Malware Incident Response Lab

Nem Negash

CMSC 426

UMBC

Table of Contents

[**Summary** 1](#_Toc12715141)

[**Malware Summary** 2](#_Toc12715142)

[**Indicators of Compromise (IOC)** 2](#_Toc12715143)

[**Technical Details / Activity Observed** 3](#_Toc12715144)

[**C2 Infrastructure**](#_Toc12715145) 4

[**Mitigation Actions**](#_Toc12715146) 5

[**Intelligence Connections** 5](#_Toc12715147)

[**Conclusion** 5](#_Toc12715148)

[**Contact Information**](#_Toc12715149) 6

Malware

# **Summary**

On November 24, 2021 there was some suspicious activity detected while monitoring the SIEM. The malicious activity was found to be coming from within the network from an unauthorized flash drive being inserted into a device that was connected to the network. It was found to be using an obscure port by using the Snort rule called “MyAgent”. The malware was packaged into a PDF file and when opened it downloads an executable file named ABEM Browser.exe behind the scenes. This malware tried to connect back to the command and control server, www.programworkshop.com , through a hardcoded user agent string/URI.

# **Malware Summary**

*Malware Details*

Filename: ABEM Browser.exe

*Malware Behavior*

The malware connects back to the command and control server through a hard-coded user agent string/URI (typical malware behavior), which explains why we are seeing suspicious traffic originating from INSIDE our network. Using [www.hybrid-analyis.com](http://www.hybrid-analyis.com), which is a public sandbox website, we can see that the malware is probably a trojan and shows that the executable contacts two domains and three hosts. It follows by attempting to do a POST HTTP request by sending files to the web server, which confirms the details highlighted in the Wireshark traffic.

# **Indicators of Compromise (IOC)**

Malicious traffic is coming from the source IP of 209.22.xxx.xx, which happens to be a computer on your network. It also is communicating with an obscure TCP port 43688. The browser attempted to make a connection using an agent identifier of “WINCSECB.”

# **Technical Details / Activity Observed**

File: ABEM Browser.exe

Size: 1.7MiB (1774168 bytes)

MD5: 5acb3d73eec11a22424887db57596e5a

SHA1: ed48c56af083dcc09aafaefc207bfdf49c022103

File Type: peexe executable

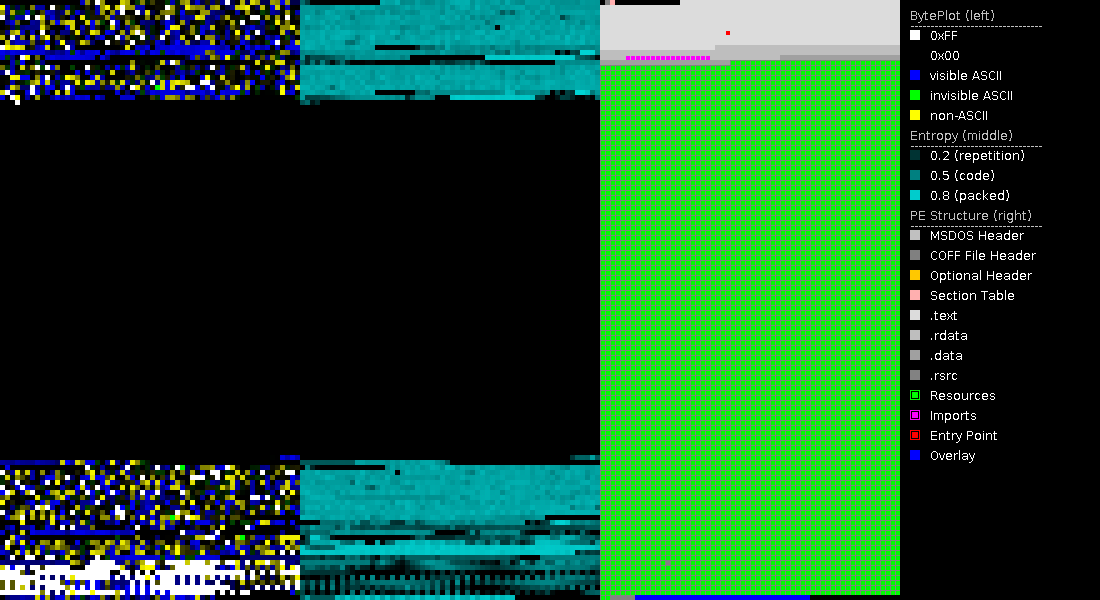


Figure 1 – Embedded Linking Object

Graphical user interface, text, application

Description automatically generated

Figure 2: Extracted string found in the malware

This malware, when executed, attempts to run the following services:

**ADVAPI32.dll**

* Advapi32 is an API that allows Windows-based applications to access to advanced functionality.

**iphlpapi.dll**

* Windows IP Helper DLL.

**KERNEL32.dll**

* includes, VirtualAlloc, VirtualFree, Sleep, IsDebuggerPresent, GetTickCount, CreateFileA, and DeleteFileA. These can all be questionable functions when seen in a potentially malicious program.

**ole32.dll**

* Library containing core OLE functions.

**OLEAUT32.dll**

* Allows applications to handle files and information created by other applications.

**SHELL32.dll**

* Library containing Windows Shell API functions.

**urlmon.dll**

* Helper for ole32.dll

**USER32.dll**

* Library containing functions related to the Windows user interface.

**VERSION.dll**

* Module containing functions for Windows version checking.

**WININET.dll**

* Module containing internet-related functions.

Though these seem to be standard Windows services, they appear to fall in line with the TTPs of the ABEM Browser malware, performing network requests like POSTs to malicious sites from within the target’s network.

# **C2 Infrastructure**

The following is a list of all C2 domains identified during investigation of these malware samples.

Domains:

programworkshop.com

abemsecure.starttest.com

# **Mitigation Actions**

Global Cyber Fusion suggests the following:

1. If possible, deploy a tiered pattern matching detection for any executable accessing the following and only the following DLLs: ADVAPI32.dll,iphlpapi.dll, KERNEL32.dll, ole32.dll, OLEAUT32.dll, SHELL32.dll, urlmon.dll, USER32.dll, VERSION.dll, WININET.dll
2. Block any traffic from going between the www.programworkshop.com and the company network

# **Intelligence Connections**

No intelligence connections have been found thus far.

# **Conclusion**

The team concludes that the company network has been compromised and the company has taken the actions mentioned above to mitigate any further issues. Any Cyber Security Service Providers (CSSP) that identify similar breaches are encouraged to contact the team. Additional information will be distributed about the situation as it is identified. CSSPs are also encouraged to explore attacker infrastructure in an authorized and secure manner. Additional IOCs obtained from such investigative acts can be of great value to the Cyber Defense Community in preventing future compromise attempts.

# **Contact Information**

**UMBC E-mail:** xk28378@umbc.edu

**Written by:** Nem Negash