Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

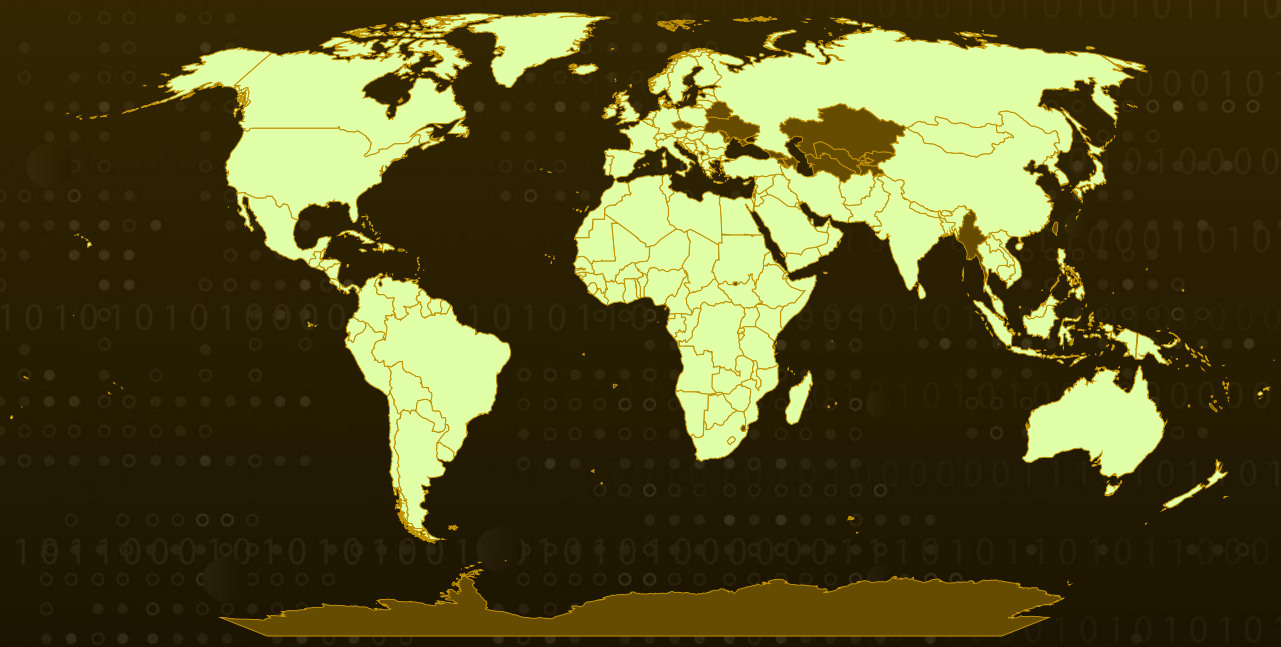
TELEPUZ: A Modular Malware-for-Hire Spreading Through ClickFix Tricks

Date of Publication	Admiralty Code	TA Number
July 17, 2026	A1	TA2026202

Summary

First Seen: Late April 2026
Targeted Regions: Global, excluding Commonwealth of Independent States (CIS) countries (Ukraine, Belarus, Armenia, Azerbaijan, Tajikistan, Georgia, Kazakhstan, Kyrgyzstan, Turkmenistan, Uzbekistan, Moldova)
Targeted Platform: Windows (64-bit)
Targeted Products: Chromium-based browsers (e.g., Chrome) and Mozilla Firefox
Malware: TELEPUZ
Attack: TELEPUZ is a lightweight, modular malware that is likely being sold as a service (MaaS). It arrives through a ClickFix scam that tricks users into running a PowerShell command, which pulls down a Go version of the Vidar stealer, which in turn installs TELEPUZ. Once on a machine it disables local defenses, escalates to SYSTEM, installs itself as a Windows service, and phones home over WebSockets to steal browser cookies, log keystrokes, run commands, capture screenshots, and inject into browsers.

Attack Regions



Attack Details

#1

A new modular malware called TELEPUZ reaches its victims through a ClickFix scam. A user lands on a booby-trapped web page that claims they need to run a quick "fix" to view the content. The page quietly plants a command in the clipboard, a trick also called pastejacking, and walks the user through pasting it into a Windows Terminal and pressing Enter. That command is PowerShell, and it downloads a second-stage file from memshowblob[.]forum into the temp folder and runs it. This second stage is a Go-based variant of the Vidar stealer, which acts as the real workhorse of the delivery chain.

#2

Vidar then pulls down two more pieces from hurgadatour[.]shop: a small stager (install.exe) and the main TELEPUZ library (telepuz.dll). The stager writes the DLL into its install folder and launches it with rundll32.exe. Once running, TELEPUZ re-launches itself under rundll32 or svchost, sets up persistence, and creates the mutex cfgmgr_mtx so only one copy runs at a time. Before doing anything noisy it runs a series of checks: it quits on machines with fewer than two CPUs, less than 2GB of memory, or too little disk space, backs off if the system language points to a CIS country, and scans for sandbox-style usernames and computer names. If it senses it is being watched, it stops. If the coast is clear, it blinds local defenses by unhooking NTDLL, patching AMSI and ETW, and stripping DLL-load notification callbacks, then looks for debuggers and builds a unique victim ID from the hardware serial number, computer name, and OS install date.

#3

From there, TELEPUZ splits into two threads. One works on gaining power: it bypasses User Account Control using the COM elevation moniker technique, with a second AppInfo ALPC and DebugObjects method held in reserve, then reaches for SYSTEM by stealing a token from a privileged process such as spoolsv.exe, msdtc.exe, WmiPrvSE.exe, or svchost.exe. It then registers itself as a Windows service named CipherAllocator so it loads inside a fresh svchost.exe instance. With that foothold, it can collect what it came for: it logs keystrokes, runs a stealer module, and pulls cookies from Chromium browsers, even working around Chrome's App-Bound Encryption by downloading a purpose-built helper binary.

#4

The second thread handles the phone-home. TELEPUZ talks to its C2 over WebSockets, optionally wrapped in TLS, using a simple JSON protocol and reaching out to the path /cdn/health with the victim ID attached. If the primary C2 (currently cal.snehamumbai[.]org, earlier cal.joycedoula[.]com[.]br, both legitimate sites the actor compromised) does not answer after ten tries, it fetches a backup address from any of four dead drops: a Telegram profile, a Steam profile, a DNS record, or a Polygon blockchain smart contract that also doubles as a kill switch. Operators can push down extra modules on demand-stealer, keylogger, and web injector and pull data back out with commands such as CreateZip and Upload, sending everything over the same C2 channel. Because the shellcode-injection command is still just a placeholder, it is clear the malware is a work in progress.

Recommendations

- **Block ClickFix Clipboard Execution:** Warn users never to paste and run commands from a web page, and use browser and endpoint controls to flag or block clipboard-driven command execution, since that is exactly how the infection starts.
- **Restrict and Log PowerShell:** Enforce PowerShell Constrained Language Mode, turn on Script Block Logging, and alert on PowerShell that uses flags like -NoP, -w h, -ep bypass, or that calls DownloadFile to a temp folder.
- **Block Known TELEPUZ Indicators:** Add the staging domains, C2 domains, IP addresses, and download URLs listed in the IoCs section to web proxies, DNS filtering, and firewall blocklists.
- **Watch for rundll32 Abuse:** Alert when rundll32.exe loads a DLL from %TEMP%, %AppData%, or %ProgramData%, or is spawned by an unusual parent, as TELEPUZ relies on rundll32 to launch its main payload.
- **Detect Unauthorized Service Creation:** Monitor for new services and their registry keys under HKLM\SYSTEM\CurrentControlSet\Services, especially the observed names CipherAllocator and PilotmasterMast, and investigate any service backed by a DLL in a user-writable path.
- **Protect Browser Credentials and Cookies:** Deploy phishing-resistant MFA and treat session cookies as sensitive, so that stolen cookies and saved credentials cannot be replayed; watch for unexpected processes reading browser profile data.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1608: Stage Capabilities	T1608.001: Upload Malware
Execution	T1204: User Execution	T1204.004: Malicious Copy and Paste
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
	T1106: Native API	
	T1129: Shared Modules	
	T1569: System Services	T1569.002: Service Execution
Persistence	T1543: Create or Modify System Process	T1543.003: Windows Service
Privilege Escalation	T1548: Abuse Elevation Control Mechanism	T1548.002: Bypass User Account Control
	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
		T1134.002: Create Process with Token
Defense Evasion	T1218: System Binary Proxy Execution	T1218.011: Rundll32
	T1112: Modify Registry	
	T1055: Process Injection	T1055.012: Process Hollowing
	T1620: Reflective Code Loading	

Tactic	Technique	Sub-technique
Defense Evasion	T1562: Impair Defenses	T1562.006: Indicator Blocking
	T1027: Obfuscated Files or Information	T1027.007: Dynamic API Resolution
		T1027.013: Encrypted/Encoded File
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1622: Debugger Evasion	
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
		T1497.003: Time Based Evasion
	T1070: Indicator Removal	T1070.004: File Deletion
Credential Access	T1539: Steal Web Session Cookie	
	T1555: Credentials from Password Stores	
	T1056: Input Capture	T1056.001: Keylogging
Discovery	T1057: Process Discovery	
	T1083: File and Directory Discovery	
	T1082: System Information Discovery	
	T1033: System Owner/User Discovery	

Tactic	Technique	Sub-technique
Discovery	T1518: Software Discovery	
	T1614: System Location Discovery	T1614.001: System Language Discovery
Collection	T1113: Screen Capture	
	T1560: Archive Collected Data	T1560.002: Archive via Library
	T1185: Browser Session Hijacking	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1573: Encrypted Channel	T1573.002: Asymmetric Cryptography
	T1105: Ingress Tool Transfer	
	T1102: Web Service	T1102.001: Dead Drop Resolver
Exfiltration	T1041: Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	580b441e2961739fd26e54e0a0ea08351cb10a51839519fc722cfa39ecd0c954, 03fa348b70819296c958c842e7646b3b7efe5fa217ed5098143003c47995a746, 58aec6e3835aaf20f7b4a7e308b36a19e7454673a6f71783871e9bcf6cae8eed, bf3b4e645a3c0c23f87c55971069014f7424ad14497371ee7567eff68ffaf343, ff791fe1532a2dc3b3c188a71bfd0177f973ef228e4d1dda1db6d3c4b0d62b3e, a955d7e2819d5fa8b5f879cb970e1a1a91327098a7383f2a03a5e1e7e19435e3, 9733a3f6409de81271f21993c7f8b9865ac9f5c68c3d4336e91afe6b312477eb, 444f1c0c82b3f6cc31d685bac68b20edbde5722ce219af9cceab0c2a6537efc1
Domains	memshowblob[.]forum, chubrik[.]sbs, betalegenda[.]cfd, mavpaprokla[.]lat, comicstar[.]lat, bigblower[.]click, momasites[.]lol, momasites[.]com, mamsites[.]lol, hardenedom[.]shop, hardendedom[.]shop, hardendom[.]shop, hardeneddom[.]shop, netblokirovka[.]asia, netblokir[.]asia, netlobikrovka[.]asia, neblokirovka[.]as, kidsko[.]shop, mazaporka[.]shop, hurgadatour[.]shop, krabsburger[.]xyz, zewaplus[.]club, cal[.]joycedoula[.]com[.]br, cal[.]snehamumbai[.]org

TYPE	VALUE
IPv4	172[.]67[.]215[.]214, 172[.]67[.]165[.]144
URLs	hxxps[:]//memshowblob[.]forum/api/index[.]php?a=grab, hxxps[:]//chubrik[.]sbs/files/xK7mR9pL2nQw5tY8/ygvfuyze[.]dll, hxxps[:]//betalegenda[.]cfd/files/xK7mR9pL2nQw5tY8/kmwvogwx[.]dll, hxxps[:]//mavpaprokla[.]lat/files/telemetriawork/telepuz[.]dll, hxxps[:]//comicstar[.]lat/files/telemetriawork/telepuz[.]dll, hxxps[:]//bigblower[.]click/files/telemetriawork/telepuz[.]dll, hxxps[:]//momasites[.]lol/files/telemetriawork/telepuz[.]dll, hxxps[:]//momasites[.]com/files/telemetrywork/telepuz, hxxps[:]//mamsites[.]lol/files/telemetrywork/telepuz[.]dll, hxxps[:]//hardenedom[.]shop/files/telemetriawork/telepuz[.]dll, hxxps[:]//hardendedom[.]shop/files/lemetriawork/epuz[.]dll, hxxps[:]//hardendom[.]shop/files/telemetry/telepuz[.]dll, hxxps[:]//hardeneddom[.]shop/files/telemetrywork/telepuz, hxxps[:]//netblokirovka[.]asia/files/telemetriawork/telepuz[.]dll, hxxps[:]//netblokir[.]asia/files/telemetriawork/telepuz[.]dll, hxxps[:]//netlobikrovka[.]asia/files/telemetriawork/telepuz[.]dll, hxxps[:]//neblokirovka[.]as/telemetry/network/telepuz[.]dll, hxxps[:]//kidsko[.]shop/files/telemetriawork/telepuz[.]dll, hxxps[:]//mazaporka[.]shop/files/telemetriawork/telepuz[.]dll, hxxps[:]//172[.]67[.]215[.]214/files/telemetriawork/telepuz[.]dll, hxxps[:]//hurgadatour[.]shop/files/telemetriawork/telepuz[.]dll, hxxp[:]//krabsburger[.]xyz/files/telemetriawork/telepuz[.]dll, hxxps[:]//zewaplus[.]club/files/telemetriawork/telepuz[.]dll, hxxps[:]//172[.]67[.]165[.]144/files/telemetriawork/telepuz[.]dll, hxxps[:]//t[.]me/chanadarkpart, hxxps[:]//steamcommunity[.]com//profiles/76561199705801219
File Path	%AppData%\Local\DCFG\Runtime\Themes\Processor\etwhost.dll, %AppData%\Roaming\StateRepository\Host\Recovery\systemreset.dll, %AppData%\Local\MiravaDevices\noraxrecovery.dll, %ProgramData%\XeroxPrint\Temp\Worker\grpeng.dll, %ProgramData%\Jundrax\Tracker\IrenScanner.dll, %ProgramData%\QualcommRF\dsp_agent.dll
Mutex	cfgmgr_mtx, bginfod_mtx, wfj64_mtx
Registry Key	HKLM\SYSTEM\CurrentControlSet\Services\CipherAllocator, HKLM\SYSTEM\CurrentControlSet\Services\PilotmasterMast

References

https://www.elastic.co/security-labs/telepuz-maas-malware-clickfix

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

July 17, 2026 • 06:50 AM

More at www.hivepro.com