Hive Pro®

Threat Level

Red

HiveForce Labs

# THREAT ADVISORY

## ATTACK REPORT

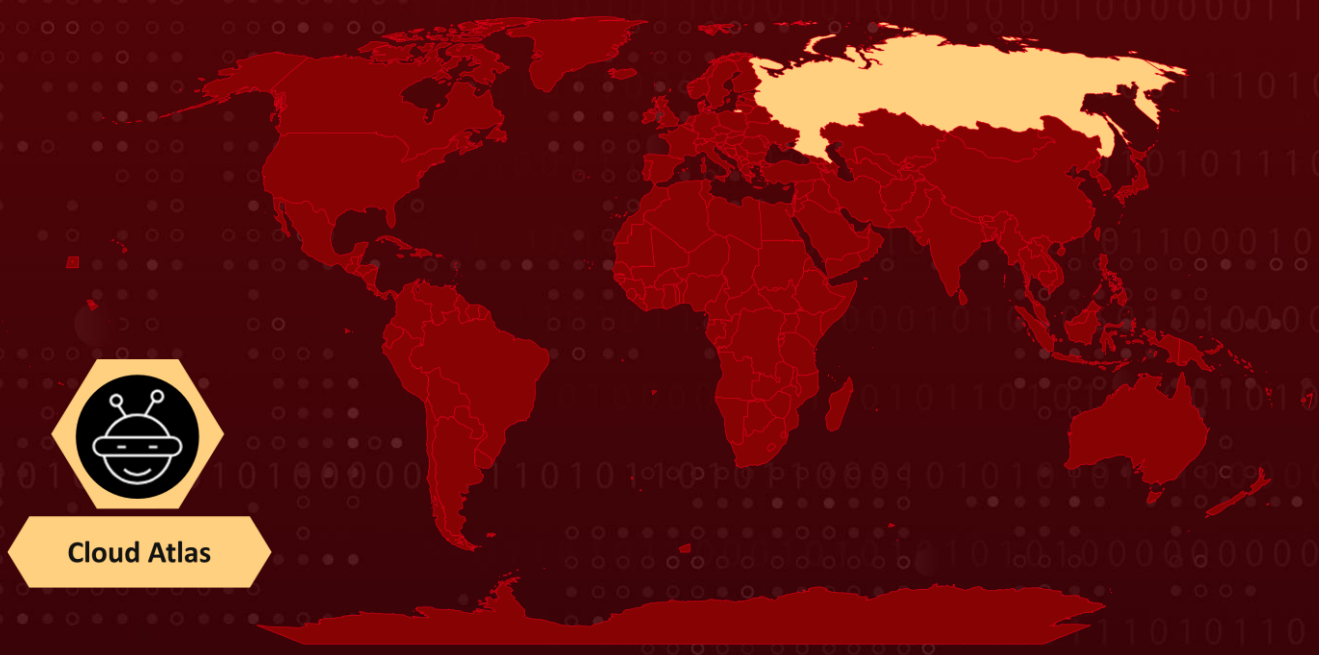
## Cloud Atlas Exploits Six-Year-Old Flaw to Target Russian Companies

| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| December 27, 2023 | A1 | TA2023522 |

# Summary

**Attack Discovered:** November 2023
**Attack Region:** Russia
**Target Industry:** Russian agro-industrial enterprise and a state-owned research company
**Actor:** Cloud Atlas ( aka Inception Framework, Oxygen, ATK 116, Blue Odin, The Rocra)
**Attack:** The threat actor Cloud Atlas has been identified in spear-phishing attacks targeting Russian enterprises. The modus operandi involves a phishing message in the initial stage, containing a lure document that exploits CVE-2017-11882, a memory corruption vulnerability in Microsoft Office's Equation Editor. This six-year-old vulnerability is leveraged to initiate the execution of malicious payloads.

## Attack Regions




## CVEs

| CVE | NAME | AFFECTED PRODUCT | ZERO -DAY | CISA KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2017-11882 | Microsoft Office Memory Corruption Vulnerability | Microsoft Office | ✗ | ✓ | ✓ |

# Attack Details

**#1** The threat actor known as Cloud Atlas has been implicated in a series of spear-phishing attacks targeting Russian enterprises. The initial stage typically involves a phishing message containing a lure document that exploits CVE-2017-11882, a six-year-old memory corruption vulnerability in Microsoft Office's Equation Editor. This exploit is used to initiate the execution of malicious payloads as part of the cyber intrusion.

**#2** Cloud Atlas is a pro-government APT group specializing in cyber espionage and the theft of confidential information. The group has been active since at least 2014. Cloud Atlas typically targets industrial enterprises and state-owned companies in countries such as Russia, Belarus, Azerbaijan, Turkey, and Slovenia.

**#3** In the latest kill chain, the successful exploitation of CVE-2017-11882 is achieved through RTF template injection, facilitating the execution of shellcode responsible for downloading and running an obfuscated HTA file. The phishing emails are sent from popular Russian email services, namely Yandex Mail and VK's Mail.ru. Following the exploitation, the malicious HTML application initiates the launch of VBS files. These VBS files, in turn, retrieve and execute an unknown VBS code from a remote server, completing the attack chain.

**#4** The Cloud Atlas group has primarily utilized targeted email with malicious attachments as their main attack vector. In light of this, organizations need to be vigilant against phishing attacks. Additionally, it is crucial to promptly patch the targeted CVE-2017-11882 to mitigate the risk of falling victim to the attack chain associated with Cloud Atlas.

# Recommendations

**Apply Patch:** Install the security patch provided by Microsoft to address the CVE-2017-11882 vulnerability. This patch closes the security gap that allows attackers to exploit the vulnerability.

**Robust Endpoint Security:** Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

**Email Security Measures:** Employ robust email security solutions to detect and block malicious attachments and links. Consider using advanced threat protection (ATP) and email filtering technologies to prevent the delivery of emails containing malicious content.

**Remain Vigilant:** It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0043<br>Reconnaissance | TA0042<br>Resource Development | TA0001<br>Initial Access | TA0002<br>Execution |
| TA0003<br>Persistence | TA0004<br>Privilege Escalation | TA0005<br>Defense Evasion | TA0007<br>Discovery |
| TA0011<br>Command and Control | T1589<br>Gather Victim Identity Information | T1589.002<br>Email Addresses | T1583<br>Acquire Infrastructure |
| T1583.001<br>Domains | T1585<br>Establish Accounts | T1585.002<br>Email Accounts | T1587<br>Develop Capabilities |
| T1587.001<br>Malware | T1587.004<br>Exploits | T1608<br>Stage Capabilities | T1608.001<br>Upload Malware |
| T1566<br>Phishing | T1566.001<br>Spearphishing Attachment | T1559<br>Inter-Process Communication | T1559.001<br>Component Object Model |

| | | | |
|---|---|---|---|
| **T1203** Exploitation for Client Execution | **T1204** User Execution | **T1204.002** Malicious File | **T1059** Command and Scripting Interpreter |
| **T1059.005** Visual Basic | **T1547** Boot or Logon Autostart Execution | **T1547.001** Registry Run Keys / Startup Folder | **T1027** Obfuscated Files or Information |
| **T1140** Deobfuscate/Decode Files or Information | **T1070** Indicator Removal | **T1070.004** File Deletion | **T1564** Hide Artifacts |
| **T1564.004** NTFS File Attributes | **T1221** Template Injection | **T1218** System Binary Proxy Execution | **T1218.005** Mshta |
| **T1082** System Information Discovery | **T1071** Application Layer Protocol | **T1071.001** Web Protocols | **T1105** Ingress Tool Transfer |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| MD5 | 7bdb049cb0cc3623e4fa1d8e2574f1ce, b1995d8a9df9bd8ce23d38b0ab454580, f611cb1a320a9d3b5df4b70b37b0fd73, 0957edfec31dd2dd05d484eed90593c7, 965d5dc42ee1efdcbc52d061624526c7, B3de2f04ceb97f8e9164399649433e1e, 2e950fe4bd76088f89433a6f2146cb67, efd493e8ebcd66f9404338532519eb90, cd8141f094cfb0dae11747ee9dc74a2f, 9c5a6ede9b0ca906cbc121cc5496b714, 0a850c27c8ce24c0a6fa5bcf7504dc30, 27d49df3e0122152dc9a3f752a099f39, ddbc081392ffa41bcb3e7a007edf727b, b0de9d6133d73c32b243cf716a7c614c |
| SHA1 | 7329424eba132feebba57e239000331e886b1656, 7c8479a818ea21fc228334dfdd55044866a95026, d59f3f2b5132ff23e3fa6d88f1b97b299af38507, a03a699031e956b4fde1ced6309b67853a54602a, a176a164e728c929f70ab2ffa44213625ae17172, 3375772e3bc60614e3e398fd019c8931d2ad83c9, 07735f3da5f5847e9df43034459e3ead4c1f3f35, 877f95ee15adb5540d0b50509a14d1cdf89fe3e1, |

| TYPE | VALUE |
| --- | --- |
| SHA1 | 85a24692089d1a8dc6354a88b6f1e08567db6b0d, 3b2109317985de28d16aef6306ba5a788eb121bf, 44a21627eed099a55e5592509e6e3333c5d3d339, 6efed9d4e8ae02808bed488566f90a4ecc361546, 151e9e6defac4a67be8916a1e119917b69e053ac, 53cea3a93a481a710e821d9c3e087fc18fb989f9 |
| SHA256 | e3d2e6f8740bc5a510239af41e77a3e07eaf09f1aa5cda78558035399db3f971, 8eb6b3ab2d18d01a46cae3cee0987fe8ecdedce2cb80666057a4880c9f37c529, 6e4349775f77b21b627d39a125cd60ad9f3df46d2b4f2a7a71df0d459cb7c9ae, cfc3178b710038666a4a4c5676b5c6befea085ad0243663791ae95f65e1468de, ea91967c2a52b1c09395613f972a319332b678493f4e2ece0e0009e1efd36bec, b6f14556490908a462f8fb61a46b1b140f40723b5725c93fe4ff87a62f036e80, baccfa04bf7cf862c05bc7180532cf609df43a091febd3d85524d6689df6e405, 1e931660cce69add24e405c9fbdd3072190c9f716c1675334f00d0bdbf84bf46, a8ec7b38eaa239c90e647a47368159fb2a6a94c0e56df5a4d8f33e5b469e7942, b9056344e65655080905c4ddb38cfb8a09675fedc4c5244a969918af5b9b39cf, 1ce69ec5b15ba2d0d7ed01cd9ae0facecf2b8fbbd32ea3b1f256310c129f5c74, bc684928f7fd575182af5f797308e9f2286e7bd8d010f6e04913a2600495bbb7, 47c530de3ad2c98b0dfb0c72a4697240e7a218701c2cce12ae217faf58c32335, c7100994bced2a532f3fc350c5db7401775be9658127233c7665e6864c6de2f7 |
| Filepath | %APPDATA%\Microsoft\Windows\khaki.xml |
| Registry | [HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run] tzautoupdate = “wscript /B “%APPDATA%\Microsoft\Windows\khaki.xml:khaki.vbs” |

| TYPE | VALUE |
| --- | --- |
| URL | hxxps://network-list[.]com/?wkbi.html_handfeed, hxxps://network-list[.]com/?wp-content_plugins/photo-gallery/css/bwg-fonts/fonts.css?ver=0.0.1time=1673472550/ballock, hxxps://network-list[.]com/?php-tag_zabbix/lowlanders, hxxps://network-list[.]com/?products_list108.htmlheader-bottom/nemoricole, hxxps://network-list[.]com/?php-wp-content/plugins/contact-form-7/includes/css/styles.css/undesirous, hxxps://network-list[.]com/?area_gifu_?iref=pc_gnavi/semisovereignty, hxxps://network-list[.]com/?qgcl.html_anapeiratic, hxxps://network-list[.]com/?php-business-and-economy/hematomancy, hxxps://network-list[.]com/?wp-includes_wlwmanifest.xml/datemark, hxxps://network-list[.]com/?rpgg.html_protophloem, hxxps://network-list[.]com/?php-pvrg.html_outblunder, hxxps://network-list[.]com/protophloem/p21, hxxps://network-list[.]com/outblunder/a63, hxxps://avito-service[.]net/service/37.html/bersim |
| Domains | avito-service[.]net, network-list[.]com |
| IP | 95.217.82[.]125 |

## Patch Link

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

## References

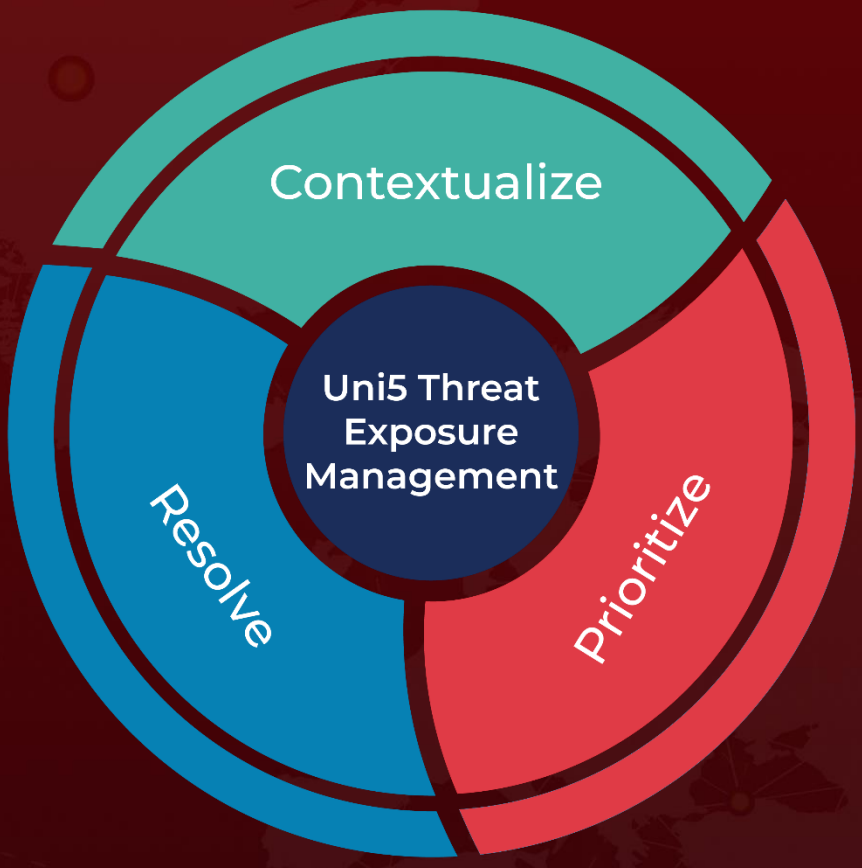
https://www.facct.ru/blog/cloud-atlas/

https://www.hivepro.com/threat-advisory/the-cloud-atlas-perpetual-threat-aims-to-persuade-entities-in-russia/

# 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 27, 2023 . 4:10 AM**



More at www.hivepro.com