Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

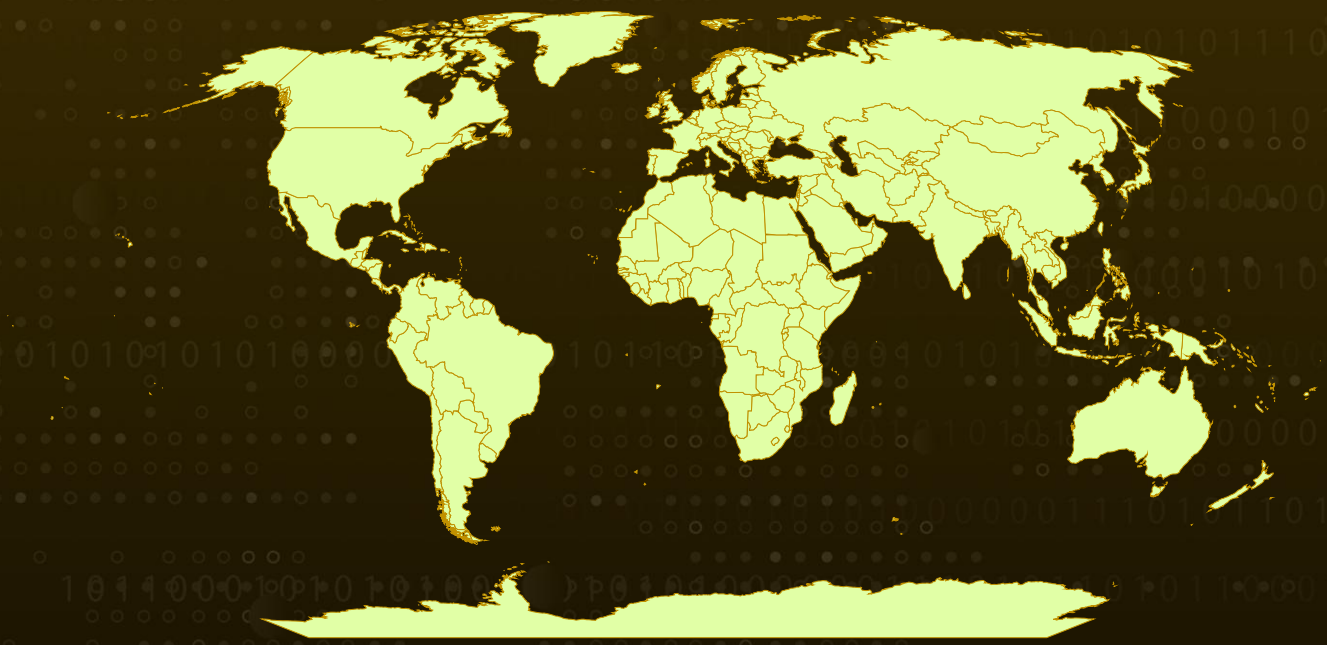
When AI Turns Against You: The Malvertising Trap of Kling AI

Date of Publication	Admiralty Code	TA Number
May 22, 2025	A1	TA2025160

Summary

First Seen: 2025
Malware: PureHVNC RAT
Targeted Industries: Banking, cryptocurrency
Targeted Countries: Worldwide
Attack: In early 2025, attackers launched a deceptive campaign by impersonating Kling AI, to trick users into downloading malware. Promoted heavily through fake social media ads, the campaign led victims to a bogus website where they were lured into clicking a button only to receive a malicious ZIP file containing a disguised Windows executable. This file triggered a stealthy loader, designed to evade detection, establish persistence, and inject a second-stage payload. That payload was a customized PureHVNC Remote Access Trojan (RAT), capable of full system control, surveillance, and data theft.

Attack Regions



Attack Details

#1 In early 2025, a deceptive cyber campaign was uncovered that impersonated Kling AI a well-known platform for generating AI-based images and videos. The attackers set up a convincing fake website that tricked users into believing they were using a legitimate AI tool. Instead of receiving actual media content, users were duped into downloading malicious files disguised as image or video outputs. These files used double extensions and special characters like Hangul Fillers to conceal their true nature as Windows executable files. Once executed, they triggered a stealthy loader built with .NET Native AOT (Ahead-of-Time) Compilation, helping it evade antivirus detection.

#2 The attack chain began with social media malvertising. Researchers identified over 70 fake promoted posts mimicking Kling AI across various platforms. When users visited the fraudulent AI site and interacted with it such as uploading an image or clicking the “Generate” button they were served a ZIP archive containing a single .exe file. Though named to resemble a media file, it was actually an application, with a 292-byte filename designed to obscure its real identity.

#3 The first-stage loader was developed in .NET and incorporated multiple evasion tactics, including checks for virtual environments and the presence of analysis tools like Wireshark, Procmon, and OllyDbg. To maintain persistence, it created a registry run key and dropped a copy of itself in the %APPDATA%\Local directory. It then injected a second-stage payload into trusted system processes such as InstallUtil.exe or AddInProcess32.exe, allowing it to operate under the radar.

#4 The second-stage payload, often obfuscated using .NET Reactor, delivered a tailored version of the PureHVNC Remote Access Trojan (RAT). This RAT provided attackers with full remote control over the compromised machines and included capabilities such as keylogging, data theft, and remote desktop access. One of its plugins, PluginWindowNotify, actively monitored foreground windows for keywords like “crypto” or “bank,” taking screenshots and alerting the attacker when sensitive information was detected.

#5 Clues in the campaign, including Vietnamese language strings in the code, ad locations, and names associated with financial transactions, suggested Vietnamese threat actors were behind the operation. This campaign is a strong reminder of how threat actors are increasingly combining social engineering, evasive malware techniques, and AI-themed lures to compromise users at scale.

Recommendations

- **Be cautious of AI tools promoted via social media ads:** Avoid downloading software or files from promoted posts or unofficial sources. Always verify URLs and stick to the legitimate websites of AI tools like Kling AI.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.
- **Block known malicious domains and fake AI websites:** Continuously update web filters and DNS security solutions to block access to domains used in this and similar campaigns. Monitor for newly registered domains that imitate popular AI services.
- **Disable autorun execution of unknown files**: Apply group policies to restrict execution from locations like %APPDATA% or %TEMP% to minimize the impact of droppers that attempt to persist using these paths.
- **Educate users about deceptive file types:** Train employees to recognize suspicious file names, especially those using double extensions (e.g., .jpg.exe) or unusual characters like Hangul fillers designed to mask executables as media files.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0006 Credential Access	TA0009 Collection	TA0011 Command and Control
T1566 Phishing	T1588 Obtain Capabilities	T1588.007 Artificial Intelligence	T1113 Screen Capture
T1132 Data Encoding	T1132.001 Standard Encoding	T1056 Input Capture	T1056.001 Keylogging

T1005 Data from Local System	**T1555** Credentials from Password Stores	**T1555.003** Credentials from Web Browsers	**T1059** Command and Scripting Interpreter
T1547 Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1204** User Execution	**T1204.001** Malicious Link
T1190 Exploit Public-Facing Application	**T1656** Impersonation	**T1055** Process Injection	**T1036** Masquerading
T1036.008 Masquerade File Type	**T1027** Obfuscated Files or Information	**T1140** Deobfuscate/Decode Files or Information	**T1560** Archive Collected Data
T1574 Hijack Execution Flow	**T1574.001** DLL	**T1497** Virtualization/Sandbox Evasion	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	F5B31BD394E0A3ADB6BD175207B8C3CCC51850C8F2CEE1149A8421736168E13E, F89298933FED52511BB78F8F377979190E37367D72CCF4F3B81374A70362CC42, BEEEA592251A0A205B3BDB34802BD2F4F5181EE38226A05EC468A86BE44E9508, 732AA8ED8CA9A12F4BFC29A693EC3EBA74ED1B2D00DE4296180D91B86D09747B, 7035B5BA24146DB537EEDB1F05E6CAD1775F9F5E81306F72422C03B288F75448, 30E26F4FD7CB0AC626950BB01E01A2C02E277727D1D3EC94286A44AF262F37CF, 2588FDFA7417D617DF2D31EDDEA710D0F964008ABC2F4860CDFF588AB9786D0A, 06D9D60DDBE835ABC5B16911A35732CC9B56EA9425DE210961A15D465823978F, 2D5E01CFACDF9F900B51B0539E0809F22CE1859EAC0886866AF35A2EB2DC2D42, 5200B27726C0BE8E6F34A3920FBD5D40AEAEC460169B1F3C7A174EBEEE6553D9,

TYPE	VALUE
SHA256	699E348260AE5B60CD822325F1C4BF2C793F6F25001357856C58520A9AF10987, D95B3EABFE9892371CB518FD6E733D2D33D2FABB2B1DF4DAB650A8F8E1EA8745, D1B712B215612C8DF5FEF02B614C616A78B723BFFBEC6E10E32BFD0B758DF41B, 39D771C12BD5DA15D3FB63905DF1E2C4C7C12B8F77C630A35B247C418950EAFE, 4BBAF3ECECD53BC4028723E87B1669268A6FADC4D480590C2D59BB4322A17DE7, B33E162A78B7B8E7DBBAB5D1572D63814077FA524067CE79C37F52441B8BD384, 0C9228983FBD928AC94C057A00D744D6BE4BD4C1B39D1465B7D955B7D35BF496, 839371CD5A5D66828AC9524182769371DEDE9606826AD7C22C3BB18FB2EE91CB, 9DAB2BADFDAE86963B2F13CE8942FE78DD66EC497F8D82DD40C0CB5BEC4FB2A7, CEE3F98B5F175219D025A92EDDEC4FD8BCAAE31E6AD99321AE7C00B822063FC3, A5BACEB97A2BE17FDD0C282292EBB0B5A56A555013A4C8FFFCC2335C504780FB, 3FBA4A0942244E9C3AD25A57A21F91B06F8732A2CA36DA948AE5F0AFA51DC72B, 557BECFCC7ECCAA5A7368A6D5583404AF26AADEDE2C345D6070E6E9FAB44A641, 1E66EBAEF295C2A32245162979D167CEBAD1FECE51B7CDB6A6C3A1D705BEFA6B
Domains	klingaimedia[.]com, klingaistudio[.]com, klingaieditor[.]com, kingaimediapro[.]com, kingaivideotext[.]com, kingaiplus[.]com
URLs	hxxps[:]//www[.]facebook[.]com/61574724896485/ hxxps[:]//www[.]facebook[.]com/61574162357787/ hxxps[:]//www[.]facebook[.]com/people/KLING-AI/61574316153107/
IPv4	185[.]149[.]232[.]197, 185[.]149[.]232[.]221, 147[.]135[.]244[.]43

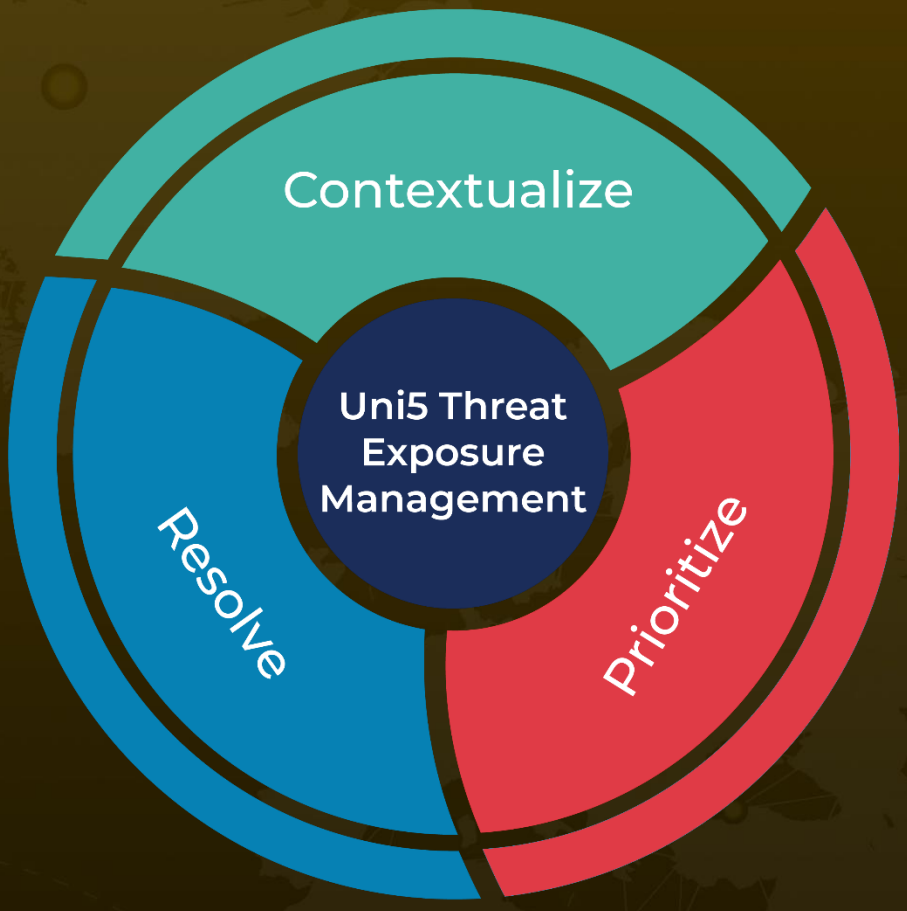
References

https://research.checkpoint.com/2025/impersonated-kling-ai-site-installs-malware/

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

May 22, 2025 • 7:50 AM

More at www.hivepro.com