Jul 03 2023

NETMANAGEIT

Intelligence Report

GuLoader- or DBatLoader/ ModiLoader-style infection for Remcos RAT

Table of contents

Overview

Entities

Observables

External References

Overview

Description

SANS Institute analyses an infection for Remcos RAT.

Confidence

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

15 / 100

Indicator

Name
https://img.softmedal.com/uploads/2023-06-23/773918053744.jpg
Description
PDF document, version 1.5 afbfc145affa16280139a70e92364d8cc9d71b951d3258df9a9855c0c1f1f567
Pattern Type
stix
Pattern
[url:value = 'https://img.softmedal.com/uploads/2023-06-23/773918053744.jpg']
Name
748c0ef7a63980d4e8064b14fb95ba51947bfc7d9ccf39c6ef614026a89c39e5
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = '748c0ef7a63980d4e8064b14fb95ba51947bfc7d9ccf39c6ef614026a89c39e5']

Name

20230626050534.1c6fdebc3dc87bee@gbwhotel.com.my

Pattern Type

stix

Pattern

[email-addr:value = '20230626050534.1c6fdebc3dc87bee@gbwhotel.com.my']

Name

top1.banifabused1.xyz

Pattern Type

stix

Pattern

[hostname:value = 'top1.banifabused1.xyz']

Name

f3b62d90f02bbecd522049f9186c67d939b77e98449d63e73de4893060f1dd48

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f3b62d90f02bbecd522049f9186c67d939b77e98449d63e73de4893060f1dd48']

Name

d7b17df67410b8d408bb768c11757162a49cfb8602e50ac98283bfd49c54a9c5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd7b17df67410b8d408bb768c11757162a49cfb8602e50ac98283bfd49c54a9c5']

Name

1d030984aa406ff1a05c1d42e67455b79665d50ea98f49713b1fd21887b7b2eb

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1d030984aa406ff1a05c1d42e67455b79665d50ea98f49713b1fd21887b7b2eb']

Name

29c766c8910fa35b76bdea7738e32f51fc063bc01e8f557c1f309a4b07c47733

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '29c766c8910fa35b76bdea7738e32f51fc063bc01e8f557c1f309a4b07c47733']

Name

https://img.softmedal.com/uploads/2023-06-23/298186187297.jpg

Pattern Type

stix

Pattern

[url:value = 'https://img.softmedal.com/uploads/2023-06-23/298186187297.jpg']

Name

103.1.151.84

Description

ISP: Acme Commerce Sdb Bhd, Malayia, Network **OS:** None ---------- Hostnames: - mail.tasekmaju.com.my ---------- Domains: - tasekmaju.com.my ---------- Services: **21:** ``` 220 (vsFTPd 3.0.2) 530 Login incorrect. 530 Please login with USER and PASS. 211-Features: EPRT EPSV MDTM PASV REST STREAM SIZE TVFS UTF8 211 End ``` ---------- **25:** ``` 220 mail.tasekmaju.com.my ESMTP Exim 4.90_1 Wed, 28 Jun 2023 08:15:17 +0800 250-mail.tasekmaju.com.my Hello 224.0.242.22 [224.0.242.22] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-CHUNKING 250-STARTTLS 250 HELP ``` ---------- **53:** ``` get lost Resolver name: mail.tasekmaju.com.my ``` ---------- **53:** ``` get lost Resolver name: mail.tasekmaju.com.my ``` ---------- **80:** ``` HTTP/1.1 200 OK Server: nginx

Date: Sat, 24 Jun 2023 08:12:25 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 1061 Connection: keep-alive Keep-Alive: timeout=60 Last-Modified: Mon, 23 Jul 2018 06:35:04 GMT ETag: "425-571a4d87dd31e" Accept-Ranges: bytes ``` ---------- **465:** ``` 220 mail.tasekmaju.com.my ESMTP Exim 4.90_1 Wed, 28 Jun 2023 08:15:19 +0800 250-mail.tasekmaju.com.my Hello 224.114.129.132 [224.114.129.132] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-CHUNKING 250 HELP ``` HEARTBLEED: 2023/06/28 00:15:27 103.1.151.84:465 - SAFE ---------- **587:** ``` 220 mail.tasekmaju.com.my ESMTP Exim 4.90_1 Fri, 30 Jun 2023 22:12:09 +0800 250-mail.tasekmaju.com.my Hello 224.0.242.22 [224.0.242.22] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-CHUNKING 250-STARTTLS 250 HELP ``` ---------- **993:** ``` * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN AUTH=LOGIN] Dovecot ready. * CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN AUTH=LOGIN A001 OK Pre-login capabilities listed, post-login capabilities have more. * ID ("name" "Dovecot") A002 OK ID completed. A003 BAD Error in IMAP command received by server. ``` HEARTBLEED: 2023/06/27 03:29:52 103.1.151.84:993 - SAFE ---------- **995:** ``` +OK Dovecot ready. +OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP-CODE USER SASL PLAIN LOGIN . ``` HEARTBLEED: 2023/06/26 03:39:02 103.1.151.84:995 - SAFE ---------- **2525:** ``` 220 mail.tasekmaju.com.my ESMTP Exim 4.90_1 Tue, 20 Jun 2023 03:55:19 +0800\r\n ``` ---------- **3306:** ``` MySQL: Protocol Version: 10 Version: 5.5.56-MariaDB Thread Id: 783623 Capabilities: 63487 Server Language: 8 Server Status: AutoCommit Extended Server Capabilities: 40975 Authentication Plugin: mysql_native_password ``` ---------- **8083:** ``` HTTP/1.1 200 OK Server: nginx Date: Fri, 30 Jun 2023 15:13:38 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Keep-Alive: timeout=60 ``` HEARTBLEED: 2023/06/30 15:13:58 103.1.151.84:8083 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '103.1.151.84']

Name

ar@gbwhotel.com.my

Pattern Type

stix

Pattern

[email-addr:value = 'ar@gbwhotel.com.my']

Name

afbfc145affa16280139a70e92364d8cc9d71b951d3258df9a9855c0c1f1f567

Description

multiple_versions

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'afbfc145affa16280139a70e92364d8cc9d71b951d3258df9a9855c0c1f1f567']

Name

ab6c5af91d0e384cc011f3e3be12b13290bfc802ce5dd8a3788100f583d4b800

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ab6c5af91d0e384cc011f3e3be12b13290bfc802ce5dd8a3788100f583d4b800']

Name

194.55.224.183

Description

ISP: Delis LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **80:** ``` HTTP/1.1 200 OK Date: Mon, 03 Jul 2023 10:41:57 GMT Server: Apache/2.4.29 (Ubuntu) Last-Modified: Wed, 12 Apr 2023 01:41:15 GMT ETag: "2aa6-5f919b42c3695" Accept-Ranges: bytes Content-Length: 10918 Vary: Accept-Encoding Content-Type: text/html ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '194.55.224.183']

Name

23.106.121.131

Description

ISP: Leaseweb Asia Pacific pte. ltd. **OS:** Windows Server 2012 R2 ---------- Hostnames: ---------- Domains: ---------- Services: **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x0f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 8.1/Windows Server 2012 R2 OS Build: 6.3.9600 Target Name: WIN-CLJ1B0GQ6JP NetBIOS Domain Name: WIN-CLJ1B0GQ6JP NetBIOS Computer Name: WIN-CLJ1B0GQ6JP DNS Domain Name: WIN-CLJ1B0GQ6JP FQDN: WIN-CLJ1B0GQ6JP pyramidrdp Administrator nee ER RE am Windows Server 2012R2 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '23.106.121.131']

Name

9abe143f74890f4336573364fce24257167977b576db98b7579e19283a126bec

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9abe143f74890f4336573364fce24257167977b576db98b7579e19283a126bec']

Attack-Pattern

Name
T1023
ID
T1023
Name
T1060
ID
T1060

Malware

Name
Remcos - S0332

Name
Trojan:Win32/ModiLoader

Name
DBatLoader

Name
GuLoader - S0561

Email-Addr

Value
ar@gbwhotel.com.my
20230626050534.1c6fdebc3dc87bee@gbwhotel.com.my

StixFile

Value
9abe143f74890f4336573364fce24257167977b576db98b7579e19283a126bec
d7b17df67410b8d408bb768c11757162a49cfb8602e50ac98283bfd49c54a9c5
f3b62d90f02bbecd522049f9186c67d939b77e98449d63e73de4893060f1dd48
1d030984aa406ff1a05c1d42e67455b79665d50ea98f49713b1fd21887b7b2eb
afbfc145affa16280139a70e92364d8cc9d71b951d3258df9a9855c0c1f1f567
748c0ef7a63980d4e8064b14fb95ba51947bfc7d9ccf39c6ef614026a89c39e5
29c766c8910fa35b76bdea7738e32f51fc063bc01e8f557c1f309a4b07c47733
ab6c5af91d0e384cc011f3e3be12b13290bfc802ce5dd8a3788100f583d4b800

Hostname

Value
top1.banifabused1.xyz

IPv4-Addr

Value
23.106.121.131
194.55.224.183
103.1.151.84

Url

Value
https://img.softmedal.com/uploads/2023-06-23/298186187297.jpg
https://img.softmedal.com/uploads/2023-06-23/773918053744.jpg

External References

- https://otx.alienvault.com/pulse/64a2f791a1e71dfaf28261a2
- https://isc.sans.edu/diary/29990