In-Depth Look at New Variant of MONSOON APT Backdoor, Part 2

blog.fortinet.com/2017/04/05/in-depth-look-at-new-variant-of-monsoon-apt-backdoor-part-2

April 5, 2017

Threat Research

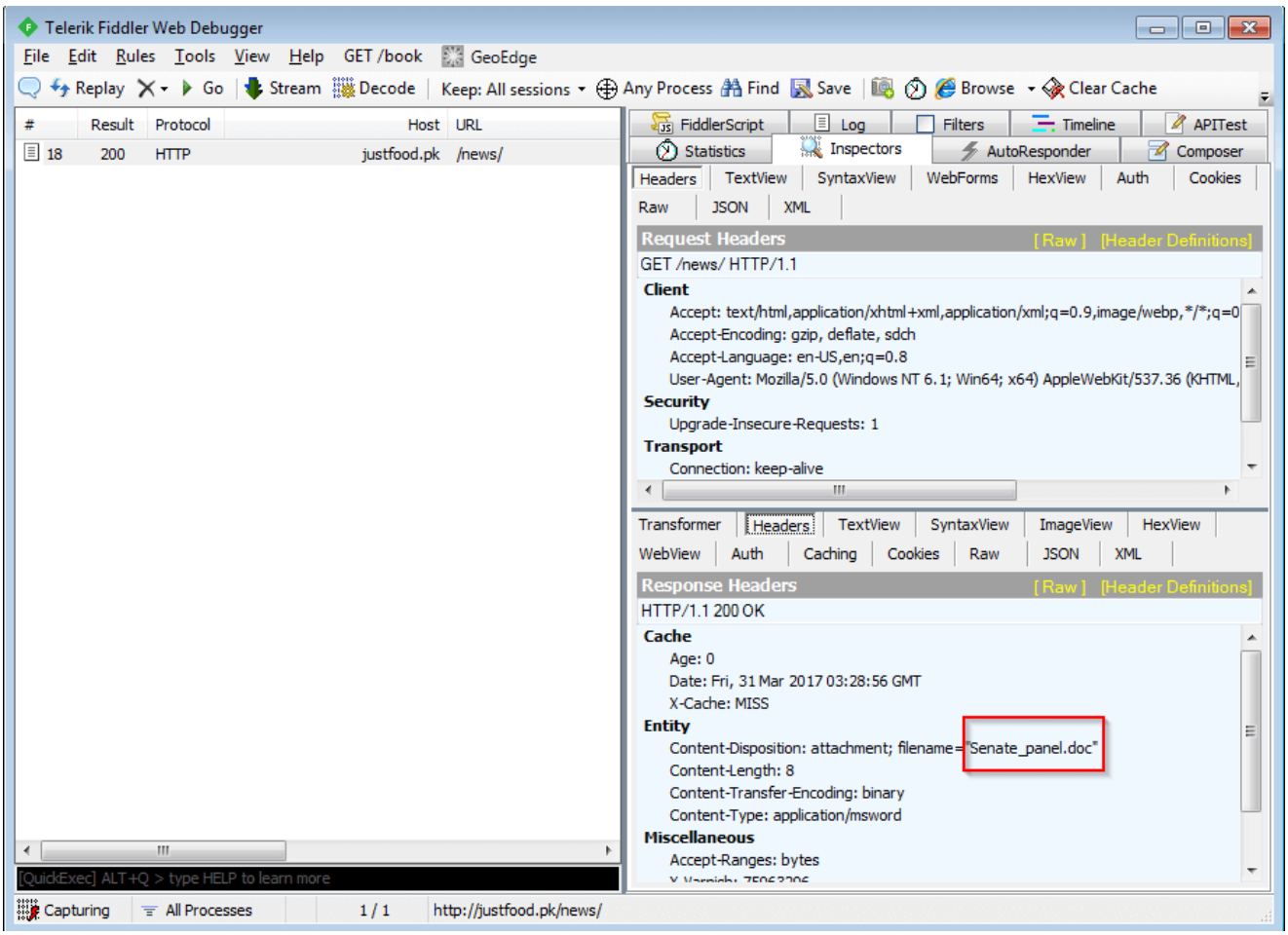
By Jasper Manuel and Artem Semenchenko | April 05, 2017
In part 1 of FortiGuard Labs' analysis of a new variant of the BADNEWS backdoor, which is actively being used in the MONSOON APT campaign, we did a deep technical analysis of what this backdoor of capable of and how the bad guys control it using the command and control server. In this part of the analysis, we will try to discover who might be behind the distribution of these files.

Who's Behind these Malicious Files

In part 1, we discussed that the BADNEWS backdoor is being dropped by a malicious RTF exploiting CVE-2015-1641. Interestingly, these RTF exploits contain an INCLUDEPICTURE field to insert a picture into the document which points to these URLs:

> hxxp://aliandqazi.com/Jobs/
>
> hxxp://www.tassonedil.it/news/
>
> hxxp://www.justfood.pk/news/

Curiously, we tried visiting the URL hxxp://www.justfood.pk/news/ from the RTF exploit to see the reply:



The URL returns the DOC file, “Senate_panel.doc.” However, the file returned is only 8 bytes long. Interestingly, it contains next sequence of bytes:

> “0D 0A 20 20-20 20 20 20”:
>
> “0D 0A” – is a “\r\n” – standard sequence of bytes for new line.
>
> “20” – is a spacebar.

There is not much we can tell from the content of this file, but the name of the returning file, “Senate_panel.doc”, is not accidental. This name is closely tied with the file content. Moreover, the initial RTF exploit was submitted on VT with this name:

Date	File name	Source	Country
2017-03-06 10:15:17	Senate_panel.doc	10219402 (web)	GB

So this is not a coincidence, and the people who crafted the RTF exploit somehow control *Justfood.pk.*

So let’s now look at this main page of the site:

Date	File name	Source	Country
2017-03-06 10:15:17	Senate_panel.doc	10219402 (web)	GB

We see that this site was hacked by somebody with the Nickname *R00T D3STR0Y3R*. And it was hacked before the RTF file was uploaded on VT.

Here is a screenshot from hacker’s database, from February of 2017.

As we can see, *Justfood.pk* was hacked by *R00T D3STR0Y3R* from the anti-Pakistan group "*LulzSec india,*" and it is happened no later than 2017-02-09.

The RTF exploit file was uploaded on VT on 2017-03-06. So there is a good chance that R00T D3STR0Y3R already controlled this site when it was used for attacks with the RTF exploit.

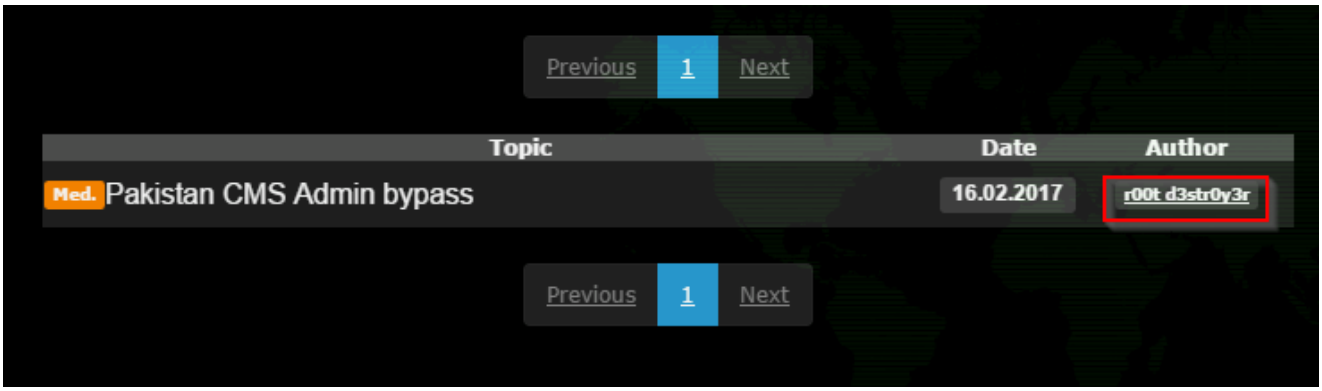
We can't tell for sure if *R00T D3STR0Y3R* stands behind the *BadNews* attacks, or this may just be a coincidence and he merely "defaced" the site that was used by another anti-Pakistan group.

But that seems unlikely. However, we think that the legal authorities of India have no need to guess since it is very probable that they can ask R00T D3STR0Y3R in person.

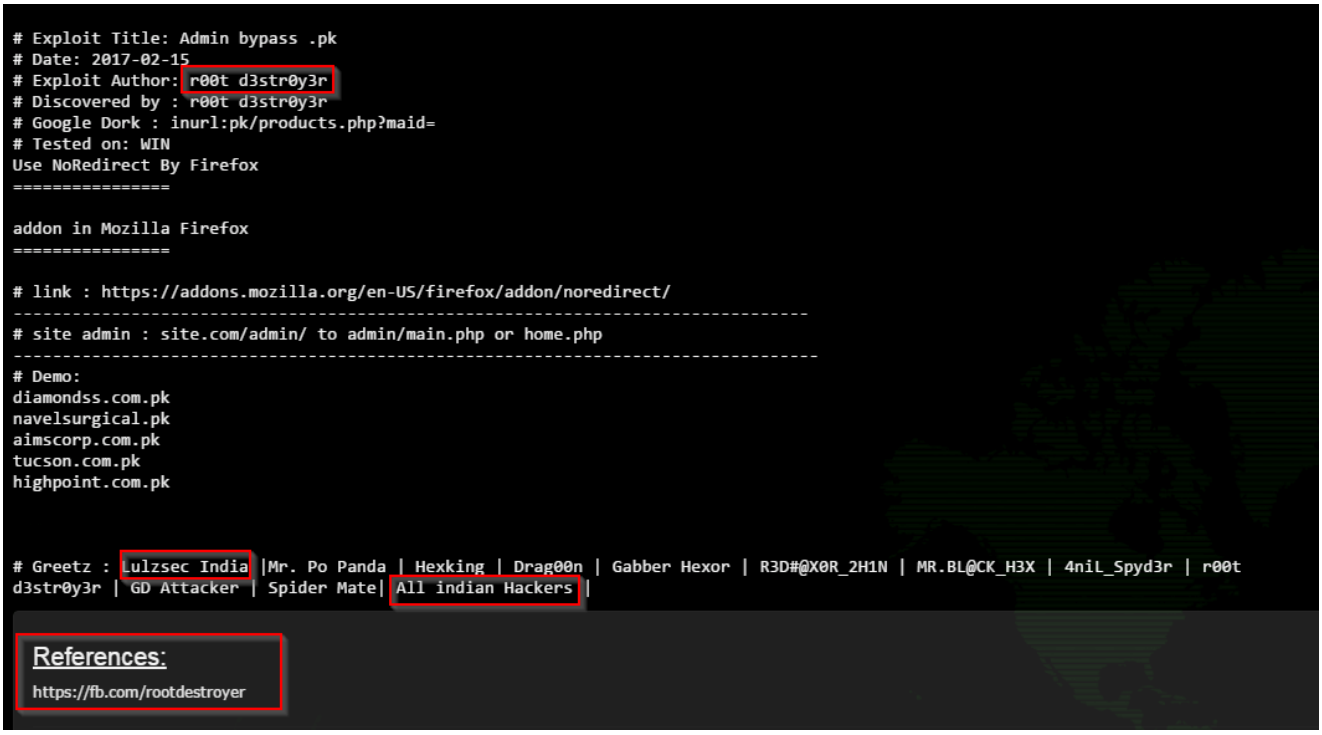
Actually, finding *R00T D3STR0Y3R's* real identity was pretty easy and straightforward.

First, we found this script on the cxsecurity site:

https://cxsecurity.com/search/author/DESC/AND/FIND/1/10/r00t+d3str0y3r/



Inside the script there are credits to "*R00T D3STR0Y3R,*" along with greetings to "*Lulzsec India*" and "*All indian Hackers*":



There is also a reference to this Facebook page.

https://www.facebook.com/rootdestroyer

We followed the link and…

Please welcome *Mukund Rajput* from the "*Dr. Jivraj mehta Institute Of Technology*":

Date	File name	Source	Country
2017-03-06 10:15:17	Senate_panel.doc	10219402 (web)	GB

This page claims that *Mukund* and *r00t d3str0y3r* are the same person.

Of course, we can't tell if this claim is true or not. But we hope that Indian Law enforcement agencies try to answer that question.

Conclusion

BADNEWS backdoor is not a sophisticated piece of malware. In fact, it doesn't use any new malware techniques at all. It is neither packed nor heavily obfuscated. Its tring obfuscation is just simple reversing and minus 1 encryption. But, it uses proven techniques to bypass the HIPS detection used by security programs by piggybacking onto a signed legitimate file, which allows it to deliver its malicious payload. It also proves, once again, that there's rarely any need to use stealthier or more sophisticated attacks, because simple techniques work.

Bad news though for the bad guys, and good news for our customers, as Fortinet covers detection for the BADNEWS backdoor as W32/Bdnews.A!tr.bdr and the malicious RTF as MSOffice/CVE_2015_1641.A!exploit.

C&C URLs were also blocked by Fortinet's Web Filter.

-= FortiGuard Lion Team =-

IOCs:

Sha256:

bf93ca5f497fc7f38533d37fd4c083523ececc34aa2d3660d81014c0d9091ae3

17c3d0fe08e1184c9737144fa065f4530def30d6591e5414a36463609f9aa53a

8e0574ebf3dc640ac82987ab6ee2a02fc3dd5eaf4f6b5275272ba887acd15ac0

0c63ef29d5a9674a00bb71a150d2ae6f3dc856a43291e79260992f08fdcd53d3

0c63ef29d5a9674a00bb71a150d2ae6f3dc856a43291e79260992f08fdcd53d3

722e8909235ae572c7baa522a675ce45ac7e10170be7428de74d04f051f473c9

f61aa8c6590926533b67467603d2f42cdb1d5e1f20a5439d7e58fdaf81710711

c9642f44d33e4c990066ce6fa0b0956ff5ace6534b64160004df31b9b690c9cd

C&C Urls:

hxxp://www.webrss.com/createfeed.php?feedid=49321

hxxp://feed43.com/0414303388550176.xml

hxxps://r0nald2017.wordpress.com/2017/02/16/my-first-post/

hxxps://github.com/r0nald2017/project1/blob/master/xml.xml

r0b1n.crabdance.com

r0nald.ignorelist.com

hxxps://musicall12.wordpress.com/29-2/

hxxp://overthemontains.weebly.com/paragliding-stuff

hxxps://raw.githubusercontent.com/Zunaid-zunaid1/project11/master/xml.xml

d0nald1.strangled.net

d0nald2.strangled.net

d0nald.strangled.net

hxxp://feed43.com/5787707581531238.xml

hxxp://www.webrss.com/createfeed.php?feedid=49297

hxxps://robins0n12.wordpress.com/2017/01/31/my-biography/

hxxps://raw.githubusercontent.com/devonkearns/cricket/master/xml.xml

maxx.crabdance.com

mu5.ignorelist.com

hxxp://80.255.3.96/r0g3r/dqvabs.php

185.82.217.200/@lb3rt/dqvabs.php

hxxp://80.255.3.96/max1mu5/dqvabs.php

Related Posts