Nov 28 2023

NETMANAGEIT

Intelligence Report

The Mahagrass Organization (APT-Q-36) uses the Spyder downloader to deliver the Remcos Trojan

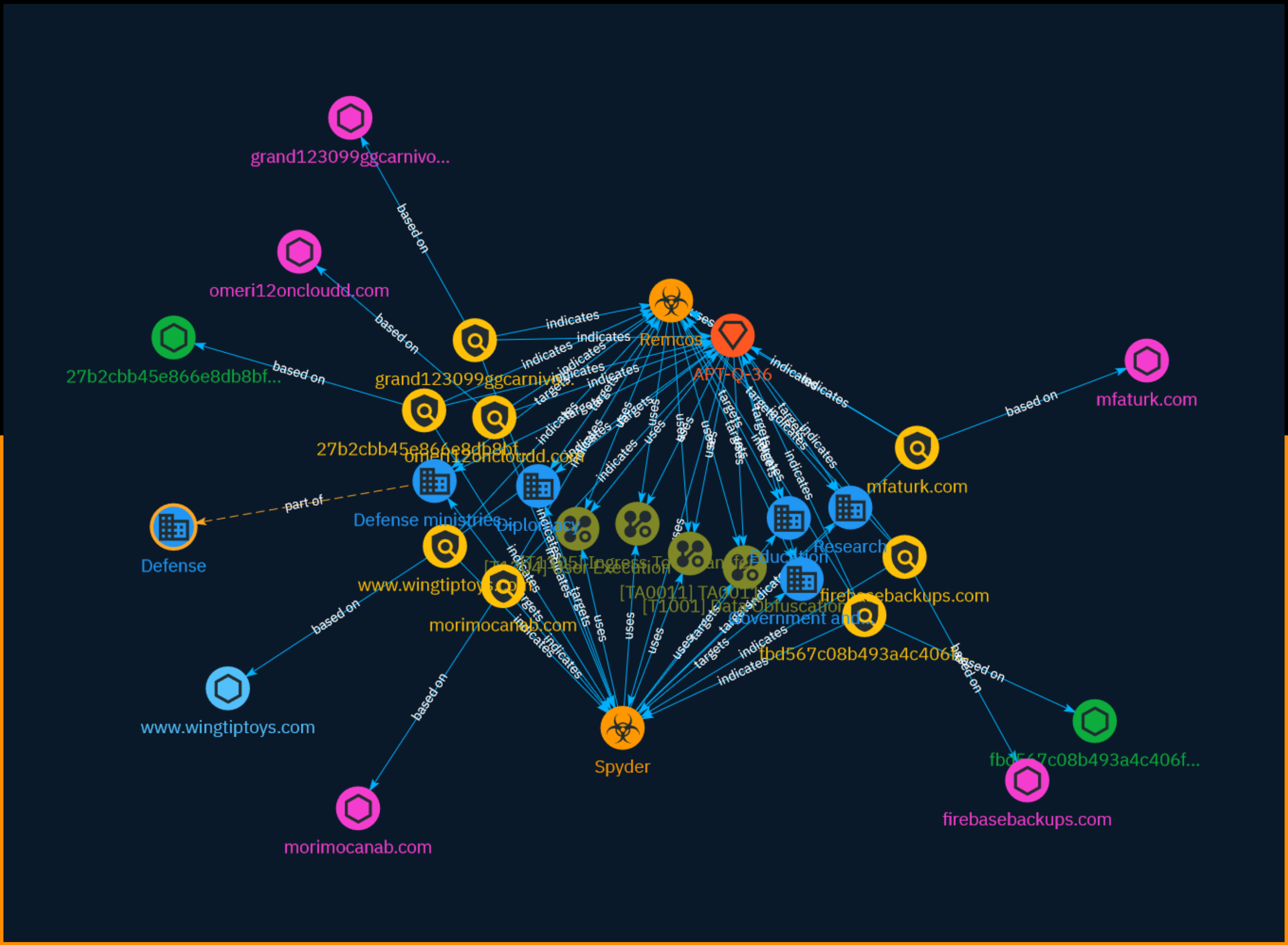

Table of contents

Overview

Entities

Observables

External References

Overview

Description

In just a few months, the Spyder downloader has undergone several updates, which shows the determination of the attack group to avoid detection by security protection software and complete the task of stealing intelligence, according to MP Weixin.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name

Data Obfuscation

ID

T1001

Description

Adversaries may obfuscate command and control traffic to make it more difficult to detect. Command and control (C2) communications are hidden (but not necessarily encrypted) in an attempt to make the content more difficult to discover or decipher and to make the communication less conspicuous and hide commands from being seen. This encompasses many methods, such as adding junk data to protocol traffic, using steganography, or impersonating legitimate protocols.

Name

User Execution

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Name

Ingress Tool Transfer

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. 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
TA0011

ID
TA0011

Sector

Name
Diplomacy
Description
Public or private entities which are actors of or involved in international relations activities.
Name
Research
Description
Private and public entities such as university research centers, labs, experimental centers etc. (except for defense, diplomacy and healthcare).
Name
Defense ministries (including the military)
Description
Includes the military and all defense related-space activities.
Name

Education

Description

Public or private entities operating to facilitate learning and acquiring knowledge and skills, composed of infrastructures and services to host teachers, students, and administrative services related to this activity. This does not include research activities.

Name

Government and administrations

Description

Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.

Name

Defense

Description

Public and private entities involved in the conception and production of weapons and the planning and conducting of military operations.

Indicator

Name

morimocanab.com

Pattern Type

stix

Pattern

[domain-name:value = 'morimocanab.com']

Name

27b2cbb45e866e8db8bf8933d6749164dc97995351704f0d33f62982a9abf955

Description

SHA256 of 68f4f27219840b4ba86462241f740bbd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '27b2cbb45e866e8db8bf8933d6749164dc97995351704f0d33f62982a9abf955']

Name

mfaturk.com

Pattern Type

stix

Pattern

[domain-name:value = 'mfaturk.com']

Name

grand123099ggcarnivol.com

Pattern Type

stix

Pattern

[domain-name:value = 'grand123099ggcarnivol.com']

Name

omeri12oncloudd.com

Pattern Type

stix

Pattern

[domain-name:value = 'omeri12oncloudd.com']

Name

fbd567c08b493a4c406fcd4d9a6d7403dc572f9b4c50fc4a56d37982c25dc457

Description

SHA256 of 2491942d8cd5807cd4615a07ad26a54a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fbd567c08b493a4c406fcd4d9a6d7403dc572f9b4c50fc4a56d37982c25dc457']

Name

www.wingtiptoys.com

Pattern Type

stix

Pattern

[hostname:value = 'www.wingtiptoys.com']

Name

firebasebackups.com

Pattern Type

stix

Pattern

[domain-name:value = 'firebasebackups.com']

Intrusion-Set

Name
APT-Q-36

Malware

Name
Spyder

Name
Remcos

Domain-Name

Value
morimocanab.com
grand123099ggcarnivol.com
firebasebackups.com
omeri12oncloudd.com
mfaturk.com

StixFile

Value
27b2cbb45e866e8db8bf8933d6749164dc97995351704f0d33f62982a9abf955
fbd567c08b493a4c406fcd4d9a6d7403dc572f9b4c50fc4a56d37982c25dc457

Hostname

Value
www.wingtiptoys.com

External References

- https://otx.alienvault.com/pulse/6566312bddcfb0e7f0991687
- https://mp.weixin.qq.com/s?__biz=MzI2MDc2MDA4OA==&mid=2247508856&idx=1&sn=256ab2e8e63a406a37088f1b133eb6ff&chksm=ea66540f