Luci Spools the Fun with Phobos Ransomware

paraflare.com/luci-spools-the-fun-with-phobos-ransomware/

Bex Nitert

Published by Bex Nitert | 3 March 2022

Bex Nitert
Director, Digital Forensics & Incident Response
March 3, 2022
5 min read.

The Digital Forensics and Incident Response (DFIR) team at ParaFlare recently helped an Australian manufacturer impacted by Phobos ransomware. Unexpectedly, our investigation found the ransomware affiliate had exploited the PrintNightmare vulnerability to escalate privileges within two minutes of gaining initial access.

To our knowledge, there are no documented examples of the PrintNightmare vulnerability being exploited by Phobos ransomware affiliates. So we decided to share our observations and indicators from the investigation. . We are using the name “Luci” for this Phobos ransomware affiliate due to the frequency of the terms “Luci” and “Lucifer” appearing in filenames, code, registry values, and the name of the Local Administrator account created by Luci.

In this article, we provide a brief introduction to the Phobos ransomware variant followed by technical details related to the use of a PrintNightmare exploit by Luci in the initial stages of the attack. Additional tools and techniques identified during the investigation will be discussed in a separate article.

Phobos Ransomware Background

Phobos ransomware is a form of malicious software used by threat actors to encrypt files on systems. The purpose is to extort a ransom fee from victims in exchange for restoring access to their data. Phobos affiliates are financially motivated and opportunistic. Most victims are small to medium sized businesses, though individuals have been impacted too.

The Phobos ransomware variant, closely related to Dharma and Crysis ransomware, first emerged in 2018 and is used by criminals with varying technical abilities. Actors that use Phobos ransomware are commonly known as “Phobos affiliates”. Distributors of Phobos provide a Ransomware as a Service (RaaS) style model to customers, enabling affiliates to undertake attacks without the need to develop their own file encrypting malware.

Unlike many of the ransomware variants in the news (REvil, LockBit, Conti, etc.) Phobos ransomware operators are not currently known to conduct data exfiltration for use in double extortion style attacks (where a ransom fee is also demanded from victims to prevent the publication of stolen data).

Phobos affiliates operate with greater autonomy, generally demand lower ransom amounts, and demonstrate less professionalism, compared to more well-known ransomware variants. While not as high profile, Phobos was one of the most reported variants of ransomware in the first half of 2021, according to a report released by the Financial Crimes Enforcement Network (FinCEN) of the United States Treasure Department1. FinCEN's observations were consistent with 2021 ransomware statistics published by Emisoft which found Phobos was the third most commonly reported ransomware strain of 2021.

The diversity of actors involved in deploying Phobos ransomware and their lack of organisation means that variations in attack behaviour are more likely to be observed. In our recent Phobos ransomware investigation, the affiliate we called Luci demonstrated more individuality than most.

Initial Access Leveraging External Remote Services and Valid Accounts

ParaFlare's observations of the attack patterns used by ransomware operators who obtain initial entry into an environment via remote access solutions have remained relatively consistent over the years. In almost all circumstances, our investigations found initial access was obtained using a local or domain administrator account. Consequently, most actors commenced their attack with privileged access and not much additional effort was required for them to achieve their objectives.

Typically, remote access credentials are compromised either through phishing, credential stuffing, brute forcing, or the exploitation of vulnerabilities in VPN appliances. The credentials may be obtained or guessed directly by the ransomware operator or purchased from an initial access broker. Insecure remote desktop protocol (RDP) connections are one of the most common initial access vectors used in Phobos ransomware attacks.

In our recent investigation, we found Luci gained remote access to a terminal server using a domain user account, $Printer_Maestro$, associated with a software package called BarTender that was used in the client environment. While the account had limited privileges, it had remote access rights, which was sufficient for Luci to gain initial access. It is unknown how Luci obtained valid credentials.

Exploitation of Windows Print Spooler Vulnerability for Privilege Escalation

In circumstances where threat actors obtain remote access with a non-administrator account, they need to find a way to escalate privileges to move laterally within the environment and deploy ransomware. Known vulnerabilities are often exploited for this purpose, however, this was the first time we had witnessed a PrintNightmare exploit used for privilege escalation in a ransomware attack. At the time of publication, ParaFlare had not identified any documented cases of PrintNightmare being exploited by Phobos ransomware affiliates.

PrintNightmare is a vulnerability in the Windows Print Spooler service (spoolsv.exe) assigned the identifier CVE-2021-34527. It is similar to other vulnerabilities including CVE-2021-1675.

Forty-five seconds after the first identified remote desktop session logon succeeded, Luci copied a password protected, self-extracting archive (SFX) file called Lucimare.exe to the desktop on the terminal server.

Although we were unable to successfully recover this SFX file, we can infer that it contained malicious files designed to exploit the PrintNightmare vulnerability based on existing logs, the SYSTEM registry, and artefacts recovered through file carving.

Our analysis found the Lucimare.exe SFX file contained a few files with modified times between 4 July 2021 and 7 July 2021. Available file hashes can be found in the indicators of compromise list at the end of the article.

Filename	Compile Time	Modified Time	Size

Lucimare.ps1	N/A	2021-07-04 03:46:48	165KB
Lucimare.dll	N/A	2021-07-07 05:04:04	91.5KB
LucimarePoc2008.exe	2021-07-07 05:02:10	2021-07-07 05:04:05	98.5KB
LucimarePoc.exe	2021-07-07 05:30:55	2021-07-07 05:35:03	98.5KB

Lucimare.exe was executed within 18 seconds from its first appearance on disk, resulting in the extraction of files to the desktop folder.

Based on data contained in the AmCache.hve (which was recovered through file carving), it appears LucimarePoc.exe was executed seven seconds later. Around the same time, three files were written to the Print Spooler's driver directory. Unfortunately, we were not able to recover these files.

- C:\Windows\System32\spool\drivers\x64\3\kernelbase.dll
- C:\Windows\System32\spool\drivers\x64\3\AddUserX64.dll
- C:\Windows\System32\spool\drivers\x64\3\mxdwdrv.dll

Remnant data suggests these files also existed in the directory C:\Windows\System32\spool\drivers\x64\3\new

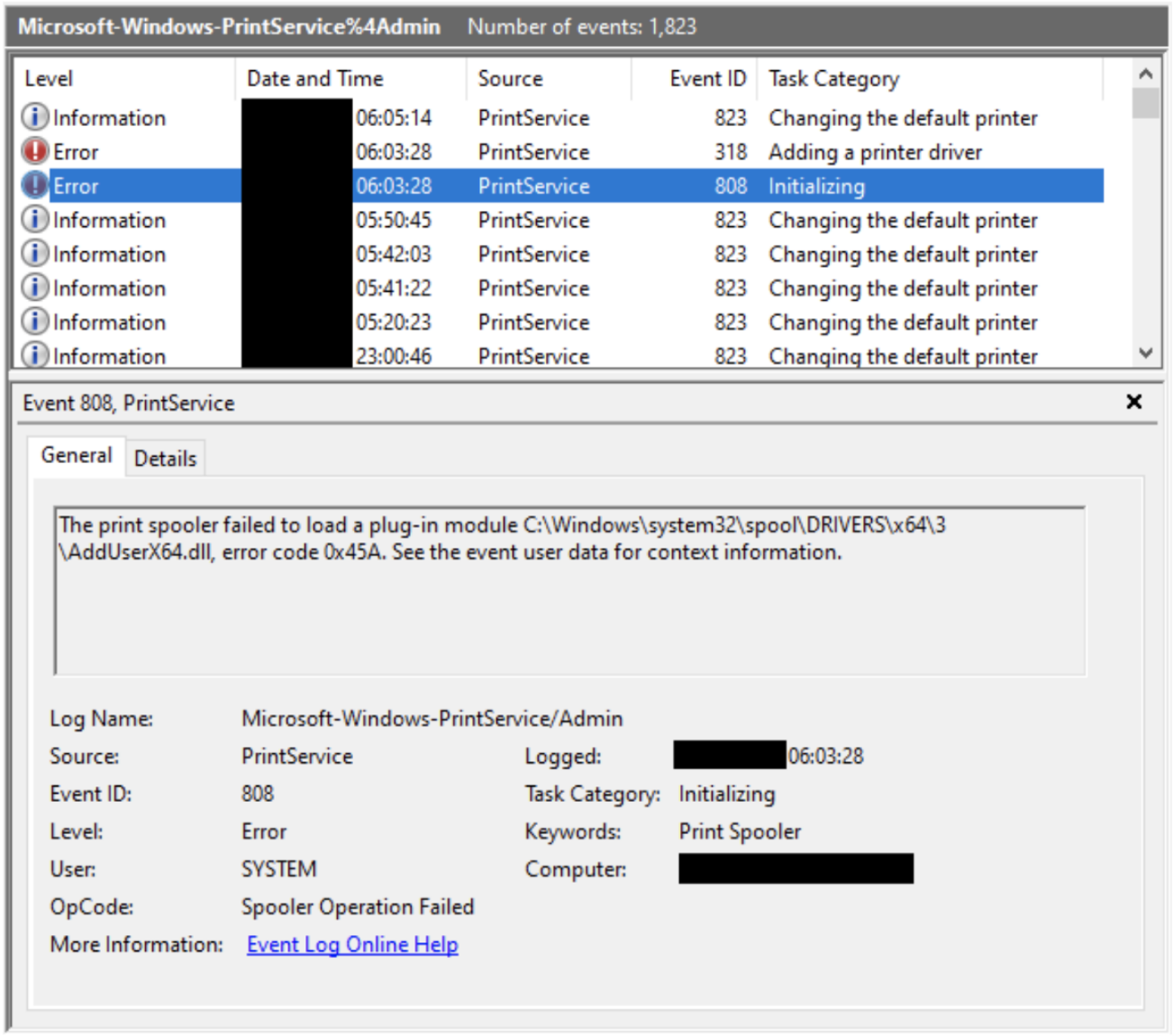
A suspicious spoolsv registry value was also set at this time with the name "LuciMarePoc"

> HKLM\SYSTEM\CurrentControlSet\Control\Print\Environments\Windows x64\Drivers\Version-3\LuciMarePoc

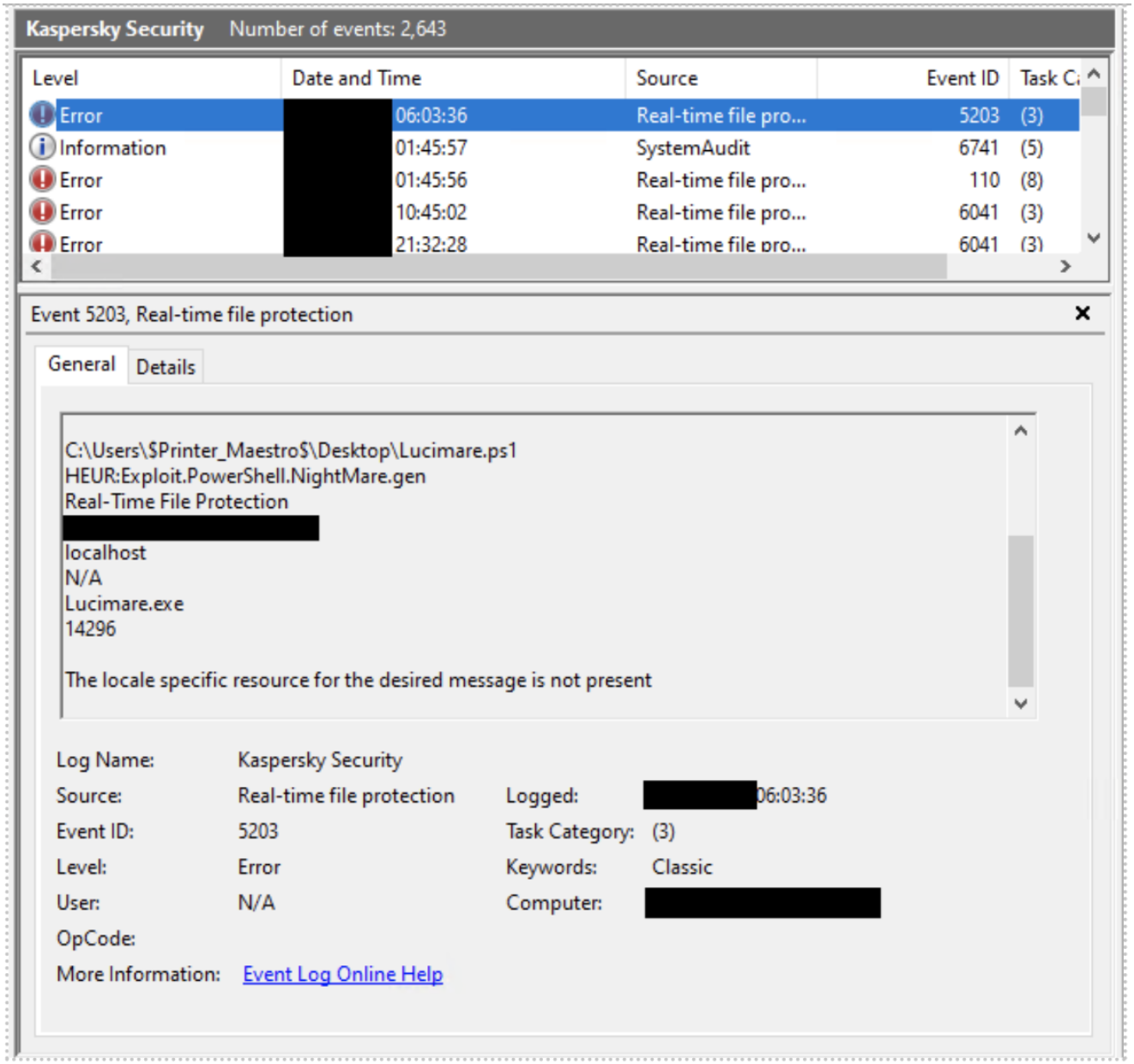
This contained references to the new drivers kernelbase.dll (Data File), AddUserX64.dll (Configuration File), and mxdwdrv.dll (Driver).

Name	Type	Value
(Default)	REG_SZ	(value not set)
Dependent Files	REG_MULTI_SZ	
Configuration File	REG_SZ	AddUserX64.dll
Data File	REG_SZ	kernelbase.dll
Driver	REG_SZ	mxdwdrv.dll
Help File	REG_SZ	
Monitor	REG_SZ	
Datatype	REG_SZ	
Previous Names	REG_MULTI_SZ	

An error with the Event ID 808 was recorded in the Microsoft-Windows-PrintService/Admin log specifying that “The print spooler failed to load a plug-in module C:\Windows\system32\spool\DRIVERS\x64\3\AddUserX64.dll”. Additional logs (e.g. Microsoft-Windows-PrintServer/Operational) that would record the successful printer plugin loading were not enabled on the server.



Seconds later LucimarePoc2008.exe executed, followed closely by the creation of a Windows Event log for Kaspersky Security, which had detected the file Lucimare.ps1 as “HEUR:Exploit.PowerShell.NightMare.gen”.



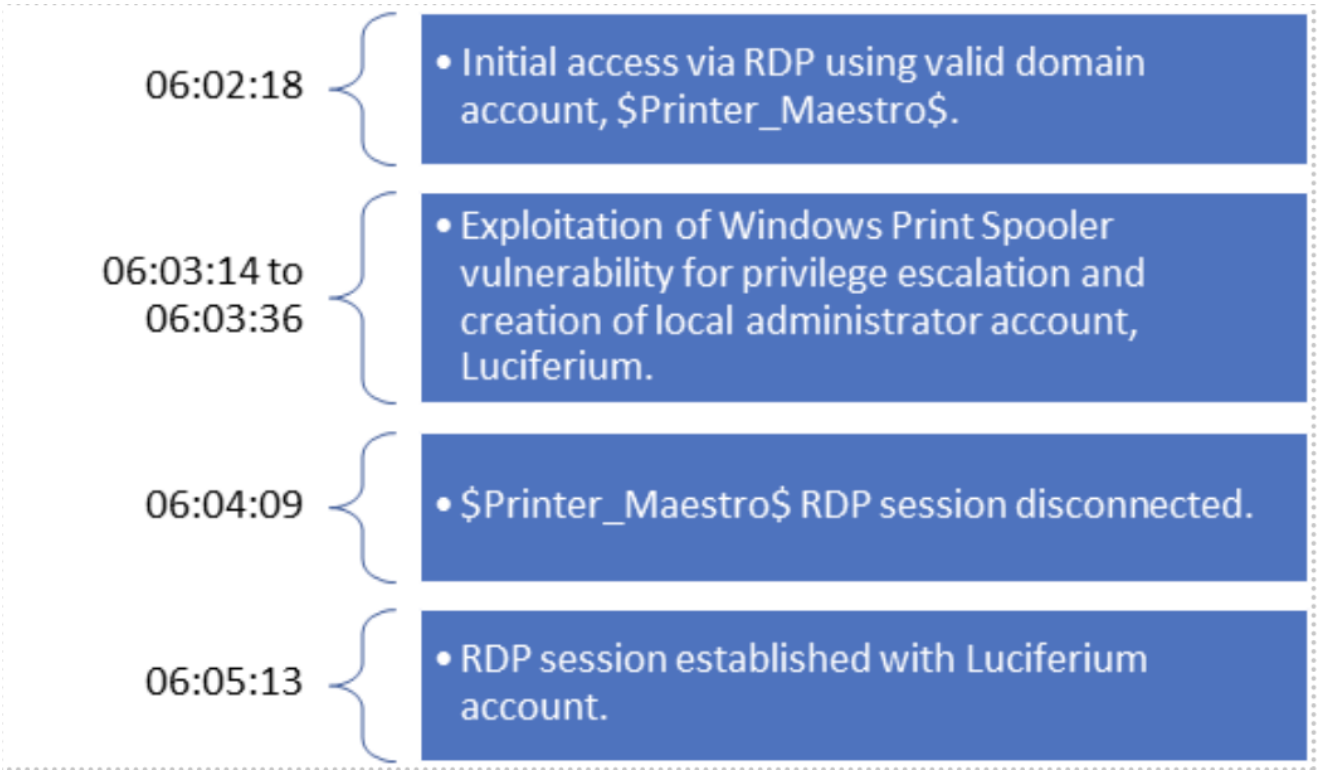
During this time, a local administrator account called “Luciferium” was created on the server. A RDP connection was established using this account less than three minutes after the initial intrusion.

The remaining phases of the attack including credential access, lateral movement, and the encryption of data will be covered in an upcoming post.

Recommendations

- Ensure operating systems and applications are patched.
- Secure remote access and enable multi-factor authentication for remote and administrator accounts at a minimum.
- Implement principle of least privilege and principle of least functionality across accounts and servers.
- Ensure there is sufficient, centralised logging.

Timeline: Initial Access to Privilege Escalation



Indicators of Compromise

Files

Phobos Ransomware (.eight extension)
Filename: Fast.exe
MD5: 6eff55b9f24c8b276848167c5d64cc9c
SHA-1: 66cfc67c4a95129a0e979c1ce025747372d69552
SHA-256: 31dba1a23db70ffb952f0e597acf95d16ab60423018a83d0ccb4f57ce0471793

Exploit Toolkit
Filename: Lucimare.exe
SHA-1: 9595bff740d66f8037f7f0346677a70dfef941c4

Filename: Lucimare.ps

Filename: Lucimare.dll

Filename: LucimarePoc2008.exe
SHA-1: c69051c612214ad8f9b57ce99ce60f1d15db453

Filename: LucimarePoc.exe
MD5: e4a6b0afc0895a844644ebcc00db7d73
SHA-1: 3482fbb6ab9c43cf7a660528d62c1283e4a058ca
SHA-256: f0d6846da6d45180a695201888edc4f9c512fb0d11ed56394aae9daa874ba88c

Printer Drivers Associated with Exploit
Filename: kernelbase.dll
File Path: C:\Windows\System32\spool\drivers\x64\3\
File Path: C:\Windows\System32\spool\drivers\x64\3\new

Filename: AddUserX64.dll
File Path: C:\Windows\System32\spool\drivers\x64\3\
File Path: C:\Windows\System32\spool\drivers\x64\3\new

Filename: mxdwdrv.dll
File Path: C:\Windows\System32\spool\drivers\x64\3\
File Path: C:\Windows\System32\spool\drivers\x64\3\new

Registry

Registry Keys Created During Exploit
HKLM\SYSTEM\CurrentControlSet\Control\Print\Environments\Windows x64\Drivers\Version-3\LuciMarePoc

Network

Malicious RDP Connections
IPv4: 185.112.82[.]235
IPv4: 185.112.82[.]236
IPv4: 185.112.82[.]237

Have a comment? Join the conversation on LinkedIn

- Blog
- Technical research