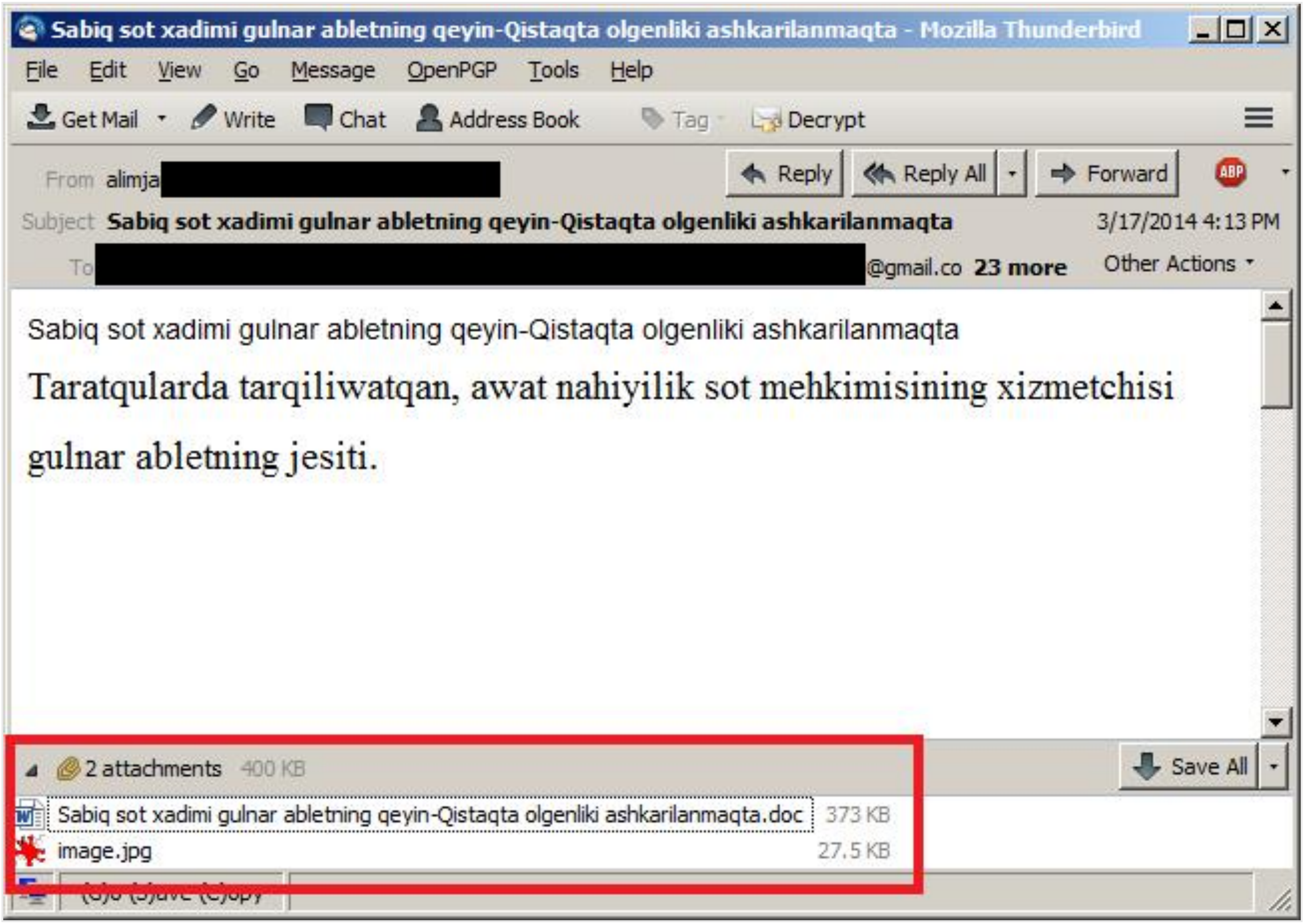
NetTraveler APT Gets a Makeover for 10th Birthday

We have written about NetTraveler before HERE and HERE.

Earlier this year, we observed an uptick in the number of attacks against Uyghur and Tibetan supporters using an updated version of the NetTraveler backdoor.

Here's an example of a targeted spear-phishing e-mail directed at Uyghur activists in March 2014.


Sabiq sot xadimi gulnar abletning qeyin-Qistaqta olgenliki ashkarilanmaqta - Mozilla Thunderbird
File Edit View Go Message OpenPGP Tools Help
Get Mail
Write
Chat
Address Book
Tag
Decrypt
Reply
Reply All
Forward
Other Actions
Save All

From alimja [redacted]

Subject **Sabiq sot xadimi gulnar abletning qeyin-Qistaqta olgenliki ashkarilanmaqta** 3/17/2014 4:13 PM

To [redacted] @gmail.co **23 more**

Sabiq sot xadimi gulnar abletning qeyin-Qistaqta olgenliki ashkarilanmaqta

Taratqularda tarqiliwatqan, awat nahiyilik sot mehkimisining xizmetchisi gulnar abletning jesiti.

2 attachments 400 KB

Sabiq sot xadimi gulnar abletning qeyin-Qistaqta olgenliki ashkarilanmaqta.doc 373 KB

image.jpg 27.5 KB

The e-mail has two attachments, a non-malicious JPG file and a 373 KB Microsoft Word .DOC file.

File name	"Sabiq sot xadimi gulnar abletning qeyin-Qistaqta olgenliki ashkarilanmaqta.doc"
MD5	b2385963d3afece16bd7478b4cf290ce
Size	381,667 bytes

The .DOC file, which in reality is a "Single File Web Page" container, also known as "Web archive file", appears to have been created on a system using Microsoft Office - Simplified Chinese.

It contains an exploit for the CVE-2012-0158 vulnerability, detected by Kaspersky Lab products as

Exploit.MSWord.CVE-2012-0158.db.

If run on a vulnerable version of Microsoft Office, it drops the main module as "net.exe" (detected by Kaspersky Lab products as **Trojan-Dropper.Win32.Agent.lifr**), which in turn installs a number of other files. The main C&C module is dumped into "**%SystemRoot%\system32\Windowsupdataney.dll**", (detected by Kaspersky as **Trojan-Spy.Win32.TravNet.qfr**).

Name	WINDOWSUPDATANEY.DLL
MD5	c13c79ad874215cfec8d318468e3d116
Size	37,888 bytes

It is registered as a service (named "Windowsupdata") through a Windows Batch file named "DOT.BAT" (detected by Kaspersky Lab products as Trojan.BAT.Tiny.b):

```
@echo off
@reg add
```

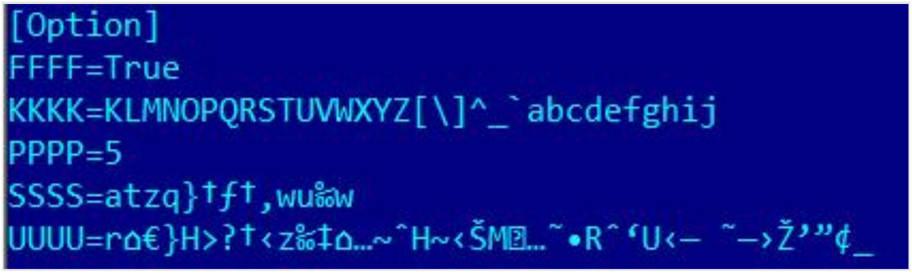
```
@echo off

@reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost" /v
Windowsupdata /t REG_MULTI_SZ /d Windowsupdata /f

@reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Windowsupdata" /v
ImagePath /t REG_EXPAND_SZ /d %SystemRoot%\System32\svchost.exe -k Windowsupdata /f

@reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Windowsupdata" /v
DisplayName /t REG_SZ /d Windowsupdata /f

@reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Windowsupdata" /v
ObjectName /t REG_SZ /d LocalSystem /f

@reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Windowsupdata" /v
ErrorControl /t REG_DWORD /d 1 /f

@reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Windowsupdata" /v Start /t
REG_DWORD /d 2 /f

@reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Windowsupdata\Parameters"
/v ServiceDll /t REG_EXPAND_SZ /d %SystemRoot%\system32\Windowsupdataney.dll /f
```

To make sure the malware isn't running multiple times, it uses the mutex "SD_2013 Is Running!" to mark its presence in the system. Other known mutexes used by older and current variants include:

- Boat-12 Is Running!
- DocHunter2012 Is Running!
- Hunter-2012 Is Running!
- NT-2012 Is Running!

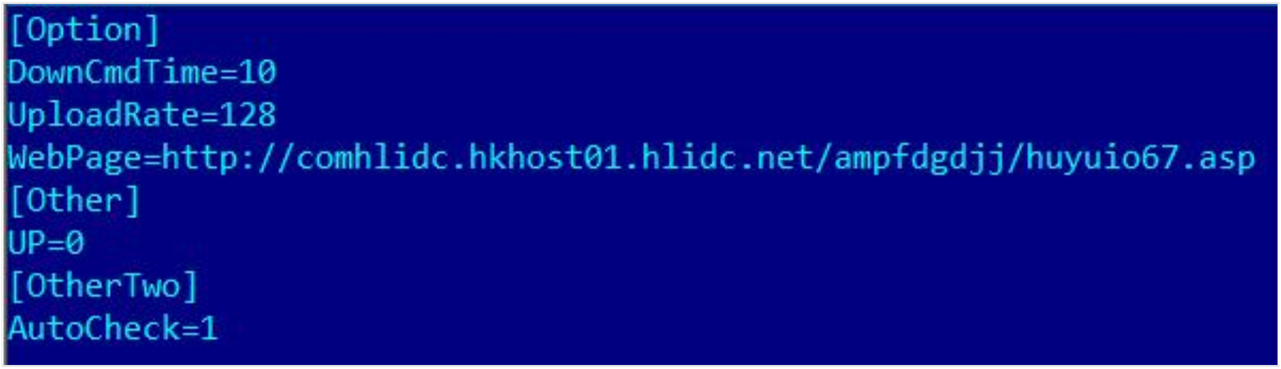
- NetTravler Is Running!
- NetTravler2012 Is Running!
- SH-2011 Is Running!
- ShengHai Is Running!
- SD2013 is Running!

The malware configuration file is written to the "SYSTEM" folder (as opposed to SYSTEM32) and has a slightly new format compared to "older" NetTraveler samples:



```
[Option]
FFFF=True
KKKK=KLMNOPQRSTUVWXYZ[\]^_`abcdefghij
PPPP=5
SSSS=atzq}†ƒ†,wu‰w
UUUU=r⌂€}H>?†‹z‰‡⌂…~ˆH~‹ŠM□…˜•Rˆ‘U‹— ˜—›Ž’”¢_
```

For the record, here's what an older NetTraveler config file looks like:



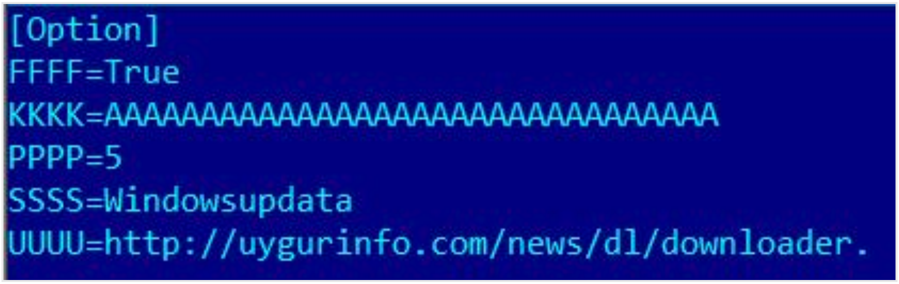
```
[Option]
DownCmdTime=10
UploadRate=128
WebPage=http://comhlidc.hkhost01.hlidc.net/ampfdgdjj/huyuio67.asp
[Other]
UP=0
[OtherTwo]
AutoCheck=1
```

Obviously, the developers behind NetTraveler have taken steps to try to hide the malware's configuration. Luckily, the encryption is relatively simple to break.

The algorithm is as follows:

for (i=0;i<string_size;i++)
decrypted[i]=encrypted[i] - (i + 0xa);

Once decrypted, the new config looks like this:



```
[Option]
FFFF=True
KKKK=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
PPPP=5
SSSS=Windowsupdata
UUUU=http://uygurinfo.com/news/dl/downloader.
```

One can easily see the command-and-control (C&C) server in the screenshot above, which is "**uyghurinfo[.]com**".

We identified several samples using this new encryption scheme. A list of all the extracted C&C servers can be found below:

C&C server	IP	IP location	Registrar
ssdcru[.]com	103.30.7.77	Hong Kong, Albert Heng, Trillion Company	SHANGHAI MEICHENG TECHNOLOGY
uygurinfo[.]com	216.83.32.29	United States, Los Angeles, Integen Inc	TODAYNIC.COM INC.
samedone[.]com	122.10.17.130	Hong Kong, Kowloon, Hongkong Dingfengxinhui Bgp Datacenter	SHANGHAI MEICHENG TECHNOLOGY
gobackto[.]net	103.1.42.1	Hong Kong, Sun Network (hong Kong) Limited	SHANGHAI MEICHENG TECHNOLOGY
worksware[.]net	N/A	N/A	SHANGHAI MEICHENG TECHNOLOGY
jojomic[.]com	was 202.146.219.14	Hong Kong, Sun Network (hong Kong) Limited	SHANGHAI MEICHENG TECHNOLOGY
angellost[.]net	was 103.17.117.201	hong kong hung tai international holdings	SHANGHAI MEICHENG TECHNOLOGY
husden[.]com	was 103.30.7.76	hong kong hung tai international holdings	SHANGHAI MEICHENG TECHNOLOGY

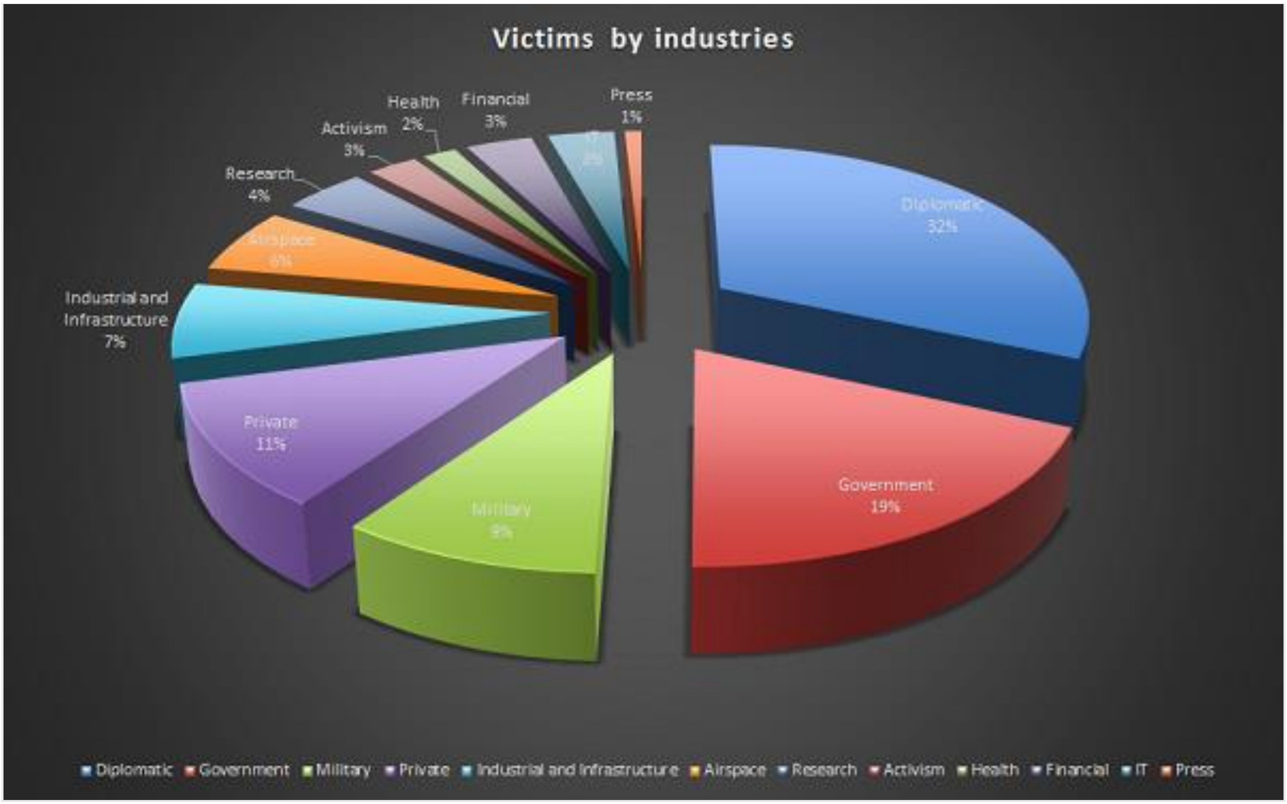
We recommend blocking all these hosts in your firewall.

Conclusion

This year, the actors behind NetTraveler celebrate 10 years of activity. Although the earliest samples we have seen appear to have been compiled in 2005, there are certain indicators that point to 2004 as the year when their activity started.

NetFile-801.exe
版权所有 (C) 2004

For 10 years NetTraveler has been targeting various sectors, with a focus on diplomatic, government and military targets.



NetTraveler victims by industry

Most recently, the main focus of interest for cyber-espionage activities revolved around space exploration, nano-technology, energy production, nuclear power, lasers, medicine and communications.

The targeting of Uyghur and Tibetan activists remains a standard component of their activities and we can assume it will stay this way, perhaps for another 10 years.