Dec 22 2023

NETMANAGEIT

Intelligence Report

New MetaStealer malvertising campaigns

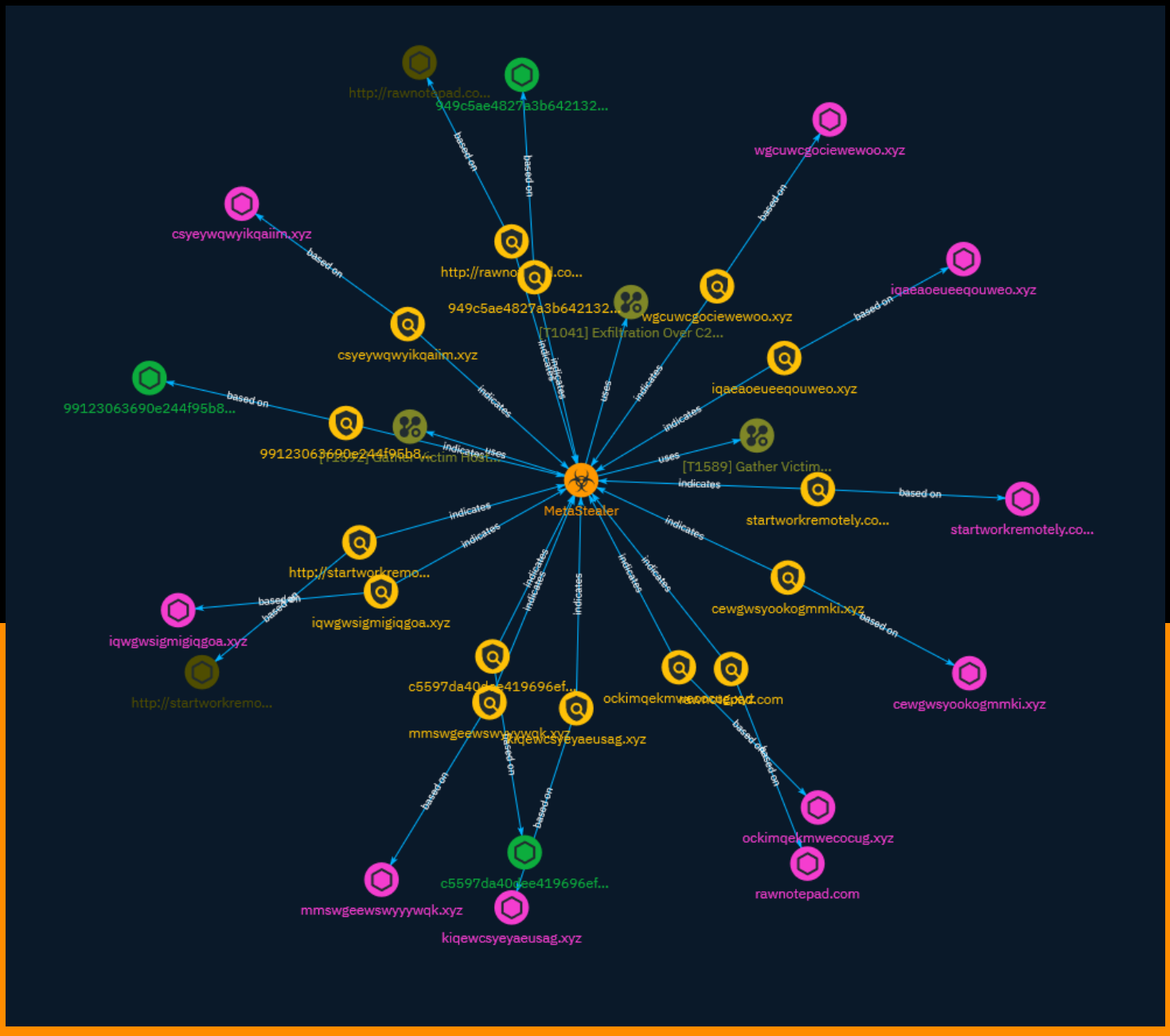

Table of contents

Overview

Entities

Observables

External References

Overview

Description

MetaStealer, a prominent malware emerging in 2022, originated from the RedLine code base and is highly sought after in criminal circles due to its stealing capabilities. Recent observations reveal threat actors employing malspam and malicious ads to distribute MetaStealer, highlighting its ongoing evolution as the malware authors announce plans for a new and enhanced version in December.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Gather Victim Identity Information
ID
T1589
Description
Adversaries may gather information about the victim's identity that can be used during targeting. Information about identities may include a variety of details, including personal data (ex: employee names, email addresses, etc.) as well as sensitive details such as credentials. Adversaries may gather this information in various ways, such as direct elicitation via [Phishing for Information](https://attack.mitre.org/techniques/T1598). Information about users could also be enumerated via other active means (i.e. [Active Scanning](https://attack.mitre.org/techniques/T1595)) such as probing and analyzing responses from authentication services that may reveal valid usernames in a system. (Citation: GrimBlog UsernameEnum) Information about victims may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)).(Citation: OPM Leak)(Citation: Register Deloitte)(Citation: Register Uber)(Citation: Detectify Slack Tokens)(Citation: Forbes GitHub Creds)(Citation: GitHub truffleHog)(Citation: GitHub Gitrob)(Citation: CNET Leaks) Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Phishing for Information](https://attack.mitre.org/techniques/T1598)), establishing operational resources (ex: [Compromise Accounts](https://attack.mitre.org/techniques/T1586)), and/or initial access (ex: [Phishing](https://attack.mitre.org/techniques/T1566) or [Valid Accounts](https://attack.mitre.org/techniques/T1078)).

Name

Gather Victim Host Information

ID

T1592

Description

Adversaries may gather information about the victim's hosts that can be used during targeting. Information about hosts may include a variety of details, including administrative data (ex: name, assigned IP, functionality, etc.) as well as specifics regarding its configuration (ex: operating system, language, etc.). Adversaries may gather this information in various ways, such as direct collection actions via [Active Scanning](https://attack.mitre.org/techniques/T1595) or [Phishing for Information](https://attack.mitre.org/techniques/T1598). Adversaries may also compromise sites then include malicious content designed to collect host information from visitors.(Citation: ATT ScanBox) Information about hosts may also be exposed to adversaries via online or other accessible data sets (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)). Gathering this information may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [Supply Chain Compromise](https://attack.mitre.org/techniques/T1195) or [External Remote Services](https://attack.mitre.org/techniques/T1133)).

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.

Indicator

Name
iqwgwsigmigiqgoa.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'iqwgwsigmigiqgoa.xyz']
Name
99123063690e244f95b89d96759ec7dbc28d4079a56817f3152834047ab047eb
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '99123063690e244f95b89d96759ec7dbc28d4079a56817f3152834047ab047eb']
Name

kiqewcsyeyaeusag.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'kiqewcsyeyaeusag.xyz']

Name

cewgwsyookogmmki.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'cewgwsyookogmmki.xyz']

Name

http://rawnotepad.com/notepad++.zip

Pattern Type

stix

Pattern

[url:value = 'http://rawnotepad.com/notepad++.zip']

Name

mmswgeewswyyywqk.xyz

Description

MetaStealer botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'mmswgeewswyyywqk.xyz']

Name

949c5ae4827a3b642132faf73275fb01c26e9dce151d6c5467d3014f208f77ca

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '949c5ae4827a3b642132faf73275fb01c26e9dce151d6c5467d3014f208f77ca']

Name

iqaeaoeueeqouweo.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'iqaeaoeueeqouweo.xyz']

Name

c5597da40dee419696ef2b32cb937a11fcad40f4f79f9a80f6e326a94e81a90f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c5597da40dee419696ef2b32cb937a11fcad40f4f79f9a80f6e326a94e81a90f']

Name

csyeywqwyikqaiim.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'csyeywqwyikqaiim.xyz']

Name

startworkremotely.com

Pattern Type

stix

Pattern

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

Name

ockimqekmwecocug.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'ockimqekmwecocug.xyz']

Name

wgcuwcgociewewoo.xyz

Description

MetaStealer botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'wgcuwcgociewewoo.xyz']

Name

rawnotepad.com

Pattern Type

stix

Pattern

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

Name

http://startworkremotely.com/Anydesk.zip

Pattern Type

stix

Pattern

[url:value = 'http://startworkremotely.com/Anydesk.zip']

Malware

Name
MetaStealer

Domain-Name

Value
cewgwsyookogmmki.xyz
kiqewcsyeyaeusag.xyz
wgcuwcgociewewoo.xyz
rawnotepad.com
iqwgwsigmigiqgoa.xyz
startworkremotely.com
mmswgeewswyyywqk.xyz
iqaeaoeueeqouweo.xyz
ockimqekmwecocug.xyz
csyeywqwyikqaiim.xyz

StixFile

Value
c5597da40dee419696ef2b32cb937a11fcad40f4f79f9a80f6e326a94e81a90f
99123063690e244f95b89d96759ec7dbc28d4079a56817f3152834047ab047eb
949c5ae4827a3b642132faf73275fb01c26e9dce151d6c5467d3014f208f77ca

Url

Value
http://startworkremotely.com/Anydesk.zip
http://rawnotepad.com/notepad++.zip

External References

- https://otx.alienvault.com/pulse/658469e72f85cfbf44de42a6
- https://www.malwarebytes.com/blog/threat-intelligence/2023/12/new-metastealer-malvertising-campaigns