Malware Analysis Report

Malware.unknown.exe

2023_01_10 | Vertica1_ | Version 1.0

Executive Summary

Info

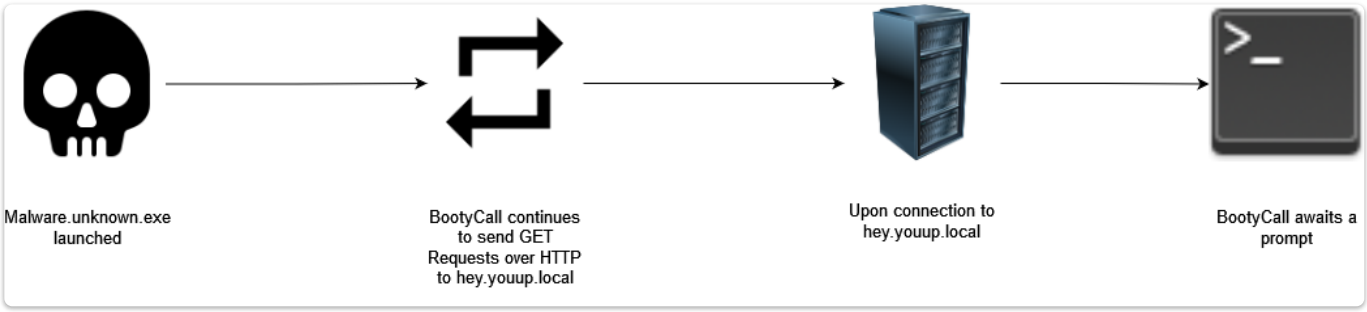
Type	Value
MD5	812a7c7eb9d7a4332b9e166aa09284d7
SHA1	ec0d565afe635c2c7863b2a05df8a49c58b703a3
SHA256	81a10784ae60a58a969e858c9c4a2ae0d4ebe46e9bd6776992461c062f70099d

On 10 January 2023, an unknown program was obtained by the Incident Response team for Big Money Enterprises, Inc. An analysis of the captured sample displayed obfuscated information that attempted to hide several URLs. Launching the program initiates an outgoing beacon that waits to establish a connection.

Due to the name of the URL, hey[.]youup, we are dubbing this program BootyCall.

High-Level Technical Summary

When the unknown malware is launched, it initiates GET request over HTTP to hey[.]youup[.]local. If the program cannot establish a connection to hey[.]youup[.]local, the program will continue to send a request every 3 seconds over a new port on the local host in sequential order.



Analysis

Static

The following methods were performed for basic static analysis:

1. Obtained hash values, Malware Behavior Catalog (MBC) identifiers, ATT&CK Tactics/Techniques from **Capa**.
2. String analysis with **FLOSS**.
3. Search of SHA256 hash value on **VirusTotal**.
4. DLLs and Win API Calls obtained using **PEstudio**.

CAPA

```
+------------------------+-----------------------------------------------------------------------------------------+
| md5                    | 812a7c7eb9d7a4332b9e166aa09284d7                                                        |
| sha1                   | ec0d565afe635c2c7863b2a05df8a49c58b703a3                                                |
| sha256                 | 81a10784ae60a58a969e858c9c4a2ae0d4ebe46e9bd6776992461c062f70099d                       |
| path                   | Malware.unknown.exe.malz                                                                |
+------------------------+-----------------------------------------------------------------------------------------+

+------------------------+-----------------------------------------------------------------------------------------+
| ATT&CK Tactic          | ATT&CK Technique                                                                        |
|------------------------+-----------------------------------------------------------------------------------------|
| DEFENSE EVASION        | Obfuscated Files or Information [T1027]                                                 |
| DISCOVERY              | File and Directory Discovery [T1083]                                                    |
|                        | System Information Discovery [T1082]                                                   |
+------------------------+-----------------------------------------------------------------------------------------+

+----------------------------+-----------------------------------------------------------------------------------+
| MBC Objective              | MBC Behavior                                                                      |
|----------------------------+-----------------------------------------------------------------------------------|
| ANTI-BEHAVIORAL ANALYSIS   | Debugger Detection::Software Breakpoints [B0001.025]                              |
| DATA                       | Check String [C0019]                                                              |
|                            | Encoding::Base64 [C0026.001]                                                      |
|                            | Non-Cryptographic Hash::MurmurHash [C0030.001]                                    |
| DEFENSE EVASION            | Obfuscated Files or Information::Encoding-Standard Algorithm [E1027.m02]          |
| FILE SYSTEM                | Read File [C0051]                                                                 |
|                            | Write File [C0052]                                                                |
| MEMORY                     | Allocate Memory [C0007]                                                           |
| PROCESS                    | Terminate Process [C0018]                                                         |
+----------------------------+-----------------------------------------------------------------------------------+

+-------------------------------------------------------+-------------------------------------------------------+
| CAPABILITY                                            | NAMESPACE                                             |
|-------------------------------------------------------+-------------------------------------------------------|
| check for software breakpoints                        | anti-analysis/anti-debugging/debugger-detection       |
| compiled with Nim                                     | compiler/nim                                          |
| encode data using Base64                              | data-manipulation/encoding/base64                     |
| reference Base64 string                               | data-manipulation/encoding/base64                     |
| hash data using murmur3                               | data-manipulation/hashing/murmur                      |
| contain a thread local storage (.tls) section         | executable/pe/section/tls                             |
| query environment variable                            | host-interaction/environment-variable                 |
| check if file exists                                  | host-interaction/file-system/exists                   |
| read file (2 matches)                                 | host-interaction/file-system/read                     |
| write file (3 matches)                                | host-interaction/file-system/write                    |
| get thread local storage value                        | host-interaction/process                              |
| allocate RWX memory                                   | host-interaction/process/inject                       |
| terminate process                                     | host-interaction/process/terminate                    |
| enumerate PE sections                                 | load-code/pe                                          |
+-------------------------------------------------------+-------------------------------------------------------+
```

FLOSS

Unique Strings

- `000102030405060708091011121314151617181920212223242526272829303132333435363738394041424344454647484950515253545556575859606162636465666768697071727374757677787980818283848586878889909192939495969798 99`
  - (00 -> 99, no spaces)
- `streams.nim`

- `net.nim`
- `BCryptGenRandom`
- `Bcrypt.dll`
- `@hwtwtwpw:w/w/whwewyw.wywowuwuwpw.wlwowcwawlw`
  - String was
  - hXXp[://]hey.youup[.]local
- `@axuxtxhx.xnxsx.xlxoxcxaxlx`
  - auth[.]ns[.]local
- `@.cBoBsBmBoBsBfBuBrBbBoBoBtBsBeBmBpBoBrBiBuBmB.BlBoBcBaBlB`
  - .cosmosfurbootsemporium[.]local
- `@Desktop\cosmo.jpeg`
- `user-agent: Nim httpclient/1.6.2`
- `MessageBoxA`
- `OPENPGPKEY`

Deobfuscated Strings

- `@hwtwtwpw:w/w/whwewyw.wywowuwuwpw.wlwowcwawlw`
  - String was padded with lowercase 'w'. Deobfuscated returns hXXp[://]hey.youup[.]local.
- `@axuxtxhx.xnxsx.xlxoxcxaxlx`
  - String was padded with lowercase 'x'. Deobfuscated returns auth[.]ns[.]local
- `@.cBoBsBmBoBsBfBuBrBbBoBoBtBsBeBmBpBoBrBiBuBmB.BlBoBcBaBlB`
  - String was padded with uppercase 'B'. Deobfuscated returns value .cosmosfurbootsemporium[.]local. Possible partial URL as the presence of the first '.' suggests a subdomain.

VirusTotal

Search result utilizing the SHA256 hash: https://www.virustotal.com/gui/file/81a10784ae60a58a969e858c9c4a2ae0d4ebe46e9bd6776992461c062f70099d

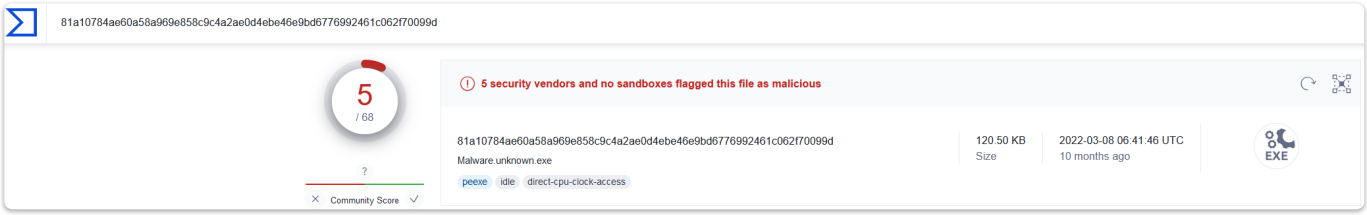


Figure 1 - Screenshot of the search summary using the SHA256 hash

PEstudio

IMPORT ADDRESS TABLE

DLLs

- KERNEL32.dll
- msvcrt.dll
- USER32.dll

Windows API calls

The below list only includes the Windows API Calls that were flagged by PEstudio.

- VirtualProtect
- GetCurrentThreadId
- GetCurrentProcessId
- TerminateProcess
- getenv

Dynamic

When program was run on local machine with no outbound connection capabilities, unknown program made no changes to files or registry.

PERSISTENCE

No persistence mechanisms were observed by the analyst at current time.

C2/BEACONING

Beacon to hXXp[://]hey[.]youup[.]local every 3 seconds.

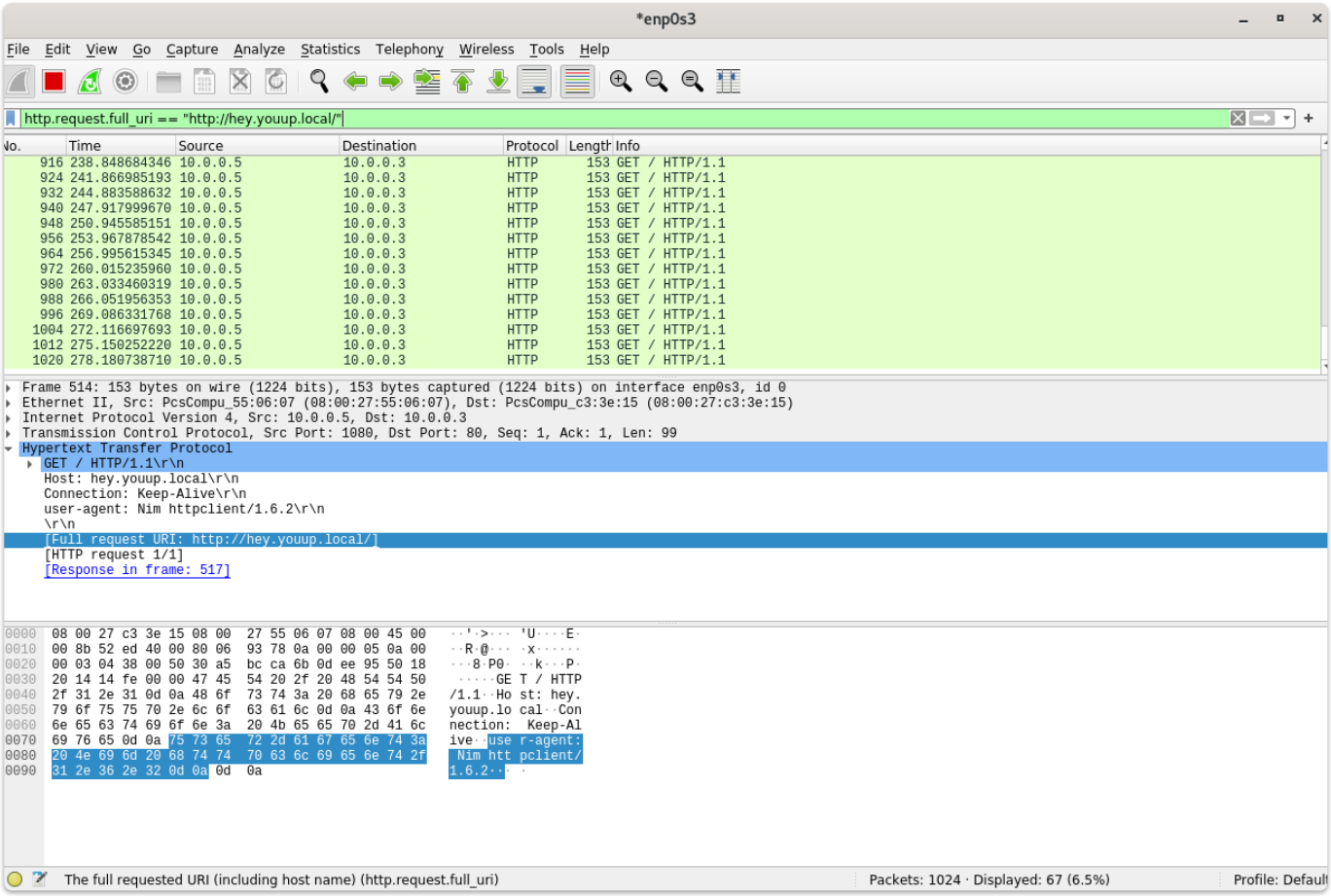


Figure 2 - Wireshark capture showing beaconing

Opens ports and then places them in 'Close Wait' status.

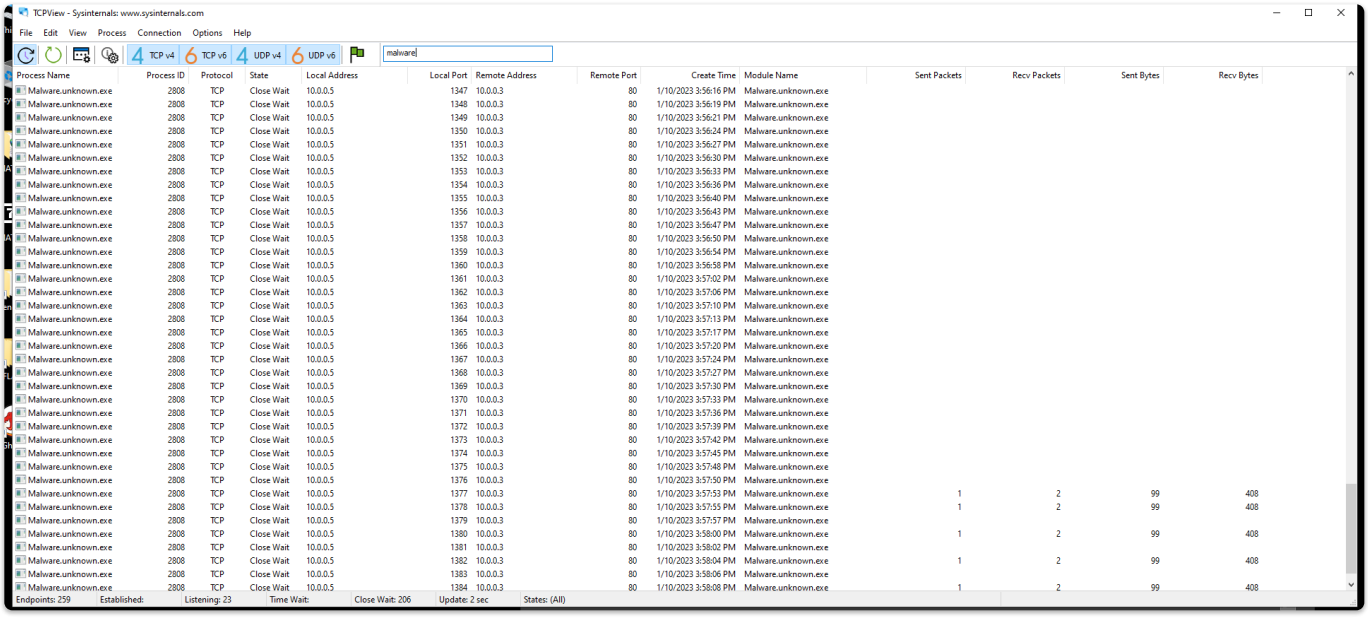


Figure 3 - TCPView showing TCP connections being opened then changed to "Close Wait" status

Program continues to beacon out to hey[.]youup[.]local (see Figure 2) until it is able to establish a connection. This was accomplished by setting up a DNS entry for the loopback address on the

analyst machine.

Figure 4 - Netcat listener using loopback address, receiving connection from program after launch

Attempting issue commands such as `whoami` and other random phrases drops the connection and the program exits.

Appendix

Indicators of Compromise

NETWORK INDICATORS

- hey[.]youup[.]local

HOST INDICATORS

- None at this time

Rule(s)

YARA

rule Training_PMAT_BootyCall : BootyCall
{
meta:

```
author = "V"
description = "Detection for the late night caller "
date = "2023-01-10"
version = "1.0"
hash = "812a7c7eb9d7a4332b9e166aa09284d7"

strings:
$c2_url = { 68 ?? 74 ?? 74 ?? 70 ?? 3a ?? 2f ?? 2f ?? 68 ?? 65 ?? 79 ?? 2e ?? 79 ?? 6f ?? 75 ?? 75 ?? 70 ?? 2e ?? 6c ?? 6f ?? 63 ?? 61 ?? 6c }

condition:
uint16(0) == 0x5A4D and
$c2_url
}
```

SURICATA

```
alert http $HOME_NET any -> $EXTERNAL_NET 80 (msg:"Beacon for BootyCall"; flow:to_server; http.header; content:"hey.youup.local"; http.user-agent; content:"Nim httpclient")
```

MITRE ATT&CK

T1027 - Obfuscated Files or Information
T1027.001 - Binary Padding
T1082 - System Information Discovery
T1083 - File and Directory Discovery