Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

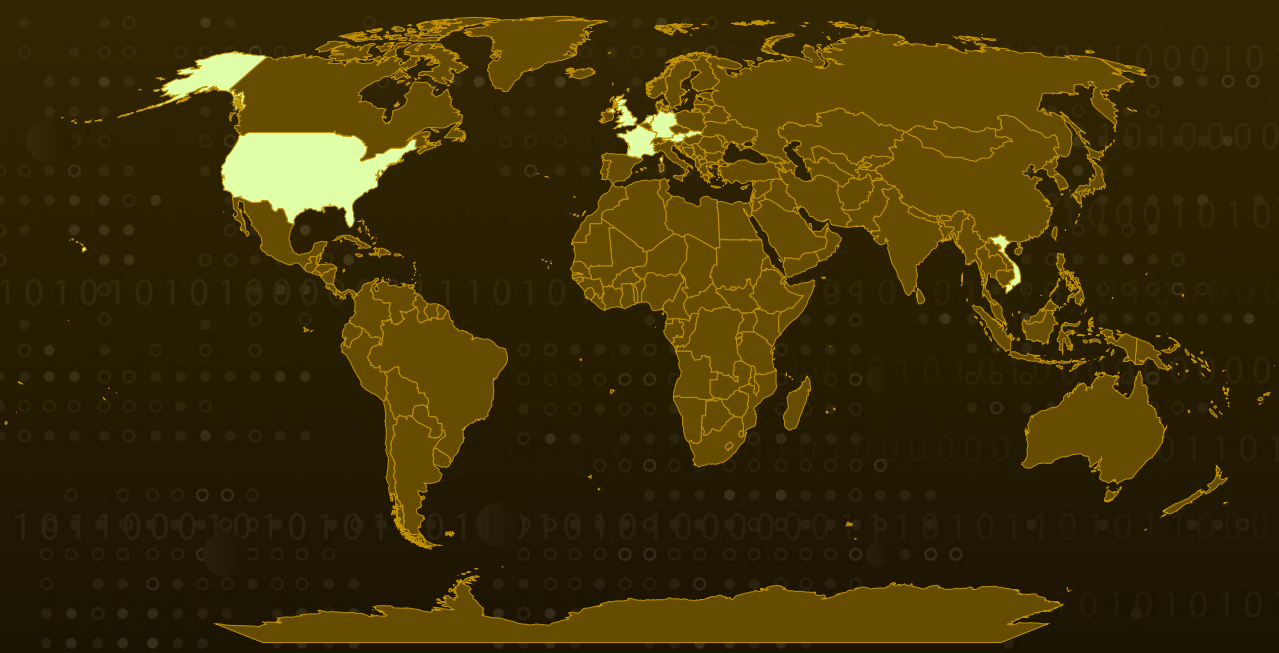
Invite Only: How Discord Links Became a Cybercrime Gateway

Date of Publication	Admiralty Code	TA Number
June 13, 2025	A1	TA2025186

Summary

Attack Discovered: 2025
Targeted Countries: United States, Vietnam, France, Germany, Slovakia, Austria, Netherlands, United Kingdom
Targeted Industry: Gaming
Affected Platform: Windows
Malware: AsyncRAT, Skuld Stealer
Attack: Cybercriminals are hijacking expired or deleted Discord invite links and turning them into traps that lead users into fake servers. Once inside, users are tricked into running a disguised “verification” that secretly installs malware. This stealthy attack downloads powerful remote access tools and info-stealers that swipe your browser passwords, Discord tokens, and even crypto wallet data all while hiding in plain sight.

Attack Regions



Attack Details

#1 Discord, once synonymous with gaming and community interaction, has increasingly become a staging ground for sophisticated cybercriminal activity. In a recent campaign, attackers are exploiting expired or deleted Discord invite links both vanity and standard to redirect unsuspecting users to malicious servers disguised as legitimate communities. These hijacked invitations are often distributed through social engineering, tricking users into believing they're joining familiar or trustworthy groups.

#2 Once a user clicks on a compromised invite, they are redirected to a fake Discord interface where a deceptive "Verify" button uses a technique called “ClickFix” to silently copy a malicious PowerShell command to their clipboard. When users paste and run this command, thinking it’s part of a routine verification step, they inadvertently kick off an infection chain. The process begins with a script download from Pastebin, which fetches a loader from GitHub. That loader retrieves encrypted payloads hosted on Bitbucket, ultimately deploying AsyncRAT for remote access and a modified version of Skuld Stealer for data theft.

#3 The infection is engineered to be stealthy and persistent. The first-stage loader sets up VBScript files for persistence and crafts exclusions to bypass Windows Defender. It also schedules a task named “checker” to ensure the malware continues to operate undetected. The second-stage executable, Rnr.exe, downloads encrypted components from Bitbucket and decrypts them using a simple XOR routine. These components are activated with a staggered schedule to avoid raising immediate suspicion.

#4 Skuld Stealer plays a crucial role in data exfiltration, targeting browser credentials, gaming sessions, Discord tokens, and cryptocurrency wallet seed phrases. It even tampers with Electron-based wallets like Exodus and Atomic by injecting malicious .asar files. Meanwhile, a memory injection tool named ChromeKatz bypasses Chrome's Application-Bound Encryption, allowing cookie theft even from modern browser versions. Exfiltrated data is compiled into a zip archive and sent to the attackers via Discord webhooks—adding another layer of obfuscation by blending malicious traffic into legitimate platform features.

#5 This infrastructure was further leveraged in a secondary campaign using a Trojanized Sims 4 cheat tool, “Sims4-Unlocker.zip,” distributed through Bitbucket and downloaded over 1,300 times. While exact victim demographics remain unknown, the presence of crypto-related data theft strongly indicates a financially motivated operation. Although Discord has disabled the malicious Safeguard bot, the threat remains active due to the attackers' use of public services like GitHub and Pastebin and the ease of recreating the attack infrastructure. This highlights the urgent need for Discord to strengthen invite link management and for users to exercise caution—even with links that seem familiar or previously safe.

Recommendations

- **Don't Trust Old or Broken Invite Links:** If a Discord invite link seems broken, expired, or unfamiliar even if it once worked don't click it again. Attackers are hijacking these links to redirect users to fake servers that look just like real ones.
- **Avoid Copy-Pasting "Verification" Commands:** Never paste or run commands from a Discord server especially if they ask you to verify your identity. If it seems strange or too technical, it's likely a trick to install malware on your device.
- **Watch Out for Suspicious Behavior After Joining a Server:** If you join a server and get instantly redirected to a fake-looking verification page, close it right away. That's a red flag. Also, be cautious if your system slows down or behaves oddly soon after.
- **Use Antivirus and Keep Everything Updated:** Make sure your device has antivirus or endpoint protection enabled. Keep your operating system, Discord client, and web browser up to date this helps block many common attack techniques.
- **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	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0010 Exfiltration
TA0011 Command and Control	T1566 Phishing	T1566.002 Spearphishing Link	T1497 Virtualization/Sandbox Evasion

T1036 Masquerading	**T1059** Command and Scripting Interpreter	**T1059.007** JavaScript	**T1059.005** Visual Basic
T1059.001 PowerShell	**T1027** Obfuscated Files or Information	**T1106** Native API	**T1140** Deobfuscate/Decode Files or Information
T1083 File and Directory Discovery	**T1056** Input Capture	**T1056.001** Keylogging	**T1113** Screen Capture
T1070 Indicator Removal	**T1070.004** File Deletion	**T1219** Remote Access Tools	**T1219.002** Remote Desktop Software
T1217 Browser Information Discovery	**T1539** Steal Web Session Cookie	**T1115** Clipboard Data	**T1082** System Information Discovery
T1048 Exfiltration Over Alternative Protocol	**T1555** Credentials from Password Stores	**T1555.001** Keychain	**T1204** User Execution
T1189 Drive-by Compromise			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	673090abada8ca47419a5dbc37c5443fe990973613981ce622f30e83683dc932, 160eda7ad14610d93f28b7dee20501028c1a9d4f5dc0437794ccfc2604807693, 5d0509f68a9b7c415a726be75a078180e3f02e59866f193b0a99eee8e39c874f, 375fa2e3e936d05131ee71c5a72d1b703e58ec00ae103bbea552c031d3bfbdbe, 53b65b7c38e3d3fca465c547a8c1acc53c8723877c6884f8c3495ff8ccc94fbe, d54fa589708546eca500fbeea44363443b86f2617c15c8f7603ff4fb05d494c1, 670be5b8c7fcd6e2920a4929fcaa380b1b0750bfa27336991a483c0c0221236a,

TYPE	VALUE
SHA256	8135f126764592be3df17200f49140bfb546ec1b2c34a153aa509465406cb46c, f08676eeb489087bc0e47bd08a3f7c4b57ef5941698bc09d30857c650763859c, db1aa52842247fc3e726b339f7f4911491836b0931c322d1d2ab218ac5a4fb08, ef8c2f3c36fff5fccad806af47ded1fd53ad3e7ae22673e28e541460ff0db49c
Domains	captchaguard[.]me, microads[.]top
URLs	hxxps[:]//captchaguard[.]me/?key=, hxxps[:]//pastebin[.]com/raw/zW0L2z2M, hxxps[:]//bitbucket[.]org/updatevak/upd/downloads, hxxps[:]//bitbucket[.]org/syscontrol6/syscontrol/downloads, hxxps[:]//bitbucket[.]org/updateservicesvar/serv/downloads, hxxps[:]//bitbucket[.]org/registryclean1/fefsed/downloads, hxxps[:]//bitbucket[.]org/htfhtthft/simshelper/downloads, hxxps[:]//github[.]com/frfs1/update/raw/refs/heads/main/installer[.]exe, hxxps[:]//github[.]com/shisuh/update/raw/refs/heads/main/installer[.]exe, hxxps[:]//github[.]com/gkwdw/wffaw/raw/refs/heads/main/installer[.]exe, hxxps[:]//bitbucket[.]org/updatevak/upd/downloads/Rnr[.]exe, hxxps[:]//bitbucket[.]org/syscontrol6/syscontrol/downloads/Rnr[.]exe, hxxps[:]//bitbucket[.]org/updatevak/upd/downloads/skul[.]exe, hxxps[:]//bitbucket[.]org/syscontrol6/syscontrol/downloads/skul[.]exe, hxxps[:]//bitbucket[.]org/updatevak/upd/downloads/AClient[.]exe, hxxps[:]//bitbucket[.]org/syscontrol6/syscontrol/downloads/AClient[.]exe, hxxps[:]//pastebin[.]com/raw/ftknPNF7, hxxps[:]//pastebin[.]com/raw/NYpQCL7y, hxxps[:]//pastebin[.]com/raw/QdseGsQL
IPv4	101[.]99[.]76[.]120, 87[.]120[.]127[.]37, 185[.]234[.]247[.]8

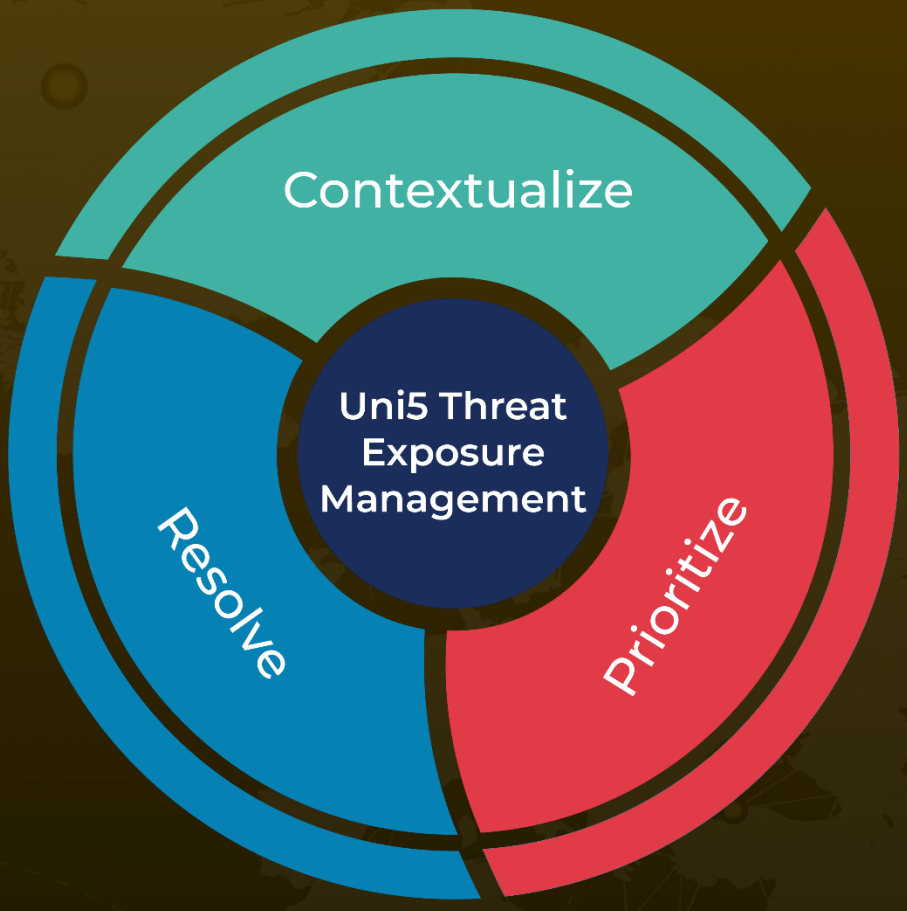
References

https://research.checkpoint.com/2025/from-trust-to-threat-hijacked-discord-invites-used-for-multi-stage-malware-delivery/

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 13, 2025 • 5:50 AM

More at www.hivepro.com