Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

ClickFix Con: Phishing Scam Turns Video Calls into Malware Havens

Date of Publication	Admiralty Code	TA Number
October 25, 2024	A1	TA2024410

Summary

Attack Commenced: March 2024
Campaign: ClickFix
Malware: Stealc, Rhadamanthys, AMOS Stealer
Affected Platforms: Windows and macOS
Targeted Region: Worldwide
Targeted Industries: Transport, Logistics

Attack: In 2024, the ClickFix phishing method intensified as cybercriminals employed deceptive Google Meet pages, phishing emails, and fake websites to spread malware. Groups such as the Slavic Nation Empire (SNE) and Scamquerteo were instrumental in this trend, managing to evade conventional security protocols and targeting users on both Windows and macOS platforms.

Attack Regions

Attack Details

#1 In May 2024, a rise in cyber threats exploiting fake Google Meet pages surfaced as part of a broader phishing campaign known as ClickFix. This method enables malware distribution through compromised websites, phishing emails, and fake video conferencing platforms that imitate Google Meet.

#2 The goal is to trick victims into running malicious code, often delivered via a PowerShell script using a ClearFake cluster to install various malware, including infostealers. These fraudulent Google Meet pages display fake pop-ups claiming microphone or headset problems, prompting users to click a "fix" button.

#3 For Windows users, this leads to the installation of malware like Stealc and Rhadamanthys, while macOS users are served with AMOS Stealer. These attacks are hazardous as they evade typical security measures like Google Safe Browsing.

#4 Earlier, in March 2024, the initial access broker TA571 began employing the ClickFix technique in phishing campaigns. As the year progressed, cybercriminals expanded the use of ClickFix by embedding it into compromised software websites, primarily via fake CAPTCHA pages.

#5 Recent campaigns have been linked to two cybercrime groups, the Slavic Nation Empire (SNE) and Scamquerteo, who have been fueling this surge in sophisticated phishing and malware attacks.

Recommendations

Recognize Phishing Indicators: Educate users to spot suspicious elements, such as fake video call interfaces, unexpected pop-ups, and "fix" buttons for supposed audio or video issues. Train employees to avoid clicking unknown or suspicious prompts in video calls.

Deploy Endpoint Detection and Response (EDR): EDR solutions can detect and respond to suspicious activities, such as attempts to install infostealers like Stealc and AMOS. Ensure your EDR can identify unusual PowerShell activity and stealthy malware variants.

Analyze Traffic to Malicious IPs: Use network monitoring to detect traffic to malicious domains and IPs linked to known malware servers. Look for connections attempting to contact command-and-control (C2) servers associated with malware like Stealc and Rhadamanthys.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0005 Defense Evasion	**TA0007** Discovery	**TA0011** Command and Control	**TA0010** Exfiltration
T1566 Phishing	**T1566.002** Spearphishing Link	**T1071.001** Web Protocols	**T1059** Command and Scripting Interpreter
T1059.001 PowerShell	**T1204** User Execution	**T1204.002** Malicious File	**T1036** Masquerading
T1036.005 Match Legitimate Name or Location	**T1070** Indicator Removal	**T1027** Obfuscated Files or Information	**T1059.003** Windows Command Shell
T1189 Drive-by Compromise	**T1574** Hijack Execution Flow	**T1105** Ingress Tool Transfer	**T1071** Application Layer Protocol
T1588.001 Malware	**T1588** Obtain Capabilities		

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	meet[.]google[.]us-join[.]com, meet[.]googie[.]com-join[.]us, meet[.]google[.]com-join[.]us, meet[.]google[.]web-join[.]com, meet[.]google[.]webjoining[.]com, meet[.]google[.]cdm-join[.]us, meet[.]google[.]us07host[.]com, googiedrivers[.]com, alienmanfc6[.]com, apunanwu[.]com, bowerchalke[.]com, carolinejuskus[.]com, cautrucanhtuan[.]com, cphoops[.]com, dekhke[.]com, iloanshop[.]com, kansaskollection[.]com, lirelasuisse[.]com, mdalies[.]com, mensadvancega[.]com, mishapagerealty[.]com, modoodeul[.]com, pabloarruda[.]com, pakoyayinlari[.]com, patrickcateman[.]com, phperl[.]com, stonance[.]com, utv4fun[.]com, us18web-zoom[.]us, webapizmland[.]com, us01web-zoom[.]us, us03web-zoom[.]us, us07web-zoom[.]us, us08web-zoom[.]us, us09web-zoom[.]us, us10web-zoom[.]us, us30web-zoom[.]us, us40web-zoom[.]us, us45web-zoom[.]us, us50web-zoom[.]us, us60web-zoom[.]us, us70web-zoom[.]us,

TYPE	VALUE
Domains	us77web-zoom[.]us, us80web-zoom[.]us, us85web-zoom[.]us, us95web-zoom[.]us, us004web-zoom[.]us, us005web-zoom[.]us, us006web-zoom[.]us, us007web-zoom[.]us, us008web-zoom[.]us, us050web-zoom[.]us, us055web-zoom[.]us, us500web-zoom[.]us, us505web-zoom[.]us, us555web-zoom[.]us, us002webzoom[.]us, us003webzoom[.]us, us4web-zoom[.]us, us5web-zoom[.]us, us6web-zoom[.]us, us01web[.]us, us03web[.]us, us08web[.]us, us09web[.]us, us15web[.]us, us20web[.]us, us40web[.]us, us50web[.]us, us55web[.]us, web05-zoom[.]us, webroom-zoom[.]us, doculuma[.]com, fatoreader[.]com, fatoreader[.]net, gamascript[.]com, verdascript[.]com, veriscroll[.]com, calipsoproject[.]com, lunacy3[.]com, lunacy4[.]com, projectcalipso[.]com, thecalipsoproject[.]com, web3dev[.]buzz, battleforge[.]cc, battleultimate[.]xyz, mybattleforge[.]xyz, myultimate[.]xyz,

TYPE	VALUE
Domains	playbattleforge[.]org, playbattleforge[.]xyz, playultimate[.]xyz, tooldream[.]live, ultimategame[.]xyz, ultimateplay[.]xyz, argongame[.]com, darkblow[.]com, missingfrontier[.]com, nightpredators[.]com, riotrevelry[.]com, thewatch[.]com, us12web[.]us, webjoining[.]com, Web3 web browser, sleipnirbrowser[.]org, sleipnirbrowser[.]xyz, cozyland[.]xyz, cozymeta[.]com, cozymeta[.]fun, cozymeta[.]xyz, cozyweb3[.]com, cozyworld[.]io, worldcozy[.]com, ngtmeta[.]io, ngtmetaland[.]io, ngtmetaweb[.]com, ngtproject[.]com, ngtstudio[.]io, ngtstudio[.]online, ngtverse[.]org, night-support[.]xyz, nightstudio[.]io, nightstudioweb[.]xyz, lastnuggets[.]com, mor-dex[.]world, mordex[.]blog, mordex[.]digital, mordex[.]homes, nor-tex[.]eu, nor-tex[.]pro, nor-tex[.]world, nor-tex[.]xyz, nort-ex[.]eu, nort-ex[.]lol,

TYPE	VALUE
Domains	nort-ex[.]world, nortex-app[.]pro, nortex-app[.]us, nortex-app[.]xyz, nortex[.]app, nortex[.]blog, nortex[.]digital, nortex[.]life, nortex[.]limited, nortex[.]lol, nortex[.]uk, nortexapp[.]com, nortexapp[.]digital, nortexapp[.]io, nortexapp[.]me, nortexapp[.]pro, nortexapp[.]xyz, nortexmessenger[.]blog, nortexmessenger[.]digital, nortexmessenger[.]pro, nortexmessenger[.]us
URLs	hxxp[:]//95[.]182[.]97[.]58/84b7b6f977dd1c65[.]php, hxxps[:]//meet[.]google[.]com-join[.]us/wmq-qcdn-orj, hxxps[:]//meet[.]google[.]us-join[.]com/ywk-batf-sfh, hxxps[:]//meet[.]google[.]us07host[.]com/coc-btru-ays, hxxps[:]//meet[.]google[.]webjoining[.]com/exw-jfaj-hpa, hxxps[:]//googledrivers[.]com/fix-error, hxxp[:]//91[.]103[.]140[.]200[:]9078/3936a074a2f65761a5eb8/6fmfpmi7[.]fwf4p, hxxps[:]//carolinejuskus[.]com/kusaka[.]php?call=launcher, hxxps[:]//carolinejuskus[.]com/f9dfbcf6a999/7cc2f5dc3c76/load[.]51f8527e20dcb05ffd8586b853937a8a[.]php?call=launcher, hxxp[:]//85[.]209[.]11[.]155/joinsystem, hxxp[:]//77[.]221[.]157[.]170[:]3004/server[.]js, hxxps[:]//us18web-zoom[.]us/stealc[.]exe, hxxps[:]//us18web-zoom[.]us/ram[.]exe, hxxps[:]//webapizmland[.]com/api/cmdruned,
IPv4	77[.]221[.]157[.]170, 95[.]182[.]97[.]58, 91[.]103[.]140[.]200, 85[.]209[.]11[.]155,
SHA256	92a8cc4e385f170db300de8d423686eeeec72a32475a9356d967bee9e3453138,

TYPE	VALUE
SHA256	a834be6d2bec10f39019606451b507742b7e87ac8d19dc0643ae58df183f773c, 2853a61188b4446be57543858adcc704e8534326d4d84ac44a60743b1a44cbfe, 94379fa0a97cc2ecd8d5514d0b46c65b0d46ff9bb8d5a4a29cf55a473da550d5

References

https://blog.sekoia.io/clickfix-tactic-the-phantom-meet/

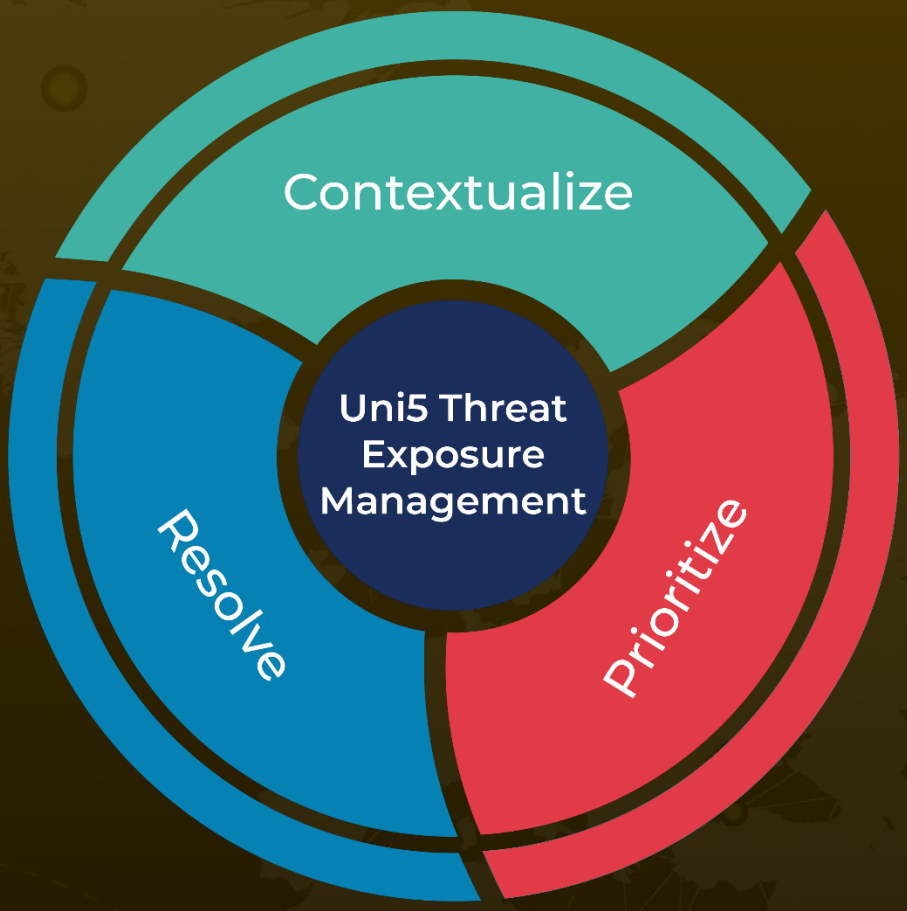
https://hivepro.com/threat-advisory/ta866-makes-a-comeback-with-extensive-email-campaign/

https://hivepro.com/threat-advisory/atomic-stealer-sneaks-in-via-fake-browser-updates/

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

October 25, 2024 • 5:00 AM

More at www.hivepro.com