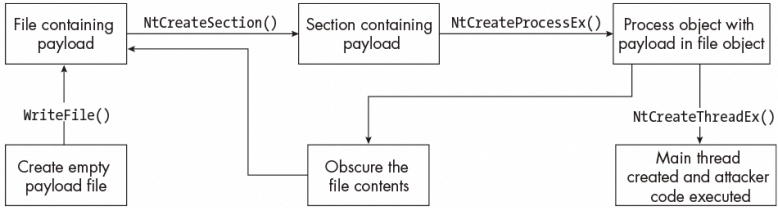
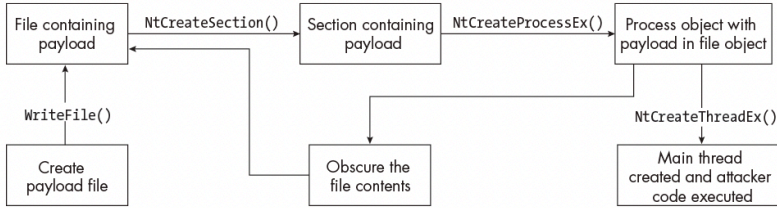
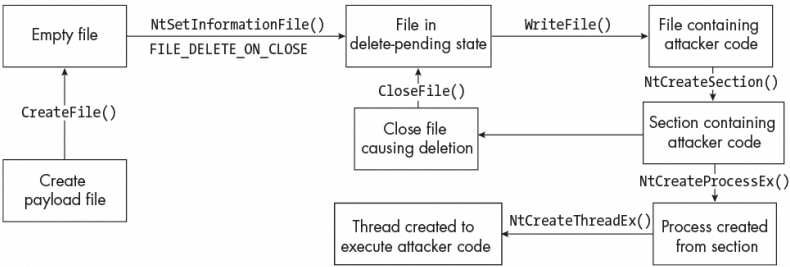
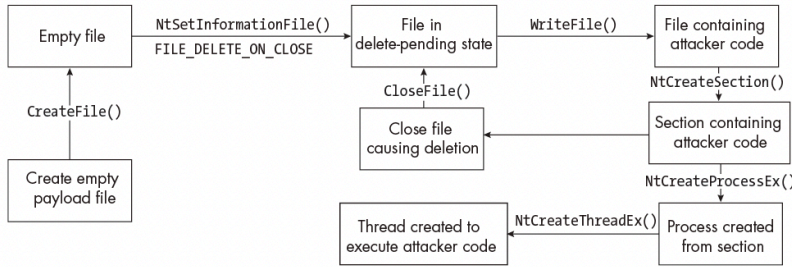


Evading EDR

The Definitive Guide to Defeating Endpoint Detection

by Matt Hand

errata updated to print 1

Page	Error	Correction	Print corrected
52	 <p>Figure 3-11: The execution flow of process herpaderping</p>	 <p>Figure 3-11: The execution flow of process herpaderping</p>	Pending
53	 <p>Figure 3-12: The process-ghosting workflow</p>	 <p>Figure 3-12: The process-ghosting workflow</p>	Pending
92	For the most part, services run as the privileged <code>NT AUTHORITY\SYSTEM</code> account,	For the most part, services run as the privileged <code>NT AUTHORITY\SYSTEM</code> account,	Pending
140	<pre>>> Where-Object {\$_Name -notlike 'WFP Built-in*'} </pre>	<pre>>> Where-Object {\$_Name -notlike 'WFP Built-in*'} </pre>	Pending
150	<pre>PS > logman.exe query 'EventLog-System' -ets</pre>	<pre>PS > logman.exe query EventLog-System -ets</pre>	Pending

Page	Error	Correction	Print corrected																				
166	<pre>logman.exe stop "TRACE_NAME" -ets</pre>	<pre>logman.exe stop TRACE_NAME -ets</pre>	Pending																				
222	<i>Listing 12-11: Loading call trees into Ghidra</i>	<i>Listing 12-11: Loading call trees into Neo4j</i>	Pending																				
257	<pre>PS > \$type = [Type]::GetTypeFromProgId(Excel.Workbook.16)</pre>	<pre>PS > \$type = [Type]::GetTypeFromProgId("Excel.Workbook.16")</pre>	Pending																				
258	<table border="1"> <thead> <tr> <th>Registry key</th> <th>Operation</th> </tr> </thead> <tbody> <tr> <td><code>SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\ .xlsx\UserChoice</code></td> <td>Delete</td> </tr> <tr> <td><code>SOFT-WARE\Microsoft\Windows\CurrentVer-si-on\Explorer\FileExts\ .xlsx\UserChoice</code></td> <td>Create</td> </tr> <tr> <td><code>SOFT-WARE\Microsoft\Windows\CurrentVer-si-on\Explorer\FileExts\ .xlsx\UserChoice\Hash</code></td> <td>Set value</td> </tr> <tr> <td><code>SOFT-WARE\Microsoft\Windows\CurrentVer-si-on\Explorer\FileExts\ .xlsx\UserChoice\ProgId</code></td> <td>Set value</td> </tr> </tbody> </table>	Registry key	Operation	<code>SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\ .xlsx\UserChoice</code>	Delete	<code>SOFT-WARE\Microsoft\Windows\CurrentVer-si-on\Explorer\FileExts\ .xlsx\UserChoice</code>	Create	<code>SOFT-WARE\Microsoft\Windows\CurrentVer-si-on\Explorer\FileExts\ .xlsx\UserChoice\Hash</code>	Set value	<code>SOFT-WARE\Microsoft\Windows\CurrentVer-si-on\Explorer\FileExts\ .xlsx\UserChoice\ProgId</code>	Set value	<table border="1"> <thead> <tr> <th>Registry key</th> <th>Operation</th> </tr> </thead> <tbody> <tr> <td><code>SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\ .xlsx\UserChoice</code></td> <td>Delete</td> </tr> <tr> <td><code>SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\ .xlsx\UserChoice</code></td> <td>Create</td> </tr> <tr> <td><code>SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\ .xlsx\UserChoice\Hash</code></td> <td>Set value</td> </tr> <tr> <td><code>SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\ .xlsx\UserChoice\ProgId</code></td> <td>Set value</td> </tr> </tbody> </table>	Registry key	Operation	<code>SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\ .xlsx\UserChoice</code>	Delete	<code>SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\ .xlsx\UserChoice</code>	Create	<code>SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\ .xlsx\UserChoice\Hash</code>	Set value	<code>SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\ .xlsx\UserChoice\ProgId</code>	Set value	Pending
Registry key	Operation																						
<code>SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\ .xlsx\UserChoice</code>	Delete																						
<code>SOFT-WARE\Microsoft\Windows\CurrentVer-si-on\Explorer\FileExts\ .xlsx\UserChoice</code>	Create																						
<code>SOFT-WARE\Microsoft\Windows\CurrentVer-si-on\Explorer\FileExts\ .xlsx\UserChoice\Hash</code>	Set value																						
<code>SOFT-WARE\Microsoft\Windows\CurrentVer-si-on\Explorer\FileExts\ .xlsx\UserChoice\ProgId</code>	Set value																						
Registry key	Operation																						
<code>SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\ .xlsx\UserChoice</code>	Delete																						
<code>SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\ .xlsx\UserChoice</code>	Create																						
<code>SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\ .xlsx\UserChoice\Hash</code>	Set value																						
<code>SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\ .xlsx\UserChoice\ProgId</code>	Set value																						