Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

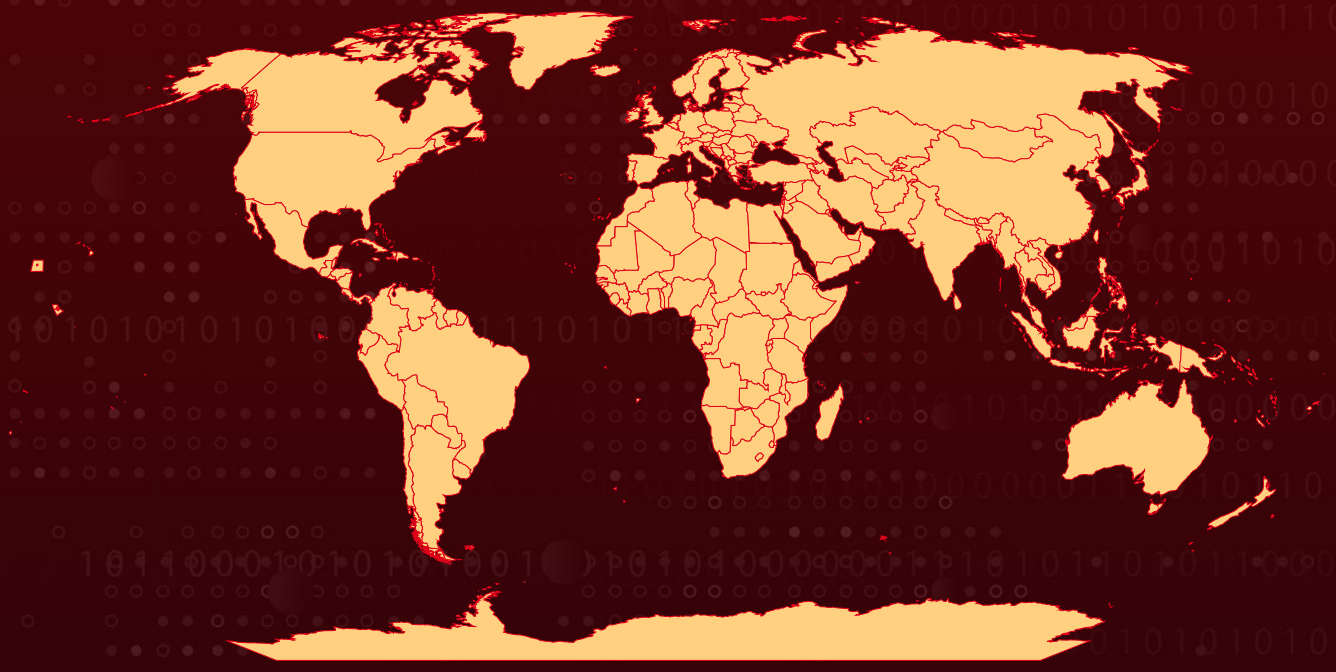
TamperedChef: A High-Severity Multi-Stage Infostealer Operation

Date of Publication	Admiralty Code	TA Number
November 20, 2025	A1	TA2025354

Summary

Attack Commenced: May 2025
Payload Activated: August 21, 2025
Targeted Region: Worldwide
Targeted Platform: Windows
Targeted Industries: Healthcare, Construction, Manufacturing, Industrial, Hospitality, Legal, Non-Profit, Technology, Retail, Transportation, Agriculture, Automotive, Education, Energy, Government
Malware: TamperedChef
Attack: The TamperedChef campaign is a sophisticated 2025 malware operation distributing signed fake PDF tools through SEO-driven malvertising to gain user trust. Its unique 56-day dormancy let the apps function normally before mass activation on August 21, deploying an obfuscated backdoor for credential theft, data exfiltration, and remote access. Using shell companies to obtain EV certificates and rapidly rotating infrastructure, the attackers heavily impacted U.S. victims and sectors like healthcare, construction, and manufacturing, making TamperedChef a high-severity, financially motivated threat.

Attack Regions



Attack Details

#1

The TamperedChef campaign is a sophisticated global malware operation that began in late June 2025, relying on highly convincing malvertising with fake, signed installers masquerading as legitimate productivity tools such as PDF editors. These applications behave normally at first to build trust while silently establishing persistent footholds. Victims are typically drawn in through poisoned search results and malicious SEO-optimized ads, often while searching for product manuals or PDF editing utilities.

#2

A defining trait of TamperedChef is its deliberate 56-day dormancy period. During this time, the fake applications provide real PDF-editing functionality while covertly laying persistence mechanisms. This delay, aligned with common Google Ads campaign cycles, enabled the malware to evade sandbox analysis and achieve broad distribution before mass activation on August 21, 2025, triggered using the "–fullupdate" command.

#3

Upon activation, the malware drops task.xml to create a scheduled task that executes a heavily obfuscated JavaScript backdoor. This backdoor runs silently, forcibly terminates browser processes, and abuses Windows DPAPI to decrypt stored passwords, cookies, and authentication tokens. It gathers machine metadata and sends the stolen data, XOR-encrypted with random keys, to attacker-controlled C2 servers. It also supports remote code execution, enabling persistent access, credential theft, data exfiltration, and potential ransomware deployment.

#4

The operators show strong industrialization, using U.S. shell companies (e.g., Stratus Core Digital LLC, DataX Engine LLC) and Malaysian entities to obtain legitimate Sectigo EV certificates, which they rapidly rotate after revocation. Their infrastructure uses short-lived NameCheap-registered domains and evolving C2 naming (from DGA-style strings to human-readable names). Though unattributed, motivations appear financially driven, initial access brokerage, credential theft, ransomware staging, with possible opportunistic espionage.

#5

Victims are mostly in the U.S. (80%), with smaller impact in Europe. Healthcare, construction, and manufacturing are heavily affected, as employees frequently search for technical manuals online. The campaign's sophistication, delayed activation, and persistence make it a high-severity threat requiring urgent detection and mitigation.

Recommendations

Hunting and Remediation: Searching for persistence indicators like the registry key HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\PDFEditorUpdater, scheduled tasks named “PDFEditorScheduledTask,” and presence in %LOCALAPPDATA%\Programs\PDFEditor\ directly aligns with known TamperedChef IOC patterns. Immediate credential resets and full system reimaging for confirmed infections are advised due to the malware’s deep persistence and evasion capabilities.

Behavioral EDR Detection: Implementing EDR tuned for behavioral patterns such as browser process termination by non-browser apps, creation of scheduled tasks using XML files, and suspicious JavaScript execution from AppData folders addresses the campaign’s obfuscation and modular tactics effectively. The use of Microsoft Sysmon with custom rules is supported by documented incident response practices.

Blocking Malicious Infrastructure: Blocking known C2 domains like api.mxpanel.com and others at the network layers, combined with DNS security and IoC feeds, is critical for containment. Monitoring HTTPS outbound from productivity apps to suspicious domains is also standard threat defense procedure.

Application Control: Enforcing strict software installation policies, allowing only vetted PDF editors and productivity suites through corporate channels, and blocking unauthorized downloads reduces user exposure to malicious installers. This is foundational to preventing initial infection vectors used by TamperedChef.

User Awareness Training: Educating users about the dangers of downloading free or unknown software alternatives and recognizing malvertising on search engines addresses the social engineering part of the attack chain. Emphasizing IT approval for software installations is an industry best practice.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0002 Execution	TA0001 Initial Access	TA0040 Impact
TA0007 Discovery	TA0004 Privilege Escalation	TA0006 Credential Access	TA0011 Command and Control
TA0010 Exfiltration	TA0009 Collection	T1518.001 Security Software Discovery	T1082 System Information Discovery
T1046 Network Service Discovery	T1555.003 Credentials from Web Browsers	T1071 Application Layer Protocol	T1071.001 Web Protocols
T1070 Indicator Removal	T1497.003 Time Based Evasion	T1497 Virtualization/Sandbox Evasion	T1553 Subvert Trust Controls
T1036 Masquerading	T1539 Steal Web Session Cookie	T1552 Unsecured Credentials	T1553.002 Code Signing
T1204 User Execution	T1012 Query Registry	T1132.001 Standard Encoding	T1059 Command and Scripting Interpreter
T1204.002 Malicious File	T1059.003 Windows Command Shell	T1059.007 JavaScript	T1547.001 Registry Run Keys / Startup Folder
T1547 Boot or Logon Autostart Execution	T1132 Data Encoding	T1518 Software Discovery	T1027 Obfuscated Files or Information
T1005 Data from Local System	T1573 Encrypted Channel	T1102 Web Service	T1041 Exfiltration Over C2 Channel
T1608 Stage Capabilities	T1189 Drive-by Compromise	T1053.005 Scheduled Task	T1053 Scheduled Task/Job
T1608.006 SEO Poisoning			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	0826824694c80b854603f4c4103133113a197d3ecbca4308899ae9d6f05847fa, 08ea829d5c97aab089abe19686d274f829aa1cee3670d2819885e33f39a4d602, 105e58c4c04b56607badd705411e3322c152b8dbb21d994e7cdec62253a0e454, 244251cab1f6df4bb39ba28645cbc4e26f84298b588b568a796d6520912c6156, 26163c7da9f0d9000937663497d7eb15df5c205cc2edbb71d664f08a5b1f80ce, 2a3f76fc7f953403653eff71f21c16d40512c1bcd7a038657bb1d0a4efbee677, 2bfa87dee2000f4e7889174f051ab88f4b690d08629b94721e321c44b7cf1bd3, 2c9895fbdf8b86715a8e501f85d206b28cf9b61478826409a8a8ea17a067da22, 35c34043a4a8b1f15ce9ab7661be6ace91348f725d59e53f04a36c41999812c7, 3d4bdd41ebc630b8b676fc39e14de75a59cebf545cf342a4dea8072f5768c13e, 406e26453a9eb779da6dd792e82cf904fbaf11b9e15471316276bb49098bdbf6, 504a614d8baae84c7c57e1786d22981fb016e4c9396ab10cc73197aa483d9261, 6438b3c4eb5810c003d6f2cf1712652d3ce0504f08ae05aec1f07594e0a58a52, 6c4e54bbf98113068bdeef172ae6fb05fe1e99bb50ae4622b06e06af35b2b043, 6e4cd57e87e034723d4c1a3ff93e8c9def0f27961da3e5bc361536e847a119cb, 898aa0bca40ec01d3564cb33f7a79f2e651f987ea65db913a62d427973ba5478, 94acbfe1958b1b985701c8232fd3262ee01ef665ba59a92489b900d8f988b233, 9704e97a395649e9ea4450b3afde5c1f1b22caa05407c4db3ef1625b9db05324, 9f572779dba2ef760f8a2bd7391dcafc099c430bcbd94c7d5247b210e1f095da,

TYPE	VALUE
SHA256	abb7541aba5abe1ff27b3867c1d45cea9c678743648ed8eed50bf32f8676e510, af1185876d9d71955e6829f2475c1dce06d33522d0d0e66817d47b9318951314, b66d89ee13a48e9c8d4a7aa2e3e1cb2b79f0b95e4f74f4184b85628656281588, b9906cc6622a11fb67d5ad9db784dc9b62a0da5bd1fd4fe8887f74bfbbfe125d, b9b4375c1992b71f9dc08ee613b2b316b8df8b9e1fdd2c7a1e98d89f43a1625f, bfdb330a8c56def312154c44aed2b36705850adaf6febced8d6d7740beb27715, c0308cc7c56443ad23fbb26671dc8f77d253e873f77c4c3d2486b34317feb417, c4f0b51308eb02c20e9bb33df80442b85b0cc0ad3ccf2598546d67c49242d506, cdf51e7f8f24b01bed83da50839b15f143569740c88c2033c43cfc9c17c1b5c8, d162b02a9163fc68ece3db162af0da2c33a595e2258aff171064a5383f41a566, e11aa8dd0b0bc4c21cb081f70565225abc192159f7deb4396aec5720941841ae, f145e61e5d89f51fd3b94fef3e8bc2571aeae4c91c701751e9f603dfd5037dd9, f181501175a30d5fce22af768321cd3de000bba5b19281f39abed236862a3107, f748022beadc73f905f9cd2d5b94be2095265433f6c9770860facda2f6b623c6, fbc7ffc5bdda978afe0f20910210752d91762b97d6d7719a5b3a1e352a4717c3, fde67ba523b2c1e517d679ad4eaf87925c6bbf2f171b9212462dc9a855faa34b, 09207f1dfdd000b42b3433b85d051e8e446a1a1f2f63ab66d47edb9b196f618c, 231ddfa8114475892dd404f27b769ab2e43e9101ec7a7d3608546154a8b75d4d, 255062c602a36f649baaec922cc8b98b27854e8e90b6ee8ded660a2e4e101b77, 37bd388296f6c46e45aa42053758ae17328cfa677ac9ba41ef925d3c8bccfb99, 3c702aa9c7e0f2e6557f3f4ac129afd2ad4cfa2b027d6f4a357c02d4185359c4, 5273bcdeb88ae274294ce71831b63a54ea8b1dd55b4b2222b5eeb0f44150f931,

TYPE	VALUE
SHA256	69b373084e47cbb54a9003ae2435adb49f184bfa11989a2800700da22a153dff, 6e8b48972fab5610363cf4063c289e1670a252fdd40c020de0e3cfcd33c819f4, 7dfa0774992032810660b413836e92f8ac3a4f6de5fa94c5f08c8159c34270e4, 83efb5f2688207a7ccf49ddb81cb094543c2fef5bf73f01342cc39b0af68e72b, 98bb0ab170efdf98414114d6c14a047d2144730f3552bb4aea36198fc49083ac, a3fc5447a9638a3469bab591d6f94ee2bc9c61fc12fd367317eec60f46955859, a696cf7cead8a2219559c802ecc395dcafd2e8f084bfcb8b011c0454519dc5f2, afb0c6b4b0af0a14ac725c025ac70e8b2d8b392094ecdb10e8a2afe2ecf47ea8, bcb46bf1c909958a09c52d22ca54dc281357e3c5bdc0f87a6f54553b7c31af9d, c541cfe6baea9c48e44f808977846c2f2a2dab4cfcca677701ceac6d8fc4e1cc, d3b7e26ed39783a6dd8fd107795d4afcf0a28dc5d9da1f4dd54ee905d9fb8f89, da3c6ec20a006ec4b289a90488f824f0f72098a2f5c2d3f37d7a2d4a83b344a0, f97c7edb0d8d9b65bf23df76412b6d2bbfbab6e3614e035789e4e1a30e40b7f1, 847dd2b363fc02d1f501207074eb4eecdff19063cc0cd7adce1572b428f970d8, bb3a744ac6a75e732dea1bd2110bc101205a2d19fdc7fbca82058f287cd61f3b, c6dddeb7286806a99a2f208d094298d7fcaaae3cfba0103f9e0fe02ff6759069, 1bbf0e1323cff3168b548c4a80ec40fd3bed7630dccb7474ba4b8099df5e79d0, 1dcd142daf1116b6a3fac113c638248bf2e0859bb55411cec2256e3d6e9e94ae, 1e351bbae5338f24ce217ac182317ac7a4aee825cbaa5fe55cc347b650d2e987, 216e604948812db2d5062b20504e9acaf271d745da544a2c5d074a5fbf111ac9, 2a3a9ab2ad245d3464b5cc1bc8270568b5c490e4972e99e8f94ab2177874d81a, 2fee5916dad509ff4fea4f4b17795677bda7316253111b2abf7f523bae2a973e,

TYPE	VALUE
SHA256	69b373084e47cbb54a9003ae2435adb49f184bfa11989a2800700da22a153dff, 6e8b48972fab5610363cf4063c289e1670a252fdd40c020de0e3cfcd33c819f4, 7dfa0774992032810660b413836e92f8ac3a4f6de5fa94c5f08c8159c34270e4, 83efb5f2688207a7ccf49ddb81cb094543c2fef5bf73f01342cc39b0af68e72b, 98bb0ab170efdf98414114d6c14a047d2144730f3552bb4aea36198fc49083ac, a3fc5447a9638a3469bab591d6f94ee2bc9c61fc12fd367317eec60f46955859, a696cf7cead8a2219559c802ecc395dcafd2e8f084bfcb8b011c0454519dc5f2, afb0c6b4b0af0a14ac725c025ac70e8b2d8b392094ecdb10e8a2afe2ecf47ea8, bcb46bf1c909958a09c52d22ca54dc281357e3c5bdc0f87a6f54553b7c31af9d, c541cfe6baea9c48e44f808977846c2f2a2dab4cfcca677701ceac6d8fc4e1cc, d3b7e26ed39783a6dd8fd107795d4afcf0a28dc5d9da1f4dd54ee905d9fb8f89, da3c6ec20a006ec4b289a90488f824f0f72098a2f5c2d3f37d7a2d4a83b344a0, f97c7edb0d8d9b65bf23df76412b6d2bbfbab6e3614e035789e4e1a30e40b7f1, 847dd2b363fc02d1f501207074eb4eecdff19063cc0cd7adce1572b428f970d8, bb3a744ac6a75e732dea1bd2110bc101205a2d19fdc7fbca82058f287cd61f3b, c6dddeb7286806a99a2f208d094298d7fcaaae3cfba0103f9e0fe02ff6759069, 1bbf0e1323cff3168b548c4a80ec40fd3bed7630dccb7474ba4b8099df5e79d0, 1dcd142daf1116b6a3fac113c638248bf2e0859bb55411cec2256e3d6e9e94ae, 1e351bbae5338f24ce217ac182317ac7a4aee825cbaa5fe55cc347b650d2e987, 216e604948812db2d5062b20504e9acaf271d745da544a2c5d074a5fbf111ac9, 2a3a9ab2ad245d3464b5cc1bc8270568b5c490e4972e99e8f94ab2177874d81a,

Note: The remaining Indicators of Compromise (IOCs) can be accessed on the platform.

References

https://www.acronis.com/en/tru/posts/cooking-up-trouble-how-tamperedchef-uses-signed-apps-to-deliver-stealthy-payloads/

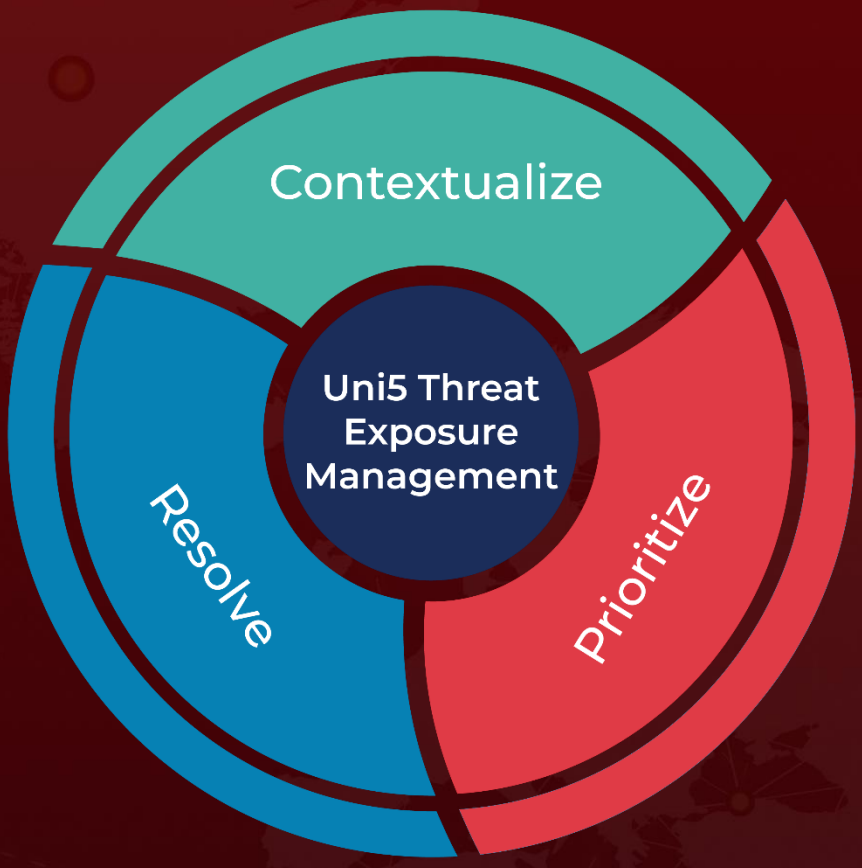
https://labs.withsecure.com/publications/tamperedchef

https://twilightcyber.com/tamperedchef-infostealer-fake-pdf-editor-malvertising-2025/

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 free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

November 20, 2025 . 11:30 PM

More at www.hivepro.com