State-sponsored hackers abuse Slack API to steal airline data

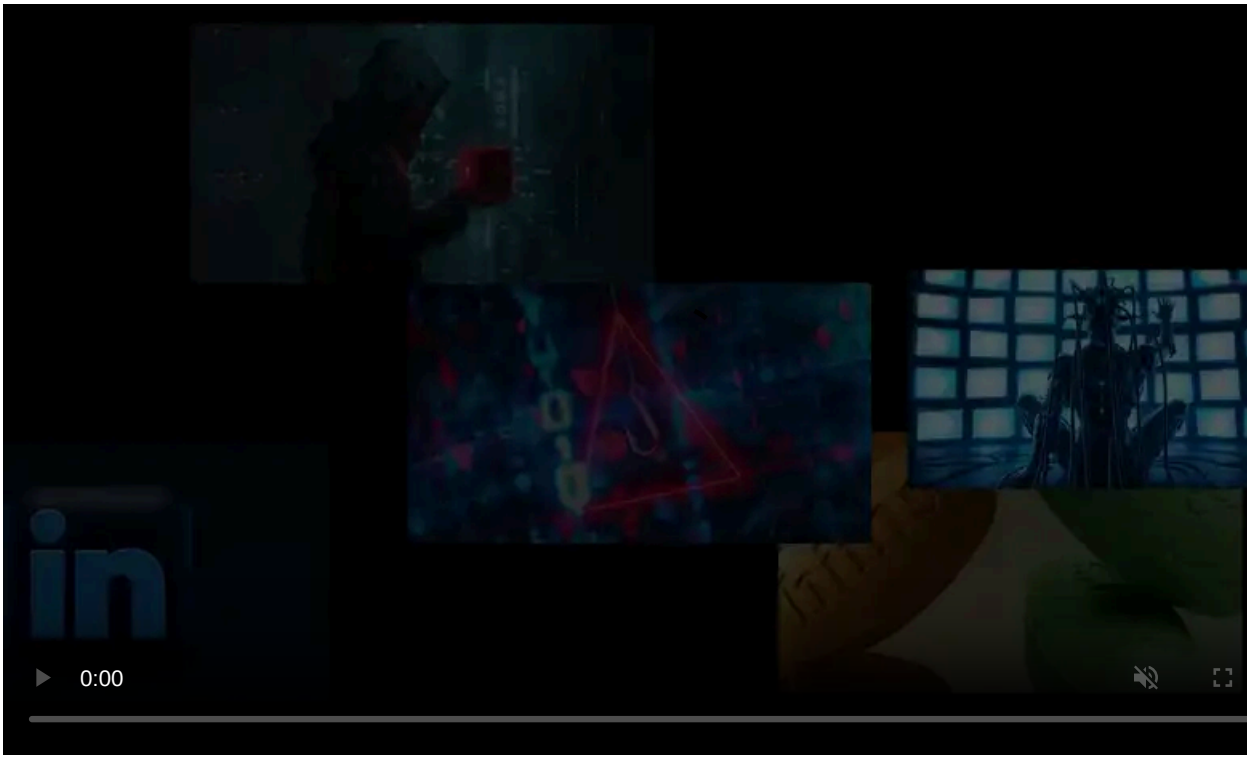
By Bill Toulas

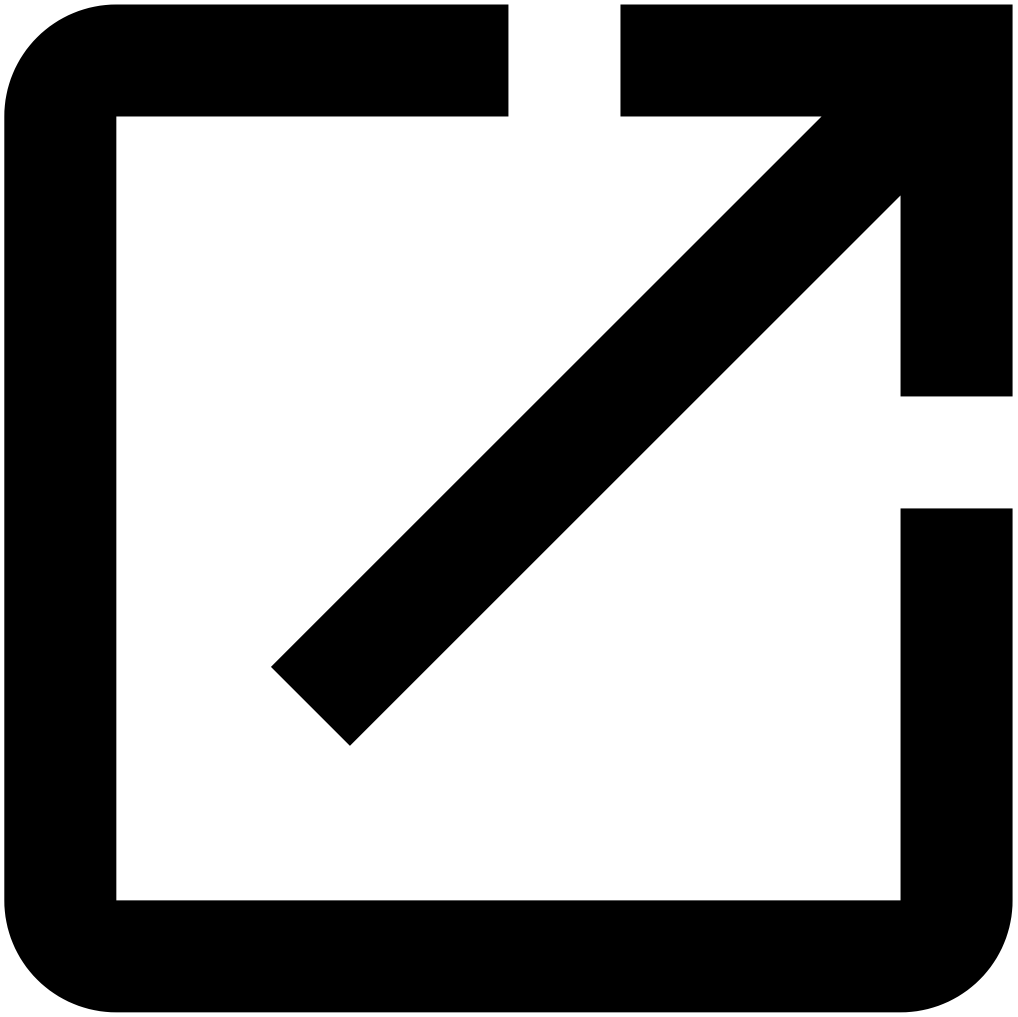
Published: 2021-12-15 · Archived: 2026-04-05 15:33:09 UTC

A suspected Iranian state-supported threat actor is deploying a newly discovered backdoor named 'Aclip' that abuses the Slack API for covert communications.

The threat actor's activity started in 2019 and targeted an unnamed Asian airline to steal flight reservation data.

According to a report by IBM Security X-Force, the threat actor is likely ITG17, aka 'MuddyWater,' a very active hacking group that maintains a targets organizations worldwide.


0:00



Abusing Slack

Slack is an ideal platform for concealing malicious communications as the data can blend well with regular business traffic due to its widespread deployment in the enterprise.

This type of abuse is a tactic that other actors have followed in the past, so it's not a new trick. Also, Slack isn't the only legitimate messaging platform to be abused for relaying data and commands covertly.

In this case, the Slack API is utilized by the Aclip backdoor to send system information, files, and screenshots to the C2, while receiving commands in return.

IBM researchers spotted the threat actors abusing this communication channel in March 2021 and responsibly disclosed it to Slack.

Slack issued the following public statement in response:

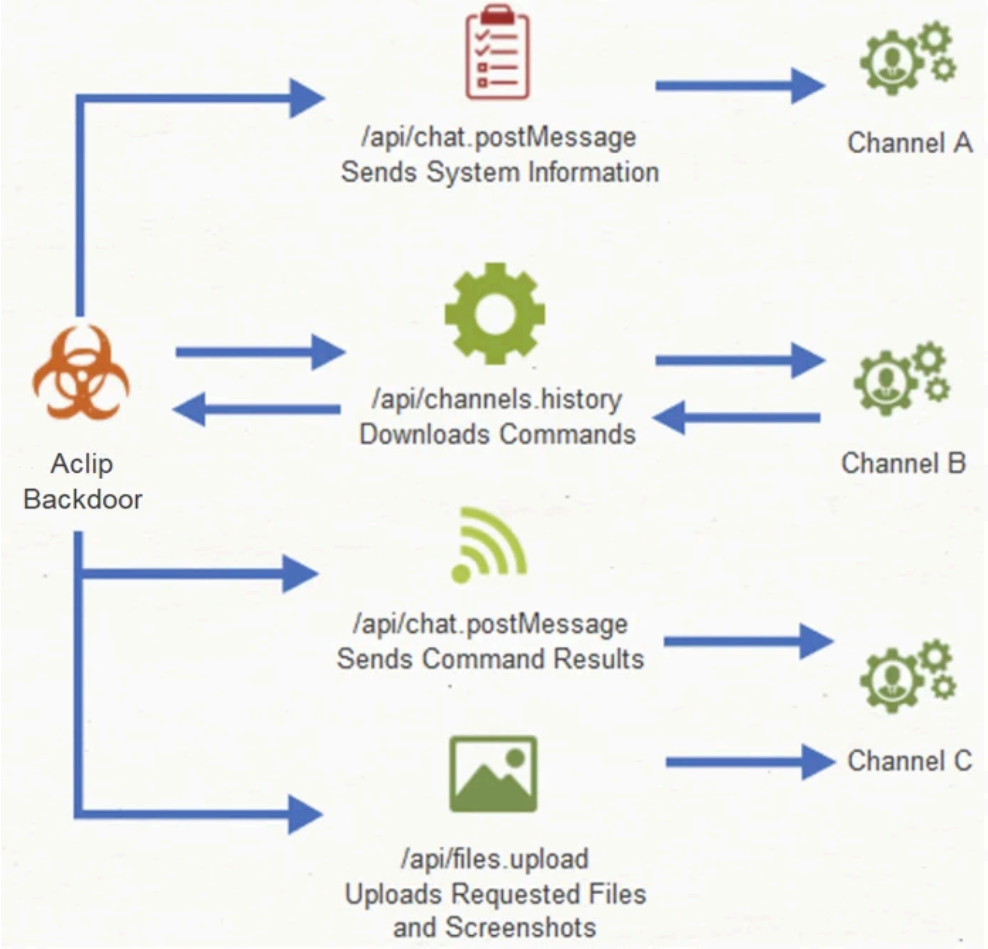
> "As detailed in this post, IBM X-Force has discovered and is actively tracking a third party that is attempting to use targeted malware leveraging free workspaces in Slack. As part of the X-Force investigation, we were made aware of free workspaces being used in this manner.
>
> We investigated and immediately shut down the reported Slack Workspaces as a violation of our terms of service. We confirmed that Slack was not compromised in any way as part of this incident, and no Slack customer data was exposed or at risk. We are committed to preventing the misuse of our platform, and we take action against anyone who violates our terms of service.
>
> Slack encourages people to be vigilant and to review and enforce basic security measures, including the use of two-factor authentication, ensuring that their computer software and anti-virus software is up to date, creating new and unique passwords for every service they use, and exercising caution when interacting with people they don't know." - Slack.

The Aclip backdoor

Aclip is a newly observed backdoor executed via a Windows batch script named 'aclip.bat,' hence the name.

The backdoor establishes persistence on an infected device by adding a registry key and launches automatically upon system startup.

Aclip receives PowerShell commands from the C2 server via Slack API functions and can be used to execute further commands, send screenshots of the active Windows desktop, and exfiltrate files.



Aclip operational diagram

Source: IBM

Upon first execution, the backdoor collects basic system information, including hostname, username, and the external IP address. This data is encrypted with Base64 and exfiltrated to the threat actor.

From then on, the command execution query phase begins, with Aclip connecting to a different channel on the actor-controlled Slack workspace.

Screenshots are taken using PowerShell's graphic library and saved to %TEMP% until exfiltration. After the images have been uploaded to the C2, they are wiped.

IBM linked the attack to MuddyWaters/ITG17 after their investigation found two custom malware samples known to be attributed to the hacking group.

"The investigation yielded two custom tools that correspond to malware previously attributed to ITG17, a backdoor 'Win32Drv.exe,' and the web shell 'OutlookTR.aspx'," explains IBM's report.

"Within the configuration of Win32Drv.exe, is the C2 IP address 46.166.176[.]210, which has previously been used to host a C2 domain associated with the Forelord DNS tunneling malware publicly attributed to MuddyWater."

How to defend

Detecting traffic that blends so well with remote collaboration tools such as Slack can be challenging, especially during a remote work boom which creates more hiding opportunities for actors.

IBM suggests focusing on strengthening your PowerShell security stance instead and proposes the following measures:

- Frequently check PowerShell logs and module logging records

- Limit PowerShell access to only specific commands and functions for each user
- Disable or restrict Windows Remote Management Service
- Create and use YARA rules to detect malicious PowerShell scripts

However, IBM warns that the abuse of messaging applications will continue to evolve as the enterprise increasingly adopts these solutions.

"With a wave of businesses shifting to a permanent or wide adoption of a remote workforce, continuing to implement messaging applications as a form of group production and chat, X-Force assesses that these applications will continue to be used by malicious actors to control and distribute malware undetected," concluded IBM.

Source: https://www.bleepingcomputer.com/news/security/state-sponsored-hackers-abuse-slack-api-to-steal-airline-data/