

Doc_78916.doc

malicious

This report is generated from a file or URL submitted to this webservice on November 21st 2017 23:32:58 (UTC)

Guest System: Windows 7 32 bit, Home Premium, 6.1 (build 7601), Service Pack 1

Report generated by Falcon Sandbox © Hybrid Analysis

Threat Score: 100/100

AV Detection: 70%

Labeled as: CVE-2017-11882

#exploit

- Overview

Sample not shared

Downloads

External Reports

Re-analyze

Hash Not Seen Before

No similar samples

Report False-Positive

Request Report Deletion

Post

Link

E-Mail

Incident Response

Risk Assessment

Remote Access

Stealer/Phishing

Persistence

Fingerprint

Exploit

Network Behavior

Reads terminal service related keys (often RDP related)

Scans for artifacts that may help identify the target

Writes data to a remote process

Reads the active computer name

Reads the cryptographic machine GUID

Scans for artifacts that may help identify the target

Possible Equation Editor exploit detected

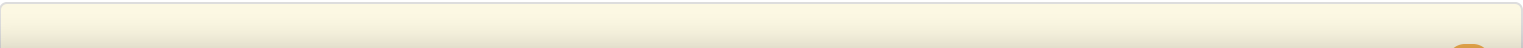
Contacts 1 domain and 1 host.

View all details

Indicators

Not all malicious and suspicious indicators are displayed. Get your own cloud service or the full version to view all details.

Malicious Indicators	5
Exploit/Shellcode	
Possible Equation Editor exploit detected	▼
Possible document exploit detected	▼
External Systems	
Sample was identified as malicious by at least one Antivirus engine	▼
Installation/Persistence	
Writes data to a remote process	▼
Unusual Characteristics	
Document analysis contacts a domain	▼



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

Paramètres des cookies

Tout refuser

Autoriser tous les cookies























Incident Response

Indicators

- Malicious (5)
- Suspicious (11)
- Informative (17)

- File Details
- Screenshots (error)
- Hybrid Analysis (3)
- Network Analysis
- Extracted Strings
- Extracted Files (7)
- Notifications
- Community (0)

Back to top

 HYBRID ANALYSIS				<div><input type="text" value="Search"/> </div>	
Reads the active computer name					
Reads the cryptographic machine GUID					
Exploit/Shellcode					
Spawns the Microsoft Equation Editor					
General					
Opened the service control manager					
Requested access to a system service					
Installation/Persistence					
Creates new processes					
Remote Access Related					
Reads terminal service related keys (often RDP related)					
Spyware/Information Retrieval					
Scans for artifacts that may help identify the target					
System Security					
Modifies proxy settings					
Queries sensitive IE security settings					
Informative				<div>17</div>	
Environment Awareness					
Reads the registry for installed applications					
Exploit/Shellcode					
Reads the Equation Editor Class Identifier (CLSID)					
General					
Contacts domains					
Contacts server					
Creates mutants					
Loads rich edit control libraries					
Process launched with changed environment					
Scanning for window names					
Spawns new processes					
Installation/Persistence					



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](#)

Network Analysis


DNS Requests

Login to Download DNS Requests (CSV)

Domain	Address	Registrar	Country
zstorage.biz	185.82.23.166	-	 Germany
<div> OSINT</div>			

Contacted Hosts

Login to Download Contacted Hosts (CSV)

IP Address	Port/Protocol	Associated Process	Details
185.82.23.166	443	mshta.exe	 Germany
<div> OSINT</div>	TCP	PID: 3816	

Contacted Countries



HTTP Traffic

No relevant HTTP requests were made.

Extracted Strings

Q

Search

All Details:

Off

⬇️ Download All Memory Strings (3.5KiB)


- All Strings (296)
- Interesting (40)
- WINWORD.EXE:3612 (218)
- screen_10.png (18)
- EQNEDT32.EXE (1)
- WINWORD.EXE (1)
- EQNEDT32.EXE:3692 (32)
- screen_5.png (20)
- screen_0.png (3)
- mshta.exe (1)
- network.pcap (1)
- PCAP (1)


%PROGRAMFILES%\Microsoft Office\Office14\wwlib.dll


,-s,,nchr,n,,u,


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











Runtime Process

WINWORD.EXE (PID: 3612)


MD5



24786575ca3d77879197ec144b3f0ac0 


SHA1


1125db2ac442a618478a2a1a769109b353b301af 


SHA256

fef673f9c1668b14a71103a7f9276e63fcfa5abfe374e4632baf604b3b9d0169 

 ~WRS{CDE0E101-8412-4BDE-8891-68D11819709D}.tmp 

 Overview

 User Did Not Share

 Hash Seen Before

Size

1KiB (1024 bytes)

Type

unknown


Description

FoxPro FPT, blocks size 0, next free block index 218103808, 1st used item "\375"


Runtime Process

WINWORD.EXE (PID: 3612)


MD5



5d4d94ee7e06bbb0af9584119797b23a 

SHA1

dbb111419c704f116efa8e72471dd83e86e49677 

SHA256

4826c0d860af884d3343ca6460b0006a7a2ce7dbccc4d743208585d997cc5fd1 

 ~\$4ae284c76f868fc51d3bb65da8caa6efacb707f265b25c30f34250b76b7507.doc 

Notifications

Runtime	▼
Environment	2
Sample was not shared with the community	
Static analysis (binary/memory) was disabled for this run	

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](#)