


<div><div><div><div></div></div><div><div>HYBRID ANALYSIS</div></div></div><div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div></div></div><div><div>Request Info</div></div></div><div><div></div></div></div> <div><div></div></div>	
Suspicious Indicators3	
Anti-Detection/Stealthyness	
Contains ability to use cryptographic services (API string)	
Environment Awareness	
Found a reference to a WMI query string known to be used for VM detection	
External Systems	
Sample was identified as malicious by at least one Antivirus engine	
Informative30	
Anti-Reverse Engineering	
Creates guarded memory regions (anti-debugging trick to avoid memory dumping)	
Cryptographic Related	
Contains ability to decode base64 data (API string)	
Environment Awareness	
Calls an API typically used to get product type	
Calls an API typically used to get system version information	
Contains ability to read software policies	
Reads the active computer name	
Reads the cryptographic machine GUID	
Reads the windows installation date	
General	
Calls an API typically used to create a directory	
Creates mutants	
Loads the .NET runtime environment	
Overview of unique CLSIDs touched in registry	
Reads configuration files	
Installation/Persistence	
Dropped files	
Touches files in the Windows directory	
Network Related	

À PROPOS DES COOKIES SUR CE SITE


En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)


Hybrid Analysis



Tip: Click an analysed process below to view more details.

Analysed 1 process in total.

 [powershell.exe](#) "-file" "C:\powersploit.ps1" (PID: 3664)

 Logged Script Calls	 Logged Stdout	 Extracted Streams	 Memory Dumps
 Reduced Monitoring	 Network Activityy	 Network Error	 Multiscan Match

Network Analysis

DNS Requests

No relevant DNS requests were made.

Contacted Hosts

No relevant hosts were contacted.

HTTP Traffic

No relevant HTTP requests were made.

Extracted Strings



Search

All Details:

Off

 Download All Memory Strings (4.3KiB)

- All Strings (481)

Interesting (312)

powershell.exe (1)

f2943f5e45befa52fb12748...
- powershell.exe:3664 (320)

screen_0.png (2)











screen_1.png (4)

"-file" "C:\powersploit.ps1"
#discover potential files containing passwords ; not complaining in case of denied access to a directory
#ensure that machine is domain joined and script is running as a domain account
#Some XML issues between versions
\$AesIV = New-Object Byte[](\$AesObject.IV.Length)
\$AesObject = New-Object System.Security.Cryptography.AesCryptoServiceProvider
\$AesObject.Key = \$AesKey
\$Base64Decoded = [Convert]::FromBase64String(\$Cpassword)
\$Changed += , \$Xml Select-Xml "/DataSources/DataSource/@changed" Select-Object -Expand Node ForEach-Object {\$_ .Value}
\$Changed += , \$Xml Select-Xml "/Drives/Drive/@changed" Select-Object -Expand Node ForEach-Object {\$_ .Value}
\$Cpassword = \$AesObject.Decrypt(\$Base64Decoded, \$AesObject.Key, [Cryptography.CryptoKeyFlags]::Default, [Cryptography.CryptoKeyUsage]::Decrypt)

Extracted Files

À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)

 HYBRID ANALYSIS	 ▾  ▾   ▾  Request Info ▾	<input type="text" value=""/>	 ▾
Size	7.0 KiB (6912 bytes)		
Type	data		
Runtime Process	powershell.exe (PID: 3664)		
MD5	c11f2e76f895be8d35a468fe84d7fe9f 		
SHA1	7fc5b6a02e36b2215fd87b90a7201f9eb58fd7a1 		
SHA256	c2feff9708b7b6fa86d88bd5b4f8e5618fe88143e74ffa2b96a5a0ab20727216 		

Notifications

Runtime

▼

Environment

1

Sample was not shared with the community

Community

ⓘ There are no community comments.

ⓘ You must be logged in to submit a comment.



À PROPOS DES COOKIES SUR CE SITE

En cliquant sur « Accepter tous les cookies », vous consentez au stockage de cookies sur votre appareil afin de nous permettre d'améliorer la navigation du site, d'analyser l'utilisation du site et d'optimiser nos initiatives marketing. [Politique d'utilisation des cookies](#)