Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

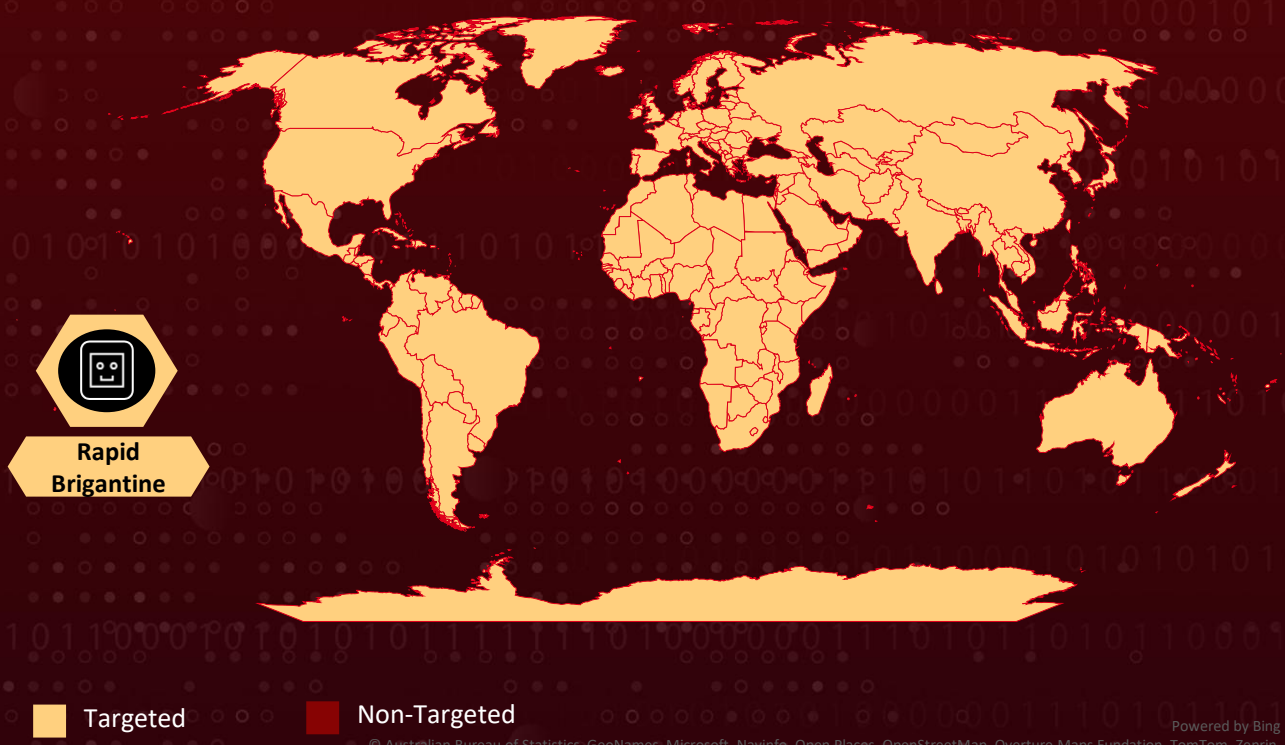
ClickFix Campaigns Deliver BabaDeda, Lorem Ipsum, and Potemkin Loaders

Date of Publication	Admiralty Code	TA Number
June 25, 2026	A1	TA2026176

Summary

First Seen: May 2026
Targeted Region: Global
Targeted Platform: Microsoft Windows
Targeted Products: Google Chrome, Mozilla Firefox, Microsoft Edge, Microsoft Defender, WordPress
Targeted Industries: Education, Financial Services, Architecture, Legal Services, Non-profit, Construction Technology, Content Publishing
Threat Actor: Rapid Brigantine (a.k.a. Vanilla Tempest, Vice Society, Vice Spider, DEV-0832)
Malware: Potemkin, RMMProject, EtherRAT, BabaDeda Loader, Lorem Ipsum Loader
Attack: Three separate ClickFix campaigns are tricking users into pasting malicious commands into Windows, and each one delivers a different loader. Potemkin drops the RMMProject RAT, along with EtherRAT, which spread across more than 11 hosts to reach the domain controller. BabaDeda Loader delivers a .NET stealer plus the DanaBot and SectopRAT stealers. Lorem Ipsum Loader, tied with the group Rapid Brigantine, installs a backdoor that leads to Oyster, Supper, and MeowBackConn, ending in Rhysida ransomware.

Attack Regions



Attack Details

#1

All three campaigns begin with ClickFix social engineering. Users visiting compromised or malicious websites are shown a fake browser-update, security-update, or CAPTCHA-style prompt instructing them to open a Windows utility, the Run dialog, or Windows Terminal, and paste an attacker-supplied command. In one chain, the pasted command abuses pcalua.exe as a living-off-the-land binary to proxy mshta.exe execution, which fetches a remote HTA that hides its window and silently downloads and installs an MSI.

#2

In another, a PowerShell command masquerading as a Microsoft Edge security intelligence update downloads a ZIP archive together with a portable, legitimately signed Node.js runtime, then launches an embedded JavaScript dropper with a hidden window and a second hidden PowerShell process with execution policy set to Bypass. A third chain presents a fake verification prompt to run a PowerShell command that stages further components. Delivery infrastructure includes at least five compromised WordPress sites spanning architecture, legal services, non-profit, construction technology, and content publishing, plus a rotating pool of themed fake-update domains. After initial execution, each chain stages a modular, multi-component Loader.

#3

Potemkin had one simple job: to deliver the next piece of malware. After the ClickFix trick installed it through an MSI file, Potemkin found its command server and loaded a tool called RMMProject straight into memory, never saving it to disk. RMMProject is the part that did the real damage, stealing browser passwords and cookies, secretly controlling the screen, and slipping its code into other programs. The attacker also dropped EtherRAT (a backdoor that hides its server address on the blockchain) and set up tunneling tools to move around the network, eventually spreading EtherRAT to more than 11 machines, including the domain controller.

#4

BabaDeda Loader delivered its malware in two different ways. One path installed a backdoor and information stealer that scans the computer, opens a secret connection to the attacker's server, and steals browser cookies, saved passwords, and files when told to. The other path dropped a fake software package that used a trusted program to load malicious code and pulled its real payload out of a hidden file, then launched the DanaBot and SectopRAT stealers in memory.

#5 The Lorem Ipsum chain in this set is operationally tied with high confidence to Rapid Brigantine, a financially motivated group active since at least mid-2022 and known for deploying Rhysida, BlackCat, Zeppelin, and Quantum Locker ransomware. The group is documented using trojanized installers signed through a malware-signing-as-a-service provider, which matches the pipeline behind earlier Lorem Ipsum activity, and the late-May pivot to ClickFix followed directly from the takedown of that certificate supply, leaving an unsigned delivery path as the only viable option.

#6 A separately documented intrusion deployed the Lorem Ipsum Loader alongside MeowBackConn on domain controllers, placing the loader squarely inside the group's established post-exploitation arsenal (Oyster, Supper, MeowBackConn) that culminates in Rhysida deployment. Whether the Lorem Ipsum operators are Rapid Brigantine personnel directly or a closely allied development team feeding tooling into the group's pipeline remains an open intelligence gap, but the operational linkage holds either way.

Recommendations

Disable the Windows Run Dialog and Restrict Windows Terminal: Use Group Policy to disable the Run dialog and the Win+R hotkey, and restrict wt.exe where feasible. Every chain in this advisory depends on the user pasting a command into one of these; if the prompt never opens, the attack fails at the first step.

Block Script Interpreters from User-Writable Paths: Use AppLocker or Windows Defender Application Control to prevent PowerShell, node.exe, mshta.exe, and pcalua.exe from running scripts or binaries staged in C:\ProgramData, AppData, and Temp directories.

Alert on Anomalous Parent-Child Process Chains: Treat wt.exe or a browser spawning PowerShell download cradles, pcalua.exe proxying mshta.exe, and portable node.exe executing from C:\ProgramData as high-fidelity detections.

Enable Tamper Protection and Monitor Defender Tampering: Turn on Microsoft Defender tamper protection and raise high-priority alerts on Stop-Service WinDefend, sc.exe config WinDefend start= disabled, bulk Add-MpPreference -ExclusionPath operations, and Set-MpPreference disable toggles.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1584: Compromise Infrastructure	T1584.006: Web Services
	T1608: Stage Capabilities	T1608.004: Drive-by Target
		T1608.001: Upload Malware
	T1583: Acquire Infrastructure	T1583.008: Malvertising
	T1588: Obtain Capabilities	T1588.003: Code Signing Certificates
Initial Access	T1189: Drive-by Compromise	
Execution	T1204: User Execution	T1204.004: Malicious Copy and Paste
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.007: JavaScript
		T1059.003: Windows Command Shell
	T1218: System Binary Proxy Execution	T1218.005: Mshta
		T1218.007: Msiexec
	T1106: Native API	
Persistence	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
Privilege Escalation	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft

Tactic	Technique	Sub-technique
Defense Evasion	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1112: Modify Registry	
	T1140: Deobfuscate/Decode Files or Information	
	T1027: Obfuscated Files or Information	
	T1620: Reflective Code Loading	
	T1574: Hijack Execution Flow	T1574.001: DLL
	T1055: Process Injection	T1055.001: Dynamic-link Library Injection
	T1218: System Binary Proxy Execution	T1218.011: Rundll32
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1497: Virtualization/Sandbox Evasion	
	T1480: Execution Guardrails	
Credential Access	T1555: Credentials from Password Stores	T1555.003: Credentials from Web Browsers
	T1539: Steal Web Session Cookie	
Discovery	T1518: Software Discovery	T1518.001: Security Software Discovery
	T1082: System Information Discovery	
	T1087: Account Discovery	
	T1057: Process Discovery	

Tactic	Technique	Sub-technique
Lateral Movement	T1021: Remote Services	T1021.002: SMB/Windows Admin Shares
		T1021.006: Windows Remote Management
	T1047: Windows Management Instrumentation	
	T1570: Lateral Tool Transfer	
Collection	T1113: Screen Capture	
	T1560: Archive Collected Data	
	T1005: Data from Local System	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1568: Dynamic Resolution	T1568.002: Domain Generation Algorithms
	T1102: Web Service	T1102.001: Dead Drop Resolver
		T1102.002: Bidirectional Communication
	T1572: Protocol Tunneling	
	T1090: Proxy	
	T1573: Encrypted Channel	
	T1105: Ingress Tool Transfer	
Impact	T1486: Data Encrypted for Impact	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	2abe5dd3a057fdef935722e50e9251c272d29fd26113187b853a1f9a9cb89d9b, 3b7ae925e2d64522b4f69b56285b05aeca8c5aab5ab46a9c02c4fafb69d881ce, cd4e5e2c65b1660470d3446539ee68adf5faeece3eaeb46583623be9911ee145, 79f7b67ce8b39070f3e1c2b90fce0ce84134782a7dedcccc1edac197ee9e089b, 2ada24dd6e517f37942b749c2bd57ddd97445e9853002cee70a0bc30d0b0ce3a, 97bc78ad3fd6549f3a7f9cb31be1ff25d50bac97c42fc6dfff44e47424c5add1, dff20059f161090c76f9f45ac2269f2965bdc96023c78c1072f8d1aa66b06919
IPv4	77[.]110[.]122[.]58, 213[.]165[.]41[.]26, 51[.]222[.]96[.]58
IPv4:Port	213[.]165[.]41[.]26[:]22603, 51[.]222[.]96[.]58[:]1080
Domains	cl[.]distritovagas[.]com, sonra[.]eutialyson[.]com, anus-staylard[.]xyz, pestrear-lamp[.]xyz, uglyshop-mare[.]xyz, rule-bead-dust[.]xyz, fair-bath-fond[.]xyz, resumeacceptable[.]com, autoupdatet[.]com, autoupdaters[.]com, autoupdatethis[.]com, openanyworddocument[.]com, kittyfreespace[.]com, searchdocumentsfree[.]com, letsdiskuss[.]com, digitalpoint[.]com
URL	hxxps[:]//cl[.]distritovagas[.]com/hte[.]hta

TYPE	VALUE
URLs	hxxps[:]//sonra[.]eutialyson[.]com/inst24[.]msi, hxxp[:]//77[.]110[.]122[.]58[:]23205/lQhEQui9a4lZ[.]exe, hxxp[:]//77[.]110[.]122[.]58[:]23205/cons_1[.]0[.]1[.]msi, hxxp[:]//77[.]110[.]122[.]58[:]44479/bjxxUmG8K3uy[.]ps1, hxxps[:]//autoupdatet[.]com/get_update?i=75975, hxxps[:]//openanyworddocument[.]com/api/init/40237612-00ac-4a85-bce9-7400f148c474
Filenames	RunSearch.exe, avast_update.bin, inst24.msi, cons_1.0.1.msi, hte.hta, Update.js, Update.zip, msedge.zip, NET Runtime Optimization Service.exe, mscoree.dll, msvcp140.dll, c8w2i9KUtgpF.bat, List.Control.dat, linguist.zip, EGGjVyW9Uloz.msi, MTSetup_v15.3.7191.msi, netdrv.dll, askndfao.dll, lQhEQui9a4lZ.exe, D0OK1nWwId9W.ps1, O67tak2KFRmJ.ps1, J6Gupb9TpYNI.ps1, fsjH6IHuUkhh.ps1, yH88LG8yCOnU.ps1, ek_full.ps1, ek_kill_av.ps1, ek_disable_av.ps1, RlLF3rizah.ini, MseKOytIWeVrP85.xml, EkYqfsgfyz.ini
File Path	C:\Users\<username>\AppData\Local\Microsoft\RunSearch\RunSearch.exe

TYPE	VALUE
File Paths	%LOCALAPPDATA%\hyper-v.ver, %TEMP%\dll_debug.log, C:\ProgramData\p\, C:\Users\<username>\AppData\Local\KafhCqGLhOS4\, C:\ProgramData\.NET Runtime Optimization Service c8w2i9KUtgpF\, C:\Windows\SysWOW64\config\systemprofile\AppData\Local\FdgW2ni2h0it\sq8whb\node.exe
Registry Key	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\RunSearch, HKCU\Software\Microsoft\Windows\CurrentVersion\Run\WindowsHost, HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\EdgeUpdate
Ethereum Contract Address	0xb3f2897f2bc797e5b9033faef8c81e92b01cb831, 0x40b57c3622c1CbfD699207F71F2dE5A8Fe256893
UUID	ab653feb-9e78-4578-87ed-2e30329fe858

References

https://www.huntress.com/blog/potemkin-loader-rmmproject-clickfix-attack

https://www.morphisec.com/blog/what-is-the-babadeda-loader-analysis-of-a-new-clickfix-malware-campaign/

https://www.bluevoyant.com/blog/orem-ipsum-clickfix-rapid-brigantine

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

June 25, 2026 • 12:50 AM

More at www.hivepro.com