



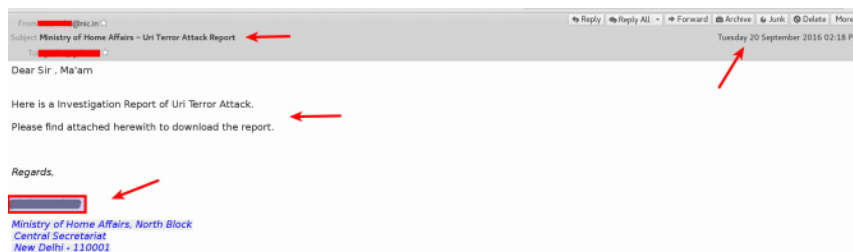
## URI TERROR ATTACK & KASHMIR PROTEST THEMED SPEAR PHISHING EMAILS TARGETING INDIAN EMBASSIES AND INDIAN MINISTRY OF EXTERNAL AFFAIRS

1 MONTH AGO • ARTICLES • ♥ 22

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 spoofed the email ids associated with Indian Ministry of Home Affairs to send out email to the victims. 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



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*)

In the second wave of attack slightly different theme was used, this time attackers used the [Jammu & 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.



## 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 triggered 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.

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.

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.

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

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

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.

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.

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 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



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

### 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.

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

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

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.



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.

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.

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)*

*84d9d0524e14d9ab5f88bbe6d2d2582 (officeupdate.exe)*

#### **Network Indicators Associated with C2:**

*khanji[.]ddns[.]net*

*139[.]190[.]6[.]180*

*39[.]40[.]141[.]25*

*175[.]110[.]165[.]110*

*39[.]40[.]144[.]245*

*39[.]40[.]167[.]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*



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):**

*028caf3b1f5174ae092ecf435c1fcc2*

*7732d5349a0cfa1c3e4bcfa0c06949e4*

*9909f8558209449348a817f297429a48*

*63698ddbdf5be7d5a7ba7f31d0d592c*

*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 officials)*
- *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.symantec.com/connect/blogs/simple-njrat-fuels-nascent-middle-east-cybercrime-scene>

Follow us on Twitter: [@monnappa22](#) [@cysinfo22](#)

SHARE: [f](#) [t](#) [g+](#) [p](#)



**MONNAPPA K A**

[in](#)

**20 COMMENTS**



**Mayur Vaishnav**

January 19, 2017 at 6:12 pm

[Reply](#)

#Nice article



**Sumith**

January 19, 2017 at 6:19 pm

[Reply](#)

Great article . Keep up the great work Monnappa!  
Using pastebin to host the code is indeed interesting idea by the attacker.



**Winston**

January 19, 2017 at 7:13 pm

[Reply](#)

what an article!!! Awesome Monappa



**Sriram**

January 19, 2017 at 7:19 pm

[Reply](#)

Great job! Very well written!



**Biprodeep Roy**

January 19, 2017 at 9:35 pm

[Reply](#)

Very Informative article!



**Yathish**

January 19, 2017 at 9:38 pm

[Reply](#)

Amazing work Monna!



**raj chandel**

January 19, 2017 at 10:08 pm

[Reply](#)

Nice Article Thanks for sharing



**Petter**

January 19, 2017 at 10:28 pm

[Reply](#)



**Donny**

January 20, 2017 at 9:46 am

Reply

Great post sir! Very informative 😊



**Karthikganesan**

January 20, 2017 at 7:20 pm

Reply

Good one monappa.continue the same



**Sebastian**

January 20, 2017 at 8:11 pm

Reply

great post ..



**Shahjahan**

January 20, 2017 at 8:38 pm

Reply

Great Analysis ! Flow chart of analysis is superb



**Nagarjuna**

January 20, 2017 at 10:43 pm

Reply

Wow..Excellent article 😊



**Amit Gupta**

January 22, 2017 at 2:04 am

Reply

Amazing analysis and brilliant conclusion.



**Ajan Kancharla**

January 23, 2017 at 3:29 pm

Reply

Wonderful work!



**Prashanth Sivarajan**

January 28, 2017 at 3:40 am

Reply

Wonderful as usual Monappa...keep up the good work.



**raj**

January 28, 2017 at 1:13 pm

Reply

Great Work



**sam**

February 2, 2017 at 12:36 pm

Reply

well done keep it up i have learn a lot from this article.



**Mark Cutting**

February 7, 2017 at 12:59 pm

Reply

Superb article. Very in depth analysis, and well worth the read. Highly recommended.



**Guru**

February 18, 2017 at 3:28 pm

Reply

Excellent article and deep analysis.

**LEAVE A REPLY**

Comment



POST COMMENT

Copyright © 2016 Cysinfo.com. All Rights Reserved

