Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

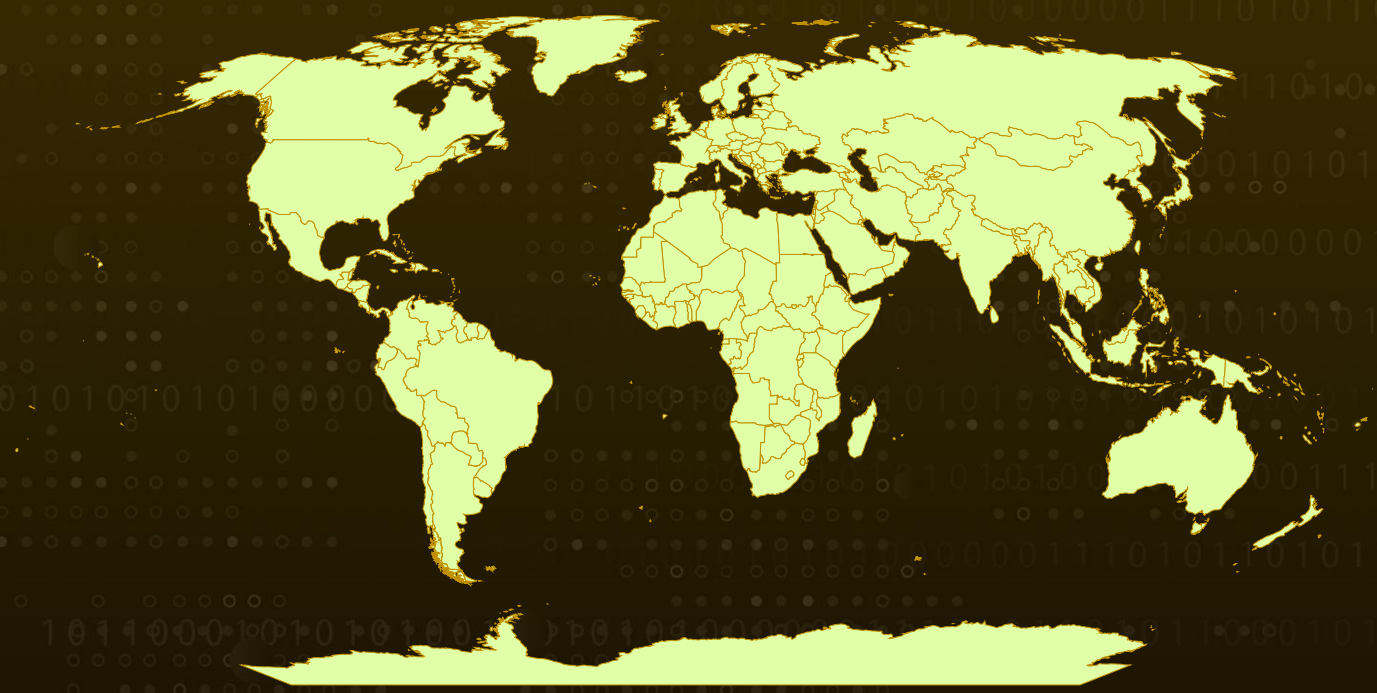
Go-Based Backdoor Exploits Telegram for Covert Command Execution

Date of Publication	Admiralty Code	TA Number
February 18, 2025	A1	TA2025045

Summary

Attack Discovered: 2025
Targeted Region: Worldwide
Attack: A newly discovered backdoor malware, written in Go, has been found using Telegram as its command-and-control (C2) channel. Although still in development, the malware is already fully functional and capable of carrying out a range of malicious activities. Its behavior suggest that the malware could be of Russian origin. It operates as a backdoor, allowing attackers to issue commands remotely via Telegram, effectively turning the messaging platform into a covert control hub.

Attack Regions



Attack Details

#1 A newly discovered Go-based backdoor malware has been identified, leveraging Telegram as its command-and-control (C2) channel. While still under development, it is already fully operational and capable of executing various malicious activities. By using Telegram for C2 communication, attackers can easily control compromised systems while blending their traffic with legitimate messaging activity. The increasing use of cloud services like OneDrive, GitHub, and Dropbox further complicates detection, as defenders struggle to differentiate between normal API usage and malicious C2 operations.

#2 When executed, the malware compiled in Golang acts as a backdoor, launching its operations through the installSelf function in the main package. This function checks whether the malware is running from a specific location C:\Windows\Temp\svchost.exe. If not, it copies itself to that directory, spawns a new process to execute the duplicate, and then terminates the original instance to evade detection.

#3 To establish C2 communication, the malware utilizes an open-source Go package for Telegram bot interactions. It initializes a bot instance using the NewBotAPIWithClient function, authenticating with a token generated via Telegram's BotFather. The malware then continuously listens for attacker-issued commands through the GetUpdatesChan function, allowing remote control via a Telegram chat.

#4 The malware supports four different commands, three of which are fully implemented. The /cmd command allows attackers to execute PowerShell commands by sending two messages one containing the command itself and another specifying the PowerShell script. The /persist command ensures the malware remains active by rechecking its location and relaunching itself if necessary. The /selfdestruct command deletes the malware's file from C:\Windows\Temp\svchost.exe, terminates its process, and sends a confirmation message to the attacker: "Self-destruct initiated."

#5 The use of Telegram and cloud-based services for C2 operations highlights a growing challenge for security teams. These platforms are widely used, easy to deploy, and difficult to distinguish from legitimate activity, making them highly attractive to cybercriminals. As these tactics evolve, defenders must prioritize monitoring suspicious API activity, strengthening endpoint security, and implementing behavioral detection strategies to identify and mitigate such threats effectively.

Recommendations

Monitor and Control Telegram API Usage: Keep a close watch on network traffic to identify any unusual activity linked to Telegram's API. Restrict the use of Telegram bots within your organization to prevent unauthorized access and potential abuse by attackers.

Enhance Endpoint Security: Utilize Endpoint Detection and Response (EDR) solutions to detect and block suspicious process executions. Implement strict controls to prevent unauthorized binaries from running in critical system directories, such as C:\Windows\Temp, to reduce the risk of malware persistence.

Strengthen PowerShell and Process Monitoring: Activate PowerShell script block logging to track and analyze executed commands for signs of suspicious activity. Continuously monitor process creation events to detect anomalies, such as unexpected PowerShell executions triggered by unknown or unauthorized processes.

Keep Systems Updated and Patched: Regularly update operating systems, security tools, and applications to protect against known vulnerabilities. Promptly apply security patches to close gaps that malware could exploit for persistence and unauthorized access.

Implement Multi Layered Security: Adopt a security strategy that can adapt to evolving threats, recognizing that attackers are continually seeking new ways to exploit existing technologies. Cloud services used for C2 communications are not limited to Telegram; other platforms like OneDrive, GitHub, and Dropbox could be similarly exploited.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0009 Collection	TA0011 Command and Control	T1083 File and Directory Discovery

T1543 Create or Modify System Process	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell	**T1070** Indicator Removal
T1113 Screen Capture	**T1190** Exploit Public-Facing Application	**T1614** System Location Discovery	**T1614.001** System Language Discovery

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	f84ca2a61f648542f970e7120de116d2

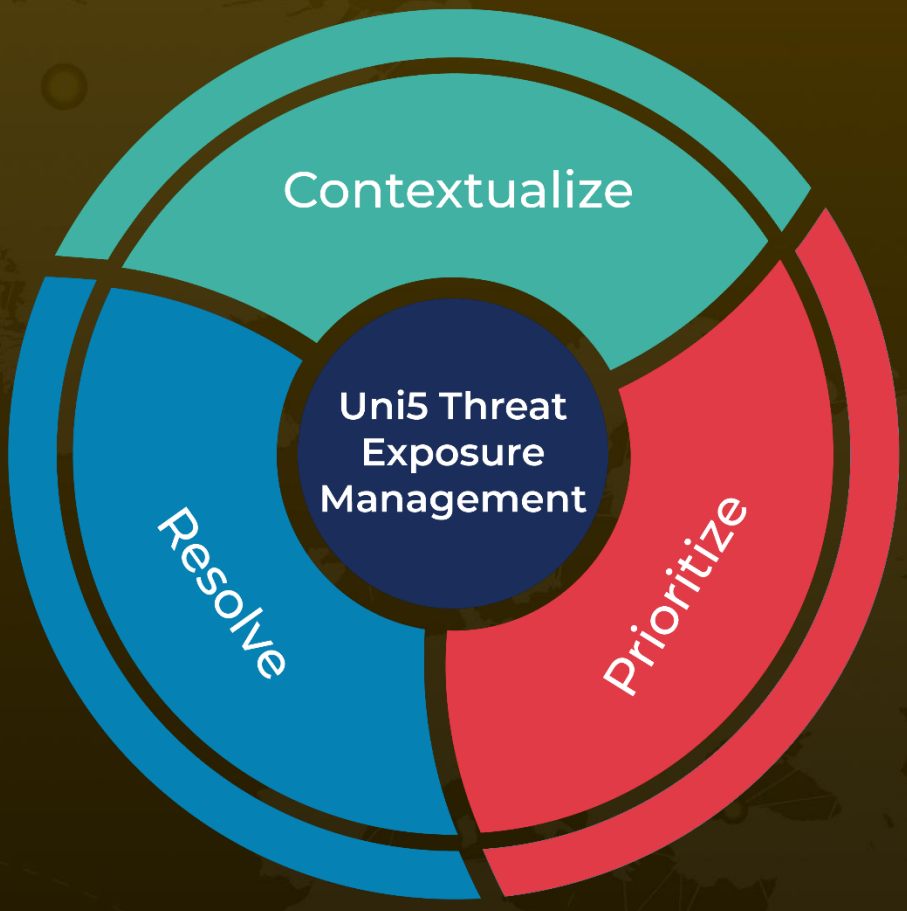
References

https://www.netskope.com/blog/telegram-abused-as-c2-channel-for-new-golang-backdoor

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

February 18, 2025 • 3:30 AM

More at www.hivepro.com