Sep 21 2023

NETMANAGEIT

Intelligence Report

Chinese Malware Appears in Earnest Across Cybercrime Threat

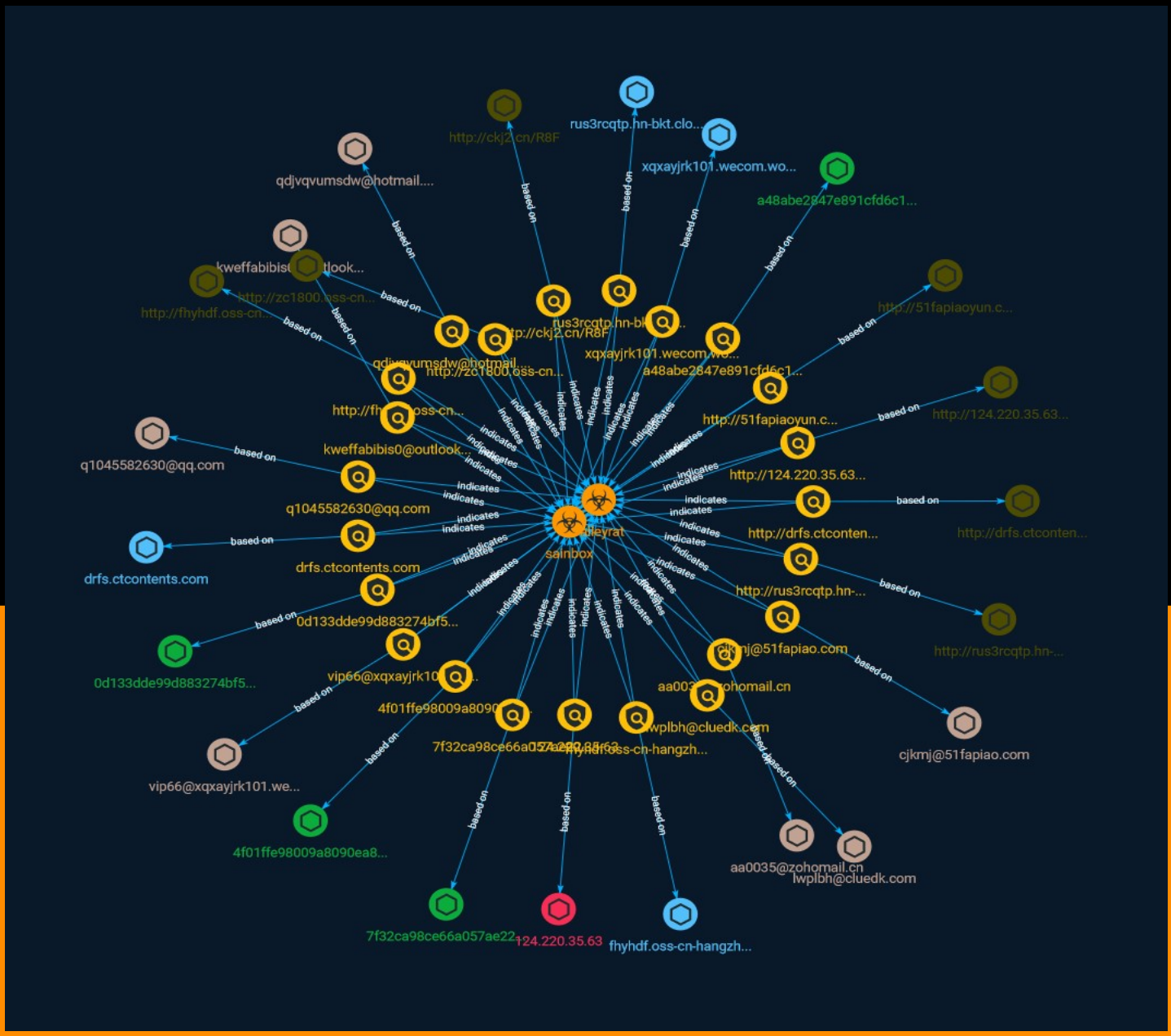

Table of contents

Overview

- Description 4
- Confidence 4

Entities

- Indicator 5
- Malware 14

Observables

- Email-Addr 15
- StixFile 16
- Hostname 17
- IPv4-Addr 18
- Url 19

External References

- External References 20

Overview

Description

Proofpoint recently observed a minor resurgence in the use of Sainbox and other Chinese-themed malware. Proofpoint research suggests that this activity does not seem to be related to a single entity but rather appears to be a cluster of activities based on temporal patterns. The appearance of ValleyRAT alongside the older families hints at the possibility of their relationship in terms of timing. Proofpoint anticipates ValleyRAT will be used more frequently in the future.

Confidence

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

15 / 100

Indicator

Name
vip66@xqxayjrk101.wecom.work
Pattern Type
stix
Pattern
[email-addr:value = 'vip66@xqxayjrk101.wecom.work']
Name
http://drfs.ctcontents.com/file/40788929/860577489/
Pattern Type
stix
Pattern
[url:value = 'http://drfs.ctcontents.com/file/40788929/860577489/']
Name
fhyhdf.oss-cn-hangzhou.aliyuncs.com

Pattern Type
stix
Pattern
[hostname:value = 'fhyhdf.oss-cn-hangzhou.aliyuncs.com']
Name
http://fhyhdf.oss-cn-hangzhou.aliyuncs.com/%E7%99%BC%E7%A5%A8.zip
Pattern Type
stix
Pattern
[url:value = 'http://fhyhdf.oss-cn-hangzhou.aliyuncs.com/%E7%99%BC%E7%A5%A8.zip']
Name
http://51fapiaoyun.com/%E5%8F%91-%E7%A5%A8.rar
Pattern Type
stix
Pattern
[url:value = 'http://51fapiaoyun.com/%E5%8F%91-%E7%A5%A8.rar']
Name
kweffabibis0@outlook.com

Pattern Type
stix
Pattern
[email-addr:value = 'kweffabibis0@outlook.com']
Name
4f01ffe98009a8090ea8a086d21c62c24219b21938ea3ec7da8072f8c4dcc7a6
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '4f01ffe98009a8090ea8a086d21c62c24219b21938ea3ec7da8072f8c4dcc7a6']
Name
124.220.35.63
Pattern Type
stix
Pattern
[ipv4-addr:value = '124.220.35.63']
Name

q1045582630@qq.com

Pattern Type

stix

Pattern

[email-addr:value = 'q1045582630@qq.com']

Name

http://124.220.35.63/laoxiang.exe

Pattern Type

stix

Pattern

[url:value = 'http://124.220.35.63/laoxiang.exe']

Name

http://ckj2.cn/R8F

Pattern Type

stix

Pattern

[url:value = 'http://ckj2.cn/R8F']

Name

a48abe2847e891cfd6c18c7cdaaa8e983051bc2f7a0bd9ef5c515a72954e1715

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a48abe2847e891cfd6c18c7cdaaa8e983051bc2f7a0bd9ef5c515a72954e1715']

Name

aa0035@zohomail.cn

Pattern Type

stix

Pattern

[email-addr:value = 'aa0035@zohomail.cn']

Name

0d133dde99d883274bf5644bd9e59af3c54c2b3c65f3d1bc762f2d3725f80582

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0d133dde99d883274bf5644bd9e59af3c54c2b3c65f3d1bc762f2d3725f80582']

Name

rus3rcqtp.hn-bkt.clouddn.com

Pattern Type

stix

Pattern

[hostname:value = 'rus3rcqtp.hn-bkt.clouddn.com']

Name

7f32ca98ce66a057ae226ec78638db95feebc59295d3afffdbf407df12b5bc79

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7f32ca98ce66a057ae226ec78638db95feebc59295d3afffdbf407df12b5bc79']

Name

http://zc1800.oss-cn-shenzhen.aliyuncs.com/piao

Pattern Type

stix

Pattern

[url:value = 'http://zc1800.oss-cn-shenzhen.aliyuncs.com/piao']

Name

cjkmj@51fapiao.com

Pattern Type

stix

Pattern

[email-addr:value = 'cjkmj@51fapiao.com']

Name

drfs.ctcontents.com

Pattern Type

stix

Pattern

[hostname:value = 'drfs.ctcontents.com']

Name

xqxayjrk101.wecom.work

Pattern Type

stix

Pattern

[hostname:value = 'xqxayjrk101.wecom.work']

Name

lwplbh@cluedk.com

Pattern Type

stix

Pattern

[email-addr:value = 'lwplbh@cluedk.com']

Name

qdjvqvumsdw@hotmail.com

Pattern Type

stix

Pattern

[email-addr:value = 'qdjvqvumsdw@hotmail.com']

Name

http://rus3rcqtp.hn-bkt.clouddn.com/26866498.zip

Pattern Type

stix

Pattern

```
[url:value = 'http://rus3rcqtp.hn-bkt.clouddn.com/26866498.zip']
```

Malware

Name
valleyrat

Name
sainbox

Email-Addr

Value
vip66@xqxayjrk101.wecom.work
kweffabibis0@outlook.com
cjkmj@51fapiao.com
aa0035@zohomail.cn
qdjvqvumsdw@hotmail.com
lwplbh@cluedk.com
q1045582630@qq.com

StixFile

Value
a48abe2847e891cfd6c18c7cdaaa8e983051bc2f7a0bd9ef5c515a72954e1715
4f01ffe98009a8090ea8a086d21c62c24219b21938ea3ec7da8072f8c4dcc7a6
7f32ca98ce66a057ae226ec78638db95feebc59295d3afffdbf407df12b5bc79
0d133dde99d883274bf5644bd9e59af3c54c2b3c65f3d1bc762f2d3725f80582

Hostname

Value
xqxayjrk101.wecom.work
drfs.ctcontents.com
rus3rcqtp.hn-bkt.clouddn.com
fhyhdf.oss-cn-hangzhou.aliyuncs.com

IPv4-Addr

Value
124.220.35.63

Url

Value
http://51fapiaoyun.com/%E5%8F%91-%E7%A5%A8.rar
http://drfs.ctcontents.com/file/40788929/860577489/
http://zc1800.oss-cn-shenzhen.aliyuncs.com/piao
http://ckj2.cn/R8F
http://rus3rcqtp.hn-bkt.clouddn.com/26866498.zip
http://fhyhdf.oss-cn-hangzhou.aliyuncs.com/%E7%99%BC%E7%A5%A8.zip
http://124.220.35.63/laoxiang.exe

External References

- https://otx.alienvault.com/pulse/650afba3f4c874c814429d65
- https://www.proofpoint.com/us/blog/threat-insight/chinese-malware-appears-earnest-across-cybercrime-threat-landscape