ID: 432024
Sample Name: xtxr8lHa5F.exe
Cookbook: default.jbs
Time: 16:56:45
Date: 09/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report xtxr8lHa5F.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: NanoCore 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 6
AV Detection: 6
E-Banking Fraud: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Signature Overview 6
AV Detection: 6
Networking: 6
E-Banking Fraud: 6
System Summary: 6
Data Obfuscation: 6
Boot Survival: 6
Hooking and other Techniques for Hiding and Protection: 6
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
Contacted IPs 11
Public 11
General Information 11
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASN 12
JA3 Fingerprints 12
Dropped Files 13
Created / dropped Files 13
Static File Info 17
General 17
File Icon 17
Static PE Info 17
General 17
Entrypoint Preview 18
Data Directories 18
Sections 18
Resources 18
Imports 18
Version Infos 18
Network Behavior 18
Snort IDS Alerts 18
Network Port Distribution 18
TCP Packets 19
UDP Packets 19
Code Manipulations 19
Statistics 19

Behavior 19
System Behavior 19
Analysis Process: xtxr8lHa5F.exe PID: 5352 Parent PID: 5544 19
General 19
File Activities 19
File Created 19
File Deleted 19
File Written 19
File Read 19
Analysis Process: schtasks.exe PID: 3696 Parent PID: 5352 20
General 20
File Activities 20
File Read 20
Analysis Process: conhost.exe PID: 5256 Parent PID: 3696 20
General 20
Analysis Process: MSBuild.exe PID: 5260 Parent PID: 5352 20
General 20
Analysis Process: MSBuild.exe PID: 5268 Parent PID: 5352 21
General 21
File Activities 22
File Created 22
File Deleted 22
File Written 22
File Read 22
Registry Activities 22
Key Value Created 22
Analysis Process: schtasks.exe PID: 5020 Parent PID: 5268 22
General 22
File Activities 23
File Read 23
Analysis Process: conhost.exe PID: 5012 Parent PID: 5020 23
General 23
Analysis Process: schtasks.exe PID: 3564 Parent PID: 5268 23
General 23
File Activities 23
File Read 23
Analysis Process: conhost.exe PID: 3016 Parent PID: 3564 24
General 24
Analysis Process: MSBuild.exe PID: 3508 Parent PID: 528 24
General 24
File Activities 24
File Created 24
File Written 24
File Read 24
Analysis Process: conhost.exe PID: 1648 Parent PID: 3508 24
General 24
Analysis Process: dhcpmon.exe PID: 1180 Parent PID: 528 25
General 25
File Activities 25
File Created 25
File Written 25
File Read 25
Analysis Process: conhost.exe PID: 1260 Parent PID: 1180 25
General 25
Analysis Process: dhcpmon.exe PID: 3776 Parent PID: 3388 25
General 25
File Activities 26
File Created 26
File Written 26
File Read 26
Analysis Process: conhost.exe PID: 996 Parent PID: 3776 26
General 26
Disassembly 26
Code Analysis 26

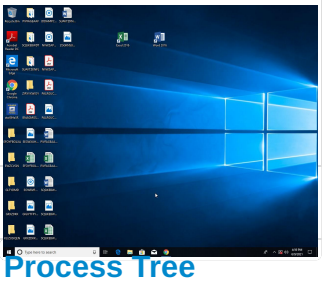
Analysis Report xtxr8lHa5F.exe

Overview

General Information

Sample Name:	xtxr8lHa5F.exe
Analysis ID:	432024
MD5:	c89c05d0f2853fa..
SHA1:	2e3a6adc296d26..
SHA256:	b2ec2e506bc974..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

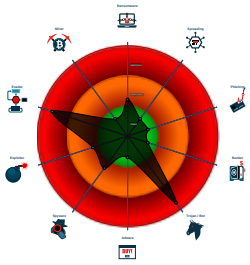
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- .NET source code references suspic…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- xtxr8lHa5F.exe (PID: 5352 cmdline: 'C:\Users\user\Desktop\xtxr8lHa5F.exe' MD5: C89C05D0F2853FA30B535AA2544006E5)
  - schtasks.exe (PID: 3696 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\rOKWrJ' /XML 'C:\Users\user\AppData\Local\Temp\tmp76E9.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5256 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - MSBuild.exe (PID: 5260 cmdline: {path} MD5: D621FD77BD585874F9686D3A76462EF1)
  - MSBuild.exe (PID: 5268 cmdline: {path} MD5: D621FD77BD585874F9686D3A76462EF1)
    - schtasks.exe (PID: 5020 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp604E.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5012 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 3564 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp6502.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 3016 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- MSBuild.exe (PID: 3508 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe 0 MD5: D621FD77BD585874F9686D3A76462EF1)
  - conhost.exe (PID: 1648 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 1180 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: D621FD77BD585874F9686D3A76462EF1)
  - conhost.exe (PID: 1260 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 3776 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: D621FD77BD585874F9686D3A76462EF1)
  - conhost.exe (PID: 996 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "ab394965-c5ce-4154-ad1c-da01ecc2",
  "Group": "Mamie",
  "Domain1": "82.64.141.173",
  "Domain2": "82.64.141.173",
  "Port": 6666,
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000013.00000002.490364012.00000000069C0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x59eb:$x1: NanoCore.ClientPluginHost • 0x5b48:$x2: IClientNetworkHost
00000013.00000002.490364012.00000000069C0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x59eb:$x2: NanoCore.ClientPluginHost • 0x6941:$s3: PipeExists • 0x5be1:$s4: PipeCreated • 0x5a05:$s5: IClientLoggingHost
00000013.00000002.490572775.0000000006A10000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
00000013.00000002.490572775.0000000006A10000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
00000013.00000002.490572775.0000000006A10000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 49 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
19.2.MSBuild.exe.6a00000.19.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x350b:$x1: NanoCore.ClientPluginHost • 0x3525:$x2: IClientNetworkHost
19.2.MSBuild.exe.6a00000.19.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x350b:$x2: NanoCore.ClientPluginHost • 0x52b6:$s4: PipeCreated • 0x34f8:$s5: IClientLoggingHost
19.2.MSBuild.exe.6990000.14.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x605:$x1: NanoCore.ClientPluginHost • 0x63e:$x2: IClientNetworkHost
19.2.MSBuild.exe.6990000.14.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x605:$x2: NanoCore.ClientPluginHost • 0x720:$s4: PipeCreated • 0x61f:$s5: IClientLoggingHost
19.2.MSBuild.exe.69a0000.15.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x13a8:$x1: NanoCore.ClientPluginHost
Click to see the 94 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

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:

.NET source code references suspicious native API functions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

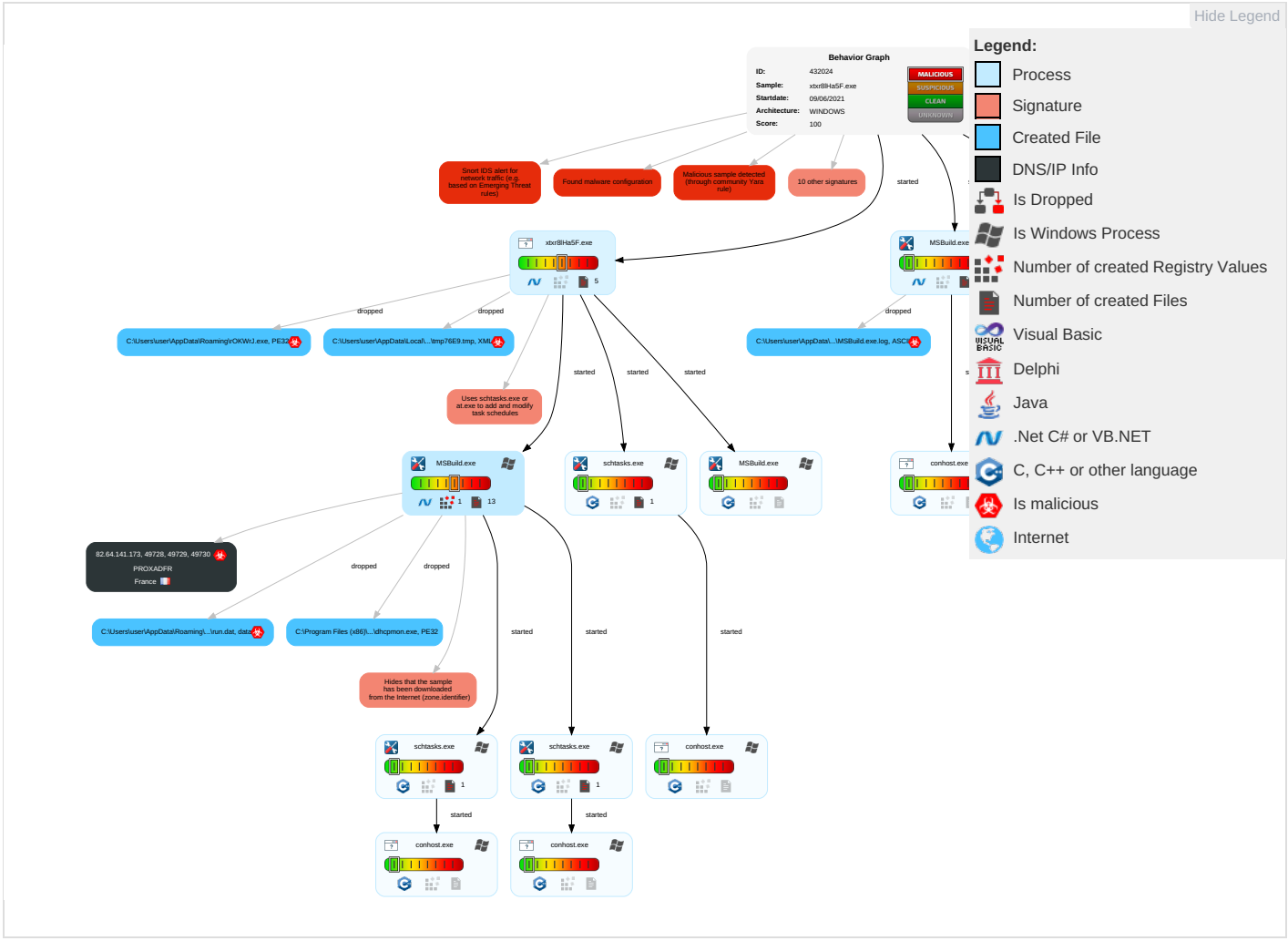
Detected Nanocore Rat

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
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1 1	Process Injection 1 2	Masquerading 2	Input Capture 1 1	System Time Discovery 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2
Default Accounts	Scheduled Task/Job 1 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1 1	Disable or Modify Tools 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	Native API 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Security Software Discovery 2 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Virtualization/Sandbox Evasion 3 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	System Information Discovery 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

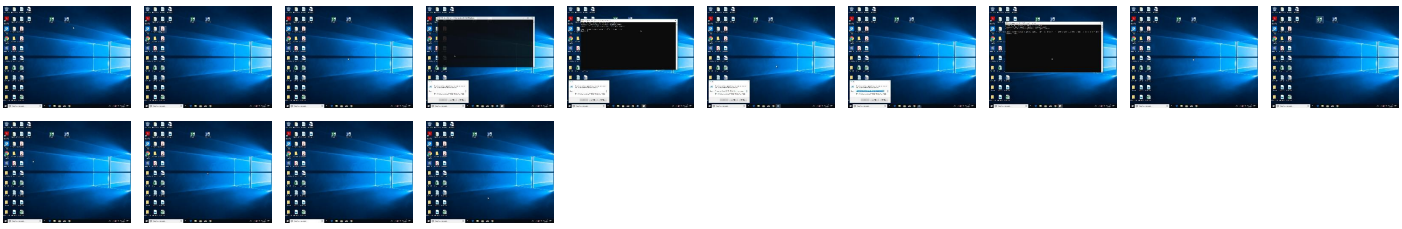
Behavior Graph



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
xtxr8lHa5F.exe	50%	Virustotal		Browse
xtxr8lHa5F.exe	37%	Metadefender		Browse
xtxr8lHa5F.exe	66%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\rOKWrJ.exe	37%	Metadefender		Browse
C:\Users\user\AppData\Roaming\rOKWrJ.exe	66%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
19.2.MSBuild.exe.6a10000.21.unpack	100%	Avira	TR/NanoCore.fadte		Download File
19.0.MSBuild.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
19.2.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
19.0.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.comy	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr-e	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr3	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krLn	0%	Avira URL Cloud	safe	
http://www.fontbureau.comceva	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://fontfabrik.comH	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	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://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.zhongyict.coJJl	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.founder.com.cn/cnt	0%	URL Reputation	safe	
http://www.founder.com.cn/cnt	0%	URL Reputation	safe	
http://www.founder.com.cn/cnt	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
82.64.141.173	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.tiro.com)	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
82.64.141.173	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
82.64.141.173	unknown	France		12322	PROXADFR	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432024
Start date:	09.06.2021
Start time:	16:56:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	xtxr8lHa5F.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:	38
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@20/14@0/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 0.9% (good quality ratio 0.8%) • Quality average: 40.9% • Quality standard deviation: 22.3%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:57:37	API Interceptor	304x Sleep call for process: xtxr8lHa5F.exe modified
16:58:22	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe" s>$(Arg0)
16:58:22	API Interceptor	690x Sleep call for process: MSBuild.exe modified
16:58:22	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
16:58:23	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PROXADFR	XPChvE6GQd	Get hash	malicious	Browse	• 91.174.106.122
	networkservice.exe	Get hash	malicious	Browse	• 78.199.3.202
	z3hir.bin	Get hash	malicious	Browse	• 78.206.151.134
	IMG001.exe	Get hash	malicious	Browse	• 82.231.211.245
	h15v4Z591T.exe	Get hash	malicious	Browse	• 212.27.48.10
	73V5c6ESki.exe	Get hash	malicious	Browse	• 212.27.48.10
	Thq0FVrAAZ.exe	Get hash	malicious	Browse	• 212.27.48.10
	FB11.exe	Get hash	malicious	Browse	• 91.160.55.21
	1.sh	Get hash	malicious	Browse	• 62.147.248.49
	PDFXCview.exe	Get hash	malicious	Browse	• 88.188.224.42
	HUahIwV82u.exe	Get hash	malicious	Browse	• 82.64.20.171
	kYfGJlQBJ3.exe	Get hash	malicious	Browse	• 78.198.121.158
	Io8ic2291n.doc	Get hash	malicious	Browse	• 78.206.229.130
	wEcncyxrEe	Get hash	malicious	Browse	• 78.199.170.243
	mozi.a.zip	Get hash	malicious	Browse	• 82.253.85.237
	WUHU95Apq3	Get hash	malicious	Browse	• 78.253.18.229
	bin.sh	Get hash	malicious	Browse	• 78.239.138.225
	evapi.exe	Get hash	malicious	Browse	• 82.64.68.235
	mssecsvr.exe	Get hash	malicious	Browse	• 78.200.246.23
	i	Get hash	malicious	Browse	• 91.166.162.40

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	GpnPv433gb.exe	Get hash	malicious	Browse	
	MPT Q2106-0405.exe	Get hash	malicious	Browse	
	http___pbfoa.org_d.exe	Get hash	malicious	Browse	
	4.exe	Get hash	malicious	Browse	
	Payment Copy.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	CN-Invoice-XXXXX9808-1901114328710090.pdf.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	4Vy2EGhzNF.exe	Get hash	malicious	Browse	
	PO-13916.jpeg.exe	Get hash	malicious	Browse	
	Balance Payment.exe	Get hash	malicious	Browse	
	updated statement.exe	Get hash	malicious	Browse	
	Quotation.exe	Get hash	malicious	Browse	
	DHL On Demand Delivery.exe	Get hash	malicious	Browse	
	DHL On Demand Delivery.pdf.exe	Get hash	malicious	Browse	
	S4aES2mPdl.exe	Get hash	malicious	Browse	
	Remcos Professional Cracked By Alcatraz3222.exe	Get hash	malicious	Browse	
	shipping documents.exe	Get hash	malicious	Browse	
	e98ba3ccd39858a7416e4769ae962ce5.exe	Get hash	malicious	Browse	
	CN-Invoice-XXXXX9808-190111432879905.exe	Get hash	malicious	Browse	

Created / dropped Files

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	261728
Entropy (8bit):	6.1750840449797675
Encrypted:	false
SSDEEP:	3072:Mao0QHGUQWWimj9q/NLpj/WWqvAw2XpFU4rwOe4ubZSif02RFi/x2uv9FeP:boZTTWxxqVpqWVRXfr802biprVu
MD5:	D621FD77BD585874F9686D3A76462EF1
SHA1:	ABCAE05EE61EE6292003AABD8C80583FA49EDDA2
SHA-256:	2CA7CF7146FB8209CF3C6CECB1C5AA154C61E046DC07AFA05E8158F2C0DDE2F6
SHA-512:	2D85A81D708ECC8AF9A1273143C94DA84E632F1E595E22F54B867225105A1D0A44F918F0FAE6F1EB15ECF69D75B6F4616699776A16A2AA8B5282100FD15CA74C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: GpnPv433gb.exe, Detection: malicious, Browse • Filename: MPT Q2106-0405.exe, Detection: malicious, Browse • Filename: http___pbfoa.org_d.exe, Detection: malicious, Browse • Filename: 4.exe, Detection: malicious, Browse • Filename: Payment Copy.exe, Detection: malicious, Browse • Filename: SOA.exe, Detection: malicious, Browse • Filename: CN-Invoice-XXXXX9808-1901114328710090.pdf.exe, Detection: malicious, Browse • Filename: SOA.exe, Detection: malicious, Browse • Filename: 4Vy2EGhzNF.exe, Detection: malicious, Browse • Filename: PO-13916.jpeg.exe, Detection: malicious, Browse • Filename: Balance Payment.exe, Detection: malicious, Browse • Filename: updated statement.exe, Detection: malicious, Browse • Filename: Quotation.exe, Detection: malicious, Browse • Filename: DHL On Demand Delivery.exe, Detection: malicious, Browse • Filename: DHL On Demand Delivery.pdf.exe, Detection: malicious, Browse • Filename: S4aES2mPdl.exe, Detection: malicious, Browse • Filename: Remcos Professional Cracked By Alcatraz3222.exe, Detection: malicious, Browse • Filename: shipping documents.exe, Detection: malicious, Browse • Filename: e98ba3ccd39858a7416e4769ae962ce5.exe, Detection: malicious, Browse • Filename: CN-Invoice-XXXXX9808-190111432879905.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....".0..|...B.....n.... .....@.. ....`.....O.....>.....`>..... ....H.....text....z... ...|..... ..`.rsrc....>.....@...~.....@..@.relo c.....@..B.....P.....H.....8).....|.....*.{.....*v.(=....r...p({...-..+..}....*....0..%.....(....-..*....(z.....&..}.....*.*..... ...0..5.....(....-..*.-.r+..ps>...z.....i(z.....&..}.....*.*.....%.....>....(?...(....*N..(@....oA...(....*:...(B...(....*:...(C...(....**....(....*....0..G.....(.....,*..(....-...}.....*.r...p(x...&.(v.....}... ...&..}.....*.*.....7.....0..f.....-.r7..ps>...z .....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\MSBuild.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	841
Entropy (8bit):	5.356220854328477
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoIvEE4xDqE4j:MxHKXwYHKhQnoPtHoxHwvEHxDqHj
MD5:	486580834B084C92AE1F3866166C9C34
SHA1:	C8EB7E1CEF55A6C9EB931487E9AA4A2098AACEDF
SHA-256:	65C5B1213E371D449E2A239557A5F250FEA1D3473A1B5C4C5FF7492085F663FB
SHA-512:	2C54B638A52AA87F47CAB50859EFF98F07DA02993A596686B5617BA99E73ABFCD104F0F33209E24AFB32E66B4B8A225D4DB2CC79631540C21E7E8C4573DFD45
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..2,"Microsoft.Build.Framework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.Build, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1037
Entropy (8bit):	5.371216502395632
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7KvEE4xDqE4j:MxHKXwYHKhQnoPtHoxHhAHKzvKvEHxD0
MD5:	C7F28B87C2CAD111D929CB9A0FF822F8
SHA1:	C2CF9E7A3F6EFD9000FE76EBE54E4E9AE5754267
SHA-256:	D1B02C20EACF464229AB063FA947A525E2ED7772259A8F70C7205DC13599EAE6
SHA-512:	E0F35874E02AB672CFF0553A0DA0864DAB14C05733D06395E4D0C9CDFC6F445E940310F8D01E3E1B28895F636DFBC1F510E103D1C46818400BA4E7371D8F254
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"Microsoft.Build.Framework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.Build, Version=4.0.0.0, Culture=neutral,

C:\Users\user\AppData\Local\Temp\tmp604E.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	5.137611098420233
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0moxtn:cbk4oL600QydbQxIYODOLedq3Zoj
MD5:	3E2B26ED8B75AE83A269595180E84EF6
SHA1:	D30A0335FCCE406BCA8BA5764288235E6192F608
SHA-256:	108BE30AEB8EB31C185A39A6726F26DACBC4E4124951C61A29ADE4B7038C71EA
SHA-512:	B6981C68FCB886CC8379A068B96931B9D4F5CC5AA9BDC467E36C4168FE6C5273A2A84D8850B12C11703EC03AC6B1F1950D1E669EFCB59FC2402CE4BBA9DC0D3
Malicious:	false
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\tmp6502.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310

C:\Users\user\AppData\Local\Temp\tmp6502.tmp	
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
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\tmp76E9.tmp	
Process:	C:\Users\user\Desktop\xtxr8lHa5F.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1639
Entropy (8bit):	5.186784683335912
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBItn:cbh47TlNQ//rydbz9I3YODOLNdq3I
MD5:	EE08731F2635FB10A5E1E6F0747AB40F
SHA1:	E0D3F0D3F2177ECC73C45479FA66DFC14C5306DF
SHA-256:	E441C2F354D1D3AA8DA9E3B2CB2737C95905B88DF668C2F9D111C9A4D2025E52
SHA-512:	F4504B5AAA6354ED918586F2DEF5A21DB83F9EEBC7121FBC8B3FB4370A3B8BD06E5315ED35AA3D094C83B360CE6431FC22B808627F56DF866F6ADDEF76C840 3
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <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>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	1856
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrw8:flC0IlC0IlC0IlC0IlC0IlC0IlC0IlCr
MD5:	838CD9DBC78EA45A5406EAE23962086D
SHA1:	C8273AACDEE03AC0CDCDDBAA83F51D04D6A4203C
SHA-256:	6E11A62511C5BBC0413128305069B780C448684B54FAA3E8DD0B4FD3DB8C9867
SHA-512:	F7D25EF1FA6F50667DD6785CC774E0AA6BC52A2231FE96E7C59D14EFDFDDA076F6399288CF6EAC8EFA8A75727893432AA155DA0E392F8CD1F26C5C5871EAC6 B5
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7.." .hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E..... {...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:i18tn:i18n
MD5:	8531FB0CEC5F18EBD29FF0B57BC853B0
SHA1:	D7ACB93014DF7917C55380CE5F8E2C10D0E12EBE

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
SHA-256:	A393F6022ED56CAF64A0865D97006C38620212D769CE5EA8B924683B700A1754
SHA-512:	E758D525129048796999A0AF64054AF4CC54096DEDE42D4D2D0375F91847AF4DEAC2019606E4E15D31ED9462CED8718A8E088F86856D1DEA8ADDE395FAE9ED3
Malicious:	**true**
Preview:	...u.+.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.221928094887364
Encrypted:	false
SSDEEP:	3:9bzY6oRDMjmPl:RzWDMCd
MD5:	AE0F5E6CE7122AF264EC533C6B15A27B
SHA1:	1265A495C42EED76CC043D50C60C23297E76CCE1
SHA-256:	73B0B92179C61C26589B47E9732CE418B07EDEE3860EE5A2A5FB06F3B8AA9B26
SHA-512:	DD44C2D24D4E3A0F0B988AD3D04683B5CB128298043134649BBE33B2512CE0C9B1A8E7D893B9F66FBBCDD901E2B0646C4533FB6C0C8C4AFCB95A0EFB95D44F8
Malicious:	false
Preview:	9iH...}Z.4..f..... 8.j....|.&X..e.F.*.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.887726803973036
Encrypted:	false
SSDEEP:	3:oMty8WddSJ8:oMLW6C
MD5:	6ECAFC0490DAB08E4A288E0042B6B613
SHA1:	4A4529907588505FC65CC9933980CFE6E576B3D6
SHA-256:	DC5F76FBF44B3E6CDDC14EA9E5BB9B6BD3A955197FE13F33F7DDA7ECC08E79E0
SHA-512:	7DA2B02627A36C8199814C250A1FBD61A9C18E098F8D691C11D75044E7F51DBD52C31EC2E1EA8CDEE5077ADCCB8CD247266F191292DB661FE7EA1B613FC6468
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

C:\Users\user\AppData\Roaming\rOKWrJ.exe	
Process:	C:\Users\user\Desktop\xtxr8lHa5F.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1245184
Entropy (8bit):	7.948556128818863
Encrypted:	false
SSDEEP:	24576:4ZBPnHeenJNTfyZbKldRTBeRmZPpYKH2k4mLM:4BeWTfyZbqdR1eCYQ4
MD5:	C89C05D0F2853FA30B535AA2544006E5
SHA1:	2E3A6ADC296D26732A3C61AC761052B8793F7DA0
SHA-256:	B2EC2E506BC9741873E39CC6FDC07802A1180136657582AE807D5F6112CFC02A
SHA-512:	BA3ECE975821799AEE081C04ED73027C4D389AD97B237E2F65D454181922EBAC7ECACF08783046A3E51C67CD283118BA57EF6F6BB6F9918F284084EBAE1D3378
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 37%, Browse • Antivirus: ReversingLabs, Detection: 66%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....X.`.....0.....@..... .....@.. .....@.....[.....@.....@...O.....=..... ..... ..H.....text..... ..... ..`.rsrc....=.....>.....@..@.reloc..... .....@..B.....t.....H.....d...4.....p7.....".(.....*..{....*"..}....*..{....*"..}....*..0.....(.....,.r...p(.....+m.....(....s.....(.....o....t.....r=..p(.....5.,..o.....&.r...p(.....r...p..(....(.....*....(....7..V.....Ba.....Br.....0.....r+..p.+..*..0.....r5..p.+..*..(..... .d...(!..... .....(!.....K..s"...(#....*F...($.....(%....*~...(&.....}.....}.....(%....*v...('.....o(...}.

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

\Device\ConDrv	
Size (bytes):	298
Entropy (8bit):	4.943030742860529
Encrypted:	false
SSDEEP:	6:zx3M1tFAbQtU1R30qyMstwYVoRRZBXVN+J0fFdCsq2UTiMdH8stCal+n:zK13l30ZMt9BFN+QdCT2UftCM+
MD5:	6A9888952541A41F033EB114C24DC902
SHA1:	41903D7C8F31013C44572E09D97B9AAFBBCE77E6
SHA-256:	41A61D0084CD7884BEA1DF02ED9213CB8C83F4034F5C8156FC5B06D6A3E133CE
SHA-512:	E6AC898E67B4052375FDDFE9894B26D504A7827917BF3E02772CFF45C3FA7CC5E0EFFDC701D208E0DB89F05E42F195B1EC890F316BEE5CB8239AB45444DAA6 E
Malicious:	false
Preview:	Microsoft (R) Build Engine version 4.7.3056.0..[Microsoft .NET Framework, version 4.0.30319.42000]..Copyright (C) Microsoft Corporation. All rights reserved.....MSBUILD : error MSB1003: Specify a project or solution file. The current working directory does not contain a project or solution file...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.948556128818863
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:	xtxr8lHa5F.exe
File size:	1245184
MD5:	c89c05d0f2853fa30b535aa2544006e5
SHA1:	2e3a6adc296d26732a3c61ac761052b8793f7da0
SHA256:	b2ec2e506bc9741873e39cc6fdc07802a1180136657582ae807d5f6112cfc02a
SHA512:	ba3ece975821799aee081c04ed73027c4d389ad97b237e2f65d454181922ebac7ecacf08783046a3e51c67cd283118ba57ef6f6bb6f9918f284084ebae1d3378
SSDEEP:	24576:4ZBPnHeenJNTfyZbKldRTBeRmZPpYKH2k4mLM:4BeWTfyZbqdR1eCYQ4
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....X.`.....0.....@..... .....@.. .....@.....[....@.....

File Icon

Icon Hash:	c4e0696969796843

Static PE Info

General

Entrypoint:	0x52dc92
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:	0x60BA58E6 [Fri Jun 4 16:46:30 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0

General

File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x12bcb0	0x12be00	False	0.948363901626	data	7.95223164837	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x12e000	0x3db0	0x3e00	False	0.926033266129	data	7.68775853308	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x132000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/09/21-16:58:25.207531	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49728	6666	192.168.2.3	82.64.141.173
06/09/21-16:58:32.018797	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49729	6666	192.168.2.3	82.64.141.173
06/09/21-16:58:38.035640	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49730	6666	192.168.2.3	82.64.141.173
06/09/21-16:58:44.066081	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49732	6666	192.168.2.3	82.64.141.173
06/09/21-16:58:50.004987	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49738	6666	192.168.2.3	82.64.141.173
06/09/21-16:58:56.037031	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49739	6666	192.168.2.3	82.64.141.173
06/09/21-16:59:03.038875	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49740	6666	192.168.2.3	82.64.141.173
06/09/21-16:59:09.644432	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49741	6666	192.168.2.3	82.64.141.173
06/09/21-16:59:15.672476	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49742	6666	192.168.2.3	82.64.141.173
06/09/21-16:59:21.725158	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	6666	192.168.2.3	82.64.141.173
06/09/21-16:59:27.712404	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49746	6666	192.168.2.3	82.64.141.173
06/09/21-16:59:34.173339	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49747	6666	192.168.2.3	82.64.141.173
06/09/21-16:59:40.286502	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49748	6666	192.168.2.3	82.64.141.173
06/09/21-16:59:46.274972	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49749	6666	192.168.2.3	82.64.141.173

Network Port Distribution

TCP Packets

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: xtxr8lHa5F.exe PID: 5352 Parent PID: 5544

General

Start time:	16:57:37
Start date:	09/06/2021
Path:	C:\Users\user\Desktop\xtxr8lHa5F.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\xtxr8lHa5F.exe'
Imagebase:	0x5c0000
File size:	1245184 bytes
MD5 hash:	C89C05D0F2853FA30B535AA2544006E5
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: 00000000.00000002.300718477.00000000047D1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.300718477.00000000047D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.300718477.00000000047D1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.297955225.00000000039C1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.297955225.00000000039C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.297955225.00000000039C1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 3696 Parent PID: 5352

General

Start time:	16:58:15
Start date:	09/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\rOKWrJ' /XML 'C:\Users\user\AppData\Local\Temp\tmp76E9.tmp'
Imagebase:	0xcf0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 5256 Parent PID: 3696

General

Start time:	16:58:15
Start date:	09/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: MSBuild.exe PID: 5260 Parent PID: 5352

General

Start time:	16:58:16
Start date:	09/06/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x7ff6741d0000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: MSBuild.exe PID: 5268 Parent PID: 5352

General

Start time:	16:58:16
Start date:	09/06/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xc40000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
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: 00000013.00000002.490364012.00000000069C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.490364012.00000000069C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.490572775.0000000006A10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.490572775.0000000006A10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.490572775.0000000006A10000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.490523889.0000000006A00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.490523889.0000000006A00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.490241521.0000000006970000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.490241521.0000000006970000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.490432497.00000000069E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.490432497.00000000069E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.490460540.00000000069F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.490460540.00000000069F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.490307408.0000000006990000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.490307408.0000000006990000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.489013213.0000000005660000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.489013213.0000000005660000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.489410894.0000000005AB0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.489410894.0000000005AB0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000000.293794804.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000000.293794804.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000000.293794804.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source:

	00000013.00000002.490092332.0000000006860000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.490092332.0000000006860000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.490925199.0000000006C90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.490925199.0000000006C90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.477945079.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.477945079.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.477945079.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.483305536.0000000003021000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.489888733.00000000065C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.489888733.00000000065C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.490328155.00000000069A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.490328155.00000000069A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000000.294410455.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000000.294410455.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000000.294410455.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.487426729.0000000004169000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.487426729.0000000004169000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.490998411.0000000006E10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000013.00000002.490998411.0000000006E10000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: schtasks.exe PID: 5020 Parent PID: 5268

General

Start time:	16:58:20
Start date:	09/06/2021
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\tmp604E.tmp'
Imagebase:	0x7ff6741d0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 5012 Parent PID: 5020

General

Start time:	16:58:20
Start date:	09/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 3564 Parent PID: 5268

General

Start time:	16:58:21
Start date:	09/06/2021
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\tmp6502.tmp'
Imagebase:	0x8d0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 3016 Parent PID: 3564

General

Start time:	16:58:21
Start date:	09/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: MSBuild.exe PID: 3508 Parent PID: 528

General

Start time:	16:58:22
Start date:	09/06/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe 0
Imagebase:	0x450000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 1648 Parent PID: 3508

General

Start time:	16:58:23
Start date:	09/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 1180 Parent PID: 528

General

Start time:	16:58:23
Start date:	09/06/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x600000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 1260 Parent PID: 1180

General

Start time:	16:58:24
Start date:	09/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: 3776 Parent PID: 3388

General

Start time:	16:58:30
Start date:	09/06/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x1e0000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 996 Parent PID: 3776

General

Start time:	16:58:31
Start date:	09/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis