Hive Pro

Threat Level

Red

THREAT ADVISORY

ACTOR REPORT

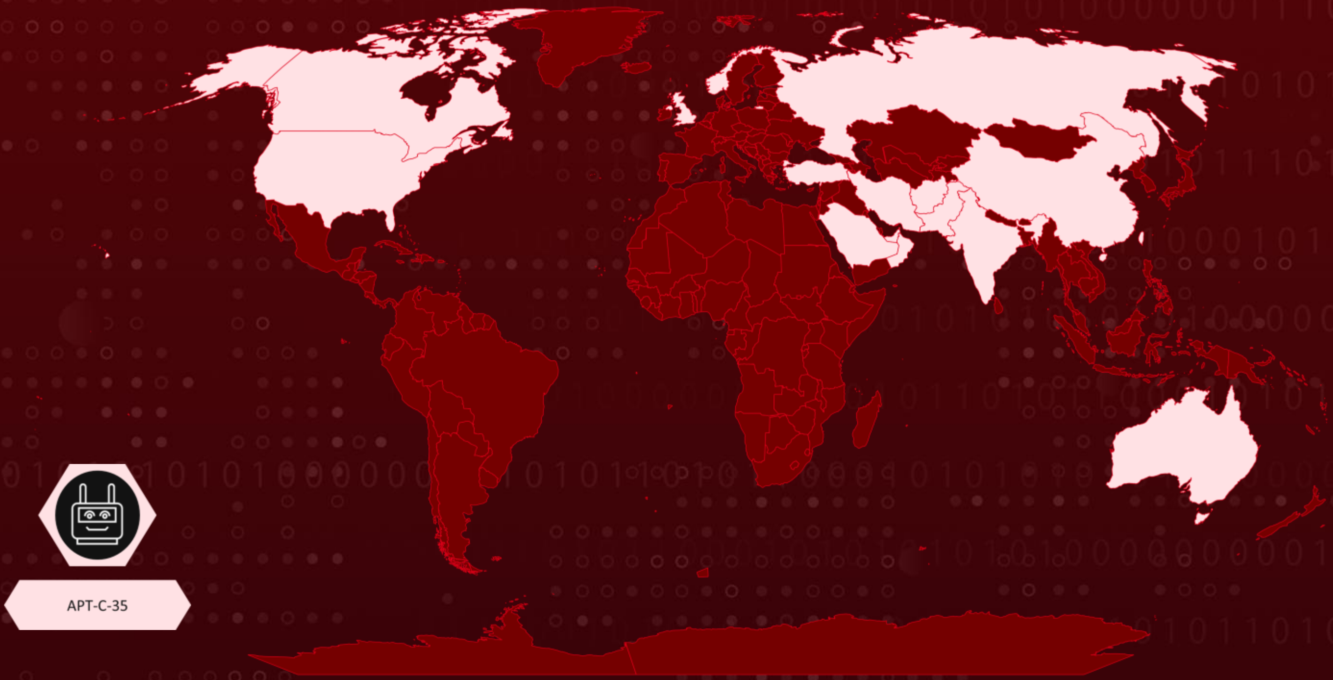
APT-C-35 infection chain adds novel Windows framework modules

Date of Publication	Admiralty code	TA Number
August 16, 2022	A1	TA2022173

Summary

APT-C-35 is an advanced persistent threat actor that has been active since 2016. The gang has upgraded its Windows spyware architecture, dubbed YTY, Jaca. They target South Asian government and military institutions, foreign ministries, and embassies.

Actor Map



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Potential MITRE ATT&CK TTPs

TA0002 Execution	**T1059** Command and Scripting Interpreter	**TA0005** Defense Evasion	**T1140** Deobfuscate/Decode Files or Information
T1221 Template Injection	**TA0004** Privilege Escalation	**T1055** Process Injection	**TA0001** Initial Access
T1195 Supply Chain Compromise	**T1566** Phishing	**T1091** Replication Through Removable Media	**TA0011** Command and Control
T1102 Web Service	**TA0003** Persistence	**T1053** Scheduled Task/Job	**T1574** Hijack Execution Flow
TA0009 Collection	**T1113** Screen Capture	**T1056** Input Capture	**T1056.001** Keylogging
T1115 Clipboard Data	**TA0010** Exfiltration	**T1020** Automated Exfiltration	

Technical Details

#1 APT-C-35s used RTF documents in their most recent spear phishing email attack. A malicious remote template is retrieved when an RTF document is opened with an HTTP GET request.

#2 When a remote template is injected and macros are enabled, the malicious code executes and calls a function that injects and invokes shellcode. The shellcode proceeds to download an encrypted blob from C2.

#3 Following that, the shellcode looks for security solutions by verifying the presence of their drivers on the victim's PC. The initial infection executes DLL, which is in charge of beaconing back to the C2 server and downloading the next component in the framework.

#4 The malware collects victims' system information using Windows Management Instrumentation (WMI). After that, the malware can encrypt the victim's data with AES-256 and beacon back to its C2 server.

Actor Detail

NAME	ORIGIN	MOTIVE	TARGET LOCATIONs	TARGET INDUSTRIES
APT-C-35 (Operation Hangover, Appin, APT-C-35, Donot, VICEROY TIGER and SectorE02)	India	Information theft and espionage	Afghanistan,Australia,Canada,China,India,Iran,Norway,Oman,Pakistan,Russia,Saudi Arabia,Singapore ,Taiwan,Turkey,United Arab Emirates,United Kingdom and United States	Financial, Government, Media, NGO, Technology, Telecommunications , Embassies and Defense.

Indicator of Compromise (IOC)

TYPE	VALUE
SHA-256	486f772d81a3b90ba76617fd5f49d9ca99dac1051a9918222cfa25117888a1d5 d566680ca3724ce242d009e5a46747c4336c0d3515ad11bede5fd9c95cf6b4ce 28c71461ac5cf56d4dd63ed4a6bc185a54f28b2ea677eee5251a5cdad07077b8 9761bae130d40280a495793fd639b2cb9d8c28ad7ac3a8f10546eb3d2fc3eefc 41c221c4f14a5f93039de577d0a76e918c915862986a8b9870df1c679469895c 2c84b325b8dc5554f216cb6a0663c8ff5d725b2f26a5e692f7b3997754c98d4d a70038cdf5aea822d3560471151ce8f8bacd259655320dea77d48ccfa5b5af4f d3a05cb5b4ae4454079e1b0a8615c449b01ad65c5c3ecf56b563b10a38ecfdef d71fa80d71b2c68c521ed22ffb21a2cff12839348af6b217d9d2156adb00e550 7fc0e9c47c02835ecbbb63e209287be215656d82b868685a61201f8212d083d9 6e7b6cc2dd3ae311061fefa151dbb07d8e8a305aed00fa591d5b1cce43b9b0de 90cb497cad8537da3c02be7e8d277d29b78b53f78d13c797a9cd1e733724cf78 93ca5ec47baeb7884c05956ff52d28afe6ac49e7aba2964e0e6f2514d7942ef8 9b2ef052657350f5c67f999947cf8cd6d06a685875c31e70d7178ffb396b5b96 80f2f4b6b1f06cf8de794a8d6be7b421ec1d4aeb71d03cccfc4b3dfd1b037993 f0c1794711f3090deb2e87d8542f7c683d45dc41e4087c99ce3dca4b28a9e6f6 5ebee134afe192cdc7fc5cc9f83b8273b6f282a6a382c709f2a21d26f532b2d3

TYPE	VALUE
Domains	worldpro[.]buzz ser.dermlogged[.]xyz doctorstrange[.]buzz clipboardgames[.]xyz beetelson[.]xyz tobaccosafe[.]xyz kotlinn[.]xyz fitnesscheck[.]xyz dayspringdesk[.]xyz srvrfontsdrive[.]xyz globalseasurfer[.]xyz esr.suppservices[.]xyz

References

https://blog.morphisec.com/apt-c-35-new-windows-framework-revealed

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

August 16, 2022 • 4:27 AM

More at www.hivepro.com