SECTRIO

MALWARE REPORT

VBS Exploit-Dropper

Date: 12/05/2021

Sanjuktasree Chatterjee

VBScript scripting is one of the most common ways the attacker uses to find out existing vulnerabilities on windows OS. The attacker can use the obfuscation method to hide from other antivirus and Microsoft inbuilt threat detection.

On 11th May 2021, we found a zero-day Visual Basic Script file in our honeypot which is highly malicious. This file is a variant of an Exploit Downloader, that drops payload through which the attacker can gain access to the victim machine and can steal valuable information from there.

File Hash: 8d0d62101bf15edc9922f0209ad95e89

Technical Analysis:

Workflow:

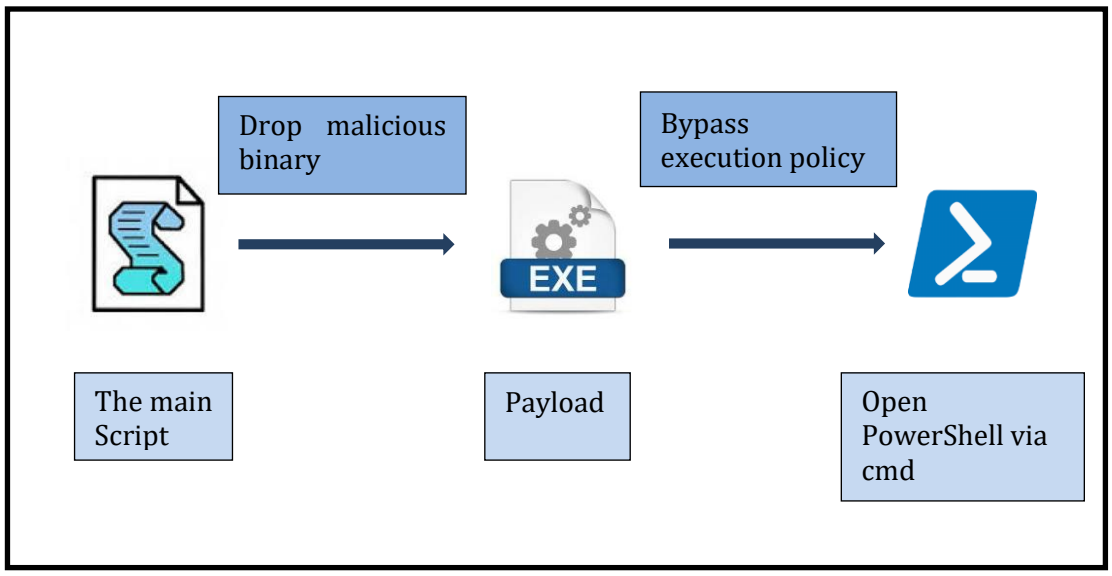

Fig: 1

In the code of the script, it uses the obfuscation technique to evade detection from the antivirus. The text has been encoded in "Base64encoding"format (Fig: 2).

```
Function iqbxOPkT(qxxVcQRENmEcUk)
    cjBrbGOyy = "<B64DECODE xmlns:dt=" & Chr(34) & "urn:schemas-microsoft-com:datatypes" &
        "dt:dt=" & Chr(34) & "bin.base64" & Chr(34) & ">" & _
        qxxVcQRENmEcUk & "</B64DECODE>"
```

Fig: 2

The file contains a large "base64" encoded characters that are shown below Fig: 3.

Fig: 3

The above code has been decoded and it shows that there is an executable file embedded into the script. The below Fig: 4 shows that it is a portable executable (PE) file which can be extracted by the process of the script and it will run on Windows OS to perform another action.

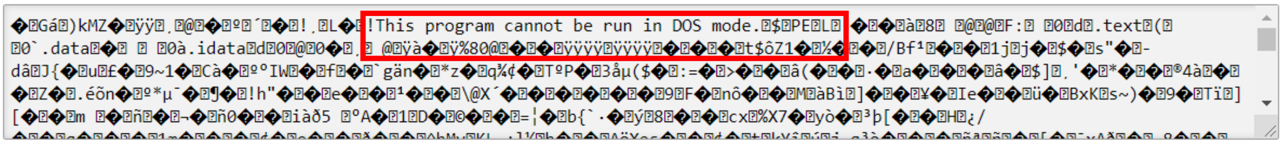

Fig: 4

When we run the script, it drops a payload in the temp folder and there is another folder that gets created under temp in which the file is dropped.

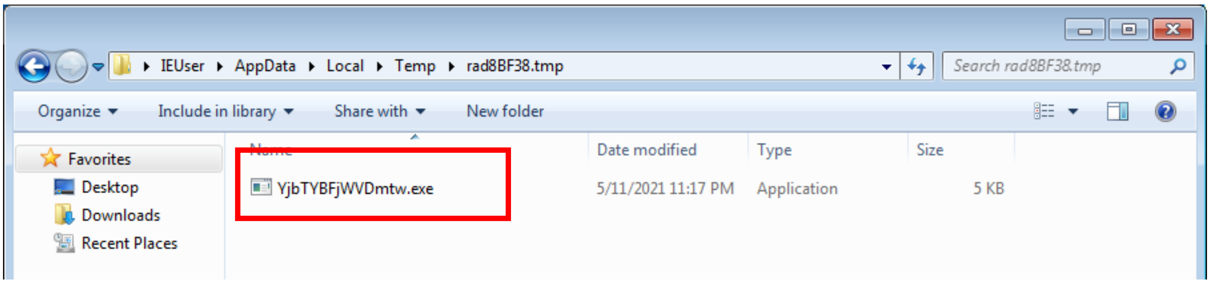

Fig: 5

Fig: 6 shows that the script will first create a folder within temp and drop the embedded payload into that. The binary is dropped in the system file so that it can hide its persistence.

```
Set AeQDFuwbbyva = CreateObject("Scripting.FileSystemObject")
Dim warsiWsAJCD
Dim QwNHQrNZmUR
Set warsiWsAJCD = AeQDFuwbbyva.GetSpecialFolder(2)
QwNHQrNZmUR = warsiWsAJCD & "\" & AeQDFuwbbyva.GetTempName()
AeQDFuwbbyva.CreateFolder(QwNHQrNZmUR)
```

Fig: 6

The embedded binary will drop with the name "`YjbTYBFjWVDmtw.exe`".

```
QwNHQrNZmUR = warsiWsAJCD & "\" & AeQDFuwbbyva.GetTempName()
AeQDFuwbbyva.CreateFolder(QwNHQrNZmUR)
letYntIc = QwNHQrNZmUR & "\" & "YjbTYBFjWVDmtw.exe"
Dim HjfuvdtJ
```

Fig: 7

When the process runs in the background, the file communicates with the IP `192.168.1.6`

No.	Time	Source	Destination	Protocol	Length	Info
8001	28.996498	10.0.2.15	192.168.1.6	TCP	62	[TCP Retransmission] 49207 → 443 [SYN] Seq=0 Wi
8002	32.100574	fe80::256b:4013:414…	ff02::1:2	DHCPv6	149	Solicit XID: 0xce86af CID: 000100011d9201c60015
8003	40.092312	fe80::256b:4013:414…	ff02::1:2	DHCPv6	149	Solicit XID: 0xce86af CID: 000100011d9201c60015
8004	41.010732	10.0.2.15	192.168.1.6	TCP	66	[TCP Port numbers reused] 49207 → 443 [SYN] Seq
8005	44.013008	10.0.2.15	192.168.1.6	TCP	66	[TCP Retransmission] 49207 → 443 [SYN] Seq=0 Wi
8006	50.103377	10.0.2.15	192.168.1.6	TCP	62	[TCP Retransmission] 49207 → 443 [SYN] Seq=0 Wi
8007	56.189883	fe80::256b:4013:414…	ff02::1:2	DHCPv6	149	Solicit XID: 0xce86af CID: 000100011d9201c60015

```
Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{53152A2F-39F7-458E-BD58-24D170992
Ethernet II, Src: PcsCompu_99:b1:5f (08:00:27:99:b1:5f), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 103.216.204.18
```

Fig: 8

Fig: 9 shows that the executable is packed to avoid detection.

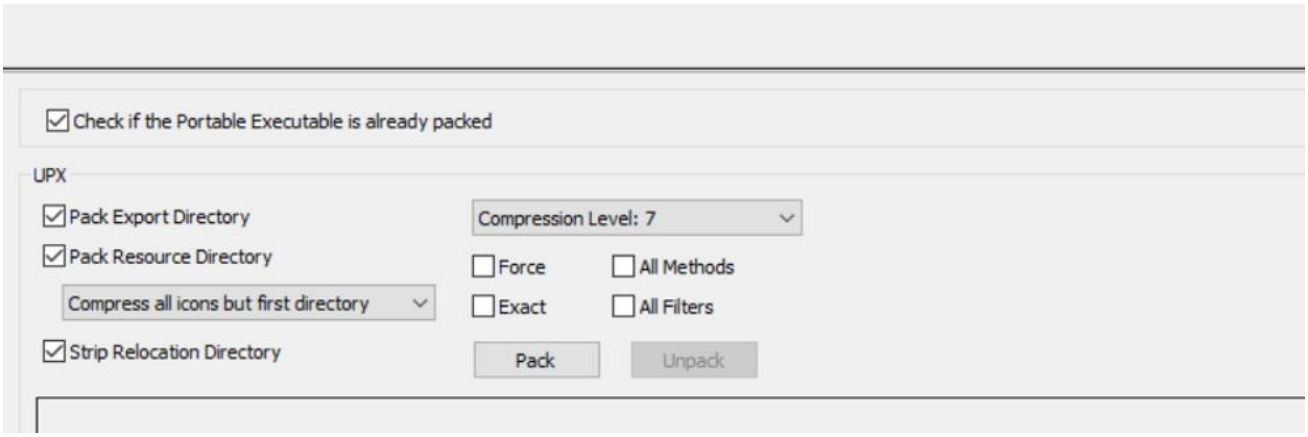

Fig: 9

The binary when executed, opens command prompt and in the background the default security settings of PowerShell which is by default restricted is changed. Because of this, any malicious script can be run through PowerShell and it will leave the system vulnerable. The attacker can gain access to all the important data on the machine.

Fig: 10

IOCS:

File Hash:

bb753c98cee0cc8403f5b7df5c6772f22da65e84f34f31501e8a99eb1450bde4

MITRE Techniques:

User Execution: Malicious File(T1204)
Scripting(T1064)
Exploit Public-Facing Application(T1190)
Command and Scripting Interpreter: PowerShell(T1059)
Execution – PowerShell(T1086)

CVE:

CVE-2018-8221
CVE 2021 24082

Sectrio Protection

Sectrio detects this script as 'SS_Gen_Dropper_VBS_AA'.
Sectrio detects the binary as "SS_Gen_Exploit_PE_AA".

Our Honeypot Network

This report has been prepared from the threat intelligence gathered by our honeypot network. This honeypot network is today operational in 72 cities across the world. These cities have at least one of the following 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

Over 12 million attacks a day is being registered across this network of individual honeypots. These attacks are studied, analyzed, categorized, and marked according to a threat rank index, a priority assessment framework that we have developed within Sectrio. The honeypot network includes over 4000 physical and virtual devices covering over 400 device architectures and varied connectivity mediums globally. These 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.