Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

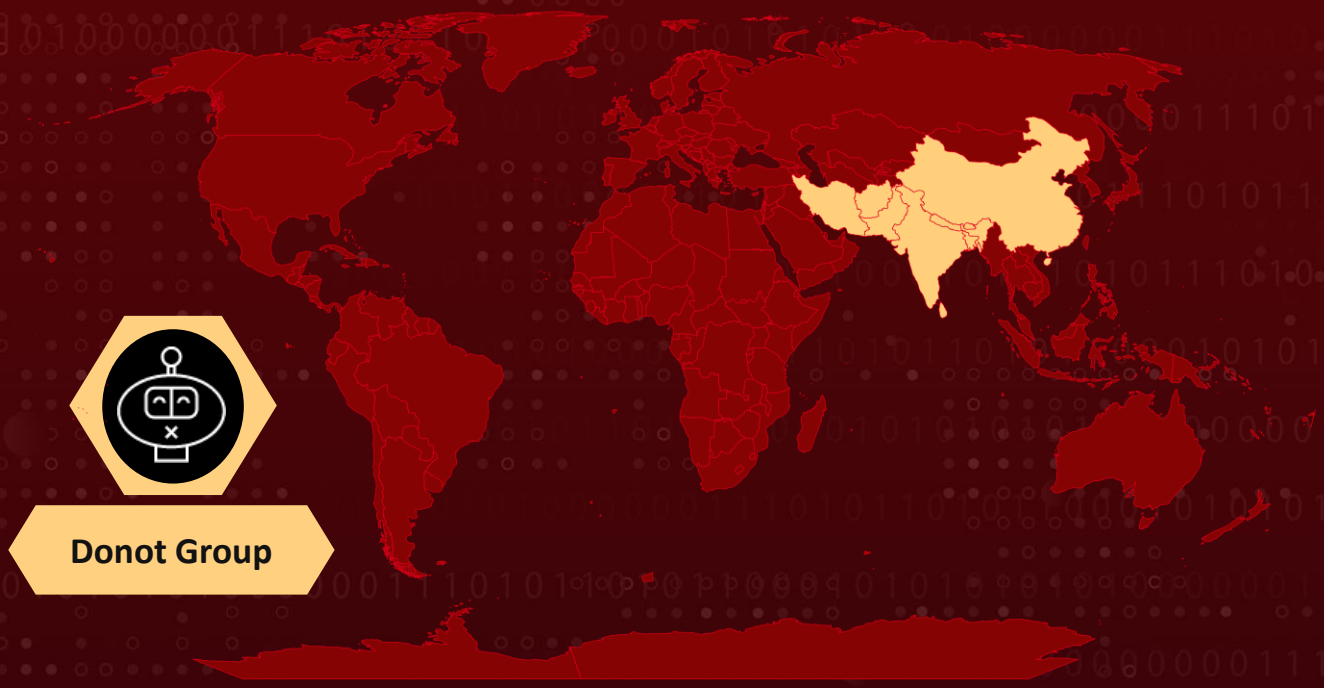
Donot APT Group Targets Government and Military Orgs in South Asia

Date of Publication	Admiralty code	TA Number
March 29, 2023	A1	TA2023164

Summary

First Appearance: 2016
Actor Name: Donot group (APT-Q-38)
Target Countries: Afghanistan, China, Bangladesh, Bhutan, India, Iran, Maldives, Nepal, Pakistan, and Sri Lanka.
Target Sectors: Government agencies, Defense military
Malware: Donot

Actor Map



Actor Details

#1 The Donot group, also known as APT-Q-38, is a state-sponsored threat actor believed to operate out of a South Asian country. They primarily engage in network espionage activities targeting government agencies, military departments, and business leaders in countries such as China, Pakistan, Sri Lanka, and other South Asian countries.

#2 Recently, the group has been observed using different methods to implant malicious DLL components, including using macro documents, self-extracting RAR archives, and EXE components. The DLL components are typically part of a three-step process that includes a downloader, plugin manager, and plugin. The group's shellcode and techniques used to execute and decrypt the code, as well as the APIs and URLs used to download and execute subsequent payloads

Actor Group

NAME	ORIGIN	TARGET COUNTRIES	TARGET INDUSTRIES
Donot Group (APT-Q-38)	South Asia	Afghanistan, China, Bangladesh, Bhutan, India, Iran, Maldives, Nepal, Pakistan, and Sri Lanka.	Government agencies, Defense military
	MOTIVE		
	Espionage and Information theft		

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actor through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0007 Discovery	TA0008 Lateral Movement
TA0011 Command and Control	TA0003 Persistence	TA0005 Defense Evasion	TA0040 Impact
TA0004 Privilege Escalation	TA0006 Credential Access	TA0009 Collection	TA0010 Exfiltration
T1059 Command and Scripting Interpreter	T1053 Scheduled Task/Job,	T1137 Office Application Startup	T1027 Obfuscated Files or Information
T1056 Input Capture	T1562 Impair Defenses	T1560 Archive Collected Data	T1113 Screen Capture
T1033 System Owner/User Discovery	T1546 Event Triggered Execution	T1574 Hijack Execution Flow	T1105 Ingress Tool Transfer
T1566 Phishing	T1070 Indicator Removal	T1204 User Execution	T1204.002 Malicious File

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	06adbb4ba31a52cc5c9258bf6d99812c d98e2d7c8e91a9d8e87abe744f6d43f9 c839d8a01c97407526b3407022823c8a 1c4fb7c41e7928bfb74784d910522771 e1d235c95a7c06b1203048972cf179fa 6de75b200652eefa4a6a3bb84da7f798 0ec8911f9764ea7b254ea19cd171535e 171c011571f94ea2f5c928bdf5d560dc 79cff3bc3cbe51e1b3fecd131b949930 dcac3a03c0c58b90cd4cbcc814d12847 e46cd1c4b32355cad39b41ef3b66b659 c231254ced08ca556bf35e587469628f 5557b32672ee9ad6be20395d447a3e52 3feb4de4375dcc3ffb4144e2fc61dd94 4c0dadc4b6938dcc9ca8951d34cb2a09 d30631ba67a28a6e4ab0c4e9584e26c2 2abc60fa1e042612e723360ccd8220c6 3c6ad03f0ab284350d8b0d3d4cf22196 07a3c19bc67c5f44c888ce75d4147ecf d7e123fe7fb8a5f56ec9d89f7787340d 20c581284cccadd8b6193c2e1c84a900 5e464d04b35a83d28c4e26c06eec28f5 9946df6c429b83009535dca8d1a5d321 ee24afbe471b5e63b06a759fa0eba0cc 7750cac1cab5e6fd9e5cadecbc3c51f6 0844b582c202dca08083d04d10bdf36e 4eaa63dd65fc699260306c743b46303b a84d7a5b8831d7494ee20b939e37e56f 3b730afd4ed953a9031a3facf111a64e cf646416025a84c5ef25b99dc999da9d
Domains	one[.]localsurfer[.]buzz orangevisitorss[.]buzz morphylogz[.]buzz crezdlack[.]buzz crushter[.]info monitoriing[.]buzz m[.]seasurfer[.]buzz bloggerboy[.]buzz sky[.]ydnmovers[.]buzz itygreyhound[.]buzz

TYPE	VALUE
Domains	balancelogs[.]buzz mayosasa[.]buzz goldliney[.]buzz briefdeal[.]buzz repidyard[.]buzz salcomp[.]buzz grapehister[.]buzz orangeholister[.]buzz blogs[.]firelive[.]pics records[.]libutires[.]info forum[.]winidowtech[.]info
URIs	hxxp://one[.]localsurfer[.]buzz/jl60UwJBkaWEkCSS/MU3gLGSnHhfDHRnwhlILSB27KZaK2doaq8s9V5M2RIgpeaD8[[.]ico|[.]png|[.]mp3|[.]mp4] hxxp://orangevisitorss[.]buzz/QcM8y7FsH12BUbxY/XNJxFhZdMSJzq1tRyF47ZXLIdqNGRqiHQQHL6DJIjl2IoxUA[[.]ico|[.]png|[.]mp3|[.]mp4] hxxp://morphylogz[.]buzz/Ik3Elidq3fc2GGig/aFwrDmHIiBWh62kZPVb4bmV0waydPv0WtgqM0QTte5iAFzF0[[.]ico|[.]png|[.]mp3|[.]mp4] hxxp://crezdlack[.]buzz/icsJOzJVtdTcGPB3/PT0w3akYLzLtd5AGs3PVEjMKJ1aO5xtfGvWbFmc4ubgXBvJO[[.]ico|[.]png|[.]mp3|[.]mp4] hxxp://crushter[.]info/m4k1doWVqrvvbjsc/AOg9AQ2SVeHsiL61tkS53q02NnMToZuOb8s5yUe8jEcBxAs0[[.]ico|[.]png|[.]mp3|[.]mp4] hxxp://monitoriing[.]buzz/3fHYKahOXhkVV3Uj/dqyWpAfXBcyQkTkzoamk25hn3cbTbeuhImfJO08uTOFCkhIa[[.]ico|[.]png|[.]mp3|[.]mp4] hxxp://m[.]seasurfer[.]buzz/33lhGEeiVe57s8gY/nmEVLghL0B5dMtBiZMAgeIVniuP4bVFETWfsZqQ2jZ1bMJYd[[.]ico|[.]png|[.]mp3|[.]mp4] hxxps://bloggerboy[.]buzz/zapterserty512wer/plekobakarester hxxps://bloggerboy[.]buzz/zapterserty512wer/xcvderioneytr hxxps://sky[.]ydnmovers[.]buzz/Kolpt523ytcserstrew/torel hxxps://sky[.]ydnmovers[.]buzz/Kolpt523ytcserstrew/meoko/P/sa hxxps://itygreyhound[.]buzz/Kolpt523ytcserstrew/torel hxxps://itygreyhound[.]buzz/Kolpt523ytcserstrew/meoko/P/sa hxxps://balancelogs[.]buzz/Kolpt523ytcserstrew/torel hxxps://balancelogs[.]buzz/Kolpt523ytcserstrew/meoko/P/sa hxxps://mayosasa[.]buzz/Testoresisty/kolimekatares hxxps://mayosasa[.]buzz/Testoresisty/bekolopexar hxxps://goldliney[.]buzz/Lomiapekaso/texadikkomanapel hxxps://goldliney[.]buzz/Lomiapekaso/ertopikana hxxps://briefdeal[.]buzz/Treolekomana/recopereta hxxps://briefdeal[.]buzz/Likorecasta/mikachar

TYPE	VALUE
URLs	hxxps://repidyard[.]buzz/Romexicarto/terokanama hxxps://repidyard[.]buzz/xoexapolicreate/ertyprmekabiops hxxps://salcomp[.]buzz/Terolekaremos/romeosata hxxps://grapehister[.]buzz/DoPstRgh512nexcvv[.]php hxxps://orangeholister[.]buzz/kolexretriya78ertdcxmega895200[.]php hxxps://blogs[.]firelive[.]pics/pooireoairoeeae/yuytetyur3544uyraif hxxps://blogs[.]firelive[.]pics/yureyuryquyey/dskjrhekjjkdhjrae hxxps://records[.]libutires[.]info/loproiaoroaspdrjro/reoriaweoprdpoi hxxps://records[.]libutires[.]info/yryerewuaoirjljrq/bcalkrhwejkarje hxxps://forum[.]winidowtech[.]info/jkdegqgegcqegog/hfogrcgegdhpgdgeq hxxps://forum[.]winidowtech[.]info/jilmvldfhqohcqhog/ntbahoghbhcghqo

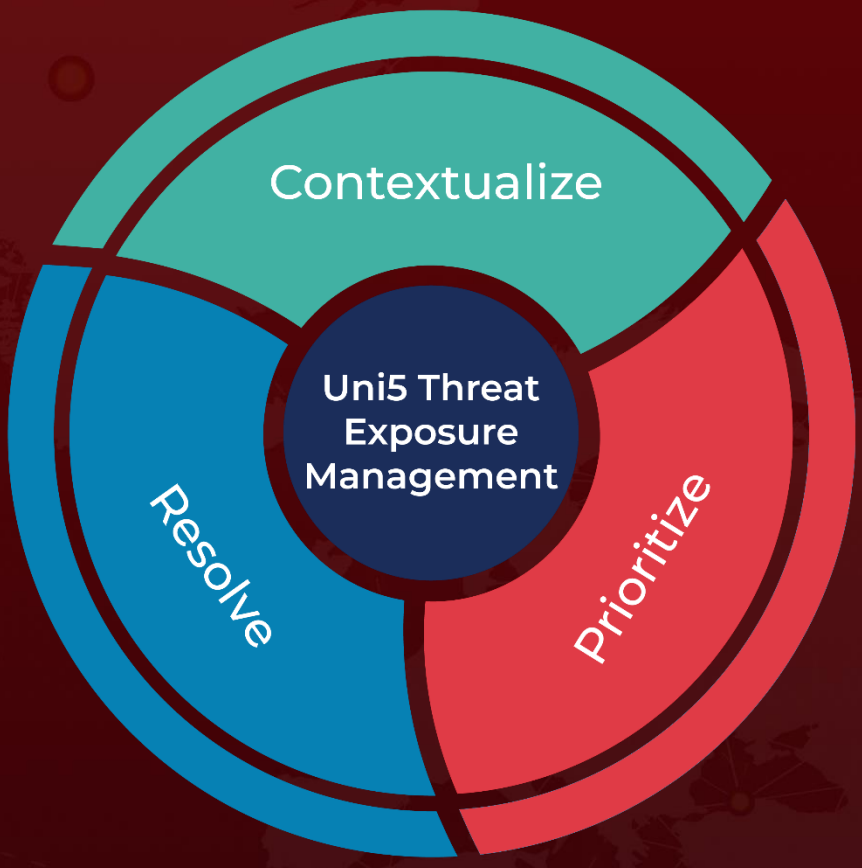
References

https://ti.qianxin.com/blog/articles/Heavy-Shadows:-Summary-of-Recent-Attack-Techniques-Used-by-Donot-Group-EN/

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

March 29, 2023 • 2:00 AM

More at www.hivepro.com