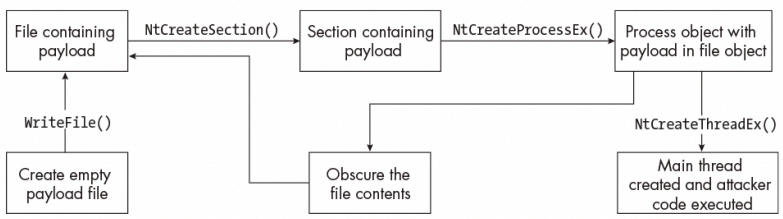
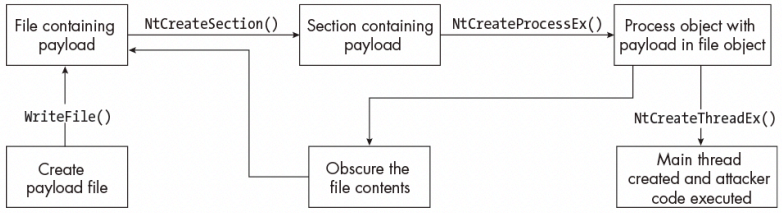
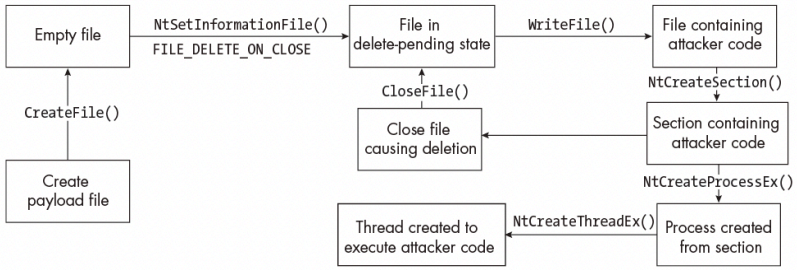
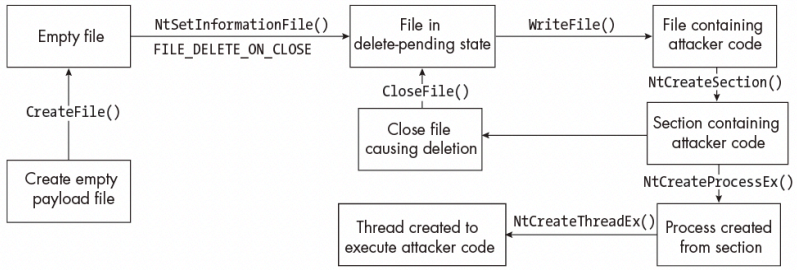
Evading EDR

The Definitive Guide to Defeating Endpoint Detection

by Matt Hand

Errata updated to print 1

Page	Error	Correction	Print corrected
52	 *Figure 3-11: The execution flow of process herpaderping*	 *Figure 3-11: The execution flow of process herpaderping*	Pending
53	 *Figure 3-12: The process-ghosting workflow*	 *Figure 3-12: The process-ghosting workflow*	Pending
92	For the most part, services run as the privileged *NT AUTHORITY/SYSTEM* account,	For the most part, services run as the privileged *NT AUTHORITY\SYSTEM* account,	Pending
140	`>> Where-Object {$_.Name -notlike 'WFP Built-in*'} |`	`>> Where-Object {$_.Name -notlike 'WFP Built-in*'} |`	Pending
150	`PS > logman.exe query 'EventLog-System' -ets`	`PS > logman.exe query EventLog-System -ets`	Pending
158	The `ExtendedData` member matches the data passed in the **`EnableProperty`** parameter of `sechost!EnableTraceEx2()`.	The `ExtendedData` member matches the data passed in the **`EnableParameters`** parameter of `sechost!EnableTraceEx2()`.	Pending

<table>
<tr><th>Page</th><th>Error</th><th>Correction</th><th>Print corrected</th></tr>
<tr><td>166</td><td>

```
logman.exe stop "TRACE_NAME" -ets
```

</td><td>

```
logman.exe stop TRACE_NAME -ets
```

</td><td>Pending</td></tr>
<tr><td>222</td><td>Listing 12-11: Loading call trees into Ghidra</td><td>Listing 12-11: Loading call trees into Neo4j</td><td>Pending</td></tr>
<tr><td>257</td><td>

```
PS > $type = [Type]::GetTypeFromProgId(Excel.Workbook.16)
```

</td><td>

```
PS > $type = [Type]::GetTypeFromProgId("Excel.Workbook.16")
```

</td><td>Pending</td></tr>
<tr><td>258</td><td>
<table>
<tr><th>Registry key</th><th>Operation</th></tr>
<tr><td>SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.xlsx\UserChoice</td><td>Delete</td></tr>
<tr><td>SOFT-WARE\Microsoft\Windows\CurrentVer-si-on\Explorer\FileExts\.xlsx\UserChoice</td><td>Create</td></tr>
<tr><td>SOFT-WARE\Microsoft\Windows\CurrentVer-si-on\Explorer\FileExts\.xlsx\UserChoice\Hash</td><td>Set value</td></tr>
<tr><td>SOFT-WARE\Microsoft\Windows\CurrentVer-si-on\Explorer\FileExts\.xlsx\UserChoice\ProgId</td><td>Set value</td></tr>
</table>
</td><td>
<table>
<tr><th>Registry key</th><th>Operation</th></tr>
<tr><td>SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.xlsx\UserChoice</td><td>Delete</td></tr>
<tr><td>SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.xlsx\UserChoice</td><td>Create</td></tr>
<tr><td>SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.xlsx\UserChoice\Hash</td><td>Set value</td></tr>
<tr><td>SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.xlsx\UserChoice\ProgId</td><td>Set value</td></tr>
</table>
</td><td>Pending</td></tr>
</table>