Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

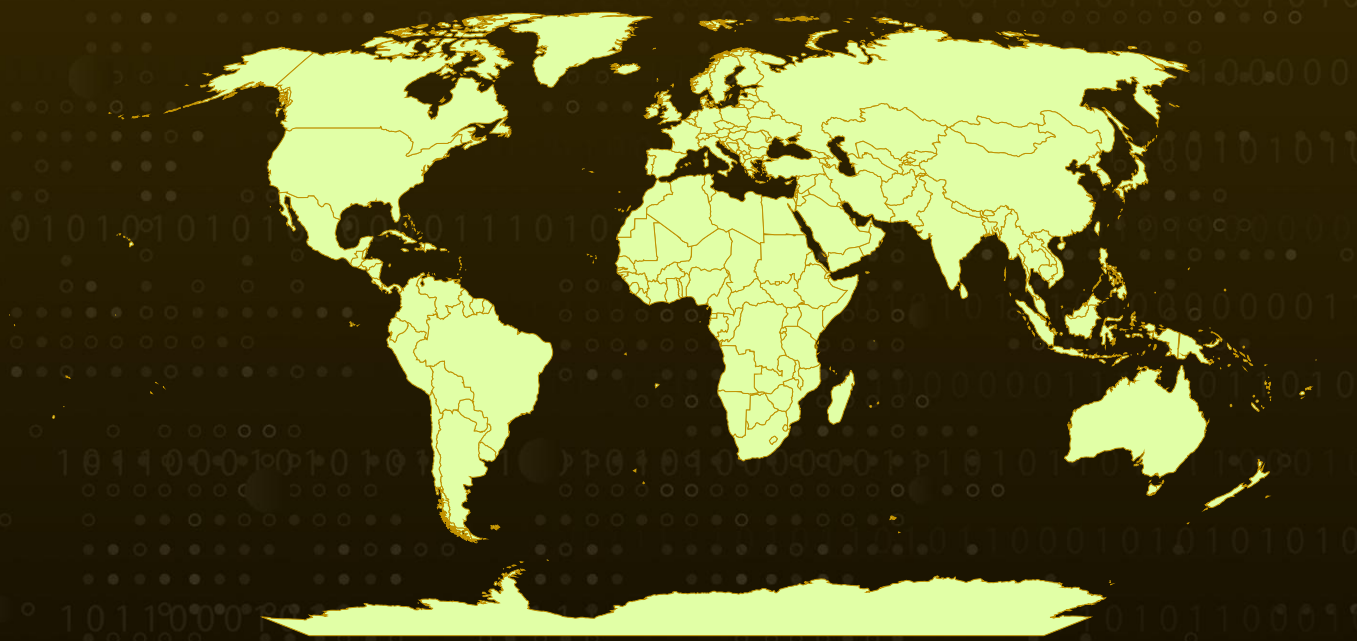
A Fake Update, a Real Threat: The FDMTP Backdoor's Supply Chain Run

Date of Publication	Admiralty Code	TA Number
August 06, 2026	A1	TA2026222

Summary

First Seen: 2025
Targeted Regions: Worldwide
Targeted Platform: Windows
Targeted Products: QuickFox VPN and network accelerator
Malware: FDMTP
Attack: FDMTP is a modular backdoor delivered through a compromised version of QuickFox, a VPN and network accelerator popular with Chinese users living abroad. Active since at least August 2025, the campaign added malicious JavaScript to trojanized Windows installers that fingerprint each device, avoid personal gaming machines, and selectively deploy the FDMTP implant onto machines showing signs of developer, financial, or translation software. Once installed, FDMTP profiles its host, reports back to a staging command server, and awaits additional plugins pushed down over a dedicated command-and-control channel. QuickFox has since removed the malicious code from its installer, though intelligence gaps remain around the campaign's full scope and intended targets.

Attack Regions



Attack Details

#1 FDMTP reaches victims through a compromised software supply chain rather than a phishing email or an exploited vulnerability. The target is QuickFox, a VPN and network accelerator used mainly by Chinese international students and expats. Attackers modified a legitimate Windows installer by adding malicious JavaScript into its Electron renderer HTML file. This tampered installer circulated in QuickFox builds from version 3.51.0 through 3.59.5, before the vendor removed the malicious code with version 3.59.6 following responsible disclosure.

#2 Once installed, the planted JavaScript reaches out to a look-alike domain designed to pass as QuickFox's own infrastructure, then pulls down a second, heavily obfuscated script disguised as Firebase analytics code. That script checks whether the machine is running Windows, confirms with its command server that the device hasn't already been infected, then checks the running processes. If the popular game platform Steam is running, the infection quietly stops; if instead a translation, financial, or developer tool is running, the script downloads a package pairing a legitimate Microsoft utility with a malicious companion file. The legitimate file loads its malicious counterpart, which decrypts and runs the final payload: an implant with fifteen internal modules known as FDMTP.

#3 This campaign has not shown credential theft or movement between machines on a network. Instead, FDMTP gathers a detailed profile of its host, including installed antivirus software, network and operating system details, and the current username, then reports this back to its command infrastructure. A follow-up request lists every running process, likely helping operators decide which infected devices are worth pursuing further. This points to a campaign still in its target-validation phase rather than actively spreading.

#4 Communication with the attackers occurs in two stages: a short web request to a staging domain to obtain command-server addresses, followed by a dedicated protocol for ongoing contact on ports in the 20800-20816 range. Through this channel, the command server can push additional plugin modules, store them in a registry key associated with the infected machine, and trigger them on demand. One observed plugin downloaded extra files to the machine, showing how operators can extend the implant's capabilities without updating the core payload.

Recommendations

Update QuickFox to a Clean Version: Upgrade all Windows installations of QuickFox to version 3.59.6 or later, the first release confirmed to have the trojanized installer components removed.

Verify Installer Integrity Before Deployment: For any QuickFox installer already downloaded, confirm its file hashes against known-clean releases before running it, since affected builds spanned versions 3.51.0 through 3.59.5.

Hunt for DLL Side-Loading via csmonitor.exe: Review endpoints for the legitimate Windows Azure Compute and Storage Emulator binary launching from non-standard paths such as the local temp directory, a strong signal of the side-loading technique used to load the FDMTP loader.

Extend Scrutiny to Personal-Use Software on Corporate Devices: Treat consumer VPN, proxy, and accelerator tools installed on work devices as part of the software supply chain risk surface, since this campaign specifically leveraged one to reach corporate endpoints.

Establish a Vetting Process for Third-Party Applications: Require security review of consumer-grade utilities before they are permitted on managed devices, particularly ones sourced outside a formal procurement or patch-management program.

Maintain Backups Isolated from Production Networks: Keep offline or segmented backups for endpoints in higher-risk categories, ensuring recovery options exist regardless of what a pushed plugin ultimately does.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1195: Supply Chain Compromise	T1195.002: Compromise Software Supply Chain
Execution	T1059: Command and Scripting Interpreter	T1059.007: JavaScript
Defense Evasion	T1027: Obfuscated Files or Information	
	T1140: Deobfuscate/Decode Files or Information	
	T1574: Hijack Execution Flow	T1574.001: DLL
	T1036: Masquerading	T1036.005: Match Legitimate Resource Name or Location
	T1480: Execution Guardrails	
Persistence	T1112: Modify Registry	
Discovery	T1057: Process Discovery	
	T1082: System Information Discovery	
	T1016: System Network Configuration Discovery	
	T1033: System Owner/User Discovery	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1104: Multi-Stage Channels	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	2B6CDAFDFE427A3DE1A94A8A2CA1F09FC4C8F90E4F59089FD9B35B73185ED01C, 3BD3B300F3278520819A06D0CB1F0EADBF946DBBC11352538246FF075EB427F1, 5CBB64375636E83B5F17D6083633CECC02E2A5F4168CD7CCA5CDEE36CCCA9B38, 6634339B813E6105B5138DE6AB67B016B8DFBF49233C29DE9BAB3207E8B50D24, 6932A20AC61FD3F93D7CFEE414F6F46834068AC7C9CA011B054A6A10DC56B3D1, 7462CE2595119C928CF516EC33148DC2A39DD9F71636A5C849C7ED93B7C5CA06, 795594AD5E6F2868CC4D8ED12DABF4F3999A1477C6B250527C5EDE9A98528FB9, A53D756F28457B1C4A239C91CDEC8ED7B7DA67A93E332E6DF9621CBEF8417474, A5D36EDC34FE54B2092349F877DAF560A98F5FEA635D1AC4A110B3518102EF96, D9DB5CBC193DDAF4C0A265804FDEF70C32451DAAF2974FA9ADF52CE1DEFAC5F7, DC666E9C148BBCA5E21D8C9A97143575C075F53360F135E0191AED9E8278D396
SHA1	11A6DF1E15663AE89F59A9E598AE8987F42A632B, 173DD4190740B96F6F733C801B6428ED4B52B607, 2CC0425A90A39AC4EEDADD59CAAAFAD5B50F8420, 3449A349B6C8045B16DF4F88D58C65C2BDF891BB, 39504CEAD410056878962053F8D027E9F299CD10, 7AB7FFE4C233A4F2440F0FDEB2E117C788792281, A195810C41F401C4B48CB557CF8CE60C2D807025, B194A997C9A653134BDB1F2D0C3137DCDACB54D5, B370B674CE877B9C0A7708C7834AEB7EDA983564, C41B4E11E6A9E3B53DA1F92B213DE9F65A825C92, E90D2730F3354FF1ADF334B03C95EAC3207D47B9
MD5	03FD832B81DD54D2BF5F610A8FF27856, 19E760EE849EB7C1F100F2B7010A763D, 1F3031167F94B166CC7B69376A01C124, 2DD8681DCD218C88D1C78DFE939EC92B, 2FFDCFB7157511789228988E26D06FD6, 30D59C3D4916AA5FB24050C6AAE7F8E4, 3B79D95F7F7B58C401A3BC79F94EBB52,

TYPE	VALUE
MD5	5E4ED6ABBF555E5A542E3D4308CCD7BF, 5F3DAF7417DD666213168EB6C7453CC7, B1D344C9A1525373BE6A3980FA85A603, E0A92209DD62DAE8460D934DC6B7DDD7
Domains	cdns3[.]51quickfox[.]cn, www[.]google-apis[.]net, www[.]icloud-cdn[.]net, www[.]techcheck1[.]com, www[.]wangmeng66[.]top, www[.]wangmeng[.]xyz, www[.]wangmengsb[.]com, www[.]yahoo-cdn[.]it[.]com
URLs	hxxp[:]//cdns3[.]51quickfox[.]cn/2025090411/update[.]zip, hxxp[:]//www[.]icloud-cdn[.]net[:]8080/GetCluster, hxxp[:]//www[.]icloud-cdn[.]net[:]8080/GetSlaver, hxxps[:]//cdns3[.]51quickfox[.]cn/script/firebase-analytics-compat[.]js, hxxps[:]//cdns3[.]51quickfox[.]cn/script/firebase-app-compat[.]js, hxxps[:]//www[.]google-apis[.]net/dfsvc[.]exe, hxxps[:]//www[.]google-apis[.]net/dfsvc[.]exe[.]config, hxxps[:]//www[.]google-apis[.]net/wangmeng[.]dll, hxxps[:]//www[.]icloud-cdn[.]net/Client[.]dll, hxxps[:]//www[.]icloud-cdn[.]net/checksum[.]bin, hxxps[:]//www[.]icloud-cdn[.]net/dnscfg[.]dll, hxxps[:]//www[.]icloud-cdn[.]net/vshost[.]exe, hxxps[:]//www[.]techcheck1[.]com/GetClusterNodes, hxxps[:]//www[.]techcheck1[.]com/GetPeers, hxxps[:]//www[.]techcheck1[.]com/Microsoft[.]VisualStudio[.]HostingProcess[.]Utilities[.]Sync[.]dll, hxxps[:]//www[.]techcheck1[.]com/config[.]etl, hxxps[:]//www[.]techcheck1[.]com/dfsvc[.]exe[.]config, hxxps[:]//www[.]techcheck1[.]com/vshost[.]exe, hxxps[:]//www[.]techcheck1[.]com/wangmeng[.]dll, hxxps[:]//www[.]wangmeng66[.]top/GetAddresses, hxxps[:]//www[.]wangmeng66[.]top/GetEndpoints, hxxps[:]//www[.]wangmeng66[.]top/GetHosts, hxxps[:]//www[.]wangmeng66[.]top/GetInstances, hxxps[:]//www[.]wangmeng66[.]top/GetMachines, hxxps[:]//www[.]wangmeng66[.]top/GetPeers, hxxps[:]//www[.]wangmeng66[.]top/GetProxies, hxxps[:]//www[.]wangmeng66[.]top/GetReplicas, hxxps[:]//www[.]wangmeng66[.]top/GetResources, hxxps[:]//www[.]wangmeng66[.]top/GetRoutes, hxxps[:]//www[.]wangmeng66[.]top/GetServers,

TYPE	VALUE
URLs	hxxps[:]//www[.]wangmeng66[.]top/GetTargets, hxxps[:]//www[.]wangmeng66[.]top/GetWorkers, hxxps[:]//www[.]wangmeng[.]xyz/GetAgents, hxxps[:]//www[.]wangmeng[.]xyz/GetEndpoints, hxxps[:]//www[.]wangmeng[.]xyz/GetInstances, hxxps[:]//www[.]wangmeng[.]xyz/GetMachines, hxxps[:]//www[.]wangmeng[.]xyz/GetMembers, hxxps[:]//www[.]wangmeng[.]xyz/GetNodes, hxxps[:]//www[.]wangmeng[.]xyz/GetPeers, hxxps[:]//www[.]wangmeng[.]xyz/GetReplicas, hxxps[:]//www[.]wangmeng[.]xyz/GetRoutes, hxxps[:]//www[.]wangmeng[.]xyz/GetServers, hxxps[:]//www[.]wangmeng[.]xyz/GetTargets, hxxps[:]//www[.]wangmeng[.]xyz/GetVips, hxxps[:]//www[.]wangmeng[.]xyz/GetWorkers, hxxps[:]//www[.]wangmengsb[.]com/GetAddresses, hxxps[:]//www[.]wangmengsb[.]com/GetAgents, hxxps[:]//www[.]wangmengsb[.]com/GetBackends, hxxps[:]//www[.]wangmengsb[.]com/GetHosts, hxxps[:]//www[.]wangmengsb[.]com/GetIps, hxxps[:]//www[.]wangmengsb[.]com/GetNodes, hxxps[:]//www[.]wangmengsb[.]com/GetPeers, hxxps[:]//www[.]wangmengsb[.]com/GetReplicas, hxxps[:]//www[.]wangmengsb[.]com/GetRoutes, hxxps[:]//www[.]wangmengsb[.]com/GetServers, hxxps[:]//www[.]wangmengsb[.]com/GetVips, hxxps[:]//www[.]wangmengsb[.]com/GetWorkers, hxxps[:]//www[.]yahoo-cdn[.]it[.]com/GetCluster, hxxps[:]//www[.]yahoo-cdn[.]it[.]com/Microsoft[.]VisualStudio[.]HostingProcess[.]Utilities[.]Sync[.]dll, hxxps[:]//www[.]yahoo-cdn[.]it[.]com/config[.]etl, hxxps[:]//www[.]yahoo-cdn[.]it[.]com/dfsvc[.]exe, hxxps[:]//www[.]yahoo-cdn[.]it[.]com/dfsvc[.]exe[.]config, hxxps[:]//www[.]yahoo-cdn[.]it[.]com/dnscfg[.]dll, hxxps[:]//www[.]yahoo-cdn[.]it[.]com/vshost[.]exe
	38[.]60[.]142[.]56, 43[.]240[.]12[.]34, 43[.]240[.]12[.]35, 45[.]125[.]15[.]100, 45[.]125[.]15[.]104, 45[.]125[.]15[.]111, 45[.]125[.]15[.]114, 45[.]125[.]15[.]115, 45[.]125[.]35[.]225,

TYPE	VALUE
IPv4	45[.]125[.]35[.]226, 45[.]125[.]35[.]227, 45[.]125[.]35[.]229, 45[.]125[.]35[.]230, 45[.]125[.]35[.]231, 45[.]125[.]35[.]232, 45[.]125[.]35[.]233, 45[.]125[.]35[.]234, 45[.]125[.]35[.]235, 45[.]125[.]35[.]236, 45[.]158[.]180[.]250, 47[.]76[.]92[.]73, 47[.]83[.]122[.]51, 47[.]86[.]14[.]22, 47[.]88[.]21[.]252, 47[.]238[.]64[.]56, 47[.]238[.]240[.]219, 47[.]239[.]4[.]179, 47[.]239[.]93[.]49, 103[.]231[.]15[.]135, 103[.]231[.]15[.]219, 103[.]231[.]15[.]248, 103[.]246[.]244[.]13, 103[.]246[.]244[.]20, 104[.]21[.]7[.]138, 104[.]21[.]37[.]164, 104[.]21[.]39[.]112, 104[.]21[.]44[.]82, 104[.]21[.]89[.]96, 104[.]21[.]95[.]64, 123[.]254[.]105[.]38, 123[.]254[.]106[.]148, 154[.]223[.]24[.]158, 154[.]223[.]54[.]159, 154[.]223[.]58[.]64, 154[.]223[.]58[.]142, 154[.]223[.]75[.]206, 170[.]33[.]128[.]5, 172[.]67[.]135[.]248, 172[.]67[.]143[.]103,

TYPE	VALUE
IPv4	172[.]67[.]144[.]222, 172[.]67[.]157[.]196, 172[.]67[.]197[.]227, 172[.]67[.]210[.]148, 202[.]181[.]25[.]71, 202[.]181[.]25[.]73
Filenames	Assist.dll, Client.dll, Microsoft.ServiceHosting.Tools.dll, config.bin, csmonitor.exe, data.dat, firebase-analytics-compat.js, firebase-app-compat.js, index.html, update.bin, update.zip
File Path	%TEMP%\quickfox\update.zip, %APPDATA%\Local\Temp\quickfox\updated\, %LocalAppData%\Microsoft\WindowsApps

References

https://www.fortinet.com/blog/threat-research/quickfox-supply-chain-attack-used-to-deploy-fdmtp-implant

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

August 06, 2026 • 08:30 AM

More at www.hivepro.com