Mapping out AridViper Infrastructure Using Augury's Malware Module

team-cymru.com/blog/2020/12/16/mapping-out-aridviper-infrastructure-using-augurys-malware-addon

Josh Hopkins View all posts by Josh Hopkins December 16, 2020

Twitter user @BaoshengbinCumt posted malware hash *faff57734fe08af63e90c0492b4a9a56* on 27 November 2020, which they attributed to AridViper (APT-C-23 / GnatSpy)[i]. This user is a researcher for Qihoo and has previously reported on the activities of AridViper.

AridViper, also known as APT-C-23 and GnatSpy, are a group active within the Middle Eastern region, known in particular to target Israeli military assets.

The Augury Malware addon was used to map out further AridViper infrastructure, by pivoting from @BaoshengbinCumt's malware seed sample.

Note – All pivots undertaken within this exercise are detailed in the below chart and within a table at the end of the page:

faff57734fe08af63e90c0492b4a9a56

This sample, a packed Windows executable, was dropped via a malicious document disguised as a Curriculum Vitae – likely delivered in a phishing campaign.

Sandboxing of the sample identified a POST request made to hostname *judystevenson[.]info* as below:

URL	User-Agent	Method
http://judystevenson.info/vcapicv/vchivmqecv/vbqsrot	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	POST

The first pivot within the Augury Malware addon was to therefore look for other malware samples that had communicated with the C2 *judystevenson[.]info*.

judystevenson[.]info

Eight further samples were identified using the *judystevenson[.]info* C2 that was identified from the initial seed sample:

6e2d058c3508694a392194dbb6e9fe44

835f86e1e83a3da25c715e89db5355cc

89e9823013f711d384824d8461cc425d

94a5e595be051b9250e678de1ff927ac

ae0b53e6b378bf74e1dd2973d604be55

c27f925a7c424c0f5125a681a9c44607

f5bac4d2de2eb1f8007f68c77bfa460e

f93faca357f9a8041a377ca913888565

When sandboxing these samples (as well as *faff57734fe08af63e90c0492b4a9a56*) it was noted that the malware dropped the following file – *C:\ProgramData\GUID.bin*. This file was then used as the next pivot point.

C:\ProgramData\GUID.bin

18 samples had dropped this file during their execution within a sandbox environment:

1eb1923e959490ee9f67687c7faec697

20d21c75b92be3cfcd5f69a3ef1deed2

3296b51479c7540331233f47ed7c38dd

471313cb47c6165ec74088fafb9a5545

4b96fecd0c6451b30619e6e836fe7ffa

4d9b6b0e7670dd5919b188cb71d478c0

8d50262448d0c174fc30c02e20ca55ff

90cdf5ab3b741330e5424061c7e4b2e2

9bb70dfa2e39be46278fb19764a6149a

9bc9765f2ed702514f7b14bcf23a79c7

9d76d59de0ee91add92c938e3335f27f

a7cf4df8315c62dbebfbfea7553ef749

c12b3336f5efc8e83fcace6f81b27642

c4a90110acd78e2de31ad9077aa4eff6

c7d7ee62e093c84b51d595f4dc56eab1

e35d13bd8f04853e69ded48cf59827ef

e8effd3ad2069ff8ff6344b85fc12dd6

edc3b146a5103051b39967246823ca09

Five C2s were identified, associated with the above samples:

escanor[.]live

jaime-martinez[.]info

krasil-anthony[.]icu

nicoledotson[.]icu

ruthgreenrtg[.]live

Further pivots were undertaken based on ImpHash values derived from these samples and the AV signature *Win32/Revokery.J*, identifying a further five associated samples:

09cd0da3fb00692e714e251bb3ee6342

142a25bb5fd4612c9f6afcaad34fce37

46871f3082e2d33f25111a46dfafd0a6

758e432ed759013e0d00723c3d2af0c6

7fcfb64b1383d0d73f32dbe365fe4fdb

In addition to the five hostnames referenced above, the following two C2s were also extracted from these samples:

benyallen[.]club

chad-jessie[.]info

Pivoting on C2 *chad-jessie[.]info* subsequently identified a further sample:

fc5b2c81debf30d251d5220097c2f846

Returning to the original sample (*faff57734fe08af63e90c0492b4a9a56*), the user agent string identified in the POST request was used as another pivot.

URL	User-Agent	Method
http://judystevenson.info/vcapicv/vchivmqecv/vbqsrot	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	POST

Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)

A significant number of samples (approx. 600) were identified using this particular user agent string within C2 communications, therefore analysis focused on samples with a similar distinctive URL pattern to those samples already identified.

In undertaking this assessment, four samples were identified:

221c5982d545b4efb2cbee4e0597d154

947fd5f93c44807986f5663a739e0f46

f65e5bb6e35a3e28c2c878824293d939

f7a3f14ddbea80a1fe8653a8b71ce4df

Five C2s were identified, associated with the above samples:

jack-fruit[.]club

lordblackwood[.]club

angeladeloney[.]info

overingtonray[.]info

camilleoconnell[.]website

Pivoting on C2 *angeladeloney[.]info* subsequently identified a further three samples:

1d815939c4c4df5039185be9506ee88a

21aa63b42825fb95bf5114419fb42157

8b7ad86f74c3fb6d51e7cfb39fdd65be

A total of 40 malware samples were identified during this exercise, communicating with 13 C2s.

All pivots, identified samples and C2s are summarised in the below table:

Hash	C2	Association	Pivot
faff57734fe08af63e90c0492b4a9a56	judystevenson[.]info	Seed Sample	C2 – judystevenson[.]info Drops – C:\ProgramData\GUID.bin UA – Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
6e2d058c3508694a392194db-b6e9fe44	judystevenson[.]info	C2 – judystevenson[.]info	Drops – C:\ProgramData\GUID.bin
835f86e1e83a3da25c715e89db5355cc	judystevenson[.]info	C2 – judystevenson[.]info	Drops – C:\ProgramData\GUID.bin ImpHash – 2b67b7d14d1479dd7935f326d05a34d2
89e9823013f711d384824d8461cc425d	judystevenson[.]info	C2 – judystevenson[.]info	Drops – C:\ProgramData\GUID.bin

94a5e595be051b9250e678de1ff927ac	judystevenson[.]info	C2 – judystevenson[.]info	Drops – C:\ProgramData\GUID.bin
ae0b53e6b378bf74e1d-d2973d604be55	judystevenson[.]info	C2 – judystevenson[.]info	Drops – C:\ProgramData\GUID.bin
c27f925a7c424c0f5125a681a9c44607	judystevenson[.]info	C2 – judystevenson[.]info	Drops – C:\ProgramData\GUID.bin
f5bac4d2de2eb1f8007f68c77bfa460e	judystevenson[.]info	C2 – judystevenson[.]info	Drops – C:\ProgramData\GUID.bin
f93faca357f9a8041a377ca913888565	judystevenson[.]info	C2 – judystevenson[.]info	Drops – C:\ProgramData\GUID.bin
1eb1923e959490ee9f67687c7faec697	nicoledotson[.]icu	Drops – C:\ProgramData\GUID.bin	ImpHash – 5d8786b378c881f44443eb17940d6af6
20d21c75b92be3cfcd5f69a3ef1deed2	nicoledotson[.]icu	Drops – C:\ProgramData\GUID.bin	
3296b51479c7540331233f47ed7c38dd	nicoledotson[.]icu	Drops – C:\ProgramData\GUID.bin	
471313cb47c6165ec74088fafb9a5545	escanor[.]live	Drops – C:\ProgramData\GUID.bin	
4b96fecd0c6451b30619e6e836fe7ffa	ruthgreenrtg[.]live	Drops – C:\ProgramData\GUID.bin	ImpHash – 2b67b7d14d1479dd7935f326d05a34d2
4d9b6b0e7670d-d5919b188cb71d478c0	nicoledotson[.]icu	Drops – C:\ProgramData\GUID.bin	ImpHash – 51e53e55ec7d8af56797a171159d5535
8d50262448d0c174fc30c02e20ca55ff	nicoledotson[.]icu	Drops – C:\ProgramData\GUID.bin	ImpHash – 5d8786b378c881f44443eb17940d6af6
90cdf5ab3b741330e5424061c7e4b2e2	nicoledotson[.]icu	Drops – C:\ProgramData\GUID.bin	ImpHash – 51e53e55ec7d8af56797a171159d5535
9bb70dfa2e39be46278fb19764a6149a	nicoledotson[.]icu	Drops – C:\ProgramData\GUID.bin	ImpHash – 51e53e55ec7d8af56797a171159d5535
9bc9765f2ed702514f7b14bcf23a79c7	nicoledotson[.]icu	Drops – C:\ProgramData\GUID.bin	ImpHash – 51e53e55ec7d8af56797a171159d5535
9d76d59de0ee91add92c938e3335f27f	krasil-anthony[.]icu	Drops – C:\ProgramData\GUID.bin	AV – Win32/Revokery.J
a7cf4df8315c62dbebfbfea7553ef749	nicoledotson[.]icu	Drops – C:\ProgramData\GUID.bin	ImpHash – 5d8786b378c881f44443eb17940d6af6
c12b3336f5efc8e83fcace6f81b27642	ruthgreenrtg[.]live	Drops – C:\ProgramData\GUID.bin	ImpHash – 2b67b7d14d1479dd7935f326d05a34d2
c4a90110acd78e2de31ad9077aa4eff6	jaime-martinez[.]info	Drops – C:\ProgramData\GUID.bin	AV – Win32/Revokery.J
c7d7ee62e093c84b51d595f4dc56eab1	nicoledotson[.]icu	Drops – C:\ProgramData\GUID.bin	ImpHash – 51e53e55ec7d8af56797a171159d5535
e35d13bd8f04853e69ded48cf59827ef	escanor[.]live	Drops – C:\ProgramData\GUID.bin	
e8effd3ad2069ff8ff6344b85fc12dd6	nicoledotson[.]icu	Drops – C:\ProgramData\GUID.bin	
edc3b146a5103051b39967246823-ca09	nicoledotson[.]icu	Drops – C:\ProgramData\GUID.bin	ImpHash – 51e53e55ec7d8af56797a171159d5535
09cd0da3fb00692e714e251b-b3ee6342	nicoledotson[.]icu	ImpHash – 51e53e55ec7d8af56797a171159d5535	
46871f3082e2d33f25111a46dfafd0a6	nicoledotson[.]icu	ImpHash – 5d8786b378c881f44443eb17940d6af6	
758e432ed759013e0d00723c3d2af0c6	ruthgreenrtg[.]live	ImpHash – 2b67b7d14d1479dd7935f326d05a34d2	

142a25bb5fd4612c9f6afcaad34fce37	benyallen[.]club chad-jessie[.]info	AV – Win32/Revokery.J	C2 – chad-jessie[.]info
7fcfb64b1383d0d73f32dbe365fe4fdb	chad-jessie[.]info	AV – Win32/Revokery.J	C2 – chad-jessie[.]info
fc5b2c81debf30d251d5220097c2f846	chad-jessie[.]info	C2 – chad-jessie[.]info	
221c5982d545b4efb2cbee4e0597d154	jack-fruit[.]club lordblackwood[.]club	UA – Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	
947fd5f93c44807986f5663a739e0f46	angeladeloney[.]info	UA – Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	C2 – angeladeloney[.]info
f65e5bb6e35a3e28c2c878824293d939	overingtonray[.]info	UA – Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	
f7a3f14ddbea80a1fe8653a8b71ce4df	camilleoconnell[.]website	UA – Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	
1d815939c4c4df5039185be9506ee88a	angeladeloney[.]info	C2 – angeladeloney[.]info	
21aa63b42825fb95bf5114419fb42157	angeladeloney[.]info	C2 – angeladeloney[.]info	
8b7ad86f74c3fb6d51e7cfb39fdd65be	angeladeloney[.]info	C2 – angeladeloney[.]info	

Recent Passive DNS data was obtained for the identified hostnames, and is summarised in the table below:

Hostname	IP	Whois
angeladeloney.info	198.54.114.246	NAMECHEAP-NET, US
benyallen.club	198.54.117.197	NAMECHEAP-NET, US
camilleoconnell.website	58.158.177.102	UCOM ARTERIA Networks Corporation, JP
chad-jessie.info	198.54.116.43	NAMECHEAP-NET, US
escanor.live	198.187.29.152	NAMECHEAP-NET, US
jack-fruit.club	198.187.29.21	NAMECHEAP-NET, US
jaime-martinez.info	162.213.253.37	NAMECHEAP-NET, US
judystevenson.info	198.54.115.130	NAMECHEAP-NET, US
krasil-anthony.icu	68.65.122.52	NAMECHEAP-NET, US
lordblackwood.club	198.54.116.157	NAMECHEAP-NET, US
nicoledotson.icu	198.54.117.200	NAMECHEAP-NET, US
overingtonray.info	104.219.248.45	NAMECHEAP-NET, US
ruthgreenrtg.live	199.188.200.253	NAMECHEAP-NET, US

The use of NameCheap infrastructure has been observed in previous analysis of this group[ii]. It is believed that in the case of camilleoconnell[.]website, the identified IP address is not associated with the activities of AridViper.

[i] https://twitter.com/BaoshengbinCumt/status/1332186267295961089

[ii] https://research.checkpoint.com/2020/hamas-android-malware-on-idf-soldiers-this-is-how-it-happened/