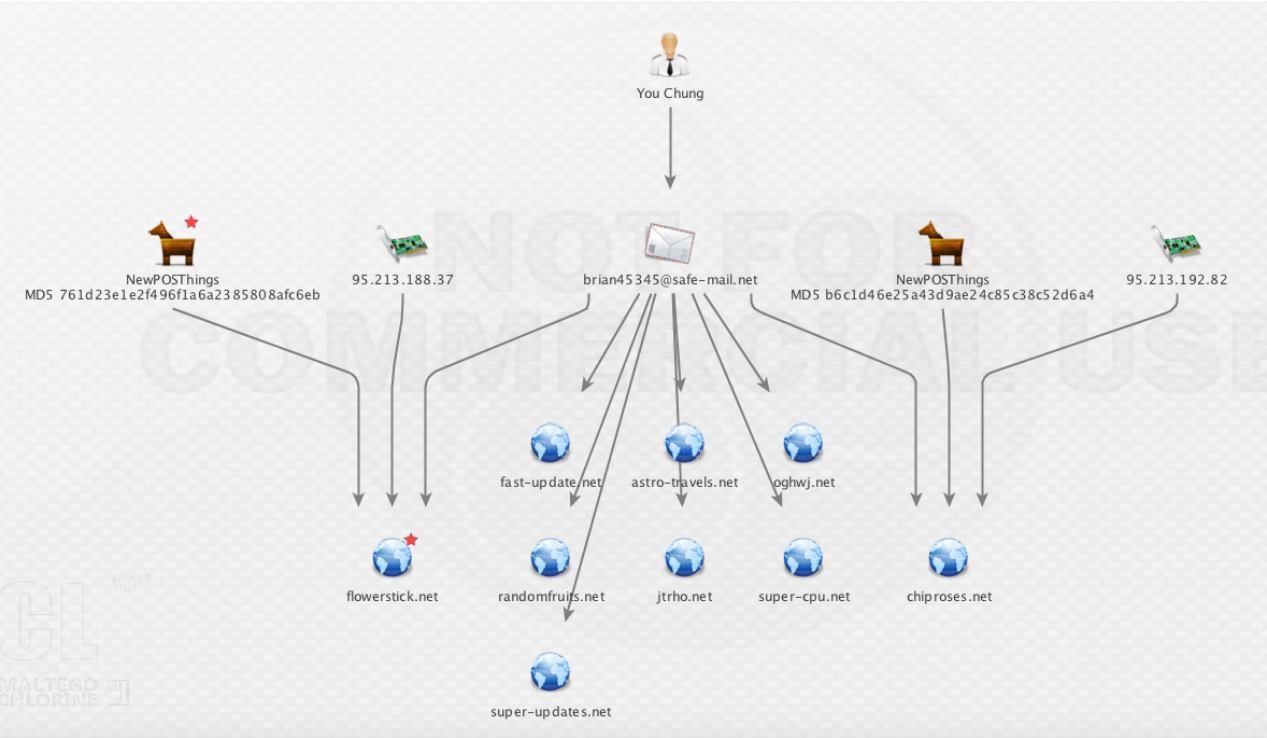
in Analysis

A Quick Look at A Likely NewPOSThings Sample

Executive Summary

- Nick Hoffman identified what is likely a new variant of NewPOSThings (**MD5: 761d23e1e2f496f1a6a2385808afc6eb**).
- Based on static analysis, the malware likely conducts the same activity observed in earlier NewPOSThings variants wherein it searches for and dumps passwords associated with VNC applications (e.g., RealVNC, UltraVNC). The malware also contains the hard-coded C2 domain **flowerstick[.]net.**
- An actor using the alias **You Chung** and email address **brian45345[at]safe-mail.net** registered nine domains–including **flowerstick[.]net**–between August 1 and September 13, 2015. These sites are almost certainly used as C2 nodes for POS and/or other malware. For example, one additional NewPOSThings sample (**MD5 b6c1d46e25a43d9ae24c85c38c52d6a4**) communicates to **chiproses[.]net**, which was registered to Chung on August 17.
- It is assumed that actors using the malware are targeting small- to medium-sized businesses given the malware's focus on VNC applications. Small businesses are generally more likely to use remote administration software for their POS terminals so that 3rd parties can manage the terminals.

Below is a Maltego graph showing the identified links between the malware, actor, and infrastructure.



Background

This afternoon, Nick Hoffman tweeted a link to a Virus Total report for a possible NewPOSThings sample with 0/56 detections. I've had an interest in POS malware for a while, so I decided to dive into this.

Nick Hoffman
@InfoSecKitten

Follow

More POS Malware with 0/53 detections -> virustotal.com/en/file/b1aa5e… Looks like a variant of NewPOSThings #posmalware #morphickdefense

12:29 AM - 26 Oct 2015

7 6

The Malware

Here are the basic details for the sample that Nick Hoffman tweeted.

```
File names target.xex
imphash 8a9d16cdb9e176c3c82504f76a420f32
File size 388.5 KB ( 397824 bytes )
MD5 761d23e1e2f496f1a6a2385808afc6eb
SHA1 0d4dbac3460a28245b119f77462a8d427cd9573a
SHA256 b1aa5e60251da1724eb03a191019a68b197831f374a955c0dd4f623fbc9826bc

Compilation timestamp 2015-08-11 17:29:43
First submission 2015-10-25 14:42:20 UTC ( 2 hours, 5 minutes ago )
Last submission 2015-10-25 14:42:20 UTC ( 2 hours, 5 minutes ago )
```

Unfortunately, the VirusTotal report doesn't provide much information. Luckily, we do have a Malwr report that we can use. Like the VirusTotal report, Malwr's automated dynamic analysis report provides no information. But, there are some useful details contained in the strings. Here is a list of interesting strings I was able to find and which can tell us a little bit more about the malware:

```
connect/5
flowerstick.net
Password
RealVnc:
TightVnc:
TigerVnc:
passwd=
UltraVnc:
Windows+8.1
Windows+8
Windows+7
Windows+Vista
Windows+Server+2003
Windows+XP
Windows+2000
targetScan.dll
Mozilla/4.0(compatible; MSIE 7.0b; Windows NT 6.0)
rSOFTWARE\RealVNC\vncserver
SOFTWARE\RealVNC\WinVNC4
Password
Software\TightVNC\Server
Software\TigerVNC\WinVNC4
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Ultravnc2_is1
ultravnc.ini
```

Firstly, the strings indicate that the malware is likely targeting

passwords for several VNC applications: RealVNC, TigerVNC, TightVNC, and UltraVNC. Previous write-ups from Palo Alto Networks and Trend Micro report that NewPOSThings searches for and dump passwords associated with these applications. Consistent with these reports, our sample contains the strings **passwd=** and **ultravnc.ini**.

Our sample also contains the same hard-coded User Agent **Mozilla/4.0(compatible; MSIE 7.0b; Windows NT 6.0)** that Palo Alto reported.

The Infrastructure & Actor

Most interesting in this sample is the existence of the hard-coded domain **flowerstick[.]net** which I assume to be the C2. It is possible that requests that the malware generates to this domain will contain **connect/5** in the URI. Lacking any dynamic analysis results though, I can't be sure.

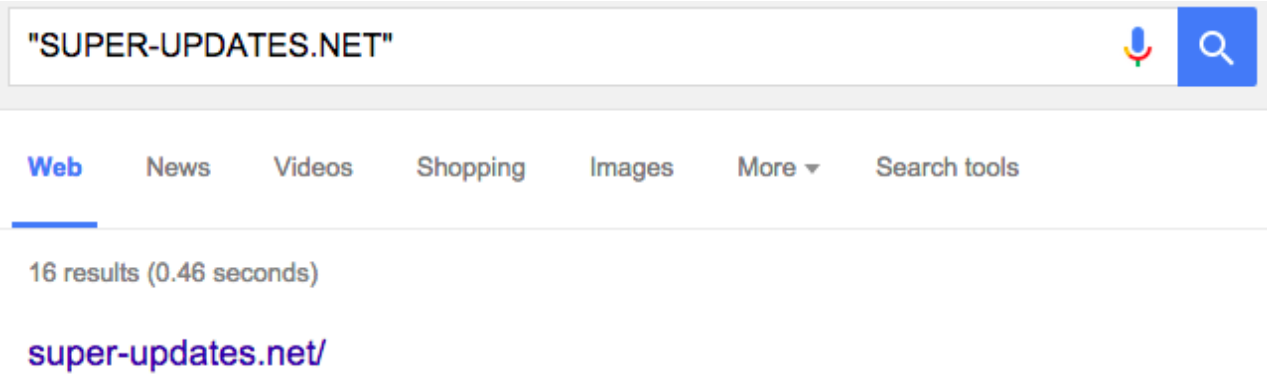
The domain **flowerstick[.]net** was created on August 1, 2015–10 days before the compilation of the malware we are examining–using the below registrant details. It has resolved to **95.213.188.37** since August 31, 2015, according to PassiveTotal.

```
Registrant Name: You Chung
Registrant Organization: Cmp
Registrant Street: 104 Rue
Registrant City: Bejing
Registrant State/Province: Bejing
Registrant Postal Code: 7050
Registrant Country: cn
Registrant Phone: +86.72768453
Registrant Phone Ext:
Registrant Fax: +86.72768453
Registrant Fax Ext:
Registrant Email: brian45345@safe-mail.net
```

The registrant **You Chung** (**brian45345[at]safe-mail.net**) has also created at least eight other sites.

```
astro-travels.net
chiproses.net
fast-update.net
flowerstick.net
jtrho.net
oghwj.net
randomfruits.net
super-cpu.net
super-updates.net
```

Some of these domains appear to have indexed directories. Because I don't have a safe, non-attrib machine at home to browse these directories, I decided not to touch them for now.



Interestingly, we can also see a clear timeline in the creation of these domains.

```
Domain Name: FLOWERSTICK.NET
Registrar: BIZCN.COM, INC.
Creation Date: 01-aug-2015

Domain Name: RANDOMFRUITS.NET
Registrar: BIZCN.COM, INC.
Creation Date: 13-aug-2015

Domain Name: SUPER-UPDATES.NET
Registrar: BIZCN.COM, INC.
Creation Date: 13-aug-2015

Domain Name: CHIPROSES.NET
Registrar: BIZCN.COM, INC.
Creation Date: 17-aug-2015

Domain Name: FAST-UPDATE.NET
Creation Date: 20-aug-2015
```

```
Domain Name: SUPER-CPU.NET
Registrar: BIZCN.COM, INC.
Creation Date: 23-aug-2015

Domain Name: ASTRO-TRAVELS.NET
Registrar: BIZCN.COM, INC.
Creation Date: 31-aug-2015

Domain Name: JTRHO.NET
Registrar: BIZCN.COM, INC.
Creation Date: 13-sep-2015

Domain Name: OGHWJ.NET
Registrar: BIZCN.COM, INC.
Creation Date: 13-sep-2015
```

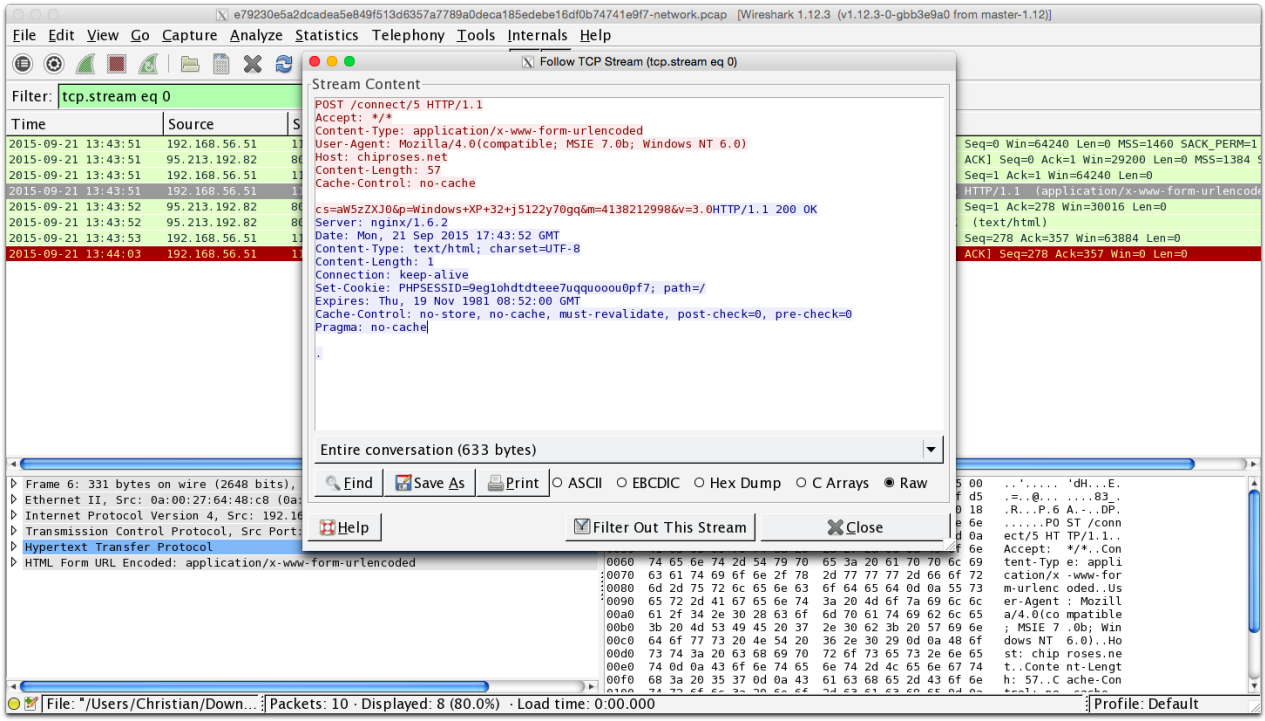
Additional NewPOSThings Sample

I found one sample that uses one of the nine **You Chung** domains for command-and-control–it is undoubtedly NewPOSThings.

```
MD5 b6c1d46e25a43d9ae24c85c38c52d6a4
SHA1 29051ca6c3e0c21065f2cbce8bfa2926f6d95fbd
SHA256 e79230e5a2dcadea5e849f513d6357a7789a0deca185edebe16df0b74741e9f7
```

Both Malwr and Payload Security have reports for this sample. Payload Security also provides a PCAP. As with our original sample (**MD5 761d23e1e2f496f1a6a2385808afc6eb**) from Nick Hoffman, this one contains various VNC-related strings and a hard-coded C2 domain, **chiproses[.]net** (**95.213.192.82**).

The PCAP also indicates that the string **connect/5** is indeed contained in the POST request URI as we originally assumed. Cool!



There is other content contained in this POST request as well:

```
cs=aW5zZXJ0&p=Windows+XP+32+j5122y70gq&m=4138212998&v=3.0
```

I'll have to look back at the Palo Alto Networks and Trend Micro posts to determine what the **cs=** and **m=** parameters are, but we can see that host OS information (**p=**) along with what is possibly the malware version (**v=**) is transmitted to the C2. Looking for these parameters and the **connect/5** URI in HTTP traffic could provide a reliable means of network detection.

Tell me what you think!

Artur Marek Maciag

October 26, 2015

Can we use this URL in the Knowledge Vault as
(EN #threats #technical #advanced #com #monitoring #newposthings #pos #malware #vnc #ioc #analysis #delivery #c2 #threatactor)?
https://docs.google.com/spreadsheets/d/17IuPDavAW-ZjsvpLhFDHQ5e4IlzBG2jowDFb5ozg1CM/edit?usp=sharing
This is part of Security Culture Initiative
https://drive.google.com/file/d/0B0TkBywht9JSM1YxLXk5NWhRdnM/view?usp=docslist_api

Reply to Artur

Christian
October 26, 2015

Of course!

Reply to Christian

Nick Hoffman
October 25, 2015

Excellent stuff! Keep up the great work!

Reply to Nick

Christian
October 25, 2015

Thank you!

Reply to Christian

Tell me what you think!

RELATED CONTENT BY TAG ANALYSIS NEWPOSTHINGS POSMALWARE