Aug 09 2024

NETMANAGEIT

Intelligence Report

Hackers Leveraging OneDrive Or Google Drive To Hide Malicious Traffic

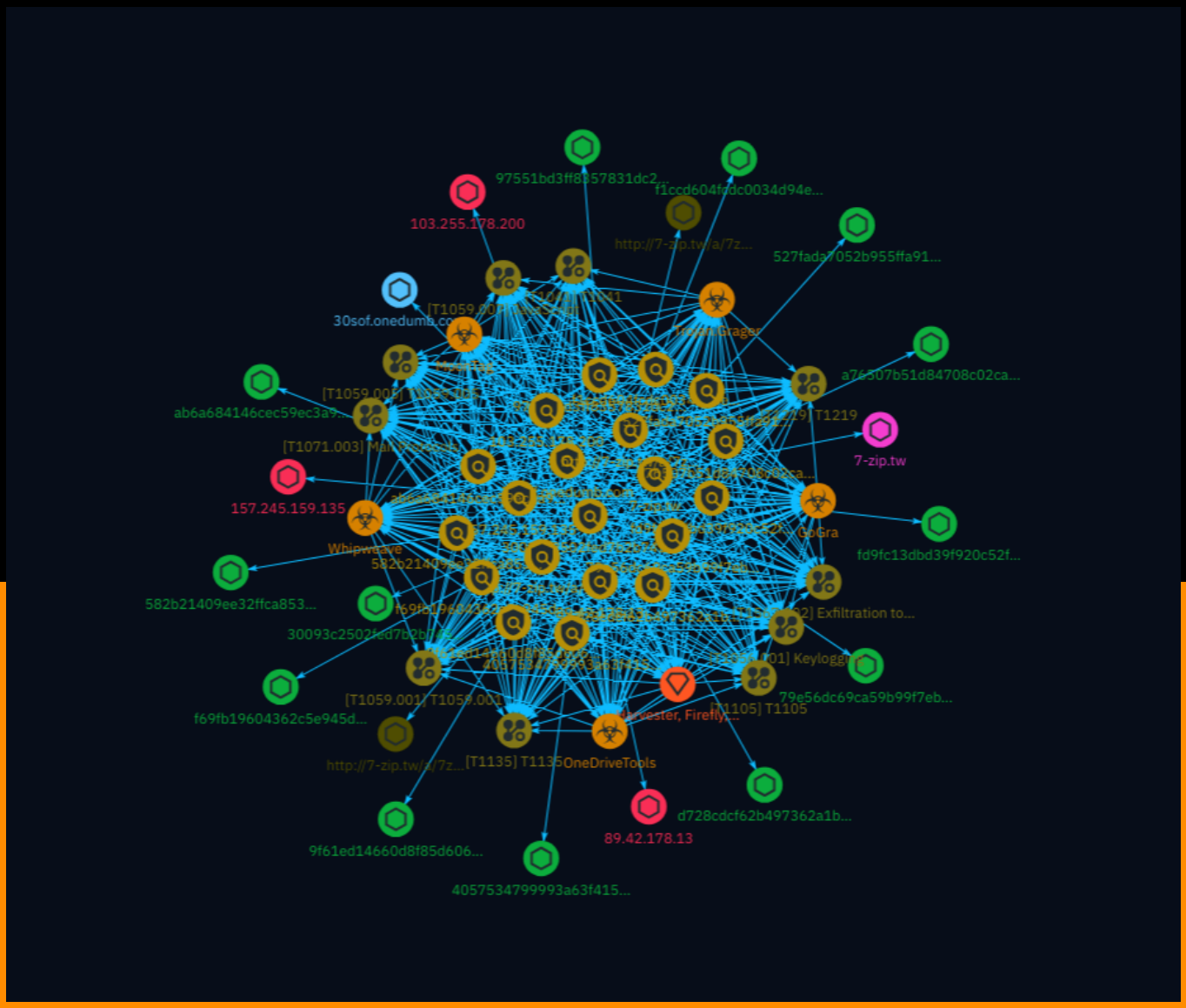

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Cyber threat actors, including nation-state groups, are utilizing legitimate cloud services like Microsoft OneDrive and Google Drive for covert operations. These services evade detection by masquerading as trusted entities, enabling data exfiltration and tool deployment. A new Go-based backdoor, GoGra, employed the Microsoft Graph API for command and control against a South Asian media organization. The Firefly group used a custom Python wrapper for a Google Drive client to exfiltrate sensitive data from a Southeast Asian military. Other malware families like Trojan.Grager, MoonTag, and OneDriveTools also leveraged cloud services for command and control infrastructure.

Confidence

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

100 / 100

Content

N/A

Attack-Pattern

Name
JavaScript
ID
T1059.007
Description
Adversaries may abuse various implementations of JavaScript for execution. JavaScript (JS) is a platform-independent scripting language (compiled just-in-time at runtime) commonly associated with scripts in webpages, though JS can be executed in runtime environments outside the browser.(Citation: NodeJS) JScript is the Microsoft implementation of the same scripting standard. JScript is interpreted via the Windows Script engine and thus integrated with many components of Windows such as the [Component Object Model](https://attack.mitre.org/techniques/T1559/001) and Internet Explorer HTML Application (HTA) pages.(Citation: JScrip May 2018)(Citation: Microsoft JScript 2007)(Citation: Microsoft Windows Scripts) JavaScript for Automation (JXA) is a macOS scripting language based on JavaScript, included as part of Apple's Open Scripting Architecture (OSA), that was introduced in OSX 10.10. Apple's OSA provides scripting capabilities to control applications, interface with the operating system, and bridge access into the rest of Apple's internal APIs. As of OSX 10.10, OSA only supports two languages, JXA and [AppleScript](https://attack.mitre.org/techniques/T1059/002). Scripts can be executed via the command line utility `osascript`, they can be compiled into applications or script files via `osacompile`, and they can be compiled and executed in memory of other programs by leveraging the OSAKit Framework.(Citation: Apple About Mac Scripting 2016) (Citation: SpecterOps JXA 2020)(Citation: SentinelOne macOS Red Team)(Citation: Red Canary Silver Sparrow Feb2021)(Citation: MDSec macOS JXA and VSCode) Adversaries may abuse various implementations of JavaScript to execute various behaviors. Common uses include hosting malicious scripts on websites as part of a [Drive-by Compromise](https://

attack.mitre.org/techniques/T1189) or downloading and executing these script files as secondary payloads. Since these payloads are text-based, it is also very common for adversaries to obfuscate their content as part of [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027).

Name

Keylogging

ID

T1056.001

Description

Adversaries may log user keystrokes to intercept credentials as the user types them. Keylogging is likely to be used to acquire credentials for new access opportunities when [OS Credential Dumping](https://attack.mitre.org/techniques/T1003) efforts are not effective, and may require an adversary to intercept keystrokes on a system for a substantial period of time before credentials can be successfully captured. In order to increase the likelihood of capturing credentials quickly, an adversary may also perform actions such as clearing browser cookies to force users to reauthenticate to systems. (Citation: Talos Kimsuky Nov 2021) Keylogging is the most prevalent type of input capture, with many different ways of intercepting keystrokes.(Citation: Adventures of a Keystroke) Some methods include: * Hooking API callbacks used for processing keystrokes. Unlike [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004), this focuses solely on API functions intended for processing keystroke data. * Reading raw keystroke data from the hardware buffer. * Windows Registry modifications. * Custom drivers. * [Modify System Image](https://attack.mitre.org/techniques/T1601) may provide adversaries with hooks into the operating system of network devices to read raw keystrokes for login sessions.(Citation: Cisco Blog Legacy Device Attacks)

Name

T1059.001

ID

T1059.001

Description

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.(Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems). PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk. A number of PowerShell-based offensive testing tools are available, including [Empire](https://attack.mitre.org/software/S0363), [PowerSploit](https://attack.mitre.org/software/S0194), [PoshC2](https://attack.mitre.org/software/S0378), and PSAttack.(Citation: Github PSAttack) PowerShell commands/scripts can also be executed without directly invoking the `powershell.exe` binary through interfaces to PowerShell's underlying `System.Management.Automation` assembly DLL exposed through the .NET framework and Windows Common Language Interface (CLI).(Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS Dec 2015)(Citation: Microsoft PSfromCsharp APR 2014)

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

T1105

ID

T1105

Description

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)). On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands such as `IEX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`. (Citation: t1105_lolbas) Adversaries may also abuse installers and package managers, such as `yum` or `winget`, to download tools to victim hosts. Adversaries have also abused file application features, such as the Windows `search-ms` protocol handler, to deliver malicious files to victims through remote file searches invoked by [User Execution](https://attack.mitre.org/techniques/T1204) (typically after interacting with [Phishing](https://attack.mitre.org/techniques/T1566) lures).(Citation: T1105: Trellix_search-ms) Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) In some cases, adversaries may be able to leverage services that sync between a web-based and an on-premises client, such as Dropbox or OneDrive, to transfer files onto victim systems. For example, by compromising a cloud account and logging into the service's web portal, an adversary may be able to trigger an automatic syncing process that transfers the file onto the victim's machine.(Citation: Dropbox Malware Sync)

Name

T1219

ID

T1219

Description

An adversary may use legitimate desktop support and remote access software to establish an interactive command and control channel to target systems within networks. These services, such as `VNC`, `Team Viewer`, `AnyDesk`, `ScreenConnect`, `LogMein`, `AmmyyAdmin`, and other remote monitoring and management (RMM) tools, are commonly used as legitimate technical support software and may be allowed by application control within a target environment.(Citation: Symantec Living off the Land)(Citation: CrowdStrike 2015 Global Threat Report)(Citation: CrySyS Blog TeamSpy) Remote access software may be installed and used post-compromise as an alternate communications channel for redundant access or as a way to establish an interactive remote desktop session with the target system. They may also be used as a component of malware to establish a reverse connection or back-connect to a service or adversary-controlled system. Adversaries may similarly abuse response features included in EDR and other defensive tools that enable remote access. Installation of many remote access software may also include persistence (e.g., the software's installation routine creates a [Windows Service](https://attack.mitre.org/techniques/T1543/003)). Remote access modules/features may also exist as part of otherwise existing software (e.g., Google Chrome’s Remote Desktop).(Citation: Google Chrome Remote Desktop)(Citation: Chrome Remote Desktop)

Name

T1059.005

ID

T1059.005

Description

Adversaries may abuse Visual Basic (VB) for execution. VB is a programming language created by Microsoft with interoperability with many Windows technologies such as [Component Object Model](https://attack.mitre.org/techniques/T1559/001) and the [Native API](https://attack.mitre.org/techniques/T1106) through the Windows API. Although tagged

as legacy with no planned future evolutions, VB is integrated and supported in the .NET Framework and cross-platform .NET Core.(Citation: VB .NET Mar 2020)(Citation: VB Microsoft) Derivative languages based on VB have also been created, such as Visual Basic for Applications (VBA) and VBScript. VBA is an event-driven programming language built into Microsoft Office, as well as several third-party applications.(Citation: Microsoft VBA) (Citation: Wikipedia VBA) VBA enables documents to contain macros used to automate the execution of tasks and other functionality on the host. VBScript is a default scripting language on Windows hosts and can also be used in place of [JavaScript](https://attack.mitre.org/techniques/T1059/007) on HTML Application (HTA) webpages served to Internet Explorer (though most modern browsers do not come with VBScript support). (Citation: Microsoft VBScript) Adversaries may use VB payloads to execute malicious commands. Common malicious usage includes automating execution of behaviors with VBScript or embedding VBA content into [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001) payloads (which may also involve [Mark-of-the-Web Bypass](https://attack.mitre.org/techniques/T1553/005) to enable execution).(Citation: Default VBS macros Blocking)

Name

Mail Protocols

ID

T1071.003

Description

Adversaries may communicate using application layer protocols associated with electronic mail delivery to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Protocols such as SMTP/S, POP3/S, and IMAP that carry electronic mail may be very common in environments. Packets produced from these protocols may have many fields and headers in which data can be concealed. Data could also be concealed within the email messages themselves. An adversary may abuse these protocols to communicate with systems under their control within a victim network while also mimicking normal, expected traffic. (Citation: FireEye APT28)

Name

T1135

ID

T1135

Description

Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement. Networks often contain shared network drives and folders that enable users to access file directories on various systems across a network. File sharing over a Windows network occurs over the SMB protocol. (Citation: Wikipedia Shared Resource) (Citation: TechNet Shared Folder) [Net](https://attack.mitre.org/software/S0039) can be used to query a remote system for available shared drives using the `net view \\\\remotesystem` command. It can also be used to query shared drives on the local system using `net share`. For macOS, the `sharing -l` command lists all shared points used for smb services.

Name

T1041

ID

T1041

Description

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

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

30093c2502fed7b2b74597d06b91f57772f2ae50ac420bcaa627038af33a6982

Pattern Type

stix

Pattern
[file:hashes.'SHA-256' = '30093c2502fed7b2b74597d06b91f57772f2ae50ac420bcaa627038af33a6982']
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']

Intrusion-Set

Name
Harvester, Firefly, UNC5330

Malware

Name
GoGra
Name
Trojan.Grager
Name
MoonTag
Name
Whipweave
Name
OneDriveTools

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
Name
Name
Name
Name
Name

Name
Name
Name
Name
Name
Name

uses

Name
Name
Name
Name
Name
Name
Name
Name
Name

based-on

Name

Domain-Name

Value
7-zip.tw

StixFile

Value
79e56dc69ca59b99f7ebf90a863f5351570e3709ead07fe250f31349d43391e6
d728cdcf62b497362a1ba9dbaac5e442cebe86145734410212d323a6c2959f0f
30093c2502fed7b2b74597d06b91f57772f2ae50ac420bcaa627038af33a6982
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://cybersecuritynews.com/hackers-onedrive-google-drive-malicious-traffic/
- https://otx.alienvault.com/pulse/66b39c9e7694a28382910cfa