Ghost Stealer / GhostLord Technical Analysis

Cybanetix

V1.0 27/06/2025

Cybanetix Limited
cybanetix.com
Registered at:
The Coade
Level 9
98 Vauxhall Walk
London
SE11 5EL
Company Registration: 10558582
VAT Number: GB 262502430

Table of Contents

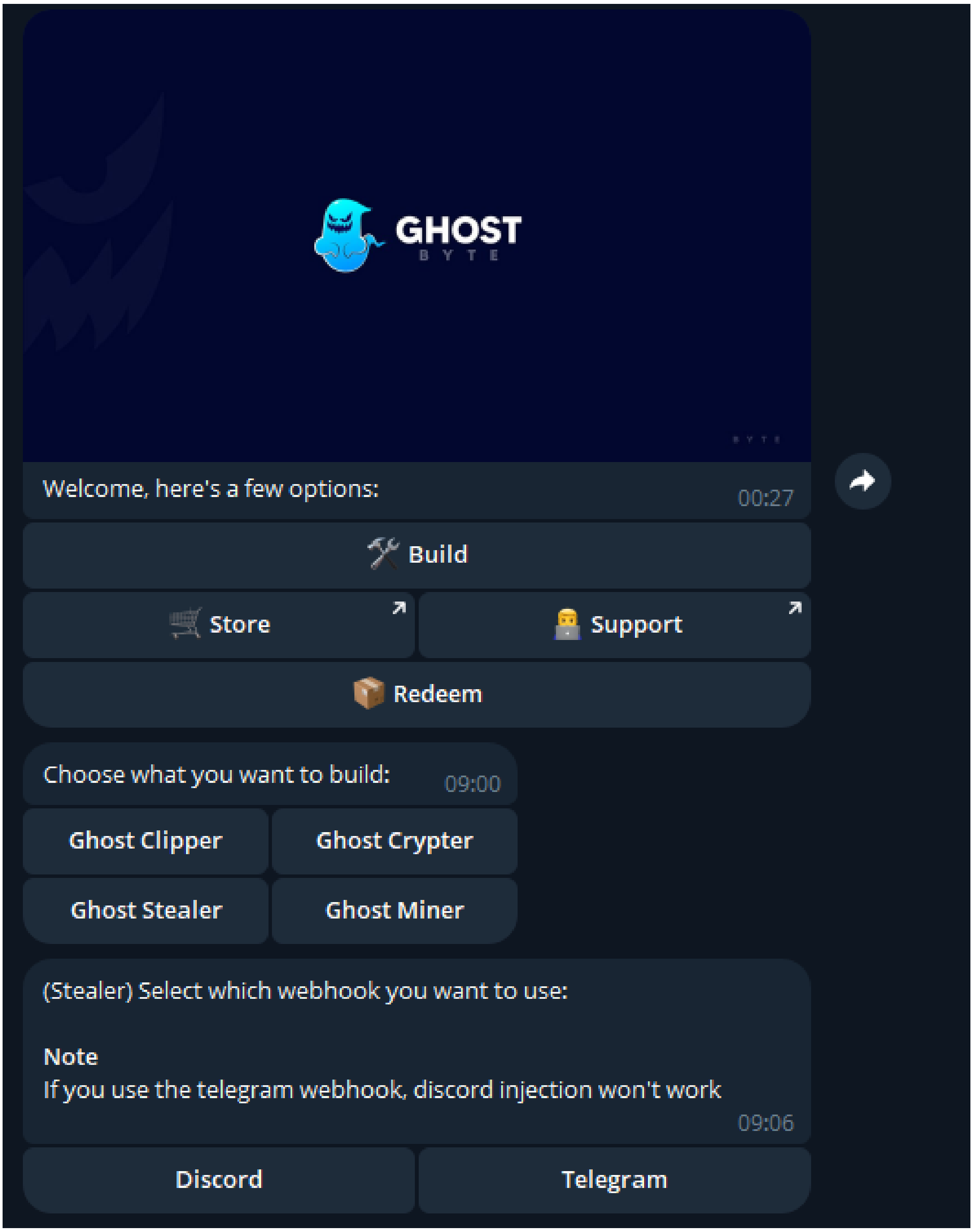
Ghost Stealer / GhostLord Technical Analysis

Overview and Classification of Ghost Stealer / GhostLord

Ghost Stealer is a malicious software classified as an information-stealing malware (infostealer). It first emerged in mid-2023 as a commodity malware sold on underground forums. Unlike the older Gh0st RAT (a remote access Trojan), Ghost Stealer is focused on silently harvesting credentials and sensitive data from infected Windows systems. It is offered as a malware-as-a-service (MaaS) tool – the developers (known by the handle "GhostByte") sell a builder that allows purchasers to generate custom infostealer executables. The pricing is low (approximately $20 for a single build or $100 for a lifetime license), making it accessible to cybercriminals. Ghost Stealer is part of a wave of inexpensive "off-the-shelf" stealers (like RedLine, Raccoon, Lumma, etc.) that are widely used in the cybercrime ecosystem.

Ghost Stealer is primarily used by financially motivated threat actors in the cybercriminal underground. It is not known to be exclusive to or developed by any Advanced Persistent Threat (APT) group. Rather, it is advertised and sold in forums and Telegram channels to anyone willing to pay, meaning a variety of low-tier actors can deploy it. To date, there are no public attributions linking Ghost Stealer to specific nation-state APT groups – it appears to be a commodity infostealer for profit-driven campaigns. (Some social media posts in late 2023 mentioned a "Ghost Stealer" in context of a group called GhostSec, but this seems to be a naming collision; the Ghost Stealer malware described here is sold by GhostByte and is unrelated to GhostSec's operations.) In fact, the malware has gone through rebranding in the criminal community – researchers noted "Ghostly Stealer" as an alias, and a later version being marketed as "Ghostlord" by 2024. These are believed to be the same family or direct successors, indicating the developers continue to evolve the product under new names to evade detection and re-market it.

As an infostealer, Ghost Stealer's core function is to steal sensitive information from an infected machine and exfiltrate it to the attacker. Infostealers like Ghost Stealer typically target data such as saved browser passwords, cookies, credit card details, cryptocurrency wallets, messaging app tokens, and other stored credentials. Ghost Stealer fits squarely in this category: it operates stealthily on the victim's system, searches for a wide range of credential sources, and sends the collected data back to its operators without the user's knowledge. It does not provide interactive remote access (unlike RATs) and is generally used as a first-stage tool to facilitate further attacks (by selling or abusing the stolen data).



Welcome, here's a few options: 00:27

Choose what you want to build: 09:00

(Stealer) Select which webhook you want to use:

Note
If you use the telegram webhook, discord injection won't work 09:06

The Ghost Stealer operation includes a builder program and support infrastructure. The threat actors behind it (GhostByte) provide a builder interface, via a Telegram bot, which buyers can use to customize and compile their own malware binaries

GhostByte's builder interface on Telegram, offering options to build Ghost Stealer and related tools.

The builder allows the customer to configure details such as the command-and-control (C2) delivery method (e.g. Telegram bot, Discord webhook, or a self-hosted server) and includes additional tools (the Ghost suite also advertises a "Ghost Clipper" for crypto wallet hijacking, a “Ghost Crypter” to obfuscate malware, and even a “Ghost Miner” for illicit cryptomining.

This user-friendly service model lowers the barrier to entry for cybercriminals – even novices can generate a fully functional, fully undetected malware executable with a few clicks. One underground advertisement touted Ghost Stealer as “undetected” by antivirus and highlighted features like a secure stub, hidden operation, anti-analysis, and a GUI builder panel.

Ghost Stealer has been actively developed and used through 2024 and into 2025. Threat intelligence sources indicate that the malware received updates as recently as June 10, 2025, suggesting continued support and addition of features. It has shown up in multiple criminal campaigns, typically targeting individuals for credential theft. Large volumes of stolen data (often called “logs”) from infostealers like Ghost Stealer are being traded on dark web marketplaces. While Ghost Stealer’s market share is smaller compared to heavyweights like RedLine or Raccoon, it contributes to the ever-growing pool of compromised accounts. For example, a Group-IB report found over 100,000 stolen account credentials (including ChatGPT accounts) on dark web markets in 2023, all lifted by various infostealers – Ghost Stealer is one of the newer malware facilitating such theft.

Technical Breakdown of Ghost Stealer Functionality

Ghost Stealer performs a multi-stage routine: it must first be delivered to victim systems, then executed to harvest data, establish persistence (if configured), and finally exfiltrate the stolen data to attackers. It also employs techniques to evade detection and analysis. Below is a detailed breakdown of each phase of Ghost Stealer’s operation:

Delivery Methods and Initial Infection

Attackers have employed various delivery methods to spread Ghost Stealer. Because it is a commodity malware, there is no single dedicated distribution; instead, different threat actors incorporate Ghost Stealer into their own campaigns. Common delivery vectors include:

- Ghost Stealer payloads are often sent via phishing emails, either as attachments or download links. Spear-phishing attachments (e.g. malicious Office documents with macros or embedded scripts) have been used to drop infostealer payloads. Phishing messages may also include links to malicious file downloads (e.g. a link claiming to be software or an update, which leads to a Ghost Stealer executable). For example, in one observed campaign from December 2023, attackers emailed a ZIP file named “Reader_Install_Setup.zip” purporting to be an Adobe Reader update; inside was an executable (`Reader_Install_Setup.exe`) that actually installed Ghost Stealer. This kind of masquerading as legitimate software is a known tactic to trick users into launching the malware.

- Like many infostealers, Ghost Stealer is also distributed through social engineering on the web. Threat actors have uploaded Ghost Stealer disguised as popular software (video players, productivity tools, games) or as "cracked" software on various forums, torrent sites, and file-sharing services. Unsuspecting users who download pirated software or cheats can unwittingly install the stealer. Security researchers note that infostealers are commonly bundled with game hacks, key generators, or illicit software activators. Attackers also use malvertising – malicious advertisements or search engine ads that lead to fake download pages – as a way to lure users searching for free software into downloading malware. Ghost Stealer fits the pattern of malware delivered via "drive-by" downloads and illegitimate software installers.

- Additional methods like malicious links on social media or chat (Discord, Telegram channels) have been used. A recent Check Point report documented a "Stargazer" distribution network on GitHub that disseminated various stealers by creating fake GitHub repositories with appealing lures (e.g. free followers, game cheats). While that report named stealers like Atlantida, Rhadamanthys, and RedLine, the same tactics could distribute Ghost Stealer as well. In general, any method that gets a user to run the malicious executable can be employed – including malicious ads, forum posts, direct messages, and even YouTube videos advertising game hacks or software accompanied by a malware link.

Once the victim executes the Ghost Stealer dropper, the initial infection stage begins. Ghost Stealer is typically packaged as a single Windows executable (often with a legitimate-looking icon and name to avoid arousing suspicion, such as `Install.exe`, `Update.exe`, etc.). Some samples have been written in or compiled with Python (packed via PyInstaller), while others may use a .NET loader stub to execute the stealer payload. Upon execution, the malware will usually unpack or decrypt its main code in memory and start its data-stealing routine. Notably, Ghost Stealer does not require administrator privileges to steal user-level data (browser passwords, etc.), so it often runs in user context. However, it may attempt UAC bypass or prompt for elevation for certain features (see Persistence below).

Ghost Stealer employs several tricks to evade immediate detection during execution:

- It may masquerade as a known process or use a fake publisher name. For instance, no obvious windows or installers are shown to the user (it runs invisibly). Attackers sometimes bundle it with decoy content (e.g., opening a benign PDF or document while the stealer works in background) to conceal its presence.

- The binary often comes obfuscated or encrypted. Strings and indicators are hidden using packing or runtime decryption, making static analysis difficult. (A sandbox analysis of a Ghost Stealer sample showed it decrypting strings at runtime and flagged it with a generic “uses string decryption to hide real strings” heuristic.)

- Ghost Stealer likely checks for analysis environments. Although specific details for Ghost Stealer are sparse, analogous malware implement anti-VM and anti-sandbox checks – e.g., looking for virtualization artifacts or debuggers. Indeed, a threat intelligence summary of Ghost Stealer mentions “anti debug” and “mutex” features. It likely calls functions like `IsDebuggerPresent` and scans for processes or system Serial IDs associated with sandboxes. If analysis is detected, Ghost Stealer may terminate itself to avoid revealing behaviors. (Researchers reporting on a similar stealer noted: “Detects and exits if running in a virtual machine to avoid analysis in controlled environments.”)

Persistence Mechanisms

Ghost Stealer can establish persistence on the system, though this may be configurable via the builder. If the attacker desires the stealer to survive reboot and continue running, Ghost Stealer provides options to achieve persistence. Known or likely persistence mechanisms include:

- Ghost Stealer can add itself to the Windows Startup programs. It may create a new value under the registry key `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` (or the HKLM equivalent) pointing to its executable, ensuring it starts every time the user logs in. This is a common technique (MITRE T1547.001). For example, the seller of a related stealer noted “automatically adds itself to startup if configured, ensuring persistence across reboots.” Ghost Stealer likely has a similar configuration toggle in its builder for “Add to startup”.

- As an alternative, Ghost Stealer could create a Scheduled Task in Windows Task Scheduler to run itself periodically or at logon (MITRE T1053). Many modern infostealers use this method to avoid the obvious registry entry. It’s not confirmed in public sources if Ghost Stealer specifically uses scheduled tasks, but it is a plausible mechanism if registry-based persistence is detected by security tools.

- A simpler persistence trick is copying itself to the Windows Startup folder in the Start Menu. Any executable or LNK shortcut placed there will run on user login. Ghost Stealer might use this method if it has write access to the user’s profile.

- A less likely approach (not documented for Ghost Stealer, but observed in others) is to drop itself in a common directory with a innocuous name and possibly set it as a runonce startup or as a service. Since Ghost Stealer’s primary goal is quick data exfiltration, long-term persistence is usually not essential; some operators may choose no persistence, running the stealer as a one-time smash-and-grab.

If Ghost Stealer runs with administrator rights (either the user was tricked into a UAC prompt or the exploit chain provided admin access), it could employ more entrenched persistence (like writing to HKLM Run keys affecting all users, or installing a Windows service). However, most often Ghost Stealer operates at user level. The malware does not typically exhibit worm-like self-propagation (no self-copy to USB or network drive by default, although PCrisk notes that some malware can attempt such propagation – Ghost Stealer currently has no known self-spreading component).

In practice, many Ghost Stealer infections have been one-time runs: the malware steals data and exits after execution, sometimes even self-deleting to cover tracks (a feature in other stealers). The builder's "Support" documentation or user feedback suggest Ghost Stealer can do a self-removal after exfiltration (to avoid leaving the binary on disk), but confirmation is limited. What is clear is that if persistence is enabled, Ghost Stealer will start with Windows and could continue to collect data over time (capturing any new browser passwords or cookies generated after the initial run, for example).

Another notable artifact is Ghost Stealer's use of a mutex. On launch, it creates a uniquely named mutex (a mutual exclusion object) to ensure that only one instance runs at a time. This prevents multiple copies from interfering with each other and can serve as an indicator if analysts find an oddly named mutex in memory. The mutex name could be a pseudo-random string or something identifiable (e.g., based on "Ghost" or the build ID) – one report alluded to a mutex but did not disclose the exact name.

Credential and Information Harvesting Techniques

Once running on a victim machine, Ghost Stealer proceeds to harvest a broad array of data. It is an all-purpose thief, grabbing any credentials or valuable user information it can find. According to advertisements and analyses, Ghost Stealer's capabilities include:

- Ghost Stealer targets nearly all major web browsers and many lesser-known ones, focusing on data stored by the browsers. It extracts saved login usernames and passwords, saved credit card numbers, cookies, and sometimes browsing history and form autofill data. The stealer accesses browser SQLite databases or files (such as the `Login Data` and `Web Data` files for Chromium-based browsers, which store passwords and credit card info, respectively). It uses known techniques to decrypt browser-stored passwords (browsers like Chrome and Edge encrypt saved passwords with the user's DPAPI key; Ghost Stealer can retrieve the required decryption key from the system and then decrypt the passwords). The malware has a very extensive browser target list – beyond Chrome, Firefox, and Edge, it includes dozens of Chromium variants. For example, Ghost Stealer explicitly supports browsers such as Brave, Opera/Opera GX, Vivaldi, Yandex, Chromium, 360Browser, Comodo Dragon, CocCoc, Maxthon, Waterfox, SeaMonkey, and many more. This comprehensive coverage ensures that even if a user is on an uncommon browser, Ghost Stealer can likely extract their data. It also steals session cookies from browsers (which can let attackers hijack logged-in web sessions without needing the password). Stolen cookies and credentials are highly valuable for further intrusions or sale on darknet markets.

- Ghost Stealer is crypto-focused and aims to steal digital currency assets. It searches the filesystem for known wallet files or credentials for popular cryptocurrency wallets. The malware's code targets wallets like Bitcoin Core, Ethereum (wallet files and keys), Litecoin, Dash, Zcash, Monero, Ripple, Stellar, and many others. It will look in the standard directories for wallet files (for instance, `wallet.dat` for Bitcoin, or the keystore files for Ethereum). Advertised targets include wallet applications such as Armory, Bytecoin, Exodus, Jaxx Liberty, Electrum, AtomicWallet, Guarda, Coinomi, etc.. If these wallets are installed on the system, Ghost Stealer will try to pilfer the wallet data – which could include private keys or recovery phrases. In an example shared by the malware author, Ghost Stealer was shown extracting the mnemonic seed phrases and passwords for wallets like Exodus and Atomic Wallet. With these seed phrases or keys, the attacker can independently recreate and empty the victim's crypto wallets. (Note: The term "Injection" in the screenshot is a bit misleading – it refers to Ghost Stealer pulling sensitive data from the wallet apps, not injecting code. It's essentially stealing secrets from those applications.)

- In addition to desktop wallets, Ghost Stealer also targets browser-based crypto wallets and extensions. Many crypto users rely on browser extensions (like MetaMask) to manage wallets. Ghost Stealer's feature list includes a long set of browser extension wallets: MetaMask, Binance Chain Wallet, Coinbase Wallet extension, Phantom (Solana wallet), TronLink, Keplr, Yoroi, Trust Wallet browser extension, and others. The stealer will search the browser's extension storage for those wallet extensions' data (which may include keys or session tokens). By grabbing this data, attackers might extract private keys or at least the seed phrases if they are stored or cached by the extension. Some extensions encrypt their secrets with a password – Ghost Stealer may still collect the encrypted vault along with any user-provided hint, enabling offline cracking. Essentially, Ghost Stealer is aimed at the DeFi/crypto community as well, given the huge list of wallets it tries to loot.

- Recognizing that many users (especially those likely to download game cheats or cracks) also have valuable gaming accounts, Ghost Stealer targets certain gaming platforms and apps. The hackforums listing for Ghost Stealer mentions it can steal credentials or session tokens from Steam and other gaming services. It explicitly lists Minecraft (various launchers), Epic Games, Riot Games, Ubisoft UPlay, and even a specific private server mod (NationsGlory). By stealing session tokens or saved passwords for these services, attackers could hijack game accounts (some of which might have valuable in-game assets or linked payment info). Steam credentials are also frequently sold. Additionally, some of these gaming platforms use the same email/password as the user's other accounts, so it feeds into credential stuffing for other services.

- Ghost Stealer is known to harvest Discord tokens. Discord (a popular chat platform) stores user authentication tokens on disk; stealing these allows an attacker to log in as the user without credentials, potentially compromising additional accounts (since Discord is often used by gaming and crypto communities). The malware grabs these tokens from Discord's storage (usually `%AppData%\Discord\Local Storage\leveldb\`). There's no indication Ghost Stealer directly targets Telegram client data or other messengers in its basic configuration, but it's possible it could grab session files for apps like Telegram, Skype, etc., if the operators customize it. The mention of "Discord injection" in the builder interface
  suggests Ghost Stealer might also have functionality to leverage the Discord client (some stealers attempt to use a running Discord instance to send data or further propagate, but in this case "Discord injection" likely refers to stealing the tokens from Discord's memory or running process). The builder screenshot warns: "If you use the Telegram webhook, Discord injection won't work"
  – implying the malware can either send results via Telegram or attempt to steal Discord info via some method, but not both at once (likely a limitation in how the payload is configured).

- Many infostealers scrape credentials from other applications as well, such as email clients (Outlook, Thunderbird), VPN clients, FTP clients (like FileZilla) or SSH keys. While Ghost Stealer's publicly advertised features focused on browsers and wallets, it's common for stealers to include modules for some of these. For instance, a general description of "Ghostly" stealer mentioned potential targets like FTP clients, VPNs, email clients, messengers, etc., depending on configuration. It's likely Ghost Stealer either currently or in a future update adds some of these targets to remain competitive. At minimum, it gathers system information that could include installed programs list, which might incidentally reveal credentials (for example, configuration files of known programs).

- Ghost Stealer collects basic host information to fingerprint the victim. This typically includes the computer name, username, IP address, OS version, hardware info, and any anti-virus product present. These details help the attacker understand their victim's environment. The malware may query the registry or use Windows APIs to get this info (e.g., `GetComputerNameW`, `GetUserNameW` were used by Lumma stealer, and Ghost Stealer likely does similar). It might also enumerate if certain security software or virtual drivers are present as part of anti-analysis (for example, checking registry keys or processes related to AV or VM).

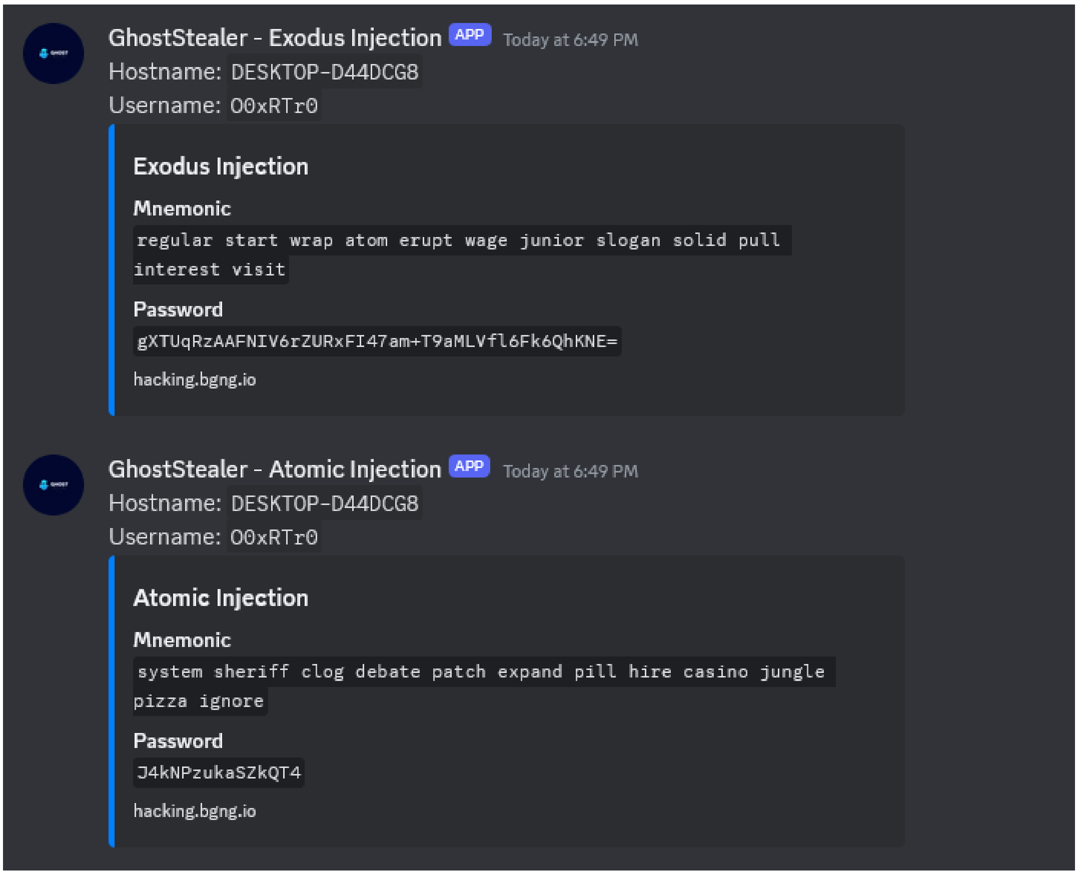
- Ghost Stealer is reported to have spyware-like capabilities including taking screenshots of the desktop and possibly activating the webcam. Marketing materials in 2024 indicated it had features such as "screenshot capture, webcam capture". This means Ghost Stealer can silently snap a screenshot of the user's screen (MITRE T1113) to possibly capture additional contextual information (like if the user is viewing a page with one-time passwords or other content not stored in files). Webcam capture (MITRE T1125) would allow taking a snapshot from any connected webcam, potentially to gather more intel or just as an intimidation factor. (Not all infostealers have this, but Ghost's adverts suggest it does.) There's also mention of "record audio and video via microphones/cameras" in a generic write-up – though that may refer to capabilities of stealers in general. It's unclear if Ghost Stealer actively records audio, but at the very least, single-frame webcam snapshots are within its toolset.

- Some info-stealers incorporate a keylogger to capture keystrokes (MITRE T1056.001), and a file grabber to grab arbitrary files matching certain extensions (MITRE T1114 for email files, or simply searching for documents). The PCrisk analysis of "Ghostly" stealer notes that many stealers have these capabilities (recording keyboard input, stealing files from the system). Ghost Stealer's documentation does not explicitly mention a keylogger or file grabber, but it wouldn't be surprising if a module exists or is planned. Even without an active keylogger, the wealth of stored credentials it steals often makes keylogging unnecessary for their purposes.

- A particularly dangerous feature relevant to cryptocurrency theft is a clipboard "clipper". This functionality monitors the system clipboard for cryptocurrency addresses and if it sees one, it replaces it with an attacker-controlled address (so that when a victim thinks they're pasting their friend's wallet address, they actually paste the attacker's address). Ghost Stealer's developers actually separate "Ghost Clipper" as a product, but it's integrated into the same ecosystem

    - The builder offers to create a Ghost Clipper – which suggests that the stealer can be built with an optional clipper component. If enabled, Ghost Stealer would continuously watch clipboard text for patterns matching crypto addresses (Bitcoin, Ethereum, etc.) and instantly swap them. This can redirect cryptocurrency transactions to the attacker's wallet. Many infostealers (like RedLine, Raccoon) have added clippers because it provides immediate profit if the victim transacts cryptocurrency.

    - We can infer Ghost Stealer has this because the author's interface clearly separates a "Ghost Stealer" and a "Ghost Clipper" build , but likely the stealer build itself can incorporate wallet injection. Indeed, the term "Exodus Injection" in the Discord logs suggests it might have injected malicious code or simply extracted secrets from the Exodus process. And the "Note: If you use the Telegram webhook, discord injection won't work" hint from the builder implies some interactive injection/hooking technique possibly for Discord or other apps, which might conflict with using Telegram as output. It's somewhat unclear, but clipboard hijacking (clipper) functionality is strongly implied by the presence of "Ghost Clipper" in the toolkit and by generic references to "cryptowallet address replacing abilities" being prevalent in stealers.



GhostStealer - Exodus Injection APP Today at 6:49 PM
Hostname: DESKTOP-D44DCG8
Username: O0xRTr0

Exodus Injection

Mnemonic
`regular start wrap atom erupt wage junior slogan solid pull interest visit`

Password
`gXTUqRzAAFNIV6rZURxFI47am+T9aMLVfl6Fk6QhKNE=`

hacking.bgng.io

GhostStealer - Atomic Injection APP Today at 6:49 PM
Hostname: DESKTOP-D44DCG8
Username: O0xRTr0

Atomic Injection

Mnemonic
`system sheriff clog debate patch expand pill hire casino jungle pizza ignore`

Password
`J4kNPzukaSZkQT4`

hacking.bgng.io

Data Exfiltration and C2 Infrastructure

After harvesting data from the victim's machine, Ghost Stealer will exfiltrate the stolen information to its operators. The malware supports multiple exfiltration channels, giving flexibility to the attacker. Key points about Ghost Stealer's C2 (Command-and-Control) and exfil mechanisms:

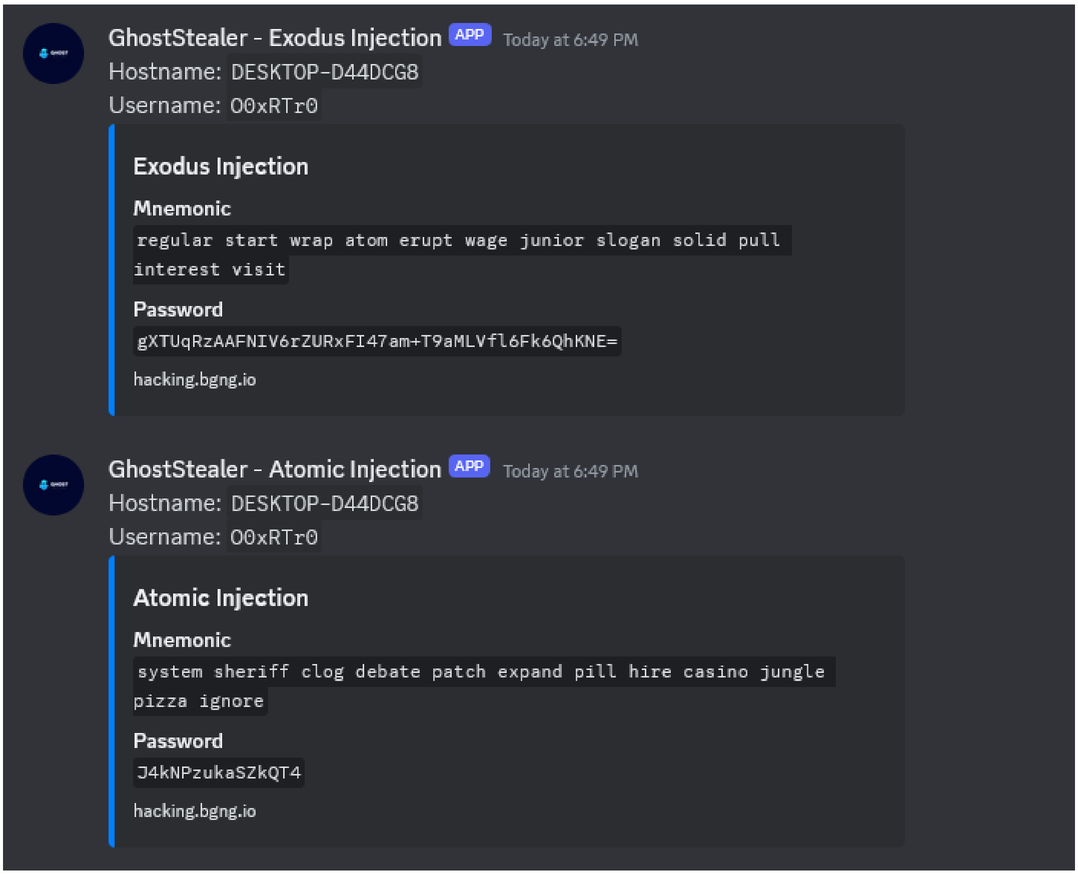
- Ghost Stealer usually aggregates all collected data into a single archive file (ZIP or similar) before exfiltration. This archive often contains a structured report: for example, text files for passwords (sorted by browser), a file for cookies, a file listing system info, and any wallet files or tokens as separate files. Many stealers generate a ZIP named after the victim's machine or some ID. (E.g., "DESKTOP-ABC123.zip" containing all loot.) This packaging (MITRE T1560 – Archive Collected Data) helps efficiently send the data in one transmission. It may also compress and/or encrypt the archive. Some malware use a static password for ZIP (like "infected" or similar), others just compress without password. The term "secure" in Ghost Stealer marketing could imply the logs are encrypted for transport, but specific details are unknown.

- One method Ghost Stealer uses is a direct HTTP(S) connection to a C2 server controlled by the attacker. In this mode, the attacker sets up a web server (or uses a provided web panel script from GhostByte) where the malware can upload the stolen data. The Ghost Stealer binary would have a configured C2 address (IP or domain) and possibly a specific port/path. For instance, an analysis in March 2025 found a Ghost Stealer sample containing a hardcoded C2 IP `147.185.221.26`. The malware attempted to connect to this IP (over a non-standard port) to presumably upload data. The sandbox flagged that behavior: "Detected C2 URLs/IPs in malware configuration". We also see that Ghost Stealer tends to connect directly to an IP without DNS lookup (likely the IP was embedded). This suggests the operator chose to use a raw IP as a destination, possibly to a panel listening on a specific port. In such cases, Ghost Stealer would perform an HTTP POST (or series of posts) with the stolen data. (By contrast, some families do FTP or SMTP email – Ghost doesn't advertise those, leaning more on HTTP or messaging API exfil.) If the GhostByte team provided a web panel, it would parse incoming data and allow the criminal to view logs via a UI. This C2 panel infrastructure is typically hosted on bulletproof servers or compromised servers. It's worth noting that the IP above (147.185.221.26) has been associated with other malware C2 (XWorm RAT and NjRAT on different ports), so it may be a reused hosting or a victim machine serving as a relay.

- A hallmark feature of Ghost Stealer is the option to use Telegram as the C2 channel. The advertisement calls it "TG sender + no host needed". This means the stolen data can be sent to the attacker through Telegram's messaging platform, rather than a self-hosted server. In practice, the attacker would set up a Telegram bot and obtain an API token and chat ID, which are then configured in the Ghost Stealer builder. When the malware runs on a victim, it will then send the stolen logs via Telegram API calls (HTTPS requests to Telegram) to deliver the data to the attacker's bot as a message or file. This has several advantages for the attacker: (1) they don't need to maintain infrastructure – Telegram serves as the transport; (2) Telegram traffic is encrypted and looks like normal API traffic, often slipping past network monitoring; (3) it's convenient – the logs pop up in the attacker's Telegram app in real time. Many modern stealers (Lumma, Raccoon v2, etc.) support Telegram exfil for these reasons. Ghost Stealer's promotional description specifically highlights "no host needed" and the presence of a built-in panel or integration with Telegram. The builder UI screenshot confirms that when building the stealer, the user is prompted to choose a webhook for data delivery: Discord or Telegram
  . If Telegram is chosen, it likely asks for the bot token and chat ID. Ghost Stealer then uses Telegram's HTTPS API (to `api.telegram.org`) to send the ZIP of stolen data. This technique maps to MITRE technique T1102 (Web Service) or T1567.002 (Exfiltration to Cloud Services), using a legitimate service as a drop box.

- Similarly, Ghost Stealer can send data via a Discord webhook. Discord allows creating webhook URLs that any client can `POST` messages to a channel. The builder's options show "Discord" as one exfil method
  . If configured, the stealer will POST the stolen data (usually as base64 text or as an attachment) to the Discord webhook URL provided. The example in the figure below actually appears to be a Discord channel receiving Ghost Stealer logs (the "GhostStealer – Exodus Injection" messages are in Discord)

– this likely came via a webhook integration that posts each stolen item to a private Discord server controlled by the attackers. Using Discord as C2 has similar benefits to Telegram: it blends with normal traffic and requires no dedicated server. However, one limitation is file size – very large log files might be truncated or not sent if they exceed Discord's message or attachment size limit. Attackers often mitigate this by splitting data or just sending key info as text.



GhostStealer - Exodus Injection APP Today at 6:49 PM
Hostname: `DESKTOP-D44DCG8`
Username: `O0xRTr0`

Exodus Injection

Mnemonic
`regular start wrap atom erupt wage junior slogan solid pull interest visit`

Password
`gXTUqRzAAFNIV6rZURxFI47am+T9aMLVfl6Fk6QhKNE=`

hacking.bgng.io

GhostStealer - Atomic Injection APP Today at 6:49 PM
Hostname: `DESKTOP-D44DCG8`
Username: `O0xRTr0`

Atomic Injection

Mnemonic
`system sheriff clog debate patch expand pill hire casino jungle pizza ignore`

Password
`J4kNPzukaSZkQT4`

hacking.bgng.io

- It's possible attackers use a combination – e.g., primary exfil via Telegram, and a backup copy to a panel or email. Ghost Stealer's builder likely only allows one selection at a time (the note about Discord injection not working if Telegram is used suggests only one channel is active to avoid conflicts
). But an attacker could build separate binaries for different channels or use a multi-output if they modify the code.

- Unlike RATs, infostealers typically do not offer interactive control or extensive back-and-forth commands. Ghost Stealer is no exception – it largely performs its pre-programmed theft tasks and sends data out, without needing to receive complex instructions from a C2 server. It's a one-directional data exfiltration in most cases (thus aligning with MITRE TA0010 – Exfiltration rather than requiring interactive C2). However, some advanced stealers can receive simple commands or updates from the server (for example, to download an updated target list or to load a plugin). There's no public evidence that Ghost Stealer has a full command shell or upload capability. It might have a primitive ability to receive a "self-destruct" command or an update instruction if using a C2 panel (for instance, LummaC2 supports receiving config updates from the server). If

Ghost Stealer's panel sends down new config or target lists, it could adjust its behavior on the fly (but again, not confirmed). For the most part, once Ghost Stealer sends the loot, the malware's job is done. Any further actions (like using the credentials or installing follow-on malware) are done by the attackers manually or via other malware.

- By using encrypted channels (HTTPS to Telegram/Discord or an HTTPS POST to a server), Ghost Stealer tries to evade network detection. From the host perspective, these look like normal TLS traffic. Many enterprise defenses might not flag an outbound HTTPS POST to a Telegram API or a cloud IP unless they do deep packet inspection. Additionally, since Ghost Stealer often terminates after exfil, it doesn't maintain a suspicious persistent connection. It may also use some degree of obfuscation for the data in transit (e.g., encoding stolen passwords in base64 or encrypting the ZIP file with a password) to avoid signature detection. The use of legitimate services as C2 is a growing trend (ATT&CK T1568).

Anti-Analysis and Evasion Techniques

Ghost Stealer incorporates several anti-analysis and evasion techniques to avoid detection by security products and to hinder malware analysts. These include:

- As noted earlier, Ghost Stealer likely checks for signs of virtualization (VMware, VirtualBox, etc.) and sandbox environments. This could involve looking for special registry keys, MAC addresses, running processes (e.g., `vboxservice.exe`), or device drivers associated with VMs. If it detects a VM, the malware may quietly exit without performing malicious actions, thereby evading automated sandboxes. (This behavior was explicitly confirmed in a related stealer's feature list: "Detects and exits if running in a virtual machine to avoid analysis in controlled environments.") Such checks help Ghost Stealer stay invisible to many malware sandboxes used by researchers and antivirus companies.

- Ghost Stealer likely uses API calls to detect if it is being debugged or monitored. Functions like `IsDebuggerPresent`, `CheckRemoteDebuggerPresent`, or raising exceptions can reveal a debugger's presence. The mention of "anti debug" in threat intel posts suggests Ghost Stealer actively tries to thwart debugging. It might also employ techniques like obfuscated control flow or packing to confuse disassemblers. Additionally, it may monitor for analysis tools (Process Monitor, Wireshark, sandbox processes, etc.) and delay or halt its execution if they're found.

- Some stealers inject parts of their code into legitimate processes (like browser processes or `explorer.exe`) to hide their presence. It's not confirmed if Ghost Stealer does code injection – its small size and straightforward data theft might not require it. However, the term "injection" in its context was about stealing wallet data (not code injection into another process). Ghost Stealer probably

runs as a separate process and may not bother with process hollowing or migration, focusing on speed. Still, the presence of "APP" tags in the Discord output (GhostStealer – Exodus Injection APP)
hints it might impersonate some application context to extract data.

- Ghost Stealer is advertised as "fully undetected" (FUD) by AV, which implies it uses crypters or polymorphic builds to evade antivirus signatures. Each build generated by the GhostByte builder can be unique (different hash, perhaps different junk code) to avoid signature-based detection. The Ghost suite even includes a "Ghost Crypter" service
– which likely provides an extra layer of obfuscation/encryption to the final binary. This means traditional antivirus may have difficulty recognizing Ghost Stealer executables, especially if they are newly generated and not yet seen in the wild. The use of a crypter can hide static indicators and make the binary look benign or random to scanners (MITRE T1027 – Obfuscated Files or Information).

- While not explicitly reported for Ghost Stealer, some malware use system tools (like `rundll32`, `regsvr32`, or PowerShell) to execute payloads in memory. Ghost Stealer being typically an EXE probably doesn't heavily rely on LOLBins, but an attacker might wrap it in a script or use an initial loader that calls PowerShell to fetch and run it (to reduce detection of dropping an EXE to disk). The FBI/CISA noted some infostealers delivered via PowerShell loader in phishing (like a fake CAPTCHA that leads user to run a base64 PowerShell command). Ghost Stealer could be part of such a chain too.

- If run with high privileges, Ghost Stealer could attempt to disable security tools. Some malware add themselves to Windows Defender's exclusion list or even turn off real-time protection (via registry or PowerShell `Set-MpPreference` cmdlets). A related stealer (Divulge, likely on the same spectrum) advertised features like "excluding itself from Windows Defender scans" and "disabling Windows Defender". It's quite possible Ghost Stealer has similar functionality, especially if the builder allows requesting admin rights. However, using such aggressive moves can sometimes backfire by triggering security alerts, so not all operators will enable this. If the target is individual home users (who might not notice Defender being turned off), it could be effective.

- For exfiltration, Ghost Stealer uses secure channels (HTTPS) which not only serve functionality but also evade network detection since the traffic is encrypted. Additionally, by sending to trusted domains (Telegram, Discord), it evades simple domain blocklists. From an analysis perspective, capturing the exfiltrated data is hard without the keys or by intercepting the network traffic via a MITM proxy (which the malware might detect if a fake certificate is present).

- After completing its tasks, Ghost Stealer may attempt to clear evidence. Some malware clear Windows event logs or command history to erase traces. While there's no direct mention of Ghost Stealer doing log deletion, it does often self-delete after running (as reported by some users of similar stealers). This means the malware binary removes itself from disk (using a batch script or scheduling a delete) to prevent forensic recovery. What remains are only the artifacts (registry entries, etc.) unless those too are cleaned.

MITRE ATT&CK Tactics and Techniques Mapped for Ghost Stealer

Ghost Stealer's behavior can be mapped to the MITRE ATT&CK framework as follows (covering the enterprise matrix tactics from Initial Access through Exfiltration). Below is a list of relevant tactics, techniques, and sub-techniques associated with Ghost Stealer, based on observed and reported functionality:

- Initial Access – Phishing (T1566): Ghost Stealer is commonly delivered via phishing. This includes Spearphishing Attachment (T1566.001) – e.g., malware-laden documents or archives sent to victims, and Spearphishing Link (T1566.002) – links to malicious downloads in emails. Attackers also use drive-by downloads and fake software downloads (which fall under user execution but initiated via social engineering).

- Execution – User Execution (T1204): The malware relies on the user to execute a file they believe is benign (e.g., opening what they think is a software installer or document). Ghost Stealer may also be executed via a script or document macro, but ultimately, it's a user-triggered execution.

- Persistence – Registry Run Keys/Startup Folder (T1547.001): If configured for persistence, Ghost Stealer adds an entry in the Registry Run keys or places a shortcut in the Startup folder to launch on logon. This ensures it persists after reboot.

- Persistence – Scheduled Task (T1053.005): (Potential) Ghost Stealer could create a scheduled task to run at intervals or at startup as an alternative persistence method.

- Privilege Escalation – ** (Ghost Stealer typically does not exploit privileges; it usually runs as user. If it prompts for admin, it's to disable defenses or access protected paths, which is more in Defense Evasion. No specific MITRE tech for just prompting UAC, but if it uses some bypass, that could be Bypass User Account Control (T1548.002)** – not confirmed in Ghost, just possible.)

- Defense Evasion – Obfuscated Files or Information (T1027): Ghost Stealer binaries are often obfuscated or crypted to avoid detection. Strings and code are hidden via encryption or packing, defeating static signatures.

- Defense Evasion – Masquerading (T1036): The malware masquerades as legitimate software (e.g., using names/icons of trustworthy apps). Also, it may spoof file metadata (like version info claiming to be Adobe or Windows process) to blend in.

- Defense Evasion – Deobfuscate/Decode Files or Information (T1140): On execution, Ghost Stealer decrypts or decodes strings and payloads (like configuration or internal code) at runtime. This is seen where it decrypts its C2 address and other data (a form of obfuscation reversal).

- Defense Evasion – Disable or Modify Tools (T1562.001): Ghost Stealer can attempt to disable security software (specifically Windows Defender) by adding itself to exclusions or turning off protections. If run with admin rights, it may tamper with AV settings to avoid detection during execution.

- Defense Evasion – Impair Defenses (T1562): More generally, by using allowed services (Telegram, Discord) for exfiltration and terminating quickly, Ghost Stealer impairs defenders' ability to catch it.

- Defense Evasion – Virtualization/Sandbox Evasion (T1497): The malware checks for virtualization or sandbox artifacts and will not fully execute in those environments. This includes anti-VM, anti-debug, and possibly time delays to thwart sandboxes.

- **Credential Access – ** (This is the core tactic for Ghost Stealer.)

- Credentials from Password Stores (T1555): Ghost Stealer obtains credentials from password stores. Specifically Credentials from Web Browsers (T1555.003) – it dumps saved passwords, cookies, and form data from browser databases. This covers a huge range of browser credential theft.

- Steal Application Access Tokens (T1552.001): It steals tokens for applications like Discord (and potentially others). Discord tokens are effectively authentication secrets that allow account access, thus falling under stealing application credentials.

- OS Credential Dumping (T1003): Not typically performed by Ghost Stealer (it doesn't dump Windows hashes or LSASS memory, since it's aimed at user-level creds, not NTLM hashes). So T1003 is not relevant here.

- Input Capture – Keylogging (T1056.001): If Ghost Stealer has a keylogger module (uncertain), it would log keystrokes to capture credentials as the user types. Many infostealers do not rely on keylogging unless they want to catch things like master passwords or dynamic content.

- Steal or Forge Authentication Certificates (T1552.004): If Ghost Stealer grabs browser certificate stores or VPN certificates, it could fall here, but no evidence it does.

- Discovery – System Information Discovery (T1082): Ghost Stealer collects host information – computer name, OS version, installed software, etc., for basic profiling. This is often logged in the report it sends.

- Discovery – Query Registry (T1012): The malware may query registry keys (for example, to get the registered owner, or AV product info, or to check for certain configurations).

- Discovery – Application Window Discovery / Browser Discovery (T1217): Lumma stealer had a technique to enumerate browser information. Ghost Stealer likewise discovers installed browsers and extensions to know what to target.

- Collection – Data from Local System (T1005): Ghost Stealer collects files from the local system such as wallet files, documents, or any target files.

- Collection – Browser Session Data (T1114.002 or T1217): It specifically collects browser session cookies and histories, which can be considered Email or Messaging data if webmail sessions are stolen, but more directly fits credentials from browsers.

- Collection – Clipboard Data (T1115): With its clipper functionality, Ghost Stealer monitors and potentially modifies clipboard content (looking for cryptocurrency addresses). Reading clipboard content is a form of data collection.

- Collection – Screen Capture (T1113): Ghost Stealer can capture screenshots of the user's desktop. This is a collection technique to gather information visible on screen.

- Collection – Video/Camera Capture (T1125): The malware reportedly can capture webcam snapshots (and possibly microphone audio), which is collection of video/image data from the camera.

- Collection – Automated Collection (T1119): The entire process of scanning numerous locations (browsers, files, etc.) is automated. Ghost Stealer doesn't require manual control to gather each item – it automatically gathers predefined data sets. This is precisely the automated log collection that infostealers do.

- Collection – Archive Collected Data (T1560): Ghost Stealer archives the stolen files into a ZIP or similar compressed file before exfiltration. This not only reduces size but also can serve to encrypt data with a password if configured.

- Exfiltration – Exfiltration Over C2 Channel (T1041): Ghost Stealer exfiltrates data over its C2 channels, whether that is a direct network connection to a C2 server or via an API call. In either case, it's sending stolen data over an application layer protocol to an external destination. This is the primary exfiltration mechanism.

- Exfiltration – Exfiltration to Cloud Service (T1567.002): When using Telegram or Discord for exfiltration, Ghost Stealer is effectively exfiltrating to a cloud service (messaging platform). This sub-technique covers using tools like social media or file-sharing services to exfiltrate data.

- Exfiltration – Automated Exfiltration (T1020): The process is fully automated once the malware runs. The user's data is bundled and sent out without any manual steps, indicating automated exfiltration.

Recent Campaign Examples Involving Ghost Stealer

Ghost Stealer has been observed in several recent malware campaigns (2023–2024), usually as part of broader credential theft or fraud operations. Here we outline a few examples and patterns of its use in the wild:

- Fake Software Installers (Late 2023): One campaign in late 2023 involved emails targeting users with a fake Adobe PDF Reader update. The email urged users to download an attached ZIP or visit a link to update their PDF software. In reality, the provided installer (`Reader_Install_Setup.exe`) was a Ghost Stealer dropper. Upon execution, it dropped Ghost Stealer which proceeded to steal passwords and crypto wallet data. This campaign illustrates a common theme: leveraging well-known software updates as lures. Many users, particularly in corporate environments, might trust an email about software updates, making this an effective initial access. Investigators analyzing the payload found the Ghost Stealer binary and identified IoCs including the hashes of the ZIP and EXE.

- YouTube and Social Media Lures (2024): Throughout 2024, researchers noted a spike in info-stealer distribution via YouTube videos and Discord channels. Threat actors create YouTube tutorials for game hacks, cracks, or “free” software and put download links in the description. For instance, a YouTube video might advertise a cheat for a popular online game or a free cryptocurrency mining bot – the download link provided would actually be a Ghost Stealer executable. These videos often had titles in broken English and prompted viewers to disable antivirus before downloading (a red flag). One specific case shared on Twitter in December 2023 involved a supposed “Goo Stealer” (which appears to be Ghost Stealer misnamed or a variant) being delivered via a ZIP file, with the infection chain analyzed by a researcher. The malware inside was Ghost Stealer, and it transmitted stolen data to a Discord webhook controlled by the attackers (evident from Discord logs). This campaign targeted gaming community members seeking cheats.

- Targeting of Crypto Users (2024): Given Ghost Stealer’s emphasis on cryptocurrency wallets, there have been campaigns aimed at crypto enthusiasts. For example, phishing emails or Twitter DMs offering “beta access” to a new crypto trading platform or airdrop have included links to malware. In mid-2024, a campaign was reported on underground forums where Ghost Stealer (branded as “GhostSec’s Ghost Stealer” by some) was marketed to steal credentials from crypto exchange accounts and wallets. One advertisement claimed “#GhostStealer – a new stealer developed by #GhostSec following the release of GhostLocker, price $99.99 (beta access)”. While the attribution to GhostSec is likely misdirection, it shows that criminals were repackaging Ghost Stealer in themes relevant to crypto (GhostLocker was a ransomware; here they imply a whole suite of “Ghost” tools). In practice, at least one campaign impersonated a cryptocurrency app and delivered Ghost Stealer, resulting in many victims’ wallet keys being stolen.

- Enterprise Credential Harvesting (2025): By 2025, Ghost Stealer has also been seen in targeted attacks against organizations as the first stage. For instance, an attack against a small finance company involved a phishing email with a OneNote attachment. The OneNote file contained an embedded script that downloaded Ghost Stealer. The malware ran and stole the credentials of the employee (including their browser-stored passwords for corporate web apps and email). These credentials were later used by the attackers to attempt a VPN breach. The incident aligns with a general trend reported by CISA/FBI where infostealers like Lumma and others are used to infiltrate organizations by stealing VPN and email passwords, which are then used for deeper intrusion. Although the advisory specifically names LummaC2, Ghost Stealer can serve the same role for any threat actor – it's essentially interchangeable as a tool to get initial foothold data (credentials) for further attacks. No APT attribution was made; the culprits were likely cybercriminals gathering data to sell or to extort the company.

- Integration in Multi-Stage Malware Chains: In some cases, Ghost Stealer appears as part of a malware bundle. For example, cracked software downloads from torrent sites sometimes carry an "all-in-one" malware package. One such torrent advertised a pirated software suite in early 2024; when executed, it not only installed a RAT (remote access Trojan) for persistent control, but also ran Ghost Stealer to gather immediate credentials (perhaps to ensure if the RAT got removed, they still got some loot). This kind of multi-stage attack maximizes returns. Security news in 2024 highlighted attacks where trojans like DarkCrystal RAT (DCRat) were paired with an infostealer in the same campaign. Ghost Stealer could easily be swapped in that role. The infostealer would vacuum up credentials and crypto wallets, then the RAT would allow hands-on intrusion into the network. Such campaigns are typically attributed to financially motivated threat groups rather than nation-states.

Importantly, Ghost Stealer continues to evolve. Its rebranding to "Ghostlord" in 2024 and ongoing updates in 2025 indicate the developers are responding to detections and adding features. We can expect to see Ghost Stealer. in future credential harvesting campaigns, possibly with improved evasiveness.

Indicators of Compromise (IOCs)

The following are indicators of compromise associated with Ghost Stealer malware. These include file hashes for malware samples, C2 network indicators, and other artifacts reported from analyses:

- Malicious Executable Hashes (Samples):
  - SHA-256: `2C85EB9B0BE85CC289CEE34BF5CD8EACB768069392D86B81956D52223164C5BA` – Example Ghost Stealer payload (compiled binary) observed in March 2025.

  - MD5: `8981C45440C214993E3263FA72C2FE45` – The MD5 for the same sample (“XClient.ghostbyte.exe”).
  - (Note: Ghost Stealer builds are often unique per attacker, so hashes vary. Use these as reference if seen in environments. Also, Ghost Stealer may be rebranded as “Ghostly” or “Ghostlord” – hashes for those versions would differ.)

- Ghost Stealer binaries can have innocent names. Known names observed include `Install.exe`, `Update.exe`, `Readme.exe`, `Server.exe`, and campaign-specific lures like `Reader_Install_Setup.exe` (used in a fake Adobe Reader phish). Any unexpected executable dropped in user temp or downloads with such names should be scrutinized. The builder does not enforce a fixed name, so this is variable.

- Ghost Stealer creates a mutex to avoid multiple instances. While the exact name is unknown due to unique build via the bot, forensic investigators might find an unusual mutex in memory for suspicious processes. (Some stealers use names like “Global\{GUID}” or “GhostMutX”). A mutex named “GhostByte” or similar could be an IOC if found.

- If persistence was enabledin the builder bot, check for registry run keys added. For example:
  `HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ <random>` with value pointing to a Ghost Stealer EXE path, or
  `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ <random>` (if run as admin).
  The value name might be innocuous (e.g., “OneDrive Update” or “SecurityUtility”) not literally “Ghost”. The path typically goes to `%AppData%` or `%Temp%`. Ghost Stealer might also set an exclusion in Defender registry (e.g., under `HKLM\Software\Microsoft\Windows Defender\Exclusions`).

- Network Indicators:

  - IP Addresses: One known C2 IP used by a Ghost Stealer sample is `147.185.221.26` (United States). This IP was contacted on a non-standard high port. It has been associated with malicious activity (XWorm RAT C2), indicating it’s likely a compromised server or malicious host servicing multiple malware. Any outbound connection to this IP (especially without a domain and on unusual port) is suspect.
  - Domains: Ghost Stealer itself may not have hardcoded domains (often raw IP or none if using Telegram). However, if a domain is used for panel, it could be a random or low-reputation domain. For example, the Discord log screenshot showed `hacking.bgng.io` which might be an attacker’s site referenced in the output
    – possibly a domain related to the campaign. “bgng[.]io” is not a known infrastructure but could be attacker-controlled. Defenders should watch for newly seen domains in network logs following user execution of unknown software.

  - Telegram API traffic: Outbound HTTPS requests to `api.telegram.org` soon after an unknown EXE runs can indicate exfiltration. Specifically, posts to URLs like `https://api.telegram.org/bot<botID>/sendMessage` or `/sendDocument`. Similarly, Discord webhooks use URLs like `https://discord.com/api/webhooks/<ID>/<token>`. Monitoring egress for those patterns from user workstations can catch Ghost Stealer and similar threats. (In corporate settings, legitimate use of these APIs from user PCs is uncommon).

- Ghost Stealer might drop temporary files during execution. For instance, a PyInstaller-based stealer will unpack a bunch of `.pyd` libraries and a Python bytecode file in a temp folder (like `%Temp%\_MEIXXXX\`). The presence of a folder `_MEI` followed by random digits is often an IOC for PyInstaller-packaged malware (the frozen Python environment) – ESET detected Ghost Stealer as `Python/PSW.Agent.AXX`, meaning it's a Python password stealer, likely PyInstaller. So, seeing an `_MEI` temp folder or unusual .pyd files (like PyQt or Crypto libraries) could indicate Ghost Stealer was run. Also, Ghost Stealer might create a log file locally before sending (some stealers write a file like `AllData.txt` then send it). If found, those files are IOCs (and contain the stolen data).

- If delivered via phishing, the filenames or content of lure documents can be IoCs. E.g., a malicious OneNote file named "Invoice_July2024.one" that drops the stealer, or a macro-enabled Word doc with keywords like "Enable Editing". The presence of an unexpected OneNote attachment in emails (which then spawns PowerShell) is an IOC pattern we've seen (one campaign used OneNote to drop stealers including presumably Ghost Stealer). Security teams should flag these patterns even if the malware payload itself is ephemeral.

- Different antivirus engines detect Ghost Stealer under generic names. For instance, Kaspersky might flag it as `UDS:DangerousObject.Multi.Generic` (a very generic cloud heuristic). ESET flagged one as `Python/PSW.Agent.AXX`, Malwarebytes as `Malware.AI.3982942871`. While these names vary, if you see alerts for "PSW (Password Stealer)" or "Agent.AXX", "Ghostly" or anything with "Stealer" on a machine, they could pertain to Ghost Stealer.

- Sometimes, if exfiltration fails, Ghost Stealer might leave behind the ZIP file of stolen data on disk. This could be in the Temp folder or the current user's folder. Such ZIPs are a goldmine to identify an IOC – they often have naming like `<MachineName>.zip` or some GUID. Inside, the presence of files like `Passwords.txt`, `Cookies.txt`, `Discord_Token.txt`, `Wallets\Exodus\wallet.dat` etc., is indicative of an infostealer (not specific to Ghost, but including Ghost).

- Unusual processes spawning or making network connections can indicate Ghost Stealer. For example, if `explorer.exe` or a Word process spawns a suspicious EXE in a user path, and that process then reads many browser database files (e.g., opens `%LocalAppData%\Google\Chrome\User Data\Default\Login Data`), that is a red flag. Ghost Stealer will open and read numerous files in browser and wallet directories – EDR telemetry of a process doing that across Chrome, Firefox, Discord folders in quick succession is a strong indicator of an infostealer in action.

In incident response, if Ghost Stealer is suspected, responders should look for evidence of data theft: check firewall/proxy logs for communication to Telegram or unknown IPs at the time of the incident, inspect the user's `%AppData%` for new files or programs, and dump memory of suspicious processes to look for the strings related to Ghost Stealer. A memory dump might reveal URLs, the Telegram bot token, or even the text of stolen passwords if the stealer held them in memory before exfiltration.

Finally, indicators such as the GhostByte contact handles can be monitored. The actor's Telegram handles were given in advertisements as `@GhostByteNews` (channel) and `@GhostByteV2` (contact). While not an IOC on a network, any sighting of those handles (or similarly named domains like ghostbyte[.]something) in your environment (e.g., a user visiting a GhostByte News channel or site) could be a clue of either the user or an attacker engaging with the Ghost Stealer service.