



Blu3-Team



Introducing the structure and methods with real examples. Operations are my own and not my employer's.

Misleading extensions Xls.exe Doc.exe Pdf.exe



June 24, 2019

I get something out of twitter almost every day and it is not uncommon to see examples a few times before the realization sinks in that you are looking at a technique that needs a rule. These should fall under the ATT&CK framework as masquerading.

I saw a [tweet](#) the other day that reminded me of a couple of signatures worth talking about. These misleading double extensions are not new but they never seem to go out of style. With modern EDRs it is an easy win.

The malware filename ended in .xls.exe but lets expand that to include other office file types.

```
index=edr ( doc OR docx OR xls OR xlsx OR pdf ) exe ( process_path=*.doc.exe OR  
process_path=*.docx.exe OR process_path=*.xls.exe OR process_path=*.xlsx.exe OR  
process_path=*.pdf.exe )
```

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS OK !

Another tweet by [blackorbird](#) shows a filename with a bunch of leading underscores "_____.exe" and lets expand that to include spaces.

```
index=edr exe process_path=*_____.exe OR process_path="* .exe"
```

Searching for Sigma rules on [Neo23x0](#) I found a related example looking for filenames in a Rar file with Pdf and then a script extension. I am sure he has these other variants somewhere as well.

```
index=edr pdf ( process_path=*.pdf.bat OR process_path=*.pdf.ps1 OR  
process_path=*.pdf.vbs OR process_path=*.pdf.vbe )
```

References:

<https://twitter.com/blackorbird/status/1140519090961825792>

<https://twitter.com/blackorbird/status/1098170487773921281>

<https://github.com/Neo23x0/sigma> gen_suspicious_strings.yar

<https://attack.mitre.org/techniques/T1036/>

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS OK !



#threathunting

Carbon Black

Masquerading

Splunk

threathunting

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

EN SAVOIR PLUS **OK !**

downloads are already under review so some other directory should be used. ...

[READ MORE](#)

Powershell DNS C2 Notes

August 25, 2019

I recently took a look at Powershell DNS C2 and found a couple of interesting things. The special case of DNS requests from powershell should be easy enough to identify using an EDR. Using splunk and stats just look for multiple remo ...

[READ MORE](#)

 [Powered by Blogger](#)

Ce site utilise des cookies provenant de Google pour fournir ses services et analyser le trafic. Votre adresse IP et votre user-agent, ainsi que des statistiques relatives aux performances et à la sécurité, sont transmis à Google afin d'assurer un service de qualité, de générer des statistiques d'utilisation, et de détecter et de résoudre les problèmes d'abus.

[EN SAVOIR PLUS](#) [OK !](#)