RAT.Unknown.exe Analysis

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Important Strings:** (Static) |Seems like there is a connection via http to a domain|

@HTTP/

@connect

@head

@iterators.nim(189, 11) `len(a) == L` the length of the seq changed while iterating over it

@Proxy-Authorization: basic

@Content-Length:

@Content-Length

@PATCH

@PUT

@POST

@Connection: Keep-Alive

@Connection

@Host:

@ HTTP/1.1

@User-Agent

@user-agent

@tables.nim(1103, 13) `len(t) ==

L` the length of the table changed while iterating over it

@SSL support is not available. Cannot connect over SSL. Compile with -d:ssl to enable.

@https

@No uri scheme supplied.

InternetOpenW

InternetOpenUrlW

@wininet

@wininet

MultiByteToWideChar

@kernel32

@kernel32

MessageBoxW

@user32

@user32

@[+] what command can I run for you

@[+] online

@NO SOUP FOR YOU

@\mscordll.exe

@Nim httpclient/1.0.6

@/msdcorelib.exe

@AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

@intrt explr

@http://serv1.ec2-102-95-13-2-ubuntu.local

Startup directory = common file path for malware to abuse (all file paths we find should be investigated) used to start programs on login

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Dynamic Analysis**

Graphical user interface, application

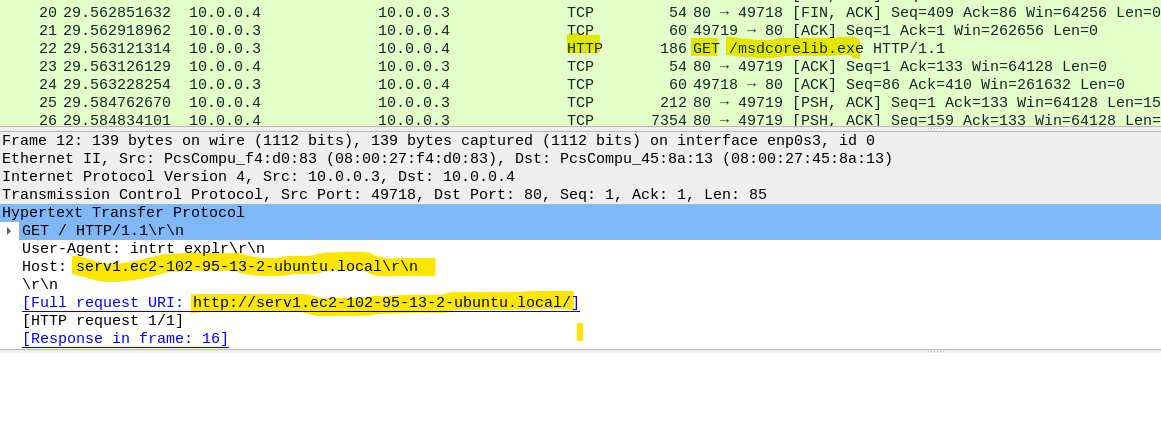
Description automatically generated

Error Message shown upon detonation

-----------------------------------------------------------------------------------------------------------------------------------

Network Based Indicators:

2 interesting Strings that we found in our static analysis turned up again in our Wireshark analysis. As these are http requests we can confirm the strings are in fact URLS



 -> a GET request signifies a POTENTIAL file download could this be located in startup directory?

------------------------------------------------------------------------------------------------------------------------------------------

**Host Based Indicators**:

Through using tcpview we found an open TCP socket in listening state



Upon connection to this socket we get the following base64 encoded string

Text

Description automatically generated

Upon further inspection we can see we have a reverse shell in which all responses are encoded

Text

Description automatically generated

Text

Description automatically generated

This confirms the malware has command injection capability and is a remote access trojan