Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

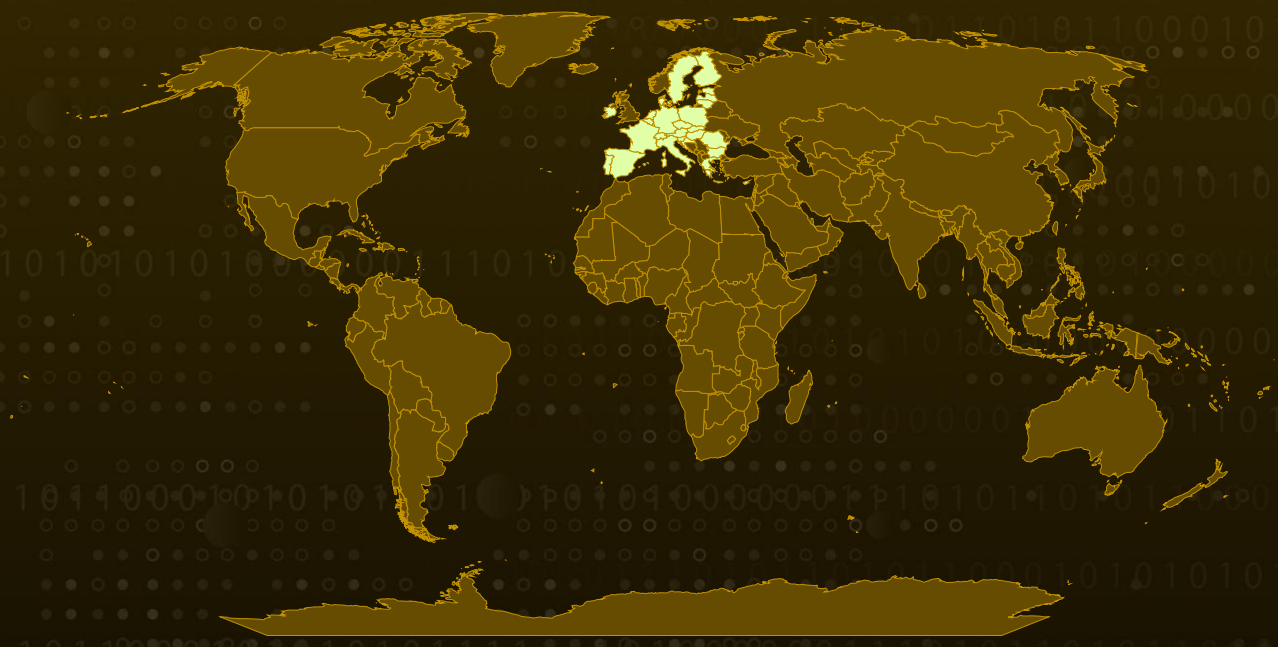
GPUGate: Weaponizing Ads and GitHub to Outsmart Sandboxes

Date of Publication	Admiralty Code	TA Number
September 9, 2025	A1	TA2025273

Summary

Attack Discovered: August 2025
Targeted Countries: European Union (EU) member countries, Western Europe
Targeted Industries: Technology and Software Development
Malware: GPUGate
Attack: GPUGate is a sophisticated malware campaign that exploits the trust users place in GitHub and Google. By planting deceptive ads at the top of search results and embedding malicious links into legitimate-looking GitHub commits, attackers trick IT professionals into downloading a convincing lookalike installer. What sets GPUGate apart is its hardware-aware design, it activates only on real machines with proper GPUs, making it nearly invisible to sandboxes and most security researchers. Once deployed, it digs deep into the system, stealing sensitive data, disabling security defenses, and preparing the ground for additional payloads, including ransomware. Uniquely, this campaign focused on entities across Western Europe, using malvertising tactics and geofencing tailored to specifically target EU countries, demonstrating a calculated and highly selective operation.

Attack Regions



Attack Details

#1 In a recent campaign threat actors are abusing GitHub's repository structure and pairing it with Google Ads, attackers successfully lured unsuspecting users onto a lookalike site that appeared indistinguishable from an official download source. At the center of this scheme was "GPUGate," a sophisticated malware strain that cleverly sidesteps traditional defenses by relying on a GPU-gated decryption routine, ensuring it only runs on real user systems rather than controlled analysis environments.

#2 A malicious Google Ad was strategically placed at the very top of legitimate search results, capitalizing on the perception that "sponsored" links are credible. To reinforce this illusion, the attackers inserted a malicious link into a real GitHub commit by editing the repository's README file. On the surface, the commit appeared authentic, but visitors who followed the link were quietly redirected to a fake domain, instead of GitHub's official release pages.

#3 Once downloaded, the executable masqueraded as a genuine GitHub Desktop installer but was anything but benign. Built on Microsoft's .NET Framework, the file was bloated in size to mirror the real installer and overwhelm sandbox environments. Inside, uncovered a "nested doll" approach: hundreds of files, including decoys and junk data, were embedded alongside malicious components designed to complicate analysis. Among them were functions resembling those in ransomware samples, and a hidden .NET module exceeding 60 MB in size, far too large and complex for most automated tools to easily dissect.

#4 What makes GPUGate stand out is its unique reliance on hardware-specific checks. Instead of triggering in any environment, the malware verifies the GPU's device name length and functionality before proceeding. Virtual machines and sandboxes, which often use generic GPU identifiers, are filtered out immediately. Only systems with proper hardware and drivers meet the criteria, allowing the malware to decrypt its payload in two distinct stages. By leveraging GPU computations for AES-CBC encryption keys, GPUGate ensures that its true capabilities remain locked away from the eyes of researchers.

#5 The campaign did not stop at stealth. GPUGate's PowerShell scripts secured persistence, tampered with Windows Defender, and downloaded additional payloads to expand its reach. Its functionality included stealing credentials, accessing sensitive local files, and even laying the groundwork for ransomware deployment. Evidence suggests the infrastructure overlaps with Atomic Stealer, a notorious infostealer linked to campaigns in Western Europe targeting IT professionals. This campaign blends malvertising, GitHub abuse, and hardware-aware evasion to target IT gatekeepers, blurring the line between malware delivery and supply chain attacks.

Recommendations

Be cautious with search ads: Avoid downloading software directly from sponsored Google Ads. Instead, type the official domain manually or bookmark trusted sites like GitHub's official release pages. Threat actors often pay for ads to place their malicious links above real results.

Verify download sources: Before installing any tool, double-check the download link. On GitHub, always use the "Releases" section of the official repository, not links hidden inside README files or commits. This simple check can stop you from pulling files hosted on fake domains.

Use layered security: Keep your antivirus and endpoint detection tools updated, but don't rely on them alone. Enable browser protections that block known phishing and malvertising sites, and use DNS filtering to catch suspicious redirects like gitpage[.]app.

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.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0010 Exfiltration	TA0011 Command and Control	TA0040 Impact	T1566 Phishing
T1566.002 Spearphishing Link	T1189 Drive-by Compromise	T1059 Command and Scripting Interpreter	T1059.001 PowerShell

T1059.005 Visual Basic	**T1053** Scheduled Task/Job	**T1053.005** Scheduled Task	**T1547** Boot or Logon Autostart Execution
T1547.009 Shortcut Modification	**T1548** Abuse Elevation Control Mechanism	**T1548.002** Bypass User Account Control	**T1562** Impair Defenses
T1562.001 Disable or Modify Tools	**T1036** Masquerading	**T1036.004** Masquerade Task or Service	**T1027** Obfuscated Files or Information
T1027.002 Software Packing	**T1140** Deobfuscate/Decode Files or Information	**T1055** Process Injection	**T1055.012** Process Hollowing
T1218 System Binary Proxy Execution	**T1218.005** Mshta	**T1564** Hide Artifacts	**T1564.001** Hidden Files and Directories
T1082 System Information Discovery	**T1518** Software Discovery	**T1518.001** Security Software Discovery	**T1083** File and Directory Discovery
T1071 Application Layer Protocol	**T1071.001** Web Protocols	**T1105** Ingress Tool Transfer	**T1573** Encrypted Channel
T1573.002 Asymmetric Cryptography	**T1008** Fallback Channels	**T1102** Web Service	**T1102.001** Dead Drop Resolver
T1555 Credentials from Password Stores	**T1555.003** Credentials from Web Browsers	**T1552** Unsecured Credentials	**T1552.001** Credentials In Files
T1005 Data from Local System	**T1115** Clipboard Data	**T1041** Exfiltration Over C2 Channel	**T1020** Automated Exfiltration
T1486 Data Encrypted for Impact	**T1489** Service Stop	**T1490** Inhibit System Recovery	**T1497** Virtualization/Sandbox Evasion

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	gitpage[.]app, fileisuwaiquw[.]icu, poiwerpolymersinc[.]online, git-freqtrade[.]com, sleeposeirer[.]online, chrome[.]browsers.it[.]com, downloadingpage[.]my, feelsifuyerza[.]com, gfweoweiou[.]online, polisywerqwe[.]xyz, largetheory[.]com, snapama[.]com, hoohle[.]xyz, ityreerrec[.]xyz, 21ow[.]icu, slepseetwork[.]online, polwique[.]blog, git-desktop[.]app
URLs	hxxps[:]//gitpage[.]app/git/mac, hxxps[:]//kololjrdtgted[.]click/zip.php
IPv4	107[.]189[.]17[.]89, 107[.]189[.]16[.]41, 107[.]189[.]25[.]128, 107[.]189[.]20[.]254, 107[.]189[.]24[.]117, 107[.]189[.]19[.]18, 104[.]194[.]134[.]4, 107[.]189[.]15[.]205, 107[.]189[.]18[.]154, 107[.]189[.]26[.]46, 107[.]189[.]27[.]207, 172[.]86[.]81[.]100, 104[.]194[.]132[.]28, 107[.]189[.]18[.]24, 45[.]59[.]125[.]245, 45[.]59[.]124[.]94, 45[.]59[.]125[.]184, 45[.]59[.]125[.]141

TYPE	VALUE
SHA256	ad07ffab86a42b4befaf7858318480a556a2e7c272604c3f1dcae0782339482e, e4d63c9aefed1b16830fdfce831f27b8e5b904c58b9172496125ba9920c7405b, 3746217c25d96bb7efe790fa78a73c6a61d4a99a8e51ae4c613efbb5be18c7b4, b13d2ecb8b7fe2db43b641c30a7ca0f8b66f4fadb92401582ac2f8cc3f21a470

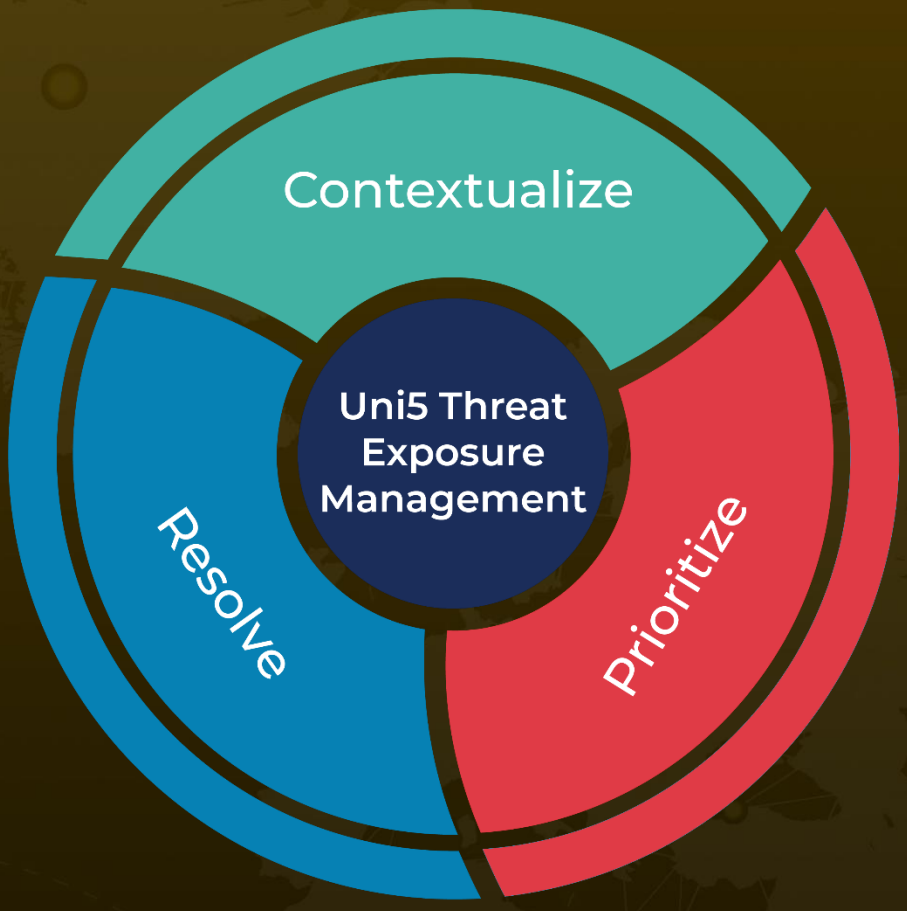
References

https://arcticwolf.com/resources/blog/gpugate-malware-malicious-github-desktop-implants-use-hardware-specific-decryption-abuse-google-ads-target-western-europe/

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

September 9, 2025 • 5:45 AM

More at www.hivepro.com