Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

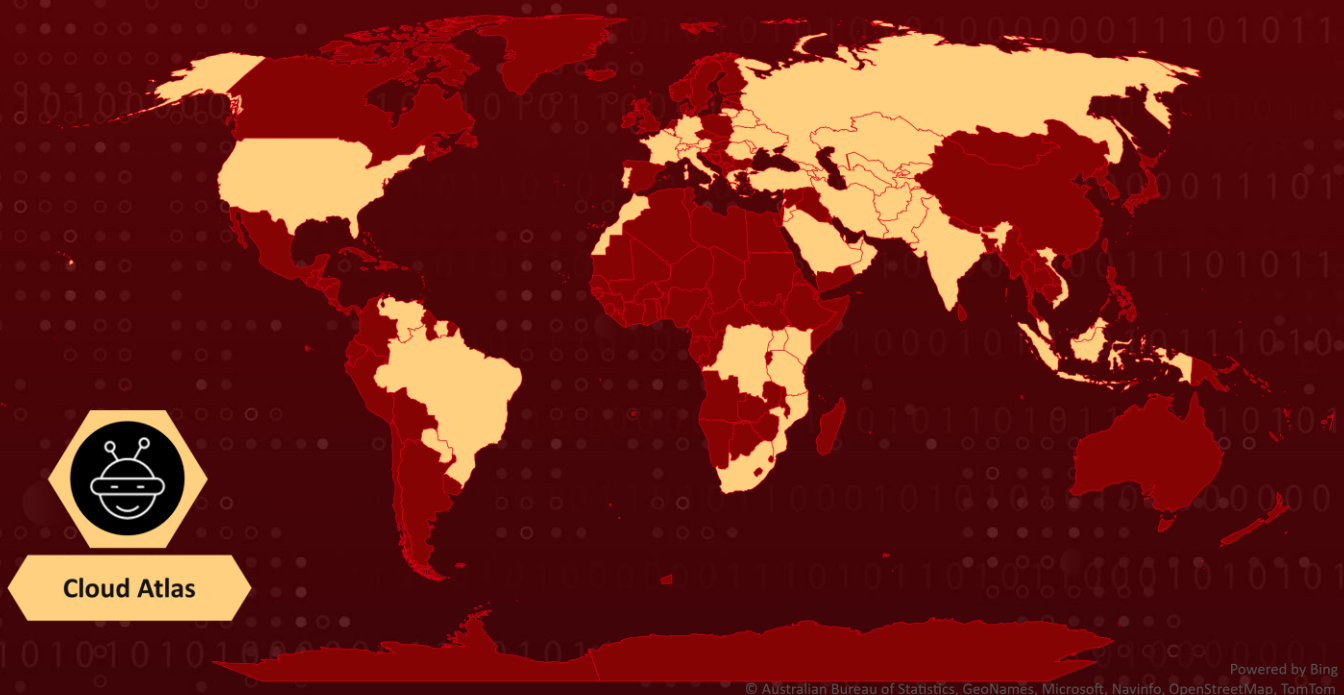
The Cloud Atlas Perpetual Threat aims to persuade entities in Russia

Date of Publication	Admiralty code	TA Number
December 13, 2022	A1	TA2022296

Summary

First Appearance: 2014
Actor Name: Cloud Atlas
Target Region: Afghanistan, Armenia, Austria, Azerbaijan, Belarus, Belgium, Brazil, Congo, Cyprus, France, Georgia, Germany, Greece, India, Indonesia, Iran, Italy, Jordan, Kazakhstan, Kenya, Kyrgyzstan, Lebanon, Lithuania, Malaysia, Moldova, Morocco, Mozambique, Oman, Pakistan, Paraguay, Portugal, Qatar, Romania, Russia, Saudi Arabia, Slovenia, South Africa, Suriname, Switzerland, Tajikistan, Tanzania, Turkey, Turkmenistan, Uganda, Ukraine, UAE, USA, Uzbekistan, Venezuela, Vietnam.
Target Sectors: Aerospace, Defense, Embassies, Energy, Engineering, Financial, Government, Oil and gas, Research.

Actor Map



CVE

CVE	NAME	PATCH
CVE-2017-11882	Microsoft Office Memory Corruption Vulnerability	✓
CVE-2018-0802	Microsoft Office Memory Corruption Vulnerability	✓

Actor Details

#1

Cloud Atlas is a cyberespionage gang. They have launched repeated, highly focused attacks on critical infrastructure spanning geographical zones and political disputes since their discovery in 2014. As their initial attack vector, Cloud Atlas has employed spear-phishing emails with malicious attachments, which are typically Microsoft Office documents that retrieve the malicious remote template from the attackers' servers.

#2

The remote templates are RTF documents that attack 5-year-old Microsoft Equation Editor vulnerabilities such as CVE-2017-11882 and CVE-2018-0802. The next stage of a Cloud Atlas intrusion is typically a PowerShell-based backdoor called PowerShower, which is placed on disk via simple Base64-encoding and string concatenation obfuscation. It makes use of the proxy when sending requests to the C&C server.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Cloud Atlas (Inception Framework, Oxygen, ATK 116 , The Rocra)	Russia **MOTIVE** Information theft and Espionage	Afghanistan,Armenia,Austria,Azerbaijan,Belarus,Belgium,Brazil,Congo,Cyprus,France,Georgia,Germany,Greece,India,Indonesia,Iran,Italy,Jordan,Kazakhstan,Kenya,Kyrgyzstan,Lebanon,Lithuania,Malaysia,Moldova,Morocco,Mozambique,Oman,Pakistan,Paraguay,Portugal,Qatar,Romania,Russia,SaudiArabia,Slovenia,SouthAfrica,Suriname,Switzerland,Tajikistan,Tanzania,Turkey,Turkmenistan,Uganda,Ukraine,UAE,USA,Uzbekistan,Venezuela,Vietnam	Aerospace,Defense,Embassies,Energy,Engineering,Financial,Government,Oilandgas,Research.

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

TA0001 Initial Access	**TA0002** Execution	**TA0005** Defense Evasion	**TA0008** Lateral Movement
TA0011 Command and Control	**T1566** Phishing	**T1203** Exploitation for Client Execution	**T1204** User Execution
T1090 Proxy	**T1140** Deobfuscate/Decode Files or Information	**T1021** Remote Services	**T1102** Web Service

Indicator of Compromise (IOC)

TYPE	VALUE
MD5	a34d585f66fc4582ed709298d00339a9 b1aad1ed2925c47f848f9c86a4f35256 f58ad9ee5d052cb9532830f59ecb5b84 57c44757d7a43d3bc9e64ec5c5e5515d 41d2627522794e9ec227d72f842edaf7 f95ceca752d219dbc251cca4cd723eae 044e167af277ca0d809ce4289121a7b5 1139c39dda645f4c7b06b662083a0b9d 3399deafaa6b91e8c19d767935ae0908 bd9907dd708608bd82bf445f8c9c06ab edc96c980bbc85d83dcd4dca49ca613f ee671a205b0204fa1a6b4e31c9539771 5488781d71b447431a025bd21b098c2c 16fbbafa294d1f4c6c043d89138d1b60 5bbc3730c943b89673453176979d6811 b684f3ee5a316e7fbcfa95ebcf86dedc
Domains	desktoppreview[.]com gettemplate[.]org driversolution[.]net translate-news[.]net technology-requests[.]net protocol-list[.]com comparelicense[.]com support-app[.]net remote-convert[.]com
IP Address	146.70.88[.]123 185.227.82[.]21

Patch Link

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-11882

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2018-0802

References

https://research.checkpoint.com/2022/cloud-atlas-targets-entities-in-russia-and-belarus-amid-the-ongoing-war-in-ukraine/

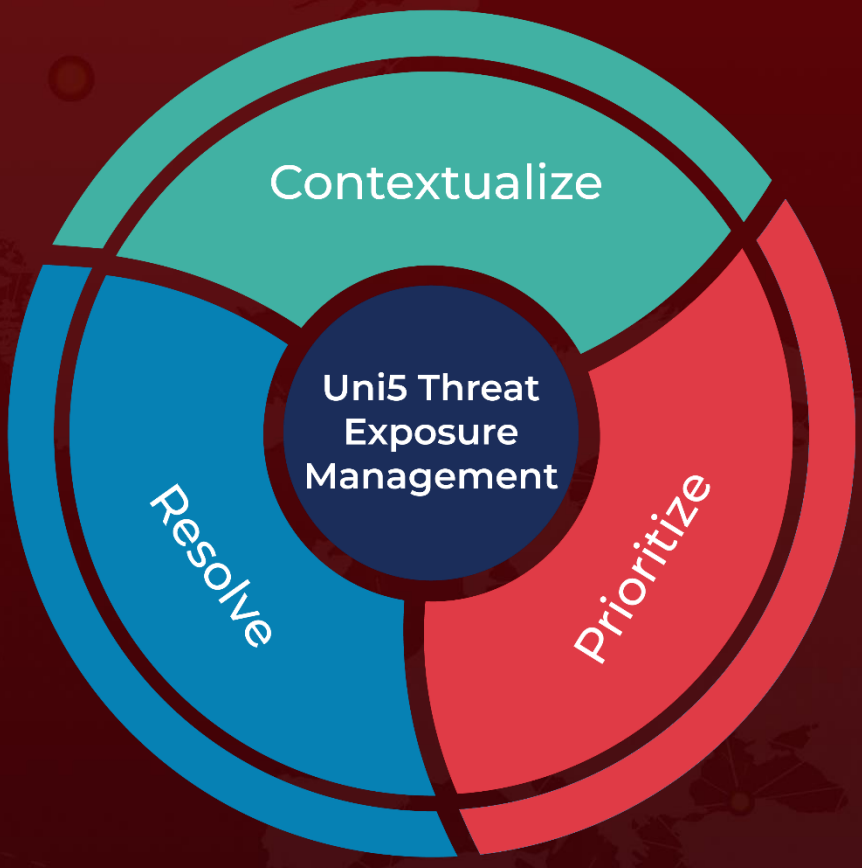
https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/apt-cloud-atlas-unbroken-threat/

https://attack.mitre.org/groups/G0100/

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

December 13, 2022 • 5:00 AM

More at www.hivepro.com