KPMG Cyber Threat Intelligence Platform

Void Rabisu – Blurring Lines between APTs & Cyber Criminals

Void Rabisu, aka Tropical Scorpious, is a threat group that has been active since 2022. Initially driven by financial motives, the group recently shifted its objectives towards cyber-espionage driven by geopolitical interests in October 2022. Previously, Rabisu deployed the Cuba Ransomware against Ukrainian targets. However, since late 2022, they have primarily been deploying the RomCom backdoor to discretely gather sensitive information. Their targets include the Parliament of Montenegro, a defense company in Europe, a bank in South America, and other entities in Ukraine, Eastern Europe, and Asia.

Initial access is through spear-phishing emails & Google Ads which redirect users to malicious websites that host trojanized MSI installers (Gimp, AstraChat, Signal, etc) of legitimate applications, embedded with RomCom malware. On execution, the installer extracts three DLLs into '%PUBLIC%\Libraries' directory that includes – loader, worker & network components. To establish persistence, it uses COM hijacking technique, by overwriting windows registry keys to load the malicious loader DLL which in-turn executes the other 2 DLLs via rundll32.exe. Network DLL then connects to the C2 server via HTTP POST requests, supporting over 40+ commands for advanced backdoor capabilities. It can collect list of installed software, steal credentials, capture screenshots, spawn CMD shell, delete files, exfiltrate data to C2 & download additional malware. To evade detection, it uses techniques including payload encryption, using signed binaries, software packing with VMProtect, & null byte padding for downloaded files.

Void Rabisu is an early indication of RaaS operators growing in sophistication & shifting their motives to resemble APT groups. Tracking such groups is becoming challenging with overlap of TTPs between those motivated by financial goals & geopolitical goals.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

The KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/TAXII/MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context. The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

Contact us:

KPMG in India Cyber Response Hotline : +91 9176 471 471

Atul Gupta
Partner, Head of Cyber Security,
KPMG in India
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner, KPMG in India
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner, KPMG in India
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner, KPMG in India
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Associate Partner,
KPMG in India
T: +91 98181 99432
E: mtembhurkar@kpmg.com

KPMG

KPMG Cyber Threat Intelligence Platform

Void Rabisu – Blurring Lines between APTs & Cyber Criminals

Indicators of Compromise: IP Addresses	
94.142.138[.]244	51.195.49[.]215

Indicators of Compromise: Domains	
dgtlocean[.]com	you-supported[.]com
gangstergo[.]com	advanced-ip-scaner[.]com
4qzm[.]com	astrachat[.]us
combinedresidency[.]org	astrachats[.]com
hexactor[.]com	chatgpt4beta[.]com
optasko[.]com	convertmypdfnow[.]net
rdpcamp[.]com	cozy-sofware[.]com
wexonlake[.]com	decropingsof[.]com

Indicators of Compromise: Hashes
ffe5e3402ec22b36607850bb7e40aae7
f77e96a9f58427d4e12121ce46b64d00
a53d5d2fc95a45bae354baaad7560b35
941962c7d370324dffefacc3feb6f320
905583246b741b01e137691953b76f64
8837fa60a4232370781492b4c688ed99
6f47723e5fc6e96ab5e9f96f6bc585fa
69072084fcad54dcdc386f6b8b591bc8
5356fc8e2ab9403dde8651f4da2ce56b
46ac4b26d35f619d8a1415b5e4365a52
36c8195e0e1ca35dc8c314959172e54c
318716a8b7616c49bf5b45345d80f6fd
29db4fd1c8ddd001a04f511ab8fa3af1
007a67bfa732084b3f8278b302bef49e
607275dd0dd4e29542ef1a2c97475379a2e37cb8
af5c5274d7b850e0b95138580f98ff1f16845905
fb73c97c17fdd5313a1a32dac5d0f226cee8f316
c9a6e240877b6bd213ff62f10a25d6699cde0f96
7b8acdcfeedc61b12d1a3b5843e442f21c844c73

KPMG

KPMG Cyber Threat Intelligence Platform

Void Rabisu – Blurring Lines between APTs & Cyber Criminals

Indicators of Compromise: Hashes
6c0864e9d6ff51f7cbf75868d32fea76c816ee1f
68619cc09efc85279945ad2ba5738361a86b1f51
5454c0a7d67d2f97d4e6fbbe99d48d8298bb58a6
50c48db4fdcb0b4d464ec5fcfee2ebd7b8405e1c
2e651c323e601dcaec9308a0b33d60172c8019b2
2b311bc4fb10a69cdba63d8486da249734cfff05
20e41885f1596a6b2b0f25c7c2c0458e0f3c0d24
04e3be2ff570eb1a479925560103af5d22961983
8d805014ceb45195be5bab07a323970a1aa8bc60cdc529712bccaf6f3103e6a6
dd65c3ad7473f211ae661ccc37f8017b9697dfffb75d415cb035399c14bc1bc9
7424de0984159e0c01da89a429e036835f253de35ec2bdade0b91db906ec54ec
a552b0b1c948e0ef4e51088f059c280a967ff40bf93ff9d62ebeb74e80f36fc5
3b26e27031a00a32f3616de5179a003951a9c92381cd8ec552d39f7285ff42ee
916153d8265a2f9344648e302c6b7b8d7e1f40f704b0df83edde43986ab68e56
e7914f823ed0763c7a03c3cfdbcf9344e1da93597733ac22fe3d31a5a4e179aa
3e293680e0f78e404fccb1ed6daa0b49d3f6ea71c81dbaa53092b7dd32e81a0d
6d3ab9e729bb03ae8ae3fcd824474c5052a165de6cb4c27334969a542c7b261d
0501d09a219131657c54dba71faf2b9d793e466f2c7fdf6b0b3c50ec5b866b2a
65778e3afc448f89680e8de9791500d21a22e2279759d8d93e2ece2bc8dae04d
2ba51d7e338242bc6a8109317b91dd13137e296693c535ceacc1288775acc81f
ff8eccca561e07a4d3b1a229b307cd1e787fe9fe21a781f361e3f01750def89c
597dd1e09bd23cd18132ce27a731d0b66c78381e90292ece0f23738773743a7c