ID: 553285
Sample Name:
g94e4BgSRN.exe
Cookbook: default.jbs
Time: 15:54:16
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

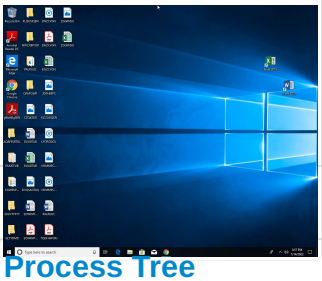
Windows Analysis Report g94e4BgSRN.exe

Overview

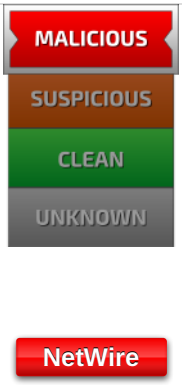
General Information

Sample Name:	g94e4BgSRN.exe
Analysis ID:	553285
MD5:	d058c6416284f29.
SHA1:	9fe97ad0c11997b.
SHA256:	c47c4a57e7521c…
Tags:	exe NetWire RAT
Infos:	

Most interesting Screenshot:



Detection

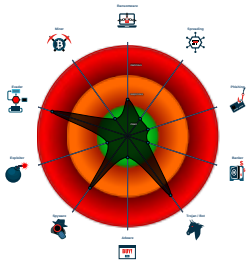


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AntiVM3
- Yara detected NetWire RAT
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Tries to detect sandboxes and other…
- Sigma detected: Suspicius Add Tas…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Contains functionality to steal Chrom…
- Sigma detected: Powershell Defende…

Classification



Process Tree

- **System is w10x64**
- g94e4BgSRN.exe (PID: 6384 cmdline: "C:\Users\user\Desktop\g94e4BgSRN.exe" MD5: D058C6416284F291D6BC7E183293DA1F)
  - powershell.exe (PID: 6780 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\SiEKNQVnm.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6788 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6796 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\SiEKNQVnm" /XML "C:\Users\user\AppData\Local\Temp\tmp2A91.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6920 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - g94e4BgSRN.exe (PID: 6976 cmdline: C:\Users\user\Desktop\g94e4BgSRN.exe MD5: D058C6416284F291D6BC7E183293DA1F)
- **cleanup**

Malware Configuration

Threatname: NetWire


```
{
  "C2 list": [
    "podzeye.duckdns.org:6688"
  ],
  "Password": "Password",
  "Host ID": "HostId-%Rand%",
  "Mutex": "-",
  "Install Path": "-",
  "Startup Name": "-",
  "ActiveX Key": "-",
  "KeyLog Directory": "-"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.286467177.00000000026AB000.00000004.00000001.sdmp	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
00000009.00000000.282165749.0000000000400000.00000040.00000001.sdmp	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
00000009.00000000.280983052.0000000000400000.00000040.00000001.sdmp	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
00000009.00000000.281635680.0000000000400000.00000040.00000001.sdmp	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
00000009.00000002.516753076.0000000000400000.00000040.00000001.sdmp	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
Click to see the 9 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.0.g94e4BgSRN.exe.400000.10.raw.unpack	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
9.0.g94e4BgSRN.exe.400000.16.unpack	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
9.0.g94e4BgSRN.exe.400000.12.unpack	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
9.0.g94e4BgSRN.exe.400000.4.unpack	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
9.0.g94e4BgSRN.exe.400000.16.raw.unpack	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
Click to see the 15 entries				

Sigma Overview

System Summary:

- Sigma detected: Suspicius Add Task From User AppData Temp
- Sigma detected: Powershell Defender Exclusion
- Sigma detected: Non Interactive PowerShell
- Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file

Networking:

- C2 URLs / IPs found in malware configuration
- Uses dynamic DNS services

System Summary:

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Contains functionality to steal Chrome passwords or cookies

Remote Access Functionality:

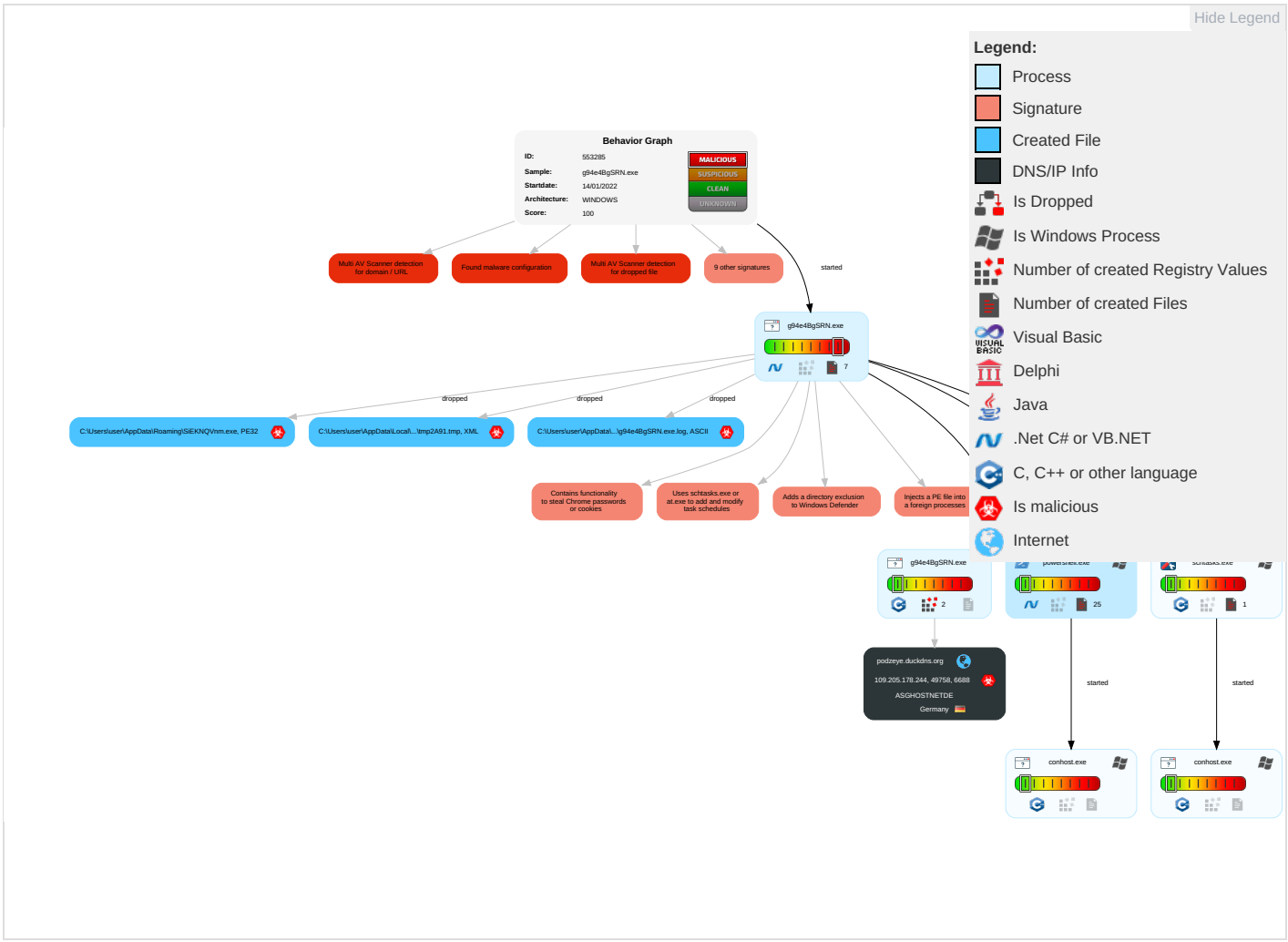
Yara detected NetWire RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping 1	Security Software Discovery 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1 1	Credentials In Files 1	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 Redirect PI Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1	Exploit SS7 Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-I Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	File and Directory Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 1 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cell Base Static

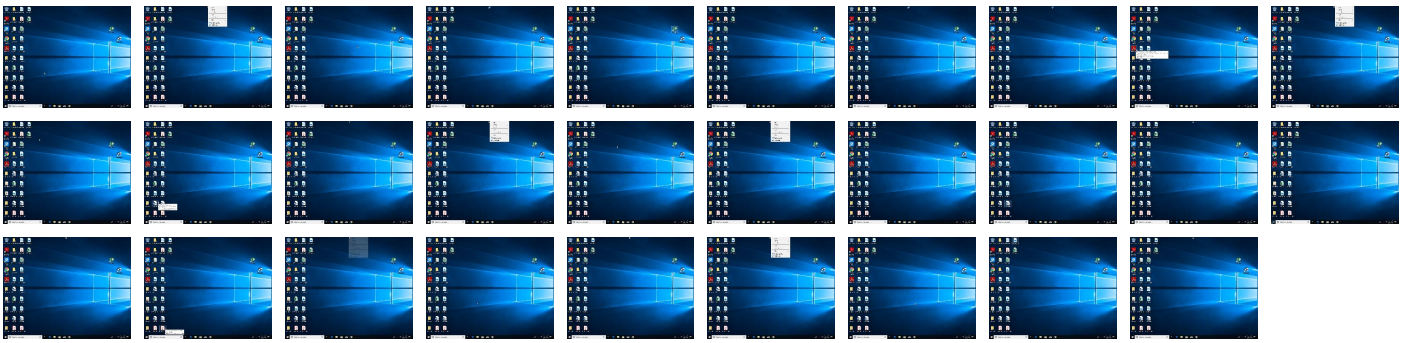
Behavior Graph



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
g94e4BgSRN.exe	49%	Virustotal		Browse
g94e4BgSRN.exe	63%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\SiEKNQVnm.exe	63%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.0.g94e4BgSRN.exe.400000.14.unpack	100%	Avira	TR/Spy.Gen		Download File
9.0.g94e4BgSRN.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen		Download File
9.0.g94e4BgSRN.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen		Download File
9.0.g94e4BgSRN.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen		Download File
9.0.g94e4BgSRN.exe.400000.18.unpack	100%	Avira	TR/Spy.Gen		Download File
0.2.g94e4BgSRN.exe.3873c18.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
9.0.g94e4BgSRN.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen		Download File
9.0.g94e4BgSRN.exe.400000.16.unpack	100%	Avira	TR/Spy.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
9.0.g94e4BgSRN.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen		Download File
9.2.g94e4BgSRN.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen		Download File
0.2.g94e4BgSRN.exe.389be38.6.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
podzeye.duckdns.org	6%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0n1	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0n	0%	Avira URL Cloud	safe	
http://www.yandex.comsocks=	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/n-u	0%	URL Reputation	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.fontbureau.comceTFp	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.carterandcone.como.2K-	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
podzeye.duckdns.org:6688	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.come	0%	URL Reputation	safe	
http://www.carterandcone.como.)K	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/k	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/f	0%	URL Reputation	safe	
http://www.tiro.comlar?	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn)	0%	URL Reputation	safe	
http://www.founder.com.cn/cn#	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
podzeye.duckdns.org	109.205.178.244	true	true	• 6%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
podzeye.duckdns.org:6688	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
109.205.178.244	podzeye.duckdns.org	Germany		12586	ASGHOSTNETDE	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553285
Start date:	14.01.2022
Start time:	15:54:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	g94e4BgSRN.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:	32
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@9/8@1/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 2.8% (good quality ratio 1.4%) • Quality average: 38.5% • Quality standard deviation: 41.8%
HCA Information:	• Successful, ratio: 100% • 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
15:55:22	API Interceptor	2x Sleep call for process: g94e4BgSRN.exe modified
15:55:26	API Interceptor	30x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\g94e4BgSRN.exe.log	
Process:	C:\Users\user\Desktop\g94e4BgSRN.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1396
Entropy (8bit):	5.340178659145498
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4bE4KnKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE47mE4l:MIHK5HKXE1qHbHKnYHKhQnoPtHoxHhA9
MD5:	200C45B4371C42E1EC65243C1288751B
SHA1:	D381B575CBD94379873AA43DB07ED18BC6150C1A
SHA-256:	953799E8B658D0797E82466EB482E238F9F73326F5B91D0503D3591DB58ED236
SHA-512:	AAE09F52FAB534CDAC85BBD0A976BC01EDB7C958A0C1FB9C78BC76C82A24ACFBA7741001DB75ECED65309BA3799FCB526EBF9DA74CC3AAE0DB689CA0FF6EE892
Malicious:	**true**
Reputation:	moderate, very likely benign file
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..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",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..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e08

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22280
Entropy (8bit):	5.345158041308615
Encrypted:	false
SSDEEP:	384:z7tCDbeFrFiyHmz4sUunFrnVLf1JNcLnudlu5cuOhhjm1dOG06JaC:2eqrnln9XSrudl8cugjqB
MD5:	7C2AF9AA7FC1BDF2B8BE132BFDEC1399
SHA1:	70F809B8D4876D06AEAB6ADF1A9780BF0125134A
SHA-256:	7DB5A3A99C17034A683F86EFFFB77073B9247DFFBD9E648AF78EB62E10E47003
SHA-512:	49D5B634906670248C726F38C4D786AF89522ADFE976678A26F2DD8D890951BE40E285174BFFC1CA7D265DAA5E152879548A6504039359EF82548B440248478A
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Reputation:	low
Preview:	@...e.....z.....h.P.....M...J.....@.....D.....fZve...F.....x.).....System.Management.AutomationH.....<@.^.L."My...:R..... .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__PSScriptPolicyTest_wrftyazc.eg3.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:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_wv32y10w.3up.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:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp2A91.tmp	
Process:	C:\Users\user\Desktop\g94e4BgSRN.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1600
Entropy (8bit):	5.133278056985278
Encrypted:	false
SSDEEP:	24:2di4+S2qh/a1Kby1moqUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtuxvn:cgeCaYrFdOFzOzN33ODOiDdKrsuTiv
MD5:	74F8CF7052E31844E3352158FDC16419
SHA1:	C86BF805FF74DF95045D87EEF800BB3F31088527
SHA-256:	61B51A73F187A78F74AD533C8057C809173351B534B7FB90F5ED69FFFF117522
SHA-512:	8C2C3FE1C6A1DCF32EF574DC61CFF031DCEE30BFA8BF2E61ACBCF1E22D0889756F094D7A826CEB5273A65EAD33C5A8B35A6ED9CA545D25C18E60BC71000E A3A
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserI d>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <Sto pIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>.

C:\Users\user\AppData\Roaming\SiEKNQVnm.exe	
Process:	C:\Users\user\Desktop\g94e4BgSRN.exe

C:\Users\user\AppData\Roaming\SiEKNQVnm.exe	
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	898560
Entropy (8bit):	6.874832837426071
Encrypted:	false
SSDEEP:	24576:t6vaGtDTmitq1QqEGNCN/uVKTPLZsLkbR:tJGtOitq1QqFNGZTPWLE
MD5:	D058C6416284F291D6BC7E183293DA1F
SHA1:	9FE97AD0C11997B7C0CA5A43AFF43CC8BDB915B6
SHA-256:	C47C4A57E7521C6886CA3764B32AD1E5D8669F2FBF6B127FE7A832F1F3B74EC5
SHA-512:	13F733FC99E5FAEB274DD1480620194E88BE23D70FDC108C3846CF471760A21AC8606364ED930A187B62EBEDC25124488CB0557D1CED271AF982D50F52FC25C
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 63%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0.....".....@.. .....@..O..... ....H.....text..... ....`.rsrc..... .....@..@.reloc..... .....@..B.....H.....p.....>..(...+.o(....*.0.....Y.+..*....0.....+...+..*..().....}.....~....%.X.....}.....s*...%.o+....}....*..().....{....}.....{....}.....{....(...+}....*..0..@.....{....~....%-.&~.....s,...%.....(...+(...+.{....(...+.+..*.0.....{.....o0....+..*...0.....{....(...+.+..*....0.....{....o1....+..*>..{.....o2....*....0..&.....r...p.{.....{.....(3..

C:\Users\user\AppData\Roaming\SiEKNQVnm.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\g94e4BgSRN.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220114\PowerShell_transcript.305090.zsWXEWae.20220114155525.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):	5795
Entropy (8bit):	5.392253149129379
Encrypted:	false
SSDEEP:	96:BZO/fNnqDo1ZyZL/fNnqDo1ZRFfdjZ5/fNnqDo1ZfkNNDZo:r
MD5:	A710E87EA4269CD157E421251E3052D7
SHA1:	6FAF0121B75D400CDB4C8090989E93A6F3F50B7A
SHA-256:	99BA73487367ACF1331EC08FFCD57E2565E37828AC3376BC16B50417AE998EB8
SHA-512:	67D7F38C716ABA229FC7681D4641E24454A226C965C699B8DEA30452B9F50264D5EA0C16C0834744B3F3B042657EE4F21F32359E7EA41A237A0D033CEA2A3DF5
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220114155526..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 305090 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\SiEKNQVnm.exe..Process ID: 6780..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: 20220114155526..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\SiEKNQVnm.exe..**********..Windows PowerShell transcript start..Start time: 20220114155929..Username: computer\user..RunAs User: computer\a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.874832837426071

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	g94e4BgSRN.exe
File size:	898560
MD5:	d058c6416284f291d6bc7e183293da1f
SHA1:	9fe97ad0c11997b7c0ca5a43aff43cc8bdb915b6
SHA256:	c47c4a57e7521c6886ca3764b32ad1e5d8669f2fbf6b127fe7a832f1f3b74ec5
SHA512:	13f733fc99e5faeb274dd1480620194e88be23d70fdc108c3846cf471760a21ac8606364ed930a187b62ebedc25124488cb0557d1ced271af982d50f52fc25cd
SSDEEP:	24576:t6vaGtDTmitq1QqEGNCN/uVKTPLZsLkbR:tJGtOitq1QqFNGZTPWLE
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0....."..... .....@.. .....@.....

File Icon

Icon Hash:	14b29272d9cce45b

Static PE Info

General

Entrypoint:	0x49b00a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61DB92BE [Mon Jan 10 01:58:22 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x99010	0x99200	False	0.802077487245	data	7.52177326572	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x9c000	0x41f0c	0x42000	False	0.324503580729	data	4.42459351507	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xde000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/14/22-15:55:34.288950	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	65447	8.8.8.8	192.168.2.5

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 15:55:34.180125952 CET	192.168.2.5	8.8.8.8	0xfa76	Standard query (0)	podzeye.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 15:55:34.288949966 CET	8.8.8.8	192.168.2.5	0xfa76	No error (0)	podzeye.duckdns.org		109.205.178.244	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: g94e4BgSRN.exe PID: 6384 Parent PID: 6140

General

Start time:	15:55:13
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\g94e4BgSRN.exe

Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\g94e4BgSRN.exe"
Imagebase:	0x270000
File size:	898560 bytes
MD5 hash:	D058C6416284F291D6BC7E183293DA1F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_NetWire_1, Description: Yara detected NetWire RAT, Source: 00000000.00000002.286467177.00000000026AB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.286586670.0000000002762000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_NetWire_1, Description: Yara detected NetWire RAT, Source: 00000000.00000002.287524308.0000000003873000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.286410302.0000000002631000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 6780 Parent PID: 6384

General

Start time:	15:55:23
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\SiEKNQVnm.exe
Imagebase:	0x380000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6788 Parent PID: 6780

General

Start time:	15:55:24
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: schtasks.exe PID: 6796 Parent PID: 6384

General

Start time:	15:55:24
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\SiEKNQVnm" /XML "C:\Users\user\AppData\Local\Temp\tmp2A91.tmp
Imagebase:	0xb0000
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

File Read

Analysis Process: conhost.exe PID: 6920 Parent PID: 6796

General

Start time:	15:55:25
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff797770000
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: g94e4BgSRN.exe PID: 6976 Parent PID: 6384

General

Start time:	15:55:26
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\g94e4BgSRN.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\g94e4BgSRN.exe
Imagebase:	0xbd0000
File size:	898560 bytes
MD5 hash:	D058C6416284F291D6BC7E183293DA1F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_NetWire_1, Description: Yara detected NetWire RAT, Source: 00000009.00000000.282165749.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_NetWire_1, Description: Yara detected NetWire RAT, Source: 00000009.00000000.280983052.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_NetWire_1, Description: Yara detected NetWire RAT, Source: 00000009.00000000.281635680.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_NetWire_1, Description: Yara detected NetWire RAT, Source: 00000009.00000002.516753076.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_NetWire_1, Description: Yara detected NetWire RAT, Source: 00000009.00000000.283998783.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_NetWire_1, Description: Yara detected NetWire RAT, Source: 00000009.00000000.276611463.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_NetWire_1, Description: Yara detected NetWire RAT, Source: 00000009.00000000.279964505.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis