

Forum:[Hack Forums](#)

Thread: [#1 All-In-1 Volt Software|Windows, Linux,Android RAT|Crypter| \\$200 2months PROMO!!](#)

Consecration - September 17, 2026, 4:23 pm

I've just completed development of my fully functional all-in-one C2 platform a comprehensive tool that integrates Windows, Linux, and Android support alongside a built-in crypter. This is an advanced, professional grade system designed for serious users who understand what they're working with. The platform is currently hosted on my own server, and you can log in to gain full access to all its features.

For this release, so you'll always have the latest improvements and fixes. Please note: this tool requires technical knowledge and responsible handling. You must know exactly what you're doing with it. If you're interested,

Feature Functionality

WINDOWS

Shell Execution Run commands via cmd.exe / PowerShell on the host
File Transfer Upload/download files in 4MB chunks with SHA-256 integrity checks
BOF (In-Memory) Execute Beacon Object Files (COFF parser) without touching disk — 55-entry catalog
.NET Assembly Run Seatbelt, Rubeus, SharpHound, Certify in-memory via PowerShell reflection
Shellcode Execution Load and run raw position-independent shellcode in memory
Process Injection CreateRemoteThread injection into a remote process
Early Bird APC Inject shellcode into a suspended process before EDR hooks load (stealthier)
Process Hollowing Spawn a legitimate process suspended and replace its memory with the payload
Screenshot Capture the target's screen via GDI
Keylogger Capture keystrokes via GetAsyncKeyState (online + offline buffering)
Webcam Capture Snap images from the target's camera
Microphone Recording Start/stop audio capture from the target's mic
Screen Control Remotely move mouse, click, type, scroll, drag
HVNC (Hidden VNC) Control a hidden desktop + browser the user never sees, live over WebSocket
Registry Manager List, read, write, delete, and enumerate registry keys/values
UAC Bypass Elevate via cmstp / windir / fodhelper techniques
Token Manipulation Steal, make, revert, and impersonate Windows access tokens
Credential Harvest Dump SAM/LSA, browser creds, WiFi keys, Windows Vault, RDP, clipboard
Crypto Wallet Stealer Extract MetaMask/Phantom vaults, BIP39 seeds, keystores, private keys
Messenger Theft Steal Discord and Telegram session/credentials
AMSI Bypass Patch AmsiScanBuffer to disable script scanning
ETW Bypass Patch all ETW providers (EtwEventWrite, NtTraceEvent, etc.) to blind telemetry

Full DLL Unhooking Reload clean ntdll/kernel32/kernelbase/advapi32 from disk to remove EDR hooks
Indirect Syscalls Halo's Gate SSN resolution to bypass userland API hooks
Sleep Encryption Ekko-style AES memory encryption during beacon sleep (defeats memory scanners)
Heap Encryption Encrypt busy heap blocks during sleep (hides config strings from scanners)
Parent PID Spoofing Spawn child processes under explorer.exe/svchost.exe
Stack Spoofing Fake the call stack to evade stack-based detection
Module Stomping Overwrite a legitimate DLL's .text section with implant code
Hardware Breakpoint Hooks Hook functions via debug registers with no code modification
Remove PE Headers Wipe MZ/PE signatures from memory so scanners can't map the module
Log Cleanup Clear Windows event logs (Security, System, PowerShell)
Sandbox Detection Detect analysis environments via uptime, CPU, hostname, env checks
Self-Cleanup Remove the binary and clear its environment on kill/kill-date
Persistence (7) registry, schtask, startup folder, WMI event (fileless), Windows service, logon script, COM hijack
Lateral Movement wmiexec, winrm, psexec, ssh, pass-the-hash, wmi-spawn, winrm-spawn
AD Commands (24) Enum (users/groups/GPO/SPN/trusts/LAPS...), Kerberoast, AS-REP, DCSync, SAM/LSA dumps, ADCS ESC1-8 abuse
Exfiltration DNS, HTTP, ICMP, SMB, clipboard, browser, WiFi, RDP, vault, SSH keys
Pivoting SMB named-pipe relay + TCP relay for internal agents
SOCKS5 Proxy Tunnel traffic through the agent into internal networks
Port Forwarding Forward local ports to remote targets through the agent

ANDROID

Feature Functionality

APK Builder Build a working APK using raw SDK tools — no Gradle or Android Studio needed
27 Decoy App Templates Disguise the agent as Calculator, VPN Shield, Crypto Wallet, Banking, etc.
Invisible Launcher App installs and hides immediately (Theme.NoDisplay)
Foreground Service Survives Android 8+ background-execution limits
Boot Persistence Auto-restarts via BroadcastReceiver on device reboot
Remote Shell Execute shell commands on the device (e.g. content query, getprop)
SMS Stealer Read SMS messages via content provider
Contacts Stealer Dump the contact list
Call Log Stealer Extract call history
Location Stealer Collect GPS / cell-tower location
Camera Stealer Capture photos from the device camera
Microphone Stealer Record audio (call/call recorder component)
Clipboard Stealer Read clipboard contents
Keylogger Capture keystrokes via AccessibilityService
Account Stealer Dump Google/system accounts on the device
Browser Stealer Extract saved browser data
File Stealer Browse and pull files from device storage
App Inventory List installed apps, launch/stop/uninstall them
Device Info Model, OS version, manufacturer, device ID, SIM/network info
Notification Listener Drain incoming notifications
Screen Recorder Record the screen to MP4 via MediaProjection
Live VNC Stream the device screen live and control it (tap/swipe/longpress)
Gesture Control Remote tap, swipe, long-press, SMS send, USSD codes
Remote Actions Flashlight, vibrate, toast, volume, brightness control

Anti-Emulator Detect Genymotion, Nox, BlueStacks, QEMU
Anti-Debug / Anti-Root Detect debuggers and rooted devices
Anti-AV/MDM Detect ~25 security packages (Avast, Intune, AirWatch, Zimperium...)
Sandbox Delay Waits 60-120s before calling back to outlast automated analysis
Dormant Mode Stays fully silent if any analysis environment is detected

LINUX

Feature Functionality

Shell Execution Run commands via /bin/sh
File Transfer Upload/download files in 4MB chunks with SHA-256 checksums
BOF (In-Memory) Execute BOFs using memfd_create — no disk artifacts
Shellcode Execution Run raw shellcode via mmap RWX memory
Screenshot Capture screen via import / scrot / xwd
Process List Enumerate running processes (ps aux)
System Info Full host info (kernel, distro, arch, users)
Network Interfaces Dump interface + IP configuration
Keylogger Capture input via xinput
Persistence (5) cron job, systemd user service, .bashrc, .profile, /etc/rc.local
Log Cleanup Clear Linux syslogs and shell history
Sandbox Detection Detect analysis environments
Credential Harvest SSH private keys, cloud keys (AWS/Azure/GCP/K8s), .env files, shell history
Lateral Movement SSH execution, pass-the-hash
Initial Access Port scanner, DNS enumeration, host discovery
Exfiltration DNS, HTTP, ICMP, SSH keys, cloud keys, directory compression
TCP Pivot Relay Cross-platform relay for connecting air-gapped internal agents
SOCKS5 Proxy Tunnel internal traffic through the Linux agent
Port Forwarding Forward local ports to internal targets through the agent
Proxy-Aware Beacon Auto-routes through HTTP_PROXY/HTTPS_PROXY corporate proxies

CRYPTER

Feature Functionality

AES-256 Variants Encrypt payloads with AES-256-GCM, CTR, or CBC
ChaCha20 / Poly1305 Modern stream cipher alternative for encryption
Salsa20 / RC4 / XOR Additional cipher options for evasion variety
5 Chain Presets standard, double-wrap, triple-threat, deep-freeze, paranoid (up to 5 layers)
3 Stub Languages Generate loaders in Go, C, or Nim to diversify signatures
4 Execution Methods thread, fiber, APC, file, or pure memory execution
Anti-Debug Block/evade debugger attachment on execution
Anti-Sandbox Detect and refuse to run in sandbox environments
Anti-VM / Anti-Emulator Detect virtualized/emulated analysis machines
Sleep (Evasion) Time-delay to outlast automated analysis
MBA Obfuscation Mixed Boolean Arithmetic to defeat signature/decompiler analysis
Junk-Code Injection Configurable junk-code density to inflate and confuse analysis
Name Dictionaries Randomize function/variable/package names per build
Daily Key Rotation Per-day seed so each build's key rotates automatically
PE Section Renaming Rename PE sections to blend with legitimate binaries
Timestamp Manipulation Forge build timestamps on generated binaries
Entropy Normalization Balance file entropy to avoid "packed file" heuristics
Execution-Gated Decryption Payload only decrypts when run (defeats static extraction)

String Encoders none / XOR / stack / RC4 string obfuscation
BuildDNA Per-build metadata fingerprint for tracking/troubleshooting
Live Build Progress Real-time progress API + build history in the Web UI

Telegram; Nemesissoft

price: \$200 (discounted) 2months

Payment method: XMR preferably

verified Middleman on HackForum is allowed, and all sales will be completed with a formal contract.

Terms of Service:

- * This tool is provided strictly for educational purposes.
- * I bear no responsibility for any actions you take using this tool.
- * Refunds will only be issued if your issue is deemed legitimate.

[contract=tid]Start Contract[/contract]

CompulsivePurchaser - September 17, 2026, 5:30 pm

So much features and flexibility it would be super nice if you could include some videos so potential buyers can visualize and decide if they want to secure a spot. This is just personal advice from a buyer on what will defo help with your sales.

Best of luck!

Consecration - September 18, 2026, 3:16 am

(Sep 17, 2026 05:30 PM)CompulsivePurchaser Wrote: [\[CITE\]](#) So much features and flexibility it would be super nice if you could include some videos so potential buyers can visualize and decide if they want to secure a spot. This is just personal advice from a buyer on what will defo help with your sales.

Best of luck!

Thank you for the heads up.

Topia - September 19, 2026, 10:29 pm

Hey this is fire ! You should include videos about it so people can know more about.
Good luck on sales

Consecration - September 20, 2026, 7:13 am

(Sep 19, 2026 10:29 PM)Topia Wrote: [\[CITE\]](#) Hey this is fire ! You should include videos about it so people can know more about.
Good luck on sales

I'm currently away for the weekend when i get on PC will do the record to share on here.

Consecration - September 25, 2026, 4:52 am

The platform is now fully functional. I pushed a round of bug fixes and everything is confirmed working end to end.

What changed in this update:

Resolved several outstanding bugs reported across the agent and panel.

Verified core flows are stable: agent check-in, command dispatch, and result return are working as expected.

Confirmed the panel and backend are talking correctly, no dropped sessions in testing.

If you have any questions features, setup, access, whatever message me directly. I answer every question personally. No forms, no waiting on a queue, just send it over and I'll get back to you.

Stanley - September 28, 2026, 11:30 am

I'm Stanley HF's helper bot. The OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley

Goldenboi - September 29, 2026, 8:39 am

Good luck with sales buddy will contact you soon about this.

Consecration - October 1, 2026, 7:25 am

(Sep 29, 2026 08:39 AM)Goldenboi Wrote: [\[CITE\]](#) Good luck with sales buddy will contact you soon about this.

Thanks buddy you can reach me on here or tg: nemesissoft

Taking sales you can message me guys.

Beamers - October 3, 2026, 9:09 am

Sent you contract regarding this , I want the 2 month promo period on your platform thanks.

Consecration - October 4, 2026, 3:22 am

(Oct 3, 2026 09:09 AM)Beamers Wrote: [\[CITE\]](#) Sent you contract regarding this , I want the 2 month promo period on your platform thanks.

I was offline on HF, contract accepted you can message me on telegram for fast response please

TG: nemesissoft