Jun 19 2023

NETMANAGEIT

Intelligence Report

Tracking Diicot: an emerging Romanian threat actor

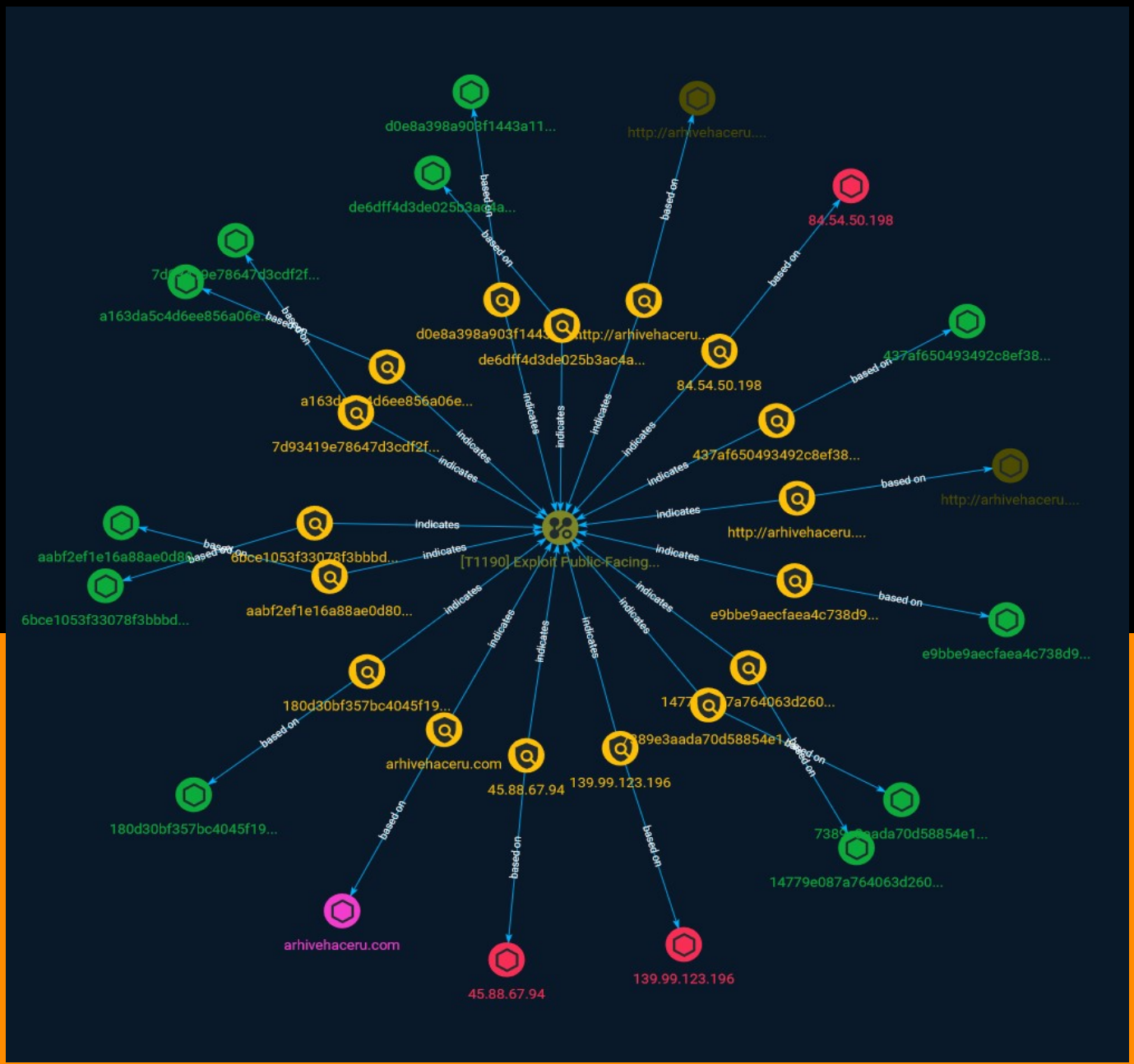

Table of contents

Overview

Entities

Observables

External References

Overview

Description

In a recent review of honeypot sensor telemetry, researchers detected an interesting attack pattern that could be attributed to the threat actor Diicot (formerly, “Mexals”).

Confidence

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

15 / 100

Attack-Pattern

Name
Exploit Public-Facing Application
ID
T1190
Description
Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration. Exploited applications are often websites/web servers, but can also include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other system with Internet accessible open sockets.(Citation: NVD CVE-2016-6662)(Citation: CIS Multiple SMB Vulnerabilities)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks)(Citation: NVD CVE-2014-7169) Depending on the flaw being exploited this may also involve [Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211). If an application is hosted on cloud-based infrastructure and/or is containerized, then exploiting it may lead to compromise of the underlying instance or container. This can allow an adversary a path to access the cloud or container APIs, exploit container host access via [Escape to Host](https://attack.mitre.org/techniques/T1611), or take advantage of weak identity and access management policies. Adversaries may also exploit edge network infrastructure and related appliances, specifically targeting devices that do not support robust host-based defenses.(Citation: Mandiant Fortinet Zero Day)(Citation: Wired Russia Cyberwar) For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities. (Citation: OWASP Top 10)(Citation: CWE top 25)

Indicator

Name

6bce1053f33078f3bbbd526162d9178794c19997536b821177f2cb0d4e6e6896

Description

Unix.Trojan.DarkNexus-7679166-0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6bce1053f33078f3bbbd526162d9178794c19997536b821177f2cb0d4e6e6896']

Name

e9bbe9aecfaea4c738d95d0329a5da9bd33c04a97779172c7df517e1a808489c

Description

Other:Malware-gen\ [Trj]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e9bbe9aecfaea4c738d95d0329a5da9bd33c04a97779172c7df517e1a808489c']

Name

180d30bf357bc4045f197b26b1b8941af9ca0203226a7260092d70dd15f3e6ab

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '180d30bf357bc4045f197b26b1b8941af9ca0203226a7260092d70dd15f3e6ab']

Name

a163da5c4d6ee856a06e4e349565e19a704956baeb62987622a2b2c43577cdee

Description

Unix.Trojan.DarkNexus-7679166-0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'a163da5c4d6ee856a06e4e349565e19a704956baeb62987622a2b2c43577cdee']

Name

14779e087a764063d260cafa5c2b93d7ed5e0d19783eeaea6abb12d17561949a

Description

LinuxHacktool_eyes_pscan2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '14779e087a764063d260cafa5c2b93d7ed5e0d19783eeaea6abb12d17561949a']

Name

aabf2ef1e16a88ae0d802efcb2525edb90a996bb5d280b4c61d2870351e3fba4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'aabf2ef1e16a88ae0d802efcb2525edb90a996bb5d280b4c61d2870351e3fba4']

Name

437af650493492c8ef387140b5cb2660044764832d1444e5265a0cd3fe6e0c39

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '437af650493492c8ef387140b5cb2660044764832d1444e5265a0cd3fe6e0c39']

Name

139.99.123.196

Description

ISP: OVH SAS **OS:** None ---------- Hostnames: - ns561970.ip-139-99-123.net ---------- Domains: - ip-139-99-123.net ---------- Services: **80:** ``` HTTP/1.1 200 OK Content-Type: text/plain Content-Length: 18 ``` ---------- **443:** ``` HTTP/1.1 200 OK Content-Type: text/plain Content-Length: 18 ``` HEARTBLEED: 2023/04/11 04:19:15 139.99.123.196:443 - SAFE ---------- **5555:** ``` HTTP/1.1 200 OK Content-Type: text/plain Content-Length: 18 ``` ---------- **7777:** ``` HTTP/1.1 200 OK Content-Type: text/plain Content-Length: 18 ``` ---------- **9000:** `````` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '139.99.123.196']

Name

d0e8a398a903f1443a114fa40860b3db2830488813db9a87ddcc5a8a337edd73

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd0e8a398a903f1443a114fa40860b3db2830488813db9a87ddcc5a8a337edd73']

Name

http://arhivehaceru.com/payload

Pattern Type

stix

Pattern

[url:value = 'http://arhivehaceru.com/payload']

Name

arhivehaceru.com

Pattern Type

stix

Pattern

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

Name

de6dff4d3de025b3ac4aff7c4fab0a9ac4410321f4dca59e29a44a4f715a9864

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'de6dff4d3de025b3ac4aff7c4fab0a9ac4410321f4dca59e29a44a4f715a9864']

Name

7389e3aada70d58854e161c98ce8419e7ab8cd93ecd11c2b0ca75c3cafed78cb

Description

Unix.Trojan.DarkNexus-7679166-0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7389e3aada70d58854e161c98ce8419e7ab8cd93ecd11c2b0ca75c3cafed78cb']

Name

7d93419e78647d3cdf2ff53941e8d5714afe09cb826fd2c4be335e83001bdabf

Description

is__elf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7d93419e78647d3cdf2ff53941e8d5714afe09cb826fd2c4be335e83001bdabf']

Name

84.54.50.198

Description

CC=US ASN=AS211252 Delis LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '84.54.50.198']

Name

45.88.67.94

Description

ISP: Delis LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDb4bM+ExZ/

Z7tiuG2h+qmfThyTw32ZgO1gP97Ydk7kWkJQ oIttxp9Wka4LvXHBp7sC3VRZch9mzw1H/Yk8FzJ9vQ0Zs/pu8mDCVsPhcvCT72sVRdzvt9oF7T1y Z/ONl4wr+ToS0w/3Q77VFHLsteGZgJs6nAq/m1tyPQBl6DF1FaCd/H+YngUHlmprivBpQEIq8icg 1HV35vEqWbefhYLjPYb+HkMugjg1E++yxdI90foDZqcAM88RgHKoofSG9iejyqQkkDlijBOCsqPO dIx23QAxn574R5QVHdv11DjvmG3A8IcgQ+8VkGbdfIHoS+AVwbzsR3QTrsUh8QKfBZjz Fingerprint: 06:da:eb:ac:ad:9f:01:32:8a:af:ea:4e:c1:24:e8:28 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa 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 aes128-cbc aes192-cbc aes256-cbc blowfish-cbc cast128-cbc 3des-cbc 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/1.1 200 OK Date: Mon, 12 Jun 2023 10:22:48 GMT Server: Apache/2.4.6 (CentOS) Last-Modified: Sat, 08 Oct 2022 10:05:05 GMT ETag: "2be-5ea830f7cb640" Accept-Ranges: bytes Content-Length: 702 Content-Type: text/html; charset=UTF-8 ``` ---------- **666:** ``` HTTP/1.0 404 NOT FOUND Content-Type: text/html; charset=utf-8 Content-Length: 232 Server: Werkzeug/2.0.3 Python/3.6.8 Date: Sat, 17 Jun 2023 09:01:56 GMT ``` ---------- **1337:** ``` HTTP/1.1 200 OK Server: Transfer.sh HTTP Server X-Made-With: <3 by DutchCoders X-Served-By: Proudly served by DutchCoders Date: Mon, 12 Jun 2023 18:15:07 GMT Content-Length: 1951 Content-Type: text/plain; charset=utf-8 45.88.67.94: Easy file sharing from the command line === made with <3 by DutchCoders Upload: $ curl --upload-file ./hello.txt http://45.88.67.94/hello.txt Encrypt with gpg & upload: $ cat /tmp/hello.txt|gpg -ac -o-|curl -X PUT --upload-file "-" http://45.88.67.94/test.txt Download & decrypt with gpg: $ curl http://45.88.67.94/nETHat/test.txt|gpg -o- > /tmp/hello.txt Encrypt with openssl & upload: $ cat /tmp/hello.txt|openssl aes-256-cbc -pbkdf2 -e|curl -X PUT --upload-file "-" http://45.88.67.94/test.txt Download & decrypt with openssl: $ curl http://45.88.67.94/nETHat/test.txt|openssl aes-256-cbc -pbkdf2 -d > /tmp/hello.txt Grep pound from syslog and transfer cat /var/log/syslog|grep pound|curl --upload-file - http://45.88.67.94/pound.log Using Keybase: # import keys from keybase $ keybase track [them] # encrypt for recipients $ cat somebackupfile.tar.gz | keybase encrypt [them] | curl --upload-file '-' http://45.88.67.94/test.txt # decrypt $ curl http://45.88.67.94/nETHat/test.md |keybase decrypt Upload to Virustotal: $ curl -X PUT --upload-file nhgbhhj http://45.88.67.94/test.txt/virustotal Virusscan: $ curl -X PUT --upload-file nhgbhhj http://45.88.67.94/test.txt/scan Add shell function to .bashrc or .zshrc or its equivalent: === transfer(){ if [$# -eq 0];then echo "No arguments specified.\nUsage:\n transfer \n ... | transfer ">&2;return 1;fi;if tty -s;then file="$1";file_name=$(basename "$file");if [! -e "$file"];then echo "$file: No such file or directory">&2;return 1;fi;if [-d "$file"];then file_name="$file_name.zip" ,;(cd "$file"&&zip -r -q - .)|curl --progress-bar --upload-file "-" "http://45.88.67.94/$file_name"|tee /dev/null,;else cat "$file"|curl --progress-bar --

upload-file "-" "http://45.88.67.94//$file_name"|tee /dev/null;fi;else file_name=$1;curl --progress-bar --upload-file "-" "http://45.88.67.94//$file_name"|tee /dev/null;fi;} === $ transfer test.txt ``` ---------- **2121:** ``` HTTP/1.0 404 NOT FOUND Content-Type: text/html; charset=utf-8 Content-Length: 232 Server: Werkzeug/2.0.3 Python/3.6.8 Date: Thu, 15 Jun 2023 14:31:13 GMT ``` ---------- **7777:** ``` ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.88.67.94']

Name

http://arhivehaceru.com:2121/api?haceru=$haceru

Pattern Type

stix

Pattern

[url:value = 'http://arhivehaceru.com:2121/api?haceru=$haceru']

Domain-Name

Value
arhivehaceru.com

StixFile

Value
a163da5c4d6ee856a06e4e349565e19a704956baeb62987622a2b2c43577cdee
d0e8a398a903f1443a114fa40860b3db2830488813db9a87ddcc5a8a337edd73
14779e087a764063d260cafa5c2b93d7ed5e0d19783eeaea6abb12d17561949a
180d30bf357bc4045f197b26b1b8941af9ca0203226a7260092d70dd15f3e6ab
7389e3aada70d58854e161c98ce8419e7ab8cd93ecd11c2b0ca75c3cafed78cb
de6dff4d3de025b3ac4aff7c4fab0a9ac4410321f4dca59e29a44a4f715a9864
7d93419e78647d3cdf2ff53941e8d5714afe09cb826fd2c4be335e83001bdabf
e9bbe9aecfaea4c738d95d0329a5da9bd33c04a97779172c7df517e1a808489c
6bce1053f33078f3bbbd526162d9178794c19997536b821177f2cb0d4e6e6896
aabf2ef1e16a88ae0d802efcb2525edb90a996bb5d280b4c61d2870351e3fba4
437af650493492c8ef387140b5cb2660044764832d1444e5265a0cd3fe6e0c39

IPv4-Addr

Value
84.54.50.198
139.99.123.196
45.88.67.94

Url

Value
http://arhivehaceru.com/payload
http://arhivehaceru.com:2121/api?haceru=$haceru

External References

- https://otx.alienvault.com/pulse/64906f1ae8efba6ea78b79ee
- https://www.cadosecurity.com/tracking-diicot-an-emerging-romanian-threat-actor/