

ID: 585264
Sample Name:
RIP_YOUR_PC_LOL.exe
Cookbook: default.jbs
Time: 17:59:22
Date: 08/03/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report RIP_YOUR_PC_LOL.exe 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Process Tree 5
Malware Configuration 6
Yara Signatures 6
Initial Sample 6
PCAP (Network Traffic) 7
Dropped Files 7
Memory Dumps 7
Unpacked PEs 8
Sigma Signatures 8
AV Detection 8
E-Banking Fraud 8
System Summary 8
Stealing of Sensitive Information 8
Remote Access Functionality 8
Joe Sandbox Signatures 8
AV Detection 8
Networking 9
Key, Mouse, Clipboard, Microphone and Screen Capturing 9
E-Banking Fraud 9
Operating System Destruction 9
System Summary 9
Data Obfuscation 9
Boot Survival 9
Hooking and other Techniques for Hiding and Protection 9
Malware Analysis System Evasion 9
HIPS / PFW / Operating System Protection Evasion 10
Lowering of HIPS / PFW / Operating System Security Settings 10
Stealing of Sensitive Information 10
Remote Access Functionality 10
Mitre Att&ck Matrix 10
Behavior Graph 11
Screenshots 12
Thumbnails 12
Antivirus, Machine Learning and Genetic Malware Detection 13
Initial Sample 13
Dropped Files 13
Unpacked PE Files 15
Domains 17
URLs 17
Domains and IPs 19
Contacted Domains 19
Contacted URLs 19
URLs from Memory and Binaries 19
World Map of Contacted IPs 29
Public IPs 29
General Information 29
Warnings 30
Simulations 30
Behavior and APIs 30
Joe Sandbox View / Context 31
IPs 31
Domains 31
ASNs 31
JA3 Fingerprints 31
Dropped Files 31
Created / dropped Files 31
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe 31
C:\ProgramData\kaosdma.txt 32
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RIP_YOUR_PC_LOL.exe.log 32
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\aaa.exe.log 32
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\gay.exe.log 32
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\healastounding.exe.log 33
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\5JOCE52U.txt 33
C:\Users\user\AppData\Local\Temp\Dcvxaamev.exe 33
C:\Users\user\AppData\Local\Temp\FFDvbcrdfqs.exe 34
C:\Users\user\AppData\Local\Temp\tmp4896.tmp 34
C:\Users\user\AppData\Local\Temp\tmp5D87.tmp 34

Copyright Joe Security LLC 2022

C:\Users\user\AppData\Roaming\0fd7de5367376231a788872005d7ed4f.exe 35
C:\Users\user\AppData\Roaming\22.exe 35
C:\Users\user\AppData\Roaming\3.exe 36
C:\Users\user\AppData\Roaming\4.exe 36
C:\Users\user\AppData\Roaming\8f1c8b40c7be588389a8d382040b23bb.exe 36
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat 37
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat 37
C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\21c8026919fd094ab07ec3c180a9f210_d06ed635-68f6-4e9a-955c-4899f5f57b9a 37
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a797c6ca3f5e7aff8fa1149c47fe9466.exe 38
C:\Users\user\AppData\Roaming\Opus.exe 38
C:\Users\user\AppData\Roaming\Pluto Panel.exe 38
C:\Users\user\AppData\Roaming___11.19.exe 39
C:\Users\user\AppData\Roaming\a.exe 39
C:\Users\user\AppData\Roaming\aaa.exe 40
C:\Users\user\AppData\Roaming\gay.exe 40
C:\Users\user\AppData\Roaming\healastounding.exe 40
C:\Users\user\AppData\Roaming\mediaget.exe 41
C:\Users\user\AppData\Roaming\test.exe 41
C:\Windows\Cursors\WUDFhosts.exe 42
C:\Windows\Help\Winlogon.exe 42
C:\Windows\Help\active_desktop_render.dll 42
Static File Info 43
General 43
File Icon 43
Static PE Info 43
General 43
Entrypoint Preview 43
Data Directories 45
Sections 46
Resources 46
Imports 46
Version Infos 46
Network Behavior 46
Snort IDS Alerts 46
Network Port Distribution 47
TCP Packets 47
UDP Packets 48
DNS Queries 50
DNS Answers 51
HTTP Request Dependency Graph 53
HTTP Packets 53
Statistics 54
Behavior 54
System Behavior 54
Analysis Process: RIP_YOUR_PC_LOL.exePID: 6880, Parent PID: 408 54
General 54
File Activities 55
File Created 55
File Written 56
File Read 58
Analysis Process: healastounding.exePID: 3572, Parent PID: 6880 59
General 59
File Activities 61
File Created 61
File Written 61
File Read 65
Analysis Process: Pluto Panel.exePID: 4236, Parent PID: 6880 65
General 65
File Activities 66
File Created 66
File Read 67
Analysis Process: test.exePID: 6236, Parent PID: 3572 67
General 67
File Activities 68
File Created 68
File Read 68
Analysis Process: 0fd7de5367376231a788872005d7ed4f.exePID: 2024, Parent PID: 6880 68
General 68
Analysis Process: gay.exePID: 1104, Parent PID: 3572 69
General 69
File Activities 69
File Created 69
File Written 70
File Read 70
Registry Activities 70
Key Value Created 70
Key Value Modified 70
Analysis Process: Opus.exePID: 3244, Parent PID: 3572 71
General 71
File Activities 72
File Created 72
File Deleted 73
File Written 73
File Read 75
Registry Activities 75
Key Value Created 75
Analysis Process: 22.exePID: 1272, Parent PID: 6880 75
General 75
Analysis Process: aaa.exePID: 3984, Parent PID: 3572 76

General 76
Analysis Process: 8f1c8b40c7be588389a8d382040b23bb.exePID: 5376, Parent PID: 3572 76
General 76
Analysis Process: 0fd7de5367376231a788872005d7ed4f.exePID: 5172, Parent PID: 2024 77
General 77
Analysis Process: 4.exePID: 2824, Parent PID: 3572 77
General 77
Analysis Process: mediaget.exePID: 4688, Parent PID: 1104 77
General 77
Disassembly 78

Copyright Joe Security LLC 2022

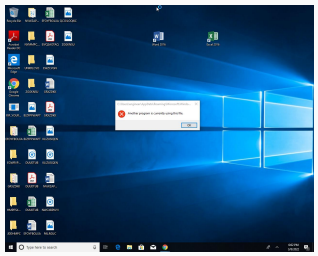
Windows Analysis Report

RIP_YOUR_PC_LOL.exe

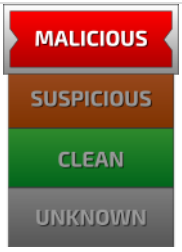
Overview

General Information

Sample Name:	RIP_YOUR_PC_LOL.exe
Analysis ID:	585264
MD5:	52867174362410.
SHA1:	7ae4e1048e4463.
SHA256:	37d8e1ce3b6e64..
Tags:	exe
Infos:	



Detection



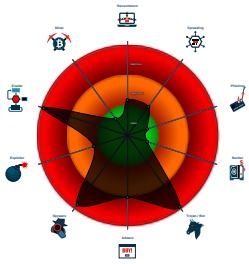
HawkEye Nanocore njRat AsyncRAT Azorult DCRat Ficker Stealer

Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected RedLine Stealer
- Yara detected MailPassView
- Yara detected HawkEye Keylogger
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Yara detected Azorult Info Stealer
- Detected Nanocore Rat
- Yara detected AsyncRAT
- Antivirus detection for dropped file
- Sigma detected: Suspect Svchost A…
- Yara detected Nanocore RAT
- Yara detected DCRat

Classification



Process Tree

- **System is w10x64**
- RIP_YOUR_PC_LOL.exe (PID: 6880 cmdline: "C:\Users\user\Desktop\RIP_YOUR_PC_LOL.exe" MD5: 52867174362410D63215D78E708103EA)
  - healastounding.exe (PID: 3572 cmdline: "C:\Users\user\AppData\Roaming\healastounding.exe" MD5: 6FB798F1090448CE26299C2B35ACF876)
    - test.exe (PID: 6236 cmdline: "C:\Users\user\AppData\Roaming\test.exe" MD5: 7E50B2929829321901792 45C60C0B59B)
    - gay.exe (PID: 1104 cmdline: "C:\Users\user\AppData\Roaming\gay.exe" MD5: 8EEDC01C11B251481DEC59E5308DCCC3)
      - mediaget.exe (PID: 4688 cmdline: "C:\Users\user\AppData\Roaming\mediaget.exe" MD5: 8EEDC01C11B251481DEC59E5308DCCC3)
        - netsh.exe (PID: 7092 cmdline: netsh firewall add allowedprogram "C:\Users\user\AppData\Roaming\mediaget.exe" "mediaget.exe" ENABLE MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
          - conhost.exe (PID: 4104 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - Opus.exe (PID: 3244 cmdline: "C:\Users\user\AppData\Roaming\Opus.exe" MD5: 759185EE3724D7563B709C888C696959)
      - schtasks.exe (PID: 6420 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp4896.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 3280 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 7052 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" / xml "C:\Users\user\AppData\Local\Temp\tmp5D87.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 4564 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - aaa.exe (PID: 3984 cmdline: "C:\Users\user\AppData\Roaming\aaa.exe" MD5: 860AA57FC3578F7037BB27FC79B2A62C)
      - aaa.exe (PID: 6256 cmdline: C:\Users\user\AppData\Roaming\aaa.exe MD5: 860AA57FC3578F7037BB27FC79B2A62C)
    - 8f1c8b40c7be588389a8d382040b23bb.exe (PID: 5376 cmdline: "C:\Users\user\AppData\Roaming\8f1c8b40c7be588389a8d382040b23bb.exe" MD5: 8F1C8B40C7BE588389A8D382040B23BB)
      - FFDvbcrdfqs.exe (PID: 6920 cmdline: "C:\Users\user\AppData\Local\Temp\FFDvbcrdfqs.exe" MD5: 78D40B12FFC837843FBF4DE2164002F6)
      - Dcvxaamev.exe (PID: 6612 cmdline: "C:\Users\user\AppData\Local\Temp\Dcvxaamev.exe" MD5: 870D6E5AEF6DEA98CED388CCE87BFBD4)
    - 4.exe (PID: 2824 cmdline: "C:\Users\user\AppData\Roaming\4.exe" MD5: E6DACE3F577AC7A6F9747B4A0956C8D7)
      - 3.exe (PID: 3964 cmdline: "C:\Users\user\AppData\Roaming\3.exe" MD5: 748A4BEA8C0624A4C7A69F67263E0839)
    - a.exe (PID: 5152 cmdline: "C:\Users\user\AppData\Roaming\a.exe" MD5: 52CFD35F337CA837D31DF0A95CE2A55E)
  - Pluto Panel.exe (PID: 4236 cmdline: "C:\Users\user\AppData\Roaming\Pluto Panel.exe" MD5: ED666BF7F4A0766FCEC0E9C8074B089B)
  - 0fd7de5367376231a788872005d7ed4f.exe (PID: 2024 cmdline: "C:\Users\user\AppData\Roaming\0fd7de5367376231a788872005d7ed4f.exe" MD5: 0FD7DE5367376231A788872005D7ED4F)
    - 0fd7de5367376231a788872005d7ed4f.exe (PID: 5172 cmdline: "C:\Users\user\AppData\Roaming\0fd7de5367376231a788872005d7ed4f.exe" MD5: 0FD7DE5367376231A788872005D7ED4F)
  - 22.exe (PID: 1272 cmdline: "C:\Users\user\AppData\Roaming\22.exe" MD5: DBF9DAA1707B1037E28A6E0694B33A4B)
    - netsh.exe (PID: 6500 cmdline: netsh ipsec static add policy name=Block MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
      - conhost.exe (PID: 3252 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - netsh.exe (PID: 6596 cmdline: netsh ipsec static add filterlist name=Filter1 MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
      - conhost.exe (PID: 7048 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - netsh.exe (PID: 5932 cmdline: netsh ipsec static add filter filterlist=Filter1 srcaddr=any dstaddr=Me dstport=135 protocol=TCP MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
      - conhost.exe (PID: 3288 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

Copyright Joe Security LLC 2022

- netsh.exe (PID: 5940 cmdline: netsh ipsec static add filter filterlist=Filter1 srcaddr=any dstaddr=Me dstport=135 protocol=UDP MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
  - conhost.exe (PID: 1616 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- netsh.exe (PID: 5748 cmdline: netsh ipsec static add filter filterlist=Filter1 srcaddr=any dstaddr=Me dstport=139 protocol=TCP MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
  - conhost.exe (PID: 6212 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- netsh.exe (PID: 5504 cmdline: netsh ipsec static add filter filterlist=Filter1 srcaddr=any dstaddr=Me dstport=139 protocol=UDP MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
  - conhost.exe (PID: 5584 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- netsh.exe (PID: 6060 cmdline: netsh ipsec static add filter filterlist=Filter1 srcaddr=any dstaddr=Me dstport=445 protocol=TCP MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
  - conhost.exe (PID: 6252 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- ___11.19.exe (PID: 6732 cmdline: "C:\Users\user\AppData\Roaming___11.19.exe" MD5: A071727B72A8374FF79A695ECDE32594)
  - svchost.exe (PID: 6552 cmdline: C:\Users\user\AppData\Local\Temp\\svchost.exe MD5: A4329177954D4104005BCE3020E5EF59)
    - cmd.exe (PID: 1852 cmdline: C:\Windows\system32\cmd.exe /c ping -n 2 127.0.0.1 > nul && del C:\Users\user\AppData\Local\Temp\svchost.exe > nul MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 1364 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - svchos.exe (PID: 1588 cmdline: C:\Users\user\AppData\Local\Temp\\svchos.exe MD5: 3B377AD877A942EC9F60EA285F7119A2)
  - HD____11.19.exe (PID: 2508 cmdline: C:\Users\user\AppData\Roaming\HD____11.19.exe MD5: B14120B6701D42147208EBF264AD9981)
- Opus.exe (PID: 6580 cmdline: C:\Users\user\AppData\Roaming\Opus.exe 0 MD5: 759185EE3724D7563B709C888C696959)
- dhcpmon.exe (PID: 6328 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 759185EE3724D7563B709C888C696959)
- dhcpmon.exe (PID: 6308 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: 759185EE3724D7563B709C888C696959)
- mediaget.exe (PID: 6036 cmdline: "C:\Users\user\AppData\Roaming\mediaget.exe" .. MD5: 8EEDC01C11B251481DEC59E5308DCCC3)
- mediaget.exe (PID: 1080 cmdline: "C:\Users\user\AppData\Roaming\mediaget.exe" .. MD5: 8EEDC01C11B251481DEC59E5308DCCC3)
- TXPlatform.exe (PID: 5700 cmdline: C:\Windows\SysWOW64\TXPlatform.exe -auto MD5: A4329177954D4104005BCE3020E5EF59)
  - TXPlatform.exe (PID: 1480 cmdline: C:\Windows\SysWOW64\TXPlatform.exe -acsi MD5: A4329177954D4104005BCE3020E5EF59)
- svchost.exe (PID: 6268 cmdline: C:\Windows\SysWOW64\svchost.exe -k " " MD5: FA6C268A5B5BDA067A901764D203D433)
- svchost.exe (PID: 6052 cmdline: C:\Windows\SysWOW64\svchost.exe -k " " MD5: FA6C268A5B5BDA067A901764D203D433)
- mediaget.exe (PID: 5644 cmdline: "C:\Users\user\AppData\Roaming\mediaget.exe" .. MD5: 8EEDC01C11B251481DEC59E5308DCCC3)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
RIP_YOUR_PC_LOL.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1308075:$x1: NanoCore.ClientPluginHost • 0x13080b2:$x2: IClientNetworkHost • 0x130bbe5:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
RIP_YOUR_PC_LOL.exe	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7bdb7:$key: HawkEyeKeylogger • 0x7dff3:$salt: 099u787978786 • 0x7c3f0:$string1: HawkEye_Keylogger • 0x7d243:$string1: HawkEye_Keylogger • 0x7df53:$string1: HawkEye_Keylogger • 0x7c7d9:$string2: holdermail.txt • 0x7c7f9:$string2: holdermail.txt • 0x7c71b:$string3: wallet.dat • 0x7c733:$string3: wallet.dat • 0x7c749:$string3: wallet.dat • 0x7db35:$string4: Keylog Records • 0x7de4d:$string4: Keylog Records • 0x7e04b:$string5: do not script --> • 0x7bd9f:$string6: \pidloc.txt • 0x7be05:$string7: BSPLIT • 0x7be15:$string7: BSPLIT
RIP_YOUR_PC_LOL.exe	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x7901:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
RIP_YOUR_PC_LOL.exe	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
RIP_YOUR_PC_LOL.exe	JoeSecurity_GenericDropper	Yara detected Generic Dropper	Joe Security	

Click to see the 12 entries

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Roaming\gay.exe	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
C:\Users\user\AppData\Roaming\gay.exe	MALWARE_Win_NjRAT	Detects NjRAT / Bladabindi	ditekSHen	• 0x81fc:$s1: netsh firewall delete allowedprogram • 0x80f2:$s2: netsh firewall add allowedprogram • 0x825c:$s3: 63 00 6D 00 64 00 2E 00 65 00 78 00 65 00 20 00 2F 00 6B 00 20 00 70 00 69 00 6E 00 67 • 0x7ee6:$s4: Execute ERROR • 0x7f46:$s4: Execute ERROR • 0x7f0a:$s5: Download ERROR • 0x82a2:$s6: [kl]
C:\Users\user\AppData\Roaming\gay.exe	njrat1	Identify njRat	Brian Wallace @botnet_hunter	• 0x80f2:$a1: netsh firewall add allowedprogram • 0x82ec:$b1: [TAP] • 0x8292:$b2: & exit • 0x825e:$c1: md.exe /k ping 0 & del
C:\Users\user\AppData\Roaming\Opus.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
C:\Users\user\AppData\Roaming\Opus.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
Click to see the 35 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000000.414257385.0000000000842000.00000002.00000001.01000000.0000000A.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000009.00000000.414257385.0000000000842000.00000002.00000001.01000000.0000000A.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000009.00000000.414257385.0000000000842000.00000002.00000001.01000000.0000000A.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000006.00000000.397644420.0000000000DA2000.00000002.00000001.01000000.00000007.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
00000006.00000000.397644420.0000000000DA2000.00000002.00000001.01000000.00000007.sdmp	INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse	Detects file containing reversed ASEP Autorun registry keys	ditekSHen	• 0x97f3:$s1: nuR\noisreVtnerruC\swodniW\tfosorciM
Click to see the 237 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.RIP_YOUR_PC_LOL.exe.206ac1d.13.raw.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
0.0.RIP_YOUR_PC_LOL.exe.206ac1d.13.raw.unpack	INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse	Detects file containing reversed ASEP Autorun registry keys	ditekSHen	• 0x99f3:$s1: nuR\noisreVtnerruC\swodniW\tfosorciM
0.2.RIP_YOUR_PC_LOL.exe.d4dd52.5.raw.unpack	MALWARE_Win_BlackMoon	Detects executables using BlackMoon RunTime	ditekSHen	• 0x4e6a:$s1: blackmoon • 0x4eaa:$s2: BlackMoon RunTime Error:
0.3.RIP_YOUR_PC_LOL.exe.5a556c1.5.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
0.3.RIP_YOUR_PC_LOL.exe.5a556c1.5.unpack	INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse	Detects file containing reversed ASEP Autorun registry keys	ditekSHen	• 0x7bf3:$s1: nuR\noisreVtnerruC\swodniW\tfosorciM
Click to see the 661 entries				

Sigma Signatures

AV Detection



Sigma detected: NanoCore

E-Banking Fraud



Sigma detected: NanoCore

System Summary



Sigma detected: Suspect Svchost Activity

Sigma detected: Suspicius Schtasks From Env Var Folder

Sigma detected: System File Execution Location Anomaly

Sigma detected: Suspicious Svchost Process

Sigma detected: File Created with System Process Name

Sigma detected: Suspicious Add Scheduled Task From User AppData Temp

Stealing of Sensitive Information



Sigma detected: NanoCore

Remote Access Functionality



Sigma detected: NanoCore

Joe Sandbox Signatures

AV Detection



Antivirus detection for dropped file

Yara detected Nanocore RAT

Multi AV Scanner detection for submitted file

Yara detected Njrat

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking



Performs DNS queries to domains with low reputation

May check the online IP address of the machine

Uses dynamic DNS services

Key, Mouse, Clipboard, Microphone and Screen Capturing



Yara detected HawkEye Keylogger

Yara detected AsyncRAT

Contains functionality to log keystrokes (.Net Source)

E-Banking Fraud



Yara detected Nanocore RAT

Yara detected Njrat

Operating System Destruction



Protects its processes via BreakOnTermination flag

System Summary



Malicious sample detected (through community Yara rule)

PE file has nameless sections

Data Obfuscation



.NET source code contains potential unpacker

Boot Survival



Yara detected AsyncRAT

Drops PE files to the startup folder

Creates autostart registry keys with suspicious names

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

Hooking and other Techniques for Hiding and Protection



Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion



Yara detected AntiVM3

Yara detected AsyncRAT

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

Copyright Joe Security LLC 2022

HIPS / PFW / Operating System Protection Evasion



Injects a PE file into a foreign processes

Sample uses process hollowing technique

.NET source code references suspicious native API functions

Lowering of HIPS / PFW / Operating System Security Settings



Yara detected AsyncRAT

Uses netsh to modify the Windows network and firewall settings

Modifies the windows firewall

Stealing of Sensitive Information



Yara detected RedLine Stealer

Yara detected MailPassView

Yara detected HawkEye Keylogger

Yara detected Azorult Info Stealer

Yara detected Nanocore RAT

Yara detected DCRat

Yara detected Generic Dropper

Yara detected Azorult

Yara detected Njrat

Yara detected Mimikatz

Yara detected Ficker Stealer

Yara detected WebBrowserPassView password recovery tool

Remote Access Functionality



Yara detected RedLine Stealer

Yara detected HawkEye Keylogger

Detected Nanocore Rat

Yara detected Nanocore RAT

Yara detected DCRat

Detected njRat

Yara detected Njrat

Detected HawkEye Rat

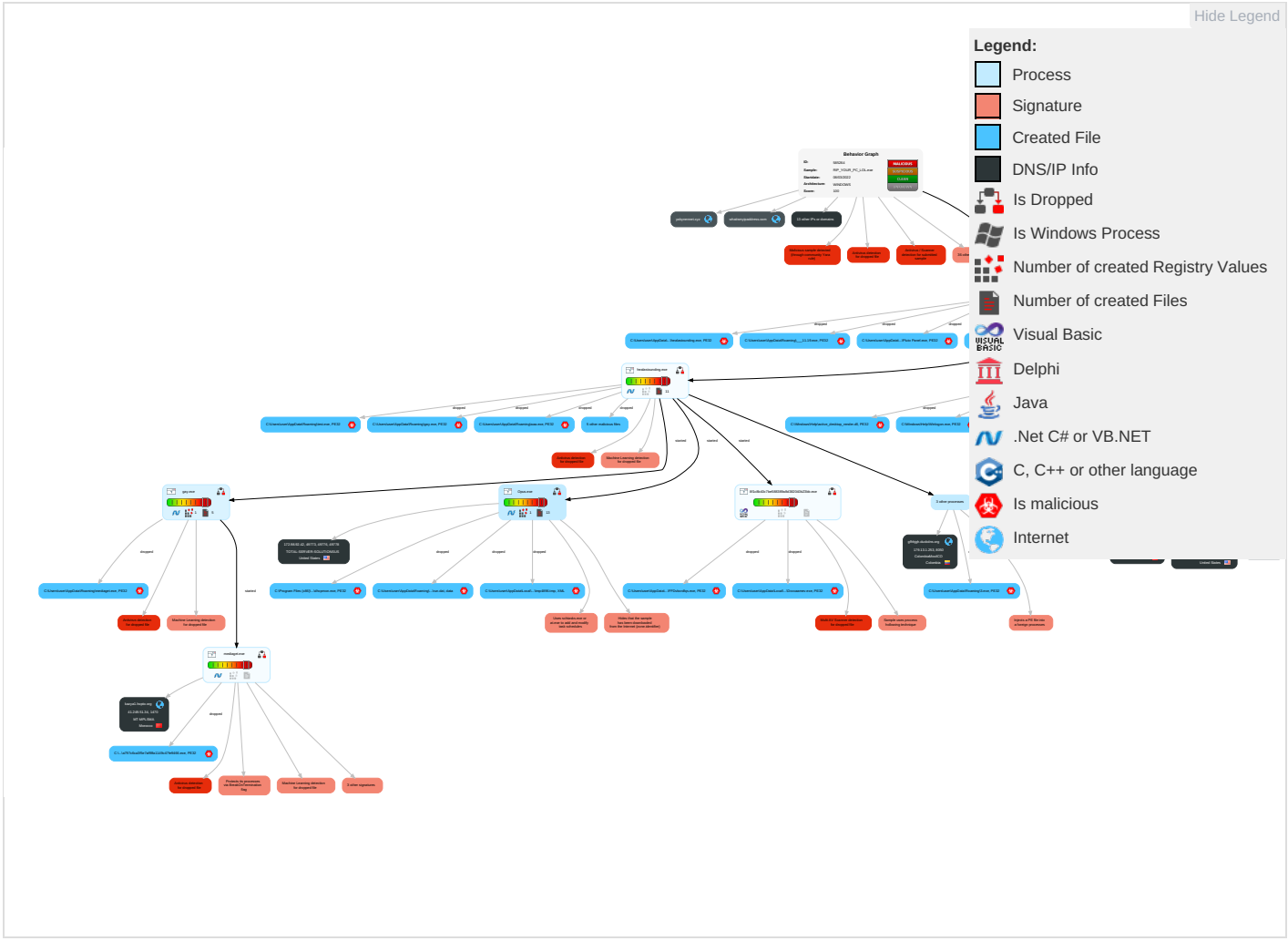
Yara detected Ficker Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Replication Through Removable Media	1 2 Native API	1 DLL Side-Loading	1 DLL Side-Loading	2 1 Disable or Modify Tools	1 2 1 Input Capture	1 System Time Discovery	1 Replication Through Removable Media	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Shared Modules	2 Windows Service	2 Windows Service	1 1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Peripheral Device Discovery	Remote Desktop Protocol	1 2 1 Input Capture	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	2 Scheduled Task/Job	2 Scheduled Task/Job	2 1 2 Process Injection	1 4 1 Obfuscated Files or Information	Security Account Manager	1 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	2 2 1 Registry Run Keys / Startup Folder	2 Scheduled Task/Job	1 5 Software Packing	NTDS	1 4 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Remote Access Software	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	2 2 1 Registry Run Keys / Startup Folder	1 Timestomp	LSA Secrets	1 Query Registry	SSH	Keylogging	Data Transfer Size Limits	2 Non-Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 DLL Side-Loading	Cached Domain Credentials	2 2 1 Security Software Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	1 1 2 Application Layer Protocol	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 2 Masquerading	DCSync	2 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 1 Virtualization/Sandbox Evasion	Proc Filesystem	2 1 Virtualization/Sandbox Evasion	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	2 1 2 Process Injection	/etc/passwd and /etc/shadow	1 Remote System Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Hidden Files and Directories	Network Sniffing	1 System Network Configuration Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

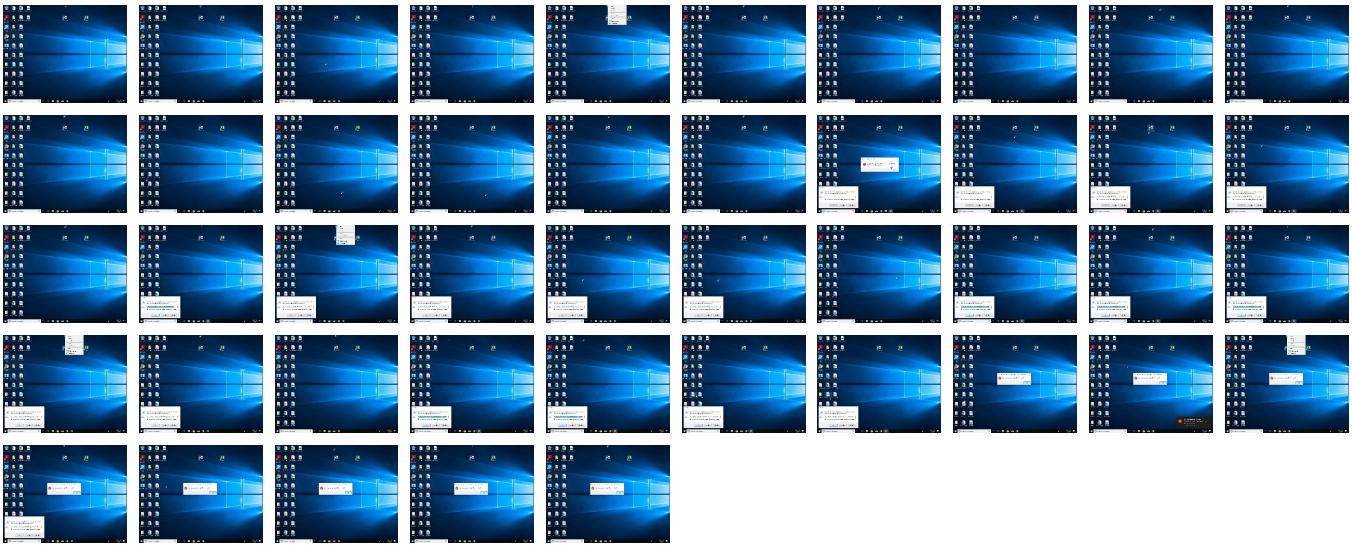
Behavior Graph



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
RIP_YOUR_PC_LOL.exe	63%	Virustotal		Browse
RIP_YOUR_PC_LOL.exe	33%	Metadefender		Browse
RIP_YOUR_PC_LOL.exe	74%	ReversingLabs	ByteCode-MSIL.Trojan.Remcos	
RIP_YOUR_PC_LOL.exe	100%	Avira	TR/AD.MExecute.lzrac	
RIP_YOUR_PC_LOL.exe	100%	Avira	SPR/Tool.MailPassView.473	
RIP_YOUR_PC_LOL.exe	100%	Avira	TR/AD.MalwareCrypter.rrsdk	
RIP_YOUR_PC_LOL.exe	100%	Avira	TR/Dropper.GR	
RIP_YOUR_PC_LOL.exe	100%	Avira	TR/Agent.aagt	
RIP_YOUR_PC_LOL.exe	100%	Avira	TR/AD.RedLineStеal.cjshc	
RIP_YOUR_PC_LOL.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
RIP_YOUR_PC_LOL.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\FFDvbcrdfqs.exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Roaming\Opus.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
C:\Users\user\AppData\Roaming\mediaget.exe	100%	Avira	TR/ATRAPS.Gen	
C:\Users\user\AppData\Roaming___11.19.exe	100%	Avira	TR/Dropper.GR	
C:\Users\user\AppData\Roaming___11.19.exe	100%	Avira	TR/Agent.aagt	
C:\Users\user\AppData\Roaming\healastounding.exe	100%	Avira	TR/AD.RedLineStealcjshc	
C:\Users\user\AppData\Roaming\healastounding.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
C:\Users\user\AppData\Roaming\0fd7de5367376231a788872005d7ed4f.exe	100%	Avira	TR/AD.MalwareCrypter.rrsdk	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
C:\Windows\Help\active_desktop_render.dll	100%	Avira	HEUR/AGEN.1245024	
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a797c6ca3f5e7aff8fa1149c47fe9466.exe	100%	Avira	TR/ATRAPS.Gen	
C:\Users\user\AppData\Roaming\gay.exe	100%	Avira	TR/ATRAPS.Gen	
C:\Users\user\AppData\Local\Temp\Dcvxaamev.exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Roaming\8f1c8b40c7be588389a8d382040b23bb.exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Roaming\22.exe	100%	Avira	HEUR/AGEN.1227810	
C:\Users\user\AppData\Roaming\Pluto Panel.exe	100%	Avira	TR/AD.MExecute.lzrac	
C:\Users\user\AppData\Roaming\Pluto Panel.exe	100%	Avira	SPR/Tool.MailPassView.473	
C:\Windows\Cursors\WUDFhosts.exe	100%	Avira	HEUR/AGEN.1213003	
C:\Users\user\AppData\Roaming\a.exe	100%	Avira	TR/AD.RedLineStealcjshc	
C:\Users\user\AppData\Roaming\3.exe	100%	Avira	HEUR/AGEN.1203070	
C:\Users\user\AppData\Roaming\test.exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Roaming\aaa.exe	100%	Avira	TR/Dropper.MSIL.Gen	
C:\Users\user\AppData\Local\Temp\FFDvbcrdfqs.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Opus.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\mediaget.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming___11.19.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\healastounding.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\4.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\0fd7de5367376231a788872005d7ed4f.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Windows\Help\active_desktop_render.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a797c6ca3f5e7aff8fa1149c47fe9466.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\gay.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Dcvxaamev.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\8f1c8b40c7be588389a8d382040b23bb.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\22.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Pluto Panel.exe	100%	Joe Sandbox ML		
C:\Windows\Cursors\WUDFhosts.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\a.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\3.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\test.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\aaa.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	85%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
C:\Users\user\AppData\Local\Temp\Dcvxaamev.exe	29%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\Dcvxaamev.exe	86%	ReversingLabs	Win32.Trojan.Fragtor	
C:\Users\user\AppData\Local\Temp\FFDvbcrdfqs.exe	29%	Metadefender		Browse

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\FFDvbcrdfqs.exe	86%	ReversingLabs	Win32.Infostealer.Azorult	
C:\Users\user\AppData\Roaming\0fd7de5367376231a788872005d7ed4f.exe	29%	Metadefender		Browse
C:\Users\user\AppData\Roaming\0fd7de5367376231a788872005d7ed4f.exe	92%	ReversingLabs	Win32.Ransomware.StopCrypt	
C:\Users\user\AppData\Roaming\22.exe	38%	Metadefender		Browse
C:\Users\user\AppData\Roaming\22.exe	86%	ReversingLabs	Win32.Trojan.BlackMoon	
C:\Users\user\AppData\Roaming\3.exe	47%	Metadefender		Browse
C:\Users\user\AppData\Roaming\3.exe	82%	ReversingLabs	ByteCode-MSIL.Trojan.SpyNoon	
C:\Users\user\AppData\Roaming\4.exe	17%	Metadefender		Browse
C:\Users\user\AppData\Roaming\4.exe	75%	ReversingLabs	Win32.Trojan.SpyNoon	
C:\Users\user\AppData\Roaming\8f1c8b40c7be588389a8d382040b23bb.exe	26%	Metadefender		Browse
C:\Users\user\AppData\Roaming\8f1c8b40c7be588389a8d382040b23bb.exe	86%	ReversingLabs	Win32.Infostealer.Azorult	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.0.22.exe.400000.12.unpack	100%	Avira	HEUR/AGEN.1227810		Download File
9.2.Opus.exe.840000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.0.8f1c8b40c7be588389a8d382040b23bb.exe.476f20.4.unpack	100%	Avira	TR/Dropper.Gen		Download File
7.0.0fd7de5367376231a788872005d7ed4f.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1242347		Download File
4.0.healastounding.exe.900000.4.unpack	100%	Avira	TR/AD.RedLineSteal.cjshc		Download File
4.0.healastounding.exe.900000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.Pluto Panel.exe.f10000.8.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
5.0.Pluto Panel.exe.f10000.8.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
9.0.Opus.exe.840000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.2.Pluto Panel.exe.f10000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
5.2.Pluto Panel.exe.f10000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
14.0.8f1c8b40c7be588389a8d382040b23bb.exe.4bdf52.2.unpack	100%	Avira	TR/Dropper.Gen		Download File
12.2.aaa.exe.2c0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
8.0.gay.exe.d0000.2.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
12.0.aaa.exe.2c0000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
0.3.RIP_YOUR_PC_LOL.exe.57b3478.6.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.0.0fd7de5367376231a788872005d7ed4f.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1242347		Download File
11.0.22.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1227810		Download File
0.2.RIP_YOUR_PC_LOL.exe.5755c99.18.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
11.0.22.exe.457136.14.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
0.1.RIP_YOUR_PC_LOL.exe.9f22de.1.unpack	100%	Avira	TR/Inject.vcoldi		Download File
14.0.8f1c8b40c7be588389a8d382040b23bb.exe.400000.3.unpack	100%	Avira	TR/Dropper.Gen		Download File
6.2.test.exe.da0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
8.2.gay.exe.d0000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
12.0.aaa.exe.2c0000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
4.2.healastounding.exe.900000.0.unpack	100%	Avira	TR/AD.RedLineSteal.cjshc		Download File

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link	Download
4.2.healastounding.exe.900000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.0.8f1c8b40c7be588389a8d382040b23bb.exe.476f20.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
4.0.healastounding.exe.900000.0.unpack	100%	Avira	TR/AD.RedLineSteal.cjshc		Download File
4.0.healastounding.exe.900000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.0.8f1c8b40c7be588389a8d382040b23bb.exe.400000.6.unpack	100%	Avira	TR/Dropper.Gen		Download File
9.2.Opus.exe.5b00000.7.unpack	100%	Avira	TR/NanoCore.fadte		Download File
14.0.8f1c8b40c7be588389a8d382040b23bb.exe.4bdf52.5.unpack	100%	Avira	TR/Dropper.Gen		Download File
11.0.22.exe.457136.21.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
0.1.RIP_YOUR_PC_LOL.exe.dda1e2.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
14.0.8f1c8b40c7be588389a8d382040b23bb.exe.400000.9.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.2.RIP_YOUR_PC_LOL.exe.e387f7.8.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.0.22.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1227810		Download File
6.0.test.exe.da0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
17.0.mediaget.exe.ab0000.3.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
0.2.RIP_YOUR_PC_LOL.exe.d587a1.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
11.0.22.exe.43de6f.2.unpack	100%	Avira	HEUR/AGEN.1245024		Download File
17.0.mediaget.exe.ab0000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
11.0.22.exe.43de6f.19.unpack	100%	Avira	HEUR/AGEN.1245024		Download File
11.0.22.exe.457136.9.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
9.0.Opus.exe.840000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.22.exe.400000.18.unpack	100%	Avira	HEUR/AGEN.1227810		Download File
14.0.8f1c8b40c7be588389a8d382040b23bb.exe.4bdf52.8.unpack	100%	Avira	TR/Dropper.Gen		Download File
11.0.22.exe.43de6f.13.unpack	100%	Avira	HEUR/AGEN.1245024		Download File
14.0.8f1c8b40c7be588389a8d382040b23bb.exe.476f20.10.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.0.RIP_YOUR_PC_LOL.exe.9f22de.1.unpack	100%	Avira	TR/Inject.vcoldi		Download File
17.2.mediaget.exe.ab0000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
14.0.8f1c8b40c7be588389a8d382040b23bb.exe.476f20.7.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.3.RIP_YOUR_PC_LOL.exe.5839748.8.unpack	100%	Avira	HEUR/AGEN.1227785		Download File
9.0.Opus.exe.840000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.gay.exe.d0000.1.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
8.0.gay.exe.d0000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
11.0.22.exe.457136.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
0.0.RIP_YOUR_PC_LOL.exe.ea57bf.9.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.2.healastounding.exe.4582ffa.11.unpack	100%	Avira	TR/Dropper.Gen		Download File
11.0.22.exe.43de6f.7.unpack	100%	Avira	HEUR/AGEN.1245024		Download File
0.0.RIP_YOUR_PC_LOL.exe.e387f7.8.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.RIP_YOUR_PC_LOL.exe.dda1e2.7.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
12.0.aaa.exe.2c0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
0.2.RIP_YOUR_PC_LOL.exe.56d4258.19.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link	Download
17.0.mediaget.exe.ab0000.1.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
0.1.RIP_YOUR_PC_LOL.exe.d587a1.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
0.2.RIP_YOUR_PC_LOL.exe.dda1e2.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.0.healastounding.exe.900000.12.unpack	100%	Avira	TR/AD.RedLineSteal.cjshc		Download File
4.0.healastounding.exe.900000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.3.RIP_YOUR_PC_LOL.exe.5956fd2.3.unpack	100%	Avira	TR/Dropper.Gen		Download File
7.0.0fd7de5367376231a788872005d7ed4f.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1242347		Download File
6.0.test.exe.da0000.2.unpack	100%	Avira	TR/Dropper.Gen		Download File
5.0.Pluto Panel.exe.f10000.4.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
5.0.Pluto Panel.exe.f10000.4.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
0.0.RIP_YOUR_PC_LOL.exe.d587a1.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
5.0.Pluto Panel.exe.f10000.12.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
5.0.Pluto Panel.exe.f10000.12.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
5.0.Pluto Panel.exe.f10000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
5.0.Pluto Panel.exe.f10000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
6.0.test.exe.da0000.3.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.2.RIP_YOUR_PC_LOL.exe.5821276.21.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.1.RIP_YOUR_PC_LOL.exe.e387f7.7.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.0.RIP_YOUR_PC_LOL.exe.1f6c52e.15.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.2.RIP_YOUR_PC_LOL.exe.1f6c52e.15.unpack	100%	Avira	TR/Dropper.Gen		Download File
7.2.0fd7de5367376231a788872005d7ed4f.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1242347		Download File
12.0.aaa.exe.2c0000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
0.2.RIP_YOUR_PC_LOL.exe.9f22de.3.unpack	100%	Avira	TR/Inject.vcoldi		Download File
7.2.0fd7de5367376231a788872005d7ed4f.exe.24f15a0.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.0.8f1c8b40c7be588389a8d382040b23bb.exe.4bdf52.11.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.1.RIP_YOUR_PC_LOL.exe.ea57bf.8.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.0.8f1c8b40c7be588389a8d382040b23bb.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
4.2.healastounding.exe.44c50a8.8.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.2.RIP_YOUR_PC_LOL.exe.57b42ae.20.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.0.0fd7de5367376231a788872005d7ed4f.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1242347		Download File
17.0.mediaget.exe.ab0000.2.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
9.0.Opus.exe.840000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.gay.exe.d0000.3.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
4.0.healastounding.exe.900000.8.unpack	100%	Avira	TR/AD.RedLineSteal.cjshc		Download File
4.0.healastounding.exe.900000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.tiro.com=	0%	Avira URL Cloud	safe	
http://www.urwpp.derasg	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd&	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.sakkal.comm	0%	Avira URL Cloud	safe	
http://www.fontbureau.comlicd	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/)	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.tiro.com&	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://schemas.microsof	0%	URL Reputation	safe	
http://www.i.	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/X	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Q	0%	URL Reputation	safe	
http://www.carterandcone.comY	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cno.W	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/J	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnm	0%	URL Reputation	safe	
http://www.carterandcone.comt	0%	URL Reputation	safe	
http://www.founder.com.cn/cncz	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.zhongyicts.co	0%	Avira URL Cloud	safe	
http://www.fonts.comC	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/)	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/eu-e	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/n	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnY	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/i	0%	URL Reputation	safe	
http://www.fontbureau.comitu	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/g	0%	URL Reputation	safe	
http://www.freeeim.com/D	0%	Avira URL Cloud	safe	
http://www.tiro.comic	0%	URL Reputation	safe	
http://www.founder.com.cn/cncz$	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn$	0%	URL Reputation	safe	
http://www.carterandcone.comkC	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/ls	0%	Avira URL Cloud	safe	
http://www.fontbureau.comFX	0%	Avira URL Cloud	safe	
http://www.urwpp.deMTq	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/C	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/J	0%	URL Reputation	safe	
http://www.founder.com.cn/cnT	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnts	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.fontbureau.comoX	0%	Avira URL Cloud	safe	
http://www.carterandcone.com.	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnv	0%	URL Reputation	safe	
http://www.fontbureau.comrsiv	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.carterandcone.como.W	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/X	0%	URL Reputation	safe	
http://www.fontbureau.comonyn	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comsiv/C	0%	Avira URL Cloud	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://www.founder.com.cp	0%	Avira URL Cloud	safe	
http://www.urwpp.deR	0%	Avira URL Cloud	safe	
http://www.fontbureau.comtu	0%	Avira URL Cloud	safe	
http://https://whatismyipaddress.comx&	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kazya1.hopto.org	41.249.51.34	true	false		high
yabynennet.xyz	45.129.99.212	true	false		high
api.ipify.org.herokudns.com	52.20.78.240	true	false		high
whatismyipaddress.com	104.16.154.36	true	false		high
pool.usa-138.com	220.86.85.75	true	false		high
hackerinvasion.f3322.net	127.0.0.1	true	false		high
us-east-1.route-1000.000webhost.awex.io	145.14.144.149	true	false		high
gfhhjgh.duckdns.org	179.13.1.253	true	false		high
files.000webhost.com	unknown	unknown	false		high
22ssh.com	unknown	unknown	false		high
123.105.12.0.in-addr.arpa	unknown	unknown	false		high
store-images.s-microsoft.com	unknown	unknown	false		high
pretorian.ac.ug	unknown	unknown	false		high
api.ip.sb	unknown	unknown	false		high
api.ipify.org	unknown	unknown	false		high
prepepe.ac.ug	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://api.ipify.org/?format=xml	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.com=	Pluto Panel.exe, 00000005.00000003.44590 3668.0000000005C80000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.urwpp.derasg	Pluto Panel.exe, 00000005.00000003.49437 3371.0000000005C80000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.493190429.0000000005C 80000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.497114575.0000000005C80000.00000004.0 0000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comd&	Pluto Panel.exe, 00000005.00000003.53943 2667.0000000005C5C000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.561809650.0000000005C 54000.00000004.00000800.00020000.0000000 0.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers	Pluto Panel.exe, 00000005.00000002.71209 0794.0000000006EE2000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.sajatypeworks.com	Pluto Panel.exe, 00000005.00000002.71209 0794.0000000006EE2000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Pluto Panel.exe, 00000005.00000002.71209 0794.0000000006EE2000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.comm	Pluto Panel.exe, 00000005.00000003.46153 5327.0000000005C80000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.462539198.0000000005C 80000.00000004.00000800.00020000.0000000 0.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://dl.dropbox.com/s/p84aaz28t0hepul/Pass.exe?dl=0	healastounding.exe, healastounding.exe, 00000004.0 0000000.385235005.0000000000902000.00000 002.00000001.01000000.00000005.sdmp, hea lastounding.exe, 00000004.00000002.53835 6356.0000000003471000.00000004.00000800. 00020000.00000000.sdmp, gay.exe, gay.exe, 00000008.00000000.411478373.0000000000 0D2000.00000002.00000001.01000000.000000 09.sdmp, mediaget.exe, 00000011.00000000 .445953483.0000000000AB2000.00000002.000 00001.01000000.0000000F.sdmp, mediaget.exe, 00000011.00000003.646152049.00000000 01338000.00000004.00000020.00020000.0000 0000.sdmp	false		high
http://www.fontbureau.comlicd	Pluto Panel.exe, 00000005.00000003.62087 6949.0000000005C5A000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.645268957.0000000005C 5A000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.630356431.0000000005C5A000.00000004.0 0000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.585753311.0000000005C5A 000.00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.593605825 .0000000005C5A000.00000004.00000800.0002 0000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://whatismyipaddress.com/-	RIP_YOUR_PC_LOL.exe, 00000000.00000000.3 66341482.00000000009F2000.00000002.00000 001.01000000.00000003.sdmp, RIP_YOUR_PC_ LOL.exe, 00000000.00000003.437188672.000 00000056F5000.00000004.00000800.00020000 .00000000.sdmp, Pluto Panel.exe, 0000000 5.00000000.393171200.0000000000F12000.00 000002.00000001.01000000.00000006.sdmp	false		high
http://www.galapagosdesign.com/DPlease	Pluto Panel.exe, 00000005.00000002.71209 0794.0000000006EE2000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/)	Pluto Panel.exe, 00000005.00000003.44819 3641.0000000005C53000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.457715522.0000000005C 56000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.452001254.0000000005C5A000.00000004.0 0000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.457092303.0000000005C5A 000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html	Pluto Panel.exe, 00000005.00000003.46283 7238.0000000005C5B000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.463380932.0000000005C 5B000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.461983546.0000000005C5B000.00000004.0 0000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.460984251.0000000005C5B 000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.site.com/logs.php	Pluto Panel.exe, 00000005.00000002.70575 3147.0000000003691000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.tiro.com&	Pluto Panel.exe, 00000005.00000003.43448 5944.0000000005C7E000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.434712918.0000000005C 7F000.00000004.00000800.00020000.0000000 0.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	Pluto Panel.exe, 00000005.00000002.71209 0794.0000000006EE2000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://whatismyipaddress.com/	Pluto Panel.exe, Pluto Panel.exe, 00000005.0000000 2.705753147.0000000003691000.00000004.00 000800.00020000.00000000.sdmp	false		high
http://www.nirsoft.net/	Pluto Panel.exe, 00000005.00000000.39317 1200.0000000000F12000.00000002.00000001. 01000000.00000006.sdmp	false		high
http://www.zhongyicts.com.cn	Pluto Panel.exe, 00000005.00000003.43748 7558.0000000005C80000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.437239432.0000000005C 80000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.436798009.0000000005C80000.00000004.0 0000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.436695339.0000000005C80 000.00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.437023378 .0000000005C80000.00000004.00000800.0002 0000.00000000.sdmp, Pluto Panel.exe, 000 00005.00000002.712090794.0000000006EE200 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.microsof	healastounding.exe	false	• URL Reputation: safe	unknown
http://www.i.	Pluto Panel.exe, 00000005.00000003.42390 9901.0000000005C85000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.425696650.0000000005C 85000.00000004.00000800.00020000.0000000 0.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/X	Pluto Panel.exe, 00000005.00000003.44819 3641.0000000005C53000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.459485550.0000000005C 5A000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.460010944.0000000005C5A000.00000004.0 0000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.452001254.0000000005C5A 000.00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.461983546 .0000000005C5B000.00000004.00000800.0002 0000.00000000.sdmp, Pluto Panel.exe, 000 00005.00000003.460984251.0000000005C5B00 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Q	Pluto Panel.exe, 00000005.00000003.45948 5550.0000000005C5A000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.457715522.0000000005C 56000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.460010944.0000000005C5A000.00000004.0 0000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.452001254.0000000005C5A 000.00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.457092303 .0000000005C5A000.00000004.00000800.0002 0000.00000000.sdmp, Pluto Panel.exe, 000 00005.00000003.461983546.0000000005C5B00 0.00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.460984251.0 000000005C5B000.00000004.00000800.000200 00.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comY	Pluto Panel.exe, 00000005.00000003.44004 5453.0000000005C80000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.441297022.0000000005C 80000.00000004.00000800.00020000.0000000 0.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cno.W	Pluto Panel.exe, 00000005.00000003.43748 7558.0000000005C80000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.437239432.0000000005C 80000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.436798009.0000000005C80000.00000004.0 0000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.436695339.0000000005C80 000.00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.437773657 .0000000005C80000.00000004.00000800.0002 0000.00000000.sdmp, Pluto Panel.exe, 000 00005.00000003.437023378.0000000005C8000 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/J	Pluto Panel.exe, 00000005.00000003.44819 3641.0000000005C53000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cnm	Pluto Panel.exe, 00000005.00000003.43669 5339.0000000005C80000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comt	Pluto Panel.exe, 00000005.00000003.43702 3378.0000000005C80000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cncz	Pluto Panel.exe, 00000005.00000003.43190 8494.0000000005C5B000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.symauth.com/cps0(	RIP_YOUR_PC_LOL.exe, 00000000.00000000.3 66341482.00000000009F2000.00000002.00000 001.01000000.00000003.sdmp, RIP_YOUR_PC_ LOL.exe, 00000000.00000003.437188672.000 00000056F5000.00000004.00000800.00020000 .00000000.sdmp, 22.exe, 0000000B.0000000 0.422804028.000000000042B000.00000008.00 000001.01000000.0000000B.sdmp	false		high
http://www.carterandcone.coml	Pluto Panel.exe, 00000005.00000002.71209 0794.0000000006EE2000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.cloudflare.com/5xx-error-landing	Pluto Panel.exe, 00000005.00000002.70600 3291.00000000036CE000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/	Pluto Panel.exe, 00000005.00000003.43408 3509.0000000005C7E000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.433444494.0000000005C 7E000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.432944886.0000000005C7F000.00000004.0 0000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.co	Pluto Panel.exe, 00000005.00000003.43777 3657.0000000005C80000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.438069908.0000000005C 80000.00000004.00000800.00020000.0000000 0.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Pluto Panel.exe, 00000005.00000003.54633 3465.0000000005C80000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.537131070.0000000005C 80000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.588600543.0000000005C80000.00000004.0 0000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.556315402.0000000005C80 000.00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.580567393 .0000000005C80000.00000004.00000800.0002 0000.00000000.sdmp, Pluto Panel.exe, 000 00005.00000003.570425092.0000000005C8000 0.00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.541181738.0 000000005C80000.00000004.00000800.000200 00.00000000.sdmp, Pluto Panel.exe, 00000 005.00000003.551450060.0000000005C80000. 00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.573427389.000 0000005C80000.00000004.00000800.00020000 .00000000.sdmp, Pluto Panel.exe, 0000000 5.00000003.569553799.0000000005C80000.00 000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000002.712090794.00000 00006EE2000.00000004.00000800.00020000.0 0000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.comC	Pluto Panel.exe, 00000005.00000003.41333 0512.0000000005C85000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.symauth.com/rpa00	RIP_YOUR_PC_LOL.exe, 00000000.00000000.3 66341482.00000000009F2000.00000002.00000 001.01000000.00000003.sdmp, RIP_YOUR_PC_ LOL.exe, 00000000.00000003.437188672.000 00000056F5000.00000004.00000800.00020000 .00000000.sdmp, 22.exe, 0000000B.0000000 0.422804028.000000000042B000.00000008.00 000001.01000000.0000000B.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/)	Pluto Panel.exe, 00000005.00000003.45948 5550.0000000005C5A000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.460010944.0000000005C 5A000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.461983546.0000000005C5B000.00000004.0 0000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.460984251.0000000005C5B 000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/eu-e	Pluto Panel.exe, 00000005.00000003.45200 1254.0000000005C5A000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/n	Pluto Panel.exe, 00000005.00000003.44819 3641.0000000005C53000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.462837238.0000000005C 5B000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.459485550.0000000005C5A000.00000004.0 0000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.457715522.0000000005C56 000.00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.463380932 .0000000005C5B000.00000004.00000800.0002 0000.00000000.sdmp, Pluto Panel.exe, 000 00005.00000003.460010944.0000000005C5A00 0.00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.464082407.0 000000005C5B000.00000004.00000800.000200 00.00000000.sdmp, Pluto Panel.exe, 00000 005.00000003.452001254.0000000005C5A000. 00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.457092303.000 0000005C5A000.00000004.00000800.00020000 .00000000.sdmp, Pluto Panel.exe, 0000000 5.00000003.461983546.0000000005C5B000.00 000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.464883846.00000 00005C5B000.00000004.00000800.00020000.0 0000000.sdmp, Pluto Panel.exe, 00000005. 00000003.460984251.0000000005C5B000.0000 0004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cnY	Pluto Panel.exe, 00000005.00000003.43748 7558.0000000005C80000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.439099390.0000000005C 80000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.437239432.0000000005C80000.00000004.0 0000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.436798009.0000000005C80 000.00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.436695339 .0000000005C80000.00000004.00000800.0002 0000.00000000.sdmp, Pluto Panel.exe, 000 00005.00000003.437773657.0000000005C8000 0.00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.437023378.0 000000005C80000.00000004.00000800.000200 00.00000000.sdmp, Pluto Panel.exe, 00000 005.00000003.439790741.0000000005C80000. 00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.438069908.000 0000005C80000.00000004.00000800.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/C	Pluto Panel.exe, 00000005.00000003.62087 6949.0000000005C5A000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.645268957.0000000005C 5A000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.630356431.0000000005C5A000.00000004.0 0000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.585753311.0000000005C5A 000.00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.593605825 .0000000005C5A000.00000004.00000800.0002 0000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/i	Pluto Panel.exe, 00000005.00000003.44819 3641.0000000005C53000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.452001254.0000000005C 5A000.00000004.00000800.00020000.0000000 0.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comitu	Pluto Panel.exe, 00000005.00000003.58575 3311.0000000005C5A000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.593605825.0000000005C 5A000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.578609523.0000000005C5A000.00000004.0 0000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/g	Pluto Panel.exe, 00000005.00000003.45948 5550.0000000005C5A000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.457715522.0000000005C 56000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.460010944.0000000005C5A000.00000004.0 0000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.457092303.0000000005C5A 000.00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.461983546 .0000000005C5B000.00000004.00000800.0002 0000.00000000.sdmp, Pluto Panel.exe, 000 00005.00000003.460984251.0000000005C5B00 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.google.com/accounts/servicelogin	Pluto Panel.exe	false		high
http://www.freeeim.com/D	RIP_YOUR_PC_LOL.exe, 00000000.00000000.3 67521899.0000000000E31000.00000002.00000 001.01000000.00000003.sdmp, RIP_YOUR_PC_ LOL.exe, 00000000.00000002.696610265.000 00000057AD000.00000004.00000800.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comic	Pluto Panel.exe, 00000005.00000003.44590 3668.0000000005C80000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cncz$	Pluto Panel.exe, 00000005.00000003.43190 8494.0000000005C5B000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn$	Pluto Panel.exe, 00000005.00000003.43190 8494.0000000005C5B000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comkC	Pluto Panel.exe, 00000005.00000003.44202 1245.0000000005C80000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.441503544.0000000005C 80000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.441818008.0000000005C80000.00000004.0 0000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/ls	Pluto Panel.exe, 00000005.00000003.44819 3641.0000000005C53000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comFX	Pluto Panel.exe, 00000005.00000003.53943 2667.0000000005C5C000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.561809650.0000000005C 54000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.570284939.0000000005C5A000.00000004.0 0000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	Pluto Panel.exe, 00000005.00000002.71209 0794.0000000006EE2000.00000004.00000800. 00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deMTq	Pluto Panel.exe, 00000005.00000003.64678 7103.0000000005C80000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	Pluto Panel.exe, 00000005.00000002.71209 0794.0000000006EE2000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/C	Pluto Panel.exe, 00000005.00000003.45948 5550.0000000005C5A000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.457715522.0000000005C 56000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.452001254.0000000005C5A000.00000004.0 0000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.457092303.0000000005C5A 000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	Pluto Panel.exe, 00000005.00000002.71209 0794.0000000006EE2000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Pluto Panel.exe, 00000005.00000002.71209 0794.0000000006EE2000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/J	Pluto Panel.exe, 00000005.00000003.45948 5550.0000000005C5A000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.457715522.0000000005C 56000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.452001254.0000000005C5A000.00000004.0 0000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.457092303.0000000005C5A 000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnT	Pluto Panel.exe, 00000005.00000003.43344 4494.0000000005C7E000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.432459781.0000000005C 7F000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.432944886.0000000005C7F000.00000004.0 0000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cnts	Pluto Panel.exe, 00000005.00000003.43748 7558.0000000005C80000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.437239432.0000000005C 80000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.436798009.0000000005C80000.00000004.0 0000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.436695339.0000000005C80 000.00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.437023378 .0000000005C80000.00000004.00000800.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	Pluto Panel.exe, 00000005.00000002.71209 0794.0000000006EE2000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	Pluto Panel.exe, 00000005.00000002.71209 0794.0000000006EE2000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

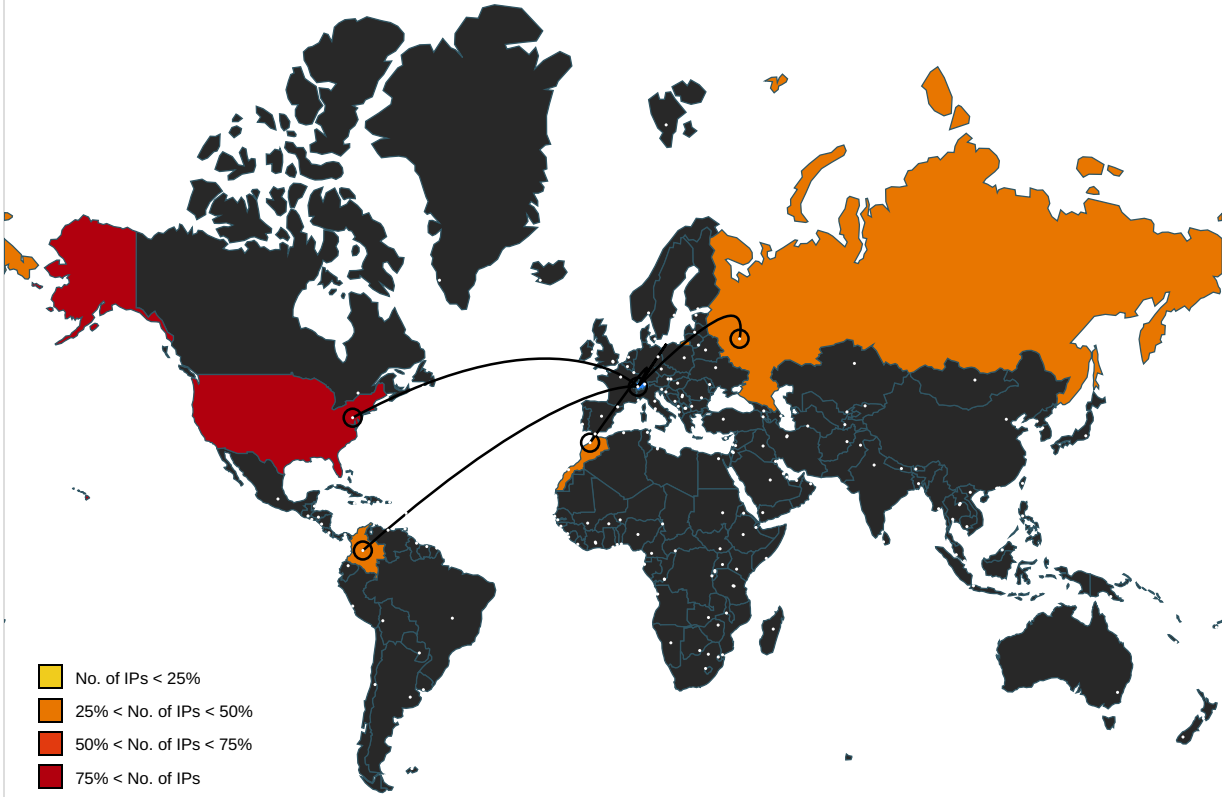
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.com	Pluto Panel.exe, 00000005.00000003.44544 3819.0000000005C80000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.437487558.0000000005C 80000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.439099390.0000000005C80000.00000004.0 0000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.437239432.0000000005C80 000.00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.436798009 .0000000005C80000.00000004.00000800.0002 0000.00000000.sdmp, Pluto Panel.exe, 000 00005.00000003.437773657.0000000005C8000 0.00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.437023378.0 000000005C80000.00000004.00000800.000200 00.00000000.sdmp, Pluto Panel.exe, 00000 005.00000003.440045453.0000000005C80000. 00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.441297022.000 0000005C80000.00000004.00000800.00020000 .00000000.sdmp, Pluto Panel.exe, 0000000 5.00000003.439790741.0000000005C80000.00 000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.442021245.00000 00005C80000.00000004.00000800.00020000.0 0000000.sdmp, Pluto Panel.exe, 00000005. 00000003.438069908.0000000005C80000.0000 0004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.445694166.0000000 005C80000.00000004.00000800.00020000.000 00000.sdmp, Pluto Panel.exe, 00000005.00 000003.445564416.0000000005C80000.000000 04.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.441503544 .0000000005C80000.00000004.00000800.0002 0000.00000000.sdmp, Pluto Panel.exe, 000 00005.00000003.441818008.0000000005C8000 0.00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.445818252.0 000000005C80000.00000004.00000800.000200 00.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comoX	Pluto Panel.exe, 00000005.00000002.71188 7980.0000000005C50000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.com.	Pluto Panel.exe, 00000005.00000003.43679 8009.0000000005C80000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.437023378.0000000005C 80000.00000004.00000800.00020000.0000000 0.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	Pluto Panel.exe, 00000005.00000002.71209 0794.0000000006EE2000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersh	Pluto Panel.exe, 00000005.00000003.58575 3311.0000000005C5A000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/staff/dennis.htm	Pluto Panel.exe, 00000005.00000002.71209 0794.0000000006EE2000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Pluto Panel.exe, 00000005.00000002.71209 0794.0000000006EE2000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.thawte.com/ThawteTimestampingCA.crl0	RIP_YOUR_PC_LOL.exe, 00000000.00000000.3 66341482.00000000009F2000.00000002.00000 001.01000000.00000003.sdmp, RIP_YOUR_PC_ LOL.exe, 00000000.00000003.437188672.000 00000056F5000.00000004.00000800.00020000 .00000000.sdmp, 22.exe, 0000000B.0000000 0.422804028.000000000042B000.00000008.00 000001.01000000.0000000B.sdmp	false		high
http://www.founder.com.cn/cnv	Pluto Panel.exe, 00000005.00000003.43190 8494.0000000005C5B000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://login.yahoo.com/config/login	Pluto Panel.exe	false		high
http://www.fontbureau.comrsiv	Pluto Panel.exe, 00000005.00000003.64526 8957.0000000005C5A000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	Pluto Panel.exe, 00000005.00000003.41376 4911.0000000005C85000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.413943860.0000000005C 85000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.413057625.0000000005C85000.00000004.0 0000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.413330512.0000000005C85 000.00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000002.712090794 .0000000006EE2000.00000004.00000800.0002 0000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Pluto Panel.exe, 00000005.00000002.71209 0794.0000000006EE2000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	Pluto Panel.exe, 00000005.00000003.64678 7103.0000000005C80000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.494373371.0000000005C 80000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.493190429.0000000005C80000.00000004.0 0000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.497114575.0000000005C80 000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	Pluto Panel.exe, 00000005.00000003.46198 3546.0000000005C5B000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000002.712090794.0000000006E E2000.00000004.00000800.00020000.0000000 0.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.como.W	Pluto Panel.exe, 00000005.00000003.43909 9390.0000000005C80000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.439790741.0000000005C 80000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.438069908.0000000005C80000.00000004.0 0000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/X	Pluto Panel.exe, 00000005.00000003.45771 5522.0000000005C56000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.457092303.0000000005C 5A000.00000004.00000800.00020000.0000000 0.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comonyn	Pluto Panel.exe, 00000005.00000003.53943 2667.0000000005C5C000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://whatismyipaddress.com/	Pluto Panel.exe, 00000005.00000002.70575 3147.0000000003691000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000002.706003291.00000000036 CE000.00000004.00000800.00020000.0000000 0.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	Pluto Panel.exe, 00000005.00000002.71209 0794.0000000006EE2000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Pluto Panel.exe, 00000005.00000003.62087 6949.0000000005C5A000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.645268957.0000000005C 5A000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.630356431.0000000005C5A000.00000004.0 0000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.585753311.0000000005C5A 000.00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.593605825 .0000000005C5A000.00000004.00000800.0002 0000.00000000.sdmp, Pluto Panel.exe, 000 00005.00000003.539432667.0000000005C5C00 0.00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.561809650.0 000000005C54000.00000004.00000800.000200 00.00000000.sdmp, Pluto Panel.exe, 00000 005.00000003.570284939.0000000005C5A000. 00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.578609523.000 0000005C5A000.00000004.00000800.00020000 .00000000.sdmp, Pluto Panel.exe, 0000000 5.00000002.712090794.0000000006EE2000.00 000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comF	Pluto Panel.exe, 00000005.00000003.64526 8957.0000000005C5A000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.539432667.0000000005C 5C000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.561809650.0000000005C54000.00000004.0 0000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comsiv/C	Pluto Panel.exe, 00000005.00000003.53943 2667.0000000005C5C000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.561809650.0000000005C 54000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.570284939.0000000005C5A000.00000004.0 0000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comTC	Pluto Panel.exe, 00000005.00000003.43748 7558.0000000005C80000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.437239432.0000000005C 80000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.437023378.0000000005C80000.00000004.0 0000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.thawte.com0	RIP_YOUR_PC_LOL.exe, 00000000.00000000.3 66341482.00000000009F2000.00000002.00000 001.01000000.00000003.sdmp, RIP_YOUR_PC_ LOL.exe, 00000000.00000003.437188672.000 00000056F5000.00000004.00000800.00020000 .00000000.sdmp, 22.exe, 0000000B.0000000 0.422804028.000000000042B000.00000008.00 000001.01000000.0000000B.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cp	Pluto Panel.exe, 00000005.00000003.43190 8494.0000000005C5B000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deR	Pluto Panel.exe, 00000005.00000003.49437 3371.0000000005C80000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.493190429.0000000005C 80000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.497114575.0000000005C80000.00000004.0 0000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comtu	Pluto Panel.exe, 00000005.00000003.57028 4939.0000000005C5A000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://whatismyipaddress.comx&	Pluto Panel.exe, 00000005.00000002.70600 3291.00000000036CE000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://whatismyipaddress.com	Pluto Panel.exe, 00000005.00000002.70575 3147.0000000003691000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/	Pluto Panel.exe, 00000005.00000003.46283 7238.0000000005C5B000.00000004.00000800. 00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.459485550.0000000005C 5A000.00000004.00000800.00020000.0000000 0.sdmp, Pluto Panel.exe, 00000005.000000 03.457715522.0000000005C56000.00000004.0 0000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.463380932.0000000005C5B 000.00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.460010944 .0000000005C5A000.00000004.00000800.0002 0000.00000000.sdmp, Pluto Panel.exe, 000 00005.00000003.464082407.0000000005C5B00 0.00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.457092303.0 000000005C5A000.00000004.00000800.000200 00.00000000.sdmp, Pluto Panel.exe, 00000 005.00000003.461983546.0000000005C5B000. 00000004.00000800.00020000.00000000.sdmp, Pluto Panel.exe, 00000005.00000003.464883846.000 0000005C5B000.00000004.00000800.00020000 .00000000.sdmp, Pluto Panel.exe, 0000000 5.00000003.460984251.0000000005C5B000.00 000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlf	Pluto Panel.exe, 00000005.00000003.56955 3799.0000000005C80000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.fontbureau.coma	Pluto Panel.exe, 00000005.00000002.71188 7980.0000000005C50000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comd	Pluto Panel.exe, 00000005.00000003.53943 2667.0000000005C5C000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Pluto Panel.exe, 00000005.00000002.71209 0794.0000000006EE2000.00000004.00000800. 00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
179.13.1.253	gfhhjgh.duckdns.org	Colombia		27831	ColombiaMovilCO	false
172.98.92.42	unknown	United States		46562	TOTAL-SERVER-SOLUTIONSUS	false
41.249.51.34	kazya1.hopto.org	Morocco		36903	MT-MPLSMA	false
52.20.78.240	api.ipify.org.herokudns.com	United States		14618	AMAZON-AESUS	false
80.87.192.115	unknown	Russian Federation		29182	THEFIRST-ASRU	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	585264
Start date:	08.03.2022
Start time:	17:59:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RIP_YOUR_PC_LOL.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:	61
Number of new started drivers analysed:	0

Copyright Joe Security LLC 2022

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.adwa.spyw.evad.winEXE@84/32@48/5
EGA Information:	• Successful, ratio: 83.3%
HDC Information:	• Successful, ratio: 15.8% (good quality ratio 14.3%) • Quality average: 70.3% • Quality standard deviation: 31.5%
HCA Information:	• Successful, ratio: 83% • 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

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 104.26.13.31, 172.67.75.172, 104.26.12.31, 20.190.160.129, 20.190.160.75, 20.190.160.6, 20.190.160.136, 20.190.160.73, 20.190.160.132, 20.190.160.69, 20.190.160.67, 20.42.65.92, 20.82.209.104, 80.67.82.211, 80.67.82.235
- Excluded domains from analysis (whitelisted): api.ip.sb.cdn.cloudflare.net, fs.microsoft.com, www.tm.lg.prod.aadmsa.akadns.net, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, www.tm.a.prd.aadg.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, login.msa.msidentity.com, iris-de-ppe-azsc-neu.northeurope.cloudapp.azure.com, e12564.dspb.akamaiedge.net, onedsblobprdeus17.eastus.cloudapp.azure.com, login.live.com, blobcollector.events.data.trafficmanager.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Execution Graph export aborted for target test.exe, PID 6236 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing behavior and disassembly information.
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:01:04	API Interceptor	1x Sleep call for process: aaa.exe modified
18:01:13	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
18:01:14	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\AppData\Roaming\Opus.exe" s>$(Arg0)
18:01:22	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
18:01:22	API Interceptor	88x Sleep call for process: Opus.exe modified
18:01:23	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run a797c6ca3f5e7aff8fa1149c47fe9466 "C:\Users\user\AppData\Roaming\mediaget.exe" ..
18:01:39	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run a797c6ca3f5e7aff8fa1149c47fe9466 "C:\Users\user\AppData\Roaming\mediaget.exe" ..
18:01:54	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a797c6ca3f5e7aff8fa1149c47fe9466.exe
18:02:13	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run a797c6ca3f5e7aff8fa1149c47fe9466 "C:\Users\user\AppData\Roaming\mediaget.exe" ..
18:02:48	Task Scheduler	Run new task: dwm path: "C:\Windows\System32\srvsvc\dwm.exe"
18:02:51	Task Scheduler	Run new task: conhost path: "C:\Windows\System32\mssip32\conhost.exe"
18:02:52	Task Scheduler	Run new task: RuntimeBroker path: "C:\Windows\System32\WindowsDefaultHeatProcessor\RuntimeBroker.exe"
18:02:52	Task Scheduler	Run new task: services path: "C:\Users\Public\Documents\My Music\services.exe"
18:02:52	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Windows Update C:\Users\user\AppData\Roaming\WindowsUpdate.exe
18:02:55	Task Scheduler	Run new task: 8f1c8b40c7be588389a8d382040b23bb path: "C:\Documents and Settings\Public\Desktop\8f1c8b40c7be588389a8d382040b23bb.exe"
18:02:55	Task Scheduler	Run new task: explorer path: "C:\Windows\winhlp32\explorer.exe"

Time	Type	Description
18:02:55	Task Scheduler	Run new task: mediaget path: "C:\Windows\CbsTemp\mediaget.exe"
18:03:04	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Windows Update C:\Users\user\App Data\Roaming\WindowsUpdate.exe
18:03:12	Autostart	Run: HKLM64\Software\Microsoft\Windows\CurrentVersion\Run dwm "C:\Windows\System32\srvsvc\dwm.exe"
18:03:22	Autostart	Run: HKLM64\Software\Microsoft\Windows\CurrentVersion\Run RuntimeBroker "C:\Windows\System 32\WindowsDefaultHeatProcessor\RuntimeBroker.exe"

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Process:	C:\Users\user\AppData\Roaming\Opus.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	208384
Entropy (8bit):	7.449669736966968
Encrypted:	false
SSDEEP:	6144:cLV6Bta6dtJmakIM5zEN/wjwJsvle+o9f/N:cLV6Btpmk1Elepd
MD5:	759185EE3724D7563B709C888C696959
SHA1:	7C166CC3CBFEF08BB378BCF557B1F45396A22931
SHA-256:	9384798985672C356A8A41BF822443F8EB0D3747BFCA148CE814594C1A894641
SHA-512:	ED754357B1B995DE918AF21FECD9D1464BDEA6778F7AB450A34E3AAE22BA7EEBC02F2442AF13774ABFDF97954E419EC9E356B54506C7E3BF12E3B76EE882FA2C
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 85%, Browse • Antivirus: ReversingLabs, Detection: 100%
Reputation:	unknown

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....d..... .....@.. ....8...W.... ..$`..... ..... ..H.....text..... ..... ..`.reloc.....@..B.rsrc...$`... ...b.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2.... ....3.... .....*.*....0..E.....s7....-(&s8....-&&s9.....,$&s:.....s;.....*.....+.....+.....+.....0.....~....o<...*..0.....~....o=...*..0.....~....o>...*..0.....~....o?...*..0.....~....o@...*..0.....-.&(A...*&+...0 ..$.....~B.....-.(...+.-.&+..B...+.~B...*.0.....-.&(A...*&+...0..

C:\ProgramData\kaosdma.txt

Process:	C:\Users\user\AppData\Roaming\0fd7de5367376231a788872005d7ed4f.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	10
Entropy (8bit):	2.6464393446710157
Encrypted:	false
SSDEEP:	3:HLLv:fv
MD5:	7AE4BED9A9648A53C3508D11671EF714
SHA1:	C349F54BAAA203AB3DC98498C49851C0704DD217
SHA-256:	C355B022F11CFAD7126BBD035784DAB1E94C3604D1528A130465E823C6EC1149
SHA-512:	7E3C40C668FAA94C9C1420B70405F41181BAE21F906C48164828E5427F66950483C4056E48C1FFF56634A5CDD943E5B1E40B8BEC798F4349E46263B21D7E1C6E
Malicious:	false
Reputation:	unknown
Preview:	84.17.52.7

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RIP_YOUR_PC_LOL.exe.log

Process:	C:\Users\user\Desktop\RIP_YOUR_PC_LOL.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	128
Entropy (8bit):	5.185983766127119
Encrypted:	false
SSDEEP:	3:QHXMKaZImrnLCR2RAVIAQyz2QyDBLnDLFv:Q3LadLCR22IAQykdL1v
MD5:	1F5C279D069793BFDB15F6DAC63D5C39
SHA1:	EFA436296EE3BC196FFC4FBD48978A4A1BB6FD34
SHA-256:	007D94877B5C9048FDC238CF6E63516F2BF398588878947E1DC4A4E55553602D
SHA-512:	48270029CAB2C46093058BDB28795ECA137656C1B4EB9E1EFD2111EA42997B29312B7A0EBFD6EB411375F799754D2403C233D0FF6B65103AEFABDE68268ED74 7
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\aaa.exe.log

Process:	C:\Users\user\AppData\Roaming\aaa.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk7v:MLF20NaL3z2p29hJ5g522r0
MD5:	80EFBEC081D7836D240503C4C9465FEC
SHA1:	6AF398E08A359457083727BAF296445030A55AC3
SHA-256:	C73F730EB5E05D15FAD6BE10AB51FE4D8A80B5E88B89D8BC80CC1DF09ACE1523
SHA-512:	DEC3B1D9403894418AFD4433629CA6476C7BD359963328D17B93283B52EEC18B3725D2F02F0E9A142E705398DDDCE244D53829570E9DE1A87060A7DABFDCE5 3
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages _v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Wind ows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\gay.exe.log

Process:	C:\Users\user\AppData\Roaming\gay.exe

File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk7v:MLF20NaL3z2p29hJ5g522r0
MD5:	80EFBEC081D7836D240503C4C9465FEC
SHA1:	6AF398E08A359457083727BAF296445030A55AC3
SHA-256:	C73F730EB5E05D15FAD6BE10AB51FE4D8A80B5E88B89D8BC80CC1DF09ACE1523
SHA-512:	DEC3B1D9403894418AFD4433629CA6476C7BD359963328D17B93283B52EEC18B3725D2F02F0E9A142E705398DDDCE244D53829570E9DE1A87060A7DABFDCE5I 3
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages _v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Wind ows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\healastounding.exe.log

Process:	C:\Users\user\AppData\Roaming\healastounding.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	128
Entropy (8bit):	5.185983766127119
Encrypted:	false
SSDEEP:	3:QHXMKaZImrnLCR2RAVIAQyz2QyDBLnDLFv:Q3LadLCR22IAQykdL1v
MD5:	1F5C279D069793BFDB15F6DAC63D5C39
SHA1:	EFA436296EE3BC196FFC4FBD48978A4A1BB6FD34
SHA-256:	007D94877B5C9048FDC238CF6E63516F2BF3985888789 47E1DC4A4E55553602D
SHA-512:	48270029CAB2C46093058BDB28795ECA137656C1B4EB9E1EFD2111EA42997B29312B7A0EBFD6EB411375F799754D2403C233D0FF6B65103AEFABDE68268ED74 7
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\5JOCE52U.txt

Process:	C:\Users\user\AppData\Roaming\0fd7de5367376231a788872005d7ed4f.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	10
Entropy (8bit):	2.6464393446710157
Encrypted:	false
SSDEEP:	3:HLLv:fv
MD5:	7AE4BED9A9648A53C3508D11671EF714
SHA1:	C349F54BAAA203AB3DC98498C49851C0704DD217
SHA-256:	C355B022F11CFAD7126BBD035784DAB1E94C3604D1528A130465E823C6EC1149
SHA-512:	7E3C40C668FAA94C9C1420B70405F41181BAE21F906C48164828E5427F66950483C4056E48C1FFF56634A5CDD943E5B1E40B8BEC798F4349E46263B21D7E1C6E
Malicious:	false
Reputation:	unknown
Preview:	84.17.52.7

C:\Users\user\AppData\Local\Temp\Dcvxaamev.exe

Process:	C:\Users\user\AppData\Roaming\8f1c8b40c7be588389a8d382040b23bb.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	335872
Entropy (8bit):	7.696824069546379
Encrypted:	false
SSDEEP:	6144:WLR0mFZcyJuOwhXdZkWwQ5eRI44axa7AP5Mb:8RHTJuOwhNZkWwQURI4xxa70ab
MD5:	870D6E5AEF6DEA98CED388CCE87BFBD4

SHA1:	2D7EEE096D38D3C2A8F12FCBA0A44B4C4DA33D54
SHA-256:	6D50833895B2E3EB9D6F879A6436660127C270B6A516CDA0253E56A3D8B7FBA0
SHA-512:	0D55AB28B2F80136AF121B870B7503551D87BBEB2848CF9A32540006CAC9A5E346D9FCCE2BF1223A22927F72A147B81487533A10B91373D4FA4429D6159FD566
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 29%, Browse • Antivirus: ReversingLabs, Detection: 86%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....>.a..... .....Y.....@.....0.....F.. .....T...P.... ..t.....d.....text..... ..`.data.....@....rsrc...t.... .....@..@..... .....

C:\Users\user\AppData\Local\Temp\FFDvbcrdfqs.exe

Process:	C:\Users\user\AppData\Roaming\8f1c8b40c7be588389a8d382040b23bb.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	290816
Entropy (8bit):	7.605066056188275
Encrypted:	false
SSDEEP:	6144:7S0BFZcouRlCLNkbI7u2KrMmCI44axa7AR5Mp:7SkZolCLybI7xI4xxa7Wap
MD5:	78D40B12FFC837843FBF4DE2164002F6
SHA1:	985BDFFA69BB915831CD6B81783AEF3AE4418F53
SHA-256:	308A15DABDC4CE6B96DD54954A351D304F1FCB59E8C93221BA1C412BCDFD1C44
SHA-512:	C6575E1771D37DED4089D963BEA95DEAC78B329ED555C991D7C559EE1970DD0887A965E88C09981529ADC9C25DF5CFD3D57E3DCE6724DA1F01F1198F0F460E 9
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 29%, Browse • Antivirus: ReversingLabs, Detection: 86%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...w>.a.....@... .....P....@.....I.. .....D..P....p..t.....d.....text...:.....@..... ..`.data.....P.....P.....@....rsrc...t....p .....`.....@..@..... .....

C:\Users\user\AppData\Local\Temp\tmp4896.tmp

Process:	C:\Users\user\AppData\Roaming\Opus.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1305
Entropy (8bit):	5.090556205433367
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0V75xtn:cbk4oL600QydbQxIYODOLedq3K5j
MD5:	1211D31E3B2DF2F76E97FEF49A693566
SHA1:	47DA0FC84FEF52FE80D25341A9A2DC97117841F3
SHA-256:	8DD44C774959C9CA5E2557721C4C09ACCC5C5307F426D4A015AEF61A8410F45C
SHA-512:	05DE66143F4D1FCAE7BB927CF508AFD02DFA910D2D244D0EDD7545A9BF9F4B478C3B00D387C84495A14865BCF565D3A25201E6E61C85DE7DB37E4EA4938C1E 49
Malicious:	**true**
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp5D87.tmp

Process:	C:\Users\user\AppData\Roaming\Opus.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped

Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755734
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\0fd7de5367376231a788872005d7ed4f.exe

Process:	C:\Users\user\Desktop\RIP_YOUR_PC_LOL.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	549556
Entropy (8bit):	6.964847007042997
Encrypted:	false
SSDEEP:	12288:eKmlz464jAfhe5pUC1jAXBoFACBfz6JMW0rwrsu:oz4d/5iCj0BoNBb6Jh3
MD5:	0FD7DE5367376231A788872005D7ED4F
SHA1:	658E4D5EFB8B14661967BE2183CC60E3E561B2B6
SHA-256:	9083992637E90E412E6F4E77331EB69EE8DB821C54BBC38533E0F889CC4CA9DD
SHA-512:	522D5BE2803FBCE0D12C325CC2EF1E3A92CEC03AEBA7D1164530093AD58CAECD827DD557CA3C182A66C6667150E731DE37BB552D19425F96CC78FE3423E1A63
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 29%, Browse • Antivirus: ReversingLabs, Detection: 92%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .4.d.Z.d.Z.d.Z.z..u.Z.z....Z.z..S.Z.CC!.g.Z.d.[..Z.z..e.Z.z..e.Z.z..e.Z .Richd.Z.....PE..L....:._..... .....@.....d.....8Y..(.....*...8.....P.....O..@..... .....text...0..... ..`.rdata.....@..@.data.....p.....T.....@....rsrc.....@..@..... ....

C:\Users\user\AppData\Roaming\22.exe

Process:	C:\Users\user\Desktop\RIP_YOUR_PC_LOL.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2101248
Entropy (8bit):	7.055994450169564
Encrypted:	false
SSDEEP:	49152:XkSw2TRlsQ1k0+eDE/C9fLtGoDs9cXpJGy:0EHZ/rDjfLe9cy
MD5:	DBF9DAA1707B1037E28A6E0694B33A4B
SHA1:	DDC1FCEC1C25F2D97C372FFFA247969AA6CD35EF
SHA-256:	A604A3FF78644533FAC5EE9F198E9C5F2FA1AE2A5828186367A9E00935CFF6B6
SHA-512:	145B606FFD58554050FF8712DDB38C1C66DD5F33EA15FD48474E1C165B2C0348D2413E16C7AD07FF1C65CE71E2BE23E3758E6D48C4F2454D5407982119706BF
Malicious:	**true**
Yara Hits:	• Rule: MALWARE_Win_BlackMoon, Description: Detects executables using BlackMoon RunTime, Source: C:\Users\user\AppData\Roaming\22.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 38%, Browse • Antivirus: ReversingLabs, Detection: 86%
Reputation:	unknown

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....(...I.U.I.U.I.U.U.U.I.U.F.U.I.U^U.U.I.U.o.U~I.U5V.U.I.U.F.U.I .U.I.U.K.U.o.U.I.U.I.U.I.U5V.U.I.URich.I.U.....PE..L....{.].....@.....P....@.....P".....@....@".....text....4.....@..... ..`.rdata..lP...P...`..P.....@..@.data.....P.....@....rsrc.....@"..... .@..@.....

C:\Users\user\AppData\Roaming\3.exe

Process:	C:\Users\user\AppData\Roaming\4.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	577536
Entropy (8bit):	5.535850322343421
Encrypted:	false
SSDEEP:	12288:aWMT5dtGv3Kom+qn4e9PtlAc7+Q4hMY1FOhcV:bMT5Sw++4ilAZ1OhcV
MD5:	748A4BEA8C0624A4C7A69F67263E0839
SHA1:	6955B7D516DF38992AC6BFF9D0B0F5DF150DF859
SHA-256:	220D8F8FF82D413C81BD02DFA001E1C478E8FBEA44BAD24F21B3A5284E15632E
SHA-512:	5FCDFDDCE3CC2E636001ED08C5F2F7590AADAA37C091F7BA94E519D298E284362721F1859C6FFBF064AE23E05D4E0E9754B515396812FBE9F9028497396799F
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DCRat_1, Description: Yara detected DCRat, Source: C:\Users\user\AppData\Roaming\3.exe, Author: Joe Security • Rule: MALWARE_Win_DCRat, Description: DCRat payload, Source: C:\Users\user\AppData\Roaming\3.exe, Author: ditekSHen • Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: C:\Users\user\AppData\Roaming\3.exe, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 47%, Browse • Antivirus: ReversingLabs, Detection: 82%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....N.... .....@.. .....@..... .@.....K..... ....H.....text...T.... ....`.rsrc... .....@..@.reloc..... . .....@..B.....0.....H.....l.....*&.(.....*J..(.....(.....*"..}....*^..}.....(.....}....*.0..{....."5-...YE....5...1...N...N...5...+... ..+...".<+>..\5.../.,+...\.!+..{..+...}..+...+....+...+...+...+...+...+..*..0..#.....n..+...t..+....+....+...+..*..0.....R.....o....(.....s.....8&.....o....(.....9....+.....+....;.. ..8....._,.....+.....,....XT.o.....8i.....,..r...p..o..

C:\Users\user\AppData\Roaming\4.exe

Process:	C:\Users\user\AppData\Roaming\healastounding.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	579127
Entropy (8bit):	7.206124159305961
Encrypted:	false
SSDEEP:	12288:xzxzTDWikLSb4NS7IODX+KEe+gpSwcxRLe4:bDWHSb4Ngse+USTR64
MD5:	E6DACE3F577AC7A6F9747B4A0956C8D7
SHA1:	86C71169025B822A8DFBA679EA981035CE1ABFD1
SHA-256:	8B4B846FE1023FA173AB410E3A5862A4C09F16534E14926878E387092E7FFB63
SHA-512:	1C8554D3D9A1B1509BA1DF569EDE3FB7A081BEF84394C708C4F1A2FB8779F012C74FBF6DE085514E0C8DEBB5079CC23C6C6112B95BF2F0AB6A8F0BD156A3E2 68
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 17%, Browse • Antivirus: ReversingLabs, Detection: 75%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b`..&...&...&.....h.+.....j.....k.>.....^.$...._..0..._..5...._...../y.,.../y ..#...&...+...._....._..'...._.'...f.'...._.'...Rich&.....PE..L....).`.....2.....0....@.....@.....0...4...d...<...0...R.....|".....T..... .....U..@.....0..`..... .....text..... ..`.rdata..".....0.....@..@.data...(7.....@....didat..... .....@.... rsrc....R...0...T.....@..@.reloc..|".....$...&.....@..B..... .....

C:\Users\user\AppData\Roaming\8f1c8b40c7be588389a8d382040b23bb.exe

Process:	C:\Users\user\AppData\Roaming\healastounding.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1241088
Entropy (8bit):	7.769765528202914
Encrypted:	false
SSDEEP:	24576:mMyMzC8+ovorlBtugg0uHqJkSkSZI7C8JaYRHwOwhNGWwQ58Xaj8rac:mMHF+lxuPHYkSfI77aYRQOayac

MD5:	8F1C8B40C7BE588389A8D382040B23BB
SHA1:	BEF5209AE90A3BD3171E1E0BE4E8148C4CCD8A6A
SHA-256:	ED58FFEE46A583C177C792B56C9FC20CCD9509D125F2E3FC90C4F48DE7E2C2A1
SHA-512:	9192B6F2F8320A728C445F9CD6E6D66495AD0EBEBD7FF193DC09EE8AE57B3933C1B75DC208E7D638DB273CB9D31B4CA24EE7BFD9729FF0CDBF432D72BB322B1F
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 26%, Browse • Antivirus: ReversingLabs, Detection: 86%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....>.a..... .....6(.....@.....k... .....P.....t.....d.....text...P..... ..`.data.....@....rsrc...t..... .....@..@..... .....

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat

Process:	C:\Users\user\AppData\Roaming\Opus.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:tiK:f
MD5:	A032CE284A49FD6CF341559395411B90
SHA1:	9A556CCC1AE76361E16EC13A4549BCEB79D6F383
SHA-256:	CE980B79958BE0B1DA2EFC904A80EFD8FA0B1E3607152100190A001AA399E1F5
SHA-512:	14D6696A4B21C6FBD461FED6F895E0FDAE6706F3DE897E4EE2E29EC9C90F129DE423F3D3476D6BABF4AE1EFAB365C92D697B1355A72CE308DBE2EED97F840E05
Malicious:	**true**
Reputation:	unknown
Preview:	!a:.p..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat

Process:	C:\Users\user\AppData\Roaming\Opus.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	42
Entropy (8bit):	4.15091348260215
Encrypted:	false
SSDEEP:	3:oNN+EaKC5fMN:oNN7aZ5fMN
MD5:	F00851831855D57C5FAB0A8B025C3ECE
SHA1:	B44A5459ED55DEF8D4F1283651C031B98BBD4F36
SHA-256:	A9CC872641CE9C8FA8134CB799FE95C76299F4202119B72F62129667DB38FC33
SHA-512:	4C9B0071735811D3E59E3E0115EECEF168AA3944D71F7C507AF3C046FA8234E020051E13DD5A2D0E4EE347A99263139697D8382AE1D465F9CED0A4315950D7A
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\AppData\Roaming\Opus.exe

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\21c8026919fd094ab07ec3c180a9f210_d06ed635-68f6-4e9a-955c-4899f5f57b9a

Process:	C:\Users\user\AppData\Roaming\8f1c8b40c7be588389a8d382040b23bb.exe
File Type:	data
Category:	dropped
Size (bytes):	49
Entropy (8bit):	1.2701062923235522
Encrypted:	false
SSDEEP:	3:/l1PL3n:fPL3
MD5:	CD8FA61AD2906643348EEF98A988B873
SHA1:	0B10E2F323B5C73F3A6EA348633B62AE522DDF39
SHA-256:	49A11A24821F2504B8C91BA9D8A6BD6F421ED2F0212C1C771BF1CAC9DE32AD75

SHA-512:	1E6F44AB3231232221CF0F4268E96A13C82E3F96249D7963B78805B693B52D3EBDABF873DB240813DF606D8C207BD2859338D67BA94F33ECBA43EA9A4FEFA08
Malicious:	false
Reputation:	unknown
Preview:	.....user.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a797c6ca3f5e7aff8fa1149c47fe9466.exe

Process:	C:\Users\user\AppData\Roaming\mediaget.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	37888
Entropy (8bit):	5.575438262402469
Encrypted:	false
SSDEEP:	384:HLWZcaCisD/WRdL5kyc/Ss4fzrngNsIhOrAF+rMRTyN/0L+EcoinblneHQM3epzN:iZcID5nc/Ss4HysIsrM+rMRa8NuM0t
MD5:	8EEDC01C11B251481DEC59E5308DCCC3
SHA1:	24BF069E9F2A1F12AEFA391674ED82059386B0AA
SHA-256:	0184983A425FEF55D46B7E0EB729A245730EE26414EBE4B155917C0124A19C2D
SHA-512:	52388313B21F14AA69C8B37E0FE0B73F66AA92F08651A16C820AAE65D341DC1AF6B48F3C8D4F657AC990EEAF4B9A01AE769BCA4D3625550011708697D22B69CC
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a797c6ca3f5e7aff8fa1149c47fe9466.exe, Author: Joe Security • Rule: MALWARE_Win_NjRAT, Description: Detects NjRAT / Bladabindi, Source: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a797c6ca3f5e7aff8fa1149c47fe9466.exe, Author: ditekSHen • Rule: njrat1, Description: Identify njRat, Source: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a797c6ca3f5e7aff8fa1149c47fe9466.exe, Author: Brian Wallace @botnet_hunter
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a..... .....@.. ..... @.....W.....@..... ....H.....text..... ....`.rsrc...@.....@..@.reloc. .....@..B.....H.....e...E.....&.(.....**..(.....*.s.....s.....s.....s.....*.0.....~....o....+..*.0.....~....o....+..*.0.....~....o....+..*.0.....~....o....+..*.0.....(....(....+..*...0.....(....+..*.0.....(....+..*.0.....(....+..*.0.. .....,,(...+.+.+....+...*.0..... .....**..(.....*....0..&.....~.....,.(...+.

C:\Users\user\AppData\Roaming\Opus.exe

Process:	C:\Users\user\AppData\Roaming\healastounding.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	208384
Entropy (8bit):	7.449669736966968
Encrypted:	false
SSDEEP:	6144:cLV6Bta6dtJmakIM5zEN/wjwJsvle+o9f/N:cLV6Btpmk1Elepd
MD5:	759185EE3724D7563B709C888C696959
SHA1:	7C166CC3CBFEF08BB378BCF557B1F45396A22931
SHA-256:	9384798985672C356A8A41BF822443F8EB0D3747BFCA148CE814594C1A894641
SHA-512:	ED754357B1B995DE918AF21FECD9D1464BDEA6778F7AB450A34E3AAE22BA7EEBC02F2442AF13774ABFDF97954E419EC9E356B54506C7E3BF12E3B76EE882FA2C
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Users\user\AppData\Roaming\Opus.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Users\user\AppData\Roaming\Opus.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Users\user\AppData\Roaming\Opus.exe, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: C:\Users\user\AppData\Roaming\Opus.exe, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: C:\Users\user\AppData\Roaming\Opus.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....d..... .....@.. ....8...W.... ..$`..... ..... ..H.....text..... ..... ..`.reloc.....@..B.rsrc...$`... ...b.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2.... ....3.... .....*.*....0..E.....s7....-(&s8....-&&s9....,$&s:.....s;.....*.....+.....+.....+.....0.....~....o<...*..0.....~....o=...*..0.....~....o>...*..0.....~....o?...*..0.....~....o@...*..0.....-.&(A...*&+...0 ..$.....~B.....-.(...+.-.&+..B...+.~B...*.0.....-.&(A...*&+...0..

C:\Users\user\AppData\Roaming\Pluto Panel.exe

Process:	C:\Users\user\Desktop\RIP_YOUR_PC_LOL.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

Category:	dropped
Size (bytes):	913920
Entropy (8bit):	7.376805169532317
Encrypted:	false
SSDEEP:	12288:ypEQtqB5urTIoYWBQk1E+VF9mOx9wi1T0hnbkOWAvyPx4+c/bUUCy:HQtqBorTlYWBhE+V3mO5vWgxE/nb
MD5:	ED666BF7F4A0766FCEC0E9C8074B089B
SHA1:	1B90F1A4CB6059D573FFF115B3598604825D76E6
SHA-256:	D1330D349BFBD3AEA545FA08EF63339E82A3F4D04E27216ECC4C45304F079264
SHA-512:	D0791EAA9859D751F946FD3252D2056C29328FC97E147A5234A52A3728588A3A1AAA003A8E32863D338EBDCA92305C48B6FA12CA1E620CF27460BF091C3B6D4
Malicious:	**true**
Yara Hits:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: C:\Users\user\AppData\Roaming\Pluto Panel.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: C:\Users\user\AppData\Roaming\Pluto Panel.exe, Author: Arnim Rupp • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: C:\Users\user\AppData\Roaming\Pluto Panel.exe, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: C:\Users\user\AppData\Roaming\Pluto Panel.exe, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: C:\Users\user\AppData\Roaming\Pluto Panel.exe, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: C:\Users\user\AppData\Roaming\Pluto Panel.exe, Author: JPCERT/CC Incident Response Group
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....C.a.....4..... .....@.. ....@.....S.... ...2.....`..... ..... ..H.....text..... ..... ..`.rsrc....2... ...2.....@..@.reloc.....` ....@..B.....H.....0}..h.....X.....2s.....*....0.....~.....(.....~....o....~....o.....9.....~....o.....+G~.....o.....o.....,). .....,.~.....~.....o....o.....1.~.....~....o.....o.....~....~....o....o.....~.....(....s....o.....(.....*.....0.. .....(....(.....(.....o.....*.....(.....(.....o... ....o.....o.....o.....*.R..(....o....o.....

C:\Users\user\AppData\Roaming___11.19.exe

Process:	C:\Users\user\Desktop\RIP_YOUR_PC_LOL.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	16322590
Entropy (8bit):	7.8569139750386485
Encrypted:	false
SSDEEP:	393216:G7BPkdKzrZciLxv8naSNtPr5rn57M84UTB9xO5/VWvJKJPkwdnfZ:uBPQwxMR7pn5qUTB9xOFVWvJKJPkwdnB
MD5:	A071727B72A8374FF79A695ECDE32594
SHA1:	B2ABA60B3332D6B8F0A56CEA310CDC2BDB4F9FFC
SHA-256:	8ECDFE60EACB5BF647AE69BCBC41DD727EA3089E92B4B08EBCA3A8D162E50745
SHA-512:	854B93FB6B9BF0FE4CAEF5572935852CE8BECF2BC7BD41B192A4B3CEFB7854A2405C6C0C06BBDD4E1026FF9440EC753911DCC935FE68118E322614C1B918E4 00
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....H..u...u...u...~...u.....u.....u.C.{...u...y...u...f...u...f...u...t.`.u.C. (...u...~...u.(.~...u.(.....u...u...u...s...u.Rich..u.....PE..L.....ca.....5.....@.....xi..... .....text..... ..`.rdata.....@..@.data....@..... .....@....rsrc..... .....@..@..... ....

C:\Users\user\AppData\Roaming\a.exe

Process:	C:\Users\user\AppData\Roaming\healastounding.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1484512
Entropy (8bit):	**7.99205858382872**
Encrypted:	**true**
SSDEEP:	24576:XsoFdKkWRoohlLUI9AMNo9p2mbfmqFycZm4lZD3Ya10Hue4MBSYcQkEaHNYK3Kyh:XrHW6ilLU1Eor3Fg4lBIM0Hue1BSYcQ4
MD5:	52CFD35F337CA837D31DF0A95CE2A55E
SHA1:	88EB919FA2761F739F02A025E4F9BF1FD340B6FF
SHA-256:	5975E737584DDF2601C02E5918A79DAD7531DF0E13DCA922F0525F66BEC4B448
SHA-512:	B584282F6F5396C3BBED7835BE67420AA14D11B9C42A88B0E3413A07A6164C22D6F50D845D05F48CB95D84FD9545D0B9E25E581324A08B3A95CED9F048D41D7
Malicious:	**true**

Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....O.....0..... ... .@.. ..... <.. ..-A6.. .....|L7.....r..... .....@....rsrc.... .....@..... ....@..... .....@..... 5.. ...V.....@....uxD5Xzb.....@7.....@....adata... ....<.....@..... ....

C:\Users\user\AppData\Roaming\aaa.exe

Process:	C:\Users\user\AppData\Roaming\healastounding.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	122880
Entropy (8bit):	7.206630188700291
Encrypted:	false
SSDEEP:	3072:zMJQH6NvccnsXOf4qhi01sXT0RZTF27rcAXIlWMhBN2/MTDM:zMxsU9i0iXT0RZo7Iwhec/MTD
MD5:	860AA57FC3578F7037BB27FC79B2A62C
SHA1:	A14008FE5E1EB88BF46266DE3D5EE5DB2E0A722B
SHA-256:	5430565C4534B482C7216A0AE75D04E201EE0DB0386682C0C010243083C28D29
SHA-512:	6639B3E2594E554C7FA811F22E1C514474D34220155B4C989AD8716DB1A0AEA65894AA23D78C12A4618C57312DA00353A77DD8E6C6BDD927BF865F2E98AFF8F
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....S.....n.... .....@.. .....@..... ..@..... ...K..... ....H.....text...t.... ....`.rsrc.....@..@.reloc..... .....@..B.....P.....H.....t.....5..x..... .....%.....(..... t.....%.....(.....*..V~....(....~....o....*....(....*R .l..q..(-.....*....0..... .....~.....E.....-...~.... ... .(...+..t.....,. .....[.+..+.....(....(!....t....('.....t.....(.....u.... ....(...+(....~.... ....~.... .....~.... .....X.k_.*.*.....(....*.(....t....~....o@...()....f.. (...+.....*....0.....(*....I.U(...+..

C:\Users\user\AppData\Roaming\gay.exe

Process:	C:\Users\user\AppData\Roaming\healastounding.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	37888
Entropy (8bit):	5.575438262402469
Encrypted:	false
SSDEEP:	384:HLWZcaCisD/WRdL5kyc/Ss4fzrngNsIhOrAF+rMRTyN/0L+EcoinblneHQM3epzN:iZcID5nc/Ss4HysIsrM+rMRa8NuM0t
MD5:	8EEDC01C11B251481DEC59E5308DCCC3
SHA1:	24BF069E9F2A1F12AEFA391674ED82059386B0AA
SHA-256:	0184983A425FEF55D46B7E0EB729A245730EE26414EBE4B155917C0124A19C2D
SHA-512:	52388313B21F14AA69C8B37E0FE0B73F66AA92F08651A16C820AAE65D341DC1AF6B48F3C8D4F657AC990EEAF4B9A01AE769BCA4D3625550011708697D22B69C C
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: C:\Users\user\AppData\Roaming\gay.exe, Author: Joe Security • Rule: MALWARE_Win_NjRAT, Description: Detects NjRAT / Bladabindi, Source: C:\Users\user\AppData\Roaming\gay.exe, Author: ditekSHen • Rule: njrat1, Description: Identify njRat, Source: C:\Users\user\AppData\Roaming\gay.exe, Author: Brian Wallace @botnet_hunter
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a..... .....@.. ..... @.....W.....@..... ....H.....text..... ....`.rsrc...@.....@..@.reloc. .....@..B.....H.....e...E.....&.(.....**..(.....*.s.....s.....s.....s.....*.0.....~....o....+..*.0.....~....o....+..*.0.....~....o....+..*.0.....~....o....+..*.0.....(....(....+..*...0.....(....+..*.0.....(....+..*.0.....(....+..*.0.. .....,(...+.+.+....+...*.0..... .....**..(.....*....0..&.....~.....,(...+.

C:\Users\user\AppData\Roaming\healastounding.exe

Process:	C:\Users\user\Desktop\RIP_YOUR_PC_LOL.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3733504
Entropy (8bit):	7.794569867865562
Encrypted:	false

SSDEEP:	98304:pAdy2TU151ZIpH8YcItGTHF+iSfI77agdayaW/ej:gy5Ls8YcItWFXlWZVy
MD5:	6FB798F1090448CE26299C2B35ACF876
SHA1:	451423D5690CFFA02741D5DA6E7C45BC08AEFB55
SHA-256:	B4F86FF48C5F6B01E0AD4543FB78E0435E81F3EC2AACA89866862157C0DACF4F
SHA-512:	9CC2421A2F3AB01D15BE62A848947B03F1A8212CFD923573CF70F8C10BD8D124AEE3B251828834236AF291EA12450AC2580A712E53A022CE11B4D71B0357D8C
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Users\user\AppData\Roaming\healastounding.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Users\user\AppData\Roaming\healastounding.exe, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: C:\Users\user\AppData\Roaming\healastounding.exe, Author: Joe Security • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: C:\Users\user\AppData\Roaming\healastounding.exe, Author: Joe Security • Rule: MALWARE_Win_NjRAT, Description: Detects NjRAT / Bladabindi, Source: C:\Users\user\AppData\Roaming\healastounding.exe, Author: ditekSHen • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: C:\Users\user\AppData\Roaming\healastounding.exe, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: C:\Users\user\AppData\Roaming\healastounding.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: njrat1, Description: Identify njRat, Source: C:\Users\user\AppData\Roaming\healastounding.exe, Author: Brian Wallace @botnet_hunter
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....8.....9.. ... 9...@.. .....`9..... ..@.....9.W.... 9.....@9..... ..... ..H.....text...4.8.. ....8..... ..`.rsrc..... 9.....8.....@..@.rel oc.....@9.....8.....@..B.....9.....H.....@.9.....`!...8.....0..f.....r...pr#..p(....t.....r9..p(.....+.....i].a...X....i2..(....o.....(.....(. ...&*...0..q.....(.....o.....s.....o.....+*.o....u.....,.o....t.....(.....,..o.....&.o....-.....,..o.....,..o.....s....z..*.....=R.....P^.....8.....lSystem.Resources.ResourceReader, mscorlib, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089#System.Res

C:\Users\user\AppData\Roaming\mediaget.exe

Process:	C:\Users\user\AppData\Roaming\gay.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	37888
Entropy (8bit):	5.575438262402469
Encrypted:	false
SSDEEP:	384:HLWZcaCisD/WRdL5kyc/Ss4fzrngNsIhOrAF+rMRTyN/0L+EcoinblneHQM3epzN:iZcID5nc/Ss4HyslsrM+rMRa8NuM0t
MD5:	8EEDC01C11B251481DEC59E5308DCCC3
SHA1:	24BF069E9F2A1F12AEFA391674ED82059386B0AA
SHA-256:	0184983A425FEF55D46B7E0EB729A245730EE26414EBE4B155917C0124A19C2D
SHA-512:	52388313B21F14AA69C8B37E0FE0B73F66AA92F08651A16C820AAE65D341DC1AF6B48F3C8D4F657AC990EEAF4B9A01AE769BCA4D3625550011708697D22B69C C
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: C:\Users\user\AppData\Roaming\mediaget.exe, Author: Joe Security • Rule: MALWARE_Win_NjRAT, Description: Detects NjRAT / Bladabindi, Source: C:\Users\user\AppData\Roaming\mediaget.exe, Author: ditekSHen • Rule: njrat1, Description: Identify njRat, Source: C:\Users\user\AppData\Roaming\mediaget.exe, Author: Brian Wallace @botnet_hunter
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a..... .....@.. ..... @.....W.....@..... ....H.....text..... ....`.rsrc...@.....@..@.reloc. .....@..B.....H.....e...E.....&.(.....**..(.....*.s.....s.....s.....s.....*.0.....~....o.....+..*.0.....~....o .....+..*.0.....~....o.....+..*.0.....~....o.....+..*.0.....(....(....+..*...0.....(....+..*.0.....(....+..*.0.....(....+..*.0.. .....,(...+.+.+....+...*.0..... .....**..(.....*....0..&.....~.....,(...+.

C:\Users\user\AppData\Roaming\test.exe

Process:	C:\Users\user\AppData\Roaming\healastounding.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	46080
Entropy (8bit):	5.459376005695359
Encrypted:	false
SSDEEP:	768:EuwCNToEjaNLWU3zKZmo2q7C8V1vBTcPI1zjbkgX3ir64oRfdwQfybTWVABDZTx:EuwCNToqaS2z8VnTh13brXSr64oZSbZH
MD5:	7E50B2929829321901792 45C60C0B59B
SHA1:	25CF641DDCDC818F32837DB236A58060426B5571
SHA-256:	A8DDE4E60DB080DFC397D7E312E7E9F18D9C08D6088E8043FEEAE9AB32ABDBB8
SHA-512:	C6D422D9FB115E1B6B085285B1D3CA46ED541E390895D702710E82A336F4DE6CC5C9183F8E6EBE35475FCCE6DEF8CC5FFA8EE4A61B38D7E80A9F40789688B8 85
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: C:\Users\user\AppData\Roaming\test.exe, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: C:\Users\user\AppData\Roaming\test.exe, Author: ditekSHen

Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...#..^.....N.... .....@.. ....@.....O..... ....H.....text...T.... ....`.rsrc.....@..@.reloc..... .....@..B.....0.....H.....Y...m.....V..;...$0.xC.=VD..b.....9A../.\.....(....*.~....*.....*.~....*.....*.~....*.....*.~....*.....*.~ ....*.....*.~....*.....*.~....*.....*.~....*.....*.~....*.....*.~....*.....**.(>.....*2~.....o?...*.s.....*.()...:(...(*.:.....(+..:....('..:.....((...9.....(v...*V(....s.... ...o....*n~....9....~....o.. .....*~~....(....9....(0...9....(@...*Vr.%.p~....(o....#...*.s...

C:\Windows\Cursors\WUDFhosts.exe

Process:	C:\Users\user\AppData\Roaming\22.exe
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	806912
Entropy (8bit):	7.921653477744872
Encrypted:	false
SSDEEP:	24576:f7hffPYBJUtGpCXX3dquvU9ckRvYLpZjQaYM8l:NfLtGoDs9cXpJG
MD5:	4A72E30C0A582B082030ADFD8345014F
SHA1:	2F92CCF13F8DFC7EEFF49903A0D1EA8DD97A7353
SHA-256:	E1315C41F50A75C308CDB023F7E48C0AA62931D5771AD8BC4220018ED5D7F976
SHA-512:	8A75925B0695284105856823190531DC4CFCF32A8AE3226EF8C1F796185AA01F8C085B6457A63B1CF81842DA2C6BAAFD4CABF7565A8D96D3460054439BBFB798
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....E[Z....E[X.D..E[Y....ogl.....b.....,8`.....b...'..b .....b.T.....<....b.....Rich.....PE..d...5..]..... ".....0....K...W...K....@.....X.....`.....W.....W..+....U..... .....W.....`.W.(.....W.....UPX0.....K.....UPX1..... ....K.....@....rsrc....0....W..... ".....@..... ....3.93.UPX!.$..

C:\Windows\Help\Winlogon.exe

Process:	C:\Users\user\AppData\Roaming\22.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	76248
Entropy (8bit):	6.357076953831382
Encrypted:	false
SSDEEP:	1536:WH8tImFvh/tAoX/V1d/Xc81qsWjcdTxekxemB:WH8imz/H111TxfAmB
MD5:	A8DDACE9435FE395325FC45DDE8BD0A3
SHA1:	DCF9BAAA9E3A27450DEBF4F35112376ED005C800
SHA-256:	6E81D7C71B3E8D731E11AD75D3DAC02A4210C9F90FAC618AF5C00CBCE3718658
SHA-512:	2C6006E42ECF31DA02A4584E69C0E55390BE5A40535330758285272 8B2CEB65033F3F5CD0B6465B3A1541D19EAB95C61B394E3403DEE558196C2F2969D82B196
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x...<O..<O..<O..1..$O..1..3O..1..ZO..A6.?O..57..>O..<O..pO..A6 ..=O..1..=O..<O..=O..A6.=O..Rich<O.....PE..L...K..Y.....@.....P.....@.....<....0..`.....@..l... @...8.....@.....text..... ..`.rdata..tF.....H.....@..@.data....0.....@....rsrc...`....0..... .....@..@.reloc..l....@.....@..B..... .....

C:\Windows\Help\active_desktop_render.dll

Process:	C:\Users\user\AppData\Roaming\22.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	995328
Entropy (8bit):	6.19848257170581
Encrypted:	false
SSDEEP:	12288:BT8s5nv9sQ1ViVNEPazI+eGGhFqxVOa+28WXvC:BT8MnlsQ1kVqPv+eDhGwdlvC
MD5:	07A36097730666FE9E5434D85A5AB989
SHA1:	780CA47C15932ED1F9640C17B9BB340410A52338
SHA-256:	1FB4CEE4D83D424E0BFCBFD97169EF717B3EBDCC5D01BA7C7C547AE606AD5C3C
SHA-512:	4A08080471C660856AF724E4480EC721C22C462346E293D93E2F9577E6D669C6B51CD81EF96DFAD943C791DFD7F7F0C2D5234A82D81CE5F1C01BB493CDA3408

Malicious:	**true**
Yara Hits:	• Rule: MALWARE_Win_BlackMoon, Description: Detects executables using BlackMoon RunTime, Source: C:\Windows\Help\active_desktop_render.dll, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .....`..... .....Rich..... PE..L...Kw.]..... !.....@.....m.....P.....p.....y.....0.. .....@.....P..t.....t ext...J:.....@..... ..`.rdata...=...P...@...P.....@..@.data.....P.....@....rsrc... ....0.....@..@.reloc...3...@...@.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.788951719729708
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.63% • Win32 Executable (generic) a (10002005/4) 49.58% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.41% • InstallShield setup (43055/19) 0.21% • UPX compressed Win32 Executable (30571/9) 0.15%
File name:	RIP_YOUR_PC_LOL.exe
File size:	23633920
MD5:	52867174362410d63215d78e708103ea
SHA1:	7ae4e1048e4463a4201bdeaf224c5b6face681bf
SHA256:	37d8e1ce3b6e6488942717aa78cb54785edc985143bcc8d9ba9f42d73a3dbd7a
SHA512:	89e17e147d3f073e479e85d0b0321f6264bbc2aa84c930ed645e8f5cde3f1e58812c3db1ba0f10bee6ce7ac0731e1e3de6747a9b3c4d63a564dd8d904bd726ab
SSDEEP:	393216:HJLgf7BPkdKzrZciLxv8naSNtPr5rn57M84UTB9xO5/VWvJKJPkwdnfZ4y5SDkFV:poBPQwxMR7pn5qUTB9xOFVWvJKJPkwd9
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...e..a.....h.....h.. ....h...@.. .....i.....@.....

File Icon



Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x1a8b4ae
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61B51365 [Sat Dec 11 21:08:53 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x168b454	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x168c000	0x598	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x168e000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x16894b4	0x1689600	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x168c000	0x598	0x600	False	0.421223958333	data	4.08611300158	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x168e000	0xc	0x200	False	0.044921875	data	0.118369631259	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x168c0a0	0x304	data		
RT_MANIFEST	0x168c3a8	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	emerge brutal
Assembly Version	14.5.48.86
InternalName	foampounding.exe
FileVersion	14.5.48.86
CompanyName	brawler
ProductName	open
ProductVersion	14.5.48.86
FileDescription	earfalserust
OriginalFilename	foampounding.exe

Network Behavior

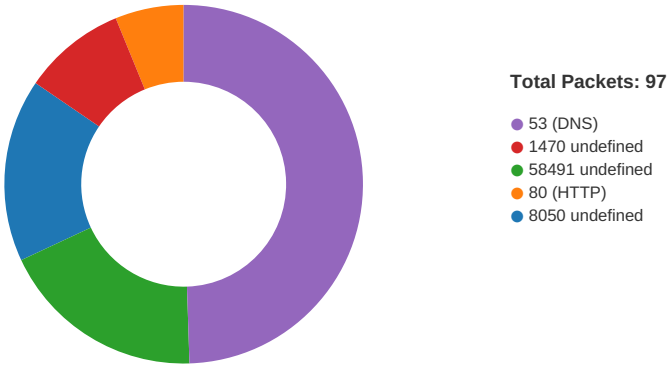
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
03/08/22-18:01:02.530765	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51748	8.8.8.8	192.168.2.6
03/08/22-18:01:29.841168	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49695	8.8.8.8	192.168.2.6
03/08/22-18:01:52.276662	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61607	8.8.8.8	192.168.2.6
03/08/22-18:02:29.169253	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52858	8.8.8.8	192.168.2.6
03/08/22-18:02:48.436398	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59871	8.8.8.8	192.168.2.6
03/08/22-18:02:48.491531	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50029	8.8.8.8	192.168.2.6
03/08/22-18:02:48.738596	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51194	8.8.8.8	192.168.2.6
03/08/22-18:02:53.688495	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50081	8.8.8.8	192.168.2.6
03/08/22-18:02:56.227160	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55083	8.8.8.8	192.168.2.6
03/08/22-18:02:58.743158	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59106	8.8.8.8	192.168.2.6
03/08/22-18:03:09.787643	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61152	8.8.8.8	192.168.2.6

Copyright Joe Security LLC 2022

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
03/08/22-18:03:11.689559	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49679	8.8.8.8	192.168.2.6
03/08/22-18:03:22.042737	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52225	8.8.8.8	192.168.2.6

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 8, 2022 18:01:02.549043894 CET	49768	8050	192.168.2.6	179.13.1.253
Mar 8, 2022 18:01:05.605629921 CET	49768	8050	192.168.2.6	179.13.1.253
Mar 8, 2022 18:01:11.606240988 CET	49768	8050	192.168.2.6	179.13.1.253
Mar 8, 2022 18:01:21.307589054 CET	49770	80	192.168.2.6	52.20.78.240
Mar 8, 2022 18:01:21.448190928 CET	80	49770	52.20.78.240	192.168.2.6
Mar 8, 2022 18:01:21.448342085 CET	49770	80	192.168.2.6	52.20.78.240
Mar 8, 2022 18:01:21.456914902 CET	49770	80	192.168.2.6	52.20.78.240
Mar 8, 2022 18:01:21.596329927 CET	80	49770	52.20.78.240	192.168.2.6
Mar 8, 2022 18:01:21.597302914 CET	80	49770	52.20.78.240	192.168.2.6
Mar 8, 2022 18:01:21.597403049 CET	49770	80	192.168.2.6	52.20.78.240
Mar 8, 2022 18:01:22.363976955 CET	49771	80	192.168.2.6	80.87.192.115
Mar 8, 2022 18:01:22.423902035 CET	80	49771	80.87.192.115	192.168.2.6
Mar 8, 2022 18:01:22.424120903 CET	49771	80	192.168.2.6	80.87.192.115
Mar 8, 2022 18:01:29.900438070 CET	49772	8050	192.168.2.6	179.13.1.253
Mar 8, 2022 18:01:32.904844999 CET	49772	8050	192.168.2.6	179.13.1.253
Mar 8, 2022 18:01:38.999099016 CET	49772	8050	192.168.2.6	179.13.1.253
Mar 8, 2022 18:01:50.012576103 CET	49773	58491	192.168.2.6	172.98.92.42
Mar 8, 2022 18:01:50.126136065 CET	58491	49773	172.98.92.42	192.168.2.6
Mar 8, 2022 18:01:50.812603951 CET	49773	58491	192.168.2.6	172.98.92.42
Mar 8, 2022 18:01:50.926179886 CET	58491	49773	172.98.92.42	192.168.2.6
Mar 8, 2022 18:01:51.429456949 CET	49773	58491	192.168.2.6	172.98.92.42
Mar 8, 2022 18:01:51.544755936 CET	58491	49773	172.98.92.42	192.168.2.6
Mar 8, 2022 18:01:52.529678106 CET	49774	1470	192.168.2.6	41.249.51.34
Mar 8, 2022 18:01:55.610013008 CET	49774	1470	192.168.2.6	41.249.51.34
Mar 8, 2022 18:01:56.268575907 CET	49775	8050	192.168.2.6	179.13.1.253
Mar 8, 2022 18:01:59.313349009 CET	49775	8050	192.168.2.6	179.13.1.253
Mar 8, 2022 18:02:01.610399961 CET	49774	1470	192.168.2.6	41.249.51.34
Mar 8, 2022 18:02:05.313823938 CET	49775	8050	192.168.2.6	179.13.1.253
Mar 8, 2022 18:02:05.928004980 CET	49776	58491	192.168.2.6	172.98.92.42
Mar 8, 2022 18:02:06.042727947 CET	58491	49776	172.98.92.42	192.168.2.6
Mar 8, 2022 18:02:06.642051935 CET	49776	58491	192.168.2.6	172.98.92.42
Mar 8, 2022 18:02:06.756652117 CET	58491	49776	172.98.92.42	192.168.2.6
Mar 8, 2022 18:02:07.345288038 CET	49776	58491	192.168.2.6	172.98.92.42
Mar 8, 2022 18:02:07.460087061 CET	58491	49776	172.98.92.42	192.168.2.6

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 8, 2022 18:02:21.598696947 CET	80	49770	52.20.78.240	192.168.2.6
Mar 8, 2022 18:02:21.623155117 CET	49770	80	192.168.2.6	52.20.78.240
Mar 8, 2022 18:02:22.540772915 CET	80	49771	80.87.192.115	192.168.2.6
Mar 8, 2022 18:02:22.544246912 CET	49771	80	192.168.2.6	80.87.192.115
Mar 8, 2022 18:02:29.260555983 CET	49777	8050	192.168.2.6	179.13.1.253
Mar 8, 2022 18:02:32.348848104 CET	49777	8050	192.168.2.6	179.13.1.253
Mar 8, 2022 18:02:38.443535089 CET	49777	8050	192.168.2.6	179.13.1.253
Mar 8, 2022 18:02:41.668142080 CET	49778	58491	192.168.2.6	172.98.92.42
Mar 8, 2022 18:02:41.783175945 CET	58491	49778	172.98.92.42	192.168.2.6
Mar 8, 2022 18:02:42.302769899 CET	49778	58491	192.168.2.6	172.98.92.42
Mar 8, 2022 18:02:42.417251110 CET	58491	49778	172.98.92.42	192.168.2.6
Mar 8, 2022 18:02:43.115386009 CET	49778	58491	192.168.2.6	172.98.92.42
Mar 8, 2022 18:02:43.230278015 CET	58491	49778	172.98.92.42	192.168.2.6
Mar 8, 2022 18:02:48.515594006 CET	49780	1470	192.168.2.6	41.249.51.34
Mar 8, 2022 18:02:51.537960052 CET	49780	1470	192.168.2.6	41.249.51.34
Mar 8, 2022 18:02:55.695036888 CET	49793	8050	192.168.2.6	179.13.1.253
Mar 8, 2022 18:02:57.647829056 CET	49780	1470	192.168.2.6	41.249.51.34
Mar 8, 2022 18:02:58.804176092 CET	49793	8050	192.168.2.6	179.13.1.253
Mar 8, 2022 18:03:02.885044098 CET	49804	58491	192.168.2.6	172.98.92.42
Mar 8, 2022 18:03:02.999629974 CET	58491	49804	172.98.92.42	192.168.2.6
Mar 8, 2022 18:03:03.617047071 CET	49804	58491	192.168.2.6	172.98.92.42
Mar 8, 2022 18:03:03.731703043 CET	58491	49804	172.98.92.42	192.168.2.6
Mar 8, 2022 18:03:04.304689884 CET	49804	58491	192.168.2.6	172.98.92.42
Mar 8, 2022 18:03:04.419482946 CET	58491	49804	172.98.92.42	192.168.2.6
Mar 8, 2022 18:03:04.804677963 CET	49793	8050	192.168.2.6	179.13.1.253
Mar 8, 2022 18:03:08.456417084 CET	49815	58491	192.168.2.6	172.98.92.42
Mar 8, 2022 18:03:08.571064949 CET	58491	49815	172.98.92.42	192.168.2.6
Mar 8, 2022 18:03:09.117554903 CET	49815	58491	192.168.2.6	172.98.92.42
Mar 8, 2022 18:03:09.232285976 CET	58491	49815	172.98.92.42	192.168.2.6
Mar 8, 2022 18:03:09.806243896 CET	49815	58491	192.168.2.6	172.98.92.42
Mar 8, 2022 18:03:09.920924902 CET	58491	49815	172.98.92.42	192.168.2.6
Mar 8, 2022 18:03:10.235430956 CET	49770	80	192.168.2.6	52.20.78.240
Mar 8, 2022 18:03:10.375109911 CET	80	49770	52.20.78.240	192.168.2.6
Mar 8, 2022 18:03:11.695297003 CET	49820	1470	192.168.2.6	41.249.51.34
Mar 8, 2022 18:03:13.931397915 CET	49825	58491	192.168.2.6	172.98.92.42
Mar 8, 2022 18:03:14.047744036 CET	58491	49825	172.98.92.42	192.168.2.6
Mar 8, 2022 18:03:14.618395090 CET	49825	58491	192.168.2.6	172.98.92.42
Mar 8, 2022 18:03:14.733145952 CET	58491	49825	172.98.92.42	192.168.2.6
Mar 8, 2022 18:03:14.805542946 CET	49820	1470	192.168.2.6	41.249.51.34
Mar 8, 2022 18:03:15.306822062 CET	49825	58491	192.168.2.6	172.98.92.42
Mar 8, 2022 18:03:15.421253920 CET	58491	49825	172.98.92.42	192.168.2.6
Mar 8, 2022 18:03:20.806010008 CET	49820	1470	192.168.2.6	41.249.51.34
Mar 8, 2022 18:03:22.143265009 CET	49838	8050	192.168.2.6	179.13.1.253

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 8, 2022 18:00:25.222332954 CET	56591	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:01:02.421529055 CET	51748	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:01:02.530765057 CET	53	51748	8.8.8.8	192.168.2.6
Mar 8, 2022 18:01:21.131813049 CET	50958	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:01:21.159094095 CET	53	50958	8.8.8.8	192.168.2.6
Mar 8, 2022 18:01:29.731457949 CET	49695	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:01:29.841167927 CET	53	49695	8.8.8.8	192.168.2.6
Mar 8, 2022 18:01:52.253196955 CET	61607	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:01:52.276662111 CET	53	61607	8.8.8.8	192.168.2.6
Mar 8, 2022 18:01:56.196608067 CET	56550	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:01:56.216669083 CET	53	56550	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 8, 2022 18:02:29.062084913 CET	52858	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:02:29.169253111 CET	53	52858	8.8.8.8	192.168.2.6
Mar 8, 2022 18:02:48.149482012 CET	50029	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:02:48.414717913 CET	59871	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:02:48.427118063 CET	51194	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:02:48.436398029 CET	53	59871	8.8.8.8	192.168.2.6
Mar 8, 2022 18:02:48.491530895 CET	53	50029	8.8.8.8	192.168.2.6
Mar 8, 2022 18:02:48.514926910 CET	51666	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:02:48.538808107 CET	53	51666	8.8.8.8	192.168.2.6
Mar 8, 2022 18:02:48.738595963 CET	53	51194	8.8.8.8	192.168.2.6
Mar 8, 2022 18:02:49.711517096 CET	57037	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:02:49.731496096 CET	53	57037	8.8.8.8	192.168.2.6
Mar 8, 2022 18:02:50.793032885 CET	60609	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:02:50.815732956 CET	53	60609	8.8.8.8	192.168.2.6
Mar 8, 2022 18:02:50.939651012 CET	54529	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:02:50.959239960 CET	53	54529	8.8.8.8	192.168.2.6
Mar 8, 2022 18:02:51.056174994 CET	62643	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:02:51.073822021 CET	53	62643	8.8.8.8	192.168.2.6
Mar 8, 2022 18:02:52.364578009 CET	54015	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:02:52.455807924 CET	53	54015	8.8.8.8	192.168.2.6
Mar 8, 2022 18:02:52.476210117 CET	52089	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:02:52.546967030 CET	53	52089	8.8.8.8	192.168.2.6
Mar 8, 2022 18:02:52.577049971 CET	54489	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:02:52.664900064 CET	53	54489	8.8.8.8	192.168.2.6
Mar 8, 2022 18:02:52.879266024 CET	52698	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:02:52.967892885 CET	53	52698	8.8.8.8	192.168.2.6
Mar 8, 2022 18:02:53.016813040 CET	53829	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:02:53.099018097 CET	53	53829	8.8.8.8	192.168.2.6
Mar 8, 2022 18:02:53.111742973 CET	61901	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:02:53.208043098 CET	53	61901	8.8.8.8	192.168.2.6
Mar 8, 2022 18:02:53.250925064 CET	58689	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:02:53.341078997 CET	53	58689	8.8.8.8	192.168.2.6
Mar 8, 2022 18:02:53.351939917 CET	50081	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:02:53.688494921 CET	53	50081	8.8.8.8	192.168.2.6
Mar 8, 2022 18:02:54.809392929 CET	49520	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:02:54.902901888 CET	65526	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:02:55.664746046 CET	53049	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:02:55.684472084 CET	53	53049	8.8.8.8	192.168.2.6
Mar 8, 2022 18:02:55.762953997 CET	52965	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:02:55.834017038 CET	53	52965	8.8.8.8	192.168.2.6
Mar 8, 2022 18:02:55.837884903 CET	52125	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:02:55.930027962 CET	55083	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:02:55.939817905 CET	53	52125	8.8.8.8	192.168.2.6
Mar 8, 2022 18:02:56.227159977 CET	53	55083	8.8.8.8	192.168.2.6
Mar 8, 2022 18:02:56.465817928 CET	58360	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:02:56.485572100 CET	53	58360	8.8.8.8	192.168.2.6
Mar 8, 2022 18:02:56.742223978 CET	56071	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:02:57.091926098 CET	53	56071	8.8.8.8	192.168.2.6
Mar 8, 2022 18:02:58.431301117 CET	59106	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:02:58.743158102 CET	53	59106	8.8.8.8	192.168.2.6
Mar 8, 2022 18:03:00.852693081 CET	61113	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:03:00.870723009 CET	53	61113	8.8.8.8	192.168.2.6
Mar 8, 2022 18:03:03.026786089 CET	60658	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:03:03.046681881 CET	53	60658	8.8.8.8	192.168.2.6
Mar 8, 2022 18:03:05.181277037 CET	60238	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:03:05.199376106 CET	53	60238	8.8.8.8	192.168.2.6
Mar 8, 2022 18:03:07.321696043 CET	65367	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:03:07.343290091 CET	53	65367	8.8.8.8	192.168.2.6
Mar 8, 2022 18:03:09.462516069 CET	61152	53	192.168.2.6	8.8.8.8

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 8, 2022 18:03:09.787642956 CET	53	61152	8.8.8.8	192.168.2.6
Mar 8, 2022 18:03:11.455007076 CET	64544	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:03:11.490103006 CET	53	64544	8.8.8.8	192.168.2.6
Mar 8, 2022 18:03:11.667885065 CET	49679	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:03:11.689558983 CET	53	49679	8.8.8.8	192.168.2.6
Mar 8, 2022 18:03:11.855283022 CET	60361	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:03:11.875169992 CET	53	60361	8.8.8.8	192.168.2.6
Mar 8, 2022 18:03:13.742429972 CET	63771	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:03:13.761302948 CET	53	63771	8.8.8.8	192.168.2.6
Mar 8, 2022 18:03:13.962951899 CET	64579	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:03:13.984797001 CET	53	64579	8.8.8.8	192.168.2.6
Mar 8, 2022 18:03:16.135138988 CET	58801	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:03:16.157701969 CET	53	58801	8.8.8.8	192.168.2.6
Mar 8, 2022 18:03:18.356760979 CET	61571	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:03:18.376470089 CET	53	61571	8.8.8.8	192.168.2.6
Mar 8, 2022 18:03:20.463649035 CET	49463	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:03:20.481589079 CET	53	49463	8.8.8.8	192.168.2.6
Mar 8, 2022 18:03:21.935733080 CET	52225	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:03:22.042737007 CET	53	52225	8.8.8.8	192.168.2.6
Mar 8, 2022 18:03:23.130189896 CET	55342	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:03:23.148067951 CET	53	55342	8.8.8.8	192.168.2.6
Mar 8, 2022 18:03:23.273044109 CET	49754	53	192.168.2.6	8.8.8.8
Mar 8, 2022 18:03:23.588294983 CET	53	49754	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 8, 2022 18:00:25.222332954 CET	192.168.2.6	8.8.8.8	0x72ed	Standard query (0)	store-images.s-microsoft.com	A (IP address)	IN (0x0001)
Mar 8, 2022 18:01:02.421529055 CET	192.168.2.6	8.8.8.8	0xf287	Standard query (0)	gfhhjgh.duckdns.org	A (IP address)	IN (0x0001)
Mar 8, 2022 18:01:21.131813049 CET	192.168.2.6	8.8.8.8	0x6641	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Mar 8, 2022 18:01:29.731457949 CET	192.168.2.6	8.8.8.8	0xd006	Standard query (0)	gfhhjgh.duckdns.org	A (IP address)	IN (0x0001)
Mar 8, 2022 18:01:52.253196955 CET	192.168.2.6	8.8.8.8	0xa2d	Standard query (0)	kazya1.hopto.org	A (IP address)	IN (0x0001)
Mar 8, 2022 18:01:56.196608067 CET	192.168.2.6	8.8.8.8	0xf35b	Standard query (0)	gfhhjgh.duckdns.org	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:29.062084913 CET	192.168.2.6	8.8.8.8	0xb207	Standard query (0)	gfhhjgh.duckdns.org	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:48.149482012 CET	192.168.2.6	8.8.8.8	0x541d	Standard query (0)	hackerinvasion.f3322.net	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:48.414717913 CET	192.168.2.6	8.8.8.8	0x771c	Standard query (0)	kazya1.hopto.org	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:48.427118063 CET	192.168.2.6	8.8.8.8	0x1458	Standard query (0)	hackerinvasion.f3322.net	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:48.514926910 CET	192.168.2.6	8.8.8.8	0x249f	Standard query (0)	yabynennet.xyz	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:49.711517096 CET	192.168.2.6	8.8.8.8	0x1de0	Standard query (0)	123.105.12.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Mar 8, 2022 18:02:50.793032885 CET	192.168.2.6	8.8.8.8	0x2c	Standard query (0)	whatismyipaddress.com	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:50.939651012 CET	192.168.2.6	8.8.8.8	0x1b81	Standard query (0)	whatismyipaddress.com	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:51.056174994 CET	192.168.2.6	8.8.8.8	0xa95e	Standard query (0)	hackerinvasion.f3322.net	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:52.364578009 CET	192.168.2.6	8.8.8.8	0x658b	Standard query (0)	prepepe.ac.ug	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:52.476210117 CET	192.168.2.6	8.8.8.8	0xb173	Standard query (0)	prepepe.ac.ug	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:52.577049971 CET	192.168.2.6	8.8.8.8	0xc570	Standard query (0)	prepepe.ac.ug	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:52.879266024 CET	192.168.2.6	8.8.8.8	0x28df	Standard query (0)	prepepe.ac.ug	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 8, 2022 18:02:53.016813040 CET	192.168.2.6	8.8.8.8	0x7f0c	Standard query (0)	prepepe.ac.ug	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:53.111742973 CET	192.168.2.6	8.8.8.8	0x73f9	Standard query (0)	prepepe.ac.ug	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:53.250925064 CET	192.168.2.6	8.8.8.8	0x59e3	Standard query (0)	prepepe.ac.ug	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:53.351939917 CET	192.168.2.6	8.8.8.8	0x1e6	Standard query (0)	hackerinvasion.f3322.net	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:54.809392929 CET	192.168.2.6	8.8.8.8	0x5dd4	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:54.902901888 CET	192.168.2.6	8.8.8.8	0x4a0c	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:55.664746046 CET	192.168.2.6	8.8.8.8	0xd501	Standard query (0)	gfhhjgh.duckdns.org	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:55.762953997 CET	192.168.2.6	8.8.8.8	0x259d	Standard query (0)	pretorian.ac.ug	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:55.837884903 CET	192.168.2.6	8.8.8.8	0x66da	Standard query (0)	pretorian.ac.ug	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:55.930027962 CET	192.168.2.6	8.8.8.8	0x349d	Standard query (0)	hackerinvasion.f3322.net	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:56.465817928 CET	192.168.2.6	8.8.8.8	0xa4a5	Standard query (0)	22ssh.com	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:56.742223978 CET	192.168.2.6	8.8.8.8	0xeaa	Standard query (0)	pool.usa-138.com	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:58.431301117 CET	192.168.2.6	8.8.8.8	0x8329	Standard query (0)	hackerinvasion.f3322.net	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:00.852693081 CET	192.168.2.6	8.8.8.8	0x4b12	Standard query (0)	hackerinvasion.f3322.net	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:03.026786089 CET	192.168.2.6	8.8.8.8	0x131b	Standard query (0)	hackerinvasion.f3322.net	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:05.181277037 CET	192.168.2.6	8.8.8.8	0xff00	Standard query (0)	hackerinvasion.f3322.net	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:07.321696043 CET	192.168.2.6	8.8.8.8	0xd5e2	Standard query (0)	hackerinvasion.f3322.net	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:09.462516069 CET	192.168.2.6	8.8.8.8	0x8118	Standard query (0)	hackerinvasion.f3322.net	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:11.455007076 CET	192.168.2.6	8.8.8.8	0x9cb7	Standard query (0)	files.000webhost.com	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:11.667885065 CET	192.168.2.6	8.8.8.8	0x6983	Standard query (0)	kazya1.hopto.org	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:11.855283022 CET	192.168.2.6	8.8.8.8	0x9062	Standard query (0)	hackerinvasion.f3322.net	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:13.742429972 CET	192.168.2.6	8.8.8.8	0x204b	Standard query (0)	22ssh.com	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:13.962951899 CET	192.168.2.6	8.8.8.8	0xd1b5	Standard query (0)	hackerinvasion.f3322.net	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:16.135138988 CET	192.168.2.6	8.8.8.8	0xcac2	Standard query (0)	hackerinvasion.f3322.net	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:18.356760979 CET	192.168.2.6	8.8.8.8	0x9ff	Standard query (0)	hackerinvasion.f3322.net	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:20.463649035 CET	192.168.2.6	8.8.8.8	0xa314	Standard query (0)	hackerinvasion.f3322.net	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:21.935733080 CET	192.168.2.6	8.8.8.8	0x52d3	Standard query (0)	gfhhjgh.duckdns.org	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:23.130189896 CET	192.168.2.6	8.8.8.8	0xecc7	Standard query (0)	hackerinvasion.f3322.net	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:23.273044109 CET	192.168.2.6	8.8.8.8	0xc444	Standard query (0)	pool.usa-138.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 8, 2022 18:00:25.247078896 CET	8.8.8.8	192.168.2.6	0x72ed	No error (0)	store-images.s-microsoft.com	store-images.s-microsoft.com-c.edgekey.net		CNAME (Canonical name)	IN (0x0001)
Mar 8, 2022 18:01:02.530765057 CET	8.8.8.8	192.168.2.6	0xf287	No error (0)	gfhhjgh.duckdns.org		179.13.1.253	A (IP address)	IN (0x0001)
Mar 8, 2022 18:01:21.159094095 CET	8.8.8.8	192.168.2.6	0x6641	No error (0)	api.ipify.org	api.ipify.org.herokudns.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 8, 2022 18:01:21.159094095 CET	8.8.8.8	192.168.2.6	0x6641	No error (0)	api.ipify.org.herokudns.com		52.20.78.240	A (IP address)	IN (0x0001)
Mar 8, 2022 18:01:21.159094095 CET	8.8.8.8	192.168.2.6	0x6641	No error (0)	api.ipify.org.herokudns.com		3.232.242.170	A (IP address)	IN (0x0001)
Mar 8, 2022 18:01:21.159094095 CET	8.8.8.8	192.168.2.6	0x6641	No error (0)	api.ipify.org.herokudns.com		3.220.57.224	A (IP address)	IN (0x0001)
Mar 8, 2022 18:01:21.159094095 CET	8.8.8.8	192.168.2.6	0x6641	No error (0)	api.ipify.org.herokudns.com		54.91.59.199	A (IP address)	IN (0x0001)
Mar 8, 2022 18:01:29.841167927 CET	8.8.8.8	192.168.2.6	0xd006	No error (0)	gfhhjgh.duckdns.org		179.13.1.253	A (IP address)	IN (0x0001)
Mar 8, 2022 18:01:52.276662111 CET	8.8.8.8	192.168.2.6	0xa2d	No error (0)	kazya1.hopto.org		41.249.51.34	A (IP address)	IN (0x0001)
Mar 8, 2022 18:01:56.216669083 CET	8.8.8.8	192.168.2.6	0xf35b	No error (0)	gfhhjgh.duckdns.org		179.13.1.253	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:29.169253111 CET	8.8.8.8	192.168.2.6	0xb207	No error (0)	gfhhjgh.duckdns.org		179.13.1.253	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:48.436398029 CET	8.8.8.8	192.168.2.6	0x771c	No error (0)	kazya1.hopto.org		41.249.51.34	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:48.491530895 CET	8.8.8.8	192.168.2.6	0x541d	No error (0)	hackerinvasion.f3322.net		127.0.0.1	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:48.538808107 CET	8.8.8.8	192.168.2.6	0x249f	No error (0)	yabynennet.xyz		45.129.99.212	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:48.738595963 CET	8.8.8.8	192.168.2.6	0x1458	No error (0)	hackerinvasion.f3322.net		127.0.0.1	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:49.731496096 CET	8.8.8.8	192.168.2.6	0x1de0	Name error (3)	123.105.12.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Mar 8, 2022 18:02:50.815732956 CET	8.8.8.8	192.168.2.6	0x2c	No error (0)	whatismyipaddress.com		104.16.154.36	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:50.815732956 CET	8.8.8.8	192.168.2.6	0x2c	No error (0)	whatismyipaddress.com		104.16.155.36	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:50.959239960 CET	8.8.8.8	192.168.2.6	0x1b81	No error (0)	whatismyipaddress.com		104.16.154.36	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:50.959239960 CET	8.8.8.8	192.168.2.6	0x1b81	No error (0)	whatismyipaddress.com		104.16.155.36	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:51.073822021 CET	8.8.8.8	192.168.2.6	0xa95e	No error (0)	hackerinvasion.f3322.net		127.0.0.1	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:52.455807924 CET	8.8.8.8	192.168.2.6	0x658b	Server failure (2)	prepepe.ac.ug	none	none	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:52.546967030 CET	8.8.8.8	192.168.2.6	0xb173	Server failure (2)	prepepe.ac.ug	none	none	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:52.664900064 CET	8.8.8.8	192.168.2.6	0xc570	Server failure (2)	prepepe.ac.ug	none	none	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:52.967892885 CET	8.8.8.8	192.168.2.6	0x28df	Server failure (2)	prepepe.ac.ug	none	none	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:53.099018097 CET	8.8.8.8	192.168.2.6	0x7f0c	Server failure (2)	prepepe.ac.ug	none	none	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:53.208043098 CET	8.8.8.8	192.168.2.6	0x73f9	Server failure (2)	prepepe.ac.ug	none	none	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:53.341078997 CET	8.8.8.8	192.168.2.6	0x59e3	Server failure (2)	prepepe.ac.ug	none	none	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:53.688494921 CET	8.8.8.8	192.168.2.6	0x1e6	No error (0)	hackerinvasion.f3322.net		127.0.0.1	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:54.832865000 CET	8.8.8.8	192.168.2.6	0x5dd4	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Mar 8, 2022 18:02:54.924410105 CET	8.8.8.8	192.168.2.6	0x4a0c	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Mar 8, 2022 18:02:55.684472084 CET	8.8.8.8	192.168.2.6	0xd501	No error (0)	gfhhjgh.duckdns.org		179.13.1.253	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:55.834017038 CET	8.8.8.8	192.168.2.6	0x259d	Server failure (2)	pretorian.ac.ug	none	none	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:55.903019905 CET	8.8.8.8	192.168.2.6	0x3236	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Mar 8, 2022 18:02:55.939817905 CET	8.8.8.8	192.168.2.6	0x66da	Server failure (2)	pretorian.ac.ug	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 8, 2022 18:02:56.227159977 CET	8.8.8.8	192.168.2.6	0x349d	No error (0)	hackerinvasion.f3322.net		127.0.0.1	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:57.091926098 CET	8.8.8.8	192.168.2.6	0xeaa	No error (0)	pool.usa-138.com		220.86.85.75	A (IP address)	IN (0x0001)
Mar 8, 2022 18:02:58.743158102 CET	8.8.8.8	192.168.2.6	0x8329	No error (0)	hackerinvasion.f3322.net		127.0.0.1	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:00.870723009 CET	8.8.8.8	192.168.2.6	0x4b12	No error (0)	hackerinvasion.f3322.net		127.0.0.1	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:03.046681881 CET	8.8.8.8	192.168.2.6	0x131b	No error (0)	hackerinvasion.f3322.net		127.0.0.1	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:05.199376106 CET	8.8.8.8	192.168.2.6	0xff00	No error (0)	hackerinvasion.f3322.net		127.0.0.1	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:07.343290091 CET	8.8.8.8	192.168.2.6	0xd5e2	No error (0)	hackerinvasion.f3322.net		127.0.0.1	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:09.787642956 CET	8.8.8.8	192.168.2.6	0x8118	No error (0)	hackerinvasion.f3322.net		127.0.0.1	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:11.490103006 CET	8.8.8.8	192.168.2.6	0x9cb7	No error (0)	files.000webhost.com	us-east-1.route-1000.000webhost.awex.io		CNAME (Canonical name)	IN (0x0001)
Mar 8, 2022 18:03:11.490103006 CET	8.8.8.8	192.168.2.6	0x9cb7	No error (0)	us-east-1.route-1000.000webhost.awex.io		145.14.144.149	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:11.689558983 CET	8.8.8.8	192.168.2.6	0x6983	No error (0)	kazya1.hopto.org		41.249.51.34	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:11.875169992 CET	8.8.8.8	192.168.2.6	0x9062	No error (0)	hackerinvasion.f3322.net		127.0.0.1	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:13.984797001 CET	8.8.8.8	192.168.2.6	0xd1b5	No error (0)	hackerinvasion.f3322.net		127.0.0.1	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:16.157701969 CET	8.8.8.8	192.168.2.6	0xcac2	No error (0)	hackerinvasion.f3322.net		127.0.0.1	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:18.376470089 CET	8.8.8.8	192.168.2.6	0x9ff	No error (0)	hackerinvasion.f3322.net		127.0.0.1	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:20.481589079 CET	8.8.8.8	192.168.2.6	0xa314	No error (0)	hackerinvasion.f3322.net		127.0.0.1	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:22.042737007 CET	8.8.8.8	192.168.2.6	0x52d3	No error (0)	gfhhjgh.duckdns.org		179.13.1.253	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:23.148067951 CET	8.8.8.8	192.168.2.6	0xecc7	No error (0)	hackerinvasion.f3322.net		127.0.0.1	A (IP address)	IN (0x0001)
Mar 8, 2022 18:03:23.588294983 CET	8.8.8.8	192.168.2.6	0xc444	No error (0)	pool.usa-138.com		220.86.85.75	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- api.ipify.org

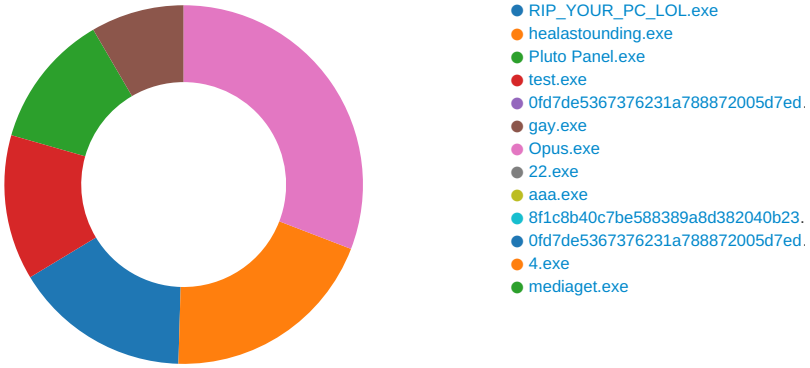
HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49770	52.20.78.240	80	C:\Users\user\AppData\Roaming\0fd7de5367376231a788872005d7ed4f.exe

Timestamp	kBytes transferred	Direction	Data
Mar 8, 2022 18:01:21.456914902 CET	1230	OUT	GET /?format=xml HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: api.ipify.org Connection: Keep-Alive
Mar 8, 2022 18:01:21.597302914 CET	1230	IN	HTTP/1.1 200 OK Server: Cowboy Connection: keep-alive Content-Type: text/plain Vary: Origin Date: Tue, 08 Mar 2022 17:01:21 GMT Content-Length: 10 Via: 1.1 vegur Data Raw: 38 34 2e 31 37 2e 35 32 2e 37 Data Ascii: 84.17.52.7

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: RIP_YOUR_PC_LOL.exe PID: **6880**, Parent PID: **408**

General

Target ID:	0
Start time:	18:00:31
Start date:	08/03/2022
Path:	C:\Users\user\Desktop\RIP_YOUR_PC_LOL.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\RIP_YOUR_PC_LOL.exe"
Imagebase:	0x9f0000
File size:	23633920 bytes
MD5 hash:	52867174362410D63215D78E708103EA
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: 00000000.00000003.388952115.00000000059C7000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: 00000000.00000003.388952115.00000000059C7000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000000.00000000.374606826.0000000001F6B000.00000002.00000001.01000000.00000003.sdmp, Author: Florian Roth • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000000.00000000.374606826.0000000001F6B000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: 00000000.00000000.374606826.0000000001F6B000.00000002.00000001.01000000.00000003.sdmp, Author: ditekSHen • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000000.00000002.693319449.0000000001F6B000.00000002.00000001.01000000.00000003.sdmp, Author: Florian Roth • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000000.00000002.693319449.0000000001F6B000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: 00000000.00000002.693319449.0000000001F6B000.00000002.00000001.01000000.00000003.sdmp, Author: ditekSHen • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000000.366341482.00000000009F2000.00000002.00000001.01000000.00000003.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000000.366341482.00000000009F2000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000000.366341482.00000000009F2000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000000.366341482.00000000009F2000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000000.366341482.00000000009F2000.00000002.00000001.01000000.00000003.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.502131214.00000000009F2000.00000002.00000001.01000000.00000003.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.502131214.00000000009F2000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.502131214.00000000009F2000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.502131214.00000000009F2000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.502131214.00000000009F2000.00000002.00000001.01000000.00000003.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000000.00000003.386628983.00000000056F5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000000.00000003.386628983.00000000056F5000.00000004.00000800.00020000.00000000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000000.371829021.0000000001893000.00000002.00000001.01000000.00000003.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000000.371829021.0000000001893000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000000.00000000.371829021.0000000001893000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000000.371829021.0000000001893000.00000002.00000001.01000000.00000003.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: njrat1, Description: Identify njRat, Source: 00000000.00000000.371829021.0000000001893000.00000002.00000001.01000000.00000003.sdmp, Author: Brian Wallace @botnet_hunter • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000003.437188672.00000000056F5000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000003.437188672.00000000056F5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000003.437188672.00000000056F5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000003.437188672.00000000056F5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000003.437188672.00000000056F5000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000001.375725825.00000000009F2000.00000002.00000001.01000000.00000003.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000001.375725825.00000000009F2000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000001.375725825.00000000009F2000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000001.375725825.00000000009F2000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000001.375725825.00000000009F2000.00000002.00000001.01000000.00000003.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.679442760.0000000001893000.00000002.00000001.01000000.00000003.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.679442760.0000000001893000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000000.00000002.679442760.0000000001893000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.679442760.0000000001893000.00000002.00000001.01000000.00000003.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: njrat1, Description: Identify njRat, Source: 00000000.00000002.679442760.0000000001893000.00000002.00000001.01000000.00000003.sdmp, Author: Brian Wallace @botnet_hunter
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71D860AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71D860AC	unknown
C:\Users\user\AppData\Roaming\healastounding.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	283A4D3	CreateFileW
C:\Users\user\AppData\Roaming\Pluto Panel.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	283A4D3	CreateFileW
C:\Users\user\AppData\Roaming\0fd7de5367376231a788872005d7ed4f.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	283A4D3	CreateFileW
C:\Users\user\AppData\Roaming\22.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	283A4D3	CreateFileW
C:\Users\user\AppData\Roaming___11.19.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	283A4D3	CreateFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RIP_YOUR_PC_LOL.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	71D734A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\healastounding.exe	0	3733504	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 0f fd 61 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 0b 00 00 fd 38 00 00 08 00 00 00 00 00 00 2e 0d 39 00 00 20 00 00 00 20 39 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 39 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELa8.9 9@ `9 @	success or wait	1	283A737	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Pluto Panel.exe	0	913920	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 43 fd 61 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 08 00 00 fd 07 00 00 34 00 00 00 00 00 00 fd 0b 08 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 08 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELCa4 @ @	success or wait	1	283A737	WriteFile
C:\Users\user\AppData\Roaming\0fd7de5367376231a788872005d7ed4f.exe	0	549556	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 20 fd 34 fd 64 fd 5a fd 64 fd 5a fd 64 fd 5a fd 7a fd dd 75 fd 5a fd 7a fd 5d 0f fd 5a fd 7a fd 9d 53 fd 5a fd 43 43 21 fd 67 fd 5a fd 64 fd 5b fd fd 5a fd 7a fd 1d 65 fd 5a fd 7a fd 9d 65 fd 5a fd 7a fd dd 65 fd 5a fd 52 69 63 68 64 fd 5a fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd 3a 1c 5f 00 00 00 00 00 00 00 00 fd 00 03	MZ@!L!This program cannot be run in DOS mode.$ 4dZdZdZzuZzZz SZCC!gZd[ZzeZzeZzeZR ichdZPEL:_	success or wait	1	283A737	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\22.exe	0	2101248	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 28 fd 06 fd 49 fd 55 fd 49 fd 55 fd 49 fd 55 fd 55 fd 55 fd 49 fd 55 1e 46 fd 55 fd 49 fd 55 5e 55 fd 55 fd 49 fd 55 fd 6f fd 55 7e 49 fd 55 35 56 fd 55 fd 49 fd 55 1e 46 fd 55 fd 49 fd 55 fd 49 fd 55 fd 4b fd 55 fd 6f fd 55 fd 49 fd 55 fd 49 fd 55 fd 49 fd 55 35 56 fd 55 fd 49 fd 55 52 69 63 68 fd 49 fd 55 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04	MZ@!L!This program cannot be run in DOS mode.$(IUIUIUUUIUFUIU^UUIUoU~IU5VUIUFUIUIUKUoUIUIU IU5VUIURichIUPEL	success or wait	1	283A737	WriteFile
C:\Users\user\AppData\Roaming___11.19.exe	0	16322590	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 1b 48 fd fd 75 1b fd fd 75 1b fd fd 75 1b fd fd 7e 1b fd fd 75 1b fd fd 7f 1b fd fd 75 1b fd fd 7f 1b 02 fd 75 1b 43 fd 7b 1b fd fd 75 1b fd fd 79 1b fd fd 75 1b fd fd 66 1b fd fd 75 1b fd fd 66 1b fd fd 75 1b fd fd 74 1b 60 fd 75 1b 43 fd 28 1b fd fd 75 1b fd fd 7e 1b fd fd 75 1b 28 fd 7e 1b fd fd 75 1b 28 fd 7f 1b fd fd 75 1b fd fd 75 1b fd fd 75 1b 07 fd 73 1b fd fd 75	MZ@!L!This program cannot be run in DOS mode.$Huuu~uuuC{uyufufut`uC(u~u(~u(uuusu	success or wait	1	283A737	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RIP_YOUR_PC_LOL.exe.log	0	128	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a	1,"fusion","GAC",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0	success or wait	1	7205A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	71DB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	71DB5544	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	71DB8738	ReadFile

Analysis Process: healastounding.exe PID: **3572**, Parent PID: **6880**

General

Target ID:	4
Start time:	18:00:38
Start date:	08/03/2022
Path:	C:\Users\user\AppData\Roaming\healastounding.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\healastounding.exe"
Imagebase:	0x900000
File size:	3733504 bytes
MD5 hash:	6FB798F1090448CE26299C2B35ACF876
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.385235005.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.385235005.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000004.00000000.385235005.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000004.00000000.385235005.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.385235005.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: njrat1, Description: Identify njRat, Source: 00000004.00000000.385235005.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Brian Wallace @botnet_hunter • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000004.00000002.538356356.0000000003471000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000004.00000002.538356356.0000000003471000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: 00000004.00000002.538356356.0000000003471000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: njrat1, Description: Identify njRat, Source: 00000004.00000002.538356356.0000000003471000.00000004.00000800.00020000.00000000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.463698979.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.463698979.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000004.00000002.463698979.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000004.00000002.463698979.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.463698979.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: njrat1, Description: Identify njRat, Source: 00000004.00000002.463698979.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.546334194.0000000004474000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000004.00000002.546334194.0000000004474000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.546334194.0000000004474000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.546334194.0000000004474000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.381351381.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.381351381.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000004.00000000.381351381.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000004.00000000.381351381.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.381351381.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: njrat1, Description: Identify njRat, Source: 00000004.00000000.381351381.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.382829254.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.382829254.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000004.00000000.382829254.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000004.00000000.382829254.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.382829254.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: njrat1, Description: Identify njRat, Source: 00000004.00000000.382829254.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.383946223.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.383946223.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000004.00000000.383946223.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000004.00000000.383946223.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.383946223.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: njrat1, Description: Identify njRat, Source: 00000004.00000000.383946223.0000000000902000.00000002.00000001.01000000.00000005.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Users\user\AppData\Roaming\healastounding.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Users\user\AppData\Roaming\healastounding.exe, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: C:\Users\user\AppData\Roaming\healastounding.exe, Author: Joe Security • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: C:\Users\user\AppData\Roaming\healastounding.exe, Author: Joe Security • Rule: MALWARE_Win_NjRAT, Description: Detects NjRAT / Bladabindi, Source: C:\Users\user\AppData\Roaming\healastounding.exe, Author: ditekSHen • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: C:\Users\user\AppData\Roaming\healastounding.exe, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: C:\Users\user\AppData\Roaming\healastounding.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: njrat1, Description: Identify njRat, Source: C:\Users\user\AppData\Roaming\healastounding.exe, Author: Brian Wallace @botnet_hunter
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71D860AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71D860AC	unknown
C:\Users\user\AppData\Roaming\test.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	148A4D3	CreateFileW
C:\Users\user\AppData\Roaming\gay.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	148A4D3	CreateFileW
C:\Users\user\AppData\Roaming\Opus.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	148A4D3	CreateFileW
C:\Users\user\AppData\Roaming\aaa.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	148A4D3	CreateFileW
C:\Users\user\AppData\Roaming\8f1c8b40c7be588389a8d382040b23bb.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	148A4D3	CreateFileW
C:\Users\user\AppData\Roaming\4.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	148A4D3	CreateFileW
C:\Users\user\AppData\Roaming\a.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	148A4D3	CreateFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\healastounding.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	71D734A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\test.exe	0	46080	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 23 fd fd 5e 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 08 00 00 fd 00 00 00 0a 00 00 00 00 00 00 4e fd 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 01 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL#^N @ @	success or wait	1	148A737	WriteFile
C:\Users\user\AppData\Roaming\gay.exe	0	37888	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 1f fd 61 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 08 00 00 fd 00 00 00 06 00 00 00 00 00 00 ab 00 00 00 20 00 00 00 fd 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 01 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELa @ @	success or wait	1	148A737	WriteFile

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Opus.exe	0	208384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 27 fd 54 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 06 00 00 fd 01 00 00 64 01 00 00 00 00 00 fd fd 01 00 00 20 00 00 00 00 02 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 03 00 00 02 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL'Td @	success or wait	1	148A737	WriteFile
C:\Users\user\AppData\Roaming\aaa.exe	0	122880	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd fd fd 53 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 08 00 00 fd 01 00 00 08 00 00 00 00 00 00 6e fd 01 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 02 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELSn @ @@	success or wait	1	148A737	WriteFile

Copyright Joe Security LLC 2022

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\8f1c8b40c7be588389a8d382040b23bb.exe	0	1241088	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 3e fd 61 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 fd 12 00 00 20 00 00 00 00 00 00 36 28 12 00 00 10 00 00 00 fd 12 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 13 00 00 10 00 00 6b 14 13 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL>a 6(@k	success or wait	1	148A737	WriteFile
C:\Users\user\AppData\Roaming\4.exe	0	579127	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 62 60 fd fd 26 01 fd fd 26 01 fd fd 26 01 fd fd fd fd 68 fd 2b 01 fd fd fd fd 6a fd fd 01 fd fd fd fd 6b fd 3e 01 fd fd fd fd 5e fd 24 01 fd fd 1d 5f fd fd 30 01 fd fd 1d 5f fd fd 35 01 fd fd 1d 5f fd fd 0a 01 fd fd 2f 79 1a fd 2c 01 fd fd 2f 79 0a fd 23 01 fd fd 26 01 fd fd 2b 00 fd fd fd 5f fd fd 17 01 fd fd fd 5f fd fd 27 01 fd fd fd 5f 66 fd 27 01 fd fd fd 5f fd fd 27 01 fd	MZ@!L!This program cannot be run in DOS mode.$b`&&&h+jk>^$_0_5_/y,/y#&+__'_f'_'	success or wait	1	148A737	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\a.exe	0	1484512	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 07 00 fd 4f 05 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 01 00 00 0c 00 00 00 00 00 00 00 20 00 00 00 20 00 00 00 fd 01 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 3c 00 00 20 00 00 2d 41 36 00 02 00 00 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELO0 @ < -A6	success or wait	1	148A737	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\healastounding.exe.log	0	128	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a	1,"fusion","GAC",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0	success or wait	1	7205A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	71DB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	71DB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	71DB8738	ReadFile

Analysis Process: Pluto Panel.exe PID: 4236, Parent PID: 6880

General

Target ID:	5
Start time:	18:00:43
Start date:	08/03/2022
Path:	C:\Users\user\AppData\Roaming\Pluto Panel.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Pluto Panel.exe"
Imagebase:	0xf10000
File size:	913920 bytes
MD5 hash:	ED666BF7F4A0766FCEC0E9C8074B089B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000002.711210574.0000000004691000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000002.711210574.0000000004691000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000005.00000000.393171200.0000000000F12000.00000002.00000001.01000000.00000006.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000000.393171200.0000000000F12000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000000.393171200.0000000000F12000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000000.393171200.0000000000F12000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000005.00000000.393171200.0000000000F12000.00000002.00000001.01000000.00000006.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000002.706080641.00000000036DB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000005.00000002.706080641.00000000036DB000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000005.00000002.712472379.0000000007710000.00000004.00000001.00040000.00000000.sdmp, Author: Arnim Rupp • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000005.00000000.394040229.0000000000F12000.00000002.00000001.01000000.00000006.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000000.394040229.0000000000F12000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000000.394040229.0000000000F12000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000000.394040229.0000000000F12000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000005.00000000.394040229.0000000000F12000.00000002.00000001.01000000.00000006.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000005.00000000.394636472.0000000000F12000.00000002.00000001.01000000.00000006.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000000.394636472.0000000000F12000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000000.394636472.0000000000F12000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000000.394636472.0000000000F12000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000005.00000000.394636472.0000000000F12000.00000002.00000001.01000000.00000006.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000005.00000002.701277187.0000000000F12000.00000002.00000001.01000000.00000006.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000002.701277187.0000000000F12000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000002.701277187.0000000000F12000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000002.701277187.0000000000F12000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000005.00000002.701277187.0000000000F12000.00000002.00000001.01000000.00000006.sdmp, Author: JPCERT/CC Incident Response Group • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000005.00000002.712461562.0000000007700000.00000004.00000001.00040000.00000000.sdmp, Author: Arnim Rupp • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000005.00000000.397247474.0000000000F12000.00000002.00000001.01000000.00000006.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000000.397247474.0000000000F12000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000000.397247474.0000000000F12000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000000.397247474.0000000000F12000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000005.00000000.397247474.0000000000F12000.00000002.00000001.01000000.00000006.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: C:\Users\user\AppData\Roaming\Pluto Panel.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: C:\Users\user\AppData\Roaming\Pluto Panel.exe, Author: Arnim Rupp • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: C:\Users\user\AppData\Roaming\Pluto Panel.exe, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: C:\Users\user\AppData\Roaming\Pluto Panel.exe, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: C:\Users\user\AppData\Roaming\Pluto Panel.exe, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: C:\Users\user\AppData\Roaming\Pluto Panel.exe, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71D860AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71D860AC	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71D860AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71D860AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	71DB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	71DB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	71DB8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	71DB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	71DB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	3230093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	3230093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	3230093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	3230093	ReadFile

Analysis Process: test.exe PID: **6236**, Parent PID: **3572**

General

Target ID:	6
Start time:	18:00:44
Start date:	08/03/2022
Path:	C:\Users\user\AppData\Roaming\test.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\test.exe"
Imagebase:	0xda0000
File size:	46080 bytes
MD5 hash:	7E50B2929829321901792 45C60C0B59B
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: 00000006.00000000.397644420.0000000000DA2000.00000002.00000001.01000000.00000007.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: 00000006.00000000.397644420.0000000000DA2000.00000002.00000001.01000000.00000007.sdmp, Author: ditekSHen • Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 00000006.00000002.701971433.0000000001354000.00000004.00000020.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000006.00000000.405813841.0000000000DA2000.00000002.00000001.01000000.00000007.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: 00000006.00000000.405813841.0000000000DA2000.00000002.00000001.01000000.00000007.sdmp, Author: ditekSHen • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000006.00000000.394727625.0000000000DA2000.00000002.00000001.01000000.00000007.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: 00000006.00000000.394727625.0000000000DA2000.00000002.00000001.01000000.00000007.sdmp, Author: ditekSHen • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000006.00000000.399704980.0000000000DA2000.00000002.00000001.01000000.00000007.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: 00000006.00000000.399704980.0000000000DA2000.00000002.00000001.01000000.00000007.sdmp, Author: ditekSHen • Rule: MALWARE_Win_AsyncRAT, Description: Detects AsyncRAT, Source: 00000006.00000002.703770994.00000000030D1000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000006.00000002.701012196.0000000000DA2000.00000002.00000001.01000000.00000007.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: 00000006.00000002.701012196.0000000000DA2000.00000002.00000001.01000000.00000007.sdmp, Author: ditekSHen • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: C:\Users\user\AppData\Roaming\test.exe, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_ASEP_REG_Reverse, Description: Detects file containing reversed ASEP Autorun registry keys, Source: C:\Users\user\AppData\Roaming\test.exe, Author: ditekSHen
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D72CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D72CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D705705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D705705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D6603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D70CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D6603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D705705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D705705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D6603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D6603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D6603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C0D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C0D1B4F	ReadFile

Analysis Process: 0fd7de5367376231a788872005d7ed4f.exe PID: 2024, Parent PID: 6880

General

Target ID:	7
Start time:	18:00:50

Start date:	08/03/2022
Path:	C:\Users\user\AppData\Roaming\0fd7de5367376231a788872005d7ed4f.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\0fd7de5367376231a788872005d7ed4f.exe"
Imagebase:	0x400000
File size:	549556 bytes
MD5 hash:	0FD7DE5367376231A788872005D7ED4F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_ficker_stealer, Description: Yara detected Ficker Stealer, Source: 00000007.00000002.468272297.00000000024F0000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 29%, Metadefender, Browse • Detection: 92%, ReversingLabs
Reputation:	low

Analysis Process: gay.exe PID: **1104**, Parent PID: **3572**

General

Target ID:	8
Start time:	18:00:51
Start date:	08/03/2022
Path:	C:\Users\user\AppData\Roaming\gay.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\gay.exe"
Imagebase:	0xd0000
File size:	37888 bytes
MD5 hash:	8EEDC01C11B251481DEC59E5308DCCC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000008.00000000.411478373.00000000000D2000.00000002.00000001.01000000.00000009.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000008.00000000.411478373.00000000000D2000.00000002.00000001.01000000.00000009.sdmp, Author: Brian Wallace @botnet_hunter • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000008.00000002.449565052.00000000000D2000.00000002.00000001.01000000.00000009.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000008.00000002.449565052.00000000000D2000.00000002.00000001.01000000.00000009.sdmp, Author: Brian Wallace @botnet_hunter • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000008.00000000.410285813.00000000000D2000.00000002.00000001.01000000.00000009.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000008.00000000.410285813.00000000000D2000.00000002.00000001.01000000.00000009.sdmp, Author: Brian Wallace @botnet_hunter • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000008.00000000.408615715.00000000000D2000.00000002.00000001.01000000.00000009.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000008.00000000.408615715.00000000000D2000.00000002.00000001.01000000.00000009.sdmp, Author: Brian Wallace @botnet_hunter • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000008.00000000.409570794.00000000000D2000.00000002.00000001.01000000.00000009.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000008.00000000.409570794.00000000000D2000.00000002.00000001.01000000.00000009.sdmp, Author: Brian Wallace @botnet_hunter • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: C:\Users\user\AppData\Roaming\gay.exe, Author: Joe Security • Rule: MALWARE_Win_NjRAT, Description: Detects NjRAT / Bladabindi, Source: C:\Users\user\AppData\Roaming\gay.exe, Author: ditekSHen • Rule: njrat1, Description: Identify njRat, Source: C:\Users\user\AppData\Roaming\gay.exe, Author: Brian Wallace @botnet_hunter
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71D860AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71D860AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\gay.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	71D734A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\gay.exe.log	0	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 23 5c 63 64 37 63 37 34 66 63 65 32 61 30 65 61 62 37 32 63 64 32 35 63 62 65 34 62 62 36 31 36 31 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	1,"fusion","GAC",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	7205A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	71DB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	71DB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	71DB8738	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER	di	unicode	!	success or wait	1	7142C863	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer	SlowContextMenuEntries	binary	60 24 B2 21 EA 3A 69 10 A2 DC 08 00 2B 30 30 9D 96 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	60 24 B2 21 EA 3A 69 10 A2 DC 08 00 2B 30 30 9D 96 01 00 00 FB 9A 79 09 67 AD D1 11 AB CD 00 C0 4F C3 09 36 BC 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7102742E	unknown

Analysis Process: Opus.exe PID: **3244**, Parent PID: **3572**

General

Target ID:	9
Start time:	18:00:53
Start date:	08/03/2022
Path:	C:\Users\user\AppData\Roaming\Opus.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\Opus.exe"
Imagebase:	0x840000
File size:	208384 bytes
MD5 hash:	759185EE3724D7563B709C888C696959
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.414257385.0000000000842000.00000002.00000001.01000000.0000000A.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.414257385.0000000000842000.00000002.00000001.01000000.0000000A.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.414257385.0000000000842000.00000002.00000001.01000000.0000000A.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.707363158.0000000003ECB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.707363158.0000000003ECB000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.414807841.0000000000842000.00000002.00000001.01000000.0000000A.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.414807841.0000000000842000.00000002.00000001.01000000.0000000A.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.414807841.0000000000842000.00000002.00000001.01000000.0000000A.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.416456851.0000000000842000.00000002.00000001.01000000.0000000A.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.416456851.0000000000842000.00000002.00000001.01000000.0000000A.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.416456851.0000000000842000.00000002.00000001.01000000.0000000A.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.700831183.0000000000842000.00000002.00000001.01000000.0000000A.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.700831183.0000000000842000.00000002.00000001.01000000.0000000A.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.700831183.0000000000842000.00000002.00000001.01000000.0000000A.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.415266906.0000000000842000.00000002.00000001.01000000.0000000A.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.415266906.0000000000842000.00000002.00000001.01000000.0000000A.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.415266906.0000000000842000.00000002.00000001.01000000.0000000A.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.708577022.0000000005870000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.708577022.0000000005870000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000009.00000002.708577022.0000000005870000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.708751563.0000000005B00000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.708751563.0000000005B00000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.708751563.0000000005B00000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000009.00000002.708751563.0000000005B00000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Users\user\AppData\Roaming\Opus.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Users\user\AppData\Roaming\Opus.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Users\user\AppData\Roaming\Opus.exe, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: C:\Users\user\AppData\Roaming\Opus.exe, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: C:\Users\user\AppData\Roaming\Opus.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71D860AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71D860AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	51407A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	514089B	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	51407A1	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	5140B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp4896.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5140D1C	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	514089B	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp5D87.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5140D1C	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	51407A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	51407A1	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71D860AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71D860AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4896.tmp	success or wait	1	112BF0E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp5D87.tmp	success or wait	1	112BF0E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	21 61 3a fd 70 01 fd 48	!a:pH	success or wait	1	5140A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 27 fd 54 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 06 00 00 fd 01 00 00 64 01 00 00 00 00 00 fd fd 01 00 00 20 00 00 00 00 02 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 03 00 00 02 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL'Td @	success or wait	2	5140B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp4896.tmp	0	1305	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	5140A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	0	42	43 3a 5c 55 73 65 72 73 5c 65 6e 67 69 6e 65 65 72 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 4f 70 75 73 2e 65 78 65	C:\Users\user\AppData\Roaming\Opus.exe	success or wait	1	5140A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp5D87.tmp	0	1310	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	5140A53	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	71DB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	71DB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	71DB8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	71E5BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	71E5BF06	unknown
C:\Users\user\AppData\Roaming\Opus.exe	unknown	4096	success or wait	1	71E5BF06	unknown
C:\Users\user\AppData\Roaming\Opus.exe	unknown	512	success or wait	1	71E5BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	71DB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	4	71DB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	71DB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	5140A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5140A53	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	5140C12	RegSetValueExW

Analysis Process: 22.exe PID: **1272**, Parent PID: **6880**

General

Target ID:	11
Start time:	18:00:57

Start date:	08/03/2022
Path:	C:\Users\user\AppData\Roaming\22.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\22.exe"
Imagebase:	0x400000
File size:	2101248 bytes
MD5 hash:	DBF9DAA1707B1037E28A6E0694B33A4B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: MALWARE_Win_BlackMoon, Description: Detects executables using BlackMoon RunTime, Source: C:\Users\user\AppData\Roaming\22.exe, Author: ditekSHen
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 38%, Metadefender, Browse • Detection: 86%, ReversingLabs
Reputation:	low

Analysis Process: aaa.exe PID: **3984**, Parent PID: **3572**

General

Target ID:	12
Start time:	18:00:57
Start date:	08/03/2022
Path:	C:\Users\user\AppData\Roaming\aaa.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\aaa.exe"
Imagebase:	0x2c0000
File size:	122880 bytes
MD5 hash:	860AA57FC3578F7037BB27FC79B2A62C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: 8f1c8b40c7be588389a8d382040b23bb.exe PID: **5376**, Parent PID: **3572**

General

Target ID:	14
Start time:	18:00:59
Start date:	08/03/2022
Path:	C:\Users\user\AppData\Roaming\8f1c8b40c7be588389a8d382040b23bb.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\8f1c8b40c7be588389a8d382040b23bb.exe"
Imagebase:	0x400000
File size:	1241088 bytes
MD5 hash:	8F1C8B40C7BE588389A8D382040B23BB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 26%, Metadefender, Browse • Detection: 86%, ReversingLabs
Reputation:	low

Analysis Process: 0fd7de5367376231a788872005d7ed4f.exe PID: **5172**, Parent PID: **2024**

General	
Target ID:	15
Start time:	18:00:59
Start date:	08/03/2022
Path:	C:\Users\user\AppData\Roaming\0fd7de5367376231a788872005d7ed4f.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\0fd7de5367376231a788872005d7ed4f.exe"
Imagebase:	0x400000
File size:	549556 bytes
MD5 hash:	0FD7DE5367376231A788872005D7ED4F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 4.exe PID: **2824**, Parent PID: **3572**

General	
Target ID:	16
Start time:	18:01:04
Start date:	08/03/2022
Path:	C:\Users\user\AppData\Roaming\4.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\4.exe"
Imagebase:	0x11d0000
File size:	579127 bytes
MD5 hash:	E6DACE3F577AC7A6F9747B4A0956C8D7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 17%, Metadefender, Browse • Detection: 75%, ReversingLabs
Reputation:	low

Analysis Process: mediaget.exe PID: **4688**, Parent PID: **1104**

General	
Target ID:	17
Start time:	18:01:07
Start date:	08/03/2022
Path:	C:\Users\user\AppData\Roaming\mediaget.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\mediaget.exe"
Imagebase:	0xab0000
File size:	37888 bytes
MD5 hash:	8EEDC01C11B251481DEC59E5308DCCC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2022

Yara matches:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000011.00000000.445953483.0000000000AB2000.00000002.00000001.01000000.0000000F.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000011.00000000.445953483.0000000000AB2000.00000002.00000001.01000000.0000000F.sdmp, Author: Brian Wallace @botnet_hunter • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000011.00000002.701265514.0000000000AB2000.00000002.00000001.01000000.0000000F.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000011.00000002.701265514.0000000000AB2000.00000002.00000001.01000000.0000000F.sdmp, Author: Brian Wallace @botnet_hunter • Rule: njrat1, Description: Identify njRat, Source: 00000011.00000003.646152049.0000000001338000.00000004.00000020.00020000.00000000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000011.00000000.445251023.0000000000AB2000.00000002.00000001.01000000.0000000F.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000011.00000000.445251023.0000000000AB2000.00000002.00000001.01000000.0000000F.sdmp, Author: Brian Wallace @botnet_hunter • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000011.00000000.447375879.0000000000AB2000.00000002.00000001.01000000.0000000F.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000011.00000000.447375879.0000000000AB2000.00000002.00000001.01000000.0000000F.sdmp, Author: Brian Wallace @botnet_hunter • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000011.00000000.446671445.0000000000AB2000.00000002.00000001.01000000.0000000F.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000011.00000000.446671445.0000000000AB2000.00000002.00000001.01000000.0000000F.sdmp, Author: Brian Wallace @botnet_hunter • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: C:\Users\user\AppData\Roaming\mediaget.exe, Author: Joe Security • Rule: MALWARE_Win_NjRAT, Description: Detects NjRAT / Bladabindi, Source: C:\Users\user\AppData\Roaming\mediaget.exe, Author: ditekSHen • Rule: njrat1, Description: Identify njRat, Source: C:\Users\user\AppData\Roaming\mediaget.exe, Author: Brian Wallace @botnet_hunter
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

Disassembly

No disassembly