KPMG Cyber Threat Intelligence Platform

Cloud Atlas – The Emergence of VBCloud Malware

TLP : Clear

KPMG. Make the Difference.

Cloud Atlas, also known as Clean Ursa, Inception, Oxygen, and Red October, is an unattributed threat activity cluster that has been active since 2014. In 2024, it used a new, undocumented backdoor called VBCloud, for enhanced data collection and exfiltration tasks while maintaining stealth. The group's recent campaigns have targeted several sectors in countries such as Russia, Belarus, Canada, Moldova, Israel, Kyrgyzstan, Turkey, and Vietnam with more than 80% of the targets located in Russia.

Cloud Atlas initiates the attack by sending a phishing email containing a malicious RTF document, which when opened by the user, downloads a malicious template. The malicious RTF template exploits a vulnerability to download and execute an HTA file hosted on the attacker's server. The HTA file leverages alternate data streams to extract and create files in %APPDATA%\Roaming\Microsoft\Windows\, constituting the VBShower backdoor. The backdoor performs operations such as reading and decrypting data files, cleaning downloaded malicious documents, and ensuring the autorun registry key is present. VBShower then proceeds to download and install the PowerShower backdoor, which probes the local network to facilitate further infiltration. The backdoors also download scripts which unpack files into the %ALLUSERPROFILE% directory and create scheduled tasks to execute VBCloud scripts. VBCloud checks the availability of the WebDAV server, creates files to confirm script activity, and downloads payloads for execution. The backdoor also searches for specific file types, collects them into ZIP archives, and uploads these archives to cloud storage before deleting them from the system.

Cloud Atlas's use of vulnerability exploitation, and multi-staged backdoors underscore the importance of implementing advanced detection systems and adopting proactive threat mitigation to defend against such sophisticated campaigns.

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.

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

KPMG in India Cyber Response Hotline: 1800 2020 502

KPMG in India contacts:

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

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

Sony Anthony
Partner
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Partner
T: +91 98181 99432
E: mtembhurkar@kpmg.com

Rishabh Dangwal
Director
T: +91 99994 30277
E: rishabhd@kpmg.com

kpmg.com/in

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Cloud Atlas – The Emergence of VBCloud Malware

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Domains	
riamir[.]net	onesoftware[.]info
yandesks[.]net	control-issue[.]net
yandisk[.]info	office-confirm[.]com
gosportal[.]net	triger-working[.]com
net-plugin[.]org	content-protect[.]net
web-privacy[.]net	serverop-parametrs[.]com
web-wathapp[.]com	

Indicators of Compromise: Hashes
9d3557cc5c444fe5d73e4c7fe1872414
cba05e11cb9d1d71f0fa70ecd1af2480
cbfb691e95ee34a324f94ed1ff91bc23
2d24044c0a5b9ebe4e01ded2bfc2b3a4
88be01f8c4a9f335d33fa7c384ca4666
a30319545fda9e2da0532746c09130eb
15fd46ac775a30b1963281a037a771b1
31b01387ca60a1771349653a3c6ad8ca
389bc3b9417d893f3324221141edea00
aa8da99d5623fafed356a14e59acbb90
016b6a035b44c1ad10d070abcdfe2f66
160a65e830eb97aae6e1305019213558
184cf8660af7538cd1cd2559a10b6622
1af1f9434e4623b7046cf6360e0a520e
1bfb9cba8aa23a401925d356b2f6e7ed
21585d5881cc11ed1f615fdb2d7acc11

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Cloud Atlas – The Emergence of VBCloud Malware

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
242e86e658fe6ab6e4c81b68162b3001
2fe7e75bc599b1c68b87cf2a3e7aa51f
36dd0fbd19899f0b23ade5a1de3c2fec
389f6e6fd9dcc84c6e944dc387087a56
3a54acd967dd104522ba7d66f4d86544
3f12bf4a8d82654861b5b5993c012bfa
49f8ed13a8a13799a34cc999b195bf16
4b96dc735b622a94d3c74c0be9858853
f45008bf1889a8655d32a0eb93b8acdd
0139f32a523d453bc338a67ca45c224d
01db58a1d0ec85adc13290a6290ad9d6
6fcee9878216019c8dfa887075c5e68e
d445d443ace329fb244edc3e5146313b
f3f28018fb5108b516d802a038f90bde
0f37e1298e4c82098dc9318c7e65f9d2
93bb6307a5dde45d92c8bdc7279d6ff63be8c541
b2769bc8a25ee6b65e58b6f2795316d67771c54b9a423bf02c3779d63b08bc4a