Cloud Cover: How Malicious Actors Are Leveraging Cloud Services

security.com/threat-intelligence/cloud-espionage-attacks

Threat Hunter TeamSymantec

The number of threat actors leveraging legitimate cloud services in their attacks has grown this year as attackers have begun to realize their potential to provide low-key and low-cost infrastructure. Traffic to and from well known, trusted services such as Microsoft OneDrive or Google Drive may be less likely to raise red flags than communications with attacker-controlled infrastructure.

In the past few weeks alone, Symantec's Threat Hunter Team has identified three further espionage operations using cloud services and found evidence of further tools in development. Marc Elias, an investigator with the Threat Hunter Team, will be presenting these findings today (August 7) at the Black Hat Conference in Las Vegas.

GoGra

A previously unseen backdoor which Symantec has named GoGra (Trojan.Gogra) was deployed against a media organization in South Asia in November, 2023. GoGra is written in Go and uses the Microsoft Graph API to interact with a command-and-control (C&C) server hosted on Microsoft mail services.

Graph is a Microsoft API designed to facilitate access to resources hosted on Microsoft cloud services, such as Microsoft 365. Authentication is carried out using OAuth access tokens.

GoGra is configured to read messages from an Outlook username "FNU LNU" whose subject line starts with the word "Input". It decrypts the message contents using the AES-256 algorithm in Cipher Block Chaining (CBC) mode, using the following key: b14ca5898a4e4133bbce2ea2315a1916.

Gogra executes commands via the cmd.exe input stream and supports an additional command named "cd" which changes the active directory. After the execution of a command, it encrypts the output and sends it to the same user with the subject "Output".

Analysis of the backdoor revealed that it is highly likely it was developed by Harvester, a nation-state-backed group uncovered by Symantec in 2021 that specializes in targeting organizations in South Asia.

GoGra is functionally similar to a known Harvester tool called Graphon, which was written in .NET. Aside from the different programming languages used, Graphon used a different AES key (juBvYU7}33Xq}ghO), did not contain the extra “cd” command, and did not have a hardcoded Outlook username to communicate with. The username was instead received from the C&C server.

Google Drive exfiltration

A previously unseen exfiltration tool was deployed by the Firefly espionage group in an attack against a military organization in South East Asia. Analysis of the tool revealed that it was a publicly available Google Drive client in a Python wrapper.

The tool was configured to search for all .jpg files in the System32 directory and upload them to Google Drive using a hardcoded refresh token.

Many of the exfiltrated files were not actual .jpg images but were instead encrypted RAR files, which were likely either created by hands-on-keyboard activity by the attackers or by another attacker-deployed tool that copied and prepared data for exfiltration. Exfiltrated data included documents, meeting notes, call transcripts, building plans, email folders, and accounting data.

Grager

A previously unseen backdoor named Trojan.Grager was deployed against three organizations in Taiwan, Hong Kong, and Vietnam in April 2024. Analysis of the backdoor revealed that it used the Graph API to communicate with a C&C server hosted on Microsoft OneDrive. Grager was downloaded from a typosquatted URL mimicking the open-source file archiver 7-Zip (hxxp://7-zip.tw/a/7z2301-x64[.]msi).

The aforementioned MSI file, which acts as a dropper, is a Trojanized 7-Zip installer that installs the real 7-Zip software into the folder “C:\Program Files (x86)\7-Zip” along with a malicious DLL named “epdevmgr.dll” (SHA2: ab6a684146cec59ec3a906d9e018b318fb6452586e8ec8b4e37160bcb4adc985), a copy of the Tonerjam malware, and the encrypted Grager backdoor into a file named “data.dat” (SHA2: 45a5dd715dc5f08f3b987a0415c2e500c549508aadf4183fdb94f749af8f1d67).

The Tonerjam malware was described by Mandiant as a launcher that decrypts and executes a shellcode payload, which in this case was the new backdoor Grager. The backdoor decrypts a client_id and refresh token for OneDrive from a blob within the file’s body. The backdoor supports the following commands:

- Retrieve machine info including machine name, user, IP address, and machine architecture
- Download/upload a file
- Execute a file
- Gather file system info including available drives, size of drives, and type of drives

There are tentative links between this tool and a group known as UNC5330. Symantec observed the Tonerjam malware described in this blog being dropped with the same file name (epdevmgr.dll) by a benign sample named (EpDevMgr.exe), which Mandiant also attributes to UNC5330. UNC5330 was described as a “suspected China-nexus espionage actor” that exploited Ivanti Connect Secure VPN vulnerabilities (CVE-2024-21893 and CVE-2024-21887) to compromise appliances in early 2024.

MoonTag

Symantec also found evidence of another backdoor called MoonTag (Trojan.Moontag) that appears to be currently in development. Several variants of the backdoor have been uploaded to VirusTotal in recent weeks, although none appeared complete. The malware, which may be named “Moon_Tag” by its developer given references in its strings, is based on code published in this Google Group. All the variants found contain functionality for communicating with the Graph API.

MoonTag samples match a YARA rule named “MAL_APT_9002_SabrePanda” that detects samples from the 9002 RAT malware family used by the Sabre Panda threat actor. We did not find strong links to attribute MoonTag to Sabre Panda, but we can attribute the MoonTag

backdoor with high confidence to a Chinese-speaking threat actor based on the Chinese language used in the Google Group post and the infrastructure used by the attackers.

Onedrivetools

Another backdoor (Trojan.Ondritols), which appears to be called Onedrivetools by its authors, has been deployed against IT services companies in the U.S. and Europe. A multi-stage backdoor, the first stage is a downloader that authenticates to Microsoft Graph API and downloads the second stage payload from OneDrive and executes it.

The main payload will download a publicly available file from GitHub. It will then create a folder in OneDrive named deviceId_n_<ip address> for each infected machine and upload the following file to OneDrive to signal the attackers the status of a new infection:

```
/v1.0/me/drive/root:/deviceId_n_<ip address>/status
```

It will then continue in a loop, authenticating itself using Graph API, creating a file called heartbeat with the content “1” and fetching the new commands to execute from a file called cmd, both files located in the victim folder. The output of the executed command will be saved in the same cmd file. The backdoor also can download files to its victims and upload files from the infected machine to OneDrive.

The attackers used a tunneling tool known as Whipweave (SHA256: 30093c2502fed7b2b74597d06b91f57772f2ae50ac420bcaa627038af33a6982), likely derived from the open-source Chinese VPN Free Connect (FCN) project, to connect to an Operational Relay Box (ORB) network known as Orbweaver which is designed to obfuscate the origin of attacks.

Rapidly developing trend

In May 2024, Symantec uncovered BirdyClient, new malware that used the Graph API to communicate with a OneDrive C&C server. The malware was used in an attack against an organization in Ukraine.

Although leveraging cloud services for command and control is not a new technique, more and more attackers have started to use it recently. Three years ago, Volexity published about BlueLight, malware developed by the North Korea-linked Vedalia espionage group (aka APT37). This was followed by Symantec’s discovery of the Graphon backdoor in October 2021.

The Russian Swallowtail espionage group (aka APT28, Fancy Bear) was found to have adopted the tactic following the discovery of Graphite—malware that used the Graph API to communicate with a OneDrive account that was acting as a C&C server. In June

2023, Symantec discovered Backdoor.Graphican, which was being used by the Flea (aka APT15, Nickel) group in a campaign against foreign affairs ministries in the Americas.

The number of actors now deploying threats that leverage cloud services suggests that espionage actors are clearly studying threats created by other groups and mimicking what they perceive to be successful techniques.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file is available to us, Symantec Endpoint products will detect and block that file.

d728cdcf62b497362a1ba9dbaac5e442cebe86145734410212d323a6c2959f0f – Trojan.Gogra

f1ccd604fcdc0034d94e575b3709cd124e13389bbee55c59cbbf7d4f3476e214 – Trojan.Gogra

9f61ed14660d8f85d606605d1c4c23849bd7a05afd02444c3b33e3af591cfdc9 – Trojan.Grager

ab6a684146cec59ec3a906d9e018b318fb6452586e8ec8b4e37160bcb4adc985 – Trojan.Grager

97551bd3ff8357831dc2b6d9e152c8968d9ce1cd0090b9683c38ea52c2457824 – Trojan.Grager

f69fb19604362c5e945d8671ce1f63bb1b819256f51568daff6fed6b5cc2f274 – Trojan.Ondritols

582b21409ee32ffca853064598c5f72309247ad58640e96287bb806af3e7bede – Trojan.Ondritols

79e56dc69ca59b99f7ebf90a863f5351570e3709ead07fe250f31349d43391e6 – Trojan.Ondritols

4057534799993a63f41502ec98181db0898d1d82df0d7902424a1899f8f7f9d2 – Trojan.Ondritols

a76507b51d84708c02ca2bd5a5775c47096bc740c9f7989afd6f34825edfcba6 – Trojan.Moontag

527fada7052b955ffa91df3b376cc58d387b39f2f44ebdcb54bc134e112a1c14 – Trojan.Moontag

fd9fc13dbd39f920c52fbc917d6c9ce0a28e0d049812189f1bb887486caedbeb – Trojan.Moontag

30093c2502fed7b2b74597d06b91f57772f2ae50ac420bcaa627038af33a6982 – Whipweave

hxxp://7-zip.tw/a/7z2301-x64[.]msi - Trojan.Grager download URL

hxxp://7-zip.tw/a/7z2301[.]msi - Trojan.Grager download URL

7-zip[.]tw – 7-Zip typosquatted domain

103.255.178[.]200 – MoonTag C&C

157.245.159[.]135 – Whipweave C&C

89.42.178[.]13 – Whipweave C&C

30sof.onedumb[.]com – Whipweave C&C

Best Practices

- Block cloud services not used by your organization
- Profile network traffic and monitor for network anomalies
  e.g. Large file is uploaded to a cloud service
- Use application whitelisting where applicable
  Block non-browser processes connecting to cloud services
- Identify critical assets in your organization and monitor them for exfiltration of data
- Activate host based and cloud audit logs

MITRE TTPs

- **Establish Accounts: Cloud Accounts**
  - ID: T1585.003
  - Sub-technique of: T1585 - Establish Accounts
  - Tactic: Resource Development
  - Description: Adversaries may create accounts with cloud providers that can be used during targeting. Adversaries can use cloud accounts to further their operations, including leveraging cloud storage services such as Dropbox, MEGA, Microsoft OneDrive, or AWS S3 buckets for Exfiltration to Cloud Storage or to Upload Tools.

- **Stage Capabilities: Upload Malware**
  - ID: T1608.001
  - Sub-technique of: T1608 - Stage Capabilities
  - Tactic: Resource Development
  - Description: Adversaries may upload malware to third-party or adversary controlled infrastructure to make it accessible during targeting. Malicious software can include payloads, droppers, post-compromise tools, backdoors, and a variety of other malicious content.
- **Stage Capabilities: Upload Tool**
  - ID: T1608.002
  - Sub-technique of: T1608 - Stage Capabilities
  - Tactic: Resource Development
  - Description: Adversaries may upload tools to third-party or adversary controlled infrastructure to make it accessible during targeting. Tools can be open or closed source, free or commercial. Adversaries may upload tools to support their operations, such as making a tool available to a victim network to enable Ingress Tool Transfer (i.e. PowerShell, Certutil) by placing it on an Internet-accessible web server.
- **Command and Scripting Interpreter: Cloud API**
  - ID: T1059.009
  - Sub-technique of: T1059 - Command and Scripting Interpreter
  - Tactic: Execution
  - Description: Adversaries may abuse cloud APIs to execute malicious commands.
- **Exfiltration Over Web Service: Exfiltration to Cloud Storage**
  - ID: T1567.002
  - Sub-technique of: T1567 - Exfiltration Over Web Service
  - Tactic: Exfiltration
  - Description: Adversaries may exfiltrate data to a cloud storage service rather than over their primary command and control channel. Cloud storage services allow for the storage, edit, and retrieval of data from a remote cloud storage server over the internet.

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.