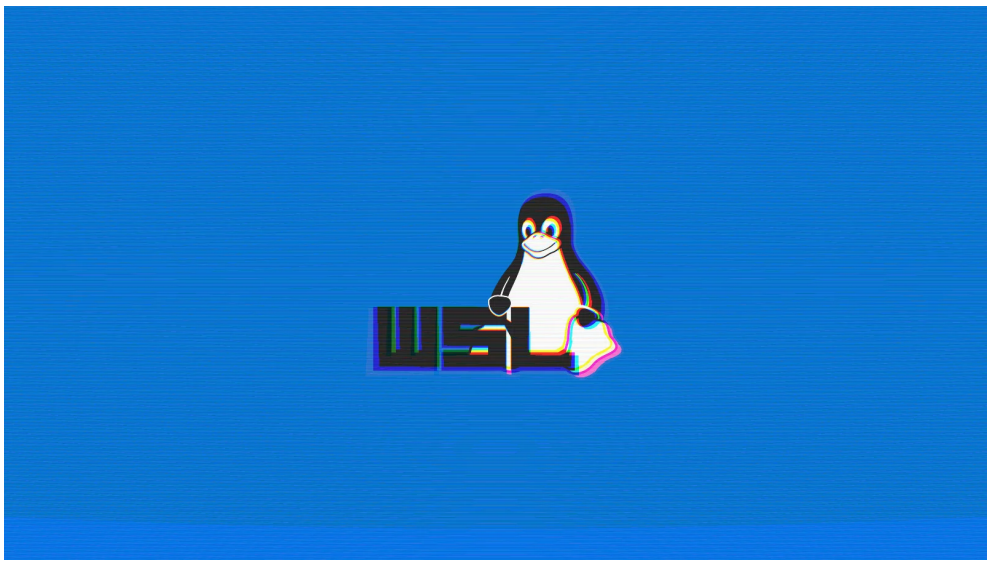
New malware uses Windows Subsystem for Linux for stealthy attacks

By **Ionut Ilascu (https://www.bleepingcomputer.com/author/ionut-ilascu/)** September 16, 2021 01:33 PM 0



Security researchers have discovered malicious Linux binaries created for the Windows Subsystem for Linux (WSL), indicating that hackers are trying out new methods to compromise Windows machines.

The finding underlines that threat actors are exploring new methods of attack and are focusing their attention on WSL to evade detection.

Using WSL to avoid detection

The first samples targeting the WSL environment were discovered in early May and continued to appear every two to three weeks until August 22. They act as loaders for the WSL environment and enjoy very low detection on public file scanning services.

In a report today, security researchers at Lumen's Black Lotus Labs say that the malicious files either have the payload embedded or fetch it from a remote server.

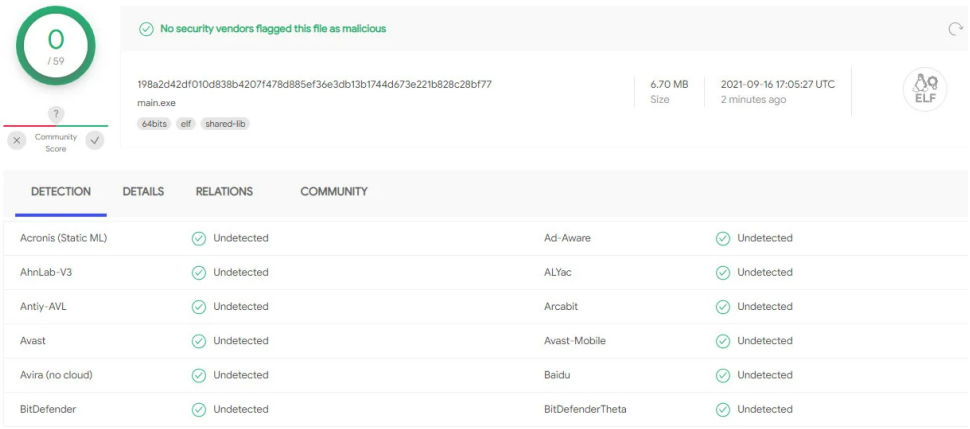
The next step is to inject the malware into a running process using Windows API calls, a technique that is neither new nor sophisticated.

From the small number of samples identified, only one came with a publicly routable IP address, hinting that threat actors are testing the use of WSL to install malware on Windows.

The malicious files rely mainly on Python 3 for carrying out their tasks and are packaged as an ELF executable for Debian using PyInstaller.

> "As the negligible detection rate on VirusTotal suggests, most endpoint agents designed for Windows systems don't have signatures built to analyze ELF files, though they frequently detect non-WSL agents with similar functionality" - Black Lotus Labs (https://blog.lumen.com/no-longer-just-theory-black-lotus-labs-uncovers-linux-executables-deployed-as-stealth-windows-loaders/)

Less than a month ago, one of the malicious Linux files was detected by just one antivirus engine on VirusTotal. Refreshing the scan on another sample showed that it went completely undetected by the engines on the scanning service



Python and PowerShell

One of the variants, written completely in Python 3, does not use any Windows API and seems to be the first attempt at a loader for WSL. It uses standard Python libraries, which makes it compatible with both Windows and Linux.

The researcher found in a test sample code that prints “Hello Sanya” in Russian. All but one file associated with this sample contained local IP addresses, while the public IP pointed to 185.63.90[.]137, already offline when the researchers tried to grab the payload.

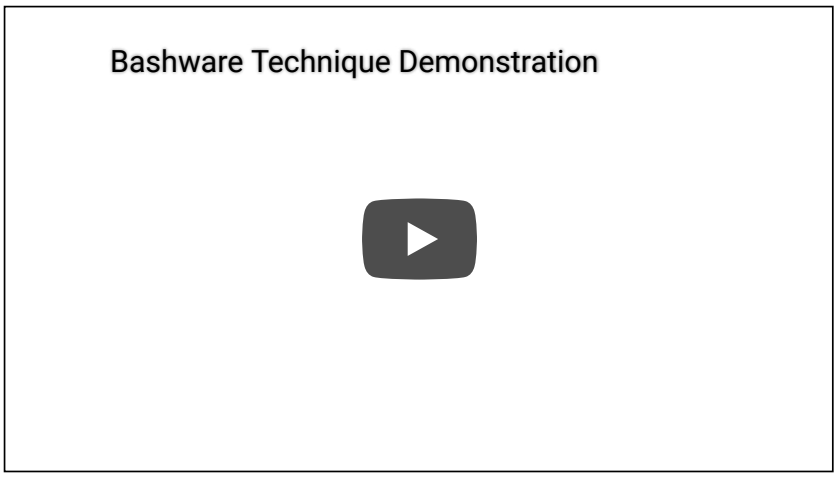
Another “ELF to Windows” loader variant relied on PowerShell to inject and execute the shellcode. One of these samples used Python to call functions that killed the running antivirus solution, established persistence on the system, and run a PowerShell script every 20 seconds.

Based on inconsistencies observed when analyzing several samples, the researchers believe that the code is still being developed, although in the final stage.

The limited visibility from the public IP address indicates activity restricted to targets in Ecuador and France between late June and early July.

Black Lotus Labs assesses that the WSL malware loaders are the work of a threat actor testing the method from a VPN or proxy node.

Microsoft introduced Windows Subsystem for Linux in April 2016. In September 2017, when WSL was freshly out of beta, researchers at Check Point demonstrated an attack they called Bashware (https://research.checkpoint.com/2017/beware-bashware-new-method-malware-bypass-security-solutions/) where WSL could be abused to hide malicious code from security products.



The report from Lumen's Black Lotus Labs provides indicators of compromise associated with the detected campaign to help defenders create detection rules. For file hashes and data on this actor's wider activity, the researchers point to the company's GitHub page (https://github.com/blacklotuslabs/IOCs/blob/main/WSL%20samples.txt).

Related Articles:

EasyWSL turns Linux docker images into a Windows 10 WSL distro (https://www.bleepingcomputer.com/news/microsoft/easywsl-turns-linux-docker-images-into-a-windows-10-wsl-distro/)

New Windows security updates break network printing (https://www.bleepingcomputer.com/news/security/new-windows-security-updates-break-network-printing/)

Windows 10 now lets you install WSL with a single command (https://www.bleepingcomputer.com/news/microsoft/windows-10-now-lets-you-install-wsl-with-a-single-command/)

Microsoft: Windows MSHTML bug now exploited by ransomware gangs (https://www.bleepingcomputer.com/news/microsoft/microsoft-windows-mshtml-bug-now-exploited-by-ransomware-gangs/)

Microsoft rolls out Office LTSC 2021 for Windows and Mac (https://www.bleepingcomputer.com/news/microsoft/microsoft-rolls-out-office-ltsc-2021-for-windows-and-mac/)