Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

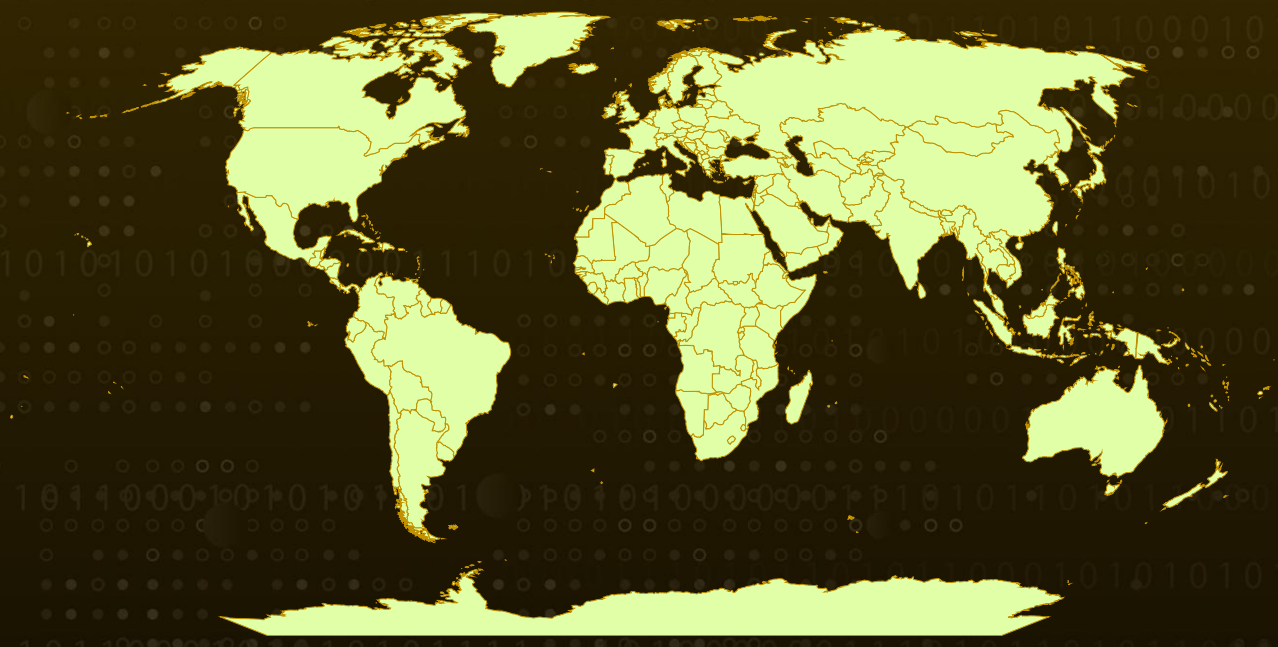
ZynorRAT: Go-Based Malware Taking Shape on Telegram

Date of Publication	Admiralty Code	TA Number
September 12, 2025	A1	TA2025279

Summary

Attack Discovered: July 2025
Targeted Countries: Worldwide
Affected Platform: Windows, Linux
Malware: ZynorRAT
Attack: ZynorRAT is a newly emerging Go-based remote access trojan that turns a simple Telegram bot into a full command-and-control hub. Still in its testing phase, the malware already packs a dangerous toolkit, from stealing files to executing arbitrary commands and planting itself in a system for persistence. The author, likely operating from Tur, has been experimenting with cloud instances and re-uploading samples to fine-tune its stealth. While not yet widely deployed, ZynorRAT shows all the hallmarks of a threat-in-the-making, one that could soon surface in underground markets as a customizable tool for attackers.

Attack Regions



Attack Details

#1 A new Remote Access Trojan known as ZynorRAT emerged in public telemetry on July 8, 2025. Built in Go and managed via a Telegram bot, the tool targets Linux systems with a Windows variant under active development. Early detection rates were inconsistent, and subsequent re-uploads suggest the author is iterating to evade scanners. Observations of chatter in Telegram channels and open-source signals indicate an evolving project that is still undergoing active refinement, rather than a polished, widely used campaign.

#2 A technical inspection of the Linux build revealed an ELF 64-bit Go binary of substantial size that preserved many symbols and human-readable artifacts, a detail that made static analysis and decompilation unusually straightforward. Mapping core routines and wrapper functions with radare2 provided clear entry points for deeper inspection, exposing the implementation of most of the RAT's capabilities. The presence of plaintext artifacts inside the binary accelerated reverse engineering and helped reconstruct the malware's behavior with confidence.

#3 At runtime, ZynorRAT turns a Telegram bot into an operator console and implements a standard RAT feature set: remote command execution, file exfiltration, system and process enumeration, screenshot capture, and persistence. Messages that fall outside its recognized command set are executed as shell input; the code prepends "bash -c" to incoming strings, effectively giving the operator the ability to run arbitrary commands on compromised hosts.

#4 For persistence on Linux, the malware abuses systemd user services by writing a service file into the user's ~/.config/systemd/user directory to survive restarts. The operator's bot shows rapid response behavior, operator-sent commands commonly return results within about a minute, and many of the hosts recorded in the bot logs appear to be cloud instances, implying test deployments on disposable infrastructure. The actor distributed executables via Dosya.co, and automated tooling helped extract a Telegram bot account along with screenshots and executed commands that corroborate active testing.

#5 Taken together, the artifacts and telemetry depict an immature but actively developed project that could be polished for broader use or offered for sale in underground markets. Repeated references to the name "Halil" and several Turkish IP addresses point toward a likely single developer or small, regionally linked operator, though some extracted IPs are likely victim systems. Defenders should prioritize runtime detection, strict outbound controls to block unauthorized Telegram bot traffic, and monitoring for unexpected systemd user service creations to blunt this tool's effectiveness while development continues.

Recommendations

- **Block unexpected Telegram bot traffic:** Don't let servers or workstations talk to Telegram bots unless you explicitly need them to. Add rules in your firewall or proxy to block outbound connections to Telegram API endpoints or known bot domains.
- **Watch for user services:** ZynorRAT installs a user-level systemd service to survive reboots. Alert on any new service files under ~/.config/systemd/user and investigate them immediately.
- **Limit permissions and use least privilege:** Don't run everyday accounts as admins. If an account is compromised, minimal permissions reduce what malware can do.
- **Harden downloads and file sharing:** Block or tightly control downloads from public file-sharing sites (e.g., Dosya.co) on critical systems. Use web filtering and scan all downloaded files in a sandbox before allowing execution.
- **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

TA0002 Execution	**TA0003** Persistence	**TA0007** Discovery	**TA0009** Collection
TA0010 Exfiltration	**TA0011** Command and Control	**T1057** Process Discovery	**T1113** Screen Capture
T1041 Exfiltration Over C2 Channel	**T1543** Create or Modify System Process	**T1543.002** Systemd Service	**T1059** Command and Scripting Interpreter
T1071 Application Layer Protocol	**T1102** Web Service	**T1102.002** Bidirectional Communication	**T1083** File and Directory Discovery

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	037e5fe028a60604523b840794d06c8f70a9c523a832a97ecaaccd9f419e364a, 47338da15a35c49bcd3989125df5b082eef64ba646bb7a2db1565bb413b69323, c890c6e6b7cc6984cd9d9061d285d814841e0b8136286e6fd943013260eb8461, 237a40e522f2f1e6c71415997766b4b23f1526e2f141d68ff334de3ff5b0c89f, 48c2a8453feea72f8d9bfb9c2731d811e7c300f3e1935bddd7188324aab7d30d, 4cd270b49c8d5c31560ef94dc0bee2c7927d6f3e77173f660e2f3106ae7131c3, a6c450f9abff8a22445ba539c21b24508dd326522df525977e14ec17e11f7d65, bceccc566fe3ae3675f7e20100f979eaf2053d9a4f3a3619a550a496a4268ef5, 8b09ba6e006718371486b3655588b438ade953beecf221af38160cbe6fedd40a, f9eb2a54e500b3ce42950fb75af30955180360c978c00d081ea561c86e54262d
Domain	api[.]telegram[.]org

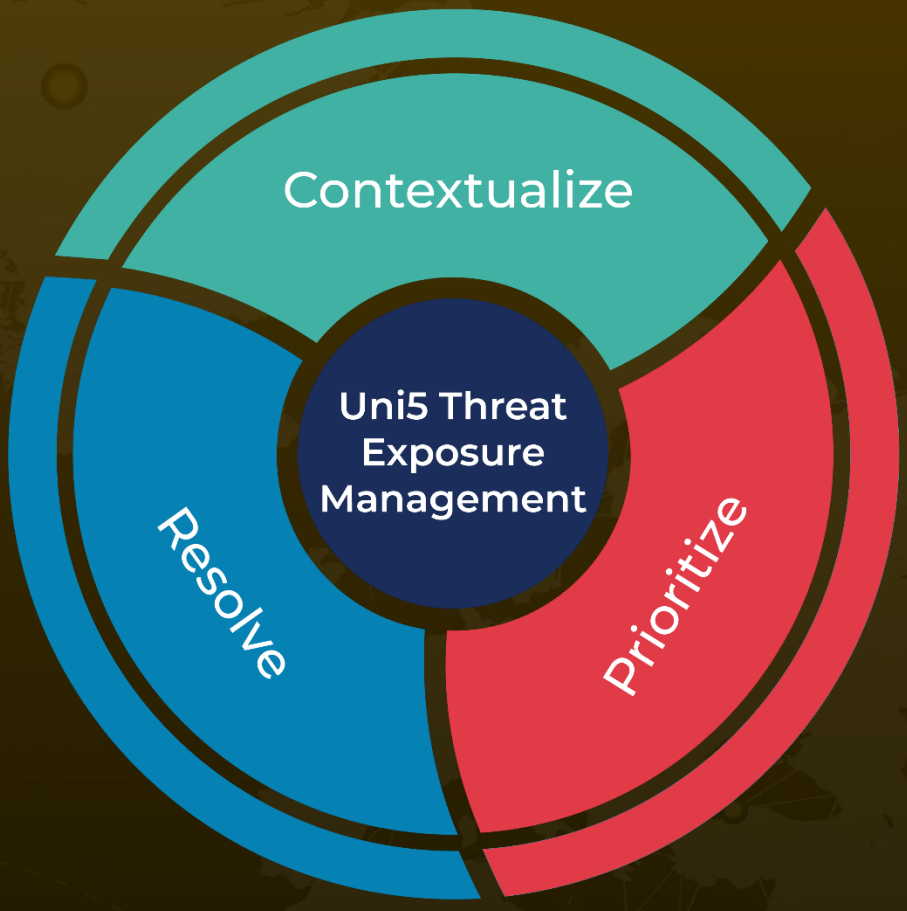
References

https://www.sysdig.com/blog/zynorrat-technical-analysis-reverse-engineering-a-novel-turkish-go-based-rat

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

September 12, 2025 • 5:30 AM

More at www.hivepro.com