NETMANAGEIT

Intelligence Report

Associated Press, ESPN, CBS among top sites serving fake virus alerts

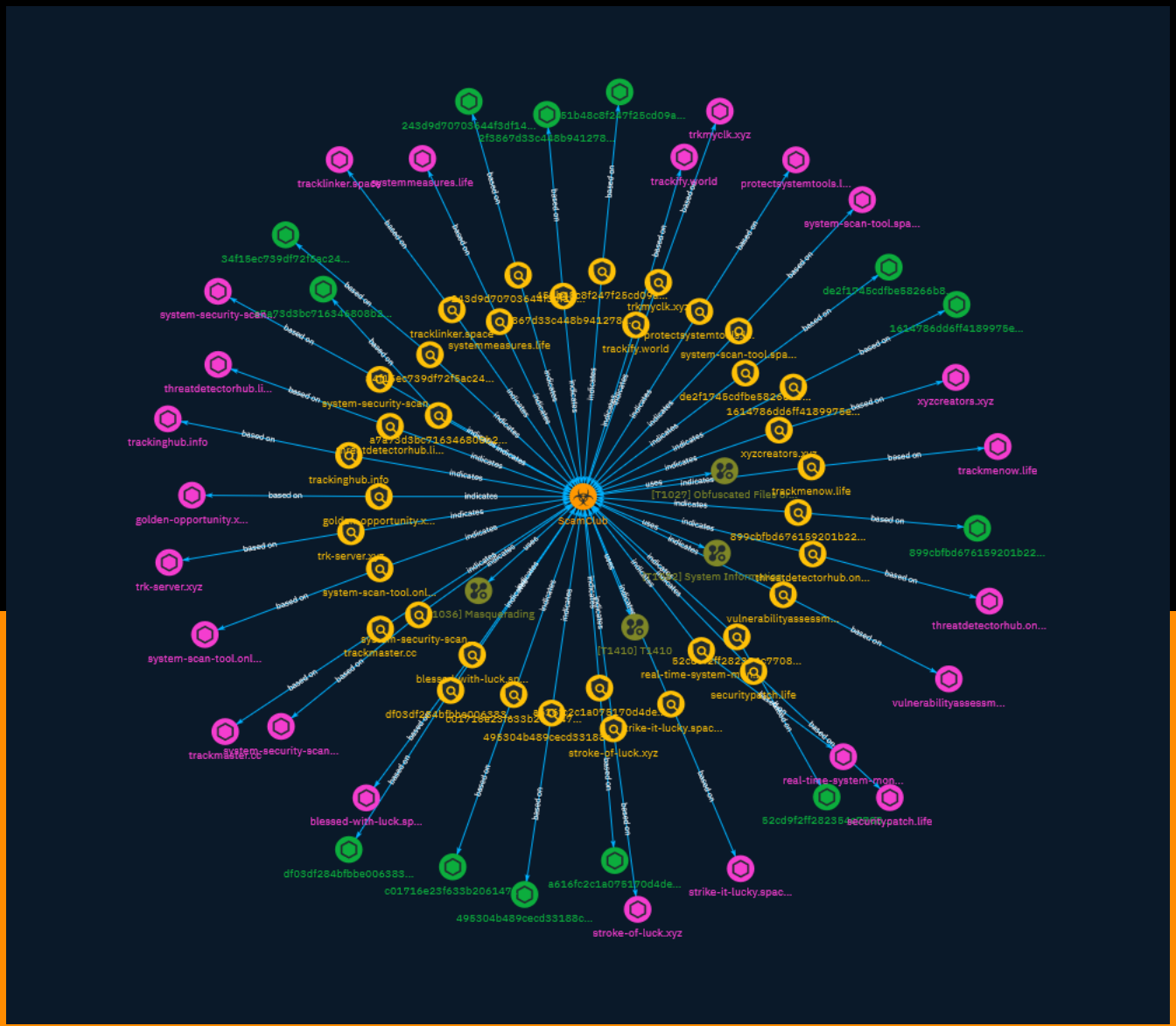

Table of contents

Overview

- Description 4
- Confidence 4
- Content 5

Entities

- Attack-Pattern 6
- Indicator 9
- Malware 22

Observables

- Domain-Name 23
- StixFile 25

External References

- External References 26

Overview

Description

ScamClub is a threat actor who's been involved in malvertising activities since 2018. Chances are you probably ran into one of their online scams on your mobile device. ScamClub is resourceful and continues to have a deep impact on the ad ecosystem.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

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
T1410
ID
T1410

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)

Name

System Information Discovery

ID

T1082

Description

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1082) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Tools such as [Systeminfo](https://attack.mitre.org/software/S0096) can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the `systemsetup` configuration tool on macOS. As an example, adversaries with user-level access can execute the `df -aH` command to obtain currently mounted disks and associated freely available space. Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather detailed system information (e.g. `show version`).(Citation: US-CERT-TA18-106A) [System Information Discovery](https://attack.mitre.org/techniques/T1082) combined with information gathered from other forms of discovery and reconnaissance can drive payload development and concealment.(Citation: OSX.FairyTale)(Citation: 20 macOS Common Tools and Techniques) Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine.(Citation: Amazon Describe Instance)(Citation: Google Instances Resource)(Citation: Microsoft Virutal Machine API)

Indicator

Name
trackinghub.info
Pattern Type
stix
Pattern
[domain-name:value = 'trackinghub.info']
Name
tracklinker.space
Pattern Type
stix
Pattern
[domain-name:value = 'tracklinker.space']
Name
system-security-scan.net

Pattern Type
stix
Pattern
[domain-name:value = 'system-security-scan.net']
Name
xyzcreators.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'xyzcreators.xyz']
Name
trackmenow.life
Pattern Type
stix
Pattern
[domain-name:value = 'trackmenow.life']
Name
c01716e23f633b206147efbe70fb37945e3857d6575fd088ea50106fb541cf1e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c01716e23f633b206147efbe70fb37945e3857d6575fd088ea50106fb541cf1e']

Name

threatdetectorhub.life

Pattern Type

stix

Pattern

[domain-name:value = 'threatdetectorhub.life']

Name

52cd9f2ff282354c77087b204d5cb32cee9066e8eea4e3c3b8f7cf4d3d3fa20f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '52cd9f2ff282354c77087b204d5cb32cee9066e8eea4e3c3b8f7cf4d3d3fa20f']

Name

system-scan-tool.online

Pattern Type

stix

Pattern

[domain-name:value = 'system-scan-tool.online']

Name

de2f1745cdfbe58266b804961bdbd5be8f533843ed7fdf4b5fe6eb0060876b56

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'de2f1745cdfbe58266b804961bdbd5be8f533843ed7fdf4b5fe6eb0060876b56']

Name

vulnerabilityassessments.life

Pattern Type

stix

Pattern

[domain-name:value = 'vulnerabilityassessments.life']

Name
system-security-scan.buzz
Pattern Type
stix
Pattern
[domain-name:value = 'system-security-scan.buzz']
Name
system-scan-tool.space
Pattern Type
stix
Pattern
[domain-name:value = 'system-scan-tool.space']
Name
blessed-with-luck.space
Pattern Type
stix
Pattern
[domain-name:value = 'blessed-with-luck.space']

Name
protectsystemtools.life
Pattern Type
stix
Pattern
[domain-name:value = 'protectsystemtools.life']
Name
trk-server.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'trk-server.xyz']
Name
golden-opportunity.xyz
Pattern Type
stix
Pattern
[domain-name:value = 'golden-opportunity.xyz']

Name
trackify.world
Pattern Type
stix
Pattern
[domain-name:value = 'trackify.world']
Name
securitypatch.life
Pattern Type
stix
Pattern
[domain-name:value = 'securitypatch.life']
Name
2f3867d33c448b941278671df9a2b8d3d6b29dec5d74b67654f5edfcc6771575
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = '2f3867d33c448b941278671df9a2b8d3d6b29dec5d74b67654f5edfcc6771575']

Name

strike-it-lucky.space

Pattern Type

stix

Pattern

[domain-name:value = 'strike-it-lucky.space']

Name

a7a73d3bc716346808b2ee8070dfe5842bb01e10aee1fa9ba87fb975d71d0f4f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a7a73d3bc716346808b2ee8070dfe5842bb01e10aee1fa9ba87fb975d71d0f4f']

Name

1614786dd6ff4189975e8226ab7e68d258817b435c3c4e145951f5147699878e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1614786dd6ff4189975e8226ab7e68d258817b435c3c4e145951f5147699878e']

Name

trackmaster.cc

Pattern Type

stix

Pattern

[domain-name:value = 'trackmaster.cc']

Name

34f15ec739df72f5ac245db3fff11ea56407e95b94e24bbb820d7999032866d8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '34f15ec739df72f5ac245db3fff11ea56407e95b94e24bbb820d7999032866d8']

Name

stroke-of-luck.xyz

Pattern Type

stix

Pattern

[domain-name:value = 'stroke-of-luck.xyz']

Name

df03df284bfbbe006383f26c0c91394f4c4c8d915d04b868a00954f63e6163e0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'df03df284bfbbe006383f26c0c91394f4c4c8d915d04b868a00954f63e6163e0']

Name

451b48c8f247f25cd09a1bf4a52fc195a74830d88bd2ffed7a5d4b7830e10621

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '451b48c8f247f25cd09a1bf4a52fc195a74830d88bd2ffed7a5d4b7830e10621']

Name

495304b489cecd33188ca2a7407d397996fd82ea99966e7c145f0dc67ab2dfb5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '495304b489cecd33188ca2a7407d397996fd82ea99966e7c145f0dc67ab2dfb5']

Name

trkmyclk.xyz

Pattern Type

stix

Pattern

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

Name

899cbfbd676159201b2281d9e0e66f3ac200ac58b674375bde04083ff87650ad

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '899cbfbd676159201b2281d9e0e66f3ac200ac58b674375bde04083ff87650ad']

Name

real-time-system-monitoring.life

Pattern Type

stix

Pattern

[domain-name:value = 'real-time-system-monitoring.life']

Name

243d9d70703644f3df148e7633f3ec461a9c43149ea58fd547e2e6fd0c47cce5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '243d9d70703644f3df148e7633f3ec461a9c43149ea58fd547e2e6fd0c47cce5']

Name

threatdetectorhub.online

Pattern Type

stix

Pattern

[domain-name:value = 'threatdetectorhub.online']

Name
a616fc2c1a075170d4decdb9d3c9ad15f2cfbcfda78dbe4c60d72132b9d006c9
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'a616fc2c1a075170d4decdb9d3c9ad15f2cfbcfda78dbe4c60d72132b9d006c9']
Name
systemmeasures.life
Pattern Type
stix
Pattern
[domain-name:value = 'systemmeasures.life']

Malware

Name
ScamClub

Domain-Name

Value
system-scan-tool.online
trackinghub.info
xyzcreators.xyz
golden-opportunity.xyz
system-scan-tool.space
blessed-with-luck.space
tracklinker.space
trkmyclk.xyz
threatdetectorhub.life
protectsystemtools.life
vulnerabilityassessments.life
trackmaster.cc
threatdetectorhub.online

system-security-scan.buzz

trackify.world

trackmenow.life

stroke-of-luck.xyz

system-security-scan.net

securitypatch.life

systemmeasures.life

real-time-system-monitoring.life

strike-it-lucky.space

trk-server.xyz

StixFile

Value
de2f1745cdfbe58266b804961bdbd5be8f533843ed7fdf4b5fe6eb0060876b56
1614786dd6ff4189975e8226ab7e68d258817b435c3c4e145951f5147699878e
451b48c8f247f25cd09a1bf4a52fc195a74830d88bd2ffed7a5d4b7830e10621
52cd9f2ff282354c77087b204d5cb32cee9066e8eea4e3c3b8f7cf4d3d3fa20f
a616fc2c1a075170d4decdb9d3c9ad15f2cfbcfda78dbe4c60d72132b9d006c9
495304b489cecd33188ca2a7407d397996fd82ea99966e7c145f0dc67ab2dfb5
2f3867d33c448b941278671df9a2b8d3d6b29dec5d74b67654f5edfcc6771575
899cbfbd676159201b2281d9e0e66f3ac200ac58b674375bde04083ff87650ad
34f15ec739df72f5ac245db3fff11ea56407e95b94e24bbb820d7999032866d8
a7a73d3bc716346808b2ee8070dfe5842bb01e10aee1fa9ba87fb975d71d0f4f
c01716e23f633b206147efbe70fb37945e3857d6575fd088ea50106fb541cf1e
243d9d70703644f3df148e7633f3ec461a9c43149ea58fd547e2e6fd0c47cce5
df03df284bfbbe006383f26c0c91394f4c4c8d915d04b868a00954f63e6163e0

External References

- https://otx.alienvault.com/pulse/6568c03a3d2441b93d7e4401
- https://www.malwarebytes.com/blog/threat-intelligence/2023/11/associated-press-espn-cbs-among-top-sites-serving-fake-virus-alerts