ID: 557770
Sample Name: yAbf8Z3qA5.exe
Cookbook: default.jbs
Time: 16:16:25
Date: 21/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

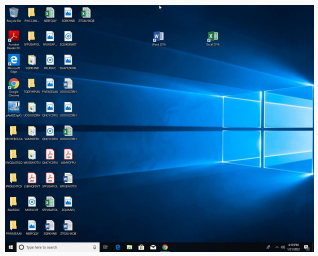
Windows Analysis Report

yAbf8Z3qA5.exe

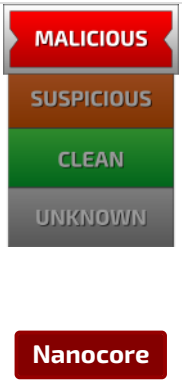
Overview

General Information

Sample Name:	yAbf8Z3qA5.exe
Analysis ID:	557770
MD5:	da3cb7622834a1..
SHA1:	2179db1ae11496.
SHA256:	78dd589c56a6d2..
Tags:	exe NanoCore RAT
Infos:	



Detection



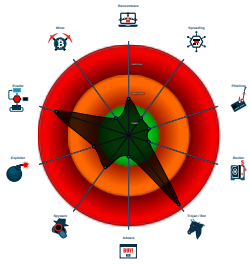
Nanocore

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Connects to many ports of the same…
- Tries to detect sandboxes and other…
- Sigma detected: Suspicius Add Tas…
- Machine Learning detection for sam…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- yAbf8Z3qA5.exe (PID: 6960 cmdline: "C:\Users\user\Desktop\yAbf8Z3qA5.exe" MD5: DA3CB7622834A14916D498C1BD8A7827)
  - schtasks.exe (PID: 5788 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\BYTkrh" /XML "C:\Users\user\AppData\Local\Temp\tmpFF62.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 2152 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - yAbf8Z3qA5.exe (PID: 6424 cmdline: {path} MD5: DA3CB7622834A14916D498C1BD8A7827)
  - yAbf8Z3qA5.exe (PID: 5964 cmdline: {path} MD5: DA3CB7622834A14916D498C1BD8A7827)
    - schtasks.exe (PID: 5884 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp6807.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 1256 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6340 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp6F7A.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 2320 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- yAbf8Z3qA5.exe (PID: 6476 cmdline: C:\Users\user\Desktop\yAbf8Z3qA5.exe 0 MD5: DA3CB7622834A14916D498C1BD8A7827)
  - schtasks.exe (PID: 5972 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\BYTkrh" /XML "C:\Users\user\AppData\Local\Temp\tmp41AB.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6644 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - yAbf8Z3qA5.exe (PID: 6716 cmdline: {path} MD5: DA3CB7622834A14916D498C1BD8A7827)
- dhcpmon.exe (PID: 4724 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: DA3CB7622834A14916D498C1BD8A7827)
  - schtasks.exe (PID: 6708 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\BYTkrh" /XML "C:\Users\user\AppData\Local\Temp\tmp4BCD.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7080 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 3924 cmdline: {path} MD5: DA3CB7622834A14916D498C1BD8A7827)
  - dhcpmon.exe (PID: 5844 cmdline: {path} MD5: DA3CB7622834A14916D498C1BD8A7827)
- dhcpmon.exe (PID: 6956 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: DA3CB7622834A14916D498C1BD8A7827)
  - schtasks.exe (PID: 240 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\BYTkrh" /XML "C:\Users\user\AppData\Local\Temp\tmp6E1A.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 392 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 6332 cmdline: {path} MD5: DA3CB7622834A14916D498C1BD8A7827)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001E.00000000.448894082.0000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000001E.00000000.448894082.0000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000001E.00000000.448894082.0000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000012.00000000.419515654.0000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000012.00000000.419515654.0000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 97 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.yAbf8Z3qA5.exe.5bb4629.9.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost
8.2.yAbf8Z3qA5.exe.5bb4629.9.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xb184:$x2: NanoCore.ClientPluginHost • 0xc25f:$s4: PipeCreated • 0xb19e:$s5: IClientLoggingHost
8.2.yAbf8Z3qA5.exe.5bb4629.9.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
8.2.yAbf8Z3qA5.exe.3ec9511.6.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
8.2.yAbf8Z3qA5.exe.3ec9511.6.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
Click to see the 80 entries				

Sigma Overview

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

System Summary

Sigma detected: Suspicius Add Task From User AppData Temp

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Jbx Signature Overview

AV Detection

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Connects to many ports of the same IP (likely port scanning)

Uses dynamic DNS services

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Yara detected AntiVM3

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

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

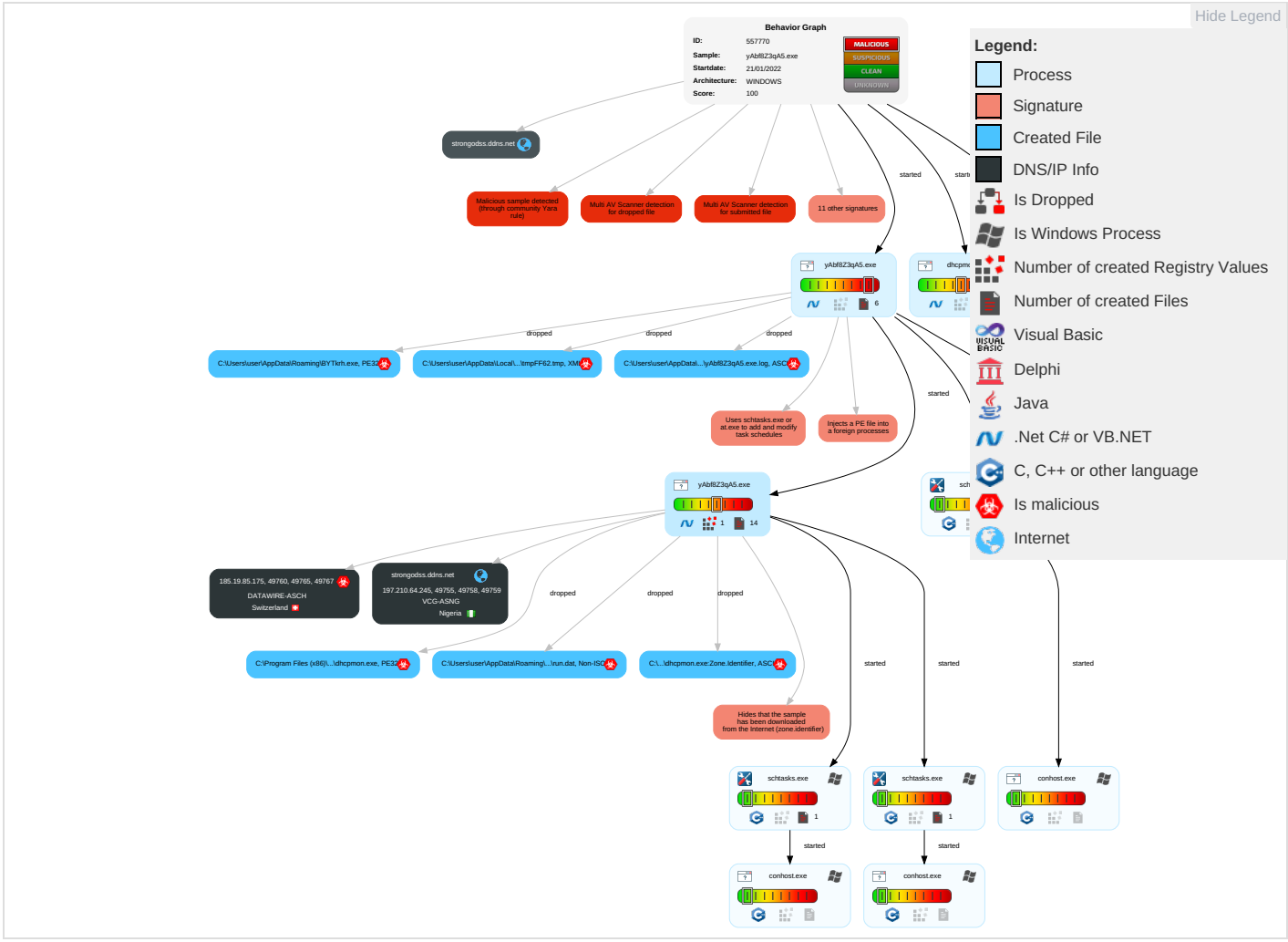
Detected Nanocore Rat

Yara detected Nanocore 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	Remote Service Effects	Impact
Valid Accounts	1 Scheduled Task/Job	1 Scheduled Task/Job	1 Access Token Manipulation	2 Masquerading	1 1 Input Capture	2 1 1 Security Software Discovery	Remote Services	1 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 1 2 Process Injection	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Scheduled Task/Job	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Access Token Manipulation	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 2 Process Injection	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	1 Non-Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	1 1 Application Layer Protocol	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 Obfuscated Files or Information	DCSync	1 3 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	3 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

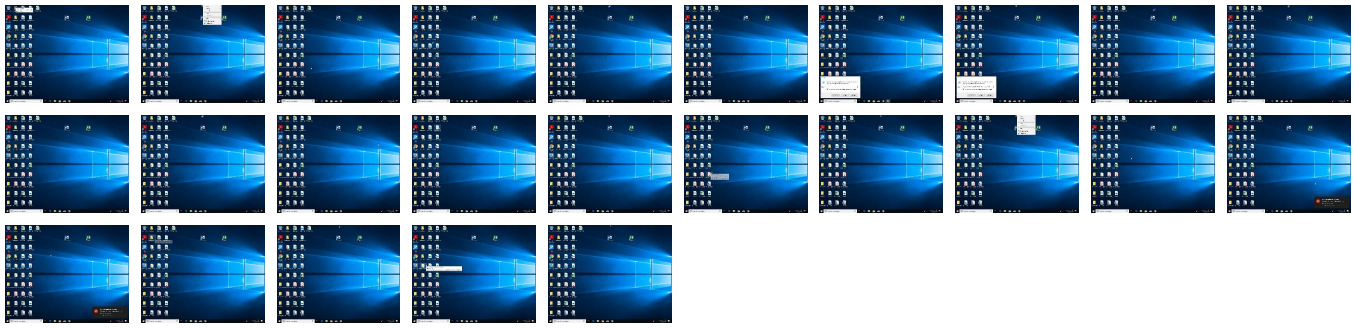
Behavior Graph



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
yAbf8Z3qA5.exe	40%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
yAbf8Z3qA5.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\BYTkrh.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	40%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\BYTkrh.exe	40%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.0.yAbf8Z3qA5.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
8.0.yAbf8Z3qA5.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.2.yAbf8Z3qA5.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.yAbf8Z3qA5.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.yAbf8Z3qA5.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.0.yAbf8Z3qA5.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.2.yAbf8Z3qA5.exe.5bb0000.10.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.carterandcone.comala	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.sakkal.comH	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.carterandcone.com)	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cny4i	0%	Avira URL Cloud	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.comm	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Negr	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Fm	0%	Avira URL Cloud	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.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.galapagosdesign.com/2	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/4	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	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.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
strongodss.ddns.net	197.210.64.245	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	yAbf8Z3qA5.exe, 00000000.00000002.392850274.0000000005DA2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	yAbf8Z3qA5.exe, 00000000.00000002.392850274.0000000005DA2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	yAbf8Z3qA5.exe, 00000000.00000002.392850274.0000000005DA2000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comala	yAbf8Z3qA5.exe, 00000000.00000003.353584518.0000000004B16000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	yAbf8Z3qA5.exe, 00000000.00000002.392850274.0000000005DA2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	yAbf8Z3qA5.exe, 00000000.00000002.392850274.0000000005DA2000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.html0	yAbf8Z3qA5.exe, 00000000.00000003.358953165.0000000004B45000.00000004.00000001.sdmp, yAbf8Z3qA5.exe, 00000000.00000003.358983600.0000000004B45000.00000004.00000001.sdmp, yAbf8Z3qA5.exe, 00000000.00000003.358928287.0000000004B45000.00000004.00000001.sdmp, yAbf8Z3qA5.exe, 00000000.00000003.358873383.0000000004B45000.00000004.00000001.sdmp, yAbf8Z3qA5.exe, 00000000.00000003.358901732.0000000004B45000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers?	yAbf8Z3qA5.exe, 00000000.00000002.392850274.0000000005DA2000.00000004.00000001.sdmp	false		high
http://www.sakkal.comH	yAbf8Z3qA5.exe, 00000000.00000003.355896740.0000000004B45000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	yAbf8Z3qA5.exe, 00000000.00000002.392850274.0000000005DA2000.00000004.00000001.sdmp, yAbf8Z3qA5.exe, 00000000.00000003.354609078.0000000004B15000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	yAbf8Z3qA5.exe, 00000000.00000002.392850274.0000000005DA2000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	yAbf8Z3qA5.exe, 00000000.00000002.392850274.0000000005DA2000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	yAbf8Z3qA5.exe, 00000000.00000003.354635060.0000000004B17000.00000004.00000001.sdmp, yAbf8Z3qA5.exe, 00000000.00000003.354609078.0000000004B15000.00000004.00000001.sdmp, yAbf8Z3qA5.exe, 00000000.00000003.353584518.0000000004B16000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com)	yAbf8Z3qA5.exe, 00000000.00000003.353584518.0000000004B16000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cny4i	yAbf8Z3qA5.exe, 00000000.00000003.353084236.0000000004B15000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://en.w	yAbf8Z3qA5.exe, 00000000.00000003.350523936.0000000004B19000.00000004.00000001.sdmp, yAbf8Z3qA5.exe, 00000000.00000003.354609078.0000000004B15000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comm	yAbf8Z3qA5.exe, 00000000.00000003.353584518.0000000004B16000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	yAbf8Z3qA5.exe, 00000000.00000002.392850274.0000000005DA2000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Negr	yAbf8Z3qA5.exe, 00000000.00000003.355077180.0000000004B18000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	yAbf8Z3qA5.exe, 00000000.00000002.392850274.0000000005DA2000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Fm	yAbf8Z3qA5.exe, 00000000.00000003.355077180.0000000004B18000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	yAbf8Z3qA5.exe, 00000000.00000002.392850274.0000000005DA2000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	yAbf8Z3qA5.exe, 00000000.00000002.392850274.0000000005DA2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	yAbf8Z3qA5.exe, 00000000.00000002.392850274.0000000005DA2000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	yAbf8Z3qA5.exe, 00000000.00000002.392850274.0000000005DA2000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	yAbf8Z3qA5.exe, 00000000.00000002.392850274.0000000005DA2000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	yAbf8Z3qA5.exe, 00000000.00000002.392850274.0000000005DA2000.00000004.00000001.sdmp, yAbf8Z3qA5.exe, 00000000.00000003.353065872.0000000004B1B000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-jones.html	yAbf8Z3qA5.exe, 00000000.00000003.358506319.0000000004B45000.00000004.00000001.sdmp, yAbf8Z3qA5.exe, 00000000.00000002.392850274.0000000005DA2000.00000004.00000001.sdmp, yAbf8Z3qA5.exe, 00000000.00000003.358477439.0000000004B45000.00000004.00000001.sdmp, yAbf8Z3qA5.exe, 00000000.00000003.358532023.0000000004B45000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/2	yAbf8Z3qA5.exe, 00000000.00000003.360074854.0000000004B45000.00000004.00000001.sdmp, yAbf8Z3qA5.exe, 00000000.00000003.360057596.0000000004B45000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/4	yAbf8Z3qA5.exe, 00000000.00000003.360074854.0000000004B45000.00000004.00000001.sdmp, yAbf8Z3qA5.exe, 00000000.00000003.360057596.0000000004B45000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	yAbf8Z3qA5.exe, 00000000.00000003.355077180.0000000004B18000.00000004.00000001.sdmp, yAbf8Z3qA5.exe, 00000000.00000002.392850274.0000000005DA2000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	yAbf8Z3qA5.exe, 00000000.00000002.392850274.0000000005DA2000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cno.	yAbf8Z3qA5.exe, 00000000.00000003.353584518.0000000004B16000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	yAbf8Z3qA5.exe, 00000000.00000002.392850274.0000000005DA2000.00000004.00000001.sdmp	false		high
http://www.ascendercorp.com/typedesigners.html	yAbf8Z3qA5.exe, 00000000.00000003.355947636.0000000004B4D000.00000004.00000001.sdmp, yAbf8Z3qA5.exe, 00000000.00000003.355902260.0000000004B4D000.00000004.00000001.sdmp, yAbf8Z3qA5.exe, 00000000.00000003.356028041.0000000004B4D000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	yAbf8Z3qA5.exe, 00000000.00000002.392850274.0000000005DA2000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	yAbf8Z3qA5.exe, 00000000.00000002.392850274.0000000005DA2000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	yAbf8Z3qA5.exe, 00000000.00000002.392850274.0000000005DA2000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	yAbf8Z3qA5.exe, 00000000.00000002.392850274.0000000005DA2000.00000004.00000001.sdmp, yAbf8Z3qA5.exe, 00000000.00000003.353584518.0000000004B16000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	yAbf8Z3qA5.exe, 00000000.00000002.392850274.0000000005DA2000.00000004.00000001.sdmp, yAbf8Z3qA5.exe, 00000000.00000003.355930974.0000000004B45000.00000004.00000001.sdmp, yAbf8Z3qA5.exe, 00000000.00000003.355896740.0000000004B45000.00000004.00000001.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.19.85.175	unknown	Switzerland		48971	DATAWIRE-ASCH	true
197.210.64.245	strongodss.ddns.net	Nigeria		29465	VCG-ASNG	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	557770
Start date:	21.01.2022
Start time:	16:16:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	yAbf8Z3qA5.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:	41
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.evad.winEXE@32/10@10/2
EGA Information:	• Successful, ratio: 80%
HDC Information:	Failed

HCA Information:	• Successful, ratio: 98% • 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

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- TCP Packets have been reduced to 100
- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target yAbf8Z3qA5.exe, PID 6424 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing behavior and disassembly information.
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: yAbf8Z3qA5.exe

Simulations

Behavior and APIs

Time	Type	Description
16:17:32	API Interceptor	809x Sleep call for process: yAbf8Z3qA5.exe modified
16:17:47	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\yAbf8Z3qA5.exe" s>$(Arg0)
16:17:47	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
16:17:50	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
16:17:52	API Interceptor	4x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\yAbf8Z3qA5.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1345024
Entropy (8bit):	7.685633845475471
Encrypted:	false
SSDEEP:	24576:KeZkjA8sCUrevlzuC6+iDUBQ2Kq1gekgwe0+U:lPCUczj/IYtKqq+F0+
MD5:	DA3CB7622834A14916D498C1BD8A7827
SHA1:	2179DB1AE11496EE06B62DFF337986316DD298EA
SHA-256:	78DD589C56A6D216F597F149BAD69D510A88FB3257B4A643A7250381126D963C
SHA-512:	88CA8D27EFB54EEB95278B6D4E92EF04E581362B2E110ABBB5E8F1BC715F0A6C1965AE5B52B567D45752F490B1FFE7188BD51672E8466F0160D7030DBBC4E68F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 40%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....~.a.....P.....v.... ... .@.. ....@.....$...O.... ....H.....text...|.... ....`.rsrc..... .....@..@.reloc..... .....@..B.....X.....H.....l[..p.....-.....0.....(....(.....(.....o....*.....(.....(.....(!.....("......(#....*N..(....o{...($....*&..(%....*.s&.....s'.....s(.....s).....s*.....*....0.....~....o+....+..*.0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0..<.....~.....(0.....,r..p.....(1...o2...s3.....~.....+..*.0.....

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

Process:	C:\Users\user\Desktop\yAbf8Z3qA5.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

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

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk70U2xANlW3ANv:MLF20NaL3z2p29hJ5g522rW2xAi3A9
MD5:	B1DB55991C3DA14E35249AEA1BC357CA
SHA1:	0DD2D91198FDEF296441B12F1A906669B279700C
SHA-256:	34D3E48321D5010AD2BD1F3F0B728077E4F5A7F70D66FA36B57E5209580B6BDC
SHA-512:	BE38A31888C9C2F8047FA9C99672CB985179D325107514B7500DDA9523AE3E1D20B45EACC4E6C8A5D096360D0FBB98A120E63F38FFE324DF8A0559F6890CC80
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\35774dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\yAbf8Z3qA5.exe.log	
Process:	C:\Users\user\Desktop\yAbf8Z3qA5.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	664
Entropy (8bit):	5.288448637977022
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk70U2xANlW3ANv:MLF20NaL3z2p29hJ5g522rW2xAi3A9
MD5:	B1DB55991C3DA14E35249AEA1BC357CA
SHA1:	0DD2D91198FDEF296441B12F1A906669B279700C
SHA-256:	34D3E48321D5010AD2BD1F3F0B728077E4F5A7F70D66FA36B57E5209580B6BDC
SHA-512:	BE38A31888C9C2F8047FA9C99672CB985179D325107514B7500DDA9523AE3E1D20B45EACC4E6C8A5D096360D0FBB98A120E63F38FFE324DF8A0559F6890CC80
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\35774dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp41AB.tmp	
Process:	C:\Users\user\Desktop\yAbf8Z3qA5.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1651
Entropy (8bit):	5.156446005056579
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB39Jtn:cbha7JlNQV/rydbz9I3YODOLNdq3z
MD5:	1F1ED6DCB0690C7C70883B9C5407E7BA
SHA1:	0BB3A61D72782A9CB28B5761334D05E946179B5D
SHA-256:	327FAC04E79BC23D133642CDB0CAEE81C09FBC95DA0775F37365CCA63F2E74F9
SHA-512:	1E475FF6C405B67871EFC616507777F8B962AAFA9F1DAF5BA309763B884CA9EC5972D483DD04A3CA89F89231A3D3BC8499CDC8DB95DE65A484E49E02FF27CBB2
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>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>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

C:\Users\user\AppData\Local\Temp\tmp4BCD.tmp	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB39Jtn:cbha7JlNQV/rydbz9I3YODOLNdq3z
MD5:	1F1ED6DCB0690C7C70883B9C5407E7BA
SHA1:	0BB3A61D72782A9CB28B5761334D05E946179B5D
SHA-256:	327FAC04E79BC23D133642CDB0CAEE81C09FBC95DA0775F37365CCA63F2E74F9
SHA-512:	1E475FF6C405B67871EFC616507777F8B962AAFA9F1DAF5BA309763B884CA9EC5972D483DD04A3CA89F89231A3D3BC8499CDC8DB95DE65A484E49E02FF27CBB2
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>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>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

C:\Users\user\AppData\Local\Temp\tmp6807.tmp	
Process:	C:\Users\user\Desktop\yAbf8Z3qA5.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1303
Entropy (8bit):	5.115382657290805
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Vjujxtn:cbk4oL600QydbQxIYODOLedq3lj
MD5:	299E78C1E1B6B7A33638B3585031F313
SHA1:	7ED90F3F1DCA6AFB31BD276F375CCF8F910D396B
SHA-256:	7D7A3F00F200FF08CD721FE52B539E76CB32B61427552C24F478E93A8F856E5C
SHA-512:	D1D04F8AC16483FAC228A618B05C58852A7AE91A18DEB401FCBD270AA9AB6F62FAF687BEF38B0837D77EC61508458E3CBA5C50ADFF903526D80A2C736CFA8578
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp6F7A.tmp	
Process:	C:\Users\user\Desktop\yAbf8Z3qA5.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755734
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpFF62.tmp	
Process:	C:\Users\user\Desktop\yAbf8Z3qA5.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1651
Entropy (8bit):	5.156446005056579
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB39Jtn:cbha7JlNQV/rydbz9l3YODOLNdq3z
MD5:	1F1ED6DCB0690C7C70883B9C5407E7BA
SHA1:	0BB3A61D72782A9CB28B5761334D05E946179B5D
SHA-256:	327FAC04E79BC23D133642CDB0CAEE81C09FBC95DA0775F37365CCA63F2E74F9
SHA-512:	1E475FF6C405B67871EFC616507777F8B962AAFA9F1DAF5BA309763B884CA9EC5972D483DD04A3CA89F89231A3D3BC8499CDC8DB95DE65A484E49E02FF27CBB2
Malicious:	**true**
Reputation:	unknown

Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>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>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

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

Process:	C:\Users\user\Desktop\yAbf8Z3qA5.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1345024
Entropy (8bit):	7.685633845475471
Encrypted:	false
SSDEEP:	24576:KeZkjA8sCUrevlzuC6+iDUBQ2Kq1gekgwe0+U:lPCUczj/IYtKqq+F0+
MD5:	DA3CB7622834A14916D498C1BD8A7827
SHA1:	2179DB1AE11496EE06B62DFF337986316DD298EA
SHA-256:	78DD589C56A6D216F597F149BAD69D510A88FB3257B4A643A7250381126D963C
SHA-512:	88CA8D27EFB54EEB95278B6D4E92EF04E581362B2E110ABBB5E8F1BC715F0A6C1965AE5B52B567D45752F490B1FFE7188BD51672E8466F0160D7030DBBC4E68F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 40%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....~.a.....P.....v.... ... .@.. .....@.....$...O.... ....H.....text...|.... ....`.rsrc..... .....@..@.reloc..... .....@..B.....X.....H.....l[..p.....-.....0.....(....(.....(.....o....*.....(.....(.....(!.....("......(#....*N..(....o{...($....*&..(%....*.s&.....s'.....s(.....s).....s*.....*....0.....~....o+....+..*.0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0..<.....~.....(0.....,!r...p.....(1...o2...s3.....~.....+..*.0.....

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

Process:	C:\Users\user\Desktop\yAbf8Z3qA5.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Yn:Y
MD5:	260CF674E1D2A820772E05F5F664454E
SHA1:	5CA7793E2231AC24C380FA1319407CC9E5343F15
SHA-256:	8EE13863FABB31C5847A2261EEAEB206BD218935970C03F99E57B6C1D247A3A9
SHA-512:	FC5BFC372ABBF6C76B6C5F9BDDAB151ED49A266F867EC5CD5E6FF6B68E59C40B8DEDF53676B899E06D68368DEF381215BCC88E5DD6D6A6B90070D6A74D45F519
Malicious:	**true**
Reputation:	unknown
Preview:	...<..H

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

Process:	C:\Users\user\Desktop\yAbf8Z3qA5.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	40
Entropy (8bit):	4.361768795973195
Encrypted:	false
SSDEEP:	3:oNN2+WckHD9WYAC:oNN2Rcs9+C
MD5:	8504094015EBA61D260077BE38F2111C
SHA1:	5B65E0E790BE98B27BEC8410A30F677BCFF0204A
SHA-256:	A8114F0BC6DA94929300F977D1A9CE21E7D6EBDE2A45DAD38DD24527428E4EB0
SHA-512:	387ADC1C0479B0B4DF2A78D4E791F43C147D60B6B4C1C61E5B1B4013298280F7B29E3DBCF84F140E79433A6EC7957F6887164B95818BEF8E46DC13311F47F1F9
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\Desktop\yAbf8Z3qA5.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.685633845475471
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	yAbf8Z3qA5.exe
File size:	1345024
MD5:	da3cb7622834a14916d498c1bd8a7827
SHA1:	2179db1ae11496ee06b62dff337986316dd298ea
SHA256:	78dd589c56a6d216f597f149bad69d510a88fb3257b4a643a7250381126d963c
SHA512:	88ca8d27efb54eeb95278b6d4e92ef04e581362b2e110abbb5e8f1bc715f0a6c1965ae5b52b567d45752f490b1ffe7188bd51672e8466f0160d7030dbbc4e68f
SSDEEP:	24576:KeZkjA8sCUrevlzuC6+iDUBQ2Kq1gekgwe0+U:lPCUczj/IYtKqq+F0+
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....~.a.....P.....v.... ... .@.. ..... @.....

File Icon

Icon Hash:	6e6a42e0b0a4a90d

Static PE Info

General

Entrypoint:	0x540f76
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:	0x61EA7EFF [Fri Jan 21 09:38:07 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x140f24	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x142000	0x9010	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x14c000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x140dec	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x13ef7c	0x13f000	False	0.818539993143	data	7.7042659795	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x142000	0x9010	0x9200	False	0.611515410959	data	6.45284679846	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x14c000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x142160	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x1425d8	0x10a8	data		
RT_ICON	0x143690	0x25a8	data		
RT_ICON	0x145c48	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0x149e80	0x3e	data		
RT_VERSION	0x149ed0	0x314	data		
RT_MANIFEST	0x14a1f4	0xe15	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2013
Assembly Version	1.0.0.0
InternalName	77vrr.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	BattleShip
ProductVersion	1.0.0.0
FileDescription	BattleShip
OriginalFilename	77vrr.exe

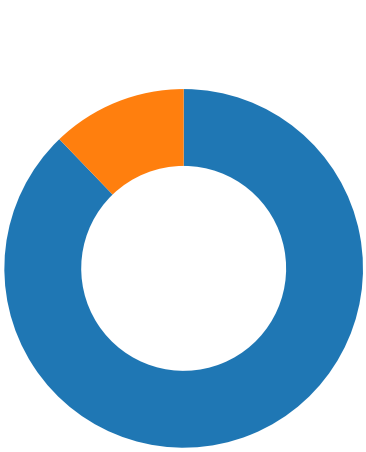
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/21/22-16:17:50.971618	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	62044	8.8.8.8	192.168.2.6
01/21/22-16:17:57.271132	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64267	8.8.8.8	192.168.2.6
01/21/22-16:18:03.701058	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49448	8.8.8.8	192.168.2.6
01/21/22-16:18:39.178099	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56061	8.8.8.8	192.168.2.6
01/21/22-16:19:04.301739	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49694	8.8.8.8	192.168.2.6
01/21/22-16:19:10.447228	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50010	8.8.8.8	192.168.2.6
01/21/22-16:19:16.524506	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63718	8.8.8.8	192.168.2.6

Network Port Distribution

Total Packets: 82



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2022 16:17:51.072984934 CET	49755	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:17:51.218764067 CET	50421	49755	197.210.64.245	192.168.2.6
Jan 21, 2022 16:17:51.218902111 CET	49755	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:17:51.733867884 CET	49755	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:17:52.171371937 CET	49755	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:17:53.140212059 CET	49755	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:17:53.157457113 CET	49755	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:17:57.274210930 CET	49758	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:17:57.421838999 CET	50421	49758	197.210.64.245	192.168.2.6
Jan 21, 2022 16:17:57.424499989 CET	49758	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:17:57.921921968 CET	49758	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:17:58.466593981 CET	49758	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:17:59.391395092 CET	49758	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:18:03.815294027 CET	49759	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:18:03.961352110 CET	50421	49759	197.210.64.245	192.168.2.6
Jan 21, 2022 16:18:03.961550951 CET	49759	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:18:04.422511101 CET	49759	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:18:04.922487974 CET	49759	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:18:05.861016989 CET	49759	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:18:09.878415108 CET	49760	50421	192.168.2.6	185.19.85.175
Jan 21, 2022 16:18:09.946851969 CET	50421	49760	185.19.85.175	192.168.2.6
Jan 21, 2022 16:18:10.454190969 CET	49760	50421	192.168.2.6	185.19.85.175
Jan 21, 2022 16:18:10.532551050 CET	50421	49760	185.19.85.175	192.168.2.6
Jan 21, 2022 16:18:11.047961950 CET	49760	50421	192.168.2.6	185.19.85.175
Jan 21, 2022 16:18:11.140558004 CET	50421	49760	185.19.85.175	192.168.2.6
Jan 21, 2022 16:18:15.174679041 CET	49765	50421	192.168.2.6	185.19.85.175
Jan 21, 2022 16:18:15.267647028 CET	50421	49765	185.19.85.175	192.168.2.6
Jan 21, 2022 16:18:15.869158983 CET	49765	50421	192.168.2.6	185.19.85.175
Jan 21, 2022 16:18:15.949668884 CET	50421	49765	185.19.85.175	192.168.2.6
Jan 21, 2022 16:18:16.626976013 CET	49765	50421	192.168.2.6	185.19.85.175
Jan 21, 2022 16:18:16.710320950 CET	50421	49765	185.19.85.175	192.168.2.6
Jan 21, 2022 16:18:20.809263945 CET	49767	50421	192.168.2.6	185.19.85.175
Jan 21, 2022 16:18:20.868350029 CET	50421	49767	185.19.85.175	192.168.2.6
Jan 21, 2022 16:18:21.470772982 CET	49767	50421	192.168.2.6	185.19.85.175
Jan 21, 2022 16:18:21.547738075 CET	50421	49767	185.19.85.175	192.168.2.6
Jan 21, 2022 16:18:22.174002886 CET	49767	50421	192.168.2.6	185.19.85.175
Jan 21, 2022 16:18:22.268377066 CET	50421	49767	185.19.85.175	192.168.2.6
Jan 21, 2022 16:18:26.466319084 CET	49774	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:18:26.611617088 CET	50421	49774	197.210.64.245	192.168.2.6
Jan 21, 2022 16:18:26.612207890 CET	49774	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:18:27.315038919 CET	49774	50421	192.168.2.6	197.210.64.245

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2022 16:18:27.815181017 CET	49774	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:18:28.705729008 CET	49774	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:18:28.721959114 CET	49774	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:18:32.912208080 CET	49776	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:18:33.057452917 CET	50421	49776	197.210.64.245	192.168.2.6
Jan 21, 2022 16:18:33.058423996 CET	49776	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:18:33.492155075 CET	49776	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:18:33.909244061 CET	49776	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:18:34.768690109 CET	49776	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:18:34.865149021 CET	49776	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:18:39.183901072 CET	49782	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:18:39.329766989 CET	50421	49782	197.210.64.245	192.168.2.6
Jan 21, 2022 16:18:39.333028078 CET	49782	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:18:39.769150019 CET	49782	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:18:40.187252998 CET	49782	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:18:41.050555944 CET	49782	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:18:42.816245079 CET	49782	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:18:43.254746914 CET	49782	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:18:47.275649071 CET	49789	50421	192.168.2.6	185.19.85.175
Jan 21, 2022 16:18:47.389262915 CET	50421	49789	185.19.85.175	192.168.2.6
Jan 21, 2022 16:18:48.004471064 CET	49789	50421	192.168.2.6	185.19.85.175
Jan 21, 2022 16:18:48.055279016 CET	50421	49789	185.19.85.175	192.168.2.6
Jan 21, 2022 16:18:48.613648891 CET	49789	50421	192.168.2.6	185.19.85.175
Jan 21, 2022 16:18:48.655435085 CET	50421	49789	185.19.85.175	192.168.2.6
Jan 21, 2022 16:18:52.663012028 CET	49793	50421	192.168.2.6	185.19.85.175
Jan 21, 2022 16:18:52.736879110 CET	50421	49793	185.19.85.175	192.168.2.6
Jan 21, 2022 16:18:53.317142010 CET	49793	50421	192.168.2.6	185.19.85.175
Jan 21, 2022 16:18:53.379509926 CET	50421	49793	185.19.85.175	192.168.2.6
Jan 21, 2022 16:18:54.004715919 CET	49793	50421	192.168.2.6	185.19.85.175
Jan 21, 2022 16:18:54.073517084 CET	50421	49793	185.19.85.175	192.168.2.6
Jan 21, 2022 16:18:58.302335024 CET	49810	50421	192.168.2.6	185.19.85.175
Jan 21, 2022 16:18:58.388991117 CET	50421	49810	185.19.85.175	192.168.2.6
Jan 21, 2022 16:18:59.036577940 CET	49810	50421	192.168.2.6	185.19.85.175
Jan 21, 2022 16:18:59.087620974 CET	50421	49810	185.19.85.175	192.168.2.6
Jan 21, 2022 16:18:59.640844107 CET	49810	50421	192.168.2.6	185.19.85.175
Jan 21, 2022 16:18:59.742108107 CET	50421	49810	185.19.85.175	192.168.2.6
Jan 21, 2022 16:19:04.303606033 CET	49823	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:19:04.448939085 CET	50421	49823	197.210.64.245	192.168.2.6
Jan 21, 2022 16:19:04.451667070 CET	49823	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:19:04.945883989 CET	49823	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:19:05.445226908 CET	49823	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:19:06.327164888 CET	49823	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:19:06.358948946 CET	49823	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:19:10.448999882 CET	49832	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:19:10.594268084 CET	50421	49832	197.210.64.245	192.168.2.6
Jan 21, 2022 16:19:10.597939968 CET	49832	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:19:11.030746937 CET	49832	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:19:11.452538967 CET	49832	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:19:12.311923027 CET	49832	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:19:12.452961922 CET	49832	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:19:16.526200056 CET	49833	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:19:16.672190905 CET	50421	49833	197.210.64.245	192.168.2.6
Jan 21, 2022 16:19:16.672384024 CET	49833	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:19:17.152721882 CET	49833	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:19:17.577976942 CET	49833	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:19:18.452989101 CET	49833	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:19:19.204643011 CET	49833	50421	192.168.2.6	197.210.64.245
Jan 21, 2022 16:19:23.220956087 CET	49834	50421	192.168.2.6	185.19.85.175
Jan 21, 2022 16:19:23.331912994 CET	50421	49834	185.19.85.175	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2022 16:17:50.858752966 CET	62044	53	192.168.2.6	8.8.8.8
Jan 21, 2022 16:17:50.971617937 CET	53	62044	8.8.8.8	192.168.2.6
Jan 21, 2022 16:17:57.240945101 CET	64267	53	192.168.2.6	8.8.8.8
Jan 21, 2022 16:17:57.271131992 CET	53	64267	8.8.8.8	192.168.2.6
Jan 21, 2022 16:18:03.679944992 CET	49448	53	192.168.2.6	8.8.8.8
Jan 21, 2022 16:18:03.701057911 CET	53	49448	8.8.8.8	192.168.2.6
Jan 21, 2022 16:18:26.446173906 CET	58384	53	192.168.2.6	8.8.8.8
Jan 21, 2022 16:18:26.463682890 CET	53	58384	8.8.8.8	192.168.2.6
Jan 21, 2022 16:18:32.849071026 CET	60261	53	192.168.2.6	8.8.8.8
Jan 21, 2022 16:18:32.866501093 CET	53	60261	8.8.8.8	192.168.2.6
Jan 21, 2022 16:18:39.156146049 CET	56061	53	192.168.2.6	8.8.8.8
Jan 21, 2022 16:18:39.178098917 CET	53	56061	8.8.8.8	192.168.2.6
Jan 21, 2022 16:19:04.282772064 CET	49694	53	192.168.2.6	8.8.8.8
Jan 21, 2022 16:19:04.301738977 CET	53	49694	8.8.8.8	192.168.2.6
Jan 21, 2022 16:19:10.426218987 CET	50010	53	192.168.2.6	8.8.8.8
Jan 21, 2022 16:19:10.447227955 CET	53	50010	8.8.8.8	192.168.2.6
Jan 21, 2022 16:19:16.503427982 CET	63718	53	192.168.2.6	8.8.8.8
Jan 21, 2022 16:19:16.524506092 CET	53	63718	8.8.8.8	192.168.2.6
Jan 21, 2022 16:19:38.879863977 CET	62116	53	192.168.2.6	8.8.8.8
Jan 21, 2022 16:19:38.897433996 CET	53	62116	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 21, 2022 16:17:50.858752966 CET	192.168.2.6	8.8.8.8	0xa512	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Jan 21, 2022 16:17:57.240945101 CET	192.168.2.6	8.8.8.8	0x2ed4	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Jan 21, 2022 16:18:03.679944992 CET	192.168.2.6	8.8.8.8	0x2acb	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Jan 21, 2022 16:18:26.446173906 CET	192.168.2.6	8.8.8.8	0x65f4	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Jan 21, 2022 16:18:32.849071026 CET	192.168.2.6	8.8.8.8	0xf095	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Jan 21, 2022 16:18:39.156146049 CET	192.168.2.6	8.8.8.8	0x9947	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Jan 21, 2022 16:19:04.282772064 CET	192.168.2.6	8.8.8.8	0xee39	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Jan 21, 2022 16:19:10.426218987 CET	192.168.2.6	8.8.8.8	0xc57b	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Jan 21, 2022 16:19:16.503427982 CET	192.168.2.6	8.8.8.8	0x53eb	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Jan 21, 2022 16:19:38.879863977 CET	192.168.2.6	8.8.8.8	0xbd07	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)

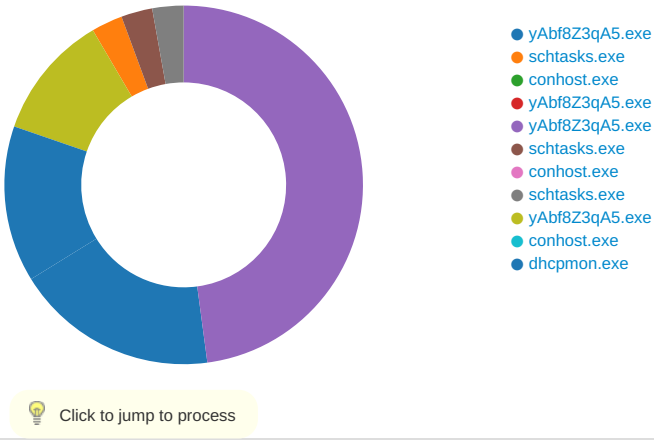
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 21, 2022 16:17:50.971617937 CET	8.8.8.8	192.168.2.6	0xa512	No error (0)	strongodss .ddns.net		197.210.64.245	A (IP address)	IN (0x0001)
Jan 21, 2022 16:17:57.271131992 CET	8.8.8.8	192.168.2.6	0x2ed4	No error (0)	strongodss .ddns.net		197.210.64.245	A (IP address)	IN (0x0001)
Jan 21, 2022 16:18:03.701057911 CET	8.8.8.8	192.168.2.6	0x2acb	No error (0)	strongodss .ddns.net		197.210.64.245	A (IP address)	IN (0x0001)
Jan 21, 2022 16:18:26.463682890 CET	8.8.8.8	192.168.2.6	0x65f4	No error (0)	strongodss .ddns.net		197.210.64.245	A (IP address)	IN (0x0001)
Jan 21, 2022 16:18:32.866501093 CET	8.8.8.8	192.168.2.6	0xf095	No error (0)	strongodss .ddns.net		197.210.64.245	A (IP address)	IN (0x0001)
Jan 21, 2022 16:18:39.178098917 CET	8.8.8.8	192.168.2.6	0x9947	No error (0)	strongodss .ddns.net		197.210.64.245	A (IP address)	IN (0x0001)
Jan 21, 2022 16:19:04.301738977 CET	8.8.8.8	192.168.2.6	0xee39	No error (0)	strongodss .ddns.net		197.210.64.245	A (IP address)	IN (0x0001)
Jan 21, 2022 16:19:10.447227955 CET	8.8.8.8	192.168.2.6	0xc57b	No error (0)	strongodss .ddns.net		197.210.64.245	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 21, 2022 16:19:16.524506092 CET	8.8.8.8	192.168.2.6	0x53eb	No error (0)	strongodss .ddns.net		197.210.64.245	A (IP address)	IN (0x0001)
Jan 21, 2022 16:19:38.897433996 CET	8.8.8.8	192.168.2.6	0xbd07	No error (0)	strongodss .ddns.net		197.210.64.245	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: yAbf8Z3qA5.exe PID: **6960**, Parent PID: **1604**

General

Start time:	16:17:25
Start date:	21/01/2022
Path:	C:\Users\user\Desktop\yAbf8Z3qA5.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\yAbf8Z3qA5.exe"
Imagebase:	0x20000
File size:	1345024 bytes
MD5 hash:	DA3CB7622834A14916D498C1BD8A7827
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.394239368.000000000C531000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.394239368.000000000C531000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.394239368.000000000C531000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming\BYTkrh.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	BCBF83	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpFF62.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	BCB5FC	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\yAbf8Z3qA5.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpFF62.tmp	success or wait	1	2300B0E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\BYTkrh.exe	0	1345024	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 7e fd 61 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 50 00 00 fd 13 00 00 fd 00 00 00 00 00 00 76 0f 14 00 00 20 00 00 00 20 14 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 14 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL~aPv @ @	success or wait	1	2300223	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpFF62.tmp	0	1651	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f	<?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> </Registratio	success or wait	1	2300223	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\yAbf8Z3qA5.exe.log	0	664	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 23 5c 63 64 37 63 37 34 66 63 65 32 61 30 65 61 62 37 32 63 64 32 35 63 62 65 34 62 62 36 31 36 31 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	1,"fusion","GAC",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Users\user\Desktop\yAbf8Z3qA5.exe	unknown	1345024	success or wait	1	2300223	ReadFile

Analysis Process: schtasks.exe PID: **5788**, Parent PID: **6960**

General

Start time:	16:17:35

Start date:	21/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\BYTkrh" /XML "C:\Users\user\AppData\Local\Temp\tmpFF62.tmp
Imagebase:	0x1170000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpFF62.tmp	unknown	2	success or wait	1	117AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpFF62.tmp	unknown	1652	success or wait	1	117ABD9	ReadFile

Analysis Process: conhost.exe PID: **2152**, Parent PID: **5788**

General

Start time:	16:17:36
Start date:	21/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: yAbf8Z3qA5.exe PID: **6424**, Parent PID: **6960**

General

Start time:	16:17:36
Start date:	21/01/2022
Path:	C:\Users\user\Desktop\yAbf8Z3qA5.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x120000
File size:	1345024 bytes
MD5 hash:	DA3CB7622834A14916D498C1BD8A7827
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: yAbf8Z3qA5.exe PID: **5964**, Parent PID: **6960**

General

Start time:	16:17:38
Start date:	21/01/2022
Path:	C:\Users\user\Desktop\yAbf8Z3qA5.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x790000
File size:	1345024 bytes
MD5 hash:	DA3CB7622834A14916D498C1BD8A7827
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.630595587.0000000005BB0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.630595587.0000000005BB0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.630595587.0000000005BB0000.00000004.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.630568364.0000000005BA0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.630568364.0000000005BA0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000000.380197922.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000000.380197922.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000000.380197922.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.628097807.0000000003EB7000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.628097807.0000000003EB7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000000.380861261.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000000.380861261.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000000.380861261.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.630404786.0000000005900000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.630404786.0000000005900000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.623546911.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.623546911.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.623546911.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000000.378603204.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000000.378603204.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000000.378603204.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000000.383163459.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000000.383163459.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000000.383163459.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	51D07A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	51D089B	CreateFileW
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	51D07A1	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	51D0B20	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	51D0B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp6807.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	51D0D1C	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	51D089B	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp6F7A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	51D0D1C	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	51D07A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	51D07A1	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp6807.tmp	success or wait	1	72637D95	unknown
C:\Users\user\AppData\Local\Temp\tmp6F7A.tmp	success or wait	1	72637D95	unknown
C:\Users\user\Desktop\yAbf8Z3qA5.exe:Zone.Identifier	success or wait	1	51D114D	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	fd fd dc 3c fd fd 48	<H	success or wait	1	51D0A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 7e fd 61 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 50 00 00 fd 13 00 00 fd 00 00 00 00 00 00 76 0f 14 00 00 20 00 00 00 20 14 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 14 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL~aPv @ @	success or wait	6	51D0B20	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	51D0B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp6807.tmp	0	1303	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	51D0A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	0	40	43 3a 5c 55 73 65 72 73 5c 65 6e 67 69 6e 65 65 72 5c 44 65 73 6b 74 6f 70 5c 79 41 62 66 38 5a 33 71 41 35 2e 65 78 65	C:\Users\user\Desktop\yAbf8Z3qA5.exe	success or wait	1	51D0A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp6F7A.tmp	0	1310	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	51D0A53	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7308BF06	unknown
C:\Users\user\Desktop\yAbf8Z3qA5.exe	unknown	4096	success or wait	1	7308BF06	unknown
C:\Users\user\Desktop\yAbf8Z3qA5.exe	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	51D0A53	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	51D0C12	RegSetValueExW

Analysis Process: schtasks.exe PID: **5884**, Parent PID: **5964**

General

Start time:	16:17:45
Start date:	21/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp6807.tmp

Imagebase:	0x1170000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp6807.tmp	unknown	2	success or wait	1	117AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp6807.tmp	unknown	1304	success or wait	1	117ABD9	ReadFile

Analysis Process: conhost.exe PID: **1256**, Parent PID: **5884**

General

Start time:	16:17:46
Start date:	21/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: **6340**, Parent PID: **5964**

General

Start time:	16:17:47
Start date:	21/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp6F7A.tmp
Imagebase:	0x1170000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp6F7A.tmp	unknown	2	success or wait	1	117AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp6F7A.tmp	unknown	1311	success or wait	1	117ABD9	ReadFile

Analysis Process: yAbf8Z3qA5.exe PID: **6476**, Parent PID: **936**

General

Start time:	16:17:48
Start date:	21/01/2022
Path:	C:\Users\user\Desktop\yAbf8Z3qA5.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\yAbf8Z3qA5.exe 0
Imagebase:	0xf30000
File size:	1345024 bytes
MD5 hash:	DA3CB7622834A14916D498C1BD8A7827
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.440223202.000000000D2E1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.440223202.000000000D2E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.440223202.000000000D2E1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Local\Temp\tmp41AB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	1ADB5FC	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp41AB.tmp	success or wait	1	3260A5E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp41AB.tmp	0	1651	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f	<?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> </Registratio	success or wait	1	326071B	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: conhost.exe PID: **2320**, Parent PID: **6340**

General

Start time:	16:17:48
Start date:	21/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: dhcpmon.exe PID: **4724**, Parent PID: **936**

General

Start time:	16:17:50
Start date:	21/01/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0xd60000

File size:	1345024 bytes
MD5 hash:	DA3CB7622834A14916D498C1BD8A7827
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.455188416.000000000CEF1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.455188416.000000000CEF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.455188416.000000000CEF1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 40%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Local\Temp\tmp4BCD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	725E9869	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4BCD.tmp	success or wait	1	18E0A5E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4BCD.tmp	0	1651	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f	<?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> </Registratio	success or wait	1	18E071B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	0	664	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	1,"fusion","GAC",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Disassembly

No disassembly