Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

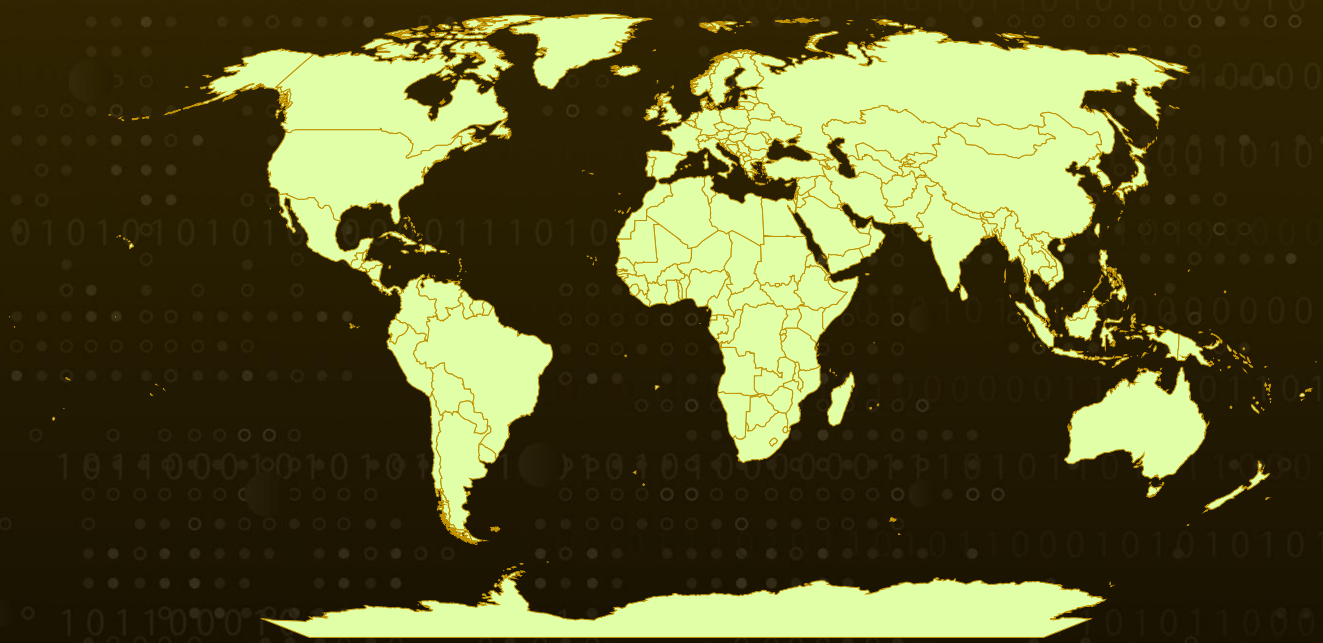
The Ghost in the Mods: How Stargazers Network is Hacking Minecraft Players

Date of Publication	Admiralty Code	TA Number
June 20, 2025	A1	TA2025196

Summary

Attack Commenced: March 2025
Targeted Countries: Worldwide
Targeted Industry: Gaming
Targeted Products: Chromium, Edge, Firefox , Steam, Discord, FileZilla, Telegram
Targeted Crypto wallets: Armory, AtomicWallet, BitcoinCore, Bytecoin, DashCore, Electrum, Ethereum, LitecoinCore, Monero, Exodus, Zcash, Jaxx
Attack: A sophisticated multi-stage malware campaign is targeting Minecraft players through a Distribution-as-a-Service (DaaS) model known as the Stargazers Ghost Network, which operates via GitHub. The campaign exploits user trust by distributing malicious Java files disguised as popular game mods, such as Oringo and Taunahi. Its ultimate goal is financial theft and data exfiltration, stealing browser data, cryptocurrency wallets, VPN credentials, and system information. All harvested information is transmitted to a Discord webhook, posing serious risks to both victims' finances and privacy.

Attack Regions



Attack Details

#1 A sophisticated cyberattack is quietly targeting the massive community of Minecraft players. This multi-stage operation cleverly uses **Stargazers Ghost Network** a "Distribution as a Service" (DaaS) platform which operates on GitHub, to spread its malicious code. It disguises itself as popular, legitimate Minecraft "Scripts & Macro" tools, think cheats or automation mods like Oringo and Taunahi. The infection begins when a player manually downloads what they believe is a new mod, a malicious JAR file, and places it into their Minecraft "mods" folder. The moment they launch the game, Minecraft automatically loads all installed mods, unknowingly activating the hidden malware.

#2 Once activated, the first stage of the attack unfolds. This initial JAR file, disguised as a Minecraft Forge mod, is a stealthy downloader. It quietly checks your system for signs of virtual machines or analysis tools, and if it finds any, it simply shuts down to stay hidden. If it passes these checks, it then reaches out to a Pastebin link to grab encrypted instructions. It decodes these instructions to find the location of the second stage of the malware, which it then loads directly into your computer's memory, leaving no trace on your hard drive.

#3 In the second stage, file named MixinLoader-v2.4.jar, is now running silently in computer's memory. This component is a dedicated thief, specifically designed to snatch valuable information related to your gaming and communication accounts. It targets your Minecraft tokens, account files from popular Minecraft launchers, and even your Discord and Telegram tokens and data. It also looks for tokens from specific cheat clients and gathers basic user details like your username and player ID. After its initial haul, this second stage then downloads and launches the third and final piece of the puzzle, while simultaneously sending the data it has collected to a hidden location via another Pastebin link.

#4 The final stage involves a potent .NET stealer. It significantly broadens the scope of what it steals, moving far beyond just gaming credentials. It's designed to raid sensitive information from your web browsers, snoop through common user folders, and target a comprehensive list of cryptocurrency wallets. Furthermore, it goes after credentials from your VPN clients, Steam, Discord, and FileZilla. This stelaer also gathers extensive information about your computer, such as what programs are running, your external IP address, the contents of your clipboard, and even takes a screenshot of your desktop.

#5 All the sensitive data collected by this final stage is then compressed into a zip file. This archive is then secretly sent to a Discord webhook. Interestingly, some of the exfiltrated data includes statistics commented in Russian, offering a potential clue about the attackers' origin. This multi-stage approach, is a classic move for financially motivated cybercriminals, showing how a seemingly small entry point, a game mod can lead to a full-scale compromise of your digital life, posing severe financial and privacy risks.

Recommendations

- **Get Strong Security Software:** Use advanced endpoint detection and response (EDR) solutions, like Check Point Threat Emulation and Harmony Endpoint , that can spot unusual behaviors and multi-stage attacks, not just known threats.
- **Be Picky About Your Software:** Only download game mods and other third-party software from official, verified sources. Be very suspicious of direct downloads from places like GitHub unless you're sure the source is trustworthy and widely recognized by security experts, not just the gaming community.
- **Turn On Two-Factor Authentication (MFA):** Enable MFA on all your important accounts gaming platforms, email, social media, banking, VPNs. This adds an extra layer of security, making stolen passwords much less useful to attackers.
- **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

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0009** Collection	**TA0010** Exfiltration
TA0011 Command and Control	**T1566** Phishing	**T1566.003** Spearphishing via Service	**T1059** Command and Scripting Interpreter
T1059.007 JavaScript	**T1656** Impersonation	**T1497** Virtualization/Sandbox Evasion	**T1567** Exfiltration Over Web Service
T1567.004 Exfiltration Over Webhook	**T1057** Process Discovery	**T1049** System Network Connections Discovery	**T1132** Data Encoding

T1027 Obfuscated Files or Information	**T1140** Deobfuscate/Decode Files or Information	**T1555** Credentials from Password Stores	**T1555.003** Credentials from Web Browsers
T1082 System Information Discovery	**T1113** Screen Capture	**T1115** Clipboard Data	**T1560** Archive Collected Data
T1588 Obtain Capabilities	**T1190** Exploit Public-Facing Application		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	05b143fd7061bdd317bd42c373c5352bec351a44fa849ded58236013126d2963, 9ca41431df9445535b96a45529fce9f9a8b7f26c08ac8989a57787462da3342f, c5936514e05e8b1327f0df393f4d311afd080e5467062151951e94bbd7519703, 9a678140ce41bdd8c02065908ee85935e8d01e2530069df42856a1d6c902bae1, 4c8a6ad89c4218507e27ad6ef4ddadb6b507020c74691d02b986a252fb5dc612, 51e423e8ab1eb49691d8500983f601989286f0552f444f342245197b74bc6fcf, 5d80105913e42efe58f4c325ac9b7c89857cc67e1dcab9d99f865a28ef084b37, 97df45c790994bbe7ac1a2cf83d42791c9d832fa21b99c867f5b329e0cc63f64, 4c944b07832d5c29e7b499d9dd17a3d71f0fd918ab68694d110cbb8523b8af49, 5590eaa4f11a6ed4351bc983e47d9dfd91245b89f3108bfd8b7f86e40d00b9fa, 7aefd6442b09e37aa287400825f81b2ff896b9733328814fb7233978b104127f, 886a694ee4be77242f501b20d37395e1a8a7a8f734f460cae269eb1309c5b196, a1dc479898f0798e40f63b9c1a7ee4649357abdc757c53d4a81448a5eea9169f, a427eeb8eed4585f2d51b62528b8b4920e72002ab62eb6fc19289ebc2fba5660,

TYPE	VALUE
SHA256	f08086257c74b1de394bf150ad8aacc99ca5de57b4baa0974bc1b59bb973d355, a1dc479898f0798e40f63b9c1a7ee4649357abdc757c53d4a81448a5eea9169f, 886a694ee4be77242f501b20d37395e1a8a7a8f734f460cae269eb1309c5b196
Domain	негры[.]рф
URLs	hxxp[:]//147[.]45[.]79[.]104/download, hxxp[:]//негры[.]рф/MixinLoader-v2.4[.]jar, hxxp[:]//185[.]95[.]159[.]125/upload, hxxps[:]//github[.]com/A1phaD3v/Oringo-Client, hxxps[:]//github[.]com/AlphaPigeonDev/Polar-Client, hxxps[:]//github[.]com/AlphaPigeonDev/Skyblock-Extras, hxxps[:]//github[.]com/P1geonD3v/Funny-Map-Extras, hxxps[:]//github[.]com/P1geonD3v/Taunahi-V3

References

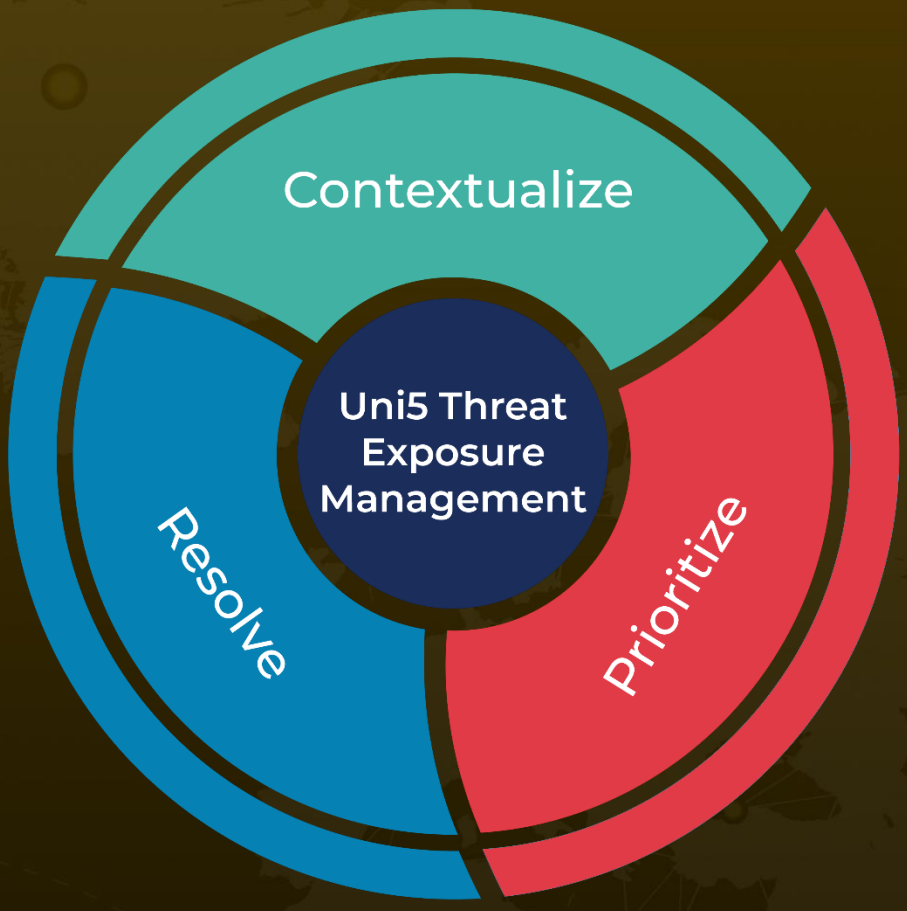
https://research.checkpoint.com/2025/minecraft-mod-malware-stargazers/#single-post

https://hivepro.com/threat-advisory/stargazers-ghost-network-3000-rogue-github-accounts-fuel-malware-spread/

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

June 20, 2025 • 5:00 AM

More at www.hivepro.com