

3337937-107-0_1.Free_Hosting.doc

malicious

This report is generated from a file or URL submitted to this webservice on July 27th 2019 06:04:47 (UTC) and action script *Heavy Anti-Evasion*

Threat Score: 100/100

AV Detection: 41%

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


Labeled as: CVE-2015-1641

#exploit

Report generated by Falcon Sandbox © Hybrid Analysis

- Overview
- Sample unavailable
- Downloads
- External Reports
- Re-analyze
- Hash Seen Before
- No similar samples
- Report False-Positive
- Request Report Deletion
- Post
- Link
- E-Mail

Incident Response

 Risk Assessment

Spyware

POSTs files to a webserver

Persistence

Modifies System Certificates Settings

Modifies auto-execute functionality by setting/creating a value in the registry

Spawns a lot of processes


Evasive

Possibly tries to evade analysis by sleeping many times

Network Behavior

Contacts 6 domains and 6 hosts.


View all details

 MITRE ATT&CK™ Techniques Detection

This report has 14 indicators that were mapped to 13 attack techniques and 7 tactics.

View all details

Additional Context

 OSINT

External References

https://community.rsa.com/community/products/netwitness/blog/2017/07/10/active-monsoon-apt-campaign-on-7-6-2017

External User Tags

#apt #badnews #malware #monsoon #rsa #rtf

Indicators

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

Malicious Indicators

15

External Systems

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

Page 1 of 11

<div><div>HYBRID ANALYSIS</div><div><div>▼</div><div>▼</div><div></div><div>▼</div><div><div>Request Info</div>▼</div></div></div> <div><div><div>Q</div><div>×</div><div>▼</div></div></div>		
	Contains ability to start/interact with device drivers	▼
	GETs files from a webserver	▼
	The analysis extracted a file that was identified as malicious	▼
	Network Related	
	Found more than one unique User-Agent	▼
	Malicious artifacts seen in the context of a contacted host	▼
	Multiple malicious artifacts seen in the context of different hosts	▼
	Pattern Matching	
	YARA signature match	▼
	System Security	
	Modifies System Certificates Settings	▼
	Unusual Characteristics	
	Checks for a resource fork (ADS) file	▼
	Document analysis contacts a domain	▼
	Possible document exploit detected	▼
	Spawns a lot of processes	▼
	Hiding 1 Malicious Indicators	
	All indicators are available only in the private webservice or standalone version	
	Suspicious Indicators	12
	Environment Awareness	
	Contains ability to query CPU information	▼
	Possibly tries to evade analysis by sleeping many times	▼
	External Systems	
	Found an IP/URL artifact that was identified as malicious by at least one reputation engine	▼
	General	
	POSTs files to a webserver	▼
	Installation/Persistence	
	Modifies auto-execute functionality by setting/creating a value in the registry	▼
	Writes data to a remote process	▼
	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](#)

 <div><div>▼</div><div>▼</div><div></div><div>▼</div><div><div>Request Info</div>▼</div></div> <div><div></div><div><div></div>▼</div></div>	
Modifies proxy settings	▼
Hiding 3 Suspicious Indicators	
All indicators are available only in the private webservice or standalone version	
Informative	23
Anti-Reverse Engineering	
Creates guarded memory regions (anti-debugging trick to avoid memory dumping)	▼
Environment Awareness	
Contains ability to query volume size	▼
Makes a code branch decision directly after an API that is environment aware	▼
Possibly tries to detect the presence of a debugger	▼
General	
Contacts domains	▼
Contacts server	▼
Contains PDB pathways	▼
Creates a writable file in a temporary directory	▼
Creates mutants	▼
Drops files marked as clean	▼
Loads rich edit control libraries	▼
Process launched with changed environment	▼
Removes Office resiliency keys (often used to avoid problems opening documents)	▼
Runs shell commands	▼
Scanning for window names	▼
Spawns new processes	▼
Installation/Persistence	
Creates new processes	▼
Dropped files	▼
Drops executable files	▼
Touches files in the Windows directory	▼
Network Related	
Found potential URL in binary/memory	▼



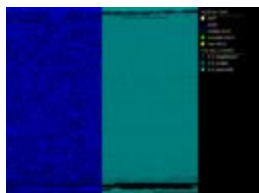
À PROPOS DES COOKIES SUR CE SITE

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](#)

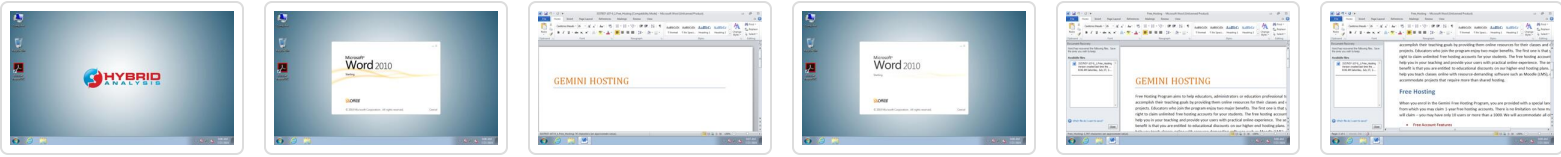
Installs hooks/patches the running process

File Details

All Details: Off

<div> <div></div> <div>3337937-107-0_1.Free_Hosting.doc</div> </div>	
Filename	3337937-107-0_1.Free_Hosting.doc
Size	947KiB (969917 bytes)
Type	<div>rtf</div>
Description	Rich Text Format data, version 1, unknown character set
Architecture	WINDOWS
SHA256	5567408950b744c4e846ba8ae726883cb15268a539f3bb21758a466e47021ae8 
Resources	
Icon	
Visualization	
Input File (PortEx)	
Classification (TrID)	
<ul style="list-style-type: none"> 100.0% (.RTF) Rich Text Format 	

Screenshots

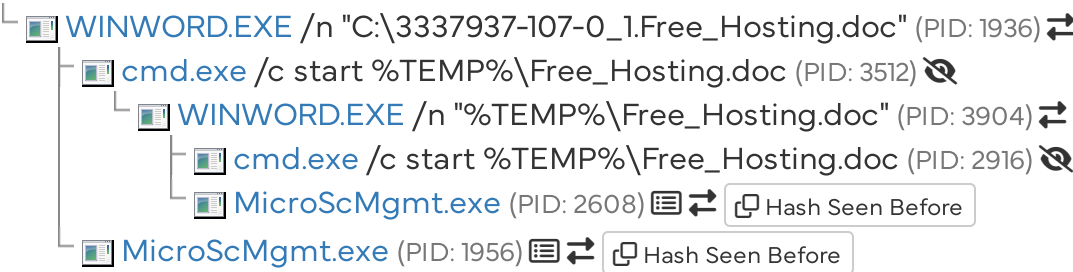


⌵ Show more

Hybrid Analysis

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









Analysed 6 processes in total.



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










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](#)

Domain	Address	Registrar	Country
en.wikipedia.org 	208.80.153.224 TTL: 230	MarkMonitor Inc. Organization: Wikimedia Foundation, Inc. Name Server: NS0.WIKIMEDIA.ORG Creation Date: Sat, 13 Jan 2001 00:12:14 GMT	 United States
feed43.com 	66.228.47.94 TTL: 5142	GANDI SAS Name Server: NS1.FEED43.COM Creation Date: Mon, 09 Jan 2006 00:00:00 GMT	 United States
isrg.trustid.ocsp.identrust.com 	23.63.75.176 TTL: 15	-	 United States
node2.feed43.com 	45.33.66.85 TTL: 1302	GANDI SAS Name Server: NS1.FEED43.COM Creation Date: Mon, 09 Jan 2006 00:00:00 GMT	 United States

Contacted Hosts

Login to Download Contacted Hosts (CSV)

IP Address	Port/Protocol	Associated Process	Details
162.255.116.10 	80 TCP	winword.exe PID: 1936 winword.exe PID: 3904	 United States
208.80.153.224 	443 TCP	microscmgmt.exe PID: 1956 microscmgmt.exe PID: 2608	 United States
66.228.47.94 	80 TCP	microscmgmt.exe PID: 1956 microscmgmt.exe PID: 2608	 United States
45.33.66.85  	443 TCP	microscmgmt.exe PID: 1956 microscmgmt.exe PID: 2608	 United States


Contacted Countries








LIMITED TRAFFIC

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

162.255.116.10:80 (www.samanthavisser.com)	OPTIONS	www.samanthavisser.com/images/	OPTIONS /images/ HTTP/1.1 User-Agent: Microsoft Office Protocol Discovery Host: www.samanthavisser.com Content-Length: 0 Connection: Keep-Alive <input type="button" value="More Details"/>
162.255.116.10:80 (www.samanthavisser.com)	GET	www.samanthavisser.com/images/	GET /images/ HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; ms-office; MSOffice 14) Accept-Encoding: gzip, d

Extracted Strings

All Details: ☐

 Download All Memory Strings (11KiB)

- All Strings (3514) Interesting (1377) ~WRO0002.doc (2592) msvcrt.dll.65387744 (195)

Free_Hosting.doc (105) MicroScMgmt.exe:1956 (2...) WINWORD.EXE:1936 (48) ~WRO0001.doc (62)

screen_5.png (38) screen_9.png (35) screen_0.png (3) jli.dll.4246765277 (167) PCAP (16)

cmd.exe (1) WINWORD.EXE (2) SSL (3) ~WRS_867A8168-76C3-4... WINWORD.EXE:3904 (3)

!" k.M]C(f2o
!'a}b]ctlQ&nGN9f=^0bN_C;=:b/8WA,eq0uzJ4Y ie][[%.olm
!/dh`=u<"+Z:rb44@2upLo^GCu
!5M~\))@=e1T\$Lgt\$^^E)*,
!=#3sTdx=%j@fZ;\PS"LH^F^=8=M8dHx2h!K<ramq2;+kK9/}tt6'lm.B#2Cy2sX#/=
!@:LA=zAPVp{T
!Cn5I9`Uo\c?1X1 ap\$XS?.0_S?M1 lou#^I3IO)/VZJz~t0[!`au1 >p'mcJ?
!cyT:uCkP0t@\qb8FL\$}Kup~A2*b@nww?MaWyZ>gt-r?
!F<J#9.SF3W'yJ'JV=../R9n
!f`_y57_a(k/":
!FV:,y[qa%B@f4A[P<Bvs7b:?

Extracted Files

 Displaying 32 extracted file(s). The remaining **188** file(s) are available in the full version and XML/JSON reports.

Malicious

5

jli.dll

Overview

Download Disabled

Extended File Details

VirusTotal Report

Metadefender Report

Extracted Streams

Hash Seen Before

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](#)

<div><div><div><div></div><div>HYBRID ANALYSIS</div></div><div><div></div><div></div><div></div><div></div><div></div></div><div>Request Info</div></div></div> <div><div>Q</div><div>×</div><div></div></div>	
<div><div>SHA256</div><div>d0c2dc9a14eba6cc692dce33e3e725459f6045331395bddb992c85a00ec19894</div><div></div></div>	
<div><div><div><div></div><div>~WRO0000.doc</div></div><div><div>Download Disabled</div><div>VirusTotal Report</div><div>Metadefender Report</div><div>Hash Not Seen Before</div></div><div><div>Size</div><div>414KiB (424446 bytes)</div></div><div><div>Type</div><div>docx</div><div>office</div></div><div><div>Description</div><div>Microsoft OOXML</div></div><div><div>AV Scan Result</div><div>Labeled as "HEUR:Exploit.MSOffice" (3/69)</div></div><div><div>Runtime Process</div><div>WINWORD.EXE (PID: 1936)</div></div><div><div>MD5</div><div>7f6dea6a7fdfe9cf49c53b468f42340d</div><div></div></div><div><div>SHA1</div><div>712067796c0a7b2b0cf9b497a1f47a0fc9beeb4bc</div><div></div></div><div><div>SHA256</div><div>e11d1be96e717b2bb098ee2ac45895d08383cb912939c702c38c1966b6805fb6</div><div></div></div></div></div>	
<div><div><div><div></div><div>~WRO0001.doc</div></div><div><div>Download Disabled</div><div>VirusTotal Report</div><div>Hash Seen Before</div></div><div><div>Size</div><div>9.6KiB (9850 bytes)</div></div><div><div>Type</div><div>docx</div><div>office</div></div><div><div>Description</div><div>Microsoft OOXML</div></div><div><div>AV Scan Result</div><div>Labeled as "CVE-2015-1641" (17/59)</div></div><div><div>Runtime Process</div><div>WINWORD.EXE (PID: 1936)</div></div><div><div>MD5</div><div>3844d888663d5dca4f277aa5786fccbf</div><div></div></div><div><div>SHA1</div><div>de367e0d9d0616ec3cd3309545f64877312f07b8</div><div></div></div><div><div>SHA256</div><div>185e6d6935be099573da18e1958d203d31e39cc5af6a23f8a72a9b912d40bf82</div><div></div></div></div></div>	
<div><div><div><div></div><div>~WRO0003.doc</div></div><div><div>Download Disabled</div><div>VirusTotal Report</div><div>Hash Seen Before</div></div><div><div>Size</div><div>9.6KiB (9850 bytes)</div></div><div><div>Type</div><div>docx</div><div>office</div></div><div><div>Description</div><div>Microsoft OOXML</div></div><div><div>AV Scan Result</div><div>Labeled as "CVE-2015-1641" (17/59)</div></div><div><div>MD5</div><div>3844d888663d5dca4f277aa5786fccbf</div><div></div></div><div><div>SHA1</div><div>de367e0d9d0616ec3cd3309545f64877312f07b8</div><div></div></div><div><div>SHA256</div><div>185e6d6935be099573da18e1958d203d31e39cc5af6a23f8a72a9b912d40bf82</div><div></div></div></div></div>	
<div><div><div><div></div><div>~WRO0002.doc</div></div><div><div>Download Disabled</div><div>VirusTotal Report</div><div>Metadefender Report</div><div>Hash Not Seen Before</div></div><div><div>Size</div><div>414KiB (424446 bytes)</div></div><div><div>Type</div><div>docx</div><div>office</div></div><div><div>Description</div><div>Microsoft OOXML</div></div><div><div>AV Scan Result</div><div>Labeled as "HEUR:Exploit.MSOffice" (3/69)</div></div><div><div>MD5</div><div>7f6dea6a7fdfe9cf49c53b468f42340d</div><div></div></div><div><div>SHA1</div><div>712067796c0a7b2b0cf9b497a1f47a0fc9beeb4bc</div><div></div></div><div><div>SHA256</div><div>e11d1be96e717b2bb098ee2ac45895d08383cb912939c702c38c1966b6805fb6</div><div></div></div></div></div>	
<div><div>Clean</div><div>5</div></div>	
<div><div><div><div></div><div>MicroScMgmt.exe</div></div><div><div>Overview</div><div>Download Disabled</div><div>Extended File Details</div><div>VirusTotal Report</div><div>Metadefender Report</div></div></div></div>	

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

Free_Hosting.doc

Download Disabled

VirusTotal Report

Hash Not Seen Before

Size

16KiB (16867 bytes)

Type

docxoffice

Description

Microsoft Word 2007+

AV Scan Result

0/60

Runtime Process

WINWORD.EXE (PID: 1936)

MD5

f464d72fda0fdc9ad38799b3a6cb0eb1

SHA1

84404b542f0aa81f781ffb42f71d154d0d866d02

SHA256

7b93ae8cff39f4d7a3a45e2d0225ffe2461ce05c5flc90368af3df01bf5ab384

~_37937-107-0_1.Free_Hosting.doc

Overview

Download Disabled

VirusTotal Report

Hash Seen Before

Size

162B (162 bytes)

Type

data

AV Scan Result

0/54

MD5

b60c0bb79b4b53294d99905c973caba3

SHA1

a7716d014025ca03b5324c8220e2459eea70b6b1

SHA256

a101d3605f8d1ca5cfb10c48dbdb24c45f2627c48f44a2bd2604b88c7b90d5f0

~_RO0000.doc

Overview

Download Disabled

VirusTotal Report

Hash Seen Before

Size

162B (162 bytes)

Type

data

AV Scan Result

0/54

MD5

b60c0bb79b4b53294d99905c973caba3

SHA1

a7716d014025ca03b5324c8220e2459eea70b6b1

SHA256

a101d3605f8d1ca5cfb10c48dbdb24c45f2627c48f44a2bd2604b88c7b90d5f0

~_RO0001.doc

Overview

Download Disabled

VirusTotal Report

Hash Seen Before

Size

162B (162 bytes)

Type

data

AV Scan Result

0/54

MD5

b60c0bb79b4b53294d99905c973caba3

SHA1

a7716d014025ca03b5324c8220e2459eea70b6b1

SHA256

a101d3605f8d1ca5cfb10c48dbdb24c45f2627c48f44a2bd2604b88c7b90d5f0































Informative

22

3337937-107-0_1.Free_Hosting.LNK

























msvcrt.dll

FSF-CTBL.FSF

<div><div>HYBRID ANALYSIS</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></div></div>	
<div><div>10D19A55.wmf</div><div><div>Download Disabled</div><div>Hash Seen Before</div></div><div><div><div><div>Size</div><div>664B (664 bytes)</div></div><div><div>Runtime Process</div><div>WINWORD.EXE (PID: 1936)</div></div><div><div>MD5</div><div>656ddbdc2244cea646b2ca50edf5a7a6 </div></div><div><div>SHA1</div><div>5becebd9bbbd2cd6a339cb54171ec8727c44fadb </div></div><div><div>SHA256</div><div>9d5a1b9b2c0645000b91eb6ee7d2791f30afed5a6d2f8924cdd7a54ad1309ff9 </div></div></div></div></div>	
<div><div>10D19A55.wmf</div><div><div>Download Disabled</div><div>Hash Seen Before</div></div><div><div><div><div>Size</div><div>664B (664 bytes)</div></div><div><div>Runtime Process</div><div>WINWORD.EXE (PID: 1936)</div></div><div><div>MD5</div><div>656ddbdc2244cea646b2ca50edf5a7a6 </div></div><div><div>SHA1</div><div>5becebd9bbbd2cd6a339cb54171ec8727c44fadb </div></div><div><div>SHA256</div><div>9d5a1b9b2c0645000b91eb6ee7d2791f30afed5a6d2f8924cdd7a54ad1309ff9 </div></div></div></div></div>	
<div><div>11AF455D.wmf</div><div><div>Download Disabled</div><div>Hash Seen Before</div></div><div><div><div><div>Size</div><div>98B (98 bytes)</div></div><div><div>Runtime Process</div><div>WINWORD.EXE (PID: 1936)</div></div><div><div>MD5</div><div>ec196f924ec35b76e7560d9781a1e031 </div></div><div><div>SHA1</div><div>b7f3ba8641a38748b4631495f5a76f645a101fcf </div></div><div><div>SHA256</div><div>8afc5b7183e5ac47628640bc7fa7b0ea24addf493a760089ef68cfcee16bc257 </div></div></div></div></div>	
<div><div>134AF136.wmf</div><div><div>Download Disabled</div><div>Hash Seen Before</div></div><div><div><div><div>Size</div><div>664B (664 bytes)</div></div><div><div>Runtime Process</div><div>WINWORD.EXE (PID: 1936)</div></div><div><div>MD5</div><div>656ddbdc2244cea646b2ca50edf5a7a6 </div></div><div><div>SHA1</div><div>5becebd9bbbd2cd6a339cb54171ec8727c44fadb </div></div><div><div>SHA256</div><div>9d5a1b9b2c0645000b91eb6ee7d2791f30afed5a6d2f8924cdd7a54ad1309ff9 </div></div></div></div></div>	
<div><div>13F4B9A9.wmf</div><div><div>Download Disabled</div><div>Hash Seen Before</div></div><div><div><div><div>Size</div><div>664B (664 bytes)</div></div><div><div>Runtime Process</div><div>WINWORD.EXE (PID: 1936)</div></div><div><div>MD5</div><div>656ddbdc2244cea646b2ca50edf5a7a6 </div></div><div><div>SHA1</div><div>5becebd9bbbd2cd6a339cb54171ec8727c44fadb </div></div><div><div>SHA256</div><div>9d5a1b9b2c0645000b91eb6ee7d2791f30afed5a6d2f8924cdd7a54ad1309ff9 </div></div></div></div></div>	
<div><div>1AABE251.wmf</div><div><div>Download Disabled</div><div>Hash Seen Before</div></div><div><div><div><div>Size</div><div>664B (664 bytes)</div></div><div><div>Runtime Process</div><div>WINWORD.EXE (PID: 1936)</div></div><div><div>MD5</div><div>656ddbdc2244cea646b2ca50edf5a7a6 </div></div><div><div>SHA1</div><div>5becebd9bbbd2cd6a339cb54171ec8727c44fadb </div></div><div><div>SHA256</div><div>9d5a1b9b2c0645000b91eb6ee7d2791f30afed5a6d2f8924cdd7a54ad1309ff9 </div></div></div></div></div>	
<div><div>1CF68E4D.wmf</div><div><div>Download Disabled</div><div>Hash Seen Before</div></div></div>	

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](#)

<div><div>HYBRID ANALYSIS</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><div></div></div><div>Q</div><div>×</div></div><div>▼</div></div></div>	
<div><div><div><div><div></div><div>210A790.wmf</div></div><div><div><div><div>Download Disabled</div><div>Hash Seen Before</div></div></div></div></div><div><div><div><div>Size</div><div>664B (664 bytes)</div></div><div><div>Runtime Process</div><div>WINWORD.EXE (PID: 1936)</div></div><div><div>MD5</div><div>656ddbdc2244cea646b2ca50edf5a7a6 </div></div><div><div>SHA1</div><div>5becebd9bbbd2cd6a339cb54171ec8727c44fadb </div></div><div><div>SHA256</div><div>9d5a1b9b2c0645000b91eb6ee7d2791f30afed5a6d2f8924cdd7a54ad1309ff9 </div></div></div></div></div></div>	<div><div>⤴</div></div>
<div><div><div><div><div></div><div>299AE512.wmf</div></div><div><div><div><div>Download Disabled</div><div>Hash Seen Before</div></div></div></div></div><div><div><div><div>Size</div><div>664B (664 bytes)</div></div><div><div>Runtime Process</div><div>WINWORD.EXE (PID: 1936)</div></div><div><div>MD5</div><div>656ddbdc2244cea646b2ca50edf5a7a6 </div></div><div><div>SHA1</div><div>5becebd9bbbd2cd6a339cb54171ec8727c44fadb </div></div><div><div>SHA256</div><div>9d5a1b9b2c0645000b91eb6ee7d2791f30afed5a6d2f8924cdd7a54ad1309ff9 </div></div></div></div></div></div>	<div><div>⤴</div></div>
<div><div><div><div><div></div><div>299EE987.wmf</div></div><div><div><div><div>Download Disabled</div><div>Hash Seen Before</div></div></div></div></div><div><div><div><div>Size</div><div>664B (664 bytes)</div></div><div><div>Runtime Process</div><div>WINWORD.EXE (PID: 1936)</div></div><div><div>MD5</div><div>656ddbdc2244cea646b2ca50edf5a7a6 </div></div><div><div>SHA1</div><div>5becebd9bbbd2cd6a339cb54171ec8727c44fadb </div></div><div><div>SHA256</div><div>9d5a1b9b2c0645000b91eb6ee7d2791f30afed5a6d2f8924cdd7a54ad1309ff9 </div></div></div></div></div></div>	<div><div>⤴</div></div>
<div><div><div><div><div></div><div>29EFC861.wmf</div></div><div><div><div><div>Download Disabled</div><div>Hash Seen Before</div></div></div></div></div><div><div><div><div>Size</div><div>664B (664 bytes)</div></div><div><div>Type</div><div>unknown</div></div><div><div>Description</div><div>ms-windows metafont .wmf</div></div><div><div>Runtime Process</div><div>WINWORD.EXE (PID: 1936)</div></div><div><div>MD5</div><div>656ddbdc2244cea646b2ca50edf5a7a6 </div></div><div><div>SHA1</div><div>5becebd9bbbd2cd6a339cb54171ec8727c44fadb </div></div><div><div>SHA256</div><div>9d5a1b9b2c0645000b91eb6ee7d2791f30afed5a6d2f8924cdd7a54ad1309ff9 </div></div></div></div></div></div>	<div><div>⤴</div></div>
<div><div><div><div><div></div><div>2A0B4B2.wmf</div></div><div><div><div><div>Download Disabled</div><div>Hash Seen Before</div></div></div></div></div><div><div><div><div>Size</div><div>664B (664 bytes)</div></div><div><div>Runtime Process</div><div>WINWORD.EXE (PID: 1936)</div></div><div><div>MD5</div><div>656ddbdc2244cea646b2ca50edf5a7a6 </div></div><div><div>SHA1</div><div>5becebd9bbbd2cd6a339cb54171ec8727c44fadb </div></div><div><div>SHA256</div><div>9d5a1b9b2c0645000b91eb6ee7d2791f30afed5a6d2f8924cdd7a54ad1309ff9 </div></div></div></div></div></div>	<div><div>⤴</div></div>
<div><div><div><div><div></div><div>2C811738.wmf</div></div><div><div><div><div>Download Disabled</div><div>Hash Seen Before</div></div></div></div></div><div><div><div><div>Size</div><div>664B (664 bytes)</div></div><div><div>Runtime Process</div><div>WINWORD.EXE (PID: 1936)</div></div><div><div>MD5</div><div>656ddbdc2244cea646b2ca50edf5a7a6 </div></div></div></div></div></div>	<div><div>⤴</div></div>

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](#)

<div>HYBRID ANALYSIS</div>		<div>Request Info</div>		<div>Q</div>	
<div>Size</div>		<div>104B (104 bytes)</div>			
<div>Type</div>		<div>unknown</div>			
<div>Description</div>		<div>ms-windows metafont .wmf</div>			
<div>Runtime Process</div>		<div>WINWORD.EXE (PID: 1936)</div>			
<div>MD5</div>		<div>656ddbdc2244cea646b2ca50edf5a7a6</div>		<div></div>	
<div>SHA1</div>		<div>5becebd9bbbd2cd6a339cb54171ec8727c44fadb</div>		<div></div>	
<div>SHA256</div>		<div>9d5a1b9b2c0645000b91eb6ee7d2791f30afed5a6d2f8924cdd7a54ad1309ff9</div>		<div></div>	
<div>~_RO0002.doc</div>				<div></div>	
<div>~_ee_Hosting.doc</div>				<div></div>	
<div>Download Disabled</div>		<div>Hash Seen Before</div>			
<div>Size</div>		<div>162B (162 bytes)</div>			
<div>Type</div>		<div>data</div>			
<div>MD5</div>		<div>f50a36c26cc8687a3780d7780d985d9a</div>		<div></div>	
<div>SHA1</div>		<div>5c4eacc552fc3714ab99610002ae8cb4ece0c0d1</div>		<div></div>	
<div>SHA256</div>		<div>39055d9cc2f8a2ef2c1b9120ae896e3d5bd3d137898eddbbb638b19eac1090f8</div>		<div></div>	
<div>~_RO0003.doc</div>				<div></div>	
<div>~_Normal.dotm</div>				<div></div>	
<div>Overview</div>		<div>Download Disabled</div>		<div>Hash Seen Before</div>	
<div>Size</div>		<div>162B (162 bytes)</div>			
<div>MD5</div>		<div>b60c0bb79b4b53294d99905c973caba3</div>		<div></div>	
<div>SHA1</div>		<div>a7716d014025ca03b5324c8220e2459eea70b6b1</div>		<div></div>	
<div>SHA256</div>		<div>a101d3605f8d1ca5cfb10c48dbdb24c45f2627c48f44a2bd2604b88c7b90d5f0</div>		<div></div>	

Notifications

Runtime	
---------	--

Community

There are no community comments.
You must be logged in to submit a comment.