Aug 09 2024

NETMANAGEIT

Intelligence Report

Cloud Cover: How Malicious Actors Are Leveraging Cloud Services

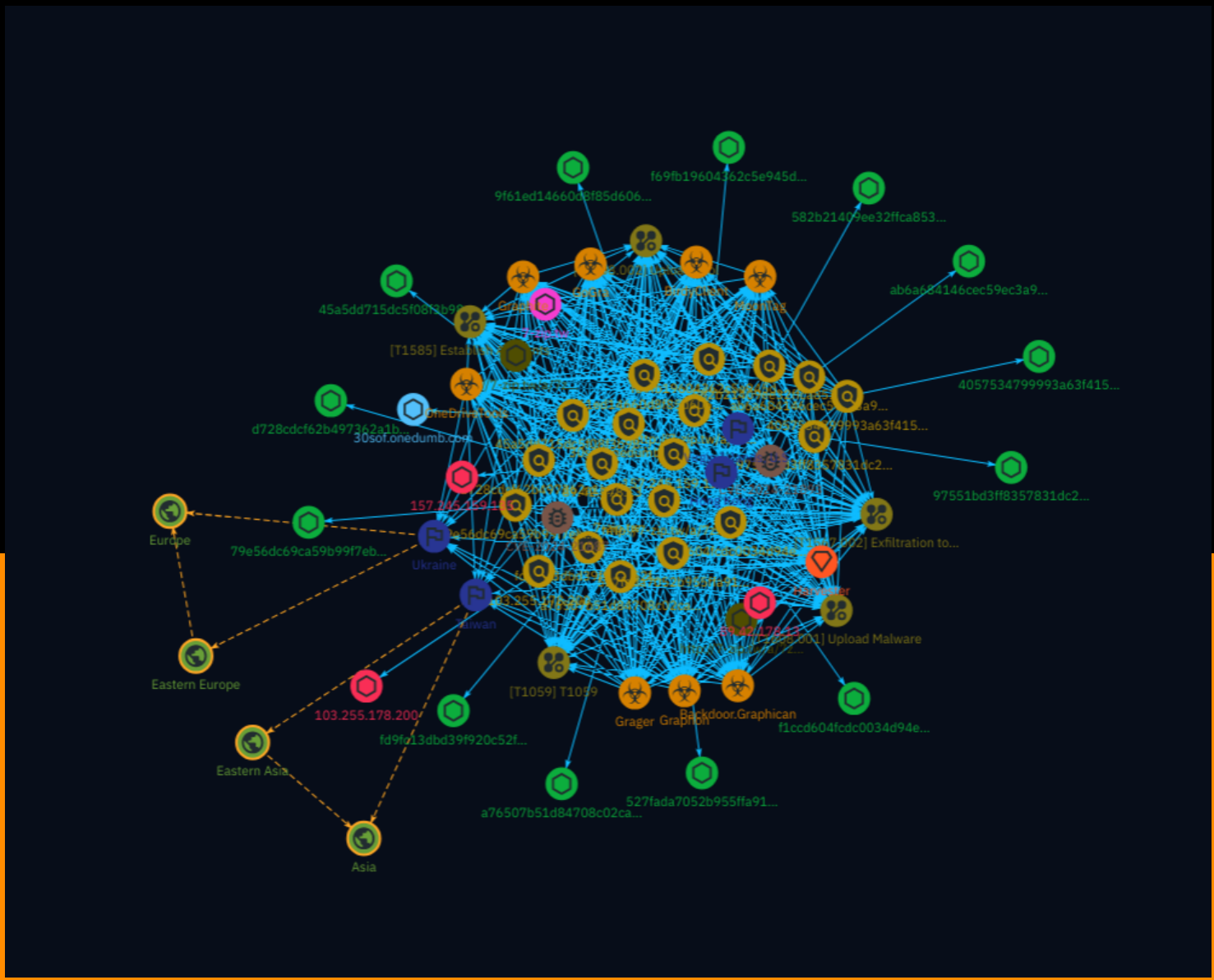

Table of contents

Overview

Entities

Observables

External References

Overview

Description

In recent times, there has been a notable rise in the exploitation of legitimate cloud services by threat actors, including nation-state groups. Attackers have realized the potential of these services to provide low-cost infrastructure, evading detection as communication to trusted platforms may not raise suspicion. Over the past few weeks, Symantec's Threat Hunter Team uncovered three espionage operations utilizing cloud services and discovered evidence of additional tools under development.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

100 / 100

Content

N/A

Attack-Pattern

Name

Establish Accounts

ID

T1585

Description

Adversaries may create and cultivate accounts with services that can be used during targeting. Adversaries can create accounts that can be used to build a persona to further operations. Persona development consists of the development of public information, presence, history and appropriate affiliations. This development could be applied to social media, website, or other publicly available information that could be referenced and scrutinized for legitimacy over the course of an operation using that persona or identity. (Citation: NEWSCASTER2014)(Citation: BlackHatRobinSage) For operations incorporating social engineering, the utilization of an online persona may be important. These personas may be fictitious or impersonate real people. The persona may exist on a single site or across multiple sites (ex: Facebook, LinkedIn, Twitter, Google, GitHub, Docker Hub, etc.). Establishing a persona may require development of additional documentation to make them seem real. This could include filling out profile information, developing social networks, or incorporating photos.(Citation: NEWSCASTER2014)(Citation: BlackHatRobinSage) Establishing accounts can also include the creation of accounts with email providers, which may be directly leveraged for [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Phishing](https://attack.mitre.org/techniques/T1566).(Citation: Mandiant APT1) In addition, establishing accounts may allow adversaries to abuse free services, such as registering for trial periods to [Acquire Infrastructure](https://attack.mitre.org/techniques/T1583) for malicious purposes.(Citation: Free Trial PurpleUrchin)

Name

Upload Tool

ID

T1608.002

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. Tools can be used for malicious purposes by an adversary, but (unlike malware) were not intended to be used for those purposes (ex: [PsExec](https://attack.mitre.org/software/S0029)). Adversaries may upload tools to support their operations, such as making a tool available to a victim network to enable [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) by placing it on an Internet accessible web server. Tools may be placed on infrastructure that was previously purchased/rented by the adversary ([Acquire Infrastructure](https://attack.mitre.org/techniques/T1583)) or was otherwise compromised by them ([Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)). (Citation: Dell TG-3390) Tools can also be staged on web services, such as an adversary controlled GitHub repo, or on Platform-as-a-Service offerings that enable users to easily provision applications.(Citation: Dragos Heroku Watering Hole)(Citation: Malwarebytes Heroku Skimmers)(Citation: Intezer App Service Phishing) Adversaries can avoid the need to upload a tool by having compromised victim machines download the tool directly from a third-party hosting location (ex: a non-adversary controlled GitHub repo), including the original hosting site of the tool.

Name

Upload Malware

ID

T1608.001

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. Adversaries may upload malware to support their operations, such as making a payload available to a victim network to enable [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) by placing it on an Internet accessible web server. Malware may be placed on infrastructure that was previously purchased/rented by the adversary ([Acquire Infrastructure](https://attack.mitre.org/techniques/T1583)) or was otherwise compromised by them ([Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)). Malware can also be staged on web services, such as GitHub or Pastebin, or hosted on the InterPlanetary File System (IPFS), where decentralized content storage makes the removal of malicious files difficult.(Citation: Volexity Ocean Lotus November 2020)(Citation: Talos IPFS 2022) Adversaries may upload backdoored files, such as application binaries, virtual machine images, or container images, to third-party software stores or repositories (ex: GitHub, CNET, AWS Community AMIs, Docker Hub). By chance encounter, victims may directly download/install these backdoored files via [User Execution](https://attack.mitre.org/techniques/T1204). [Masquerading](https://attack.mitre.org/techniques/T1036) may increase the chance of users mistakenly executing these files.

Name

Exfiltration to Cloud Storage

ID

T1567.002

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. Examples of cloud storage services include Dropbox and Google Docs. Exfiltration to these cloud storage services can provide a significant amount of cover to the adversary if hosts within the network are already communicating with the service.

Name

T1059

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Indicator

Name
7-zip.tw
Pattern Type
stix
Pattern
[domain-name:value = '7-zip.tw']
Name
97551bd3ff8357831dc2b6d9e152c8968d9ce1cd0090b9683c38ea52c2457824
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '97551bd3ff8357831dc2b6d9e152c8968d9ce1cd0090b9683c38ea52c2457824']
Name

a76507b51d84708c02ca2bd5a5775c47096bc740c9f7989afd6f34825edfcba6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a76507b51d84708c02ca2bd5a5775c47096bc740c9f7989afd6f34825edfcba6']

Name

89.42.178.13

Pattern Type

stix

Pattern

[ipv4-addr:value = '89.42.178.13']

Name

http://7-zip.tw/a/7z2301.msi

Pattern Type

stix

Pattern

[url:value = 'http://7-zip.tw/a/7z2301.msi']

Name

527fada7052b955ffa91df3b376cc58d387b39f2f44ebdcb54bc134e112a1c14

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '527fada7052b955ffa91df3b376cc58d387b39f2f44ebdcb54bc134e112a1c14']

Name

30sof.onedumb.com

Pattern Type

stix

Pattern

[hostname:value = '30sof.onedumb.com']

Name

9f61ed14660d8f85d606605d1c4c23849bd7a05afd02444c3b33e3af591cfdc9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9f61ed14660d8f85d606605d1c4c23849bd7a05afd02444c3b33e3af591cfdc9']

Name

157.245.159.135

Pattern Type

stix

Pattern

[ipv4-addr:value = '157.245.159.135']

Name

f1ccd604fcdc0034d94e575b3709cd124e13389bbee55c59cbbf7d4f3476e214

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f1ccd604fcdc0034d94e575b3709cd124e13389bbee55c59cbbf7d4f3476e214']

Name

582b21409ee32ffca853064598c5f72309247ad58640e96287bb806af3e7bede

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '582b21409ee32ffca853064598c5f72309247ad58640e96287bb806af3e7bede']

Name

fd9fc13dbd39f920c52fbc917d6c9ce0a28e0d049812189f1bb887486caedbeb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fd9fc13dbd39f920c52fbc917d6c9ce0a28e0d049812189f1bb887486caedbeb']

Name

103.255.178.200

Pattern Type

stix

Pattern

[ipv4-addr:value = '103.255.178.200']

Name

4057534799993a63f41502ec98181db0898d1d82df0d7902424a1899f8f7f9d2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4057534799993a63f41502ec98181db0898d1d82df0d7902424a1899f8f7f9d2']

Name

79e56dc69ca59b99f7ebf90a863f5351570e3709ead07fe250f31349d43391e6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '79e56dc69ca59b99f7ebf90a863f5351570e3709ead07fe250f31349d43391e6']

Name

http://7-zip.tw/a/7z2301-x64.msi

Pattern Type

stix

Pattern

[url:value = 'http://7-zip.tw/a/7z2301-x64.msi']

Name

ab6a684146cec59ec3a906d9e018b318fb6452586e8ec8b4e37160bcb4adc985

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'ab6a684146cec59ec3a906d9e018b318fb6452586e8ec8b4e37160bcb4adc985']
Name
d728cdcf62b497362a1ba9dbaac5e442cebe86145734410212d323a6c2959f0f
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'd728cdcf62b497362a1ba9dbaac5e442cebe86145734410212d323a6c2959f0f']
Name
f69fb19604362c5e945d8671ce1f63bb1b819256f51568daff6fed6b5cc2f274
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'f69fb19604362c5e945d8671ce1f63bb1b819256f51568daff6fed6b5cc2f274']

Name
45a5dd715dc5f08f3b987a0415c2e500c549508aadf4183fdb94f749af8f1d67
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '45a5dd715dc5f08f3b987a0415c2e500c549508aadf4183fdb94f749af8f1d67']

Intrusion-Set

Name
Harvester

Country

Name
Taiwan
Name
Hong Kong
Name
Virgin Islands, U.S.
Name
Ukraine

Region

Name
Europe
Name
Asia
Name
Eastern Europe
Name
Eastern Asia

Malware

Name
BirdyClient
Name
GoGra
Name
Backdoor.Graphican
Name
Graphite
Name
MoonTag
Name
Grager
Name
Graphon

Name
OneDriveTools

uses

Name
Name
Name
Name
Name
Name

targets

Name
Name
Name
Name
Name

indicates

Name
Name
Name
Name
Name
Name
Name
Name
Name
Name

Name
Name
Name
Name
Name
Name
Name
Name
Name
Name
Name
Name

Name
Name
Name
Name
Name
Name
Name

located-at

Name

based-on

Name

Domain-Name

Value
7-zip.tw

StixFile

Value
79e56dc69ca59b99f7ebf90a863f5351570e3709ead07fe250f31349d43391e6
d728cdcf62b497362a1ba9dbaac5e442cebe86145734410212d323a6c2959f0f
45a5dd715dc5f08f3b987a0415c2e500c549508aadf4183fdb94f749af8f1d67
40575347999993a63f41502ec98181db0898d1d82df0d7902424a1899f8f7f9d2
9f61ed14660d8f85d606605d1c4c23849bd7a05afd02444c3b33e3af591cfdc9
a76507b51d84708c02ca2bd5a5775c47096bc740c9f7989afd6f34825edfcba6
ab6a684146cec59ec3a906d9e018b318fb6452586e8ec8b4e37160bcb4adc985
582b21409ee32ffca853064598c5f72309247ad58640e96287bb806af3e7bede
f69fb19604362c5e945d8671ce1f63bb1b819256f51568daff6fed6b5cc2f274
527fada7052b955ffa91df3b376cc58d387b39f2f44ebdcb54bc134e112a1c14
fd9fc13dbd39f920c52fbc917d6c9ce0a28e0d049812189f1bb887486caedbeb
97551bd3ff8357831dc2b6d9e152c8968d9ce1cd0090b9683c38ea52c2457824
f1ccd604fcdc0034d94e575b3709cd124e13389bbee55c59cbbf7d4f3476e214

Hostname

Value
30sof.onedumb.com

IPv4-Addr

Value
89.42.178.13
103.255.178.200
157.245.159.135

External References

- https://symantec-enterprise-blogs.security.com/threat-intelligence/cloud-espionage-attacks
- https://otx.alienvault.com/pulse/66b3580bcb0f4106534933ef