News

Where There is Smoke, There is Fire: South Asian Cyber Espionage Heats Up

Posted August 2, 2013 by TCIRT & filed under Research.

Summary:

The global proliferation of cyber espionage may be serving as a catalyst for regional entities within South Asia to adopt their own cyber espionage capabilities. Irrespective of the threats sophistication or motivation, South Asian cyber threats are likely emulating behaviors of larger regional powers to strategically influence national, organizational or individual objectives.

The ThreatConnect Intelligence Research Team (TCIRT) has identified an example of South Asian cyber espionage that is likely transcending sectors and regional geographic boundaries. Analyses of multiple customized malware binaries hosted within a small U.S. subnet have likely been used to target Indian military or government entities. The malware contains specific artifacts that point to a commercial Pakistani entity. Although the TCIRT cannot conclusively confirm direct involvement, several hypotheses have been developed which may account for the malware and observed activity. All of the following information and threat indicators are available within ThreatConnect.com and have been shared with the ThreatConnect community.

Operational Caveat: The ThreatConnect Intelligence Research Team has contacted the affected service providers and notified them of the activity observed.

Details associated with this threat have been shared with the ThreatConnect Community within Incident "20130731A: South Asia Cyber Espionage Heats Up".

It Takes Two to Tango:

Globalization has woven the Internet into a fabric that interlaces practically every aspect of modern living. Throughout the years, as evidenced in countless media reports, world superpowers have recognized and utilized the Internet as a powerful source for intelligence collection, and on occasion we have been offered glimpses as to how they are leveraging cyber espionage in support of their national diplomatic, military or economic objectives.

Similar to a younger sibling looking up to a big brother, regional and middle powers within South Asia are seeking to leverage global cyber espionage in an effort to achieve parity with nation states who have far-reaching diplomatic power, modernized militaries and influential economies. Ultimately, these emergent economies are likely seeking to hasten their path to success in fulfilling national objectives via the "short-cut" that cyber espionage offers.

Individual countries within the Indo-Pak subcontinent are increasingly involved in cyber attacks and targeted espionage campaigns. South Asia is no stranger to deeply rooted conventional conflict which is most often a strong harbinger of cyber conflict. On March 17th, 2013, the Norwegian-based, global telecommunications provider Telenor reported a network breach from an unknown sophisticated threat actor that targeted Telenor executives using custom malware implants. The attackers were responsible for pilfering email archives and documents from Telenor executives, compromising their intellectual property and business operations.

Nearly two months later, the Norwegian antivirus and security firm Norman issued an investigative analysis report titled Operation Hangover: Unveiling an Indian Cyberattack Infrastructure that detailed cyber espionage activities associated with the Telenor compromise. They noted similar targeting campaigns that were observed exploiting numerous industries and organizations within Norway, Pakistan, US, Iran, China, Taiwan, Thailand, Jordan, Indonesia, UK, Germany, Austria, Poland, and Romania. Norman speculated that a group associated with an identified private Indian information security company likely carried out the espionage campaigns.

Norman's 43 page assessment concluded that a sophisticated Indian exploitation team was indeed responsible for the network breach and Telenor compromise. The TCIRT believes that a possible theory that supports an Indian attack scenario is that the Telenor subsidiary, Telenor Pakistan, is a strategic communications infrastructure provider. Telenor Pakistan provides voice, data content and mobile communications to more than 3,500 cities and towns within Pakistan. Persistent remote Indian access to a strategic communications service provider, such as Telenor Pakistan, would certainly yield unparalleled signals intelligence collection capability. The information obtained would be of strategic value to Indian intelligence services.

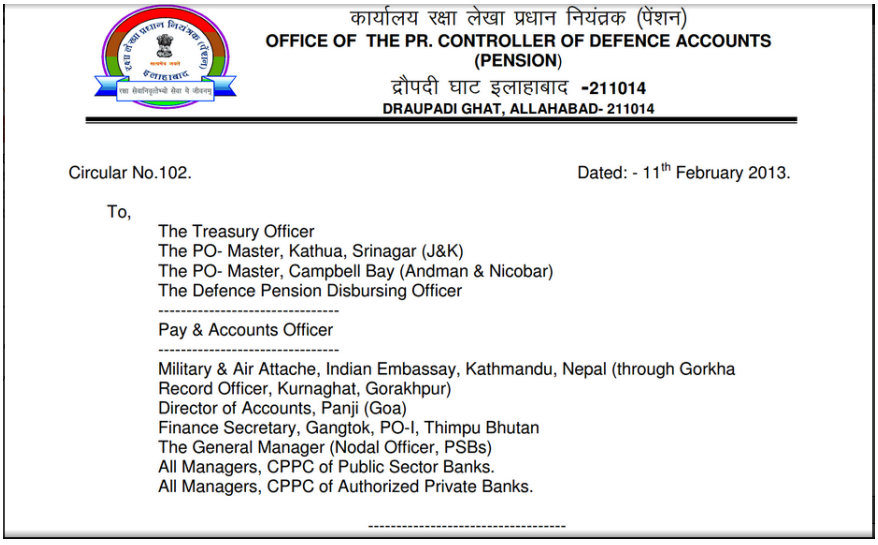
New Findings:

In light of the recent revelation of Indian involvement in the targeting of Telenor, it is critical for us to consider the borderless nature of cyber espionage and to understand how regional cyber conflicts can spill across geographies and affect critical commercial business operations.

As part of an ongoing TCIRT focused research and analysis, we have found custom malware being used operationally "in the wild" that may be targeting Indian military and government related entities, as well as other unidentified South Asian targets. This activity is possibly linked to an identified Pakistani information security company.

The Malware:

In late May 2013, TCIRT identified a malicious file hosted at [http://]199.91.173[.]43/new_salary/salary_revision.scr (Kansas City, Missouri). This file was a self-extracting (SFX) archive that, when executed, presents the target victim with a 12 page decoy PDF document. The document was an official Government of India (GoI), Ministry of Defense (MoD) pension memorandum of record. It is highly likely that the malware and decoy document would be tailored for and delivered to specific recipients associated with the GoI or MoD.



कार्यालय रक्षा लेखा प्रधान नियंत्रक (पेंशन)
OFFICE OF THE PR. CONTROLLER OF DEFENCE ACCOUNTS
(PENSION)
द्रौपदी घाट इलाहाबाद -211014
DRAUPADI GHAT, ALLAHABAD- 211014

Circular No.102. Dated: - 11th February 2013.

To,

The Treasury Officer
The PO- Master, Kathua, Srinagar (J&K)
The PO- Master, Campbell Bay (Andman & Nicobar)
The Defence Pension Disbursing Officer

Pay & Accounts Officer

Military & Air Attache, Indian Embassy, Kathmandu, Nepal (through Gorkha Record Officer, Kurnaghat, Gorakhpur)
Director of Accounts, Panji (Goa)
Finance Secretary, Gangtok, PO-I, Thimpu Bhutan
The General Manager (Nodal Officer, PSBs)
All Managers, CPPC of Public Sector Banks.
All Managers, CPPC of Authorized Private Banks.

The SFX dropper contained multiple custom executable files, as well as legitimate Microsoft Visual C++ Runtime Library files, which are part of the codebase used to develop and required to execute the backdoor code. The malware also uses the legitimate cURL library in the form of libcurld.dll. The open-source cURL library is a multiprotocol transfer library used primarily for FTP and HTTP transactions.

Name	Size	Packed Size	Modified
ExtractPDF.exe	58 880	26 323	2013-05-28 04:59
libcurld.dll	378 368	138 988	2013-04-26 05:24
Microsoft.VC90.DebugCRT.manifest	532	336	2007-11-06 08:24
msvcr90d.dll	1 180 672	334 722	2007-11-06 13:19
Start.exe	61 440	27 640	2013-05-30 01:48
winsocks.exe	158 208	71 697	2013-05-23 10:21
salary.pdf	462 635	412 557	2013-05-30 15:52

The main backdoor component is found in winsocks.exe. The files ExtractPDF.exe and Start.exe simply serve as utilities to open the PDF file and execute the winsocks.exe backdoor component. When executed, the winsocks.exe backdoor requests a PHP update callback at [http://]199.91.173[.]43/fetch_updates_8765.php?compname=<COMPUTERNAME>.

0000000200C8	0000004216C8	0	http://199.91.173.43/fetch_updates_8765.php?compname=
00000020100	000000421700	0	userfile
0000000210C	00000042170C	0	%02d/%02d/%d %02d:%02d
00000020144	000000421744	0	.docx
0000000214C	00000042174C	0	.pptx
0000000215C	00000042175C	0	.xlsx
0000000216C	00000042176C	0	APPDATA
00000020174	000000421774	0	\version.txt
00000020184	000000421784	0	\execute.exe
00000020194	000000421794	0	\pathfile.txt
000000201A4	0000004217A4	0	\tempfile.txt
000000201B4	0000004217B4	0	http://199.91.173.43/version.txt
000000201D8	0000004217D8	0	http://199.91.173.43/iexplore.exe
00000020200	000000421800	0	bad cast
0000000233C	00000042193C	0	e+000
00000020356	000000421956	0	GAIsProcessorFeaturePresent
00000020374	000000421974	0	KERNEL32
00000020380	000000421980	0	1#QNAN
00000020388	000000421988	0	1#INF
00000020390	000000421990	0	1#IND
00000020398	000000421998	0	1#SNAN
00000020400	000000421A00	0	C:\Users\Tranchulas\Documents\Visual Studio 2008\Projects\upload\Release\upload.pdb

A version.txt file is also requested by the malware. This file contained a version number 1.0, likely denoting the version of the backdoor and/or the command and control (C2) backend. The winsocks.exe backdoor also contains hardcoded strings of Office file extensions, telegraphing the likely intention of the attackers in collecting and exfiltrating office automated documents from victim networks.

Another variant of this backdoor uses the same winsocks.exe with a different dropping mechanism and was found at [http://]199.91.173[.]43/Classified_Video.flv.scr and [http://]199.91.173[.]43/sarbajit_leaked_video.wmv.scr. Both of these .scr files have the same MD5.

In this SFX, Windows batch files had replaced the ExtractPDF.exe and Start.exe with a decoy Flash video (FLV) file was used in place of the decoy PDF. An FLV file is an interesting choice of decoy document since it is not a standard video format for media players. The dynamic DNS domains windowsupdate.no-ip[.]biz and masalavideos.no-ip[.]biz were also being mapped to IP Address 199.91.173.43 as of late May 2013, when the video themed malicious attachments were being operationalized. When opened the flash video simply displays a couple kissing passionately. Implementing the use of free dynamic DNS services, such as those of NO-IP within targeting and exploitation phases of attack, are very common techniques used by a variety sophisticated threat groups.

The file sarbajit_leaked_video.wmv.scr contains a compile time of May 28, 2013 19:53:26 UTC. The filename is possibly a misspelled reference to Sarabjit Singh, an Indian national who was arrested and convicted of terrorism and espionage charges in 1991 by Pakistani authorities. After a protracted 22 year legal battle, Sarabjit Singh would become the victim of a severe beating by Pakistani prisoners and would later die of his injuries in a Lahore hospital on May 2, 2013. News of the attack and subsequent death of Sarabjit Singh incited protests in India that increased regional Indo-Pakistani tensions and served as a catalyst for bilateral governmental negotiations between Delhi and Islamabad. This file was created 26 days after the death of Sarabjit Singh, and would be of relevance to targeted Indian entities, much like the official Government of India (GoI), Ministry of Defense (MoD) pension memorandum.

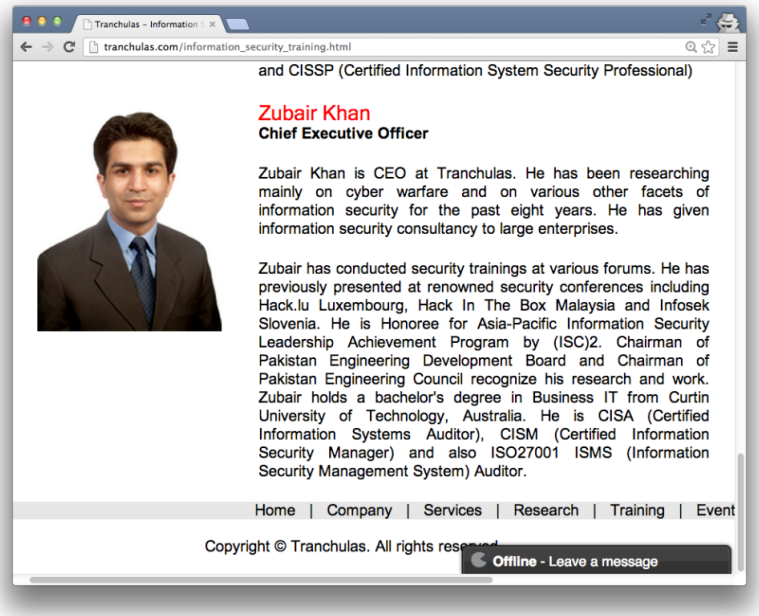
Significant Malware Artifacts:

Operational Caveat: It is important to note that there are information gaps which diminish our ability to establish a definitive explanation for the malicious activity and identify the responsible entities behind the authorship and use of the identified malware. Below the TCIRT simply highlights the facts associated with specific artifacts identified within the malware.

Most of the dropped malware binaries contained a debug string that sheds light on the possible developers and operators of the malware.

Hosting & C2 IP Address	Parent File	Dropped File	MD5 Hash (Dropped File)	Compile Date	Debug String	Callback
199.91.173.43	Classified_Video.flv.scr Salary_Revision.scr Sarbajit_Leaked_Video.wmv.scr	winsocks.exe	03f528e752dee57b1ff050a72d30de60	5/23/2013	C:\Users\Tranchulas\Documents\Visual Studio 2008\Projects\upload\Release\upload.pdb	fetch_updates_8765.php
199.91.173.43	salary_revision.scr	ExtractPDF.exe	3779e7aaf019e2d4064b006ca0090275	5/28/2013	C:\Users\Cath\documents\visual studio 2010\Projects\ExtractPDF\Release\ExtractPDF.p	
199.91.173.43	salary_revision.scr	Start.exe	9512de5b4615561af6881285159e2bb4	5/30/2013	C:\Users\Cath\documents\visual studio 2010\Projects\Start\Release\Start.pdb	
Likely 199.91.173.45	Unknown Likely downloaded as window.dll	windefender.exe	801c8bac8aea4d0226e47551c808a331	6/14/2013	C:\Users\Cert-India\Documents\Visual Studio 2008\Projects\ufile\Release\ufile.pdb	fetch_updates_8765_tb.php is_array.php
Likely 199.91.173.45	Unknown Likely downloaded as window.dll	windefender.exe	a21f2cb65a3467925c1615794cce7581	6/25/2013	C:\Users\umairaziz27\Documents\Visual Studio 2008\Projects\usb\Release\usb.pdb	fetch_updates_8765_tb.php is_array.php
199.91.173.45	Naxalites_Funded_by_Pakistan.docx.scr	showppt.exe	165ac370b54e664812e4c15b2396ccd6	6/26/2013		Downloads update_dll.dll (Start.exe) and window.dll (windefender.exe)
199.91.173.45	OBL_Leaked_Report.scr	windefender.exe	35663e66d02e889d35aa5608c61795eb	7/9/2013	C:\Users\Cert-India\Documents\Visual Studio 2008\Projects\ufile\Release\ufile.pdb	fetch_updates_8765_tb.php is_array.php
199.91.173.45	OBL_Leaked_Report.scr	Start.exe	0303b07ed9e11626399b91278539c9ff	7/9/2013		

The significance of the username Tranchulas within the debug path of the winsocks.exe binary is that Tranchulas is a Pakistani information security consulting company with offices in the United Kingdom, United States, and Pakistan. The CEO of Tranchulas is Zubair Khan, a Pakistani national and information security executive who has "been researching mainly on [sic] cyber warfare". Khan also likely maintains a close relationship to the Pakistani government. According to this online biography, he is responsible for the penetration testing of Pakistani homeland security solutions and has consulted for the Pakistani National Database and Registration Authority (NADRA).



Proximity to such sensitive security programs suggest a certain level of trust on behalf of the Pakistani government, and may indicate that official Pakistani entities could have access to Tranchulas technical support for various security projects or programs. An ironic, yet noteworthy observation is that the Tranchulas website boasts Telenor as a client.

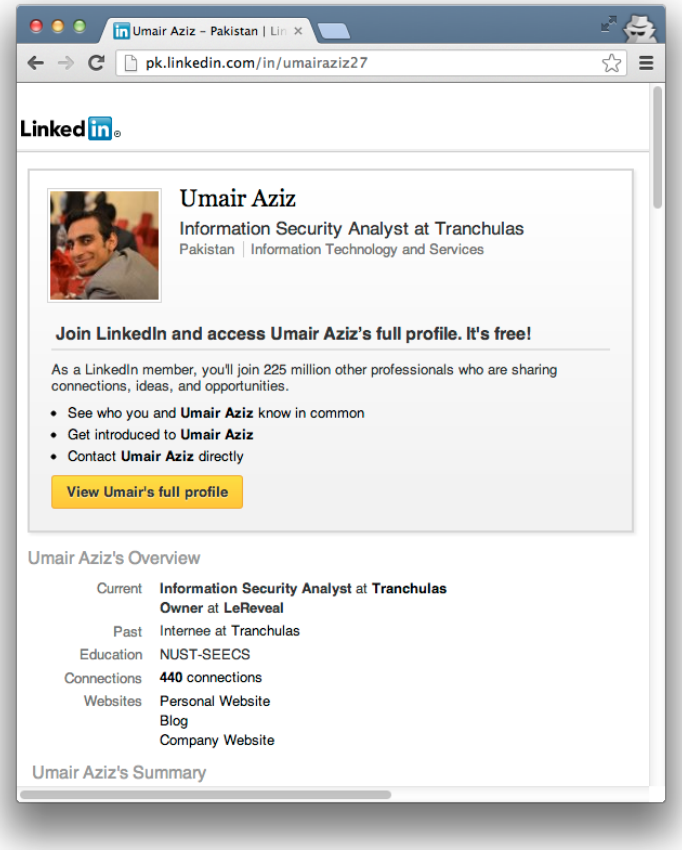
Tranchulas also serves as an official sponsor for the Pakistan CERT in addition to maintaining the official Pakistan CERT website (cert.org.pk).

On July 2, 2013 a similar file windefender.exe (MD5: a21f2cb65a3467925c1615794cce7581) was identified containing a strong association to Tranchulas. This particular binary contained the following debug string:

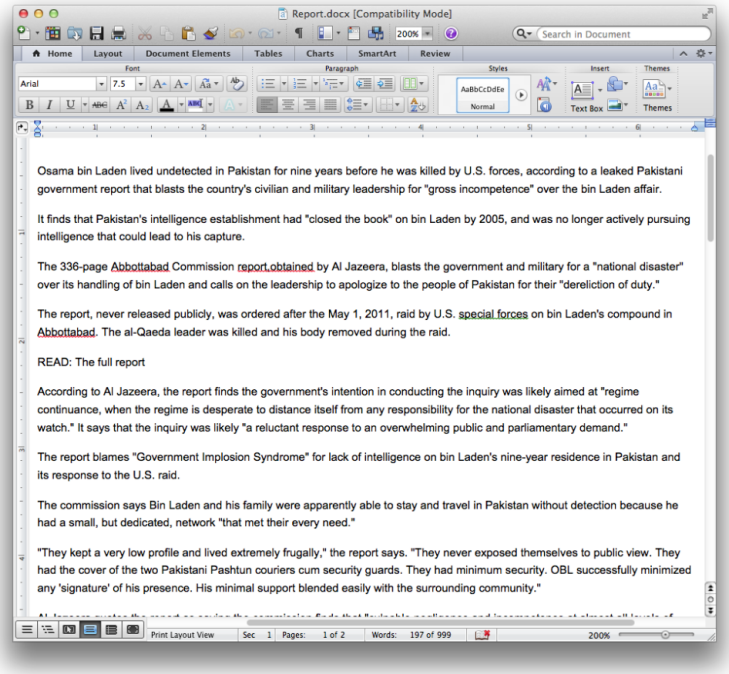
C:\Users\umairaziz27\Documents\Visual Studio 2008\Projects\usb\Release\usb.pdb

The username "UmairAziz27" reveals a Twitter account @umairaziz27 for an "Optimistic Patriot by choice" who is "Working as InfoSec Analyst at @Tranchulas."

Umair Aziz (*umairaziz27*) maintains a LinkedIn professional profile that highlights his employment at Tranchulas and reveals that he was educated at the National University of Sciences and Technology School of Electrical Engineering and Computer Science (NUST-SEECS) in Pakistan.



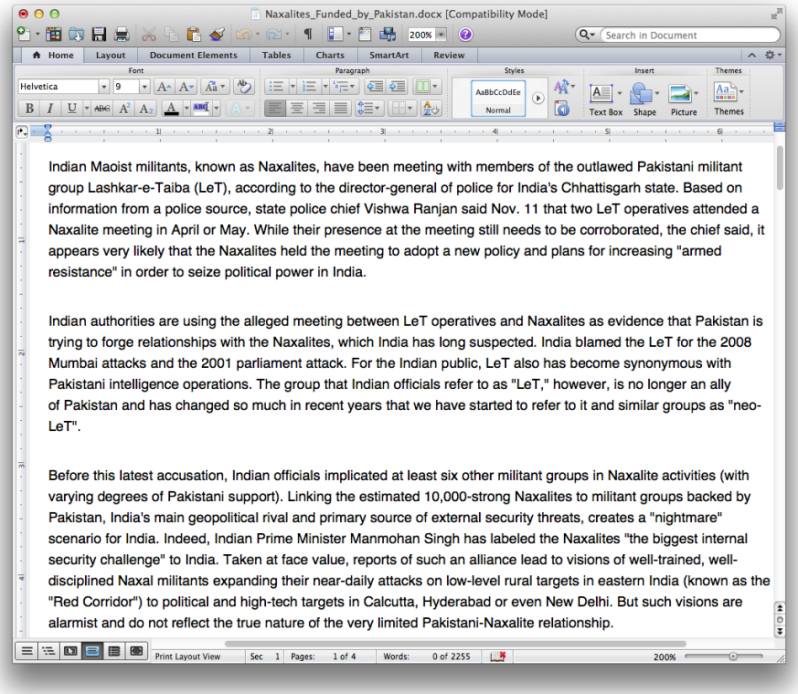
A second host within the same 199.91.173[.]40/29 subnet was also identified hosting similar zipped malware at [http://]199.91.173[.]45/OBL_Leaked_Report.zip and [http://]199.91.173[.]45/Naxalites_Funded_By_Pakistan.zip. The OBL_Leaked_Report.zip contained a .scr file that drops a decoy document pertaining to the alleged incompetence of Pakistani authorities in locating Osama Bin Laden (OBL).



This OBL malware drops a windefender.exe backdoor component (MD5: 35663e66d02e889d35aa5608c61795eb) In this case, the debug string is:

C:\Users\Cert-India\Documents\Visual Studio 2008\Projects\ufile\Release\ufile.pdb.

The binaries that contain the "umairaziz27" and "Cert-India" debug strings are designed to call back to [http://]199.91.173[.]45/fetch_updates_8765_tb.php?compname=<COMPUTERNAME> and [http://]199.91.173[.]45/is_array.php?compname=<COMPUTERNAME>. Meanwhile, the Naxalites_Funded_By_Pakistan.scr file drops a slightly different malware component and an alternate decoy document.



The dropped implant, showppt.scr (MD5: 165ac370b54e664812e4c15b2396ccd6), is a downloader that connects to [http://]199.91.173[.]45/ and downloads both legitimate library files and malicious second stage binaries.

Working Hypotheses:

The use of Tranchulas and UmairAziz27 in the malware debugging paths, in addition to the multiple targeting campaigns that maintain themes likely aimed at Indian entities or involving Pakistan related issues, leads us to assess the following competing hypotheses which may be considered as plausible explanations for the identified activity:

- Hypothesis 1: Tranchulas developed the malicious binaries, and staged them for offensive exploitation operations on behalf of an unidentified customer.

- Hypothesis 2: Tranchulas developed and sold the malicious binaries to an unidentified customer, where they were later operationalized by an unidentified entity.
- Hypothesis 3: An unidentified third party unaffiliated with Tranchulas developed the malware, deliberately including misleading software artifacts as a direct effort to create speculation and shift blame toward Tranchulas.
- Hypothesis 4: A rogue Tranchulas employee used company resources without company knowledge to develop the malware, where an unknown operator later used it offensively.
- Hypothesis 5: Indian entities actively sought and utilized the services of Pakistan based information security company, Tranchulas, for an officially sanctioned and authorized penetration test. The malicious implants were subsequently developed and used as part of official Tranchulas service offerings, while the files and infrastructure used for the audit were submitted to publicly available malware analysis services.
- Hypothesis 6: An unidentified Indian entity developed and used this malware as a realistic simulated exercise to perform penetration testing and evaluate their readiness in the event of actual Pakistani affiliated offensive network operations. The files and infrastructure used for the simulation were submitted to publicly available malware analysis services.

Conclusion:

Considering the long-standing regional tensions between India and Pakistan, South Asia serves as a likely flashpoint for conventional conflict to carry over and play out within cyberspace. Public and private sectors alike should begin to increase their awareness of emerging cyber threats from the lesser-known middle powers. Regardless of sophistication, these threats may support future belligerents who have or will eventually possess the capability and intent to disrupt critical business operations.

Details associated with this threat have been shared with the ThreatConnect Community within Incident "*20130731A: South Asia Cyber Espionage Heats Up*". If you or your organization is interested in obtaining crowd-sourced threat intelligence that increases your awareness of emerging cyber threats, please register at ThreatConnect.com and join our community.

Tags: Cyber Espionage, India, Pakistan, South Asia, Telenor

Previous article Next article

No Comments

Recent Posts

Categories

- Research

Archives

- January 2014
- December 2013
- November 2013
- October 2013
- September 2013
- August 2013

Threat Connect. Identify the Threat Sign up for Free

Follow Us

- Facebook
- Twitter

Contact Us • Privacy Policy • Terms of Service

Threat Intelligence

- Why Threat Intelligence is Important
- How to Develop Threat Intelligence
- Community Collaboration Case Study

Platform

- Capabilities
- Integrations
- ThreatConnect™ API
- ThreatConnect™ Cloud
- Cloud Security
- Upgrade

Communities

- Private Communities
- Moderated Common Community
- Moderated Subscriber Communities
- Intelligence Research Team
- Data Privacy

Methodology

- Diamond Model of Intrusion Analysis
- Threat Inference Engine
- Collaborative Intelligence

News & Events

- In The News
- Press Releases
- Blog

About

- Leadership
- Careers
- Contact Us