Feb 08 2024

NETMANAGEIT

Intelligence Report

RedCurl cyber spies aim for Australia, Singapore and Hong Kong

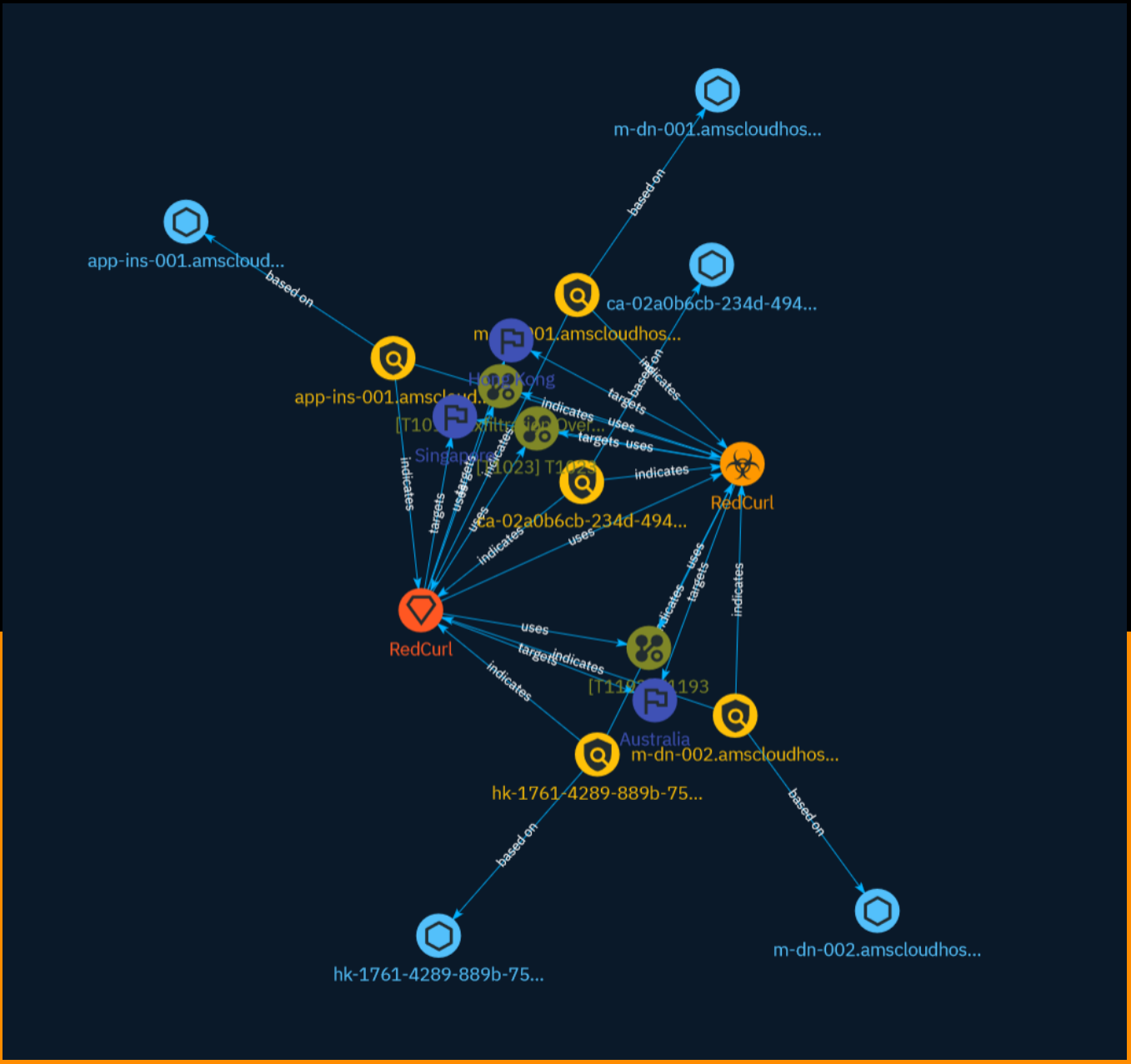

Table of contents

Overview

Entities

Observables

External References

Overview

Description

RedCurl, a Russian-speaking group, have been ramping up attacks outside of Russia since October 2023. New attacks have been observed in Australia, Singapore, and Hong Kong.

Confidence

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

15 / 100

Content

N/A

Indicator

Name
hk-1761-4289-889b-75c0fec903cb.bmrresources.com
Pattern Type
stix
Pattern
[hostname:value = 'hk-1761-4289-889b-75c0fec903cb.bmrresources.com']
Name
ca-02a0b6cb-234d-4944-92f4-5fa0f32c5a36.unitgrapigs.com
Pattern Type
stix
Pattern
[hostname:value = 'ca-02a0b6cb-234d-4944-92f4-5fa0f32c5a36.unitgrapigs.com']
Name
m-dn-001.amscloudhost.com

Pattern Type
stix
Pattern
[hostname:value = 'm-dn-001.amscloudhost.com']
Name
m-dn-002.amscloudhost.com
Pattern Type
stix
Pattern
[hostname:value = 'm-dn-002.amscloudhost.com']
Name
app-ins-001.amscloudhost.com
Pattern Type
stix
Pattern
[hostname:value = 'app-ins-001.amscloudhost.com']
Name
hk-1761-4289-889b-75c0fec903cb.bmrresources.com

Pattern Type

stix

Pattern

[hostname:value = 'hk-1761-4289-889b-75c0fec903cb.bmrresources.com']

Name

ca-02a0b6cb-234d-4944-92f4-5fa0f32c5a36.unitgrapigs.com

Pattern Type

stix

Pattern

[hostname:value = 'ca-02a0b6cb-234d-4944-92f4-5fa0f32c5a36.unitgrapigs.com']

Name

m-dn-001.amscloudhost.com

Pattern Type

stix

Pattern

[hostname:value = 'm-dn-001.amscloudhost.com']

Name

m-dn-002.amscloudhost.com

Pattern Type
stix
Pattern
[hostname:value = 'm-dn-002.amscloudhost.com']
Name
app-ins-001.amscloudhost.com
Pattern Type
stix
Pattern
[hostname:value = 'app-ins-001.amscloudhost.com']

Malware

Name
RedCurl

Name
RedCurl

Intrusion-Set

Name
RedCurl

Name
RedCurl

Attack-Pattern

Name
T1023
ID
T1023
Name
T1193
ID
T1193
Name
Exfiltration Over Other Network Medium
ID
T1011
Description
Adversaries may attempt to exfiltrate data over a different network medium than the command and control channel. If the command and control network is a wired Internet

connection, the exfiltration may occur, for example, over a WiFi connection, modem, cellular data connection, Bluetooth, or another radio frequency (RF) channel. Adversaries may choose to do this if they have sufficient access or proximity, and the connection might not be secured or defended as well as the primary Internet-connected channel because it is not routed through the same enterprise network.

Name

T1023

ID

T1023

Name

T1193

ID

T1193

Name

Exfiltration Over Other Network Medium

ID

T1011

Description

Adversaries may attempt to exfiltrate data over a different network medium than the command and control channel. If the command and control network is a wired Internet connection, the exfiltration may occur, for example, over a WiFi connection, modem, cellular data connection, Bluetooth, or another radio frequency (RF) channel. Adversaries may choose to do this if they have sufficient access or proximity, and the connection might

not be secured or defended as well as the primary Internet-connected channel because it is not routed through the same enterprise network.

Country

Name
Hong Kong
Name
Australia
Name
Singapore
Name
Hong Kong
Name
Australia
Name
Singapore

Hostname

Value
m-dn-001.amscloudhost.com
hk-1761-4289-889b-75c0fec903cb.bmrresources.com
ca-02a0b6cb-234d-4944-92f4-5fa0f32c5a36.unitgrapigs.com
m-dn-002.amscloudhost.com
app-ins-001.amscloudhost.com
m-dn-001.amscloudhost.com
hk-1761-4289-889b-75c0fec903cb.bmrresources.com
ca-02a0b6cb-234d-4944-92f4-5fa0f32c5a36.unitgrapigs.com
m-dn-002.amscloudhost.com
app-ins-001.amscloudhost.com

External References

- https://www.facct.ru/blog/redcurl-2024/
- https://otx.alienvault.com/pulse/65c3a063489291c99b632ea8