Jan 25 2024

NETMANAGEIT

Intelligence Report

Vextrio Operates Massive Criminal Affiliate Program

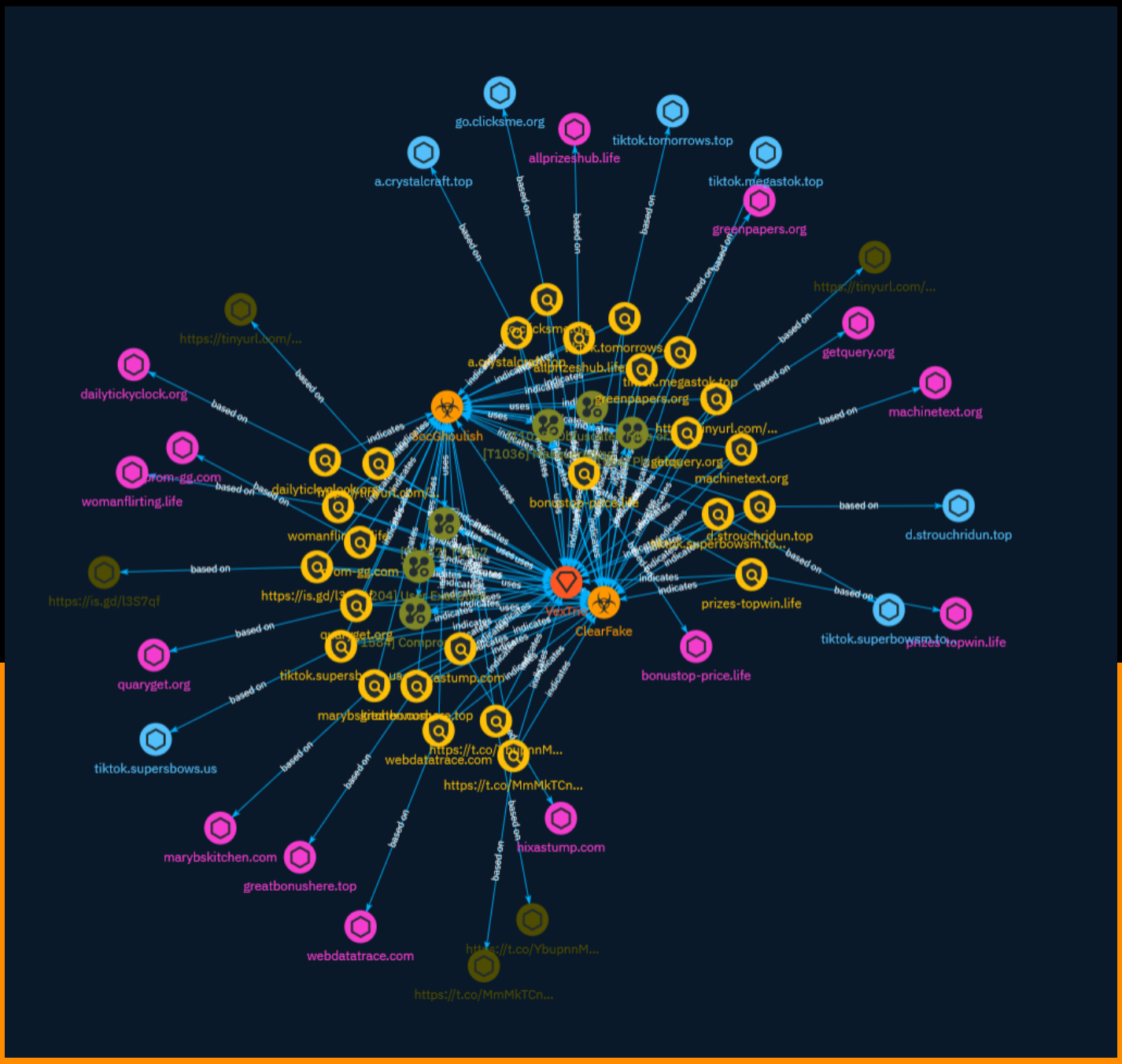

Table of contents

Overview

Entities

Observables

External References

Overview

Description

VexTrio is the single most pervasive threat in our customers' networks. Operating a massive network of its own, VexTrio is seen in more networks than any other actor and accounts for the most threats by query volume of any actor. Of their more than 70k known domains, nearly half have been observed in customer networks. We have seen VexTrio activity in as much as 19% of networks on a single day since 2020, and in over half of all customer networks in the last two years.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
T1457
ID
T1457
Name
Compromise Infrastructure
ID
T1584
Description
Adversaries may compromise third-party infrastructure that can be used during targeting. Infrastructure solutions include physical or cloud servers, domains, and third-party web and DNS services. Instead of buying, leasing, or renting infrastructure an adversary may compromise infrastructure and use it during other phases of the adversary lifecycle. (Citation: Mandiant APT1)(Citation: ICANNDomainNameHijacking)(Citation: Talos DNSpionage Nov 2018)(Citation: FireEye EPS Awakens Part 2) Additionally, adversaries may compromise numerous machines to form a botnet they can leverage. Use of compromised infrastructure allows adversaries to stage, launch, and execute operations. Compromised infrastructure can help adversary operations blend in with traffic that is seen as normal, such as contact with high reputation or trusted sites. For example, adversaries may leverage compromised infrastructure (potentially also in conjunction with [Digital

Certificates](https://attack.mitre.org/techniques/T1588/004)) to further blend in and support staged information gathering and/or [Phishing](https://attack.mitre.org/techniques/T1566) campaigns.(Citation: FireEye DNS Hijack 2019) Additionally, adversaries may also compromise infrastructure to support [Proxy](https://attack.mitre.org/techniques/T1090) and/or proxyware services.(Citation: amnesty_nso_pegasus)(Citation: Sysdig Proxyjacking) By using compromised infrastructure, adversaries may make it difficult to tie their actions back to them. Prior to targeting, adversaries may compromise the infrastructure of other adversaries.(Citation: NSA NCSC Turla OilRig)

Name

Masquerading

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

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

User Execution

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop

hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219).(Citation: Telephone Attack Delivery)

Name

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control

mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Indicator

Name
womanflirting.life
Pattern Type
stix
Pattern
[domain-name:value = 'womanflirting.life']
Name
a.crystalcraft.top
Pattern Type
stix
Pattern
[hostname:value = 'a.crystalcraft.top']
Name
https://tinyurl.com/288tobvb

Pattern Type

stix

Pattern

[url:value = 'https://tinyurl.com/288tobvb']

Name

https://t.co/MmMkTCn6Kd

Pattern Type

stix

Pattern

[url:value = 'https://t.co/MmMkTCn6Kd']

Name

getquery.org

Description

FAKEUPDATES payload delivery domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'getquery.org']

Name
d.strouchridun.top
Pattern Type
stix
Pattern
[hostname:value = 'd.strouchridun.top']
Name
tiktok.supersbows.us
Pattern Type
stix
Pattern
[hostname:value = 'tiktok.supersbows.us']
Name
prizes-topwin.life
Pattern Type
stix
Pattern
[domain-name:value = 'prizes-topwin.life']

Name
webdatatrace.com
Pattern Type
stix
Pattern
[domain-name:value = 'webdatatrace.com']
Name
hixastump.com
Pattern Type
stix
Pattern
[domain-name:value = 'hixastump.com']
Name
allprizeshub.life
Pattern Type
stix
Pattern
[domain-name:value = 'allprizeshub.life']

Name
https://is.gd/l3S7qf
Pattern Type
stix
Pattern
[url:value = 'https://is.gd/l3S7qf']
Name
tiktok.tomorrows.top
Pattern Type
stix
Pattern
[hostname:value = 'tiktok.tomorrows.top']
Name
bonustop-price.life
Pattern Type
stix
Pattern
[domain-name:value = 'bonustop-price.life']

Name

tiktok.superbowsm.top

Pattern Type

stix

Pattern

[hostname:value = 'tiktok.superbowsm.top']

Name

machinetext.org

Description

FAKEUPDATES payload delivery domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'machinetext.org']

Name

marybskitchen.com

Pattern Type

stix

Pattern

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

Name

go.clicksme.org

Pattern Type

stix

Pattern

[hostname:value = 'go.clicksme.org']

Name

greatbonushere.top

Pattern Type

stix

Pattern

[domain-name:value = 'greatbonushere.top']

Name

https://tinyurl.com/2ykfey8v

Pattern Type

stix

Pattern

[url:value = 'https://tinyurl.com/2ykfey8v']

Name

tiktok.megastok.top

Pattern Type

stix

Pattern

[hostname:value = 'tiktok.megastok.top']

Name

quaryget.org

Description

FAKEUPDATES payload delivery domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'quaryget.org']

Name

dailytickyclock.org

Description

FAKEUPDATES payload delivery domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'dailytickyclock.org']

Name

https://t.co/YbupnnMAtX

Pattern Type

stix

Pattern

[url:value = 'https://t.co/YbupnnMAtX']

Name

prom-gg.com

Pattern Type

stix

Pattern

[domain-name:value = 'prom-gg.com']

Name
greenpapers.org
Description
FAKEUPDATES payload delivery domain (confidence level: 100%)
Pattern Type
stix
Pattern
[domain-name:value = 'greenpapers.org']

Intrusion-Set

Name
VexTrio

Malware

Name
SocGhoulish

Name
ClearFake

Domain-Name

Value
webdatatrace.com
womanflirting.life
bonustop-price.life
marybskitchen.com
allprizeshub.life
getquery.org
greatbonushere.top
prom-gg.com
hixastump.com
quaryget.org
prizes-topwin.life
dailytickyclock.org
machinetext.org

greenpapers.org

Hostname

Value
tiktok.megastok.top
d.strouchridun.top
tiktok.supersbows.us
a.crystalcraft.top
tiktok.superbowsm.top
go.clicksme.org
tiktok.tomorrows.top

Url

Value
https://t.co/YbupnnMAtX
https://tinyurl.com/288tobvb
https://t.co/MmMkTCn6Kd
https://is.gd/l3S7qf
https://tinyurl.com/2ykfey8v

External References

- https://blogs.infoblox.com/cyber-threat-intelligence/cybercrime-central-vextrio-operates-massive-criminal-affiliate-program/
- https://otx.alienvault.com/pulse/65b1428ce0e4701b256fdb89