Aug 18 2023

NETMANAGEIT

Intelligence Report

Raccoon Stealer Announce Return After Hiatus

Table of contents

Overview

Entities

Observables

External References

Overview

Description

First observed in 2019 and advertised as a ‘Malware-as-a-Service’ (MaaS) threat on various cybercriminal forums, Raccoon is an information stealer targeting victim credentials and cryptocurrency wallets.

Confidence

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

15 / 100

Indicator

Name
telecut.in
Pattern Type
stix
Pattern
[domain-name:value = 'telecut.in']
Name
https://telete.in/jiocacossa
Pattern Type
stix
Pattern
[url:value = 'https://telete.in/jiocacossa']
Name
xn--r1a.website

Pattern Type
stix
Pattern
[domain-name:value = 'xn--r1a.website']
Name
https://tttttt.me/brikitiki
Pattern Type
stix
Pattern
[url:value = 'https://tttttt.me/brikitiki']
Name
tlgr.org
Pattern Type
stix
Pattern
[domain-name:value = 'tlgr.org']
Name
95.216.186.40

Description

CC=FI ASN=AS24940 Hetzner Online GmbH

Pattern Type

stix

Pattern

[ipv4-addr:value = '95.216.186.40']

Name

195.201.225.248

Description

CC=DE ASN=AS24940 Hetzner Online GmbH

Pattern Type

stix

Pattern

[ipv4-addr:value = '195.201.225.248']

Name

tttttt.me

Pattern Type

stix

Pattern

[domain-name:value = 'tttttt.me']

Name

https://tttttt.me/ch0koalpengold

Pattern Type

stix

Pattern

[url:value = 'https://tttttt.me/ch0koalpengold']

Name

xn--r1a.live

Pattern Type

stix

Pattern

[domain-name:value = 'xn--r1a.live']

Name

de7ccff53ca27db1ed1e3e0d0df07f2e3364ec6b7e60622dc7726cba56831eb7

Description

Win32:RansomX-gen\ [Ransom]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'de7ccff53ca27db1ed1e3e0d0df07f2e3364ec6b7e60622dc7726cba56831eb7']

Name

8815b21c44c22aec31f7fa6e69dcb83a60c572f8365ff02b5c6f12154e01a4c2

Description

Win32:PWSX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8815b21c44c22aec31f7fa6e69dcb83a60c572f8365ff02b5c6f12154e01a4c2']

Name

xn--r1a.click

Pattern Type

stix

Pattern

[domain-name:value = 'xn--r1a.click']

Name

012e382049b88808e2d0b26e016dc189f608deea9b6cc993ce24a57c99dd93d1

Description

Win32:DropperX-gen\ [Drp]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '012e382049b88808e2d0b26e016dc189f608deea9b6cc993ce24a57c99dd93d1']

Name

xn--r1a.site

Pattern Type

stix

Pattern

[domain-name:value = 'xn--r1a.site']

Name

https://telete.in/bpa1010100102

Pattern Type

stix

Pattern

[url:value = 'https://telete.in/bpa1010100102']

Name

https://tttttt.me/antitantief3

Pattern Type

stix

Pattern

[url:value = 'https://tttttt.me/antitantief3']

Name

75c3a83073d9b15d4f47308b5d688f1ec07422419e3bd54e78f6ef8683d42e5c

Description

Win32:RansomX-gen\ [Ransom]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '75c3a83073d9b15d4f47308b5d688f1ec07422419e3bd54e78f6ef8683d42e5c']

Name

624b7ae8befcf91dbf768d9703147ac8f9bd46b08ffe14a75c77e88736bf07d0

Description

Win32:DropperX-gen\ [Drp]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '624b7ae8befcf91dbf768d9703147ac8f9bd46b08ffe14a75c77e88736bf07d0']

Name

bfb37c9adc809e880f56dd10898b5425242330d6e2fa69e014a98e6dc18ce416

Description

#Lowfi:Lua:Mampa:99!ml

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bfb37c9adc809e880f56dd10898b5425242330d6e2fa69e014a98e6dc18ce416']

Name

3c5120a6e894b64924dc44f3cdc0da65f277b32870f73019cefeacf492663c0e

Description

Win32:BotX-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3c5120a6e894b64924dc44f3cdc0da65f277b32870f73019cefeacf492663c0e']

Name

https://tttttt.me/kokajakprozak

Pattern Type

stix

Pattern

[url:value = 'https://tttttt.me/kokajakprozak']

Name

telete.in

Pattern Type
stix
Pattern
[domain-name:value = 'telete.in']
Name
caf3eca514de58e215b5e9f568f748293be64a3c82e15c2f905903cd9bfacc1c
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'caf3eca514de58e215b5e9f568f748293be64a3c82e15c2f905903cd9bfacc1c']
Name
https://telete.in/baudemars
Pattern Type
stix
Pattern
[url:value = 'https://telete.in/baudemars']
Name

97e95e99fd499ec45a7c1d8683d5731ce5e7a8fb8b710622e578cd169a00d8d9

Description

Delphi

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '97e95e99fd499ec45a7c1d8683d5731ce5e7a8fb8b710622e578cd169a00d8d9']

Name

a2420c7f0c7bf5d3c0893aff6b7440a09c0531632434d2bbb6f8ed98b04317b9

Description

#Lowfi:Lua:Mampa:99!ml

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a2420c7f0c7bf5d3c0893aff6b7440a09c0531632434d2bbb6f8ed98b04317b9']

Name

18c27b85f26566dd782171e00ea5b5872546b23526cca0ebb185caca35fdec93

Description
Win32:DropperX-gen\ [Drp]
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '18c27b85f26566dd782171e00ea5b5872546b23526cca0ebb185caca35fdec93']
Name
xn--r1a.link
Pattern Type
stix
Pattern
[domain-name:value = 'xn--r1a.link']
Name
40175d0027919244b6b56fe5276c44aba846d532501e562da37831403c9ed44e
Description
Win32:MalwareX-gen\ [Trj]
Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '40175d0027919244b6b56fe5276c44aba846d532501e562da37831403c9ed44e']

Name

24499fbfd8a2b2663899841f3cf424b60d60c26351b5d491fd475adf9e301256

Description

Win32:DropperX-gen\ [Drp]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '24499fbfd8a2b2663899841f3cf424b60d60c26351b5d491fd475adf9e301256']

Name

tgraph.io

Pattern Type

stix

Pattern

[domain-name:value = 'tgraph.io']

Malware

Name
Raccoon

Attack-Pattern

Name
Boot or Logon Autostart Execution
ID
T1547
Description
Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel. Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.
Name
Phishing
ID
T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Screen Capture

ID

T1113

Description

Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations. Taking a screenshot is also typically possible through native utilities or API calls, such as `CopyFromScreen`, `xwd`, or `screencapture`.(Citation: CopyFromScreen .NET)(Citation: Antiquated Mac Malware)

Name
Exfiltration Over C2 Channel
ID
T1041
Description
Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

Domain-Name

Value
tttttt.me
xn--r1a.click
tlgr.org
xn--r1a.website
xn--r1a.link
telete.in
xn--r1a.site
telecut.in
tgraph.io
xn--r1a.live

StixFile

Value
a2420c7f0c7bf5d3c0893aff6b7440a09c0531632434d2bbb6f8ed98b04317b9
de7ccff53ca27db1ed1e3e0d0df07f2e3364ec6b7e60622dc7726cba56831eb7
caf3eca514de58e215b5e9f568f748293be64a3c82e15c2f905903cd9bfacc1c
18c27b85f26566dd782171e00ea5b5872546b23526cca0ebb185caca35fdec93
012e382049b88808e2d0b26e016dc189f608deea9b6cc993ce24a57c99dd93d1
3c5120a6e894b64924dc44f3cdc0da65f277b32870f73019cefeacf492663c0e
8815b21c44c22aec31f7fa6e69dcb83a60c572f8365ff02b5c6f12154e01a4c2
97e95e99fd499ec45a7c1d8683d5731ce5e7a8fb8b710622e578cd169a00d8d9
624b7ae8befcf91dbf768d9703147ac8f9bd46b08ffe14a75c77e88736bf07d0
75c3a83073d9b15d4f47308b5d688f1ec07422419e3bd54e78f6ef8683d42e5c
bfb37c9adc809e880f56dd10898b5425242330d6e2fa69e014a98e6dc18ce416
24499fbfd8a2b2663899841f3cf424b60d60c26351b5d491fd475adf9e301256
40175d0027919244b6b56fe5276c44aba846d532501e562da37831403c9ed44e

IPv4-Addr

Value
95.216.186.40
195.201.225.248

Url

Value
https://tttttt.me/brikitiki
https://telete.in/bpa1010100102
https://tttttt.me/kokajakprozak
https://tttttt.me/antitantief3
https://telete.in/baudemars
https://tttttt.me/ch0koalpengold
https://telete.in/jiocacossa

External References

- https://otx.alienvault.com/pulse/64dca4eb3f10605dbeff12ac
- https://cyberint.com/blog/financial-services/raccoon-stealer/