

Harvester: APT Group Expands Toolset With New GoGra Linux Backdoor

✓ security.com/threat-intelligence/harvester-new-linux-backdoor-gogra



The Harvester APT group has developed a new, highly-evasive, Linux version of its [GoGra backdoor](#). The malware uses the legitimate Microsoft Graph API and Outlook mailboxes as a covert command-and-control (C2) channel, allowing it to bypass traditional perimeter network defenses.

The Symantec and Carbon Black Threat Hunter Team linked this new Linux malware to a previously known Windows espionage campaign by Harvester due to similarities in code, demonstrating that the threat actor is actively expanding its cross-platform capabilities.

While we did not observe victims in this campaign, initial VirusTotal submissions originated from India and Afghanistan, which indicates that these regions were the primary targets of this espionage activity. Also, the use of localized decoy documents highlights a tailored approach that may be aimed at a specific regional demographic. Historically, Harvester has targeted victims in South Asia.

Harvester is believed to be a nation-state-backed group that [has been active since at least 2021](#). It is known to use both custom malware and publicly available tools in its attacks. One of its tools is a custom backdoor called Graphon, which has similarities with GoGra and also uses Microsoft infrastructure for its C2 activity.

Attack chain

The attackers use social engineering lures to gain initial access to victim networks by deploying tailored decoy documents. The attackers actively masquerade malicious ELF files as standard document files by appending extensions like “. pdf”, with a subtle space between the filename and the extension to ensure that the file still executes as a Linux binary. Depending on the specific campaign, the dropper displays either a PDF or an OpenDocument Text (ODT) file disguised as a PDF. One decoy document masqueraded as material from "Zomato Pizza". Zomato is a popular Indian food delivery service. Another was named `umrah.pdf`, referencing the Islamic pilgrimage to Mecca. Other examples of deceptive filenames used in lure documents included “TheExternalAffairesMinister. pdf” and “Details Format. pdf”.

A Go dropper is then used to embed and deploy a roughly 5.9 MB i386 executable. The malware writes its internal payload to `~/.config/systemd/user/userservice` and ensures execution upon system reboot by setting up a systemd user unit and an XDG autostart entry. This autostart entry actively masquerades as the legitimate "Conky" Linux system monitor.

Abuse of Microsoft Graph API for C2

One of the most notable features of this new backdoor is [its abuse of legitimate Microsoft cloud infrastructure](#). The inner i386 implant comes equipped with hardcoded, plaintext Azure AD application credentials, including a tenant ID, client ID, and client secret. These credentials allow the malware to request OAuth2 tokens from Microsoft.

It uses OData queries to poll a specific mailbox folder, named “Zomato Pizza”, at two-second intervals. OData (Open Data Protocol) query is the syntax used to filter, sort, and shape data when interacting with the Microsoft Graph API. Interestingly, the Windows version of the malware used a mailbox named “Dragan Dash”. [Dragan Dash Kitchen](#) is a food delivery restaurant located in the Indian city of Hyderabad.

The backdoor filters for incoming email messages with a subject line starting with the word ‘Input’. Upon receiving an email, it decrypts the base64-wrapped message body using AES-CBC encryption, and executes the payload on the host via `/bin/bash -c`.

Execution results are AES-encrypted and emailed back to the operator via a reply message using the subject line ‘Output’. Following exfiltration, the implant issues an HTTP DELETE command to wipe the original tasking message and remove evidence of its presence.

Cross-platform capabilities: Linux vs Windows variants

Analysis by our team has confirmed that this new Linux threat and a previously analyzed Windows variant of GoGra share a nearly identical underlying codebase, pointing towards a multi-platform development strategy by the Harvester threat actors.

Despite using different deployment architectures and operating systems, the underlying C2 logic remains unchanged. Analysts also identified several matching, hardcoded spelling errors across both platforms, which points towards the same developer being behind both tools.

- **Identical string typos:** Cross-platform typos include strings such as `json:"@odata.ontext"`, error occurred in decryption :, and `Commad Executed`.
- **Identical function name typos:** The function names `ExcuteCommand` and `DeleteingMessage` exhibit identical spelling errors across all builds.

Feature	Linux variant	Windows variant
Target OS architecture	Linux variant targets using an x86-64 dropper and an i386 payload	Windows variant targets using an x64 DLL
Internal Go package	OUTLOOKCLIENT/services	NEWCLIENT/services
Beacon interval	Sleeps for 2 seconds uniformly	Sleeps for 5 minutes when encountering an HTTP 204 response
Target mailbox folder	Zomato Pizza	Dragan Dash
AES encryption key	b14ca5898a4e4133bbce2ea2315a1916	b14ca5898a4e4133bbce2ea2315a1916

Conclusion

The use of a new Linux backdoor shows that Harvester is continuing to expand its toolset and actively develop new tooling in order to go after a wider range of victims and machines.

While we did not see victims in this activity, it seems clear that the group continues to retain an interest in the South Asia region for espionage purposes.

Protection/Mitigation

For the latest protection updates, please visit the [Symantec Protection Bulletin](#).

Indicators of Compromise (IOCs)

9c23c65a8a392a3fd885496a5ff2004252f1ad4388814b20e5459695280b0b82 – GoGra Linux Backdoor

2d0177a00bed31f72b48965bee34cec04cb5be8eeea66ae0bb144f77e4d439b1 – GoGra Linux Backdoor

74ac41406ce7a7aa992f68b4b3042f980027526f33ec6c8d84cb26f20495c9dc – GoGra Linux Backdoor

57cd5721bae65c29e58121b5a9b00487a83b6c37dded56052cab2a67f90ea943 –

TheExternalAffairesMinister.zip – ZIP file containing GoGra Linux Backdoor

d8d84eaba9b902045ae4fe044e9761ad0ce9051b85feea3f1cf9c80b59b2b123 – ZIP file containing GoGra Linux Backdoor

About the Author

 Threat Hunter Team

Threat Hunter Team

Symantec and Carbon Black

The Threat Hunter Team is a group of security experts within Broadcom whose mission is to investigate targeted attacks, drive enhanced protection in Symantec and Carbon Black products, and offer analysis that helps customers respond to attacks.

You might also enjoy

 [Harvester: Nation-State-Backed Group Uses New Toolset to Target Victims in South Asia](#)

[Harvester: Nation-State-Backed Group Uses New Toolset to Target Victims in South Asia](#)

- [18 Oct 2021](#)
- [4 Min Read](#)

 Graph: Growing number of threats leveraging Microsoft API

Graph: Growing number of threats leveraging Microsoft API

- [2 May 2024](#)
- [5 Min Read](#)

Cloud Cover: How Malicious Actors Are Leveraging Cloud Services

Cloud Cover: How Malicious Actors Are Leveraging Cloud Services

- [7 Aug 2024](#)
- [9 Min Read](#)