Recent Cloud Atlas activity

By GReAT

Published: 2019-08-12 · Archived: 2026-04-02 11:08:47 UTC

Also known as Inception, Cloud Atlas is an actor that has a long history of cyber-espionage operations targeting industries and governmental entities. We first reported Cloud Atlas in 2014 and we've been following its activities ever since.

From the beginning of 2019 until July, we have been able to identify different spear-phishing campaigns related to this threat actor mostly focused on Russia, Central Asia and regions of Ukraine with ongoing military conflicts.

Countries targeted by Cloud Atlas recently

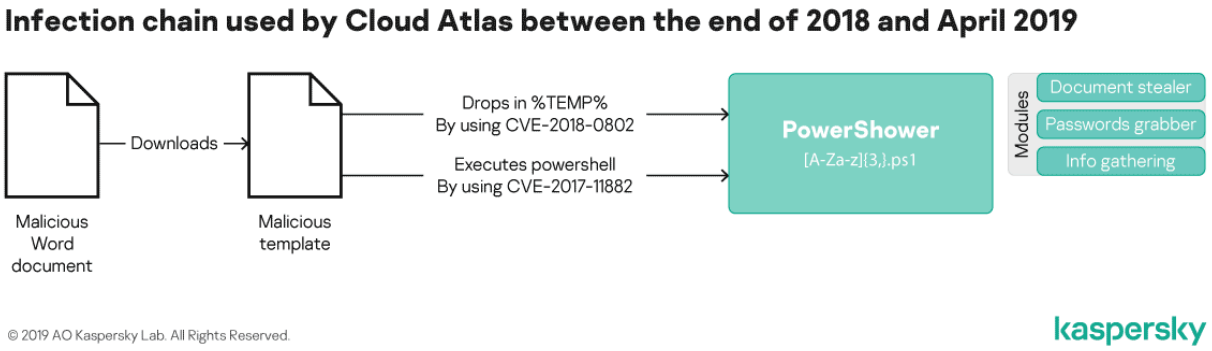
Cloud Atlas hasn't changed its TTPs (Tactic Tools and Procedures) since 2018 and is still relying on its effective existing tactics and malware in order to compromise high value targets.

The Windows branch of the Cloud Atlas intrusion set still uses spear-phishing emails to target high profile victims. These emails are crafted with Office documents that use malicious remote templates – allowlisted per victims – hosted on remote servers. We described one of the techniques used by Cloud Atlas in 2017 and our colleagues at Palo Alto Networks also wrote about it in November 2018.

Previously, Cloud Atlas dropped its "validator" implant named "PowerShower" directly, after exploiting the Microsoft Equation vulnerability (CVE-2017-11882) mixed with CVE-2018-0802. During recent months, we have seen a new infection chain, involving a polymorphic HTA, a new and polymorphic VBS implant aimed at executing PowerShower, and the Cloud Atlas second stage modular backdoor that we disclosed five years ago in our first blogpost about them and which remains unchanged.

Let’s meet PowerShower

PowerShower, named and previously disclosed by Palo Alto Networks in their blogspot (see above), is a malicious piece of PowerShell designed to receive PowerShell and VBS modules to execute on the local computer. This malware has been used since October 2018 by Cloud Atlas as a validator and now as a second stage. The differences in the two versions reside mostly in anti-forensics features for the validator version of PowerShower.



The PowerShower backdoor – even in its later developments – takes three commands:

Command	Description
0x80 (Ascii “P”)	It is the first byte of the magic PK. The implant will save the received content as a ZIP archive under %TEMP%\PG.zip.
0x79 (Ascii “O”)	It is the first byte of “On resume error”. The implant saves the received content as a VBS script under “%APPDATA%\Microsoft\Word\[A-Za-z]{4}.vbs” and executes it by using Wscript.exe
Default	If the first byte doesn’t match 0x80 or 0x79, the content is saved as an XML file under “%TEMP%\temp.xml”. After that, the script loads the content of the file, parses the XML to get the PowerShell commands to execute, decodes them from Base64 and invokes IEX. After executing the commands, the script deletes “%TEMP%\temp.xml” and sends the content of “%TEMP%\pass.txt” to the C2 via an HTTP POST request.

A few modules deployed by PowerShower have been seen in the wild, such as:

- A PowerShell document stealer module which uses 7zip (present in the received PG.zip) to pack and exfiltrate *.txt, *.pdf, *.xls or *.doc documents smaller than 5MB modified during the last two days;
- A reconnaissance module which retrieves a list of the active processes, the current user and the current Windows domain. Interestingly, this feature is present in PowerShower but the condition leading to the execution of that feature is never met in the recent versions of PowerShower;
- A password stealer module which uses the opensource tool LaZagne to retrieve passwords from the infected system.

We haven't yet seen a VBS module dropped by this implant, but we think that one of the VBS scripts dropped by PowerShower is a dropper of the group's second stage backdoor documented in our article back in 2014.

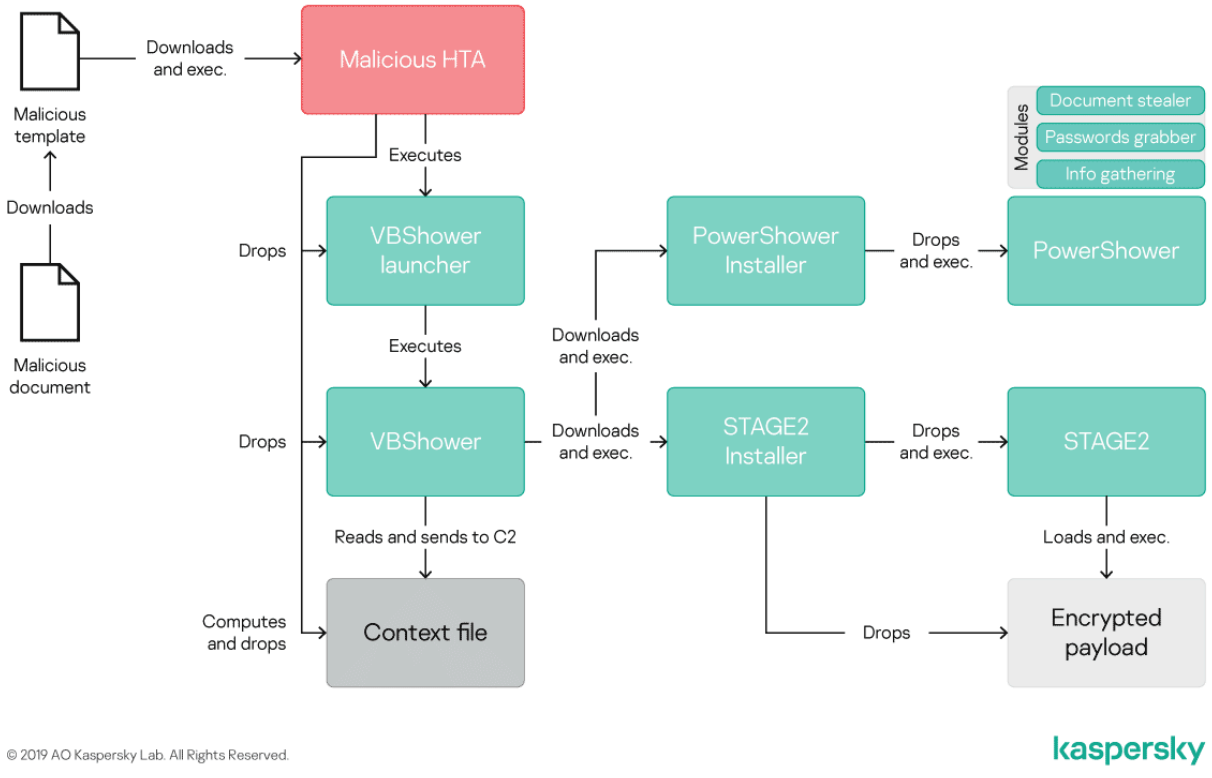
And his new friend, VBShower

During its recent campaigns, Cloud Atlas used a new "polymorphic" infection chain relying no more on PowerShower directly after infection, but executing a polymorphic HTA hosted on a remote server, which is used to drop three different files on the local system.

- A backdoor that we name **VBShower** which is polymorphic and replaces PowerShower as a validator;
- A tiny launcher for VBShower ;
- A file computed by the HTA which contains contextual data such as the current user, domain, computer name and a list of active processes.

This "polymorphic" infection chain allows the attacker to try to prevent IoC-based defence, as each code is unique by victim so it can't be searched via file hash on the host.

Updated infection chain used by Cloud Atlas



kaspersky

The VBShower backdoor has the same philosophy of the validator version of PowerShower. Its aim is to complicate forensic analysis by trying to delete all the files contained in "%APPDATA%\..\Local\Temporary Internet Files\Content.Word" and "%APPDATA%\..\Local Settings\Temporary Internet Files\Content.Word\".

Once these files have been deleted and its persistence is achieved in the registry, VBShower sends the context file computed by the HTA to the remote server and tries to get via HTTP a VBS script to execute from the remote

server every hour.

At the time of writing, two VBS files have been seen pushed to the target computer by VBShower. The first one is an installer for PowerShower and the second one is an installer for the Cloud Atlas second stage modular backdoor which communicates to a cloud storage service via Webdav.

Final words

Cloud Atlas remains very prolific in Eastern Europe and Central Asia. The actor's massive spear-phishing campaigns continue to use its simple but effective methods in order to compromise its targets.

Unlike many other intrusion sets, Cloud Atlas hasn't chosen to use open source implants during its recent campaigns, in order to be less discriminating. More interestingly, this intrusion set hasn't changed its modular backdoor, even five years after its discovery.

IoCs

Some emails used by the attackers

- infocentre.gov@mail.ru
- middleeasteye@asia.com
- simbf2019@mail.ru
- world_overview@politician.com
- infocentre.gov@bk.ru

VBShower registry persistence

- Key : HKCU\Software\Microsoft\Windows\CurrentVersion\Run\[a-f0-9A-F]{8}
- Value : wscript //B "%APPDATA%\[A-Za-z]{5}.vbs"

VBShower paths

- %APPDATA%\[A-Za-z]{5}.vbs.dat
- %APPDATA%\[A-Za-z]{5}.vbs
- %APPDATA%\[A-Za-z]{5}.mds

VBShower C2s

- 176.31.59.232
- 144.217.174.57
