Apr 19 2024

NETMANAGEIT

Intelligence Report

Analysis of the APT31 indictment

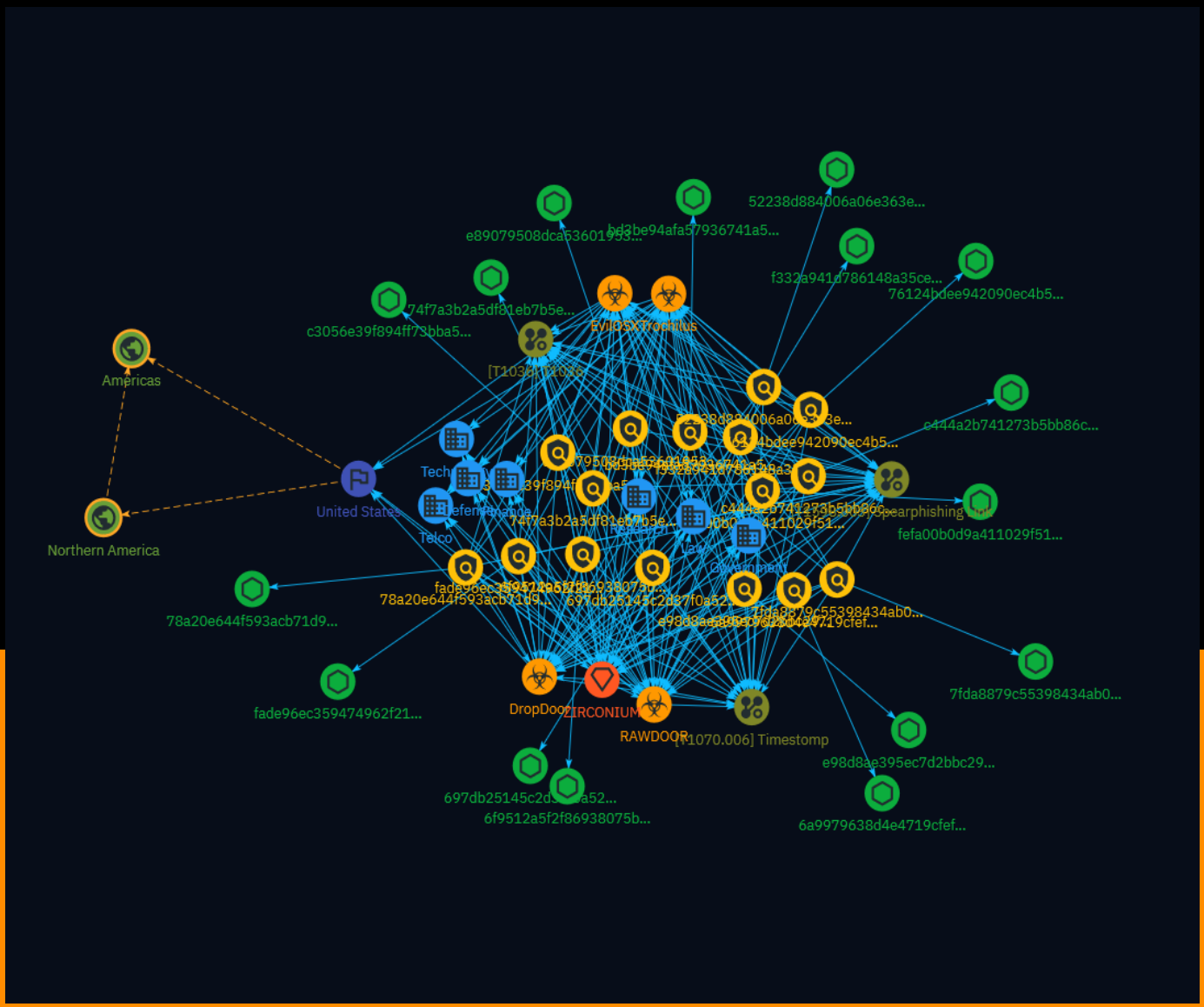

Table of contents

Overview

- Description 4
- Confidence 4
- Content 5

Entities

- Indicator 6
- Malware 13
- Sector 14
- Intrusion-Set 16
- Attack-Pattern 17
- Country 20
- Region 21

Observables

- StixFile 22

External References

- External References 24

Overview

Description

The U.S. Department of Justice released an indictment of seven hackers associated with APT31, a hacking group supporting China's Ministry of State Security active for 14 years. The indictment reveals APT31 tradecraft including: front companies, malware like RAWDOOR, two-phase attacks via email tracking then exploitation, compromising subsidiaries for access, and quickly shifting targets based on political events.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

fefa00b0d9a411029f51f34bfa4ed2327559edfcd4fad5cfc1234c1c01a97c5a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fefa00b0d9a411029f51f34bfa4ed2327559edfcd4fad5cfc1234c1c01a97c5a']

Name

fade96ec359474962f2167744ca8c55ab4e6d0700faa142b3d95ec3f4765023b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fade96ec359474962f2167744ca8c55ab4e6d0700faa142b3d95ec3f4765023b']

Name

f332a941d786148a35cec683edb965ea4bbd6ff6bd871880f30dc7d42b922443

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f332a941d786148a35cec683edb965ea4bbd6ff6bd871880f30dc7d42b922443']

Name

e98d8ae395ec7d2bbc29c21fa2bf79e26ada9d8bd5098487027b32aeae8b03b7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e98d8ae395ec7d2bbc29c21fa2bf79e26ada9d8bd5098487027b32aeae8b03b7']

Name

e89079508dca536019535bb021ae388a990d9cb64e1e6bd769e6a29ec237d8be

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e89079508dca536019535bb021ae388a990d9cb64e1e6bd769e6a29ec237d8be']

Name

c444a2b741273b5bb86c5197d931cbd3b121043e6e6cb5604b02719415d92b08

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c444a2b741273b5bb86c5197d931cbd3b121043e6e6cb5604b02719415d92b08']

Name

bd3be94afa57936741a5debde1eff537dcd7c7bc79ccfa9739c4614efc424eeb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bd3be94afa57936741a5debde1eff537dcd7c7bc79ccfa9739c4614efc424eeb']

Name

c3056e39f894ff73bba528faac04a1fc86deeec57641ad882000d7d40e5874be

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c3056e39f894ff73bba528faac04a1fc86deeec57641ad882000d7d40e5874be']

Name

7fda8879c55398434ab0f423b0f1c75658bddd925d90437ad2e6fd8723cb1d78

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7fda8879c55398434ab0f423b0f1c75658bddd925d90437ad2e6fd8723cb1d78']

Name

78a20e644f593acb71d94be96ed1e3a9ba7515be2c50aef844277a9e5c03637a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '78a20e644f593acb71d94be96ed1e3a9ba7515be2c50aef844277a9e5c03637a']

Name

76124bdee942090ec4b5f2a7e08ffe6dae758bc747d6565f6c5941ab81d79044

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '76124bdee942090ec4b5f2a7e08ffe6dae758bc747d6565f6c5941ab81d79044']

Name

74f7a3b2a5df81eb7b5e0c5c4af8548e61dc37c608dda458b75b58852f2f2cfd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '74f7a3b2a5df81eb7b5e0c5c4af8548e61dc37c608dda458b75b58852f2f2cfd']

Name

6f9512a5f2f86938075b14e34928d07cdc78f46ed9401dea799f131f7a3d9644

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6f9512a5f2f86938075b14e34928d07cdc78f46ed9401dea799f131f7a3d9644']

Name

6a9979638d4e4719cfef65bdd6e1d7c0b28b84df9ca73a3bc1e919e9a1df50df

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6a9979638d4e4719cfef65bdd6e1d7c0b28b84df9ca73a3bc1e919e9a1df50df']

Name

697db25145c2d37f0a521b3ca6b49f1f4d7c3e0c2e57804f5317b3d0b6d242fb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '697db25145c2d37f0a521b3ca6b49f1f4d7c3e0c2e57804f5317b3d0b6d242fb']

Name

52238d884006a06e363e546dcfa88c1b2cbdadd80c717e415ac26956900f40bf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '52238d884006a06e363e546dcfa88c1b2cbdadd80c717e415ac26956900f40bf']

Malware

Name
DropDoor
Name
EvilOSX
Name
RAWDOOR
Name
Trochilus

Sector

Name
Telco
Name
Research
Description
Private and public entities such as university research centers, labs, experimental centers etc. (except for defense, diplomacy and healthcare).
Name
Law
Description
All judicial activities of the state and related private entities.
Name
Technology
Description

Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.

Name

Government

Description

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

Name

Finance

Description

Public and private entities involved in the allocation of assets and liabilities over space and time.

Name

Defense

Description

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

Intrusion-Set

Name
ZIRCONIUM

Description
[ZIRCONIUM](https://attack.mitre.org/groups/G0128) is a threat group operating out of China, active since at least 2017, that has targeted individuals associated with the 2020 US presidential election and prominent leaders in the international affairs community. (Citation: Microsoft Targeting Elections September 2020)(Citation: Check Point APT31 February 2021)

Attack-Pattern

Name
Timestomp
ID
T1070.006
Description
Adversaries may modify file time attributes to hide new or changes to existing files. Timestomping is a technique that modifies the timestamps of a file (the modify, access, create, and change times), often to mimic files that are in the same folder. This is done, for example, on files that have been modified or created by the adversary so that they do not appear conspicuous to forensic investigators or file analysis tools. Timestomping may be used along with file name [Masquerading](https://attack.mitre.org/techniques/T1036) to hide malware and tools.(Citation: WindowsIR Anti-Forensic Techniques)
Name
T1036
ID
T1036
Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

Name

Spearphishing Link

ID

T1598.003

Description

Adversaries may send spearphishing messages with a malicious link to elicit sensitive information that can be used during targeting. Spearphishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Spearphishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)) and/or sending multiple, seemingly urgent messages. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, the malicious emails contain links generally accompanied by social engineering text to coax the user to actively click or copy and paste a URL into a browser.(Citation: TrendMictro Phishing) (Citation: PCMag FakeLogin) The given website may be a clone of a legitimate site (such as an online or corporate login portal) or may closely resemble a legitimate site in appearance and have a URL containing elements from the real site. URLs may also be obfuscated by taking advantage of quirks in the URL schema, such as the acceptance of integer- or hexadecimal-based hostname formats and the automatic discarding of text before an “@” symbol: for example, `hxxp://google.com@1157586937`.(Citation: Mandiant URL Obfuscation 2023) Adversaries may also link to "web bugs" or "web beacons" within phishing messages to verify the receipt of an email, while also potentially profiling and

tracking victim information such as IP address.(Citation: NIST Web Bug) Adversaries may also be able to spoof a complete website using what is known as a "browser-in-the-browser" (BitB) attack. By generating a fake browser popup window with an HTML-based address bar that appears to contain a legitimate URL (such as an authentication portal), they may be able to prompt users to enter their credentials while bypassing typical URL verification methods.(Citation: ZScaler BitB 2020)(Citation: Mr. D0x BitB 2022) Adversaries can use phishing kits such as `EvilProxy` and `Evilginx2` to proxy the connection between the victim and the legitimate website. On a successful login, the victim is redirected to the legitimate website, while the adversary captures their session cookie (i.e., [Steal Web Session Cookie](https://attack.mitre.org/techniques/T1539)) in addition to their username and password. This may enable the adversary to then bypass MFA via [Web Session Cookie] (https://attack.mitre.org/techniques/T1550/004).(Citation: Proofpoint Human Factor) From the fake website, information is gathered in web forms and sent to the adversary. Adversaries may also use information from previous reconnaissance efforts (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)) to craft persuasive and believable lures.

Country

Name
United States

Region

Name
Northern America

Name
Americas

StixFile

Value
fefa00b0d9a411029f51f34bfa4ed2327559edfcd4fad5cfc1234c1c01a97c5a
fade96ec359474962f2167744ca8c55ab4e6d0700faa142b3d95ec3f4765023b
f332a941d786148a35cec683edb965ea4bbd6ff6bd871880f30dc7d42b922443
e98d8ae395ec7d2bbc29c21fa2bf79e26ada9d8bd5098487027b32aeae8b03b7
e89079508dca536019535bb021ae388a990d9cb64e1e6bd769e6a29ec237d8be
c444a2b741273b5bb86c5197d931cbd3b121043e6e6cb5604b02719415d92b08
c3056e39f894ff73bba528faac04a1fc86deeec57641ad882000d7d40e5874be
bd3be94afa57936741a5debde1eff537dcd7c7bc79ccfa9739c4614efc424eeb
7fda8879c55398434ab0f423b0f1c75658bddd925d90437ad2e6fd8723cb1d78
78a20e644f593acb71d94be96ed1e3a9ba7515be2c50aef844277a9e5c03637a
76124bdee942090ec4b5f2a7e08ffe6dae758bc747d6565f6c5941ab81d79044
697db25145c2d37f0a521b3ca6b49f1f4d7c3e0c2e57804f5317b3d0b6d242fb
74f7a3b2a5df81eb7b5e0c5c4af8548e61dc37c608dda458b75b58852f2f2cfd

6f9512a5f2f86938075b14e34928d07cdc78f46ed9401dea799f131f7a3d9644

6a9979638d4e4719cfef65bdd6e1d7c0b28b84df9ca73a3bc1e919e9a1df50df

52238d884006a06e363e546dcfa88c1b2cbdadd80c717e415ac26956900f40bf

External References

- https://harfanglab.io/en/insidethelab/apt31-indictment-analysis/
- https://otx.alienvault.com/pulse/661e7f1cb38ad06fd3a91835