Hive Pro

Threat Level

Red

HiveForce Labs

# THREAT ADVISORY

## ATTACK REPORT

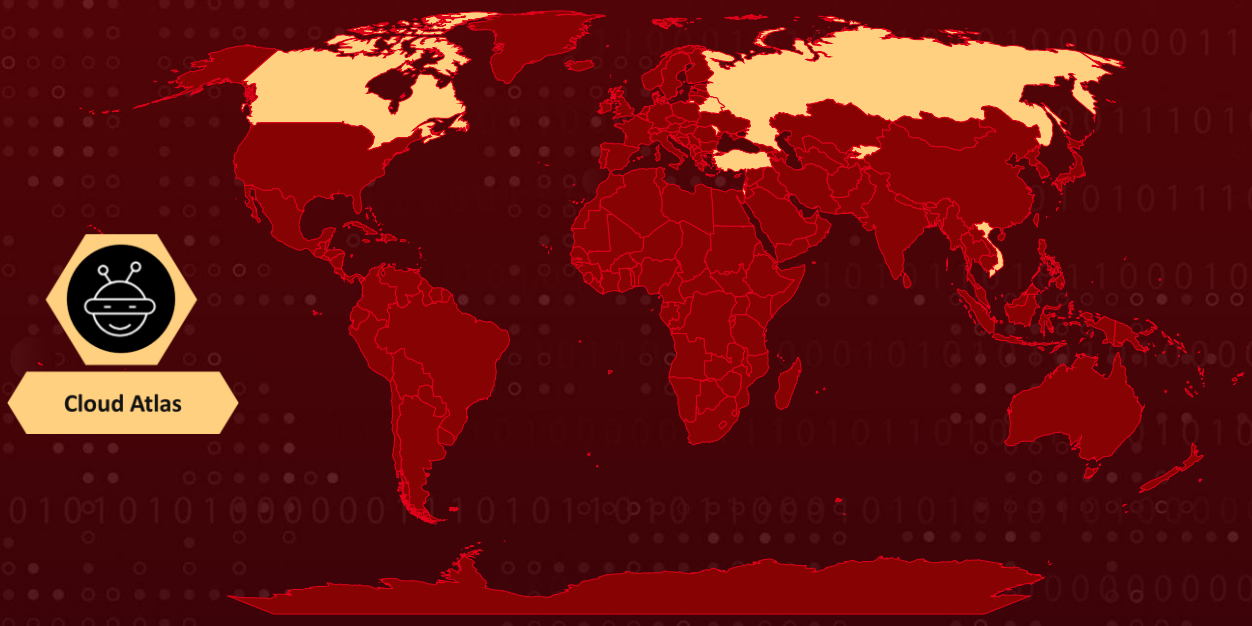
# Unveiling Cloud Atlas: A Novel Backdoor Expansion


| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| December 24, 2024 | A1 | TA2024471 |

# Summary

**Attack Commenced:** 2024
**Threat Actor:** Cloud Atlas
**Malware:** VBShower, VBCloud, PowerShower
**Targeted Countries:** Russia, Belarus, Canada, Moldova, Israel, Kyrgyzstan, Vietnam, Turkey
**Attack:** The cyber threat group Cloud Atlas unveiled a sophisticated, previously unknown toolset, targeting victims with phishing emails that exploit a known vulnerability. This clever attack chain drops malicious files, including the VBShower and PowerShower backdoors, allowing attackers to stealthily infiltrate systems. Cloud Atlas continues to evolve its methods to remain under the radar.

## Attack Regions




## CVE

| CVE | NAME | AFFECTED PRODUCT | ZERO-DAY | CISA KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2018-0802 | Microsoft Office Memory Corruption Vulnerability | Microsoft office | ✓ | ✓ | ✓ |

# Attack Details

**#1** Cloud Atlas employed a previously undocumented toolset, which it extensively utilized in 2024. Victims are infected through phishing emails containing a malicious document that exploits a vulnerability in the formula editor (CVE-2018-0802), enabling the download and execution of malware.

**#2** Upon opening, the document retrieves a malicious template formatted as an RTF file from a remote server controlled by the attackers. This template contains an exploit for the formula editor, which triggers the download and execution of an HTML Application (HTA) file hosted on the same command-and-control (C2) server.

**#3** The malicious HTA file extracts and writes several files to disk, which are components of the VBShower backdoor. VBShower functions as a loader, subsequently downloading and installing another backdoor, PowerShower. Building on the group's prior methods of file and information exfiltration, this operation integrates new tactics to evade detection.

**#4** VBCloud leverages public cloud storage services, such as WebDAV servers, as C2 infrastructure. This approach effectively blends malicious traffic with legitimate network activity, complicating detection and blocking by traditional security measures.

**#5** Simultaneously, the group continues to deploy VBShower, a versatile loader that delivers malicious scripts and erases traces of its activities by deleting logs and downloaded files. Primarily serving as the initial backdoor, VBShower lays the groundwork for further intrusions.

**#6** PowerShower complements these tools by conducting advanced tasks like network reconnaissance and credential harvesting. It employs PowerShell scripts to probe Active Directory, execute Kerberoasting attacks, and extract sensitive information.

# Recommendations

**Regular Patching and Updates:** Implement a comprehensive update strategy focusing on CVE-2018-0802. Prioritize identifying and patching affected assets, especially vulnerable Microsoft Office versions. Ensure all operating systems, third-party applications, and security software are regularly updated to maintain overall system security.

**Enforce Application Whitelisting:** Implement strict application whitelisting policies to prevent unauthorized or malicious executables from running within your environment.

**Behavior Monitoring:** Implement behavior monitoring on endpoints to continuously track and analyze user, application, and device activities in real-time. Use advanced analytics and machine learning algorithms to detect anomalies and suspicious behaviors, enabling rapid identification and response to potential security threats across your network.

**Monitor Network Traffic:** Track network activity for anomalies such as excessive data transfers to unfamiliar IP addresses or unusual RDP usage patterns.

To **mitigate Kerberoasting attacks**, implement strong password policies for service accounts with Service Principal Names (SPNs). Use complex passwords of at least 25 characters, rotate them every 30 days, and utilize group managed service accounts (gMSAs) for automated password management. This significantly reduces the risk of attackers cracking ticket-granting service (TGS) hashes.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0001<br>Initial Access | TA0002<br>Execution | TA0003<br>Persistence | TA0006<br>Credential Access |
| TA0005<br>Defense Evasion | TA0007<br>Discovery | TA0009<br>Collection | TA0011<br>Command and Control |

| | | | |
|---|---|---|---|
| **TA0010** Exfiltration | **T1001** Data Obfuscation | **T1105** Ingress Tool Transfer | **T1564.003** Hide Artifacts: Hidden Window |
| **T1558.003** Steal or Forge Kerberos Tickets: Kerberoasting | **T1087** Account Discovery | **T1069.002** Permission Groups Discovery: Domain Groups | **T1069.001** Permission Groups Discovery: Local Groups |
| **T1615** Group Policy Discovery | **T1201** Password Policy Discovery | **T1557** Adversary-in-the-Middle | **T1567.002** Exfiltration Over Web Service: Exfiltration to Cloud Storage |
| **T1041** Exfiltration Over C2 Channel | **T1560** Archive Collected Data | **T1566** Phishing | **T1204.002** User Execution: Malicious File |
| **T1059.005** Command and Scripting Interpreter: Visual Basic | **T1547.001** Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder | **T1070.004** Indicator Removal: File Deletion | **T1140** Deobfuscate/Decode Files or Information |
| **T1083** File and Directory Discovery | **T1012** Query Registry | **T1082** System Information Discovery | **T1033** System Owner/User Discovery |
| **T1057** Process Discovery | **T1053** Scheduled Task/Job | **T1071.001** Application Layer Protocol: Web Protocols | |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| Domains | content-protect[.]net,<br>control-issue[.]net,<br>office-confirm[.]com,<br>onesoftware[.]info,<br>serverop-parametrs[.]com,<br>web-privacy[.]net,<br>net-plugin[.]org,<br>triger-working[.]com,<br>yandesks[.]net,<br>yandisk[.]info,<br>mirconnect[.]info,<br>sber-cloud[.]info, |

| TYPE | VALUE |
| --- | --- |
| Domains | gosportal[.]net,<br>riamir[.]net,<br>web-wathapp[.]com,<br>yandisk[.]info,<br>yandesktop[.]com,<br>web-wathapp[.]com,<br>webdav[.]opendrive[.]com,<br>webdav[.]mydrive[.]ch,<br>webdav[.]yandex[.]ru,<br>kim[.]nl[.]tab[.]digital |
| MD5 | 9d3557cc5c444fe5d73e4c7fe1872414,<br>cba05e11cb9d1d71f0fa70ecd1af2480,<br>cbfb691e95ee34a324f94ed1ff91bc23,<br>2d24044c0a5b9ebe4e01ded2bfc2b3a4,<br>88be01f8c4a9f335d33fa7c384ca4666,<br>a30319545fda9e2da0532746c09130eb,<br>31b01387ca60a1771349653a3c6ad8ca,<br>15fd46ac775a30b1963281a037a771b1,<br>389bc3b9417d893f3324221141edea00,<br>160a65e830eb97aae6e1305019213558,<br>184cf8660af7538cd1cd2559a10b6622,<br>1af1f9434e4623b7046cf6360e0a520e,<br>1bfb9cba8aa23a401925d356b2f6e7ed,<br>21585d5881cc11ed1f615fdb2d7acc11,<br>242e86e658fe6ab6e4c81b68162b3001,<br>2fe7e75bc599b1c68b87cf2a3e7aa51f,<br>36dd0fbd19899f0b23ade5a1de3c2fec,<br>389f6e6fd9dcc84c6e944dc387087a56,<br>3a54acd967dd104522ba7d66f4d86544,<br>3f12bf4a8d82654861b5b5993c012bfa,<br>49f8ed13a8a13799a34cc999b195bf16,<br>4b96dc735b622a94d3c74c0be9858853,<br>f45008bf1889a8655d32a0eb93b8acdd,<br>aa8da99d5623fafed356a14e59acbb90,<br>016b6a035b44c1ad10d070abcdfe2f66,<br>0139f32a523d453bc338a67ca45c224d,<br>01db58a1d0ec85adc13290a6290ad9d6,<br>0f37e1298e4c82098dc9318c7e65f9d2,<br>6fcee9878216019c8dfa887075c5e68e,<br>d445d443ace329fb244edc3e5146313b,<br>f3f28018fb5108b516d802a038f90bde |
| SHA1 | cc7a18fad126d2b910e7d1f99e43e76510bee3f0,<br>4cc55e152e8bee21ef43fd5e8b7595662227e5e3,<br>aebd9d7dcac429f05d40e585d27ff7647a34909e, |

| TYPE | VALUE |
| --- | --- |
| SHA1 | 7318a2615618b1e5ded947b0bdf5683bc910918c, e5a597c143592d6f4c2f69c515c2b230989561f5, db5525ef7d4b6a92af91fb1ebc4e0e6b8e13365f, 7c75f00f89fbd1e4977032e945c2468590c60450, ac8ec1e17bd90430113b2c083793682e68e03311, 9c60869ae3697662102c8dd54bd45fbf2588d02e, ed492410a934c27b4b1cd81d2cb01190ad24faa6, c1fcf0db984815dcee8b6323f173ba4097a0fc24, 6e94c09756b6dcba5ce9ea7e34af19e5e1777de0, 54129ab2bc800982a99bda32002620ec572cc1bf, cf3cf5df1206b14f7d528c5e58d7ff6ace719ed2, 93dec8070a822b63eb6b23c342e56272642d9128, 0cd6b538b3db7c8f48b05ab456ca673bad8068dc, d7dfda94d354ee218bf06cf232ca47858b0fc7ff, 0db2dcea98298669b2bb3cebeb9e72a66f5c84c2, cda338eb207311ff14e4f49306a972ba3759f03b, 1deb1ed97dd971cedf81fe13e8dc86c3ef9d9851, f6ee2629b0180e1cdc4a9603e7c783035a32d25d, 3790e6f13b5927f3647bbf606b7d416d2aff8c4f, 40bcb307884ad84bc884c1f2b701e680c7ffc151, 7bb42d09cdae0c34592bd4bfe5125836812bd765, ce843abe13b0178e0e12dc0719be1cb164b158e4, 3f8094e77185af6143eb7dd7ea5c51e9add7f5f1, 10c647af079537c18a1b9f94af596e65a238fcc0, 93bb6307a5dde45d92c8bdc7279d6ff63be8c541, b5b67df4643043aab9533cc1156e44532b4d26c6, 06393cf9bd61e1894dc90e2720f8cbb8778f726f, f5eae20a841a8b44350226522271cc805372dac6 |
| SHA256 | 1c5df7daf20c2235e7576b7399d83a85acad8252b08d07135b2481118a7c47ce, 31978d00e77c3d043116563d1b23e44fecba5c01b0fd17c1a0d2f4811294800d, 92088064194a9960d43d70db1452978c7bd325436d798e5b5fe25289fe79d112, fd8a336452c27fcb65b88e0d47e888e683d5bacb63c140926c4a0557b4b48d80, 2e73cde9ce49cfd1970824f23d1fd4afd9b139f18f1aafc523814ecbdf4550ee, 1031e6d27ac96e53a4a3f5d5072029fca47b8b9b703860b5ab61bb06be777075, c4f97cd48cc2ca11acc9e49ac18b8763752853beaabf149fe313b295fa01b2d6, 7b0683a60a10657963cbcfcc9d0480e7812a3894ffb3b0d6d92bab0dc2fde0b4, |

| TYPE | VALUE |
| --- | --- |
| SHA256 | a9f53fc9f350446632111b500550567a8273d0f7838d27099c41f523a0a550b9,<br>55f3f668364b3986a2c4ea528d00031c7a0ab67df54cef8affe92a21737f86c9,<br>25230923690d4ce004d0592eac057f8d4ceb942f8334fb9d28d1363271ad3c89,<br>d9c670f4b5c67958c8f8d705d66c0dbc2ab95e8edc441903e0c68de0aa7b4379,<br>a8bf032dea0fec1c6ef2926edcc03baedcadae149fcbcfb75925a98f290408cf,<br>366f6984d8aa9e78bca46788162f510bbafc10ede3d3ad4c4f53fb42bee00c55,<br>26295b543d1cb6cce1337cc06c1c8a8a0ee30e9aac580710f26bff7d5cc18193,<br>69b3f4877c7e051dc87d78b8d760e34b6a60000a10ea64351b577d6cb4df8967,<br>9ca81de013b9f9de63c80275fb662510241f97c4d1daab10ab6418a9d0a89cb6,<br>f482cfe98e589bffd7eee76be5caf4040c69d4c0a8efbd10dcffaefab146ecd4,<br>aa509fe7b7d6531866c3506e2c006e31926504685e685d93f658e3efb709400e,<br>678b30bcb599663bc7c26b4dc2ba49ee34048841c83531ca7c7f5ea2e3dee962,<br>97497246227ef159a1bedf6ce97c8b81eb9cc86d34f5fbd00d7fe31862b3946d,<br>1aaf4c0e8653d11adf5d36096130bb3d76384e932a476ae104eefcc0f9823d72,<br>75b2e65bebea849d0bd0bab6599f477e6ebd0e74c2ffa960d2360db771e3f583,<br>a5ad86dd7e6b35b45957e9b0986b5fc633a0968d2887b702e1753a469ec57407,<br>81ab65c7b54f501a2e2962346764a6dcb587f32d5ee62b3569a4ba348152fdb9,<br>3d55f9a70a1b01432fc0432e5b43ff6c8fa4a8a7a9ed5a787d9cf2a579b12c80,<br>614e7290bf7974e22e7eac04c1443565ca52e626f9ce4f93f8f33468293c7556,<br>b2769bc8a25ee6b65e58b6f2795316d67771c54b9a423bf02c3779d63b08bc4a,<br>9047d2116b226b35170d1e8a7c81ce0fd25822f6bdf21db39fa3fd28700420a8,<br>957bbadda00231d45959c3f900d6ac805afbb1cb086192ad68549f3cf0cb8ec2,<br>5928b83d2626a85231618d6ba169a0133530a71bb71104c948b4b30e45aef0e0 |

## Patch Link

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

## References

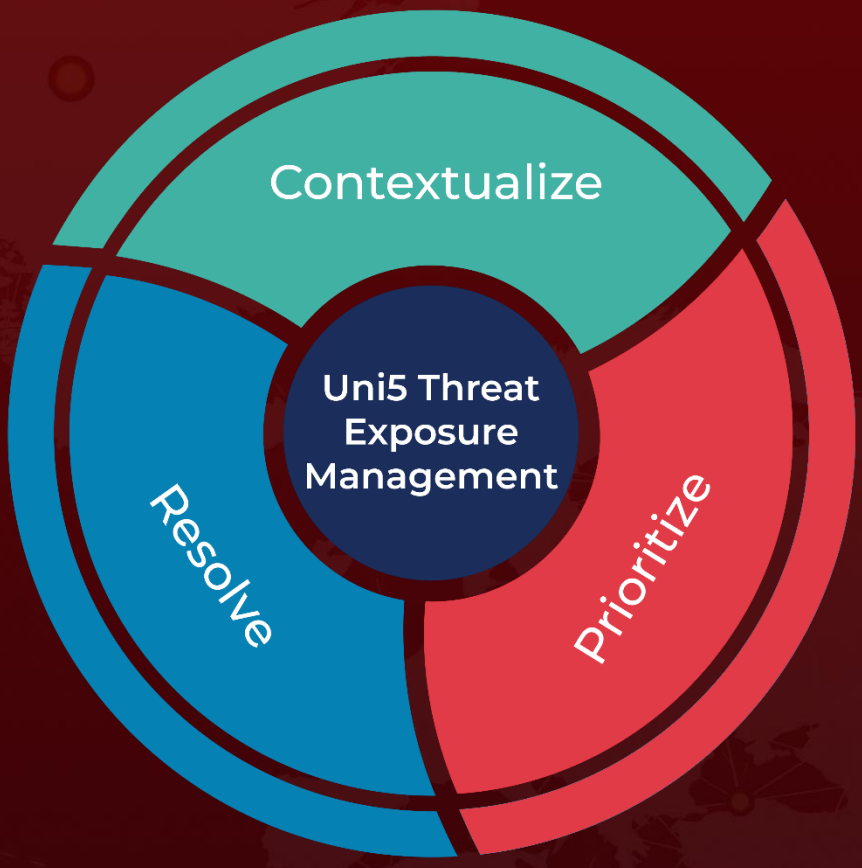
https://securelist.com/cloud-atlas-attacks-with-new-backdoor-vbcloud/115103/

https://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 24, 2024 . 9:30 AM**



More at www.hivepro.com