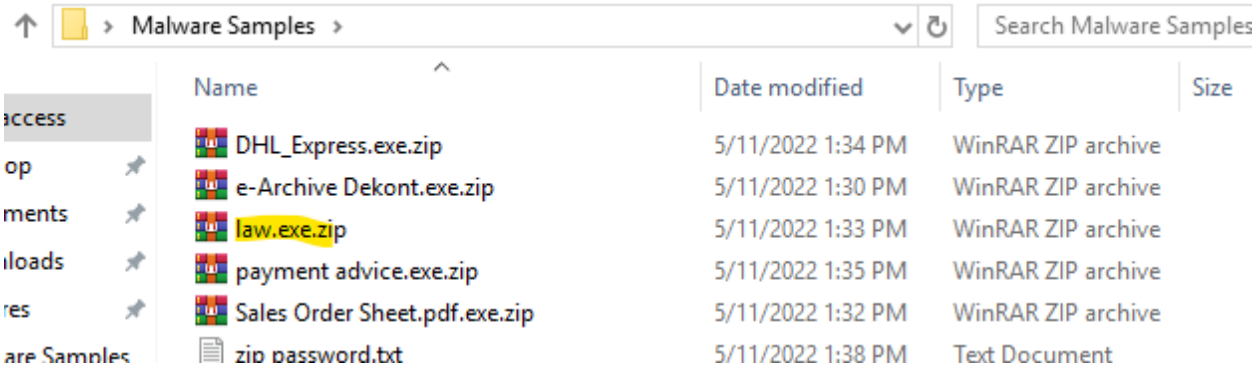
Malware Analysis (Playbook)

By: Ryan Stewart

Preparing



Before executing the suspicious program, “law.exe.zip,”it is crucial to prepare our monitoring tools. These tools log all activities that occur from the moment the malware is run. If not executed beforehand, we might miss detecting malicious activities, even though they are carried out by the malware.

To visualize the process activities, we will utilize 'Process Hacker. Keep in mind that, as we run the malware by clicking on the desktop, the associated process may appear under the **'explorer.exe' process.** Hence, it's essential to pay special attention to this process during our analysis.

Pre-analysis Prep

explorer.exe	4500	0.14	228 B/s	27.04 MB	EC2AMAZ...\LetsDefend	Windows Explorer
tvnserver.exe	3700	0.02	214 B/s	1.71 MB	EC2AMAZ...\LetsDefend	TightVNC Server
ProcessHacker.exe	6692	0.20		11.41 MB	EC2AMAZ...\LetsDefend	Process Hacker
Procmon64.exe	4616			4.7 MB	EC2AMAZ...\LetsDefend	Process Monitor
Fiddler.exe	2796	0.02		71.46 MB	EC2AMAZ...\LetsDefend	Fiddler

-Process Hacker

Before running the suspicious program, "law.exe.zip," it is crucial to set up monitoring tools to capture various activities. The following tools will be employed:

- **Procmon:** To monitor process, file, registry, and network activities.
- **RegShot:** To record registry activities.
- **Wireshark/Fiddler:** For analyzing network activities. (HTTP, DNS, SMTP)

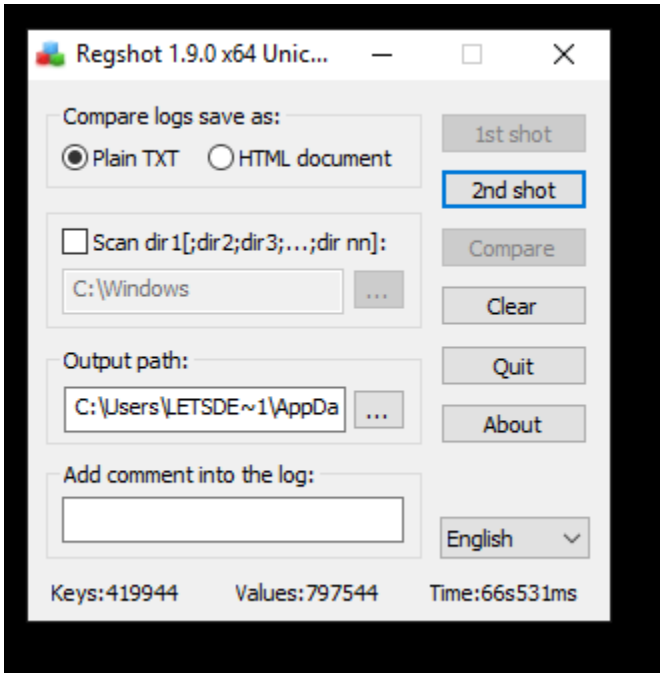
Analysis Steps

1. Procmon Analysis:

- Execute 'Procmon' to capture process, file, registry, and network activities.
- Generate the first shot with 'RegShot' to record registry activities before running the malware.

1. **Unusual Process Names:**
   - Normal: `explorer.exe`, `svchost.exe`
   - Suspicious: `random123.exe`, `malicious_process.exe`
2. **Unexpected Process Spawning:**
   - Normal: `svchost.exe` spawns `services.exe`
   - Suspicious: `explorer.exe` spawns an unknown process with a random name
3. **Unusual File Access:**
   - Normal: `C:\Program Files\Application\file.txt`
   - Suspicious: `C:\Windows\System32\random_file.exe`
4. **Registry Modifications:**
   - Normal: `HKLM\Software\Microsoft\Windows\CurrentVersion\Run`
   - Suspicious: `HKCU\Software\RandomMalware\Key`
5. **Network Connections:**
   - Normal: `192.168.1.1:80`, `www.google.com:443`
   - Suspicious: `123.456.789.0:666` (unusual port or known malicious IP)
6. **Excessive CPU or Disk Usage:**

    - Normal: Routine system processes with consistent resource usage
    - Suspicious: `malicious_process.exe` **consuming 99% CPU suddenly**
7. **Command-Line Arguments:**
    - Normal: `cmd.exe /c ping google.com`
    - Suspicious: `malicious_process.exe -execute -payload`
8. **Creation of Auto-Start Mechanisms:**
    - Normal: `HKLM\Software\Microsoft\Windows\CurrentVersion\Run`
    - Suspicious: `Scheduled Task created by unknown process`
9. **Injection Techniques:**
    - Normal: No signs of injected code
    - Suspicious: `explorer.exe` injecting code into another process
10. **API Hooking:**
    - Normal: No manipulation of system APIs
    - Suspicious: `malicious_process.exe` modifying system APIs
11. **Unexpected DLL Loading:**
    - Normal: Loading signed DLLs from system directories
    - Suspicious: Loading unsigned DLLs from an obscure location
12. **Pattern of Evasive Actions:**
    - Normal: No attempts to terminate security processes
    - Suspicious: `malicious_process.exe` terminating antivirus processes



(1st Shot)

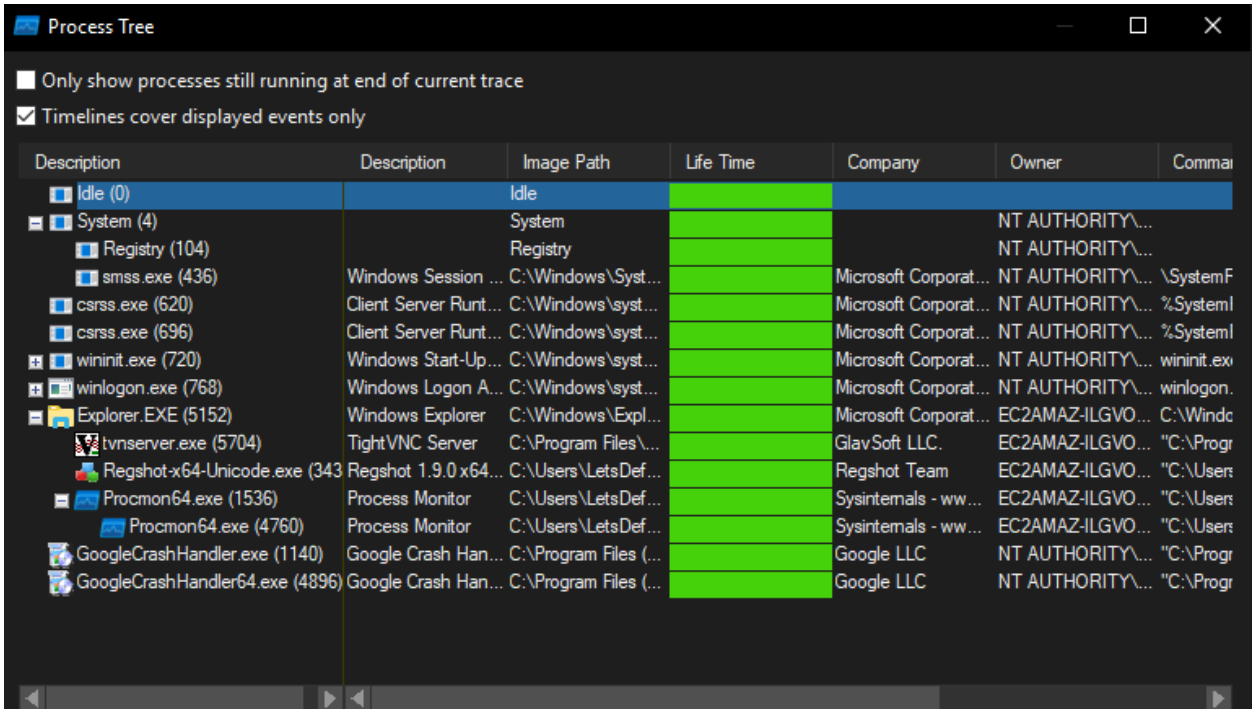
These examples highlight the kind of anomalies or patterns that you might detect when analyzing Procmon logs. **Remember**, context is crucial, and these indicators may vary based on the specifics of your system and the behavior of legitimate applications. Always investigate deviations from the norm and cross-reference findings with threat intelligence sources.

2. Executing the Malware:

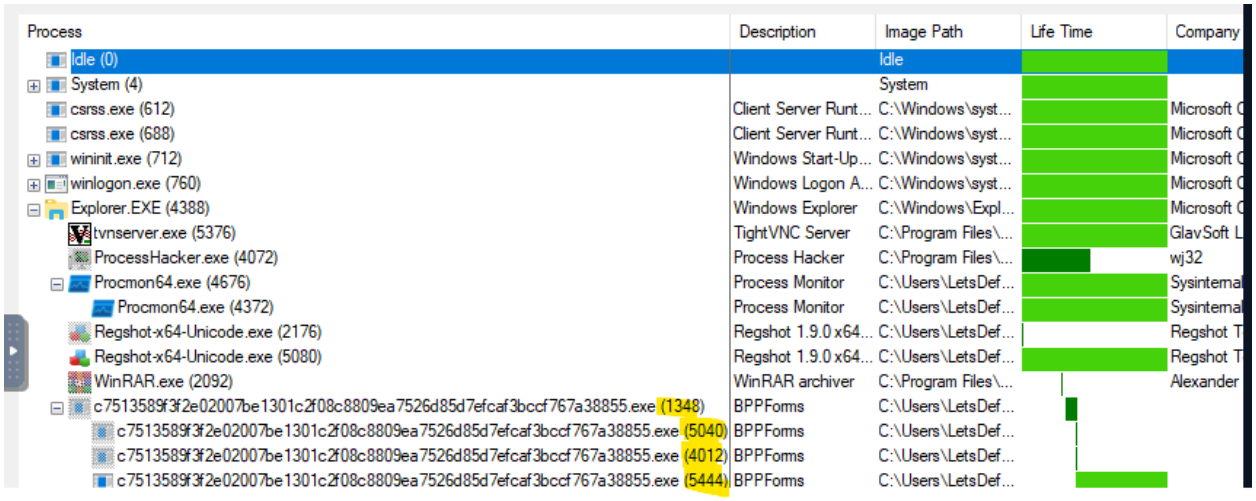
- Run 'law.exe.zip,' on the virtual machine (VM) and **allow sufficient time** (5-10 mins) for the malware to perform its activities. (Run as administrator)
- Take the second shot with 'RegShot' to record changes in registry activities.

3. Process Activities:

- Analyze process activities using 'Process Hacker' and 'Procmon.'
- Identify and examine the processes associated with the malware.
- Utilize 'Procmon' to display the process tree and detect any terminated processes.



(Pre-exposed)



Process	Description	Image Path	Life Time	Company
Idle (0)		Idle		
System (4)		System		
csrss.exe (612)	Client Server Runt...	C:\Windows\syst...		Microsoft C
csrss.exe (688)	Client Server Runt...	C:\Windows\syst...		Microsoft C
wininit.exe (712)	Windows Start-Up...	C:\Windows\syst...		Microsoft C
winlogon.exe (760)	Windows Logon A...	C:\Windows\syst...		Microsoft C
Explorer.EXE (4388)	Windows Explorer	C:\Windows\Expl...		Microsoft C
tvnserver.exe (5376)	TightVNC Server	C:\Program Files\...		GlavSoft L
ProcessHacker.exe (4072)	Process Hacker	C:\Program Files\...		wj32
Procmon64.exe (4676)	Process Monitor	C:\Users\LetsDef...		Sysinternal
Procmon64.exe (4372)	Process Monitor	C:\Users\LetsDef...		Sysinternal
Regshot-x64-Unicode.exe (2176)	Regshot 1.9.0 x64...	C:\Users\LetsDef...		Regshot T
Regshot-x64-Unicode.exe (5080)	Regshot 1.9.0 x64...	C:\Users\LetsDef...		Regshot T
WinRAR.exe (2092)	WinRAR archiver	C:\Program Files\...		Alexander
c7513589f3f2e02007be1301c2f08c8809ea7526d85d7efcaf3bccf767a38855.exe (1348)	BPPForms	C:\Users\LetsDef...		
c7513589f3f2e02007be1301c2f08c8809ea7526d85d7efcaf3bccf767a38855.exe (5040)	BPPForms	C:\Users\LetsDef...		
c7513589f3f2e02007be1301c2f08c8809ea7526d85d7efcaf3bccf767a38855.exe (4012)	BPPForms	C:\Users\LetsDef...		
c7513589f3f2e02007be1301c2f08c8809ea7526d85d7efcaf3bccf767a38855.exe (5444)	BPPForms	C:\Users\LetsDef...		

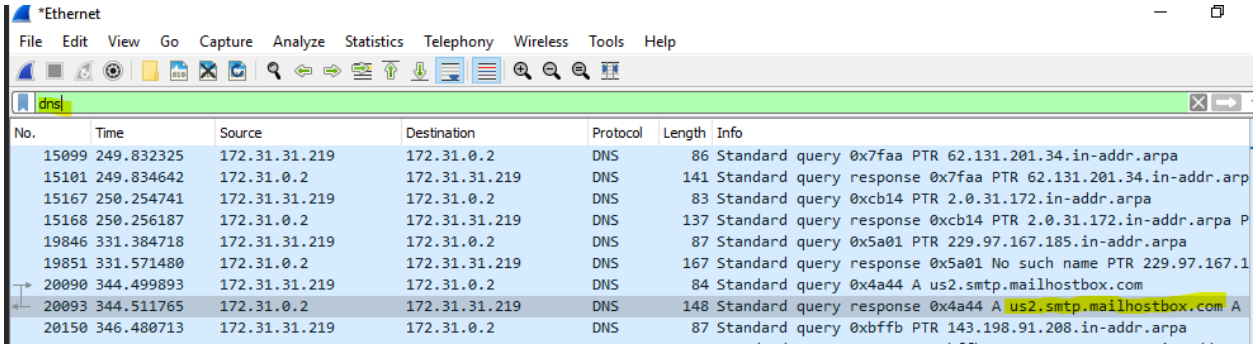
(After exposure)

Upon reviewing the image above, it becomes apparent that the initial process launches its own malware (**PID 1348**), initiating multiple instances of its own malware (**PIDs 5040, 4012, and 5444**) repeatedly.

We identified malicious processes (PIDs 1348, 5040, 4012, 5444) using Procmon. Now, our focus shifts to uncovering the network, file, and registry activities associated with these processes.

4. Network Activities:

- Use '**Wireshark/Fiddler**' to observe connections established during malware execution.
- Identify communication with the domain "us2.smtp.mailboxhost.com "

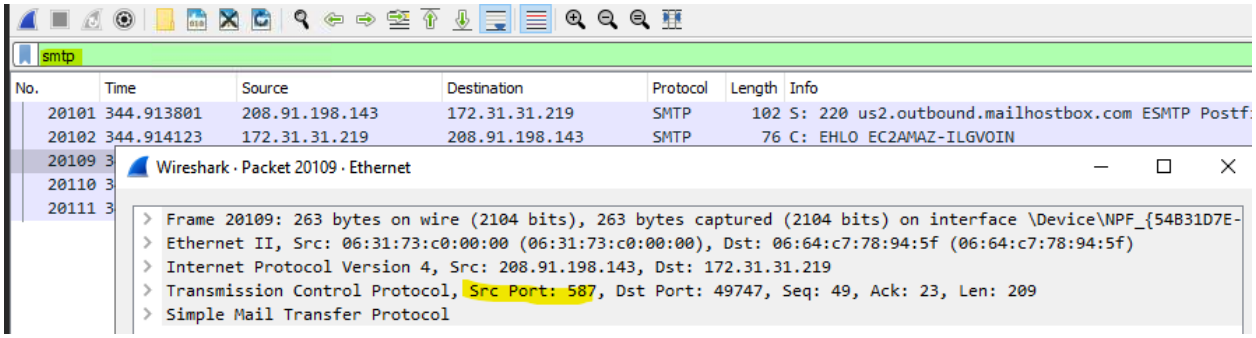


*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
15099	249.832325	172.31.31.219	172.31.0.2	DNS	86	Standard query 0x7faa PTR 62.131.201.34.in-addr.arpa
15101	249.834642	172.31.0.2	172.31.31.219	DNS	141	Standard query response 0x7faa PTR 62.131.201.34.in-addr.arp
15167	250.254741	172.31.31.219	172.31.0.2	DNS	83	Standard query 0xcb14 PTR 2.0.31.172.in-addr.arpa
15168	250.256187	172.31.0.2	172.31.31.219	DNS	137	Standard query response 0xcb14 PTR 2.0.31.172.in-addr.arpa P
19846	331.384718	172.31.31.219	172.31.0.2	DNS	87	Standard query 0x5a01 PTR 229.97.167.185.in-addr.arpa
19851	331.571480	172.31.0.2	172.31.31.219	DNS	167	Standard query response 0x5a01 No such name PTR 229.97.167.1
20090	344.499893	172.31.31.219	172.31.0.2	DNS	84	Standard query 0x4a44 A us2.smtp.mailhostbox.com
20093	344.511765	172.31.0.2	172.31.31.219	DNS	148	Standard query response 0x4a44 A us2.smtp.mailhostbox.com A
20150	346.480713	172.31.31.219	172.31.0.2	DNS	87	Standard query 0xbffb PTR 143.198.91.208.in-addr.arpa



Illustrative examples of what you might observe in Fiddler logs:

1. **Unusual Domain or IP Addresses:**
   - Normal: `www.google.com`
   - Suspicious: `malicious-domain.xyz` or `192.168.0.100`

2. **Unencrypted Communication:**
   - Normal: `https://www.example.com`
   - Suspicious: `http://malicious-site.com` (unencrypted HTTP)

3. **Unexpected Ports:**
   - Normal: `443` for HTTPS
   - Suspicious: Traffic on non-standard ports like `8080` or `6666`

4. **Uncommon User-Agent Strings:**
   - Normal: `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36`
   - Suspicious: `EvilUserAgent/1.0` or any uncommon or known-malicious string

5. **Unusual URI Patterns:**
   - Normal: `/path/to/resource`
   - Suspicious: `/malicious/path` or `obfuscated/URI/here`

6. **Unusual Content Types:**
   - Normal: `text/html`, `application/json`
   - Suspicious: Unexpected or uncommon content types like `application/x-msdownload`

7. **Large File Downloads:**
   - Normal: Downloading a small image or script
   - Suspicious: Downloading a large executable file or archive

8. **Multiple Failed Connections:**

- Normal: Occasional 404 errors
- Suspicious: Consecutive failed connections to different domains or resources

9. **Unusual Response Codes:**
   - Normal: `200` (OK), `404` (Not Found)
   - Suspicious: `500` (Internal Server Error), `302` (Found) without an apparent reason

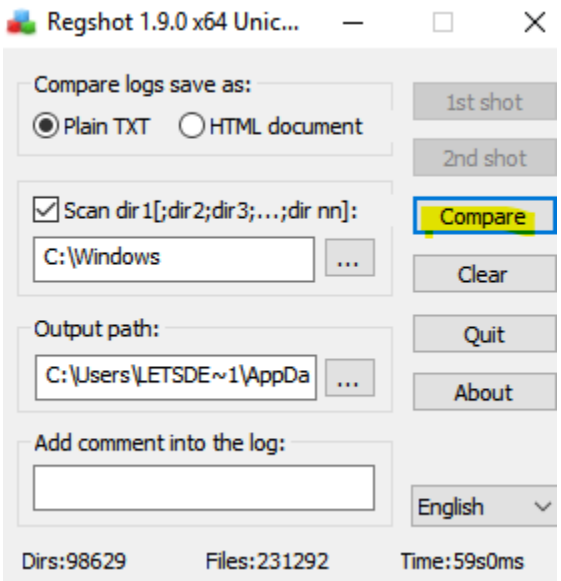
10. **Unusual Timing Patterns:**
    - Normal: Consistent response times
    - Suspicious: Irregular timing or unusually long delays for specific requests

11. **Unusual Request Methods:**
    - Normal: `GET`, `POST`, `HEAD`
    - Suspicious: Uncommon methods like `PUT`, `DELETE`, or combinations like `GET` with a request body

12. **Unexpected Cookies or Headers:**
    - Normal: Cookies and headers typical for the application
    - Suspicious: Unusual or malicious cookies, headers, or metadata

When using Fiddler/Wireshark, these examples illustrate the types of **anomalies or patterns** analysts might encounter that could indicate potential security issues. Always investigate deviations from the norm, cross-reference findings with threat intelligence sources, and consider the context of your specific network and application environment.

Now it's time to compare the pre-exposed shot with the exposure shot after the malware installation.



5. Registry Activities:

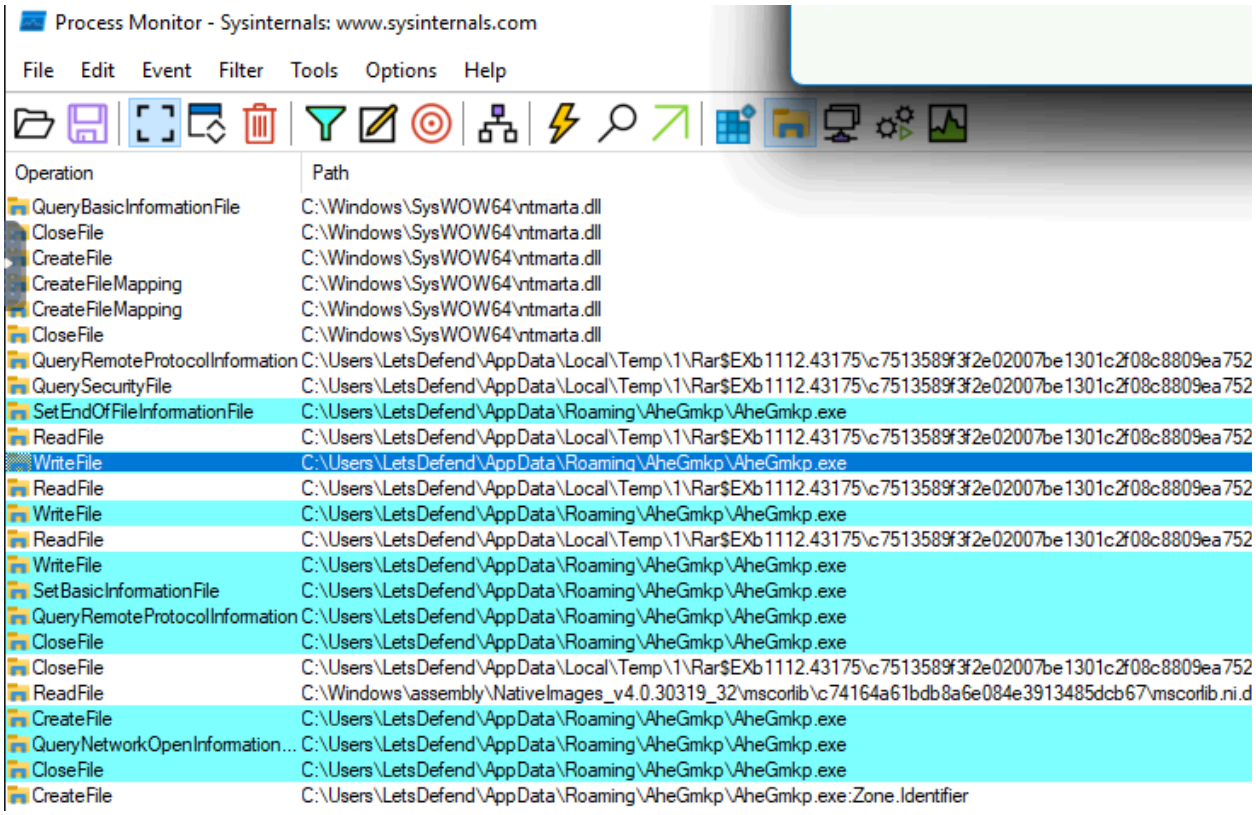
In malware analysis, specific registry keys are often examined as they can provide valuable insights into the system's configuration and potential malicious activities. Here are some common registry keys that analysts may look for:

1. **Run and RunOnce Keys:**
    - `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`
    - `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce`
    - `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`
    - `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce`

Keep in mind that these registry keys can be used by both legitimate software and malicious programs. Analyzing them in the context of the overall system behavior is crucial for accurate threat assessment.

- Examine registry activities, focusing on keys under `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`.
- Detect applications installed on the system by attackers.

6. File Activities:



Operation	Path
QueryBasicInformationFile	C:\Windows\SysWOW64\ntmarta.dll
CloseFile	C:\Windows\SysWOW64\ntmarta.dll
CreateFile	C:\Windows\SysWOW64\ntmarta.dll
CreateFileMapping	C:\Windows\SysWOW64\ntmarta.dll
CreateFileMapping	C:\Windows\SysWOW64\ntmarta.dll
CloseFile	C:\Windows\SysWOW64\ntmarta.dll
QueryRemoteProtocolInformation	C:\Users\LetsDefend\AppData\Local\Temp\1\Rar$EXb1112.43175\c7513589f3f2e02007be1301c2f08c8809ea752
QuerySecurityFile	C:\Users\LetsDefend\AppData\Local\Temp\1\Rar$EXb1112.43175\c7513589f3f2e02007be1301c2f08c8809ea752
SetEndOfFileInformationFile	C:\Users\LetsDefend\AppData\Roaming\AheGmkp\AheGmkp.exe
ReadFile	C:\Users\LetsDefend\AppData\Local\Temp\1\Rar$EXb1112.43175\c7513589f3f2e02007be1301c2f08c8809ea752
WriteFile	C:\Users\LetsDefend\AppData\Roaming\AheGmkp\AheGmkp.exe
ReadFile	C:\Users\LetsDefend\AppData\Local\Temp\1\Rar$EXb1112.43175\c7513589f3f2e02007be1301c2f08c8809ea752
WriteFile	C:\Users\LetsDefend\AppData\Roaming\AheGmkp\AheGmkp.exe
ReadFile	C:\Users\LetsDefend\AppData\Local\Temp\1\Rar$EXb1112.43175\c7513589f3f2e02007be1301c2f08c8809ea752
WriteFile	C:\Users\LetsDefend\AppData\Roaming\AheGmkp\AheGmkp.exe
SetBasicInformationFile	C:\Users\LetsDefend\AppData\Roaming\AheGmkp\AheGmkp.exe
QueryRemoteProtocolInformation	C:\Users\LetsDefend\AppData\Roaming\AheGmkp\AheGmkp.exe
CloseFile	C:\Users\LetsDefend\AppData\Roaming\AheGmkp\AheGmkp.exe
CloseFile	C:\Users\LetsDefend\AppData\Local\Temp\1\Rar$EXb1112.43175\c7513589f3f2e02007be1301c2f08c8809ea752
ReadFile	C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\c74164a61bdb8a6e084e3913485dcb67\mscorlib.ni.d
CreateFile	C:\Users\LetsDefend\AppData\Roaming\AheGmkp\AheGmkp.exe
QueryNetworkOpenInformation...	C:\Users\LetsDefend\AppData\Roaming\AheGmkp\AheGmkp.exe
CloseFile	C:\Users\LetsDefend\AppData\Roaming\AheGmkp\AheGmkp.exe
CreateFile	C:\Users\LetsDefend\AppData\Roaming\AheGmkp\AheGmkp.exe:Zone.Identifier

- Use 'Procmon' to filter file creation activities.
- Identify the creation of the file "aheGmkp.exe" under "**C:\Users\LetsDefend\AppData\Roaming**".
- Verify the file's hash using 'HashMyFiles.'

7. Results

- Summarize findings, including:
    - Copying the malware to "**C:\Users\LetsDefend\AppData\Roaming**" as "aheGmkp.exe."
    - The malware establishes a connection for data hijacking with the domain "**us2.smtp.mailboxhost.com**."
    - **The malware communicates over** port 587.
    - The executable file generated by the malicious application and saved in the AppData directory is named: **aheGmkp.exe**
    - The Registry Key utilized by the malware for ensuring persistence is: HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN

8. Artifacts

MD5: N/A
SHA256: N/A
File Name: c7513589f3f2e02007be1301c2f08c8809ea7526d85d7efcaf3bccf767a38855.exe
File Name: aheGmkp.exe
Domain: us2.smtp.mailboxhost.com
URL: N/A