baseVISION TI Report

Infostealer Malware - The Silent Credential Harvesting Epidemic

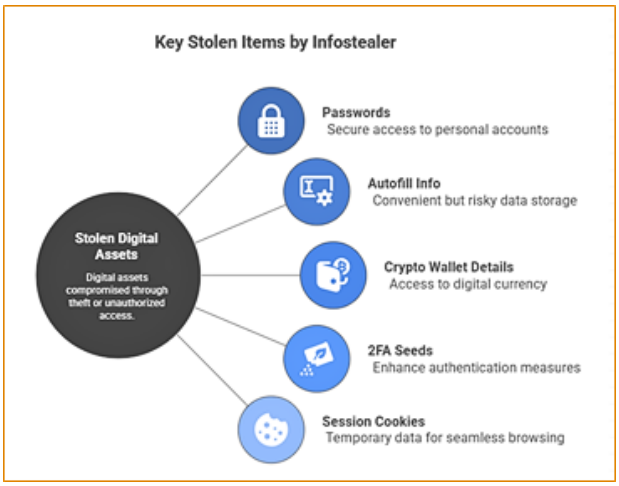
December 2025

baseVISION

Christmas Cookies on the Table. Sessions Cookies on the Dark Web.

Infostealer malware is a common type of cyber threat that enters systems to collect and send out sensitive data from infected devices. This data can lead to account takeovers, identity theft, and ransomware attacks. These tools mainly target login details, browser data, and app tokens, which put company security at risk and affect leader choices. In the first half of 2025, more than 2.67 million devices got infected worldwide, leading to over 204 million stolen credentials – a big jump from last year, driven by Malware-as-a-Service (MaaS) models that make these tools easy to get and use.

This is a 220% increase from 2023 levels, and stolen credentials now play a role in 32% of global breaches, according to the Verizon 2025 Data Breach Investigations Report (DBIR). **Key stolen items include passwords, autofill info, crypto wallet details, two-factor authentication (2FA) seeds, and session cookies** from over 45 browsers and apps, such as Chrome, Telegram, and Epic Games. MaaS options like Perion Stealer and LummaC2 cost as little as $14 per month, which helps create a cybercrime network that works like regular software services. Recent trends show more advanced methods, including AI help to avoid detection – for example, using Microsoft's Agentic OS for "agent-aware" theft – and links to ransomware chains, where stolen data helps attackers get in.



A 2025 analysis of 50,000 infected devices (from June to August) shows gamers as a top target, with 41% of infections tied to gaming files like fake mods or cheats, led by LummaC2 at 72% of cases. In a recently published investigation by our baseVISION Security Operations Center (SOC), they observed a similar malware campaign leveraging malicious game modifications (mods) to infiltrate online gaming environments and push the infostealer malware Stealit.

Victim counts keep rising, with the U.S. seeing over 50% of infections, hitting tech sectors (14% infection rate) and small-to-medium businesses (SMBs) the hardest. For leaders, this report stresses the need for active threat hunting, zero-trust identity setups, and ways to stop MaaS growth to cut financial and reputation risks.

1. Introduction

Over the past months, **baseVISION has seen a marked rise in infostealer activity across its customer base**, cutting across sectors, sizes, and maturity levels. This is no longer anecdotal noise but a structural trend. In 2025, infostealer malware has become a key pillar of the cybercrime ecosystem, acting as the foundation for an estimated 81% of double-extortion ransomware cases. Unlike ransomware that disrupts openly and noisily, **infostealers work quietly in the background, blending in with normal processes while they pull data over time.**

As we head into the holidays and start eating more Christmas cookies, most people are unaware that **another kind of cookie is being consumed—browser session cookies.** Modern infostealers no longer just steal passwords; they systematically harvest session tokens, VPN and cloud access, MFA-protected logins, messaging sessions, crypto wallets, and sensitive files. With these "digital cookies" in hand, attackers can impersonate users, bypass authentication, and move laterally into corporate environments without ever triggering a traditional login alert.

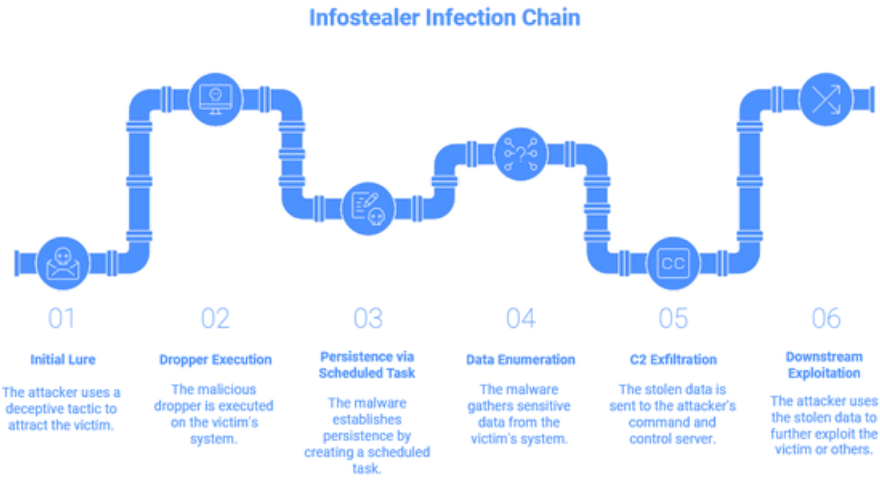
This stolen access is then monetized at scale, feeding underground markets and enabling ransomware, business email compromise, and supply chain intrusions. **Infostealers are currently one of the most operationally efficient and financially successful cybercrime tools in the ecosystem.** This report brings together current trends from dark web monitoring, incident response engagements, and live threat telemetry to give leaders a clear, actionable view of the risk landscape. As part of this effort, o**ur Extended Threat Intelligence & Hunting (XTI&H) solution continuously monitors these threats, identifies exposed identities, and proactively hunts active infostealer activity across our customers' environments**—so that this year, the only cookies being freely shared are the ones on the table, not the ones protecting your organization.

2. What is an Infostealer Malware?

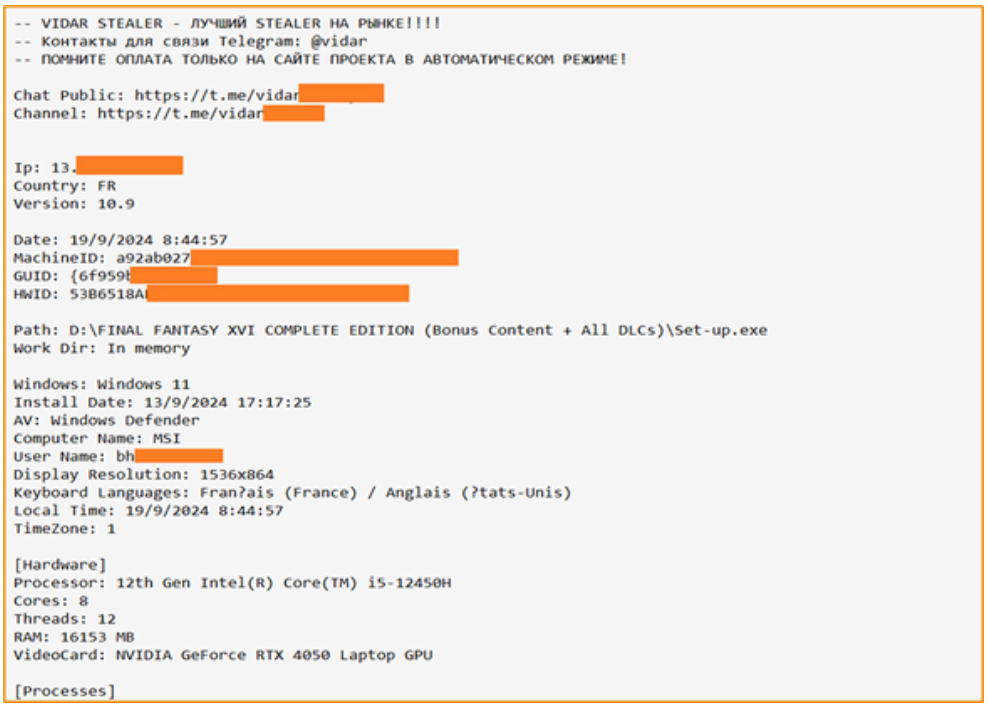
Infostealer malware is a group of trojans that break into systems to gather and send out user data. They often come through phishing tricks (like fake software or PDF tools), social engineering tricks, or bad ads. Once inside, they stay put using scheduled tasks, registry changes, or DLL side-loading. When running, they check and grab data in the background, often dodging basic antivirus with living-off-the-land (LOTL) tricks.

Main parts include:

- **Check Modules:** Look for browsers, apps, and other programs.
- **Send-Out Tools:** Use HTTP/HTTPS signals to control servers (C2), often hidden as crash reports.
- **Anti-Forensics Features:** Checks for virtual machines, process injections (like into Discord or browsers), and AI-based changes like "agent-aware" theft through OS-linked AI agents.

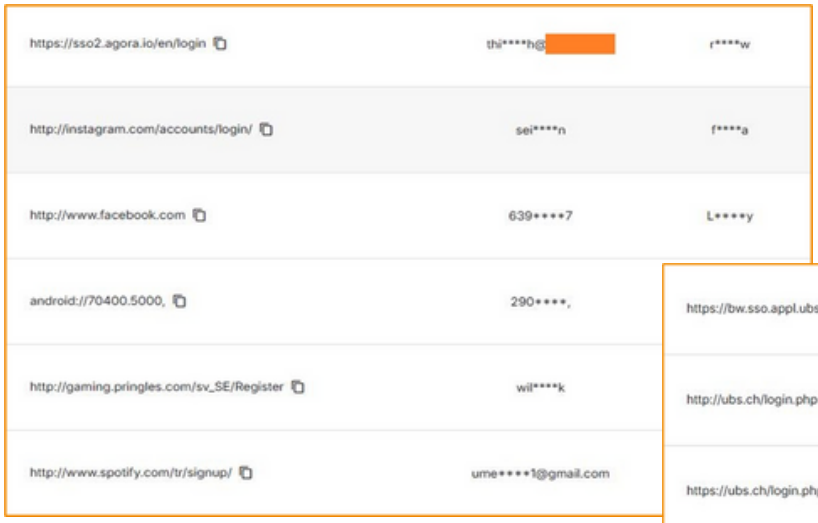


IInfostealer activity observed demonstrates that it is not only corporate resources that are being compromised, but also highly sensitive **personal** data siphoned directly from infected user machines. As illustrated in the screenshots, the panel exposes detailed host information (hostname, IP address, OS details, and the exact infection date), alongside the victim's user profile, browser data and authentication material. The malware exfiltrates complete browser cookie stores, saved logins, and file system content – and its documents – as well as **online banking credentials.** This data set enables a wide spectrum of abuse: account takeover against corporate and personal services, direct banking fraud, identity theft, impersonation of employees or executives, and highly tailored social-engineering attacks against both the victim and their contacts.

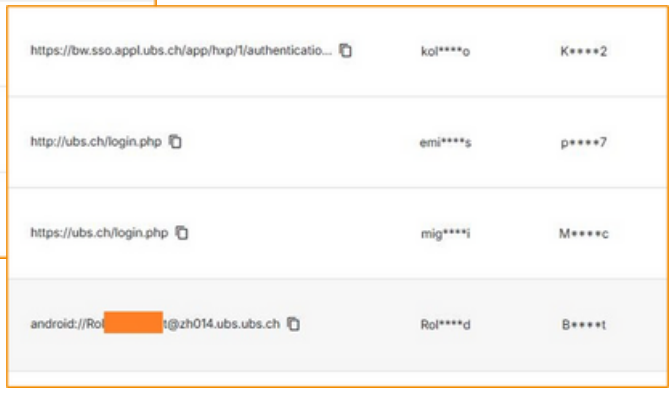


Vidar Stealer's Victim Showing System Info

Additionally, infostealer do exfiltrate, social media logins (**Instagram, Facebook, else**), and even **Android device data** from the victim's infected mobile phone. In some cases, the victim's browsing histories and active sessions contain sensitive services such as pornographic websites. In the criminal ecosystem, these artefacts are routinely weaponized for **blackmail and sextortion**, social-media account hijacking, SIM-swap and phone-number fraud, fake "support" or recovery scams, romance scams, and further credential stuffing against other services. At the same time, the very same depth of visibility can, under strict legal and ethical controls, be leveraged to **identify and track high-risk targets**, including **pedocriminals, drug traffickers, and other most-wanted individuals** whose access patterns and accounts surface in infostealer logs.



Victim's Browsing History



Various Victims Showing Banking Logins

Recently, a new twist comes from Microsoft's Windows 11 Agentic OS update, which adds AI agents to the taskbar for tasks like file sorting or email sending. These agents can access files, apps, and UI elements in a trusted way. Attackers can use Cross-Prompt Injection Attacks (XPIA) to hide bad instructions in files (like white text on white background in a PDF). When a user asks the agent to "summarize this," it follows the hidden orders, pulls sensitive data like keys, seeds, and cookies from Recall, browser tabs, Slack, or notes, and sends it out in JSON format – all without antivirus alerts, since the agent does the work. Microsoft noted this risk in May 2025 blogs, calling XPIA a way malicious content overrides agent rules for data theft or malware setup. This shifts infostealers from simple file grabs to "agent hijacking," where the AI itself gets used, bypassing many defenses by tapping in-memory data or cloud links. The update places an active AI agent directly on the taskbar, creating a centralized data hub for attackers to exploit. Why steal a password when you can steal the entire session memory? **Agentic stealers capture the "Why" and "How," not just the "What."** Microsoft's own words from May 19, 2025: "Cross-Prompt Injection (XPIA): Malicious content embedded in UI elements or documents can override agent instructions…" This trend marks a shift to "Agent-Aware Stealer" and "Agent Hijacking" for centralized data exploitation, with over 30 million compromised machines reported in related infostealer intelligence.

2.1 Types of Data Stolen

Infostealers grab a wide range of items but focus on high-value ones that help spread attacks and make money. Different common targets may lead to various **impact on organizations.**

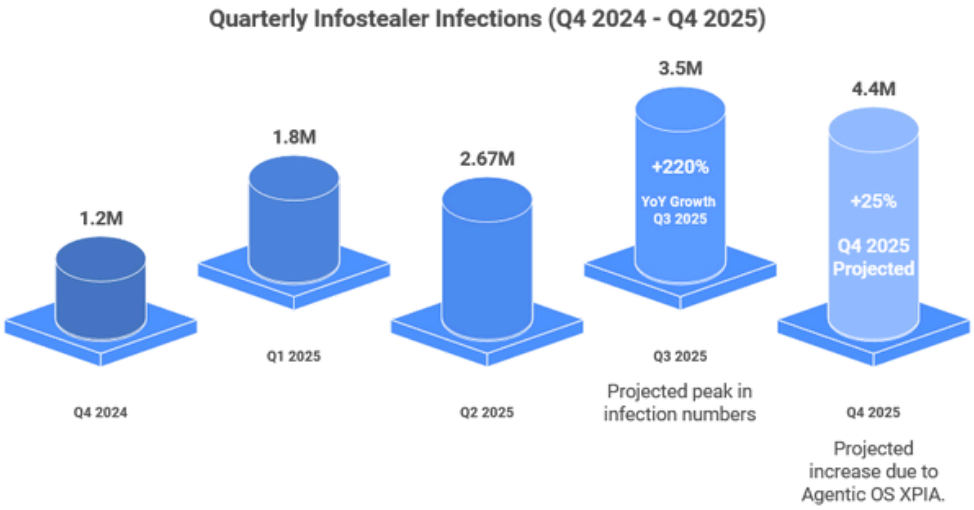
When looking at stolen credentials, around 30% of the compromised devices can be classified as enterprise-licensed systems. However, 46% of all compromised devices that contained corporate credentials were actually non-managed endpoints storing both personal and business logins. These systems are most likely tied to BYOD (Bring Your Own Device) usage or to corporate devices being used in ways that fall outside approved policy.

Infostealer capabilities may differ a bit: new infostealer types like Perion Stealer hit around 45 browsers and gaming setups, while Bee Stealer targets CVV/IBAN for card fraud. In organizations, this data causes 14% of tech sector infections, often leading to ransomware by groups like Play and Akira. Most ransomware victims had their credentials exposed in infostealer logs in the days leading up to the attack, with the most common gap being just two days. This underscores a direct connection between infostealer infections and subsequent ransomware deployment, indicating that stolen credential logs are frequently used as a staging ground for targeted ransomware operations. With Agentic OS, stealers can now grab "contextual" items like in-memory tokens or cloud data without full disk scans, making theft faster and harder to spot. For gamers, stolen data often includes Roblox, Fortnite, or Valorant accounts, leading to identity theft, financial loss, and privacy breaches.

2.2 Statistics on Victims and Infections

Infostealer spread in 2025 is huge, with low-cost MaaS speeding it up. Here are some key numbers:

- **Global Infections:** 2.67 million devices in H1 2025, creating 204 million credentials – up 800% in theft volume over four months.
- **Breach Role:** Stolen credentials caused 32% of breaches (Verizon DBIR 2025), with IBM X-Force seeing more AI-boosted phishing.
- **Regional Split:** U.S. (over 50% of victims), EMEA (big rise), tech/manufacturing hit most (14% rate).
- **Campaign Examples:** LummaC2 hit approximately 10 million devices, with 394,000 Windows endpoints in May 2025 (Microsoft/FBI data). Agentic OS risks could add 20-30% more infections by Q4, per Hudson Rock estimates, as XPIA exploits grow. ClickFix attacks surged 517% in 2025, becoming the second most common vector after phishing, with over 133,000 new logs from ACR Stealer alone in May.
- **Gamer-Specific Stats:** From June-August 2025, analysis of 50,000 infected devices showed 41% tied to gaming files (e.g., cheats, mods for GTA, Roblox, Valorant)—GTA6 is not even out yet! LummaC2 caused 72% of these, with over 22,000 gaming-related infections.



2.2.1 Malware-as-a-Service (MaaS) Availability

MaaS has made infostealer operations more organized, letting new attackers run big campaigns easily. These platforms act like software services, with paid levels, web dashboards for log handling, and Telegram help. New infostealer variants are created regularly, often with high capabilities like broad browser targeting, advanced evasion, and specialized theft (e.g., crypto or financial data). A prime example is Perion Stealer, launched in November 2025, which quickly gained attention for supporting 45+ browsers, anti-VM checks, and Discord token injection – showing how fast emerging threats can rival established ones. The table below highlights prominent MaaS infostealers active in 2025, based on dark web listings, detections, and threat reports.

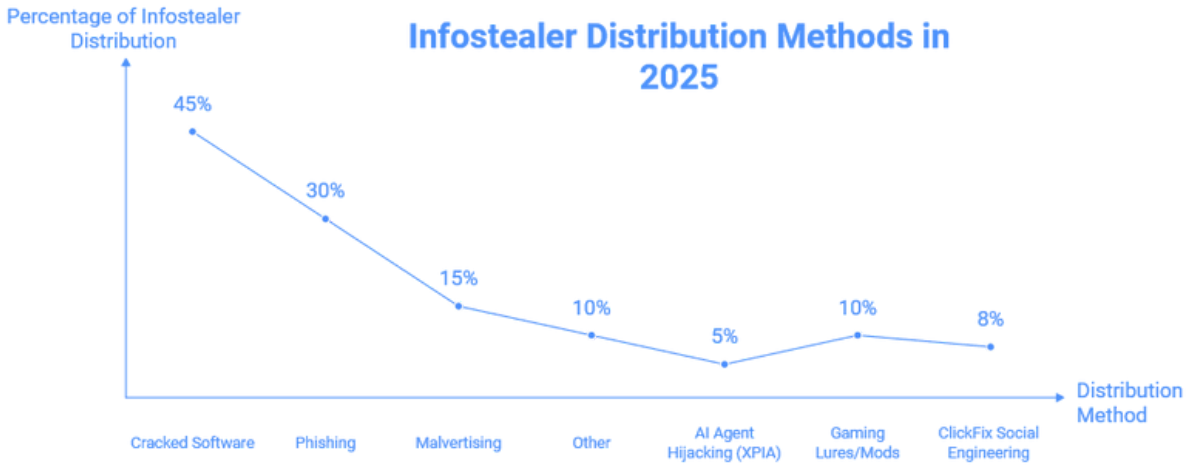
MaaS Variant	Pricing Model	Key Features	Popularity Trend
LummaC2	$250/month or $20K source code	Advanced obfuscation, global C2, crypto wallet focus, frequent updates	Dominant (#1 overall, highest dark web listings)
RisePro	Subscription-based (varies)	Affordable, broad credential harvesting, bundling hundreds of	Fastest-growing (#2 in many reports)
Vidar	Subscription (undisclosed)	Fork-based with major rewrites (v2.0), strong evasion, wide targeting	Surging (#3, veteran with renewed activity)
StealC	Low-cost subscription	New versions with improved loaders, clipboard hijacking	Established top 5, steady growth
RedLine	$100–$200/month	Long-time features like keylogging, form grabbing	Holding strong (#5, despite some declines)
Perion Stealer	Bronze ($14/week), Diamond ($60/ Lifetime)	45+ browsers, anti-VM, Discord injection, gaming focus	Emerging high-capability threat (Nov 2025 launch)
Rhadamanthys	Subscription (mid-tier)	Modular design, RAT hybrids, persistent access	Rising fast in H2 2025
ACR Stealer	Subscription (undisclosed)	Evasion upgrades, SEO poisoning distribution	Surging variants

This landscape evolves quickly – law enforcement disruptions (e.g., against Lumma domains) often boost competitors like RisePro or Vidar. Monitor dark web forums and threat intel feeds for the latest high-capability newcomers. Stops like LockBit shifts have spread MaaS further, with 30% expected growth in dark web sales. This links infostealers to ransomware, providing "new access" for groups. Agentic OS opens doors for MaaS updates, like XPIA kits for $50-100, per dark web forums.

2.2.2 Current Trends: Increase or Decrease?

Infostealer risks are clearly growing in size, skill, and effect:

- **Size Jump:** 220% growth 2023-2025; H1 2025 infections beat all of 2024 by 54% in linked ransomware cases.
- **Skill Rise:** Move to RAT mixes (e.g., AsyncRAT) for lasting access; AI ties (e.g., Agentic OS XPIA) dodge AV; NFC fraud via mobile MaaS like SuperCard X.
- **Spread Changes:** Main use of cracked apps (SEO tricks) and phishing; LummaC2 stops some signals, but ACRStealer variants take over. A clear pattern in "converter tool" themed RATs includes similar payload sites (e.g., ez2convertapp[.]com, pdfskillsapp[.]com), droppers pulling binaries, staging in %localappdata%, and persistence via Run keys/scheduled tasks.
- **ClickFix Campaign:** This social engineering trick spreads infostealers like Redline, LummaC2, Rhadamanthys, ACR, Lampion, and PureRAT via malvertising, phishing emails, or fake sites. It fools users into pasting malicious PowerShell/CMD commands from bogus error pages (e.g., fake Windows Updates, reCAPTCHA checks, or Cloudflare verifications) to "fix" issues like stalled audio/video or security scans. New 2025 waves hide payloads in PNG images' pixels (steganography) for evasion or target hotels for credential theft to send fraud emails via Booking.com/Expedia. Attacks jumped 517% in 2025, with 76 incidents in one month alone, now the #2 vector after phishing and hitting Windows/macOS/Linux.
- **Gamer Targeting:** Cybercriminals focus on gamers with fake cheats/mods, exploiting piracy culture; 41% of 50k infections in mid-2025 via gaming lures, with "crack" (17%) and cheats (9%) as top baits.
- **No Drop Expected:** Takedowns (e.g., 2,300 LummaC2 domains seized) leave leftovers, and new strains (Katz, Cyber) keep it going. Agentic OS adds a fresh vector, with early XPIA tests in wild samples, predicting 25% more corporate hits by year-end.



3. Technical Analysis case study: baseVISION Investigation on Malicious PDF Tool Campaign (ConvertMate)

Our baseVISION Security Operations Center (SOC) unit has observed a malware campaign, tracked internally as ConvertMate, which leverages malvertising to distribute the trojanized PDF conversion tool "ConvertMate". The campaign targets end users by redirecting them from malicious advertisements to a fraudulent, attacker-controlled website hosting the malicious PDF tool executable.

Once executed, the malware establishes persistence, performs credential and browser data collection, and exfiltrates the collected information to remote infrastructure.
A proactive threat hunt was conducted across all customer environments to identify affected devices and residual artifacts dating back up to 90 days.

3.1 Initial Access and Execution

Initial access is achieved through social engineering via malvertising, which redirects users to a fake PDF conversion website. Execution relies on a downloaded executable which does not require administrative privileges, and was not initially detected by Microsoft Defender. The installer also drops and launches a secondary malicious binary identified as "UpdateRetriever".

3.2 Persistence

The malware establishes persistence through the Windows Task Scheduler, where a scheduled task is created during execution and triggers the malicious binary on a daily basis, ensuring long-term persistence without user interaction.

3.3 Credential and Data Access

Observed activity indicates that the malware focuses on credential harvesting and browser data access. This includes access to Google Chrome browser data, interaction with the Windows Data Protection API (DPAPI) to retrieve protected credential material, and launching of child processes associated with credential store access. The scheduled task subsequently triggers the malicious binary, which establishes outbound network connections, and exfiltrates collected browser and credential data to a remote server controlled by the threat actor. Due to the initial lack of detection, this activity likely persisted undetected for an extended period before discovery.

3.4 Detection Status

Affected customers have been notified where traces of the campaign were identified and as of now, Defender is detecting the malicious binaries involved in the campaign as threats "Trojan:MSIL/Malgent!MSR" and "Trojan:Win32/Leonem!rfn".

3.5 Threat Hunting and Validation

To validate the scope of the campaign and identify affected hosts, advanced hunting queries were executed focusing on:

- Network activity initiated by the malicious binary (UpdateRetriever)
- Scheduled task creation associated with persistence mechanisms
- DPAPI access events indicating credential theft behavior

These queries enabled identification of both active infections and historical artifacts related to the ConvertMate campaign.

3.6 Mitigation Recommendations

To reduce the likelihood of similar attacks in the future, the following mitigations are recommended:

- Enforce Application Control for Business to block execution of unknown or unsigned binaries;
- Educate users on the risks of executing unverified third-party tools, particularly those obtained via advertisements or search engine results:
- Monitor for suspicious scheduled task creation and unusual browser credential access activity.
- Use Threat Intelligence Feeds to enable **real-time detection, faster incident response, better risk assessment**, and proactive defense by identifying malicious IPs, domains, and attacker tactics before they hit your network.

* Only when signed up for CS Hub (NCSC)

4. Threat Hunting for Infostealer Malware

Proactive threat hunting is essential to detect infostealer activity early—before credential and data exfiltration occurs—by focusing on anomalous persistence mechanisms and suspicious execution behaviors. The following hunting queries provided by our threat hunters hunt for non-standard tasks executing from user-writable directories, excluding benign apps. Our Proactive Threat Hunting service continuously searches for stealthy adversary activity across your environment, using intelligence-led hypotheses, behavioral analytics, and expert-led investigations to detect threats early and reduce dwell time.

4.1 KQL Hunting Queries

4.1.1 Scheduled Task Persistence Hunt (Core Query for Anomalous Tasks):

Reasoning: Identifies persistence via tasks like those in Perion Stealer; group by host/hash for IOC enrichment. Expected Yield: 7+ undetected hosts in tested environments.

```
let timeframe = 90d;
let commonBinaries = dynamic([
    @"(?i)Microsoft\\OneDrive\\[^\\]+\\OneDriveLauncher\.exe",
    @"(?i)ClickShare\\ClickShare\.exe",
    @"(?i)Mozilla Firefox\\default-browser-agent\.exe",
    @"(?i)Mozilla Firefox\\firefox\.exe",
    @"(?i)Microsoft\\EdgeUpdate\\MicrosoftEdgeUpdate\.exe",
    @"(?i)Google\\GoogleUpdater\\[^\\]+\\updater\.exe",
    @"(?i)Google\\Chrome\\User
Data\\PlatformExperienceHelper\\platform_experience_helper\.exe",
    @"(?i)Opera\\autoupdate\\opera_autoupdate\.exe",
    @"(?i)Dropbox\\DropboxUpdater\\[^\\]+\\updater\.exe",
    @"(?i)DropboxUpdate\\Update\\DropboxUpdate\.exe",
    @"(?i)BraveSoftware\\Update\\BraveUpdate\.exe",
    @"(?i)PowerToys\\PowerToys\.exe"
    ]);
let union_pattern = strcat(@"(", strcat_array(commonBinaries, "|"), @")");
DeviceEvents
| where TimeGenerated > ago(timeframe)
| where ActionType in (dynamic(["ScheduledTaskUpdated", "ScheduledTaskCreated"]))
| extend TaskName = tostring(parse_json(AdditionalFields)["TaskName"])
| extend TaskContent = tostring(parse_json(AdditionalFields)["TaskContent"])
| extend TaskActionsExecCommand =
tostring(parse_json(TaskContent)["Actions"]["Exec"]["Command"])
| where TaskActionsExecCommand contains "AppData\\Local\\"
| extend AppDataPath = tostring(split(tolower(TaskActionsExecCommand),
"appdata\\local\\")[-1])
| where not (TaskActionsExecCommand matches regex union_pattern)
| summarize
    FirstSeen = min(TimeGenerated),
    LastSeen = max(TimeGenerated),
    Occurences = count(),
    Devices = make set(DeviceName, 10000),
    TaskNames = make_set(TaskName, 10000),
    Commands = make_set(TaskActionsExecCommand, 10000)
    by AppDataPath
| sort by Occurences asc
```

4.1.2 Process Injection and Enumeration Hunt (Browser/Discord Targeting):

Reasoning: Detects DLL loading (e.g., Update.dll in PDF converter lures) into browsers; correlate with network beacons to C2 domains like pwrtail[.]com.

```
let suspicious = dynamic(["update.dll"]);
let lookback = 30d;
DeviceImageLoadEvents
| where TimeGenerated > ago(lookback)
| where FileName has_any (suspicious)
| extend SuspiciousPath = iif(
      // DLLs loading from user-writable locations is suspicious
      tolower(FolderPath) has @"\appdata\" or
      tolower(FolderPath) has @"\temp\"    or
      tolower(FolderPath) has @"\programdata\" or
      tolower(FolderPath) has @"\downloads\",
      true, false)
| summarize
    FirstSeen=min(TimeGenerated),
    LastSeen=max(TimeGenerated),
    LoadCount=count(),
    Hosts=make_set(DeviceName, 1000),
    Processes=make_set(InitiatingProcessFileName, 1000),
    Hashes=make_set(SHA1,1000)
  by FileName, FolderPath, SuspiciousPath
| order by LastSeen desc
| sort by SuspiciousPath desc
```

4.1.3 Exfiltration Beacon Hunt (HTTP to Suspicious Domains):

Reasoning: Spots JSON from agent-aware stealers; use UEBA for odd scores.

```
let timeframe = 90d;
let domains = dynamic(["pwrtail.com", "skillcli.com"]);
DeviceNetworkEvents
| where TimeGenerated > ago(timeframe)
| extend Timekey = bin(TimeGenerated, 2min)
| where RemoteUrl has_any (domains) and RemotePort == 443
| join kind=inner (
    DeviceProcessEvents
    | where TimeGenerated > ago(timeframe)
    | extend Timekey = bin(TimeGenerated, 2min)
    )
    on DeviceName, InitiatingProcessSHA1, Timekey
| summarize Connections = count() by DeviceName, RemoteUrl,
InitiatingProcessFileName
```

4.1.4 ConvertMate: Check for External Connections by Known Malicious Binary

Reasoning: Finds outbound connections from the ConvertMate binary.

```
let timeframe = 90d;
let suspicious = dynamic(["updateretreiver", "convertmate", "conmate"]);
DeviceNetworkEvents
| where TimeGenerated > ago(timeframe)
| where InitiatingProcessFolderPath has_any (suspicious)
| summarize
    Occurences = count(),
    Devices = make_set(DeviceName, 1000),
    RemoteURLs = make_set(RemoteUrl, 1000),
    RemoteIPs = make_set(RemoteIP, 1000)
    by InitiatingProcessFolderPath
```

4.1.5 ConvertMate: Check for Known Persistence Mechanism (Task Scheduler)

Reasoning: Detects scheduled tasks created by the malware.

```
let timeframe = 90d;
let suspicious = dynamic(["updateretreiver", "convertmate", "conmate"]);
DeviceEvents
| where TimeGenerated > ago(timeframe)
| where ActionType in (dynamic(["ScheduledTaskUpdated",
"ScheduledTaskCreated"]))
| where AdditionalFields has_any (suspicious)
```

4.1.6 ConvertMate: Detect Processes Accessing DPAPI-Protected Credentials

Reasoning: Identifies attempts by malware or its spawned processes to retrieve sensitive data from credential stores.

```
let ignore = dynamic(["msedge.exe", "chrome.exe", "brave.exe",
"msedgewebview2.exe"]);
DeviceEvents
| extend Timekey = bin(TimeGenerated, 2min)
| where TimeGenerated > ago(24h)
| where ActionType == "DpapiAccessed"
| extend
    DpapiDataAccessed = todynamic(AdditionalFields).DataDescription,
    DpapiOperation = todynamic(AdditionalFields).OperationType
| join kind=inner (
    DeviceProcessEvents
    | extend Timekey = bin(TimeGenerated, 2min) // if dpapi access within 2min
of process creation
    )
    on DeviceId, InitiatingProcessId, Timekey
| where DpapiDataAccessed has_any (dynamic(["Google Chrome", "Microsoft Edge",
"Chromium", "Brave Browser", "Opera"])) //Chromium will include electron and
such
| where not (InitiatingProcessFileName has_any (ignore))
| summarize
    count(),
    make_set(InitiatingProcessCommandLine, 1000),
    make_set(ProcessCommandLine, 1000)
    by
    InitiatingProcessParentFileName,
    InitiatingProcessFileName,
    tostring(DpapiDataAccessed),
    tostring(DpapiOperation)
```

5. Indicators of Compromise (IOC) (1/2)

TYPE	IOCs	Note
Domain	pdfskillsapp[.]com	Fake PDF converter – landing page
Domain	dldtalent[.]com	Secondary payload host (PDFSkills.exe dropper)
Domain	pwrtail[.]com	C2 server (PDFSkills campaign)
Domain	skillcli[.]com	C2 server (PDFSkills campaign)
Domain	ez2convertapp[.]com	Fake PDF converter – part of converter-tool cluster
Domain	convertyfileapp[.]com	Fake PDF converter – part of converter-tool cluster
Domain	powerdocapp[.]com	Fake PDF converter – part of converter-tool cluster
Domain	infinitedocsapp[.]com	Fake PDF converter – part of converter-tool cluster
Domain	convertmasterapp[.]com	Fake PDF converter – part of converter-tool cluster
Domain	pdfclickapp[.]com	Fake PDF converter – part of converter-tool cluster
Domain	zappdfapp[.]com	Fake PDF converter – part of converter-tool cluster
Domain	conmateapp[.]com	Landing page – ConvertMate campaign
Domain	banifuri[.]com	C2 domain – ConvertMate campaign
Domain	confetly[.]com	C2 domain – ConvertMate campaign
Domain	takelecon[.]com	C2 domain – ConvertMate campaign
Hash	2b4b63737a540d342d32a9edca06195b5c028c3b4fb9af578a736d731e7fdddd	PDFSkills.exe dropper (SHA256)
Hash	c4c29485dc0ffd7dbb2d0226854f42434931307ee307ce72fe2fdedb35794bb7	Dropper beacon hash (PDFSkills campaign)
Hash	08b9f93000512b45f8c2e8d3d6624536b366e67c40fd4b958db58e3a1d129c3d	ConvertMate.exe installer (SHA256) – ConvertMate campaign
Hash	09c2af472ab86b62a702e94a39df2bef09205f4249ed871cbeece751c1e7ef4f	UpdateRetreiver.exe malicious binary (SHA256) – ConvertMate campaign

5. Indicators of Compromise (IOC) (2/2)

TYPE	IOCs	Note
File	%LocalAppData%\PDFSkills\PDFSkills_Updater.exe	Persistence binary – PDFSkills campaign
File	%LocalAppData%\PDFSkills\Update.dll	Payload DLL – PDFSkills campaign
File	%LocalAppData%\ConvertMate\UpdateRetreiver.exe	Persistence & exfil binary – ConvertMate campaign
File	Update.dll	Common side-loaded DLL used in many converter-tool infostealers
Process	UpdateRetreiver.exe	Malicious process name – ConvertMate & similar converter campaigns
Task	ConvertMateTask	Scheduled task name – ConvertMate campaign
Task	PDFSkills_Updater	Scheduled task name – PDFSkills campaign
Registry	HKCU\Software\Microsoft\Windows\CurrentVersion\Run	Common Run key persistence used by converter-tool clusters
Detection	Trojan:MSIL/Malgent!MSR	Microsoft Defender detection name – ConvertMate binaries (post Nov 2025)
Detection	Trojan:Win32/Leonem!rfn	Microsoft Defender detection name – ConvertMate binaries (post Nov 2025)
Pattern	Scheduled task executing from %LocalAppData% (excluding known good apps)	Generic persistence pattern across almost all 2025 converter-tool infostealers
Pattern	Fake “crash report” or “update” HTTP POSTs with large JSON payloads	Generic exfiltration pattern used by LummaC2, Perion, ACR, ConvertMate, etc.

6. References

[1] Flare. “Why Gamers Are Cybercriminals’ Favorite Target in 2025.” Flare.io, 2025.
https://flare.io/learn/resources-post/cybercrime-favorite-target-gamers/
[2] Infostealers.com. “Microsoft’s New Update Creates an Agentic OS Infostealer Attack Vector.” Infostealers.com, 2025.
https://www.infostealers.com/article/microsofts-new-update-creates-an-agentic-os-infostealer-attack-vector/
[3] Verizon. 2025 Data Breach Investigations Report (DBIR). Verizon, 2025.
[4] Hudson Rock. Infostealer infection statistics and Agentic OS impact projections (2025).
[5] Microsoft & FBI. Joint report on LummaC2 infections (May 2025).
[6] ReliaQuest. “ClickFix Attacks Surge 517% in 2025.” ReliaQuest Threat Research, 2025.
[7] Proofpoint. “GHOSTPULSE and ClickFix: The Evolution of Social Engineering Delivery.” Proofpoint, 2025.
[8] Trend Micro. “ClickFix Campaigns Deliver ACR Stealer, Rhadamanthys, and PureRAT.” Trend Micro Research, 2025.
[9] Cisco Talos. “ClickFix: Steganography in PNG Images and Hotel Booking Fraud.” Talos Intelligence, 2025.
[10] Deep Instinct. “ClickFix Becomes the #2 Infostealer Delivery Vector in 2025.” Deep Instinct Blog, 2025.
[11] IBM X-Force. 2025 Threat Intelligence Index.
[12] Internal SOCRadar License on dark-web monitoring feeds & MaaS data (Perion, LummaC2, ACRStealer, SnakeStealer, Bee Stealer)
[13] National Cyber Security Centre (NCSC-NL). “Nieuwe malwarecampagne ontdekt via ManualFinder.” August 29, 2025.
https://www.ncsc.nl/actueel/nieuws/2025/08/29/nieuwe-malwarecampagne-ontdekt-via-manualfinder
[14] Luke Acha. “Suspicious Converter – Obfuscated Strings and ConvertMate Analysis.” LukeAcha.com, November 2025.
https://blog.lukeacha.com/2025/11/suspicious-converter-obfuscated-strings.html
[15] JoeSandbox Analysis Report #1787332 (ConvertMate / UpdateRetreiver.exe).
https://www.joesandbox.com/analysis/1787332/0/html