non etici creano malware. Vendono licenze software via Internet, dove il costo del modello MaaS (malware as a service) varia tra 125 e 200 dollari statunitensi al mese.
2. secondo, il proprietario della rete di malware infetta le vittime tramite metodi popolari, come allegati email e macro. Questo attaccante può utilizzare il servizio spam-as-a-service, che costa tra 100 e 500 dollari statunitensi per un milione di email inviate, e liste email mirate, che costano tra 25 e 50 dollari statunitensi per un milione di indirizzi email.
3. terzo, una volta che il malware infetta le vittime, l'operatore della rete vende l'accesso ai loro dispositivi su piattaforme che vendono informazioni rubate (es. Genesis Market, chiuso ad aprile 2023). La fascia di prezzo varia tra 1 e 350 dollari statunitensi, e il valore di un record di una vittima dipende dal numero di servizi compromessi. Questo fornisce una visione del valore di vendita al dettaglio diretto delle informazioni della vittima da parte del proprietario della rete di malware. Tipicamente, l'accesso a una vittima di malware costa tra 1 e 20 dollari statunitensi, con una mediana di 5 dollari statunitensi.

4. infine, un acquirente degli accessi della vittima alla fine trae profitto ottenendo l'accesso ai conti online della vittima o vendendo le credenziali individuali. I prezzi di vendita sono tipicamente tra 1 e 30 dollari statunitensi, con una mediana di 7 dollari statunitensi.

Ma è possibile quantificare i danni prodotti dagli infostealer?

Sembra molto difficile e soggettivo: dipende dalle circostanze, dall'importanza del dato che viene esfiltrato, dagli attacchi che vengono portati successivamente. Inoltre, non tutte le violazioni vengono denunciate.

Se, a causa di un infostealer, un attacco ransomware va a segno, i danni sono molteplici, oltre al puro riscatto richiesto dai criminali:

- le attività di remediation per ripristinare i sistemi
- disservizi alle attività aziendali
- perdita di fatturato
- danni alla reputazione aziendale

CybelAngel ha calcolato i costi medi basandosi sui propri dati: il costo medio di recupero da un attacco ransomware è di 1,82 milioni di dollari, mentre il costo medio del riscatto per ripristinare i dati persi è di 2,6 milioni di dollari, riducibile a 1,6 milioni utilizzando i backup. Anche i costi in termine di tempo sono pesanti: il 45% delle organizzazioni con backup sono riuscite a recuperare entro una settimana, ma solo il 39% delle organizzazioni che hanno pagato il riscatto sono state in grado di farlo.

Un esempio, Independent Living Systems (ILS), un servizio di amministrazione sanitaria con sede a Miami, ha subito una violazione dei dati che ha colpito 4,2 milioni di persone. Questo ha portato a 5 cause legali e alla revisione delle misure di sicurezza informatica. Il settore sanitario è particolarmente vulnerabile agli attacchi ransomware a causa della mancanza di risorse e della presenza di molte terze parti.

Secondo un sondaggio condotto da IBM, l'impatto finanziario di un data breach ha raggiunto una media di quasi 5 milioni di dollari (con questa media quasi raddoppiata se prendiamo in considerazione gli USA), con i settori finanziario e sanitario che sono quelli che più hanno subìto l'impatto.

STRATEGIE DI MITIGAZIONE

I SETTORI PIU’ COLPITI

Le strategie di mitigazione e rilevamento degli infostealer includono diverse misure tecniche e organizzative. Implementare un approccio olistico che combini misure tecniche, organizzative e comportamentali è fondamentale per mitigare il rischio.

Tecniche di mitigazione

Focalizzandoci sulle misure di rilevamento e mitigazione più efficaci nell'identificare e prevenire le infezioni da infostealer, possiamo trovare:

- protezione degli endpoint
- autenticazione forte
- aggiornamenti e patch
- segmentazione della rete
- monitoraggio continuo

Per la protezione degli Endpoint risulta fondamentale l'utilizzo di soluzioni EDR (Endpoint Detection and Response) e XDR (Extended Detection and Response) atte a rilevare e bloccare attività anomale.

L' Autenticazione Forte è ormai imprescindibile. Occorre implementare sistemi MFA (Multi-Factor Authentication) per aggiungere un ulteriore livello di sicurezza oltre alla password e ridurre l'efficacia del furto di credenziali.

Mantenere tutti i software e i sistemi operativi aggiornati con le ultime patch di sicurezza consente di ridurre le vulnerabilità sfruttabili.

Dividere la rete in segmenti più piccoli consente di limitare la propagazione del malware in caso di infezione.

Il Monitoraggio Continuo e logging dei sistemi aiuta a rilevare attività sospette, eventuali compromissioni e a rispondere rapidamente agli incidenti.

Best practice organizzative

Vediamo ora quali sono le misure organizzative e comportamentali da adottare:

- implementare politiche di sicurezza per la protezione delle informazioni sensibili.
- Prevedere la Formazione e la Consapevolezza educando i dipendenti sulle migliori pratiche di sicurezza informatica, come il riconoscimento delle email di phishing e l'importanza delle password sicure, informandoli sulle ultime minacce e tecniche di attacco utilizzate dai cybercriminali.

Non ultimo promuovere una cultura volta all'uso responsabile delle risorse aziendali e incoraggiando la segnalazione tempestiva degli incidenti o eventi significativi per una rapida risposta e mitigazione.

- Prevedere e Condurre regolari valutazioni di sicurezza e test di penetrazione per identificare e correggere le vulnerabilità.

Monitoraggio continuo

Focalizzandosi sull'importanza del monitoraggio continuo, le soluzioni EDR/XDR e SIEM sono strumenti che possono svolgere un ruolo chiave nella mitigazione degli infostealer.

Soluzioni avanzate di EDR/XDR che monitorano e analizzano le attività sugli endpoint sono necessarie per individuare comportamenti sospetti. Utilizzano tecniche come il keylogging, il form grabbing e la cattura di screenshot per intercettare i dati sensibili prima che vengano esfiltrati.

Il SIEM (Security Information and Event Management) raccoglie e analizza i log e gli eventi di sicurezza da diverse fonti all'interno dell'organizzazione (le applicazioni, i sistemi di sicurezza e l'hardware). Questo permette di identificare comportamenti anomali, "scrutando" gli eventi con l'aiuto di regole e motori di analisi, che potrebbero indicare la presenza di un infostealer.

Vediamo come queste tecnologie possono contribuire alla protezione contro gli infostealer:

- Rilevamento
  - monitorano costantemente il comportamento degli endpoint, rilevando attività sospette come l'accesso non autorizzato alla memoria, la raccolta di dati o l'estrazione di informazioni.
  - Questi malware eseguono operazioni anomale, come l'accesso a file di configurazione dei browser o l'intercettazione di input da tastiera. Gli strumenti EDR/XDR rilevano tali comportamenti e li bloccano in tempo reale.
- Contenimento
  - Quando viene rilevato un potenziale infostealer, interviene l'EDR e può isolare automaticamente il dispositivo compromesso dalla rete per impedire la propagazione.
  - Blocchi basati su policy per bloccare automaticamente processi o connessioni sospette, evitando che il malware comunichi con i server di comando e controllo

- **Risposta e mitigazione**
  - Gli EDR/XDR possono eseguire azioni correttive automatizzate, come terminare il processo malevolo, eliminare file dannosi o rimuovere modifiche al sistema.
  - forniscono strumenti per analizzare in dettaglio l'attacco e risalire alla sua origine, migliorando la velocità della risposta.
- **Prevenzione**
  - Gli strumenti XDR/SIEM centralizzano i dati da più fonti (endpoint, rete, cloud) per identificare pattern sospetti e prevenire futuri attacchi (hunting minacce).
  - Molti infostealer sfruttano vulnerabilità note. Gli EDR/XDR prevedono l'attivazione di tool aggiuntivi di Patch management che aiutano a identificare e correggere le vulnerabilità (CVE) prima che possano essere sfruttate.
- **Apprendimento continuo**
  - Queste soluzioni ricevono aggiornamenti costanti sulle nuove tecniche e firme degli infostealer, migliorando la capacità di rilevamento.
  - Attraverso il Machine Learning gli algoritmi di apprendimento migliorano la capacità di distinguere tra attività legittime e malevole, anche in presenza di varianti sconosciute di infostealer.

Integrando i dati da più livelli (email, rete, server, cloud), per avere una visione completa dell'environment aziendale, questa modalità permette di correlare eventi su più livelli per rilevare campagne di infostealer più sofisticate e ridurre i falsi positivi e migliorare l'efficacia del rilevamento.

In sintesi quali sono le Best Practice contro gli infostealer?

- Configurare policy rigorose: Bloccare esecuzioni da directory sospette (es. cartelle temporanee).
- Monitorare l'attività delle credenziali: Gli infostealer spesso mirano a rubare password; il monitoraggio delle autenticazioni anomale è fondamentale.
- Simulare attacchi: Utilizzare simulazioni di infostealer per testare l'efficacia delle soluzioni.
- Formazione degli utenti: Educare il personale sui rischi degli infostealer per prevenire l'esecuzione accidentale di malware.

CONFORMITA’ NORMATIVE E REGOLAMENTI

Il Regolamento UE 679/2016, meglio conosciuto come GDPR (General Data Protection Regulation), ha un impatto significativo sulla gestione e prevenzione degli attacchi da infostealer per le aziende europee, sia dal punto di vista delle responsabilità legali che delle misure tecniche da adottare. Dobbiamo ricordare che il GDPR richiede che le aziende siano in grado di dimostrare di aver adottato tutte le misure necessarie per proteggere i dati personali e prevenire attacchi (accountability e implementazione di Policy specifiche). Un infostealer è un tipo di malware che ruba informazioni sensibili come credenziali di accesso, dati bancari, informazioni personali e aziendali.

Il GDPR stabilisce che le aziende siano responsabili della protezione dei dati personali che trattano, inclusi quelli che potrebbero essere compromessi tramite attacchi informatici come quelli da infostealer. L'art. 32 del GDPR dimostra l'importanza del GDPR sull'implementazione di misure proattive nella difesa da attacchi da infostealer; al punto 1 riporta "*tenendo conto dello stato dell'arte e dei costi di attuazione, … il titolare del trattamento come il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio …", s*pecificando alla lettera d) "*una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento*".

In caso di violazione dei dati, le aziende devono rispondere alle normative in modo tempestivo e adeguato:

> *Obbligo di notifica: l'azienda ha l'obbligo di notificare la violazione entro 72 ore da quando prende coscienza dell'accaduto (cioè da quando si accorge dell'attacco subito) all'autorità di protezione dei dati (Ente del Garante per la protezione dei dati personali) e, se vengono compromessi dei dati personali, si deve procedere con una comunicazione agli interessati, spiegando l'accaduto e il tipo di danno che il dato può aver subito; tale comunicazione è necessaria se la violazione comporta un rischio elevato per gli interessati.*

Di rilevante importanza è la valutazione del rischio e le misure di sicurezza che l'azienda deve mettere in campo. Le violazioni dei dati tramite infostealer sono un rischio concreto, e le aziende devono adottare soluzioni per prevenirle, come ad esempio:

- Crittografia
- Autenticazione multifattoriale (MFA)
- Monitoraggio continuo
- Formazione sulla sicurezza
- Audit regolari

In questi ultimi anni, la Comunità Europea ha affrontato il tema della protezione dei dati personali attraverso il GDPR; all'interno del Regolamento vi è una carenza di linee guida specifiche su determinate minacce particolari come le minacce da infostealer, lasciando così le aziende ad affrontare minacce senza le necessarie raccomandazioni per affrontarle in modo efficace.

Un ulteriore problema può essere l'applicazione del GDPR in ambito internazionale (extra UE) dove le normative potrebbero essere meno rigorose rispetto al GDPR stesso; quindi, con maggiori possibilità di attacco perché con misure di sicurezza non implementate correttamente. Inoltre, molti attacchi provengono spesso da Paesi extra UE, dove le leggi sulla protezione dei dati sono molto più deboli.

Una mancanza di linee guida lascia un vuoto significativo quando si tratta di affrontare minacce raffinate come quelle date dagli infostealer. Inoltre, in alcune aziende italiane, non viene ancora percepito il reale pericolo dato da questi malware raffinati e la necessità di investire in misure di sicurezza proattive; la non corretta applicazione delle misure di sicurezza da applicare alla realtà aziendale (in Italia si è passati dalle "misure minime" alle "misure adeguate" senza specificare quali potrebbero essere le "misure adeguate"). Una protezione "preventiva" con un monitoraggio in tempo reale per rilevare attacchi può sicuramente ridurre il rischio contro gli infostealer.

Analisi Forense e Intelligence

I dati raccolti da campagne di threat intelligence sono fondamentali per l'attribuzione degli attacchi legati agli infostealer. Questi dati includono informazioni su indicatori di compromissione (IoC), tecniche, tattiche e procedure (TTP) utilizzate dagli attaccanti, e altre informazioni rilevanti che possono essere correlate con gli attacchi osservati. L'analisi di questi dati permette di identificare modelli e collegamenti tra diversi attacchi, facilitando l'attribuzione a specifici gruppi di minaccia o attori malevoli.

L'analisi forense digitale gioca un ruolo cruciale nel tracciare le operazioni post-compromissione degli infostealer. Questa analisi include l'esame dei registri di sistema, la raccolta di prove digitali, e l'analisi dei dati esfiltrati per comprendere l'entità della compromissione e le tecniche utilizzate dagli attaccanti. L'obiettivo è identificare le tracce lasciate dagli infostealer, ricostruire la sequenza degli eventi e determinare l'impatto dell'attacco.

BACKGROUND E STATO DELL'ARTE

Correlazione tra infostealer e ransomware

Diversi studi evidenziano una correlazione preoccupante tra le infezioni da infostealer e gli attacchi ransomware. Quasi un terzo delle aziende colpite da ransomware nel 2023 aveva subito precedentemente un'infezione da malware infostealer. Questa connessione si basa su dati pubblici e confermati, ma la reale esposizione potrebbe essere ancora maggiore, poiché molti incidenti ransomware non vengono divulgati.

L'aumento delle capacità avanzate degli infostealer, come la crittografia migliorata per eludere i rilevamenti o la capacità di ripristinare cookie di autenticazione scaduti, sta aumentando significativamente il rischio per le organizzazioni. Questa evoluzione consente agli attaccanti di mantenere accessi persistenti alle reti compromesse.

Il ruolo del Malware-as-a-Service (MaaS)

Il modello Malware-as-a-Service (MaaS) facilita l'accesso a strumenti avanzati anche a criminali informatici con competenze limitate, aumentando l'impatto delle campagne di infostealer. Attraverso il MaaS, gli operatori possono acquistare malware e accedere a un flusso continuo di dati di identità rubati, amplificando l'efficacia del crimine informatico.

Evoluzione degli attacchi di acquisizione account (ATO)

Sono state identificate evoluzioni negli attacchi di Account Takeover (ATO), che ora sfruttano cookie di sessione rubati per effettuare il dirottamento delle sessioni. Questo metodo consente agli attaccanti di bypassare completamente i meccanismi di autenticazione, impersonando utenti legittimi senza essere rilevati.

Limiti delle difese tradizionali

Nonostante la diffusione di strumenti avanzati di sicurezza, le misure tradizionali come gli antivirus e i sistemi EDR si sono dimostrate inefficaci contro gli infostealer:

- Il 54% dei dispositivi infetti nella prima metà del 2024 disponeva già di soluzioni antivirus o EDR attive.
- Gli attacchi basati su dirottamento di sessioni neutralizzano anche le moderne soluzioni di autenticazione multifattoriale (MFA) e senza password.

Strategie di difesa avanzate

Le ricerche sottolineano la necessità di passare da una semplice rimozione delle infezioni alla gestione del rischio a lungo termine. Le strategie consigliate includono:

- reimpostazione delle credenziali delle applicazioni compromesse
- invalidazione dei cookie di sessione rubati per impedire accessi non autorizzati.
- implementazione di sistemi di rilevamento proattivo per identificare e bloccare attività sospette associate agli infostealer.

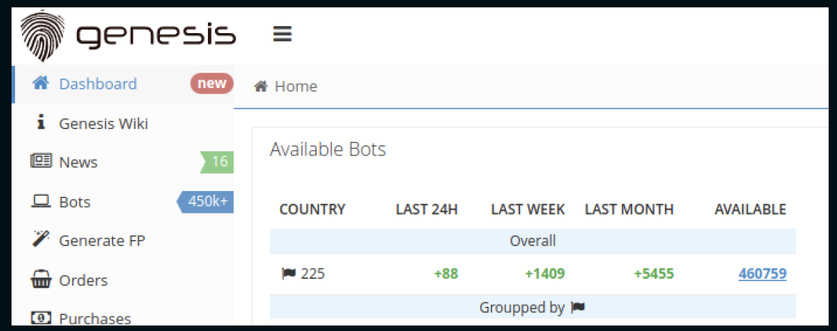
In conclusione, il crescente legame tra infostealer e ransomware richiede alle organizzazioni di affrontare il problema con un approccio olistico e preventivo. Migliorare la resilienza contro gli infostealer non solo riduce il rischio di attacchi futuri, ma limita anche la probabilità di escalation in attacchi ransomware devastanti. In un panorama in rapida evoluzione, la protezione degli asset digitali richiede soluzioni adattive e una gestione proattiva delle minacce.

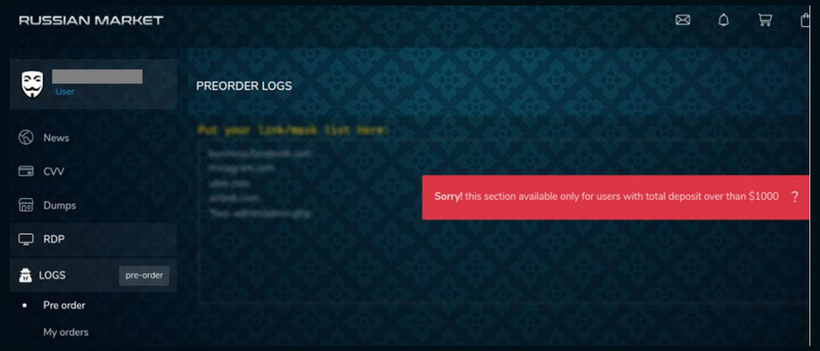
Gli infostealer rappresentano una crescente minaccia nell'ecosistema della criminalità informatica, agendo come strumenti avanzati per il furto di credenziali e dati sensibili.

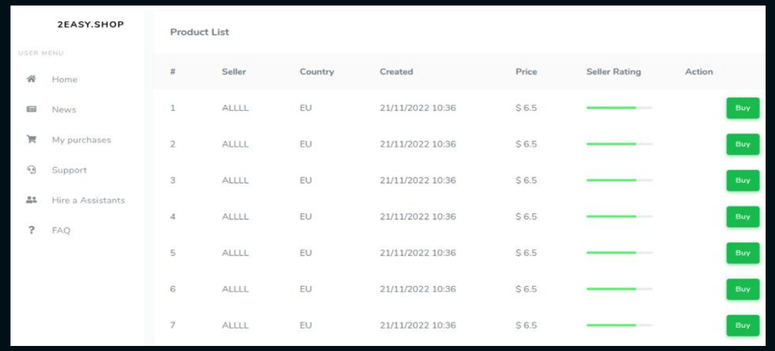
Questi malware, distribuiti attraverso phishing, siti compromessi o software dannosi, esfiltrano rapidamente informazioni da dispositivi compromessi, vendendo successivamente sotto forma di log sui mercati underground.

Struttura operativa e mercati

- **Modello di business:** Gli infostealer sono spesso offerti come servizi basati su abbonamento (MaaS) con costi che variano da $50 a oltre $1.000 al mese. Questa infrastruttura include server di comando e controllo (C2) ospitati e pannelli di gestione per la configurazione e il monitoraggio.
- **Mercati sotterranei:** Forum come Russian Market, Genesis Market e 2easy dominano il commercio di log e bot. Questi marketplace offrono infrastrutture automatizzate, garantendo anonimato e accessibilità globale, spesso tramite Tor o I2P







- **Telegram:** La piattaforma Telegram sta emergendo come alternativa ai forum tradizionali, grazie alla crittografia avanzata e al supporto per canali privati. I vantaggi di questa piattaforma per i criminali informatici includono la sua attenzione alla privacy, alla crittografia e a un'interfaccia di programmazione delle applicazioni (API) open source che consente ai "client non ufficiali" (app di messaggistica alternative che utilizzano l'API di Telegram) di comunicare con l'app ufficiale e l'interfaccia web. I criminali informatici utilizzano questi canali e gruppi per vendere infostealer come Titan Stealer . Alcuni canali sono nascosti e richiedono inviti o autorizzazioni specifiche per l'accesso. Tuttavia, la mancanza di reputazione e la prevalenza di truffe limitano il suo utilizzo esclusivo per la vendita di malware.

Evoluzione tecnica

Gli infostealer si sono evoluti dal trojan ZeuS del 2006 fino a varianti moderne come RedLine, RaccoonV2 e Vidar. Questi malware mostrano funzionalità avanzate:

- **Adattabilità:** Personalizzazione per obiettivi specifici.
- **Evasione:** Meccanismi anti-rilevamento e crittografia avanzata.
- **Modularità:** Supporto per payload secondari come ransomware.

Alcuni esempi includono:

- **RedLine:** Popolare per la sua semplicità e capacità di esfiltrare credenziali e dati di completamento automatico.
- **RaccoonV2:** Sviluppato attivamente, con funzionalità di evasione migliorate.
- **Vidar:** Oltre al furto di dati, può distribuire ransomware.

L’ecosistema degli infostealer include:

- **Sviluppatori**: Creano e migliorano continuamente il malware.
- **Broker di accesso iniziale (IAB):** Distribuiscono gli infostealer e vendono dati rubati.
- **Clienti**: Utilizzano i dati per scopi dannosi, come frodi finanziarie o attacchi ransomware.

La crescente sofisticazione dei parser di log consente di estrarre informazioni utili da dataset complessi, abbassando la barriera tecnica per l’uso di questi strumenti.

Minacce emergenti

Gli infostealer sponsorizzati dallo stato, come Graphiron utilizzato dalla Russia o varianti cinesi per operazioni di spionaggio, evidenziano un impiego crescente per il cyberspionaggio e la raccolta di intelligence.

Mitigazione

Le organizzazioni devono adottare misure proattive per difendersi, tra cui:

- Implementazione di policy BYOD sicure.
- Utilizzo di software di sicurezza avanzati.
- Educazione degli utenti sui rischi associati a phishing e download sospetti.

L’espansione del fenomeno degli infostealer rappresenta una minaccia significativa per individui, aziende e infrastrutture critiche. L’evoluzione del loro ecosistema dimostra una crescente accessibilità al crimine informatico, rendendo essenziale un approccio integrato alla cybersecurity.

.

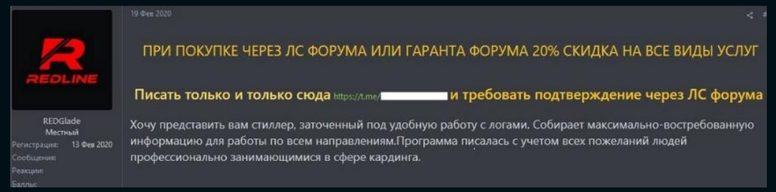
DIETRO LE QUINTE DI XFILESTEALER

INTERVISTA ESCLUSIVA CON LO SVILUPPATORE

Disclaimer

Questo documento è stato creato esclusivamente a scopo educativo e di ricerca. L'intervista con lo sviluppatore di XFileStealer è stata condotta per comprendere meglio le tecniche utilizzate nello sviluppo di malware e per migliorare le difese contro tali minacce. Non incoraggiamo né supportiamo in alcun modo l'uso o la distribuzione di software dannoso. Invitiamo tutti a rispettare le leggi e a utilizzare le proprie competenze informatiche in modo etico e responsabile.

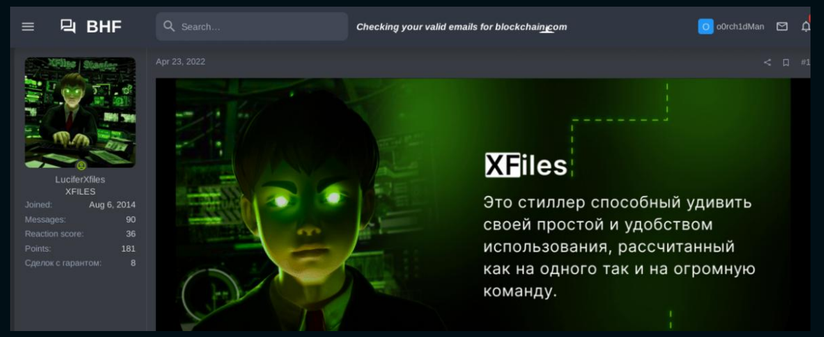
Uno degli infostealer più diffusi a livello globale è Redline, sviluppato da un individuo noto con il nickname Redglade. Questo malware veniva pubblicizzato e venduto su canali Telegram e siti del dark web, tra cui il forum BHF

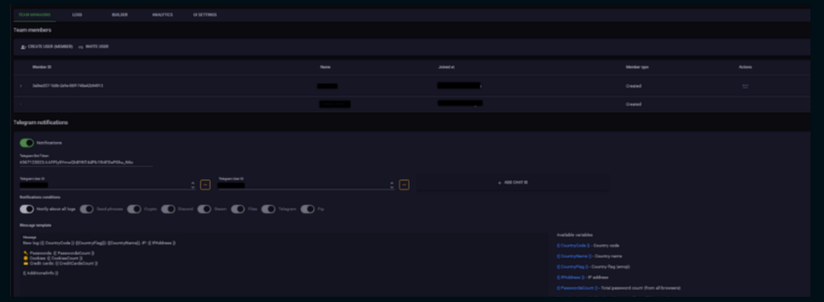


primo post di vendita risalente a Marzo 2020

Grazie alla cooperazione delle forze dell'ordine internazionali, lo sviluppatore Maxim Rudometov è stato arrestato e tutti i server gestiti sono stati chiusi.

Nel forum BHF, il banner per la vendita di Redline è stato rimosso e sostituito da un altro infostealer, XFilesStealer, noto dal 2021. Questo malware ha infettato migliaia di dispositivi in tutto il mondo, grazie alla sua capacità di offuscamento e al prezzo competitivo di 200 dollari al mese (MaaS).





Pannello di amministrazione

Di seguito riportiamo le principali feature del Malware pubblicizzato dal Threat Actors *(traduzione dal post ufficiale)*:

XFiles è uno stealer sorprendentemente facile da usare, progettato sia per un singolo che per un grande team Stub nativo, scritto nel linguaggio di programmazione C. Le build create sono uniche al 70% grazie al nostro sviluppo interno:

- Quando possibile vengono utilizzate chiamate di sistema, negli altri casi viene utilizzata WinAPI, non vengono utilizzate né richieste librerie di terze parti, la decodifica del log raccolto avviene interamente sul server
- Dashboard disponibile per Windows ed a breve disponibile anche un'interfaccia Web
- Bypass garantito di Windows Defender
- Per l'abbonamento Professional: viene rilasciato un file dll univoco per bypassare gli avvisi di sicurezza del browser
- Recupero dei Cookie tramite token
  - Se il browser nel pc della vittima è aperto colleziona sino ad 1GB di estensione
  - Il Malware funziona sui Sistemi operativi a partire da Windows 7 sino a Windows 11.
- Non viene attivato il malware nei paesi CIS
  - La raccolta dei dati è fatta in memoria, nessuna traccia viene lasciata sul disco
  - Raccoglie dinamicamente dal browser Cookie, password, autofill,carte di credito.
- Supporta oltre 50 browser (Google Chrome, Chronium, Opera, Edge, Firefox, etc)
- Raccoglie tutte le possibili criptovalute, portafogli Nft, 2Fa, OTP e gestori di autenticazione
  - Raccoglie crypto wallet installati sul Desktop quali ad esempio
    Armory, Atomic, Coinomi, BitcoinCore, Exodus, JaxxLiberty, Guarda, EverSurf, MoneroCore, etc
  - Colleziona le VPN presenti sul Desktop con tutte le informazioni presenti

Intervista con lo sviluppatore di XFileStealer

Siamo riusciti a entrare in contatto con lo sviluppatore di **XFilesStealer**, che ci ha concesso un' intervista.

Q: Can you tell us a bit about your background and how you got into developing infostealers?

A: It always seemed to me that working as a "White Hat" was not for me, it was boring. That's why I started developing malware. We are currently developing a new HVNC module for our stealer. Stay tuned :)

Q: What tools and programming languages do you prefer to use and why?

A: In our XFiles project, we use "extended C" as we call it to develop the stub, it allows us to do nasty things that are difficult for researchers to analyze. Desktop panel written in C# with Blazor and we also use WebView2 to support JavaScript and HTML. Backend is written using C#. Tools: We use VSCodium, Visual Studio, and many other tools.

Q: How have you seen infostealers evolve over the years?

A: Infostealers are developing too slowly. I don't want to name names, but they're just as lazy as they have not changed their codebase in years.

Q: What are the emerging trends in the development and use of infostealers?

A: AI. Everyone is talking about it. As we can see, there is little to no use of artificial intelligence by some malware developers nowadays. We plan to use LLM.

Q: How might defense techniques evolve to counter next-generation infostealers?

A: Google is trying to stop us from stealing the data of our victims. As of version 127 of Google Chrome, they use "App Bound Encryption", but implemented it poorly. The protection methods need to be implemented not only in antivirus products, but also in the software itself, which is actually easy to do for a large company like Google. They don't care about their users. So, to answer your question, stealer protection is easy to implement, they can start using polymorphic encryption, for example, generate an encryption/decryption code and ship it with each new version of the browser, it's actually so trivial to do, again, Google doesn't care about its users.

Q: Can you share any interesting or memorable experiences you've had in your work with infostealers?

A: Yes, one of my most memorable experiences was when our client told us that he had found a wallet with ~25 ETH. He successfully infected the victim and stole her wallet using out stealer.

Q: Have you been or are you part of a collective?

A: Maybe.

Q: Has the shutdown of Redline's C2 servers positively impacted the sales of your malware?

A: We got richer.

Q: What is the current number of affiliates purchasing the services of xfilestealer, and what is the total number of infected machines?

A: X00 clients, [redacted] victims.

Q: In terms of geolocation, is there a particular country that is more affected?

A: CIS is blocked, devices from such countries will not be able to connect to our C2 servers. We do not disclose which country is more affected, this information belongs to our customers.

Q: What is the approximate business turnover of your infostealer ?

A: "extended C".

Q: The current currency of choice is Bitcoin. Do you think it will remain this way in the future or be replaced?

A: The future of bitcoin is in the hands of Donald Trump and his team. I hope that in his hands, during his period, bitcoin will reach $200,000. As I wrote this, Bitcoin had already reached $96,000.

Q: What makes your infostealer better or worse compared to others on the market?

A: We have real support 24/7, respond quickly and professionally. As I say "extended C" many times, it's really a game changer, it has a lot of custom features, these features make analyzing our malware as difficult as possible, even now it's just the beginning, we're planning to use (AI) LLM to make the analysis even more difficult.

Q: Is there any advice you would give to avoid falling victim to infostealers?

A: We created XFiles to make money for ourselves and for the clients of our project. We don't care about the victims of our malware, it's their fault that they installed some bullshit from the internet.

Q: Have you ever considered becoming a white hat?

A: I've been in a white hat for a long time, I don't want to go back.

Con la chiusura di Redline, nel 2025 XFilesStealer potrà diventare uno dei MaaS più diffusi a livello globale.

Considerazioni del gruppo Darklab

Lo sviluppatore di XFileStealer afferma che lavorare come "White Hat" era monotono, ma non considera i rischi legali e morali del suo attuale percorso. Molti sviluppatori di malware finiscono per essere arrestati e costretti a vivere nell'ombra. Inoltre, non riconosce gli sforzi continui delle comunità di sicurezza per migliorare le difese. L'uso dell'intelligenza artificiale nei malware è preoccupante, ma anche le tecnologie di difesa stanno integrando l'AI per contrastare queste minacce. Le critiche a Google per la loro implementazione della "App Bound Encryption" ignorano i continui miglioramenti delle misure di sicurezza da parte delle grandi aziende. L'atteggiamento dello sviluppatore verso le vittime del malware dimostra una totale mancanza di etica e responsabilità sociale.

INFOSTEALER & BUSINESS

REALTA’ DI UNA MINACCIA SEMPRE PIU’ PERVASIVA E DIROMPENTE

Indagando nei “luoghi” del dark web dove vengono pubblicati e pubblicizzati i “frutti” del mestiere degli infostealer, abbiamo cercato di analizzare: la tipologia dei dati, la tipologia di informazioni che vengono offerte, il prezzo a cui vengono venduti i dati.

In questo documento abbiamo già analizzato quanto può valere un framework per sviluppare il proprio infostealer o quanto può valere un tool di info stealing da utilizzare nelle proprie campagne di furto di dati. Per chi non vuole comprare tool o sistemi di sviluppo è possibile acquistare per molto meno pacchetti già pronti di dati.

I dump delle credenziali esfiltrare vengono venduti in “pacchetti” già elaborati, magari divisi per: nazione di provenienza o tipologia di servizio (accessi per i vari social network, per i servizi di posta online, accesso ai servizi bancari ecc.)

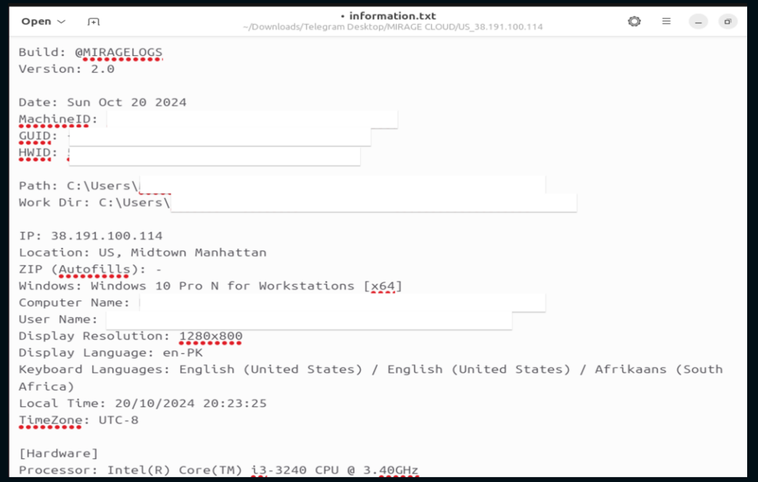
Sono in vendita anche pacchetti di accesso ai servizi “privati” delle aziende ed organizzazioni, come ad esempio: intranet aziendali, servizi gestionali, pannelli di controllo, ecc.

Altra categoria di dati di accesso in vendita, non meno importante delle altre, è quella delle credenziali di accesso alle pagine di amministrazione dei siti web e relativi CMS di gestione (Wordpress, Joomla, Drupal, ecc), credenziali che permettono la modifica arbitraria dei siti web o la pubblicazione di pagine che a loro volta vengono utilizzate per campagne di phishing. Anche il furto delle credenziali di accesso ai cPanel dei domini è molto pericoloso, perché permette la modifica delle zone DNS, delle aree FTP, dei database associati al dominio.

Dalla nostra analisi abbiamo constato che vengono offerti gratuitamente dump in formato “raw” (quindi senza nessuna aggregazione) come sample della “bontà” della “merce” in vendita. In altri casi su alcune fonti attenzionate dalla nostra ricerca, vengono postati con frequenza giornaliera i “dump” liberamente scaricabili e pronti per una successiva elaborazione e utilizzo.

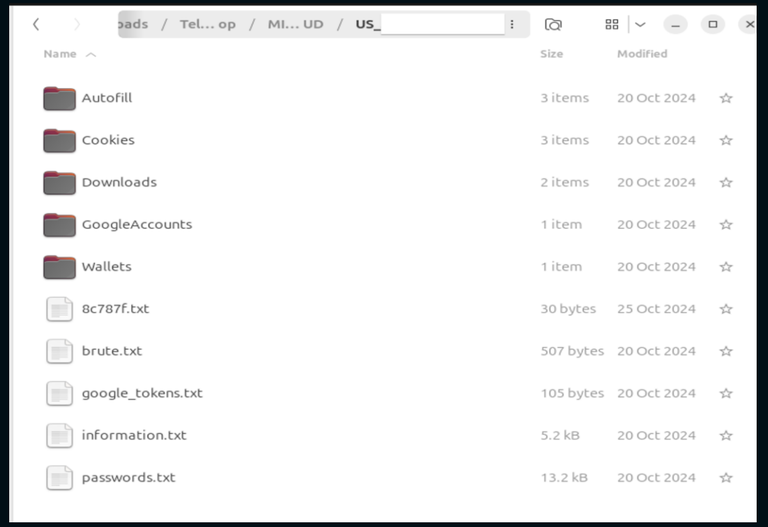
Dump RAW offerto liberamente

I dump contengono almeno 3 informazioni di base: l'URL del servizio a cui l'utente si è autenticato, il nome utente e la password in chiaro; dall'analisi condotta i dump contengono informazioni aggiuntive quali: la versione del sistema operativo, informazioni sul computer da cui le informazioni sono state rubate (es. CPU, RAM ecc), la nazione di provenienza (dedotta dalla geolocalizzazione dell'IP pubblico della connessione).



Dump delle informazioni sull'utente e il computer vittima

I dump da noi analizzati, che in generale sono quelli generati dagli infostealer e inviati ai server di comando per essere archiviati e successivamente elaborati contengono cookies di sessione (utili per tentare il bypass della autenticazione a 2 fattori o autenticarsi senza password nei siti internet), dump completi delle "casseforti" di password dei browser, dump dei dati di autofill, ecc.



Struttura di un pacchetto di dati esfiltrati

Passiamo ora all'approccio scientifico con cui abbiamo condotto la ricerca. Abbiamo messo a punto un sistema di data mining che si occupa di fare scraping di canali telegram utilizzando le API offerte dalla piattaforma di messaging Telegram.

Il sistema di scraping "#TelegramScrap: A comprehensive tool for scraping Telegram data" (SILVA, Ergon Cugler de Moraes. Web Scraping Telegram Posts and Content. feb 2023) è stato messo a punto da un ricercatore (Ergon Cugler de Moraes Silva), sviluppato in Python e messo a disposizione su Google Colab e repository GitHub. Lo strumento permette di definire:

- lo spazio temporale su cui condurre lo scraping dei post
- i canali telegram su cui condurre le attività di scraping
- la possibilità di inserire parole chiave da cercare all'interno dei post

Lo strumento produce un file in formato Apache Parquet, ossia un formato open source progettato per l'archiviazione e il recupero efficiente dei dati. Il sistema offre anche uno script di conversione dei dati da Parquet a Excel per una più agevole analisi dei dati.

Il dataset preso in considerazione è così composto:

- I dati analizzati provengono da 6 canali telegram e fanno riferimento un time frame dal 1 Giugno 2024 al 1 Dicembre 2024

SERVIZIO OFFERTO	PREZZO
1000 private logs (America/Europa/Africa/Asia/AU)	**69,00 $**
1000 private logs (country by your request)	**90,00 $**
SUBSCRIPTION ELITE - 1 WEEK	**100,00 $**
SUBSCRIPTION ELITE - 1 MONTH	**220,00 $**
SUBSCRIPTION ELITE - 6 MONTH	**1.000,00 $**
SUBSCRIPTION ELITE - LIFETIME	**1.270,00 $**
LOGS BY REQUEST - 1000 Facebook logs	**140,00 $**
LOGS BY REQUEST - 1000 PayPal logs	**120,00 $**
LOGS BY REQUEST - 1000 Bank logs	**189,00 $**
LOGS BY REQUEST - 1000 Crypto logs	**200,00 $**
Training guide "How to use logs" + 100 private logs for testing	**40,00 $**
8.694.600 Logs only 2023-2024 YEAR (Jan-Nov)	**Trattativa privata**

GDPR & PRIVACY

LINEE GUIDA PER GARANTIRE LA PROTEZIONE DEI DATI IN UN PANORAMA TECNOLOGICO IN CONTINUA EVOLUZIONE

Introduzione normativa

Il **Regolamento Generale sulla Protezione dei Dati (GDPR)** è entrato in vigore il 24 maggio 2016 e si applica a far data dal 25 maggio 2018; rappresenta una pietra miliare nella protezione dei dati personali in Europa, ma non è la prima norma che tratta tale argomento.

La storia della protezione delle informazioni personali inizia negli Stati Uniti alla fine del XIX secolo, quando si parla per la prima volta di privacy, separandola dalla protezione dei dati. La privacy si riferisce alla tutela della sfera privata dell'individuo (attività escludente), mentre la protezione dei dati riguarda tutte le informazioni su una persona (attività includente), come definito dal GDPR, che non parla mai di privacy, ma sempre di protezione dei dati.

Nel 1890 a Boston, con l'avvento della tecnologia, i media iniziano a pubblicare fotografie private, spingendo gli avvocati Warren e Brandeis a scrivere un articolo, *The Right to Privacy*, dove affermano che ogni individuo ha diritto alla riservatezza della sua vita privata, da difendere dall'intrusione di terzi o dello Stato.

Il concetto di privacy si diffonde anche in Europa, ma con un contesto differente: mentre negli USA si cerca di proteggersi da intrusi privati (giornali, aziende, persone), in Europa l'attenzione è rivolta alla protezione della sfera privata contro lo Stato. Questo interesse cresce nel periodo post-bellico, quando si temono ancora le intrusioni degli Stati, come quelli fascista e nazista. Le leggi fondamentali in Europa includono l'articolo 8 della CEDU (1950) e l'articolo 2 della Costituzione Italiana (1947), che sanciscono il diritto al rispetto della vita privata e dei diritti inviolabili dell'individuo.

Nel 1978, in Germania, viene adottata la prima legge nazionale per la protezione dei dati, seguita dalla Convenzione 108 del Consiglio d'Europa nel 1981. Con l'integrazione del mercato unico europeo e la creazione della Comunità Europea nel 1992, emerge la necessità di una normativa europea per la protezione dei dati personali. Nel 1995, viene emanata la Direttiva 46, che porta all'adozione del Codice Privacy in Italia (D.Lgs. 196/2003). Nel 2007, il Trattato di Lisbona conferisce valore giuridico alla Carta di Nizza, che inserisce il diritto alla protezione dei dati personali, base giuridica del GDPR.

Ma, con l'evoluzione della tecnologia, si è avuto anche l'evoluzione delle minacce alla privacy; la comparsa degli infostealer segna un'evoluzione delle minacce alla privacy, spostando il focus dalla difesa contro l'intrusione fisica da parte

di terzi (come i giornali o lo Stato, come nel caso della protezione della privacy storicamente discussa) alla protezione contro le minacce digitali. Mentre in passato le leggi sulla privacy e la protezione dei dati si concentravano sulla difesa della vita privata dall'intrusione fisica o da parte di entità pubbliche, con l'ascesa di internet e delle tecnologie digitali, la protezione dei dati personali è diventata una questione sempre più urgente. Gli infostealer

mettono in evidenza la vulnerabilità dei dati quando vengono archiviati e trasmessi in formati elettronici, un aspetto non completamente considerato dalle normative sulla privacy del passato.

Con l'obiettivo di garantire che i dati degli individui siano trattati in modo sicuro, trasparente e in conformità con le normative europee, il GDPR ha introdotto un insieme di regole più rigorose riguardanti, anche in un contesto digitale, la raccolta, l'elaborazione, la conservazione e la gestione dei dati personali, con l'intento di dare agli utenti maggiore controllo sulle proprie informazioni personali.

Il GDPR si basa su tre competenze specifiche:

- **gestionale:** chi determina le finalità e i mezzi del trattamento di dati personali è il titolare del trattamento in base alla propria organizzazione, in base alla tipologia della propria attività, in base ai processi aziendali e sistemi informativi, gestionali (art. 4)
- **cyber security:** riguarda la gestione dell'infrastruttura informatica e della rete da parte del titolare del trattamento o da quelle realtà che in qualità di amministratori di sistema esterni ne gestiscono la manutenzione e l'adeguamento ai cambiamenti tecnologici ed evoluzioni delle minacce informatiche (art. 25)
- **legale:** importante è l'aspetto legale del Regolamento, dato che si parla sempre di una normativa che prevede delle regole e misure da adottare. Capire il funzionamento dei processi aziendali, la suddivisione dei ruoli e i soggetti coinvolti nell'intero processo aziendale, sia all'interno che all'esterno.

In questo contesto, il GDPR è cruciale perché stabilisce le linee guida per garantire la protezione dei dati in un panorama tecnologico in continua evoluzione, dove le minacce alla sicurezza, come i cyber attacchi e i malware (inclusi gli infostealer), sono sempre più sofisticati.

La crescente diffusione degli infostealer e l'adozione di soluzioni di lavoro remoto hanno reso ancora più urgente la protezione dei dati personali contro tali minacce.

Il GDPR, sebbene non sia specificamente indirizzato alla protezione contro gli infostealer, fornisce un quadro legale che può contribuire significativamente alla mitigazione di questi attacchi, attraverso diverse disposizioni chiave:

- **Obbligo di protezione dei dati fin dalla progettazione (Privacy by Design) e per impostazione predefinita (Privacy by Default) art. 25 cons. 78:**
  - Il GDPR impone alle aziende di implementare misure di sicurezza tecniche e organizzative per garantire la protezione dei dati fin dall'inizio dei loro processi di trattamento. Questo include la protezione contro i malware come gli infostealer, con l'adozione di strumenti di crittografia, autenticazione multifattoriale (MFA) e soluzioni di monitoraggio avanzato - art. 32 cons. 74 75 76 77
  - Il principio di minimizzazione dei dati obbliga le aziende a raccogliere solo i dati strettamente necessari per uno scopo specifico. L'art. 5 specifica che i dati debbano essere "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati". Questo riduce la quantità di dati particolari (ex sensibili) che potrebbero essere rubati in caso di attacco.
- **Valutazione d'impatto sulla protezione dei dati (DPIA) art. 35 cons. 75, 84, 89, 90, 91, 92, 93:**
  - Le aziende sono tenute a condurre valutazioni di impatto sulla protezione dei dati (DPIA) quando intraprendono attività che potrebbero comportare rischi elevati per i diritti e le libertà degli individui. Questo può includere l'implementazione di nuove tecnologie o la gestione di dati particolarmente sensibili. Nel caso di attività che potrebbero esporre i dati a rischi derivanti da malware come gli infostealer, una DPIA aiuta a identificare vulnerabilità e a mitigare i rischi prima che possano concretizzarsi.
- **Diritti rafforzati per gli utenti (diritti degli interessati: artt. dal 15 al 22):**
  - il diritto all'accesso, alla rettifica, alla cancellazione (diritto all'oblio), alla limitazione del trattamento, alla portabilità dei dati, al diritto di opposizione, al diritto di reclamo all'Autorità di controllo (art. 77). In caso di attacco da infostealer, la maggior parte dei diritti risultano essere NON applicabili; sarà valutata l'applicabilità in base al tipo di attacco subito dall'azienda.

- **Responsabilità delle aziende (accountability):**
  - le organizzazioni sono tenute ad adottare misure adeguate a proteggere i dati personali, dimostrando la conformità alle normative attraverso audit e documentazione.
- **Notifiche obbligatorie in caso di violazioni (art.33):**
  - in caso di violazione dei dati personali, le aziende devono notificare l'incidente entro 72 ore da quando si viene a conoscenza dell'incidente all'autorità di protezione dei dati e agli utenti interessati, se necessario. Questo obbligo di trasparenza aiuta a limitare i danni, avvisando rapidamente gli utenti sui rischi derivanti dalla violazione.
- **Formazione continua dei dipendenti (art. 29, 32):**
  - Il GDPR sottolinea l'importanza di formare e sensibilizzare i dipendenti riguardo alla sicurezza dei dati, per prevenire minacce come il phishing, che spesso è il vettore di infezione per gli infostealer. Sensibilizzare i dipendenti sui pericoli degli attacchi di social engineering e su come adottare pratiche sicure di gestione dei dati è un elemento cruciale per ridurre il rischio di compromettere i dati personali aziendali.
- **Monitoraggio e audit dei sistemi:**
  - Il GDPR impone alle aziende di implementare un sistema di monitoraggio per rilevare attività sospette che possano indicare un attacco informatico, come quelli condotti da infostealer. Il monitoraggio continuo dei sistemi aziendali permette di identificare rapidamente eventuali compromissioni dei dati e di intervenire tempestivamente.

IMPATTI SULLA PRIVACY

UNO SGUARDO IN RELAZIONE AI PRINCIPI DEL GDPR

Violazione della riservatezza:

Il GDPR pone un grande accento sulla protezione della Riservatezza, Integrità, Disponibilità (RID) del dato. L'articolo 32 stabilisce che le aziende devono garantire il corretto trattamento dei dati: trattati in modo sicuro, con adeguate misure tecniche e organizzative, garantendo la riservatezza dei dati personali. Gli infostealer minano la riservatezza dei dati, rubando informazioni riservate da sistemi aziendali o dispositivi personali, tramite attacchi di phishing, malware e altre tecniche invasive.

In che modo l'infostealer può minare la riservatezza del dato? Ad esempio attraverso:

- furto di credenziali: gli infostealer sono spesso progettati per raccogliere username e password da browser, applicazioni di gestione delle credenziali e altre fonti, che possono essere utilizzate per accedere a sistemi aziendali e rubare dati sensibili.
- intercettazione dei dati: possono raccogliere informazioni riservate come dettagli bancari, numeri di carte di credito, comunicazioni riservate, contratti aziendali e altro. La riservatezza dei dati viene violata quando questi dati vengono trasferiti o venduti a malintenzionati, esponendo gli individui e le organizzazioni a rischi significativi.
- compromissione di sistemi aziendali: un infostealer che infetta un sistema aziendale potrebbe ottenere accesso a una vasta gamma di dati personali, violando le misure di sicurezza previste dall'articolo 32, che stabilisce che i dati devono essere protetti contro la perdita, distruzione o accesso non autorizzato.

Raccolta illecita di dati personali:

L'articolo 5 del GDPR illustra quali siano i principi applicabili al trattamento dati e stabilisce che i dati personali devono essere:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Attraverso un infostealer, le organizzazioni si trovano, a loro insaputa, a subire una raccolta illecita di dati quali:

- credenziali d'accesso: gli infostealer sono specializzati nel raccogliere credenziali di accesso (username e password) da sistemi e servizi online. Questa raccolta di dati avviene senza il consenso esplicito dell'utente e può permettere ai malintenzionati di compromettere ulteriori informazioni personali o aziendali.
- informazioni finanziarie: uno degli obiettivi principali di questi malware è raccogliere informazioni particolari (ex sensibili), come numeri di carte di credito, conti bancari, dati fiscali e transazioni finanziarie. La raccolta di questi dati personali senza il consenso dell'utente costituisce una violazione palese della norma sulla licenza del trattamento dei dati.
- dati personali particolari (ex sensibili): gli infostealer possono anche essere utilizzati per raccogliere dati personali particolari, come numeri di previdenza sociale, dati sulla salute o altre informazioni protette, che sono soggette a restrizioni ancora più severe in base al GDPR (artt. 6 e 9).

I danni che possono ricadere sugli interessati possono essere di vario genere:

- danni fisici
- danni psicologici
- altri danni materiali
- danni economici
- danni sociali
- perdite finanziarie
- furto o usurpazione identità
- pregiudizio alla reputazione
- discriminazione

Di importanza rilevante è la valutazione dei rischi sui trattamenti dei dati (che coinvolge il RID - Riservatezza, Integrità, Disponibilità dei dati - su tutti i trattamenti effettuati dall'azienda) che l'organizzazione deve implementare e aggiornare ogni qualvolta si implementi un nuovo trattamento in azienda o nel caso di una violazione dei dati con coinvolgimento dei dati di interessati.

Responsabilità del trattamento dati:

Il GDPR stabilisce chiaramente che le aziende e gli organismi che trattano i dati personali sono responsabili della protezione dei dati stessi, e in caso di violazione, devono rispondere adeguatamente e tempestivamente. L'articolo 24 del GDPR attribuisce alle aziende la responsabilità (accountability) di garantire che siano implementate adeguate misure di sicurezza per proteggere i dati personali trattati.

Come devono agire le aziende che gestiscono dati personali compromessi:

Notifica delle violazioni: in caso di violazione dei dati personali dovuta a un attacco da infostealer, le aziende devono notificare l'incidente entro 72 ore da quando l'azienda ha preso coscienza di essere sotto attacco all'autorità competente e agli individui interessati (articolo 33 e 34 del GDPR). Caso diverso se l'azienda rientra all'interno della Direttiva NIS 2 dove i tempi e le modalità di attuazione cambiano. Da quando si viene a conoscenza di un incidente di impatto significativo, l'azienda deve dare un preallarme allo CSIRT entro le 24 ore con informazioni anche minime, ma precise. Le ulteriori comunicazioni dopo 72 ore e ulteriormente dopo un mese per le ultime informazioni. È interessante evidenziare che se vengono violati dati personali

all’interno di una azienda in NIS 2, la normativa di riferimento che prende il sopravvento è la Direttiva stessa. Ovviamente resta obbligatoria la segnalazione presso l’Ente del Garante per la protezione dei dati personali nel caso di compromissione di dati personali.

Responsabilità per il trattamento non sicuro: se un'azienda non ha adottato misure di sicurezza adeguate per proteggere i dati personali (ad esempio, crittografia, autenticazione forte, monitoraggio costante), potrebbe essere ritenuta responsabile per la violazione dei dati. Il mancato rispetto delle disposizioni del GDPR sulla sicurezza dei dati potrebbe comportare sanzioni che arrivano fino al 4% del fatturato annuale globale.

Rischio reputazionale: oltre alle sanzioni economiche, una violazione dei dati causata da un infostealer potrebbe danneggiare gravemente la reputazione dell'azienda, minando la fiducia dei clienti e dei partner commerciali. La responsabilità di proteggere i dati personali non riguarda solo le implicazioni legali, ma anche l'integrità dell'azienda sul mercato.

Conformità, sanzioni e prevenzione

Per le aziende, rispettare i principi e i requisiti del GDPR è essenziale non solo per evitare sanzioni severe, ma anche per proteggere la fiducia dei clienti e garantire la sicurezza dei dati personali. La prevenzione, la corretta notifica delle violazioni, e l'adozione di misure proattive, come cifratura, segmentazione dei dati e formazione continua del personale, sono passaggi chiave per mitigare i rischi associati agli infostealer e altre minacce informatiche. Le aziende devono essere pronte a rispondere in modo rapido ed efficace, riducendo così il rischio di violazioni gravi, le potenziali sanzioni legali ed economiche e gli eventuali risarcimenti danni.

Segnalazione di violazioni (articolo 33):

L'articolo 33 del GDPR stabilisce l'obbligo per le aziende di notificare le violazioni dei dati personali alle autorità di protezione dei dati, nonché agli interessati, nei casi in cui la violazione possa comportare un rischio che lede i loro diritti e libertà. La tempestività e l'accuratezza della notifica sono cruciali per la conformità al GDPR.

1. Notifica alle autorità competenti: se una violazione dei dati personali è stata accertata, le aziende devono informare l'autorità competente per la protezione dei dati entro 72 ore dall'avvenuto accertamento della violazione. La

notifica deve contenere informazioni dettagliate, come la natura della violazione, i dati coinvolti, le possibili conseguenze e le misure adottate per mitigarne gli effetti.

2. Notifica agli interessati (arti. 34): se la violazione comporta un rischio elevato per i diritti e le libertà degli interessati (ad esempio, furto di credenziali, accesso a dati bancari, ecc.), l'azienda deve informare direttamente gli utenti senza ingiustificato ritardo. Questo permette agli utenti di prendere misure preventive (ad esempio, cambiare le password) per proteggere i propri dati.
3. Contenuto della notifica: la notifica deve essere chiara e contenere informazioni essenziali, come la descrizione della violazione, le categorie di dati compromessi, le misure intraprese dall'azienda per affrontare la violazione e le azioni che gli utenti possono intraprendere per proteggere sé stessi. È bene scrivere all'interno della comunicazione un indirizzo mail per poter dare agli interessati la possibilità di richiedere ulteriori informazioni. Nel caso di compromissioni di tantissimi interessati è consigliabile effettuare anche una comunicazione attraverso comunicato stampa.
4. Rilevanza in caso di infostealer: un attacco da infostealer che comporti la raccolta di credenziali o altre informazioni particolari impone una risposta rapida e trasparente. Il ritardo nella notifica o l'assenza di una comunicazione adeguata può esporre l'azienda a sanzioni e danneggiare la sua reputazione.

Sanzioni amministrative

Le sanzioni sono disciplinate dagli articoli 83 ed 84 del GDPR. Ogni autorità di vigilanza (in Italia l'Ente del Garante per la protezione dei dati personali) deve garantire, in ogni singolo caso, che la sanzione sia effettiva, proporzionata e dissuasiva.

Sanzioni afflittive

Fino a 10 milioni di euro, o per le imprese, fino al 2% del fatturato annuo globale dell'esercizio precedente, nei casi di:

- inosservanza degli obblighi del titolare e del responsabile del trattamento;
- inosservanza degli obblighi dell'organismo di certificazione;
- inosservanza degli obblighi dell'organismo di controllo.

Fino a 20 milioni di euro, o per le imprese, fino al 4% del fatturato annuo globale dell'esercizio precedente, nei casi di:

- inosservanza dei principi base del trattamento; inosservanza dei diritti degli interessati;

- inosservanza delle disposizioni sul trasferimento dei dati personali in paesi terzi o verso organizzazioni internazionali;
- inosservanza di un ordine, limitazione provvisoria o definitiva o di un ordine di sospensione dei flussi da parte dell'autorità di controllo. Inosservanza di un ordine correttivo dell'autorità di controllo.

Sanzioni correttive

L'Autorità di controllo può:

- rivolgere avvertimenti/ammonimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono violare il GDPR o l'abbiano violato;
- ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i relativi diritti, nonché di conformare i trattamenti alle disposizioni del GDPR, anche specificando in che modo e dentro quale termine;
- ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali;
- imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;
- ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali;
- revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti;
- infliggere una sanzione amministrativa pecuniaria in aggiunta alle presenti misure;
- ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

Di seguito il dettaglio ed i parametri utilizzati per eventuali sanzioni:

- la natura, la gravità e la durata della violazione, anche in considerazione del numero degli interessati e dei danni da questi subiti;
- il carattere intenzionale o colposo dell'infrazione;

- le azioni intraprese dal titolare o del responsabile, anche sotto il profilo tecnico, e le misure organizzative attuate per prevenire le violazioni;
- eventuali rilevanti violazioni precedenti da parte del titolare o del responsabile;
- il livello di cooperazione con l'autorità di vigilanza, al fine di porre rimedio alla violazione e mitigarne i possibili effetti negativi;
- le categorie di dati personali oggetto della violazione;
- il modo in cui l'autorità di controllo è venuto a conoscenza della violazione (notifica);
- il rispetto di eventuali provvedimenti precedentemente imposti dall'autorità di controllo;
- l'adesione a codici di condotta o a meccanismi di certificazione riconosciuti;
- ogni altro fattore aggravante o attenuante applicabile alle circostanze del caso;
- i benefici finanziari ottenuti, o le perdite evitate, direttamente o indirettamente, per effetto della violazione commessa.

Se il titolare o il responsabile hanno commesso, intenzionalmente o per negligenza, più violazioni alle disposizioni del Regolamento connesse a una stessa operazione di trattamento di dati personali, l'importo totale della sanzione non dovrà superare l'importo indicato per la violazione più grave.

Con il Regolamento Europeo non vengono abrogati i provvedimenti del Garante; pertanto, detti provvedimenti restano in vigore e la loro violazione è sanzionata come previsto dall'art.162 (altre fattispecie) del suddetto Decreto 196/03. Per esempio, la violazione del provvedimento relativo all'Amministratore di Sistema viene sanzionata dall'art.162 comma 2ter come inosservanza di provvedimenti con una sanzione che prevede il pagamento di una somma da trentamila euro a centottantamila euro.

Oltre alle sanzioni amministrative vi sono dei risvolti penali che possono colpire le aziende.

Sanzioni penali

Art. 167 Codice Privacy – Trattamento illecito di dati:

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2 sexies e 2 octies, o delle misure di garanzia di cui all'articolo 2 septies ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2 quinquiesdecies arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni.

3. Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per se' o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento all'interessato.

4. Il Pubblico ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante.

5. Il Garante trasmette al pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attività di accertamento nel caso in cui emergano elementi che facciano presumere l'esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al più tardi al termine dell'attività di accertamento delle violazioni delle disposizioni di cui al presente decreto.

6. Quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita.

Art. 167 bis Codice Privacy – Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala

1. Salvo che il fatto costituisca più grave reato, chiunque comunica o diffonde al fine di trarre profitto per sé o altri ovvero al fine di arrecare danno, un archivio

automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli 2-ter, 2-sexies e 2-octies, è punito con la reclusione da uno a sei anni.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, è punito con la reclusione da uno a sei anni, quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione.

3. Per i reati di cui ai commi 1 e 2, si applicano i commi 4, 5 e 6 dell'articolo 167.

Art. 167 ter Codice Privacy – Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala

1.Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per se' o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala è punito con la reclusione da uno a quattro anni.

2. Per il reato di cui al comma 1 si applicano i commi 4, 5 e 6 dell'articolo 167.

Art.168 Codice Privacy - Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante

Viene punito chiunque, durante gli accertamenti di fronte al Garante, dichiari il falso o presenti documenti non veri. Ma, anche chi intenzionalmente interrompa o impedisca il corretto svolgimento di un procedimento presso il Garante può subire una sanzione.

Art.170 Codice Privacy – Inosservanza di provvedimenti del Garante

Se non vengono rispettate le decisioni del Garante, è sempre prevista come sanzione la pena detentiva

Art.171 Codice Privacy – Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori

Continua ad essere punito l'utilizzo di impianti audiovisivi utilizzati per controllare a distanza i propri dipendenti, se non è stato prima concordato con le parti in questione. È vietato, inoltre, svolgere indagini per conoscere le opinioni politiche, religiose e le appartenenze sindacali di un lavoratore, prima di decidere se assumerlo o meno (permangono le sanzioni di cui all'art. 38 dello Statuto dei Lavoratori L. 300/1970).

Art.172 Codice Privacy – Pene accessorie

La condanna per uno dei delitti previsti dal presente codice importa la pubblicazione della sentenza.

Le implicazioni legali possono ricadere nella:

- **responsabilità civile e penale:** le aziende potrebbero essere soggette anche a richieste di risarcimento danni da parte degli interessati colpiti dalla violazione dei dati. Gli interessati potrebbero fare causa per danni diretti (ad esempio, frodi finanziarie) derivanti dalla raccolta illecita delle loro informazioni sensibili.
- **controlli e audit:** le autorità competenti potrebbero eseguire audit per verificare se le misure di protezione dei dati siano state adottate correttamente. Se una violazione è stata causata dalla negligenza nell'implementare misure di sicurezza adeguate contro attacchi come quelli da infostealer, l'azienda potrebbe essere ritenuta colpevole di non aver rispettato le disposizioni del GDPR.

La responsabilità, in virtù del principio di *accountability*, è in capo al titolare del trattamento e non è "delegabile". Il GDPR specifica che il titolare del trattamento deve essere in grado di dimostrare la liceità del trattamento stesso; di seguito si riporta l'art. 24 par. 1 GDPR: *"Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario."*

Per quanto riguarda il risarcimento del danno, il Considerando 146 del Regolamento sottolinea che *"Il titolare del trattamento o il responsabile del trattamento dovrebbe risarcire i danni cagionati a una persona da un trattamento non conforme al presente regolamento ma dovrebbe essere esonerato da tale responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile."*

Qualora i titolari del trattamento o i responsabili del trattamento siano coinvolti nello stesso trattamento, ogni titolare del trattamento o responsabile del trattamento sarà chiamato a rispondere in solido per la totalità del danno, salvo dimostri che l'evento dannoso non gli sia imputabile e fermo restando, in ogni caso, il diritto di proporre un'azione di regresso nei confronti degli altri titolari o responsabili coinvolti nel medesimo trattamento.

Il risarcimento del danno viene rafforzato anche dall'art. 82 GDPR che stabilisce che *"Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento".*

È necessario specificare che un titolare del trattamento risponde per il danno cagionato dal trattamento che violi il Regolamento, mentre il soggetto nominato responsabile del trattamento ai sensi dell'art. 28 GDPR risponde solo in caso di inadempimento degli obblighi del GDPR specificatamente diretti ai responsabili del trattamento ovvero qualora abbia agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

Misure di mitigazione

La prevenzione è cruciale per ridurre i rischi derivanti da infostealer e altre minacce informatiche. Il GDPR enfatizza l'adozione di misure proattive per proteggere i dati personali, e le aziende devono implementare misure di sicurezza tecniche e organizzative adeguate per evitare violazioni. Interessante è la figura del DPO (artt. 37, 38, 39) che viene vista come una misura di sicurezza tecnico organizzativa.

Di seguito vengono riportati alcune misure di mitigazione del rischio

- La crittografia è una delle misure di sicurezza più efficaci contro gli attacchi da infostealer. Crittografando i dati, anche se un malintenzionato riesce ad accedere ai sistemi aziendali, i dati sottratti non saranno leggibili senza le chiavi di decrittazione. Il GDPR enfatizza che i dati particolari devono essere protetti da misure adeguate, e la crittografia è una delle soluzioni più raccomandate.
- La segmentazione dei dati consiste nel separare i dati in "blocchi" o "settori", rendendo più difficile l'accesso non autorizzato. Se un infostealer compromette una parte del sistema, la segmentazione riduce il rischio che l'attaccante ottenga accesso a tutti i dati sensibili.
- Controlli di accesso: implementare una gestione rigorosa dei privilegi di accesso assicura che solo i dipendenti autorizzati possano accedere ai dati sensibili. Limitarne l'accesso riduce la possibilità che i dati vengano compromessi in caso di attacco.

- Monitoraggio continuo: le aziende devono monitorare costantemente i loro sistemi informatici per rilevare attività sospette che possano indicare un'infezione da infostealer. L'uso di strumenti di rilevamento delle minacce avanzate e sistemi di gestione delle informazioni sulla sicurezza (SIEM) aiuta a identificare e rispondere rapidamente agli attacchi.
- Formazione del personale: la formazione regolare dei dipendenti su come riconoscere e reagire a tentativi di phishing e altre tecniche di social engineering è fondamentale per ridurre il rischio che un infostealer venga installato nei sistemi aziendali. La consapevolezza del personale è una delle prime linee di difesa contro questi attacchi.
- Aggiornamenti e patching regolari: mantenere software e sistemi operativi aggiornati è essenziale per ridurre le vulnerabilità che possono essere sfruttate dagli infostealer. Le aziende devono implementare un processo rigoroso di aggiornamenti regolari per risolvere eventuali falle di sicurezza.

Collegamento con normative globali

Le normative che si occupano della protezione dei dati sono molteplici e vengono applicate in contesti diversi dalla Comunità Europea. Alcune di queste normative condividono principi simili, come la protezione dei dati personali e la trasparenza nei confronti degli interessati, ma presentano anche differenze significative nel modo in cui vengono implementate e nel loro ambito di applicazione. Un esempio importante di normativa che regola la protezione dei dati è il California Consumer Privacy Act (CCPA), che si applica negli Stati Uniti, nello stato della California, ma con implicazioni per le aziende a livello globale, data la sua portata. Le aziende che operano a livello internazionale, e in particolare quelle che trattano dati personali di residenti sia nell'UE che in California, devono assicurarsi di essere conformi a entrambe le normative. Questo richiede un approccio integrato alla protezione dei dati, che tenga conto delle diverse esigenze normative e delle best practices di sicurezza. Ma quali sono le differenze tra le due normative? Di seguito un breve confronto tra il GDPR e il CCPA in relazione alla protezione dei dati contro minacce come gli infostealer e ad altre problematiche legate alla privacy.

Ambito di applicazione

- ***GDPR**: si applica a tutte le aziende che trattano dati personali di residenti nell'Unione Europea, indipendentemente da dove si trovano le aziende. La sua portata è globale, in quanto include qualsiasi azienda che fornisce beni o servizi a persone nell'Unione Europea, o che monitora il loro comportamento.*
- ***CCPA**: si applica alle aziende che raccolgono, utilizzano o condividono i dati personali dei residenti in California. È principalmente focalizzato sulle aziende con sede in California o che fanno affari con i californiani. Tuttavia, la sua applicabilità si estende anche alle aziende che soddisfano determinati criteri di fatturato o volume di dati trattati.*

Definizione di dati personali

- ***GDPR**: definisce i dati personali come "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale". Include anche dati particolari, come informazioni su razza, etnia, opinioni politiche, religioni, e dati sanitari.*
- CCPA: anche il CCPA definisce i dati personali come "informazioni che identificano, si riferiscono a, descrivono, sono ragionevolmente associabili a, o potrebbero ragionevolmente essere collegate, direttamente o indirettamente, a un particolare consumatore o nucleo familiare". Tuttavia, il CCPA non ha una categoria separata di dati sensibili come nel GDPR, pur trattando categorie particolari di dati, come quelli finanziari o relativi alla geolocalizzazione, con misure specifiche.

Diritti degli interessati

- ***GDPR**: fornisce diritti completi agli utenti, inclusi il diritto di accesso, rettifica, cancellazione, limitazione del trattamento, portabilità dei dati, e opposizione al trattamento, revoca del consenso, diritto di produrre reclamo all'autorità di controllo. Il diritto di accesso ai dati personali è particolarmente importante in caso di attacchi da infostealer, poiché consente agli utenti di sapere quali dati sono stati compromessi e se sono stati utilizzati per scopi illeciti.*

- ***CCPA**: concede ai consumatori il diritto di sapere quali dati personali vengono raccolti su di loro, il diritto di richiedere l'eliminazione dei propri dati e il diritto di opt-out (cioè di non consentire la vendita dei propri dati a terzi). Tuttavia, rispetto al GDPR, non offre un diritto esplicito alla portabilità dei dati o un diritto di correzione.*

Notifica delle violazioni:

- ***GDPR**: le aziende devono notificare alle autorità di protezione dei dati le violazioni di dati entro 72 ore dall'avvenuto accertamento della violazione e, se necessario, agli utenti coinvolti, se la violazione comporta un rischio elevato per i diritti e le libertà degli interessati.*
- ***CCPA**: anche il CCPA richiede alle aziende di notificare agli interessati in caso di violazione dei dati, ma il periodo di notifica non è così stretto come quello del GDPR. Il CCPA impone che le notifiche siano inviate entro un periodo ragionevole, ma senza specificare un tempo preciso come nel GDPR.*

Sanzioni

- ***GDPR**: le violazioni del GDPR possono comportare sanzioni molto severe, che vanno fino al 4% del fatturato annuale globale o fino a 20 milioni di euro (a seconda* di quale cifra sia maggiore). *Le sanzioni sono proporzionali alla gravità della violazione e all'entità del danno subito dalle persone interessate.*
- ***CCPA**: il CCPA prevede sanzioni per le violazioni che vanno da 2.500 USD per ogni violazione non intenzionale a 7.500 USD per violazione intenzionale. Sebbene le multe siano inferiori rispetto al GDPR, le aziende possono essere anche citate in giudizio dai consumatori per danni derivanti dalla violazione della privacy.*

Misure di protezione dei dati

- ***GDPR: il GDPR richiede che le aziende implementino misure di sicurezza tecniche e organizzative adeguate, come la cifratura dei dati e l'adozione di politiche per prevenire la perdita e l'accesso non autorizzato ai dati. Le aziende devono condurre una valutazione dell'impatto sulla protezione dei dati (DPIA) quando trattano dati che potrebbero comportare un alto rischio per la privacy degli utenti.***
- ***CCPA: anche il CCPA incoraggia l'adozione di misure di sicurezza per proteggere i dati personali, ma non è dettagliato come il GDPR riguardo alle misure specifiche da implementare. Tuttavia, il CCPA richiede che le aziende forniscano ai consumatori la possibilità di controllare la raccolta e l'uso dei propri dati, rendendo essenziale la trasparenza sulle pratiche aziendali di trattamento dei dati.***

ISO/IEC 27001:2022

La norma **ISO/IEC 27001:2022** è una versione aggiornata dello standard internazionale per la gestione della sicurezza delle informazioni che fornisce un insieme di controlli di riferimento per la sicurezza delle informazioni basati sulle best practices internazionali, la cui implementazione viene guidata dalla norma ISO/IEC 27002.

La **ISO/IEC 27001:2022** applica un approccio sistemico e integrato per mitigare il rischio legato alle minacce informatiche, tra cui anche gli infostealer. Attraverso una combinazione di misure preventive, rilevative e reattive, l'organizzazione può proteggere i suoi sistemi informatici e i dati da questo tipo di minaccia. L'adozione di un sistema di gestione per la sicurezza delle informazioni basato sullo standard ISO/IEC 27001:2022 aiuta le organizzazioni a creare una cultura di sicurezza e robusti controlli che rendono più difficile per gli infostealer avere successo e, in caso di violazione, limita i danni.

Sebbene i principi generali della versione 2022 non siano drasticamente diversi rispetto alla precedente, questa edizione ha migliorato e raffinato alcuni aspetti legati alla gestione della sicurezza e al trattamento delle minacce emergenti, come gli infostealer.

Tra le principali novità, è sicuramente di preminente attenzione l'introduzione di un nuovo controllo di sicurezza molto importante all'interno dell'annex A, ovvero quello relativo alla Threat Intelligence.

Il nuovo controllo prevede che le informazioni sulle minacce di sicurezza devono essere raccolte e analizzate ai fini della Threat Intelligence, con lo scopo di rendere consapevoli le organizzazioni delle appropriate misure di mitigazione che devono mettere in campo.

L'attuazione di questo controllo prevede che, tra le altre cose, siano identificate e analizzate le informazioni raccolte dalle fonti interne ed esterne.

Questo nuovo controllo di sicurezza ha ovviamente una diretta correlazione con il problema degli infostealer in quanto l'attività di Threat Intelligence contribuisce a rendere consapevoli le organizzazioni dei principali infostealer in corso di diffusione e delle misure di detection e mitigazione, ovvero può rilevare informazioni esfiltrate dagli infostealer e già rese disponibili nei canali del dark web. Queste potrebbero essere coppie di username e password, utilizzabili per un accesso iniziale all'infrastruttura dell'organizzazione.

Risulta quindi evidente che l'attività di Threat Intelligence sia fondamentale per una difesa efficace.

La norma ISO/IEC 27001 inoltre, sempre ci fornisce ulteriori indicazioni sui controlli e sulle procedure di sicurezza volte a gestire la riservatezza dei dati che, ovviamente, è minata dall'azione degli infostealer.

La ISO/IEC 27001:2022 dunque si applica specificamente alla mitigazione degli infostealer nei seguenti punti:

1. Valutazione e gestione del rischio (punto 8.2 - 8.3 e Annex A)

- **Identificazione e valutazione dei rischi**: La gestione del rischio è fondamentale per affrontare le minacce legate agli infostealer. La versione 2022 della norma enfatizza la necessità di aggiornare regolarmente la valutazione dei rischi, in modo che le organizzazioni possano identificare tempestivamente minacce come gli infostealer e valutare il rischio associato a tale minaccia.
- **Risposta ai rischi**: Una volta identificato il rischio degli infostealer, la norma richiede l'adozione di misure per ridurre, trasferire o accettare il rischio, a seconda della gravità e delle risorse disponibili. Ad esempio, la riduzione del rischio potrebbe comportare l'implementazione di software antivirus, l'adozione di un sistema di controllo degli accessi o l'implementazione di soluzioni di monitoraggio avanzate.
- **Come implementare operativamente questo requisito:** sono reperibili online svariati tools di valutazione e gestione del rischio. Uno strumento molto valido è quello elaborato da Cesare Gallotti, per il quale maggiori informazioni sono reperibili al sito https://blog.cesaregallotti.it/
- **Errori comuni nell'implementazione del requisito:** considerare la valutazione dei rischi come un mero adempimento documentale, aggiornare la valutazione dei rischi a cadenza periodica senza considerare eventuali necessità derivanti da minacce emergenti, utilizzare metodologie inadeguate che non consentono di far emergere reali rischi, definire un piano di trattamento del rischio che rimane "sulla carta".

2. Controllo degli accessi e delle identità (Annex A, Controllo A.5.15 A.5.16)

- **Controllo degli accessi basato sul rischio**: La ISO/IEC 27001:2022 richiede una gestione rigorosa degli accessi. La protezione dalle minacce come gli infostealer dipende anche dalla capacità di prevenire l'accesso non autorizzato

ai sistemi. Ciò include il rafforzamento delle politiche di autenticazione, come l'adozione di sistemi di autenticazione multifattore (MFA), sistemi IAM (gestione delle identità e degli accessi), che rendono molto più difficile per gli attaccanti accedere alle risorse aziendali.

- **Gestione degli account e dei privilegi**: La norma sottolinea il principio del "minimo privilegio", che limita l'accesso alle informazioni solo a chi ne ha realmente bisogno. Questo aiuta a prevenire che un infostealer ottenga privilegi elevati per rubare dati sensibili.

- **Come implementare operativamente questo requisito:** password robuste, MFA, token fisici, certificati digitali sono alcuni delle semplici azioni che si possono adottare da subito. Inoltre tutti gli utenti non dovrebbero operare ordinariamente con privilegi amministrativi (nè locali nè tantomeno di dominio) e, in caso di sistemi windows, lo UAC (controllo account utente) dovrebbe essere impostato al massimo livello. Nessun utente comune infine dovrebbe aver possibilità di eseguire script (es. script Powershell).

- **Errori comuni nell'implementazione del requisito:** password non robuste e assenza di autenticazione multifattore sono le principali lacune per le aziende, unitamente al riuso di credenziali identiche su più sistemi. Altra problematica frequente è la libertà totale da parte degli utenti comuni di installare applicazioni sui sistemi in quanto amministratori della propria macchina. Questo espone l'azienda ad un gravissimo rischio di esecuzione di malware.

3. Protezione dalle minacce informatiche (Annex A, Controllo A.8.7 A.8.8)

- **Sicurezza operativa**: La **ISO/IEC 27001:2022** enfatizza l'importanza di monitorare e proteggere costantemente i sistemi informatici. Implementare soluzioni anti-malware aggiornate e di livello enterprise su tutte le risorse aziendali è un passo cruciale per proteggersi contro gli infostealer.

- **Aggiornamenti di sicurezza**: Una parte fondamentale nella protezione contro gli infostealer è mantenere aggiornato il software, applicando regolarmente le patch di sicurezza per risolvere vulnerabilità che potrebbero essere sfruttate dai malware. La ISO/IEC 27001:2022 richiede l'adozione di un processo per la gestione delle vulnerabilità e degli aggiornamenti di sicurezza.

- **Come implementare operativamente questo requisito:** acquistare soluzioni evolute di livello enterprise per la protezione dal malware, come ad esempio EDR / XDR, dai principali e blasonati vendor. Implementare procedure di patching dei sistemi, considerando la necessità di applicazione tempestiva degli aggiornamenti e la necessità di mantenere comunque la disponibilità dei sistemi (ad esempio è possibile implementare una policy di aggiornamento a gruppi di macchine per evitare indisponibilità in caso qualcosa andasse storto durante gli aggiornamenti).

- **Errori comuni nell'implementazione del requisito:** utilizzare antivirus free o di livello home, non applicare regolarmente le patch di sicurezza su tutti gli apparati (incluse stampanti, switch, firewall, etc), utilizzare sistemi operativi "end of life", utilizzare versioni craccate di software potenzialmente vettori di malware.

4. Monitoraggio e gestione degli incidenti di sicurezza (Annex A, Controllo A.8.15 A.8.16 A.5.24 A.5.25 A.5.26)

- **Rilevamento delle minacce**: La versione 2022 della norma spinge verso l'adozione di sistemi di monitoraggio continuo che siano in grado di rilevare attività sospette o anomale, che potrebbero indicare la presenza di un infostealer. Ciò può includere il monitoraggio dei log di sistema e l'utilizzo di strumenti avanzati per la rilevazione di attacchi, come quelli che sfruttano l'intelligenza artificiale per identificare comportamenti dannosi.

- **Gestione degli incidenti**: In caso di un attacco da infostealer, la **ISO/IEC 27001:2022** prevede che l'organizzazione abbia in atto un piano di risposta agli incidenti. Questo piano dovrebbe includere la capacità di isolare rapidamente i sistemi compromessi, raccogliere prove per l'analisi post-incidente e informare tempestivamente tutte le parti coinvolte.

- **Come implementare operativamente questo requisito:** acquistare soluzioni evolute di rilevamento e mitigazione delle minacce, adottare un SIEM, contrattualizzare un SOC (security operation center) 24/24 7/7. Redigere e testare un piano di incident response, business continuity e disaster recovery.

- **Errori comuni nell'implementazione del requisito:** disporre di log ma non sottoporli ad analisi, disporre di sistemi di registrazione dei log che non garantiscono inalterabilità. Ulteriore grave errore nella gestione della sicurezza di un'organizzazione è non disporre di procedure di risposta agli incidenti.

5. Formazione e sensibilizzazione (Annex A, Controllo A.6.3)

- **Educazione del personale**: Gli infostealer si diffondono spesso attraverso attacchi di phishing o altre tecniche di social engineering; quindi, la formazione continua del personale è cruciale. La **ISO/IEC 27001:2022** mette in evidenza la necessità di programmi di sensibilizzazione che aiutino i dipendenti a riconoscere le minacce legate agli infostealer, come e-mail sospette o link pericolosi.
- **Test di phishing**: La norma suggerisce anche l'adozione di esercitazioni di phishing simulate per allenare i dipendenti a identificare tentativi di furto di informazioni.
- **Come implementare operativamente questo requisito:** pianificare periodicamente la formazione per il personale e verificarne sul campo l'efficacia.
- **Errori comuni nell'implementazione del requisito:** effettuazione di formazione standard non personalizzata sulle caratteristiche e sulle minacce che possono impattare l'organizzazione. Ulteriore tipico errore è l'esecuzione di una formazione "una tantum" senza effettuare aggiornamenti successivi.

6. Sicurezza delle comunicazioni e protezione dei dati (Annex A, Controllo A.8.24)

- **Protezione dei dati sensibili**: Gli infostealer spesso mirano a esfiltrare informazioni riservate. La **ISO/IEC 27001:2022** sottolinea l'importanza di criptare i dati sensibili, sia in transito che a riposo, per evitare che vengano intercettati o modificati durante il loro trasferimento.
- **Comunicazioni sicure**: L'adozione di protocolli sicuri per la comunicazione (come TLS/SSL) è una misura prevista dalla norma per proteggere i dati durante la trasmissione, contribuendo a prevenire che vengano rubati da infostealer o attacchi simili.
- **Come implementare operativamente questo requisito:** attivare la crittografia ai diversi livelli sui sistemi; ad esempio in caso di sistemi windows è possibile attivare Bitlocker per effettuare la crittografia del disco dei PC, oppure in caso di database è opportuno che siano crittografati. E' molto importante anche proteggere con crittografia i dischi virtuali delle macchine virtuali.
- **Errori comuni nell'implementazione del requisito:** assenza di crittografia.

7. Controllo e verifica delle terze parti (Annex A, Controllo A.5.20 e seguenti)

- **Gestione dei fornitori**: Gli infostealer possono entrare nei sistemi attraverso vulnerabilità introdotte da terze parti (fornitori, partner, ecc.) o infettare sistemi di terze parti nei quali sono contenuti dati di accesso alle infrastrutture dell'organizzazione. La **ISO/IEC 27001:2022** suggerisce di applicare rigorosi controlli di sicurezza anche ai fornitori e ai partner, assicurandosi che abbiano misure di sicurezza adeguate e che non rappresentino una via d'ingresso per infostealer.

- **Come implementare operativamente questo requisito:** definire una procedura di qualifica dei fornitori che contempli l'analisi preventiva dei requisiti di sicurezza offerti dal fornitore prima della contrattualizzazione anche mediante checklist od audit. Inserire in tutti i contratti specifiche clausole per la sicurezza delle informazioni definendo anche i livelli di servizio garantiti. Effettuare un monitoraggio periodico del mantenimento dei requisiti da parte dei fornitori.

- **Errori comuni nell'implementazione del requisito:** un tipico errore delle organizzazioni è il controllo della sicurezza del fornitore solo dopo la stipula del contratto e l'avvio del servizio. Ulteriore errore comune è la totale assenza di sistemi di monitoraggio della sicurezza del fornitore in quanto vige la convinzione che "è una responsabilità del fornitore".

In sintesi, la ISO 27001 aiuta a mitigare il rischio di infostealer attraverso una gestione olistica della sicurezza delle informazioni, che comprende la protezione preventiva, il monitoraggio proattivo, la gestione del rischio e l'educazione degli utenti. Ogni controllo specifico previsto dallo standard contribuisce a ridurre le probabilità di una violazione da infostealer e a limitare l'impatto in caso di attacco.

Nella precedente trattazione abbiamo analizzato a campione alcune misure di mitigazione rispetto agli infostealer, ma suggeriamo al lettore di valutare all'interno della propria organizzazione l'adozione di un sistema di gestione dell'information security, cybersecurity and privacy protection basato sulla norma ISO/IEC 27001 in modo tale da collocare specifici controlli a presidio dei rischi all'interno di un sistema strutturato e tracciato.

Un ulteriore approfondimento tematico per il lettore può essere il cybersecurity framework del NIST.

CONCLUSIONI

Gli infostealer sono il perfetto Babbo Natale al contrario: invece di portare regali, si prendono le tue password e, già che ci sono, svuotano pure i tuoi conti correnti. E il bello (o brutto, dipende dai punti di vista)? Non serve nemmeno essere esperti di hacking per usarli. Il crimine informatico ha avuto un'evoluzione affascinante: dai virus amatoriali degli anni '80, creati più per divertirsi che per altro, ai malware moderni progettati per rubare ogni dato utile. È un po' come una gara senza fine, dove i criminali sono sempre un passo avanti sfruttando internet, il cloud e l'automazione per affinare i loro strumenti. Gli infostealer sono il culmine di questa evoluzione: ladri digitali discreti e straordinariamente efficienti, pronti a sfruttare ogni debolezza. Grazie al Malware-as-a-Service, chiunque può diventare un "ladro del weekend", acquistando pacchetti di malware chiavi in mano per pochi spicci. E per chi vuole puntare in alto, ci sono persino opzioni premium.

La morale è semplice: ogni progresso tecnologico porta nuove opportunità, sia per noi che per i cybercriminali. La differenza? La fa chi è preparato a rispondere. Capire l'origine e l'evoluzione delle minacce non è solo interessante, è essenziale per non farsi cogliere di sorpresa nella prossima fase di questa sfida.

Questi malware non si fermano al furto di dati: li usano come trampolino di lancio per attacchi ancora più devastanti, come ransomware e frodi bancarie. Sono fulmini a ciel sereno: rapidi, distruttivi e costosi. Il risultato? Per le aziende, il conto è salatissimo: milioni spesi in ripristino, clienti che se ne vanno e una reputazione in fumo. E tutto può iniziare con una mail apparentemente innocua o un link che promette miracoli… o il solito iPhone gratis.

I settori più colpiti? Finanza, sanità e retail, dove ogni dato rubato può trasformarsi in una catastrofe. Ma non tutto è perduto. Possiamo combatterli, eccome. Però no, un antivirus del 2015 e un pizzico di fortuna non bastano. Serve un piano serio. La crittografia è un buon inizio, l'autenticazione multifattoriale un'ottima seconda mossa, ma la vera arma segreta? Formare il tuo personale. Perché, diciamolo: se i tuoi dipendenti cliccano su ogni link sospetto, puoi avere il sistema più sicuro del mondo, ma hai già perso.

Esatto, la vera svolta è la formazione del personale: insegnare ai tuoi dipendenti a riconoscere un'email di phishing può fare la differenza tra un sistema intatto e una catastrofe. A questo si aggiungono simulazioni di attacchi e aggiornamenti costanti dei sistemi, perché anche un software obsoleto può

trasformarsi nella porta d'ingresso per i criminali. Infine, un monitoraggio continuo garantisce di restare sempre un passo avanti. La verità è semplice: aspettare di essere colpiti per reagire è il miglior regalo che possiamo fare agli infostealer. Meglio prevenire, proteggere e dimostrare che la sicurezza è una priorità.

Gli infostealer non sono leggende digitali: sono una realtà quotidiana. Ogni giorno, milioni di dati vengono rubati e trasformati in armi per attacchi futuri. Nessuno è immune, dai piccoli negozi alle grandi multinazionali. Non possiamo eliminare la minaccia, ma possiamo renderci un bersaglio difficile. La realtà degli infostealer è spietata, ma con la giusta strategia possiamo affrontarla. E, soprattutto, possiamo dimostrare che non siamo vittime passive, ma avversari pronti a combattere.

Il GDPR non è solo una noiosa normativa burocratica: è la spina dorsale della protezione dei dati personali e un'arma contro minacce come gli infostealer. Nel panorama attuale, dove il furto di informazioni sensibili è all'ordine del giorno, i principi sanciti dal GDPR rappresentano un punto di riferimento fondamentale. La crittografia dei dati, l'adozione di autenticazione forte e la gestione tempestiva delle violazioni non sono solo obblighi regolamentari, ma strumenti pratici per difendere le informazioni aziendali e la fiducia dei clienti.

Ma il GDPR è molto più di una serie di regole: è un'opportunità per trasformare la sicurezza in un vantaggio competitivo. Implementare i suoi principi non significa solo evitare multe, ma costruire un'infrastruttura sicura e resiliente. Pensiamo, ad esempio, al principio di Privacy by Design: integrare la protezione dei dati fin dalle prime fasi di sviluppo di un sistema riduce drasticamente i punti deboli sfruttabili dai criminali.

La conformità non si ferma qui. Le aziende devono effettuare audit regolari, aggiornare le proprie policy di sicurezza e formare il personale per riconoscere e gestire potenziali minacce. Inoltre, una risposta rapida e trasparente in caso di violazione non è solo un obbligo normativo, ma una strategia fondamentale per preservare la reputazione aziendale.

In un mondo digitale sempre più complesso, il GDPR è sia una guida che un'arma: chi lo utilizza con intelligenza non solo protegge i dati, ma dimostra ai clienti di essere un partner affidabile e sicuro. E in un mercato sempre più competitivo, questa fiducia può fare la differenza tra il successo e il fallimento. Il GDPR non è un costo: è un investimento nel futuro.

E il futuro? Non sarà più semplice. Gli infostealer diventeranno più intelligenti, sfruttando intelligenza artificiale e tecniche

sempre più raffinate. Ma possiamo e dobbiamo reagire con innovazione, investendo non solo in tecnologia, ma anche in consapevolezza. Proteggere i tuoi dati oggi significa proteggere la fiducia dei tuoi clienti domani.

Quindi, meglio ripassare i punti chiave per essere al sicuro questo Natale e il prossimo:

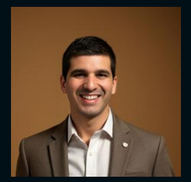
- implementare soluzioni avanzate di sicurezza: strumenti come EDR e XDR non solo rilevano attività sospette in tempo reale, ma aiutano a rispondere rapidamente agli attacchi.
- crittografia e segmentazione dei dati: proteggere le informazioni sensibili con crittografia end-to-end e limitare l'accesso ai dati solo a chi ne ha davvero bisogno è essenziale.
- autenticazione multifattoriale (MFA): una barriera efficace contro il furto di credenziali, che impedisce agli attaccanti di accedere ai sistemi anche se in possesso di username e password.
- formare e sensibilizzare il personale: insegnare ai dipendenti a riconoscere phishing e social engineering riduce drasticamente le possibilità che l'attacco abbia successo.
- creare simulazioni periodiche: test di phishing e altre esercitazioni aiutano a mantenere alta l'attenzione del personale e a migliorarne la prontezza.
- monitorare continuamente i sistemi: rilevare attività anomale in tempo può fare la differenza tra bloccare un attacco e subirlo.
- tenere aggiornati i software: patchare regolarmente sistemi e applicazioni elimina vulnerabilità sfruttabili dagli attaccanti.

E con questo, Buon Natale a tutti voi lettori e #StaySafe!

"Il miglior antivirus è il personale formato." *Cit. Agostino Ghiglia*

CONTRIBUTORI

Andrea Mario Muscarà
Cybersecurity Analyst & Ethical Hacker



Francesco Demarcus
Senior Security Manager, Direttore Tecnico

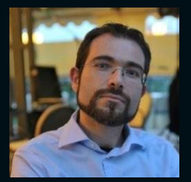
Manuel Pomarè
Direttore tecnico & Cyber Threat Intelligence Expert

Cristiano Nadal
Cybersecurity Analyst & Ethical Hacker

Luca Stivali
Cyber Security Enthusiast e imprenditore nel settore IT

Pietro Melillo
Docente Red Hot Cyber, CISO ed esperto di Cyber Threat Intelligence

Domenico Ciervo
Cybersecurity & IT Compliance Manager



Luca Poiana
IT Manager

Giuliana Dolci
DPO, Lead auditor ISO/IEC 27001:2022 e formatore

Matteo Villa
Privacy & Cybersecurity Specialist CPEH Certified Professional Ethical Hacker

BIBLIOGRAFIA

- *https://www.swascan.com/wp-content/uploads/2023/05/Report-Q1-2023-Def-1.pdf*
- *https://www.deloitte.com/global/en/services/risk-advisory/content/future-of-cyber.html*
- *Malware Finances and Operations: a Data-Driven Study of the Value Chain for Infections and Compromised Access https://arxiv.org/pdf/2306.15726*
- *Cost of a data breach 2024 | IBM*
- *https://cybelangel.com/the-true-cost-of-ransomware-attacks/*
- Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati
- D. lgs n. 196/2003 - Codice privacy
- D. Lgs 101/2018 - Decreto di attuazione
- Storia della Privacy - Privacy lab - prof. Francesco Pizzetti ex Garante per la protezione dei dati personali
- California Consumer Privacy Act - State of California Department of Justice
- European Data Protection Board (EDPB) - Comitato europeo per la protezione dei dati: organizzazione indipendente nonché Garante europeo della protezione dei dati