Jul 04 2023

NETMANAGEIT

Intelligence Report

The suspected Maha grass organization uses the WarHawk backdoor variant Spyder to spy on many countries

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Maha Grass, also known as Patchwork, White Elephant, Hangover, Dropping Elephant, etc., Qi Anxin internal tracking number APT-Q-36. The organization is generally considered to have a South Asian background. Its earliest attack activities can be traced back to November 2009, and it has been active for more than 10 years. The organization mainly conducts cyber espionage activities against countries in the Asian region, targeting organizations in the fields of government, military, electric power, industry, scientific research and education, diplomacy, and economy.

Confidence

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

15 / 100

Indicator

Name
http://alibababackupcloud.com/spyder/smile.php
Pattern Type
stix
Pattern
[url:value = 'http://alibababackupcloud.com/spyder/smile.php']
Name
137d47864fb79c1a892265690bc8c64d67945847058b5a49ad5785ac902ae105
Description
SHA256 of 53b3a018d1a4d935ea7dd7431374caf1
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = '137d47864fb79c1a892265690bc8c64d67945847058b5a49ad5785ac902ae105']

Name

http://cloudplatfromservice.one/cpidr/balloon.php

Pattern Type

stix

Pattern

[url:value = 'http://cloudplatfromservice.one/cpidr/balloon.php']

Name

http://alibababackupcloud.com/spyder/

Pattern Type

stix

Pattern

[url:value = 'http://alibababackupcloud.com/spyder/']

Name

cloudplatfromservice.one

Pattern Type

stix

Pattern

[domain-name:value = 'cloudplatfromservice.one']

Name

192.169.7.142

Description

ISP: QuadraNet Enterprises LLC **OS:** Windows Server 2022 (build 10.0.20348) ------------------------- Hostnames: - nordns.crowncloud.net ------------------------- Domains: - crowncloud.net ------------------------- Services: **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows Server 2022 OS Build: 10.0.20348 Target Name: WIN-G4QUV98HSF9 NetBIOS Domain Name: WIN-G4QUV98HSF9 NetBIOS Computer Name: WIN-G4QUV98HSF9 DNS Domain Name: WIN-G4QUV98HSF9 FQDN: WIN-G4QUV98HSF9 ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '192.169.7.142']

Name

39e62d69ec3da04c3a3778fcd8dfbfc75cce9ac1e62df75537cc1b022d951cf5

Description

ConventionEngine_Term_Desktop SHA256 of e3b37459489a863351d855e594df93bf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '39e62d69ec3da04c3a3778fcd8dfbfc75cce9ac1e62df75537cc1b022d951cf5']

Name

f5766ece18b863c7747d739b4a0b944cdb13e9993dbc3401d4ea1923dbb0578a

Description

SHA256 of eb9068161baa5842b40d5565130526b9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f5766ece18b863c7747d739b4a0b944cdb13e9993dbc3401d4ea1923dbb0578a']

Name

http://gclouddrives.com/spyder/

Pattern Type

stix

Pattern

[url:value = 'http://gclouddrives.com/spyder/']

Name

3b7336d5851a59a95680b6b15abff99f86c83ab53b0b11da952cf171c6ee9dd4

Description

SHA256 of 1f599f9ab4ce3da3c2b47b76d9f88850

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3b7336d5851a59a95680b6b15abff99f86c83ab53b0b11da952cf171c6ee9dd4']

Name

plainboardssixty.com

Pattern Type

stix

Pattern

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

Name

b41d54a9686b312f9e114f62e6bf11e21c8e97dda477d488ca19e2afa45efc9e

Description
SHA256 of 1f4b225813616fbb087ae211e9805baf
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'b41d54a9686b312f9e114f62e6bf11e21c8e97dda477d488ca19e2afa45efc9e']
Name
http://gclouddrives.com/spyder/smile.php
Pattern Type
stix
Pattern
[url:value = 'http://gclouddrives.com/spyder/smile.php']
Name
88c10674bb6a53791bfe08497948699bf57ea9980a878a3a5fc1afb160d1d234
Description
SHA256 of 87d94635372b874f18acb3af7c340357
Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '88c10674bb6a53791bfe08497948699bf57ea9980a878a3a5fc1afb160d1d234']

Name

gclouddrives.com

Pattern Type

stix

Pattern

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

Name

http://cloudplatfromservice.one/cpidr/

Pattern Type

stix

Pattern

[url:value = 'http://cloudplatfromservice.one/cpidr/']

Name

http://plainboardssixty.com/drive/bottom.php

Pattern Type

stix

Pattern

[url:value = 'http://plainboardssixty.com/drive/bottom.php']

Name

http://plainboardssixty.com/drive/chilli.php

Pattern Type

stix

Pattern

[url:value = 'http://plainboardssixty.com/drive/chilli.php']

Name

076eaa395b1c0b473b252a04f286ea504286cf67bf439bd1ade67051c4b24da3

Description

Win32/WarHawk SHA256 of 1fa3f364bcd02433bc0f4d3113714f16

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '076eaa395b1c0b473b252a04f286ea504286cf67bf439bd1ade67051c4b24da3']

Name

alibababackupcloud.com

Pattern Type

stix

Pattern

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

Name

http://plainboardssixty.com/drive/

Pattern Type

stix

Pattern

[url:value = 'http://plainboardssixty.com/drive/']

Malware

Name
WarHawk

Intrusion-Set

Name
Sidewinder

Description
[Sidewinder](https://attack.mitre.org/groups/G0121) is a suspected Indian threat actor group that has been active since at least 2012. They have been observed targeting government, military, and business entities throughout Asia, primarily focusing on Pakistan, China, Nepal, and Afghanistan.(Citation: ATT Sidewinder January 2021)(Citation: Securelist APT Trends April 2018)(Citation: Cyble Sidewinder September 2020)

Domain-Name

Value
gclouddrives.com
cloudplatfromservice.one
alibababackupcloud.com
plainboardssixty.com

StixFile

Value
076eaa395b1c0b473b252a04f286ea504286cf67bf439bd1ade67051c4b24da3
3b7336d5851a59a95680b6b15abff99f86c83ab53b0b11da952cf171c6ee9dd4
137d47864fb79c1a892265690bc8c64d67945847058b5a49ad5785ac902ae105
f5766ece18b863c7747d739b4a0b944cdb13e9993dbc3401d4ea1923dbb0578a
88c10674bb6a53791bfe08497948699bf57ea9980a878a3a5fc1afb160d1d234
b41d54a9686b312f9e114f62e6bf11e21c8e97dda477d488ca19e2afa45efc9e
39e62d69ec3da04c3a3778fcd8dfbfc75cce9ac1e62df75537cc1b022d951cf5

IPv4-Addr

Value
192.169.7.142

Url

Value
http://alibabab ackupcloud.com/spyder/smile.php
http://plainboardssixty.com/drive/
http://cloudplatfromservice.one/cpidr/balloon.php
http://cloudplatfromservice.one/cpidr/
http://gclouddrives.com/spyder/smile.php
http://gclouddrives.com/spyder/
http://plainboardssixty.com/drive/bottom.php
http://alibabab ackupcloud.com/spyder/
http://plainboardssixty.com/drive/chilli.php

External References

- https://otx.alienvault.com/pulse/64a445050a5e0f1018b5bf6d
- https://mp.weixin.qq.com/s/ewGyvlmWUD45XTVsoxeVpg