Sherlock Scenario

Forela's CTO, Dutch, stores important files on a separate Windows system because the domain environment at Forela is frequently breached due to its exposure across various industries. On 24 January 2025, our worst fears were realised when an intruder accessed the fileserver, installed utilities to aid their actions, stole critical files, and then deleted them, rendering them unrecoverable. The team was immediately informed of the extortion attempt by the intruders, who are now demanding money. While our legal team addresses the situation, we must quickly perform triage to assess the incident's extent. Note from the manager: We enabled SmartScreen Debug Logs across all our machines for enhanced visibility a few days ago, following a security research recommendation. These logs can provide quick insights, so ensure they are utilised.

Artifacts

We are provided with a password protected zip file, which contains evtx log files we have to analyse these files to clear this challange.

Important!

If you are using a linux environment like me you wouldn't be able to view evtx log files, because **evtx (Event Log) file** is a proprietary log format used by Windows Event Viewer to store system, security, and application logs. These logs help in monitoring system performance, security events, and troubleshooting issues. For the purpose of this challange I used evtx2json. For more information visit https://github.com/vavarachen/evtx2json.

Evtx2json Installation:

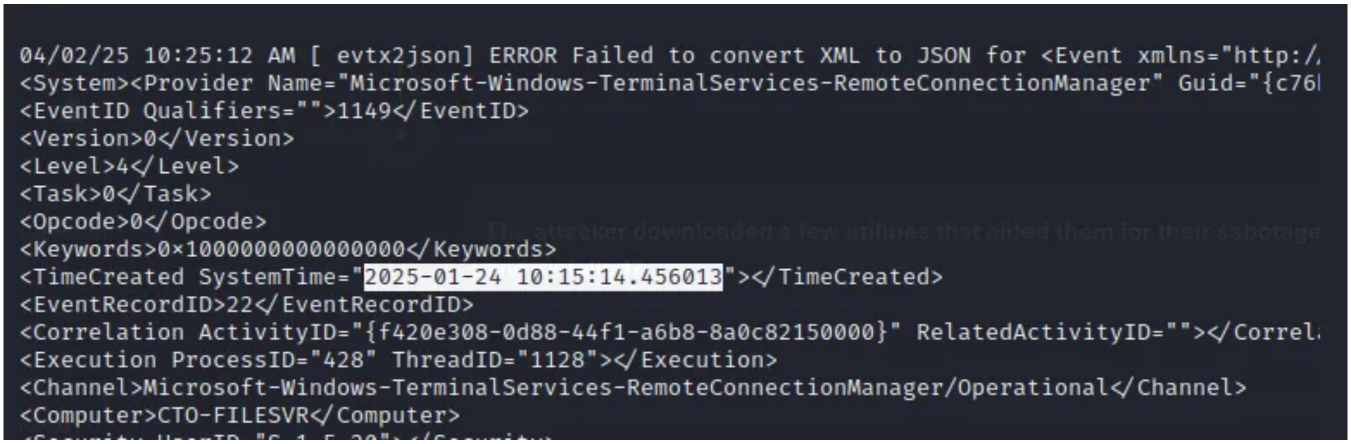
```
git clone https://github.com/vavarachen/evtx2json
pip install --user --requirement requirements.txt
```

Then cd to evtx2json folder, then run:

“python evtx2json.py process_files — files /path/to/file.evtx folder/*.evtx”.

Alternative method: There are several evtx to json/evtx to csv online converters.

Task 1: The attacker logged in to the machine where Dutch saves critical files, via RDP on 24th January 2025. Please determine the timestamp of this login.



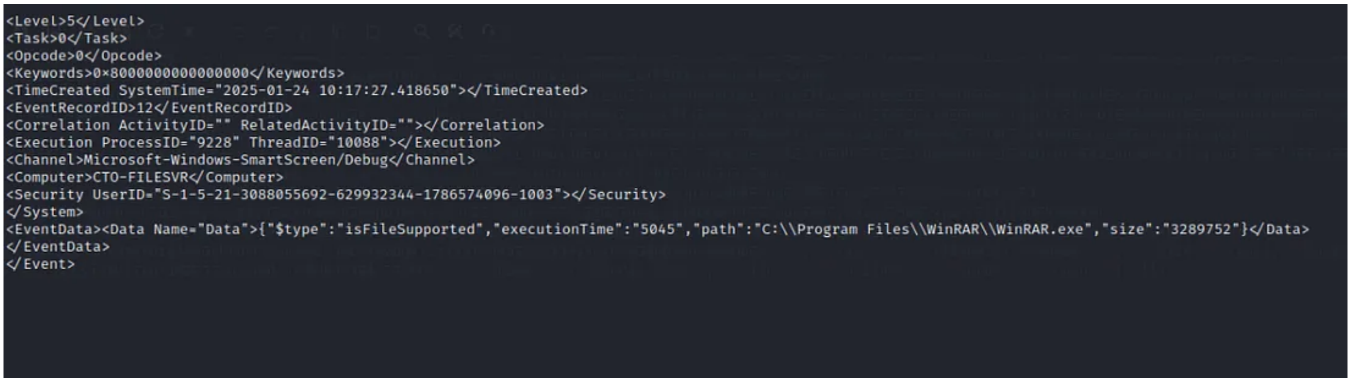
```
04/02/25 10:25:12 AM [ evtx2json] ERROR Failed to convert XML to JSON for <Event xmlns="http:/
<System><Provider Name="Microsoft-Windows-TerminalServices-RemoteConnectionManager" Guid="{c76
<EventID Qualifiers="">1149</EventID>
<Version>0</Version>
<Level>4</Level>
<Task>0</Task>
<Opcode>0</Opcode>
<Keywords>0×1000000000000000</Keywords>
<TimeCreated SystemTime="2025-01-24 10:15:14.456013"></TimeCreated>
<EventRecordID>22</EventRecordID>
<Correlation ActivityID="{f420e308-0d88-44f1-a6b8-8a0c82150000}" RelatedActivityID=""></Correl
<Execution ProcessID="428" ThreadID="1128"></Execution>
<Channel>Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational</Channel>
<Computer>CTO-FILESVR</Computer>
<Security UserID="S-1-5-20"></Security>
```

Use Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational Log and filter for event id 1149

Event id 1149 in Windows Event logs refers to: Remote Desktop Services: User authentication succeeded

Answer: 2025–01–24 10:15:14

Task 2: The attacker downloaded a few utilities that aided them for their sabotage and extortion operation. What was the first tool they downloaded and installed?

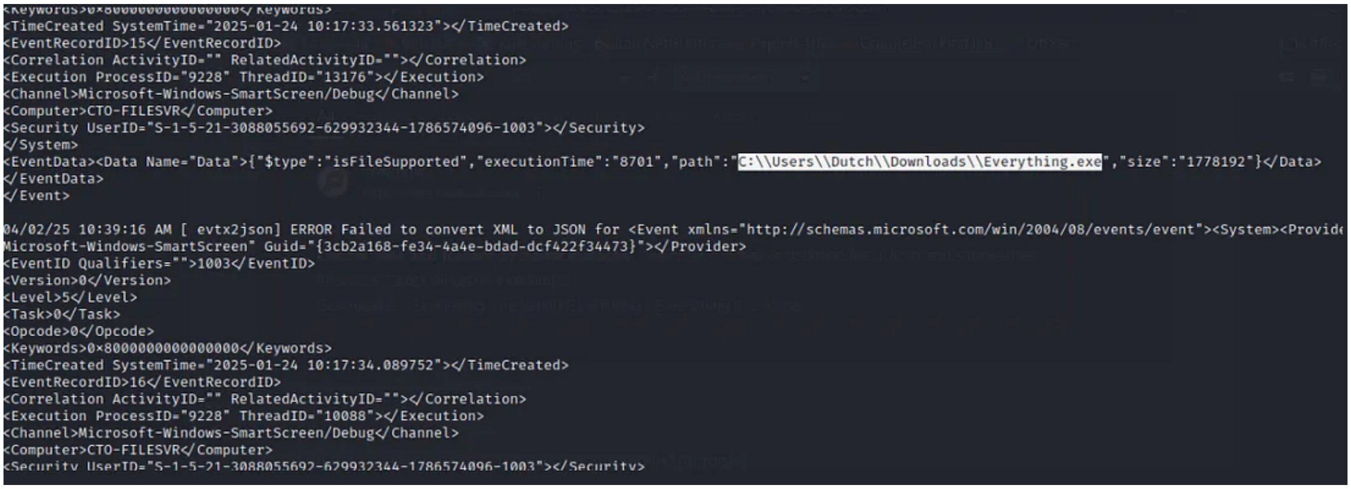


```
<Level>5</Level>
<Task>0</Task>
<Opcode>0</Opcode>
<Keywords>0×8000000000000000</Keywords>
<TimeCreated SystemTime="2025-01-24 10:17:27.418650"></TimeCreated>
<EventRecordID>12</EventRecordID>
<Correlation ActivityID="" RelatedActivityID=""></Correlation>
<Execution ProcessID="9228" ThreadID="10088"></Execution>
<Channel>Microsoft-Windows-SmartScreen/Debug</Channel>
<Computer>CTO-FILESVR</Computer>
<Security UserID="S-1-5-21-3088055692-629932344-1786574096-1003"></Security>
</System>
<EventData><Data Name="Data">{"$type":"isFileSupported","executionTime":"5045","path":"C:\\Program Files\\WinRAR\\WinRAR.exe","size":"3289752"}</Data>
</EventData>
</Event>
```

Use Smartscreen Debug Log. The extra backslashes in the file path are a result of how the data is represented in certain tools or file formats.

Answer: Winrar

Task 3: They then proceeded to download and then execute the portable version of a tool that could be used to search for files on the machine quickly and efficiently. What was the full path of the executable?

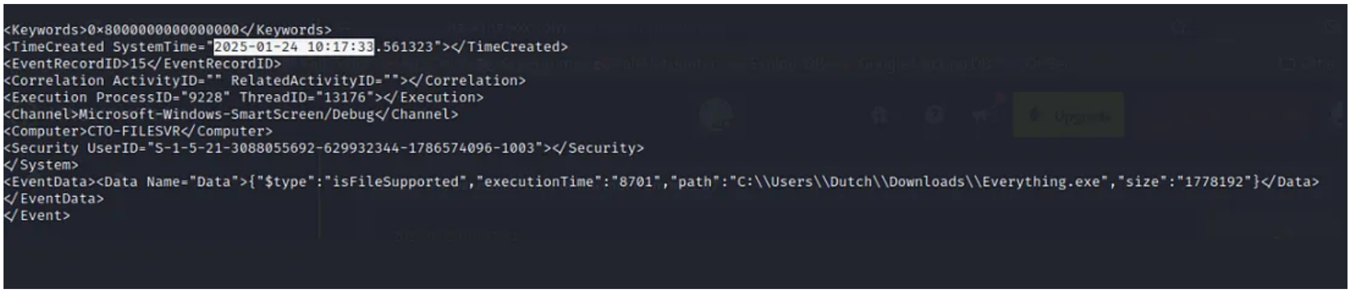


```
<Keywords>0×8000000000000000</Keywords>
<TimeCreated SystemTime="2025-01-24 10:17:33.561323"></TimeCreated>
<EventRecordID>15</EventRecordID>
<Correlation ActivityID="" RelatedActivityID=""></Correlation>
<Execution ProcessID="9228" ThreadID="13176"></Execution>
<Channel>Microsoft-Windows-SmartScreen/Debug</Channel>
<Computer>CTO-FILESVR</Computer>
<Security UserID="S-1-5-21-3088055692-629932344-1786574096-1003"></Security>
</System>
<EventData><Data Name="Data">{"$type":"isFileSupported","executionTime":"8701","path":"C:\\Users\\Dutch\\Downloads\\Everything.exe","size":"1778192"}</Data>
</EventData>
</Event>

04/02/25 10:39:16 AM [ evtx2json] ERROR Failed to convert XML to JSON for <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provide
Microsoft-Windows-SmartScreen" Guid="{3cb2a168-fe34-4a4e-bdad-dcf422f34473}"></Provider>
<EventID Qualifiers="">1003</EventID>
<Version>0</Version>
<Level>5</Level>
<Task>0</Task>
<Opcode>0</Opcode>
<Keywords>0×8000000000000000</Keywords>
<TimeCreated SystemTime="2025-01-24 10:17:34.089752"></TimeCreated>
<EventRecordID>16</EventRecordID>
<Correlation ActivityID="" RelatedActivityID=""></Correlation>
<Execution ProcessID="9228" ThreadID="10088"></Execution>
<Channel>Microsoft-Windows-SmartScreen/Debug</Channel>
<Computer>CTO-FILESVR</Computer>
<Security UserID="S-1-5-21-3088055692-629932344-1786574096-1003"></Security>
```

Use Smartscreen Debug Log. Everything.exe is a windows utility that can rapidly find files and folders by name.

Answer: C:\Users\Dutch\Downloads\Everything.exe

Task 4: What is the execution time of the tool from task 3?

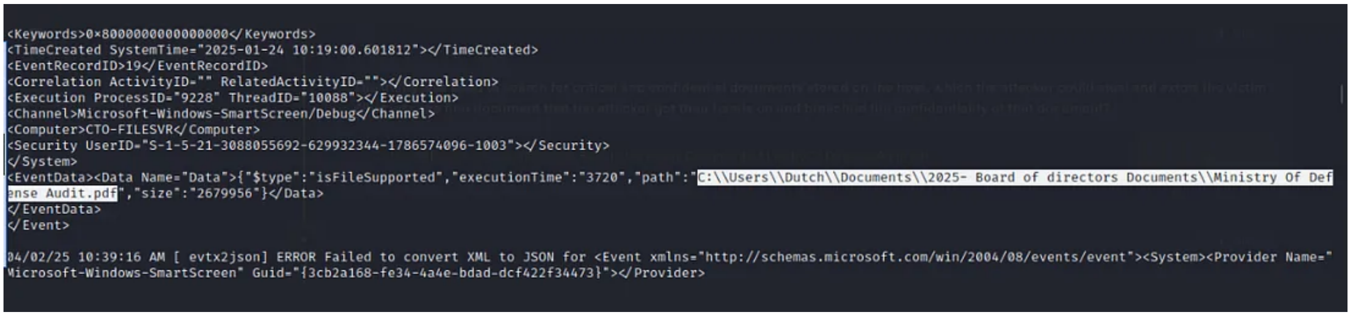


```
<Keywords>0×8000000000000000</Keywords>
<TimeCreated SystemTime="2025-01-24 10:17:33.561323"></TimeCreated>
<EventRecordID>15</EventRecordID>
<Correlation ActivityID="" RelatedActivityID=""></Correlation>
<Execution ProcessID="9228" ThreadID="13176"></Execution>
<Channel>Microsoft-Windows-SmartScreen/Debug</Channel>
<Computer>CTO-FILESVR</Computer>
<Security UserID="S-1-5-21-3088055692-629932344-1786574096-1003"></Security>
</System>
<EventData><Data Name="Data">{"$type":"isFileSupported","executionTime":"8701","path":"C:\\Users\\Dutch\\Downloads\\Everything.exe","size":"1778192"}</Data>
</EventData>
</Event>
```

Use Smartscreen Debug Log.

Answer: 2025–01–24 10:17:33

Task 5: The utility was used to search for critical and confidential documents stored on the host, which the attacker could steal and extort the victim. What was the first document that the attacker got their hands on and breached the confidentiality of that document?

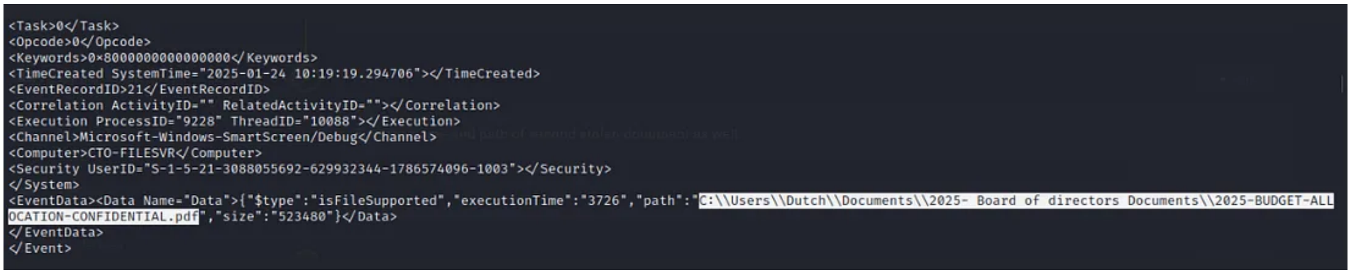


```
<Keywords>0×8000000000000000</Keywords>
<TimeCreated SystemTime="2025-01-24 10:19:00.601812"></TimeCreated>
<EventRecordID>19</EventRecordID>
<Correlation ActivityID="" RelatedActivityID=""></Correlation>
<Execution ProcessID="9228" ThreadID="10088"></Execution>
<Channel>Microsoft-Windows-SmartScreen/Debug</Channel>
<Computer>CTO-FILESVR</Computer>
<Security UserID="S-1-5-21-3088055692-629932344-1786574096-1003"></Security>
</System>
<EventData><Data Name="Data">{"$type":"isFileSupported","executionTime":"3720","path":"C:\\Users\\Dutch\\Documents\\2025- Board of directors Documents\\Ministry Of Def
ense Audit.pdf","size":"2679956"}</Data>
</EventData>
</Event>

04/02/25 10:39:16 AM [ evtx2json] ERROR Failed to convert XML to JSON for <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="
Microsoft-Windows-SmartScreen" Guid="{3cb2a168-fe34-4a4e-bdad-dcf422f34473}"></Provider>
```

Use Smartscreen Debug Log.

Answer: C:\Users\Dutch\Documents\2025- Board of directors Documents\Ministry Of Defense Audit.pdf

Task 6: Find the name and path of second stolen document as well.

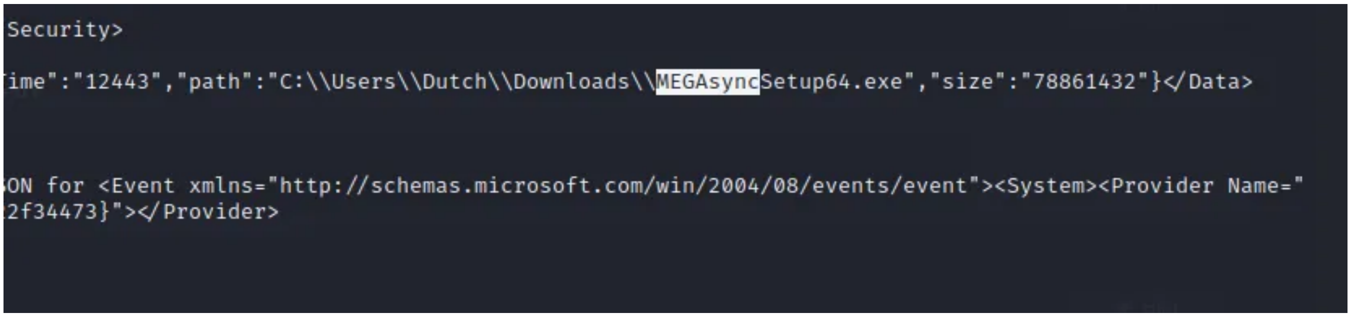


```
<Task>0</Task>
<Opcode>0</Opcode>
<Keywords>0×8000000000000000</Keywords>
<TimeCreated SystemTime="2025-01-24 10:19:19.294706"></TimeCreated>
<EventRecordID>21</EventRecordID>
<Correlation ActivityID="" RelatedActivityID=""></Correlation>
<Execution ProcessID="9228" ThreadID="10088"></Execution>
<Channel>Microsoft-Windows-SmartScreen/Debug</Channel>
<Computer>CTO-FILESVR</Computer>
<Security UserID="S-1-5-21-3088055692-629932344-1786574096-1003"></Security>
</System>
<EventData><Data Name="Data">{"$type":"isFileSupported","executionTime":"3726","path":"C:\\Users\\Dutch\\Documents\\2025- Board of directors Documents\\2025-BUDGET-ALL
OCATION-CONFIDENTIAL.pdf","size":"523480"}</Data>
</EventData>
</Event>
```

Use Smartscreen Debug Log.

Answer: C:\Users\Dutch\Documents\2025- Board of directors Documents\2025-BUDGET-ALLOCATION-CONFIDENTIAL.pdf

Task 7: The attacker installed a Cloud utility as well to steal and exfiltrate the documents. What is name of the cloud utility?

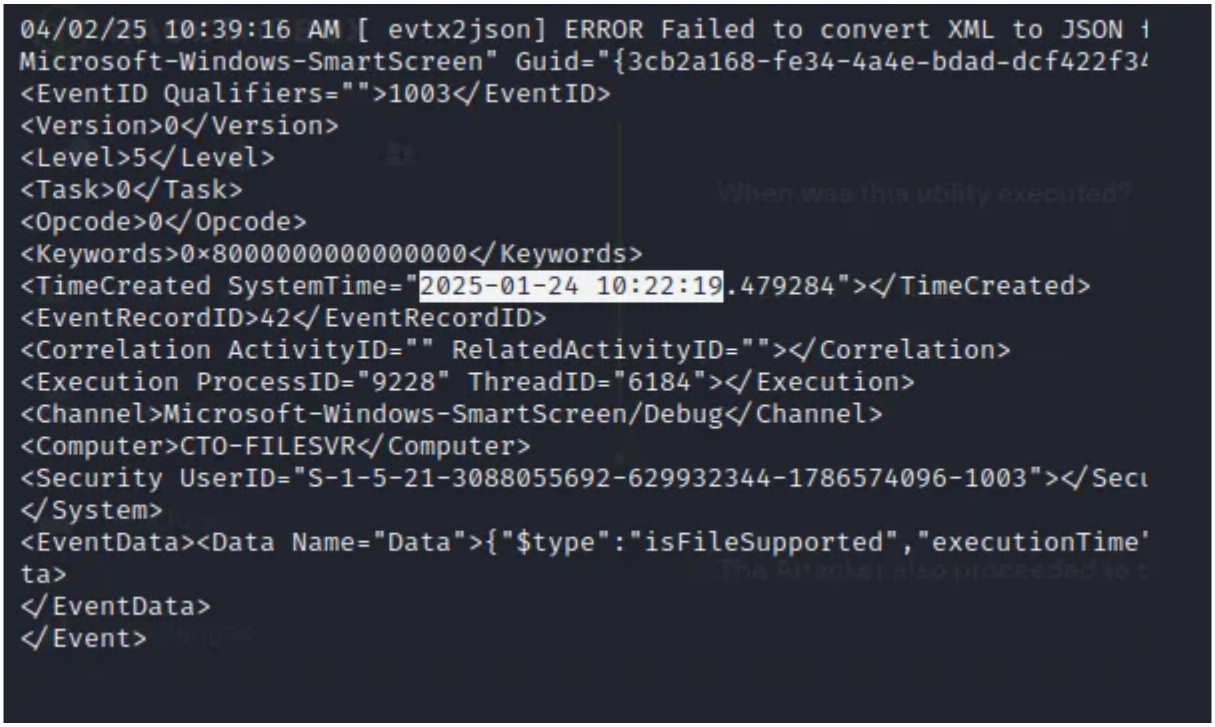


```
Security>

ime":"12443","path":"C:\\Users\\Dutch\\Downloads\\MEGAsyncSetup64.exe","size":"78861432"}</Data>


ON for <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name="
2f34473}"></Provider>
```

Use Smartscreen Debug Log.

Answer: MEGAsync

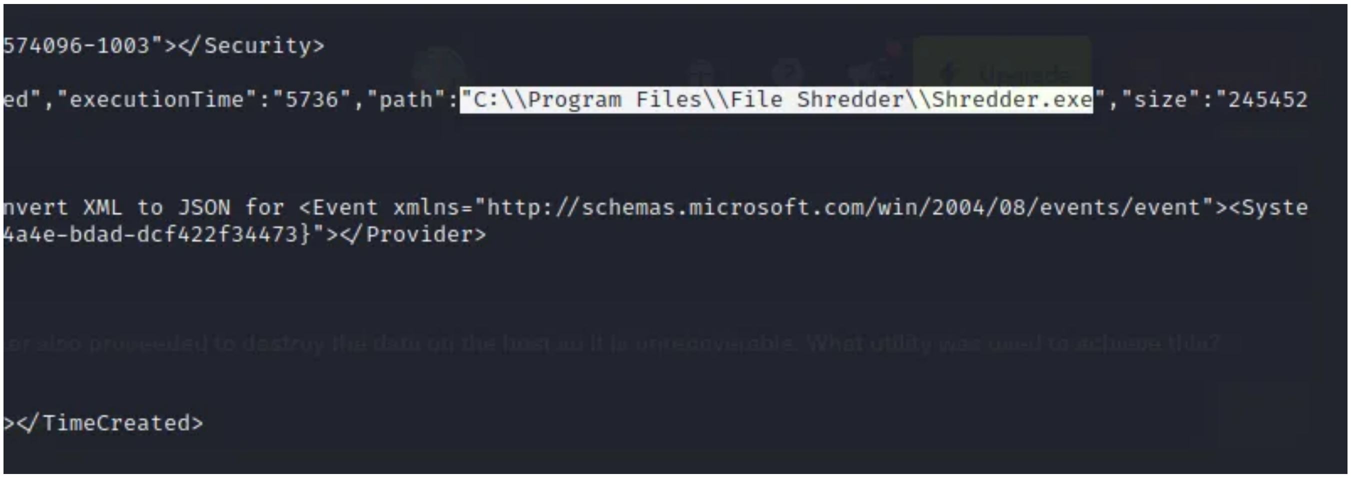
Task 8: When was this utility executed?



```
04/02/25 10:39:16 AM [ evtx2json] ERROR Failed to convert XML to JSON f
Microsoft-Windows-SmartScreen" Guid="{3cb2a168-fe34-4a4e-bdad-dcf422f34
<EventID Qualifiers="">1003</EventID>
<Version>0</Version>
<Level>5</Level>
<Task>0</Task>
<Opcode>0</Opcode>
<Keywords>0x8000000000000000</Keywords>
<TimeCreated SystemTime="2025-01-24 10:22:19.479284"></TimeCreated>
<EventRecordID>42</EventRecordID>
<Correlation ActivityID="" RelatedActivityID=""></Correlation>
<Execution ProcessID="9228" ThreadID="6184"></Execution>
<Channel>Microsoft-Windows-SmartScreen/Debug</Channel>
<Computer>CTO-FILESVR</Computer>
<Security UserID="S-1-5-21-3088055692-629932344-1786574096-1003"></Secu
</System>
<EventData><Data Name="Data">{"$type":"isFileSupported","executionTime'
ta>
</EventData>
</Event>
```

Find evidence of execution of the utility itself, and not of the setup.

Task 9: The Attacker also proceeded to destroy the data on the host so it is unrecoverable. What utility was used to achieve this?

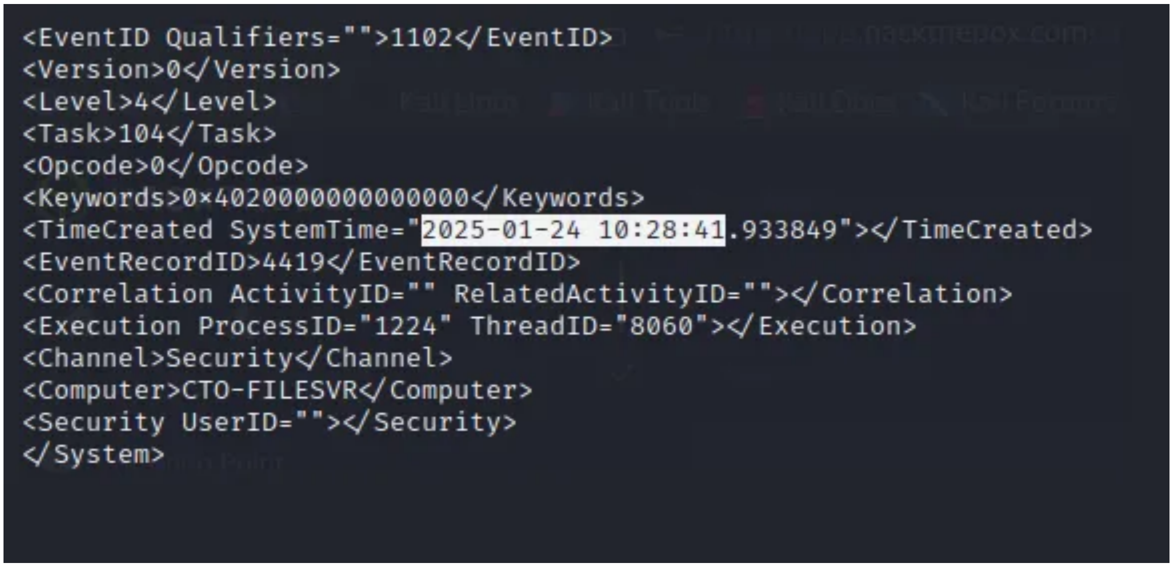


```
574096-1003"></Security>

ed","executionTime":"5736","path":"C:\\Program Files\\File Shredder\\Shredder.exe","size":"245452


nvert XML to JSON for <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><Syste
4a4e-bdad-dcf422f34473}"></Provider>


></TimeCreated>
```

Use Smartscreen Debug Log.

Answer: File Shredder

Task 10: The attacker cleared 2 important logs, thinking they covered all their tracks. When was the security log cleared?



```
<EventID Qualifiers="">1102</EventID>
<Version>0</Version>
<Level>4</Level>
<Task>104</Task>
<Opcode>0</Opcode>
<Keywords>0x4020000000000000</Keywords>
<TimeCreated SystemTime="2025-01-24 10:28:41.933849"></TimeCreated>
<EventRecordID>4419</EventRecordID>
<Correlation ActivityID="" RelatedActivityID=""></Correlation>
<Execution ProcessID="1224" ThreadID="8060"></Execution>
<Channel>Security</Channel>
<Computer>CTO-FILESVR</Computer>
<Security UserID=""></Security>
</System>
```

Filter for event id 1102 in security log. “Event ID 1102 refers to the audit log was cleared”.

Answer: 2025–01–24 10:28:41