Jun 10 2023

NETMANAGEIT

Intelligence Report

Analysis of the RecordBreaker secret-stealing Trojan spread through video sites

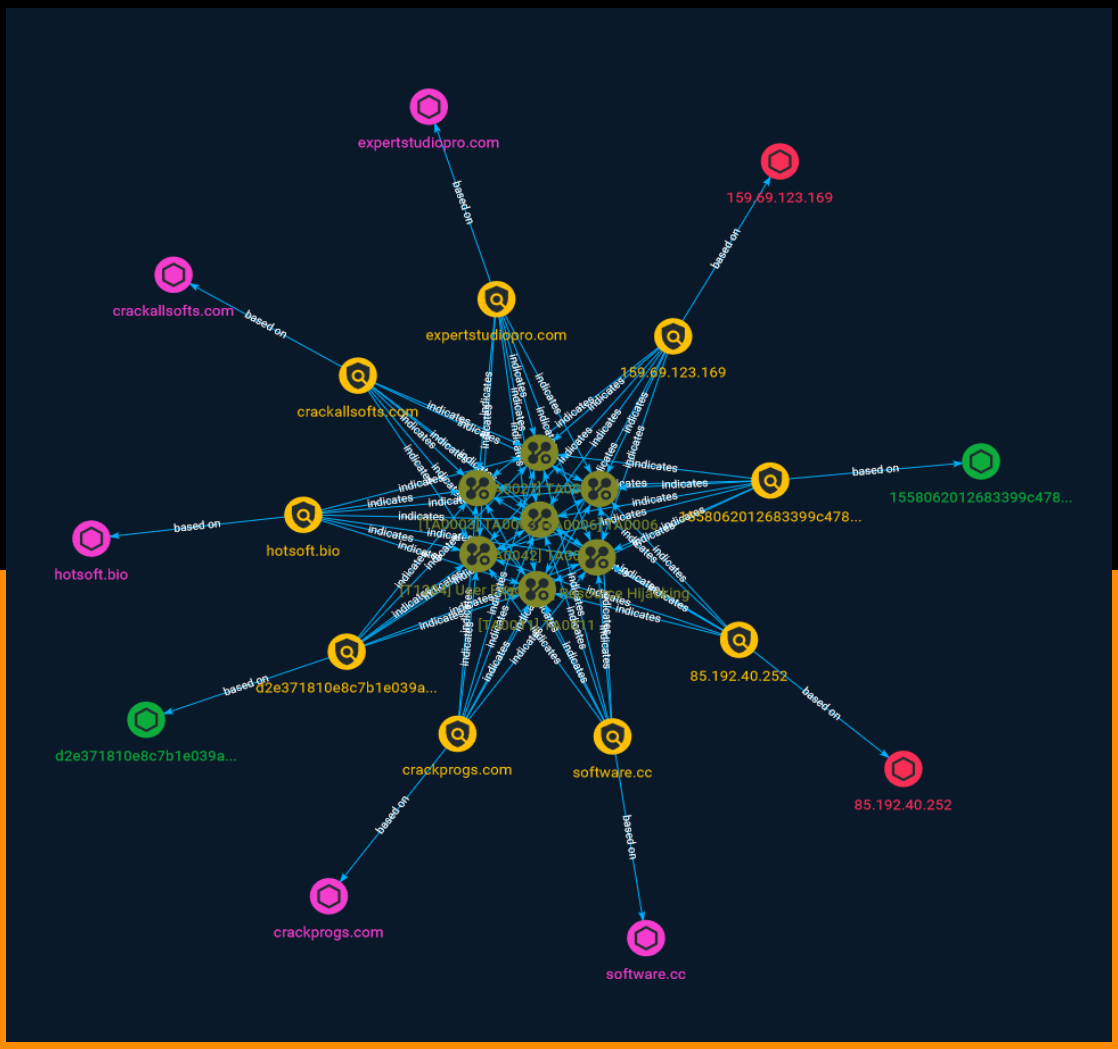

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Recently, Antiy CERT has detected attacks spread through video websites. Attackers stole video creator accounts with more than 100,000 subscribers, released demo videos related to cracked versions of popular software, and induced victims to download the RecordBreaker secret-stealing Trojan horse.

Confidence

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

15 / 100

Attack-Pattern

Name
TA0042
ID
TA0042
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

TA0027

ID

TA0027

Name

Resource Hijacking

ID

T1496

Description

Adversaries may leverage the resources of co-opted systems in order to solve resource intensive problems, which may impact system and/or hosted service availability. One common purpose for Resource Hijacking is to validate transactions of cryptocurrency networks and earn virtual currency. Adversaries may consume enough system resources to negatively impact and/or cause affected machines to become unresponsive.(Citation: Kaspersky Lazarus Under The Hood Blog 2017) Servers and cloud-based systems are common targets because of the high potential for available resources, but user endpoint systems may also be compromised and used for Resource Hijacking and cryptocurrency mining.(Citation: CloudSploit - Unused AWS Regions) Containerized environments may also be targeted due to the ease of deployment via exposed APIs and the potential for scaling mining activities by deploying or compromising multiple containers within an environment or cluster.(Citation: Unit 42 Hildegard Malware)(Citation: Trend Micro Exposed Docker APIs) Additionally, some cryptocurrency mining malware identify then kill off processes for

competing malware to ensure it’s not competing for resources.(Citation: Trend Micro War of Crypto Miners) Adversaries may also use malware that leverages a system's network bandwidth as part of a botnet in order to facilitate [Network Denial of Service](https://attack.mitre.org/techniques/T1498) campaigns and/or to seed malicious torrents.(Citation: GoBotKR)

Name
TA0003
ID
TA0003
Name
TA0006
ID
TA0006
Name
TA0011
ID
TA0011

Indicator

Name

d2e371810e8c7b1e039a02a578b1af0c6250665e85206b97a1ecb71aa5568443

Description

SHA256 of e72d497c94bb1ed882ac98931f70e82e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd2e371810e8c7b1e039a02a578b1af0c6250665e85206b97a1ecb71aa5568443']

Name

159.69.123.169

Description

ISP: Hetzner Online GmbH **OS:** Ubuntu ---------- Hostnames: - static.169.123.69.159.clients.your-server.de ---------- Domains: - your-server.de ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLWuy8X96ep5J0eQRqEjmkQKl32lGYCjow7YAM3FWmuVfXMvDzJukkJatoFZ1LyDNfwXyvpXVU5KL1SPC3UuF30= Fingerprint: e0:7b:

7c:0a:e8:8a:2d:b2:ce:53:c4:d2:f6:ce:bc:03 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 404 Not Found Server: nginx/1.18.0 (Ubuntu) Date: Sun, 21 May 2023 11:36:36 GMT Content-Type: text/html; charset=utf-8 Content-Length: 139 Connection: keep-alive Vary: Accept-Encoding Vary: Accept-Encoding Vary: Accept-Encoding Content-Security-Policy: default-src 'none' Cross-Origin-Embedder-Policy: require-corp Cross-Origin-Opener-Policy: same-origin Cross-Origin-Resource-Policy: same-origin X-DNS-Prefetch-Control: off Expect-CT: max-age=0 X-Frame-Options: SAMEORIGIN Strict-Transport-Security: max-age=15552000; includeSubDomains X-Download-Options: noopen X-Content-Type-Options: nosniff Origin-Agent-Cluster: ?1 X-Permitted-Cross-Domain-Policies: none Referrer-Policy: no-referrer X-XSS-Protection: 0 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '159.69.123.169']

Name

software.cc

Pattern Type

stix

Pattern

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

Name

crackallsofts.com

Pattern Type

stix

Pattern

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

Name

1558062012683399c47811f8c6f582a25951980ab703ef262e006c1c51ecb1c6

Description

stack_string SHA256 of aa6cf53b4389f2eac3ad5718b7300f80

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1558062012683399c47811f8c6f582a25951980ab703ef262e006c1c51ecb1c6']

Name

crackprogs.com

Pattern Type

stix

Pattern

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

Name

expertstudiopro.com

Pattern Type

stix

Pattern

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

Name

85.192.40.252

Description

ISP: LLC Digital Network **OS:** Ubuntu ---------- Hostnames: - fluttering-blood.aeza.network ---------- Domains: - aeza.network ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.1 Key type: ecdsa-sha2-nistp256 Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBI+5gokxmiq0d/QkUcXXyndV2xthqQwkmSZ1gHmFe6xEmcDLsnGwF47pN4r1c7b9Mnxin5OfbJ012uIH2vnXsgQ= Fingerprint: 84:57:f6:1e:5d:12:b1:c3:e3:8b:54:e5:68:74:4a:b1 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 sntrup761x25519-sha512@openssh.com diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519

Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 301 Moved Permanently Server: nginx/1.18.0 (Ubuntu) Date: Fri, 12 May 2023 03:47:47 GMT Content-Type: text/html Content-Length: 169 Connection: keep-alive Location: https://laplas.app/ ``` ----------

Pattern Type
stix

Pattern
[ipv4-addr:value = '85.192.40.252']

Name
hotsoft.bio

Pattern Type
stix

Pattern
[domain-name:value = 'hotsoft.bio']

Domain-Name

Value
crackprogs.com
software.cc
expertstudiopro.com
hotsoft.bio
crackallsofts.com

StixFile

Value
d2e371810e8c7b1e039a02a578b1af0c6250665e85206b97a1ecb71aa5568443
1558062012683399c47811f8c6f582a25951980ab703ef262e006c1c51ecb1c6

IPv4-Addr

Value
159.69.123.169
85.192.40.252

External References

- https://otx.alienvault.com/pulse/648340f66e6baaa298b44a9d
- https://mp.weixin.qq.com/s/K8r6ZLC9LX6fRx-zwTR_hw