Hive Pro

Threat Level

Red

HiveForce Labs

# THREAT ADVISORY

ATTACK REPORT

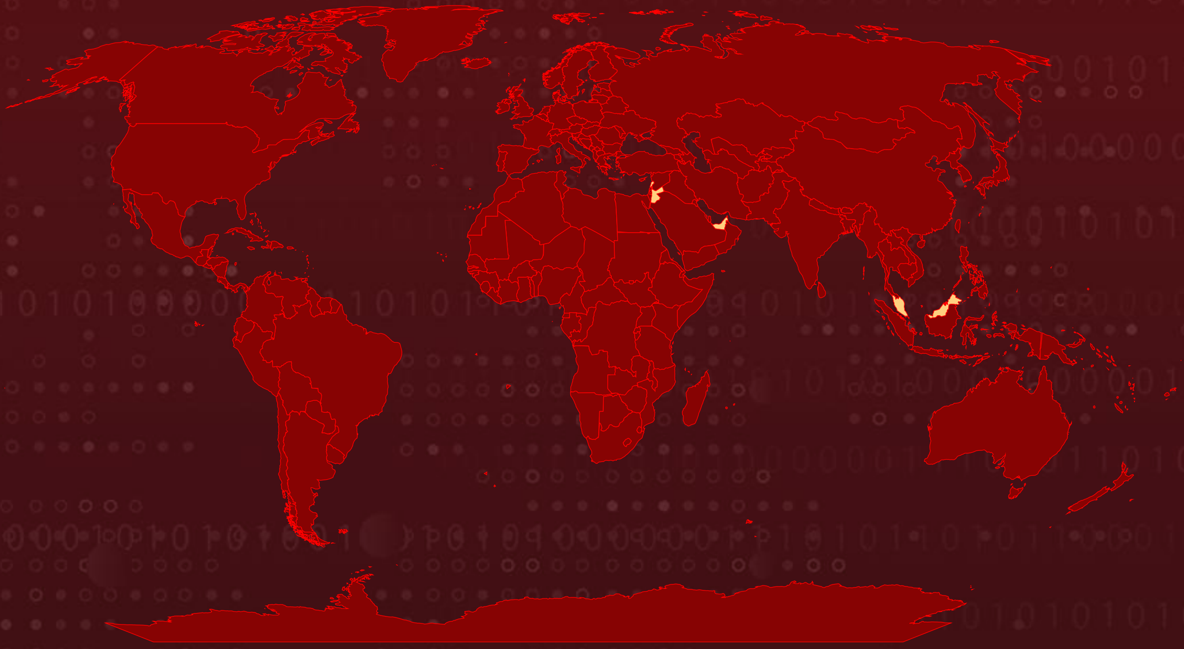
# GodRAT Reloaded: Legacy Code, Modern Tactics

| Date of Publication | Admiralty Code | TA Number |
|---|---|---|
| August 20, 2025 | A1 | TA2025254 |

# Summary

**Attack Discovered:** September 2024
**Targeted Countries:** Hong Kong, United Arab Emirates, Lebanon, Malaysia, Jordan
**Targeted Industry:** Financial Firms (trading and brokerage)
**Affected Platform:** Windows
**Malware:** GodRAT, AsyncRAT
**Attack:** The recent GodRAT campaign shows how old malware families can be repurposed with new tricks to stay dangerous. Disguised as financial documents and spread through Skype, GodRAT uses steganography to hide its code in images, loaders to inject malicious shellcode, and plugins to steal files and browser passwords. It gathers detailed system information, communicates with remote servers, and even drops additional tools like Chrome and Edge password stealers. With its roots in the Gh0st RAT family, GodRAT highlights how legacy malware can evolve into a persistent threat against industries like finance, blending stealth, modularity, and data theft into a powerful attack chain.

## Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

# Attack Details

#1

In September 2024, financial institutions were hit by a wave of malicious activity delivered through Skype messenger. Attackers disguised .scr files as financial documents, luring victims into execution. These files unleashed GodRAT, a Remote Access Trojan built on the Gh0st RAT codebase. What set this campaign apart was its creative use of steganography, hiding shellcode inside image files to bypass detection. Once triggered, the malware connected to a C2 server to retrieve additional payloads, including plugins for file management and browser password theft. The campaign remains active, with the most recent detection reported on August 12, 2025.

#2

GodRAT employed multiple loaders to inject shellcode into memory, either embedding it directly in the loader binary or extracting it from image files. One loader, decoded its shellcode with a hardcoded XOR key before injecting it into a process. Another loader extracted hidden shellcode bytes from images and executed them in new threads. Persistence was achieved by creating registry entries tied to legitimate executables, ensuring the malware could relaunch stealthily.

#3

Once activated, the shellcode searched for configuration markers like “godinfo” and decoded them using XOR operations. It then reached out to its C2 server with the request “GETGOD,” prompting the delivery of second-stage payloads such as bootstrap code, configuration files, and a UPX-packed DLL named ONLINE.dll. This RAT DLL adjusted its behavior depending on command-line arguments, appending the flag “-Puppet” for process creation and validation, a nod to its ties with the earlier AwesomePuppet RAT. From there, GodRAT collected system information, including OS details, hostnames, active processes, usernames, antivirus presence, and capture drivers, before compressing and encoding the data for exfiltration.

#4

The malware’s true power lay in its modular design. The FileManager plugin enabled attackers to control infected systems with ease, listing, deleting, and modifying files; executing applications; creating directories; and unzipping delivered archives with a portable 7zip dropped into the victim’s AppData directory. Using this capability, the attackers deployed a Chrome password stealer to harvest stored credentials and save them in “google.txt.” A similar tool targeted Microsoft Edge by pulling data directly from browser SQLite databases and decrypting saved passwords. Alongside this, additional implants such as AsyncRAT were observed, extending the attackers’ control and persistence. As modern malware continues to recycle and repurpose the code of older families while layering in new tactics, it underscores the constant evolution of the threat landscape, where legacy tools gain fresh relevance through adaptation.

# Recommendations

**Be cautious with unexpected files and links:** Avoid opening .scr files or any unusual attachments sent through messaging apps like Skype, even if they look like financial documents. Cybercriminals often disguise malware in these formats to trick users into clicking.

**Harden user accounts and passwords:** Encourage strong, unique passwords and enable multi-factor authentication (MFA) wherever possible. This makes it much harder for attackers to use stolen credentials from password stealers like those deployed in this campaign.

**Monitor for unusual activity:** Keep an eye on outbound network connections to unknown or suspicious IP addresses. GodRAT communicates regularly with its Command-and-Control servers, and this traffic can sometimes be detected as an early warning sign.

**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

| | | | |
|---|---|---|---|
| TA0001<br>Initial Access | TA0002<br>Execution | TA0003<br>Persistence | TA0004<br>Privilege Escalation |
| TA0005<br>Defense Evasion | TA0006<br>Credential Access | TA0007<br>Discovery | TA0009<br>Collection |
| TA0010<br>Exfiltration | TA0011<br>Command and Control | T1566<br>Phishing | T1566.003<br>Spearphishing via Service |
| T1027<br>Obfuscated Files or Information | T1027.003<br>Steganography | T1059<br>Command and Scripting Interpreter | T1059.003<br>Windows Command Shell |

| | | | |
|---|---|---|---|
| **T1547**<br>Boot or Logon Autostart Execution | **T1547.001**<br>Registry Run Keys / Startup Folder | **T1071**<br>Application Layer Protocol | **T1204**<br>User Execution |
| **T1204.002**<br>Malicious File | **T1071.001**<br>Web Protocols | **T1082**<br>System Information Discovery | **T1518**<br>Software Discovery |
| **T1518.001**<br>Security Software Discovery | **T1560**<br>Archive Collected Data | **T1041**<br>Exfiltration Over C2 Channel | **T1574**<br>Hijack Execution Flow |
| **T1574.001**<br>DLL | **T1083**<br>File and Directory Discovery | **T1070**<br>Indicator Removal | **T1027.002**<br>Software Packing |
| **T1555**<br>Credentials from Password Stores | **T1555.003**<br>Credentials from Web Browsers | **T1005**<br>Data from Local System | **T1105**<br>Ingress Tool Transfer |
| **T1055**<br>Process Injection | **T1036**<br>Masquerading | | |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| MD5 | cf7100bbb5ceb587f04a1f42939e24ab,<br>d09fd377d8566b9d7a5880649a0192b4,<br>e723258b75fee6fbd8095f0a2ae7e53c,<br>a6352b2c4a3e00de9e84295c8d505dad,<br>6c12ec3795b082ec8d5e294e6a5d6d01,<br>bb23d0e061a8535f4cb8c6d724839883,<br>160a80a754fd14679e5a7b5fc4aed672,<br>2750d4d40902d123a80d24f0d0acc454,<br>441b35ee7c366d4644dca741f51eb729,<br>318f5bf9894ac424fd4faf4ba857155e,<br>512778f0de31fcce281d87f00affa4a8,<br>6cad01ca86e8cd5339ff1e8fff4c8558,<br>58f54b88f2009864db7e7a5d1610d27d,<br>64dfcdd8f511f4c71d19f5a58139f2c0,<br>8008375eec7550d6d8e0eaf24389cf81,<br>04bf56c6491c5a455efea7dbf94145f1,<br>5f7087039cb42090003cc9dbb493215e, |

| TYPE | VALUE |
|---|---|
| MD5 | 31385291c01bb25d635d098f91708905,<br>cdd5c08b43238c47087a5d914d61c943,<br>605f25606bb925d61ccc47f0150db674,<br>961188d6903866496c954f03ecff2a72,<br>4ecd2cf02bdf19cdbc5507e85a32c657,<br>17e71cd415272a6469386f95366d3b64 |
| SHA256 | 18DADAC8E7591EF9BCC79B5417DF7751A3C08B204D98CEBF6FF4C54B3B5610C8,<br>0E2889F6475AEA625D18B200A2CACDAC745ECB22044F6366F21AFC2E24046025,<br>C52FB4EDDF64779B7BEDA43D26618251EEFE84BBB7F1C8EBB725E5E2DFDCFE4A,<br>D6D2A1D7993558CCEBD268A58BD008C6DC7042BC0FBC5B3FC218A961ED7A202D,<br>F26262D8E0ED5E998CED23B48A877711B655AD4CAEE0B8C68D86A0122074302A,<br>48D0D162BD408F32F8909D08B8E60A21B49DB02380A13D366802D22D4250C4E7,<br>E26EFC253A47BF311ABFF125F53F860C0CABAA58592B3407DE1380A6D3170265,<br>44EF5A168D1A929E833B55DF13DD5A79F3E8019723DFB9366855DF13B33C0BA6,<br>DA34B4041090EAFB852985866DD9FC5C435B5654A4C671A2C7F73BE2804E2C22,<br>2E33A3C604C4212547BDBB31BD842B365EF28EB7B9A84564FB8EF3C0268F6268,<br>51B7478388593F90516D04053B95DD0861D93D6195341B36272D2474D196BA86,<br>CED343EE088F8FDDAF74D3B85C0D9176A3DB852E580467CA6C60EC86BD5E2132,<br>67C713A44186315D7CBFEC4745B7DD199D86711F48C5F0778A71871AC3B02624,<br>B673444DAF876EEFF6AA81BFCD86F68FA7E5C4C48EFFF183D94EDFBB57D93EF5,<br>25A6B3369731B0F15C03944ED8103848539D25B95230CF80F809DD9352FD156E,<br>315D105619543931F1945D8298705267E48C0B19826E38627CC9FFEC7BE04F7A,<br>ED1DFD2E913E1C53D9F9AB5B418F84E0F401ABFDF8E3349E1FCFC98663DCB23F,<br>C5F5D5A9BA824E235ABD02E9D09052CA8A17B8C18253C7B25727A17DF675E66B,<br>8A1A19741DC3626CFF78E1C54DE827058060A42F3ACADDF6D5C3DEBE7071185B |

| TYPE | VALUE |
|---|---|
| File Paths | C:\users\[username]\downloads\2023-2024clientlist &.scr,<br>C:\users\[username]\downloads\2024-11-15_23.45.45 .scr,<br>C:\Users\[username]\Downloads\2024-08-01_2024-12-31Data.scr,<br>C:\Users\[username]\\Downloads\2025TopDataTransaction&.scr,<br>C:\Users\[username]\Downloads\2024-2025Top&Data.scr,<br>C:\Users\[username]\Downloads\2025TopClineData&1.scr,<br>C:\Users\[username]\Downloads\Corporate customer transaction &volume.pif,<br>C:\telegram desktop\Company self-media account application qualifications&.zip,<br>C:\Users\[username]\Downloads\个人信息资料&.pdf.pif,<br>%ALLUSERSPROFILE%\bugreport\360Safe2.exe,<br>%ALLUSERSPROFILE%\google\chrome.exe,<br>%ALLUSERSPROFILE%\google\msedge.exe,<br>%LOCALAPPDATA%\valve\valve\SDL2.dll,<br>%LOCALAPPDATA%\bugreport\LoggerCollector.dll,<br>%ALLUSERSPROFILE%\bugreport\LoggerCollector.dll,<br>%LOCALAPPDATA%\bugreport\bugreport_.exe |
| IPv4 | 103[.]237[.]92[.]191,<br>118[.]99[.]3[.]33,<br>118[.]107[.]46[.]174,<br>154[.]91[.]183[.]174,<br>156[.]241[.]134[.]49,<br>47[.]238[.]124[.]68 |
| URL | hxxps[:]//holoohg[.]oss-cn-hongkong[.]aliyuncs[.]com/HG[.]txt |
| Domain | wuwu6[.]cfd |

## References

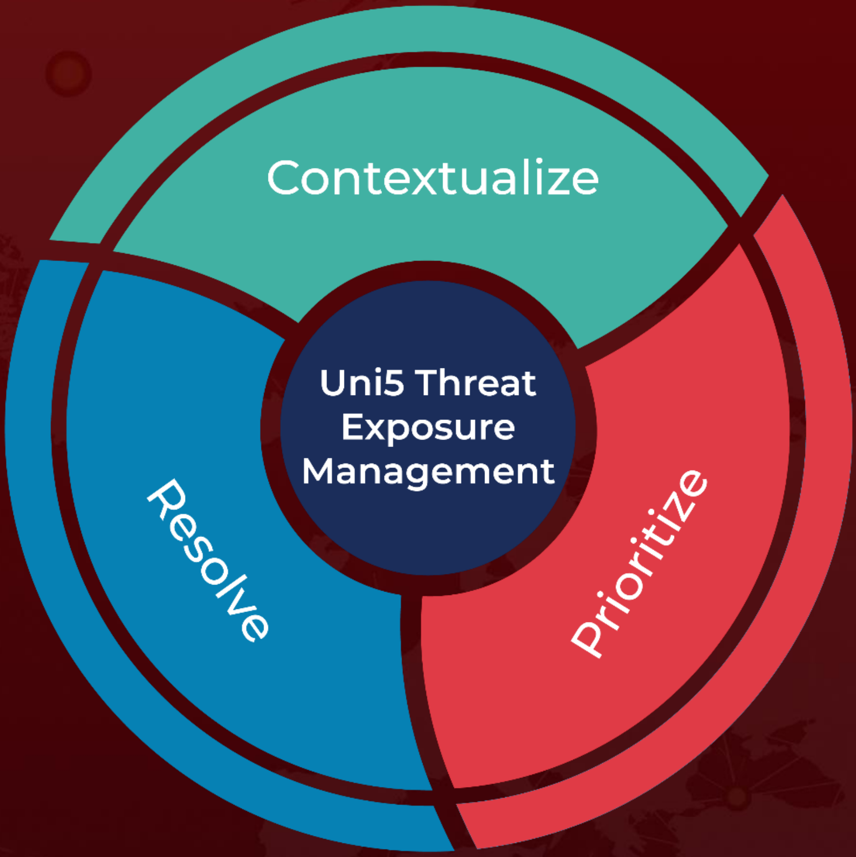
https://securelist.com/godrat/117119/

https://hivepro.com/threat-advisory/blind-eagles-banking-trap-phishing-colombias-financial-sector/

# 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

**August 20, 2025 • 5:45 AM**

More at www.hivepro.com