ID: 412302
Sample Name: PAYMENT SLIP.exe
Cookbook: default.jbs
Time: 15:40:17
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

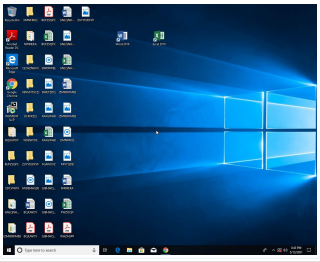
Analysis Report PAYMENT SLIP.exe

Overview

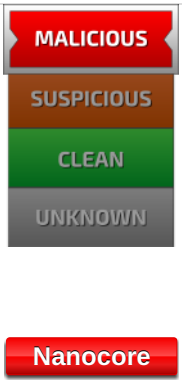
General Information

Sample Name:	PAYMENT SLIP.exe
Analysis ID:	412302
MD5:	50c9d58f6195048.
SHA1:	79df49a23af28b6..
SHA256:	80726d3e380e4a..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



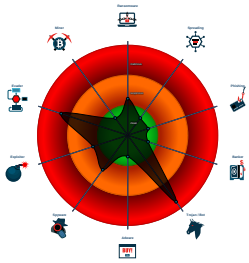
Nanocore

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…
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e….
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Executable has a suspicious name (…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- PAYMENT SLIP.exe (PID: 6804 cmdline: 'C:\Users\user\Desktop\PAYMENT SLIP.exe' MD5: 50C9D58F61950484825D85A9A1372A7D)
  - MSBuild.exe (PID: 7012 cmdline: 'C:\Users\user\Desktop\PAYMENT SLIP.exe' MD5: 88BBB7610152B48C2B3879473B17857E)
  - PAYMENT SLIP.exe (PID: 7116 cmdline: 'C:\Users\user\Desktop\PAYMENT SLIP.exe' MD5: 50C9D58F61950484825D85A9A1372A7D)
    - MSBuild.exe (PID: 4228 cmdline: 'C:\Users\user\Desktop\PAYMENT SLIP.exe' MD5: 88BBB7610152B48C2B3879473B17857E)
    - PAYMENT SLIP.exe (PID: 5704 cmdline: 'C:\Users\user\Desktop\PAYMENT SLIP.exe' MD5: 50C9D58F61950484825D85A9A1372A7D)
      - MSBuild.exe (PID: 6504 cmdline: 'C:\Users\user\Desktop\PAYMENT SLIP.exe' MD5: 88BBB7610152B48C2B3879473B17857E)
      - PAYMENT SLIP.exe (PID: 6900 cmdline: 'C:\Users\user\Desktop\PAYMENT SLIP.exe' MD5: 50C9D58F61950484825D85A9A1372A7D)
        - MSBuild.exe (PID: 6948 cmdline: 'C:\Users\user\Desktop\PAYMENT SLIP.exe' MD5: 88BBB7610152B48C2B3879473B17857E)
- hmhrpib.exe (PID: 6024 cmdline: 'C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe' MD5: 50C9D58F61950484825D85A9A1372A7D)
  - MSBuild.exe (PID: 6372 cmdline: 'C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe' MD5: 88BBB7610152B48C2B3879473B17857E)
    - schtasks.exe (PID: 6508 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp3E70.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6608 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- hmhrpib.exe (PID: 6376 cmdline: 'C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe' MD5: 50C9D58F61950484825D85A9A1372A7D)
  - MSBuild.exe (PID: 6940 cmdline: 'C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe' MD5: 88BBB7610152B48C2B3879473B17857E)
- MSBuild.exe (PID: 6800 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe 0 MD5: 88BBB7610152B48C2B3879473B17857E)
  - conhost.exe (PID: 6876 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "c473d7c4-8173-4cff-8fb5-dfc81a12",
  "Group": "sea",
  "Domain1": "seaudo.hopto.org",
  "Domain2": "23.254.130.71",
  "Port": 3030,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "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
0000000C.00000002.911350836.00000000044F F000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000008.00000002.706739434.0000000002F3 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000008.00000002.706739434.0000000002F3 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
00000008.00000002.706739434.0000000002F3 0000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000002.706739434.0000000002F30000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
Click to see the 92 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.PAYMENT SLIP.exe.3160000.5.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
6.2.PAYMENT SLIP.exe.3160000.5.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
6.2.PAYMENT SLIP.exe.3160000.5.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
6.2.PAYMENT SLIP.exe.3160000.5.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xe0f5:$a: NanoCore • 0xe105:$a: NanoCore • 0xe339:$a: NanoCore • 0xe34d:$a: NanoCore • 0xe38d:$a: NanoCore • 0xe154:$b: ClientPlugin • 0xe356:$b: ClientPlugin • 0xe396:$b: ClientPlugin • 0xe27b:$c: ProjectData • 0xec82:$d: DESCrypto • 0x1664e:$e: KeepAlive • 0x1463c:$g: LogClientMessage • 0x10837:$i: get_Connected • 0xefb8:$j: #=q • 0xefe8:$j: #=q • 0xf004:$j: #=q • 0xf034:$j: #=q • 0xf050:$j: #=q • 0xf06c:$j: #=q • 0xf09c:$j: #=q • 0xf0b8:$j: #=q
10.2.PAYMENT SLIP.exe.24e0000.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 190 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

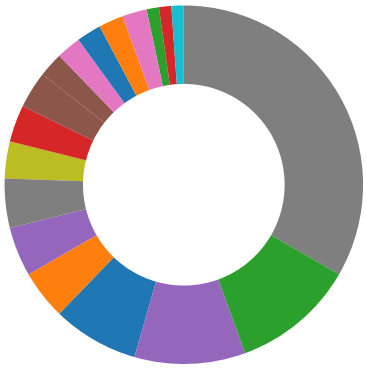
Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Signature Overview



- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

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)

Executable has a suspicious name (potential lure to open the executable)

Initial sample is a PE file and has a suspicious name

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)

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

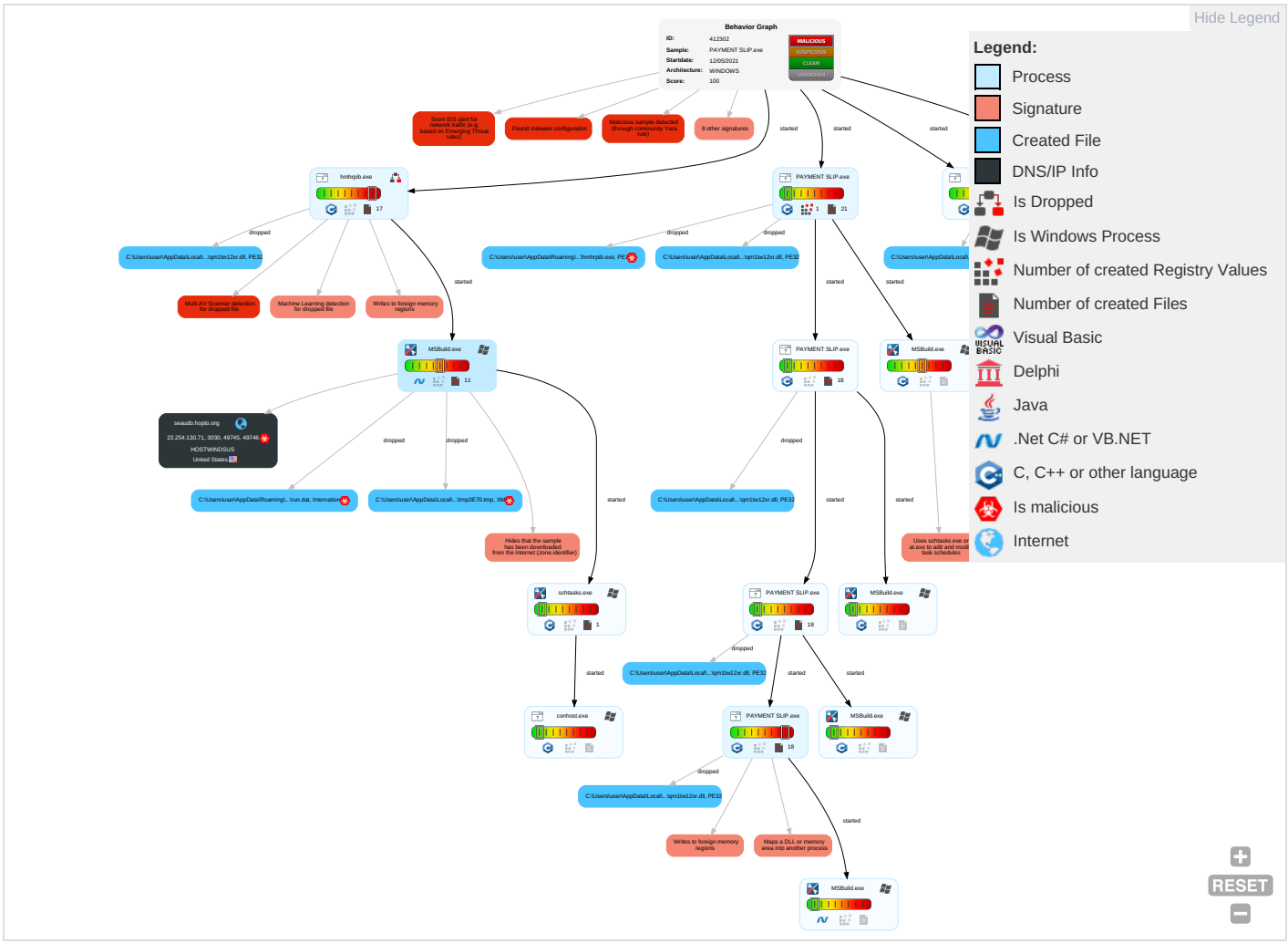
Detected Nanocore Rat

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	Networ Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1	Input Capture 1 1	File and Directory Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesd Insecur Networ Commu
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 1	Process Injection 2 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 1 5	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encrypted Channel 1 2	Exploit Redirec Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 2	Security Account Manager	Security Software Discovery 1 1 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Standard Port 1	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Registry Run Keys / Startup Folder 1	Software Packing 1 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Software 1	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 3 1	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 1	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 3 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 1 2	Jammir Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 2 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecur Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

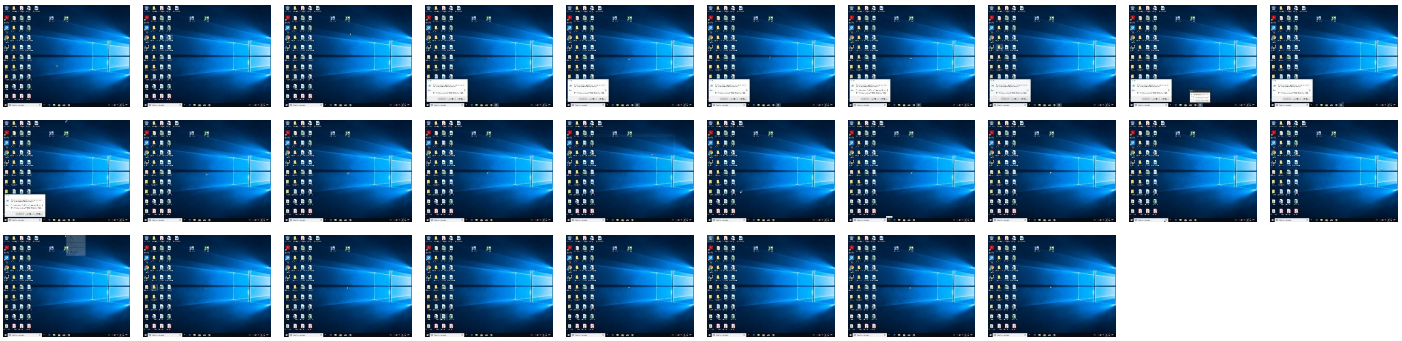
Behavior Graph



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
PAYMENT SLIP.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe	43%	ReversingLabs	Win32.Backdoor.Androm	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.PAYMENT SLIP.exe.23e0000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
19.2.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
20.2.PAYMENT SLIP.exe.2f50000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
12.2.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
22.2.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.2.MSBuild.exe.4507ac8.19.unpack	100%	Avira	TR/NanoCore.fadte		Download File
12.2.MSBuild.exe.61a0000.33.unpack	100%	Avira	TR/NanoCore.fadte		Download File
1.2.PAYMENT SLIP.exe.3110000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.2.PAYMENT SLIP.exe.3060000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
23.254.130.71	1%	Virustotal		Browse
23.254.130.71	0%	Avira URL Cloud	safe	
seaudo.hopto.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
seaudo.hopto.org	23.254.130.71	true	true		unknown

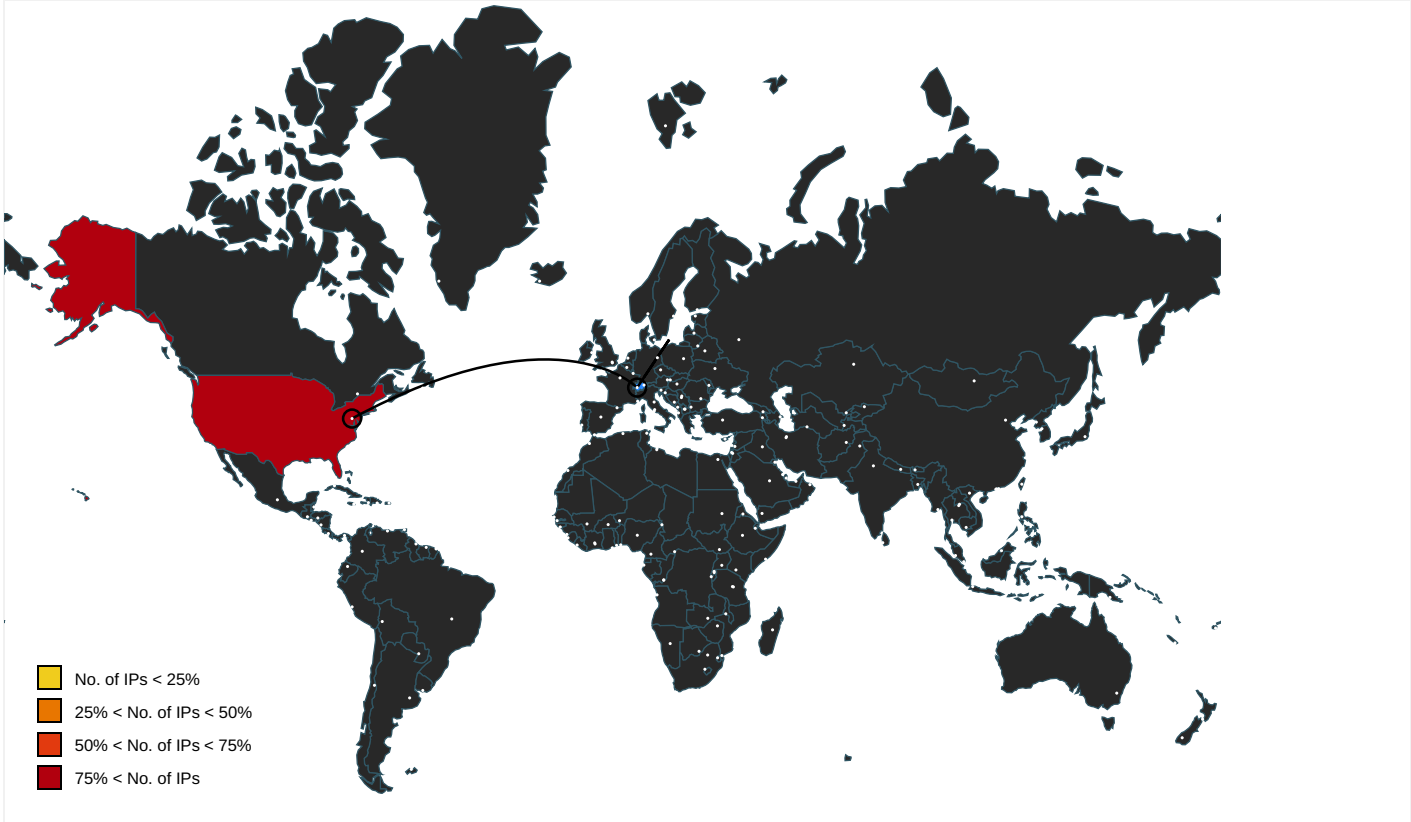
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
23.254.130.71	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
seaudo.hopto.org	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	PAYMENT SLIP.exe	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.254.130.71	seaudo.hopto.org	United States		54290	HOSTWINDSUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412302
Start date:	12.05.2021
Start time:	15:40:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PAYMENT SLIP.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:	30
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@26/31@17/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 54.1% (good quality ratio 52.4%) • Quality average: 85.9% • Quality standard deviation: 23.7%
HCA Information:	• Successful, ratio: 94% • 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 • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.139.144, 104.43.193.48, 92.122.145.220, 13.88.21.125, 104.42.151.234, 20.82.209.183, 8.241.78.254, 67.26.73.254, 8.241.90.254, 8.241.83.126, 8.241.126.249, 52.155.217.156, 20.54.26.129, 92.122.213.247, 92.122.213.194, 20.82.210.154 • Excluded domains from analysis (whitelisted): store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, iris-de-prod-azsc-neu.northeurope.cloudapp.azure.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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 NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:41:13	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run jnckjcfx C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe
15:41:21	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run jnckjcfx C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe
15:41:28	API Interceptor	2x Sleep call for process: hmhrpib.exe modified
15:41:32	API Interceptor	752x Sleep call for process: MSBuild.exe modified
15:41:34	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HOSTWINDSUS	210503_McDermott_NFE_RFQ.exe	Get hash	malicious	Browse	• 104.168.175.179
	ATT82166.HTM	Get hash	malicious	Browse	• 23.254.226.43
	H8iVAWlIfH.exe	Get hash	malicious	Browse	• 23.254.224.129
	PO.exe	Get hash	malicious	Browse	• 104.168.175.179
	ATT81583.HTM	Get hash	malicious	Browse	• 23.254.226.43
	DQhf1tNmwkbpjig.exe	Get hash	malicious	Browse	• 104.168.175.179
	PO.exe	Get hash	malicious	Browse	• 104.168.175.179
	quote.exe	Get hash	malicious	Browse	• 104.168.175.179
	List.exe	Get hash	malicious	Browse	• 104.168.175.179
	PURCHASE.exe	Get hash	malicious	Browse	• 104.168.175.179
	b0YXIQaXcjPgzWg.exe	Get hash	malicious	Browse	• 104.168.175.179
	SAMSUNG gFLNG FEED Update RFQ Documents and C.exe	Get hash	malicious	Browse	• 104.168.175.179
	cvhost.exe	Get hash	malicious	Browse	• 192.236.147.83
	cvhost.exe	Get hash	malicious	Browse	• 192.236.147.83
	SecuriteInfo.com.W32.AIDetect.malware1.9937.exe	Get hash	malicious	Browse	• 192.236.147.83
	SecuriteInfo.com.W32.AIDetect.malware1.32629.exe	Get hash	malicious	Browse	• 192.236.147.83
	PROJECT_EB200_RFQ_ITEMS_DOCUMENTS.pdf.exe	Get hash	malicious	Browse	• 104.168.175.179
	RFQ-EB200-PLOO1_Bidding.pdf.exe	Get hash	malicious	Browse	• 104.168.175.179
	po.exe	Get hash	malicious	Browse	• 104.168.175.179
	f5WPatHVT0.exe	Get hash	malicious	Browse	• 192.236.147.83

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\MSBuild.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	325
Entropy (8bit):	5.334380084018418
Encrypted:	false
SSDEEP:	6:Q3LadLCR22IAQykdL1tZbLsbFLIP12MUAvvro6ysGMFLIP12MUAvvrs:Q3LaJU20NaL1tZbgbe4MqJsGMe4M6
MD5:	65CE98936A67552310EFE2F0FF5BDF88
SHA1:	8133653A6B9A169C7496ADE315CED322CFC3613A
SHA-256:	682F7C55B1B6E189D17755F74959CD08762F91373203B3B982ACFFCADE2E871A
SHA-512:	2D00AC024267EC384720A400F6D0B4F7EDDF49FAF8AB3C9E6CBFBBAE90ECADACA9022B33E3E8EC92E4F57C7FC830299C8643235EB4AA7D8A6AFE9DD1775F57C3
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\MSBuild.exe.log	
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..2,"Microsoft.Build.Engine, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.Build.Framework, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\nsb1C63.tmp\qm1tw12xr.dll	
Process:	C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	3.7496483038392974
Encrypted:	false
SSDEEP:	48:Sa/T+kBvwunRLZ6AL0rpRVaS53RS9BNZYWrTZxZ4Vo:+kBvFLgALER8S53RS9dtng
MD5:	EE2F349BA112FE569BD9AB1368E65791
SHA1:	9CEB495D81A804E604111D98C1169B4A9B640510
SHA-256:	5A97B6F5313D875AE40429BB27D486F7B745EEFDF5C116E434DC08770923FA9F
SHA-512:	D4CD1A797307B4FC4D9C3E80979BDDE682F64931FCF6D9CFCAE333646A242C143C2F77D2D6A80E01452A614E7981339E7E17580871B48518DC71A58339970B64
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....!..... .....@.....%..K.... ..... .....text..... ..... ..`.rdata..+.... .....@..@.data...&....0.....@..... .....

C:\Users\user\AppData\Local\Temp\nsd2D5A.tmp	
Process:	C:\Users\user\Desktop\PAYMENT SLIP.exe
File Type:	data
Category:	dropped
Size (bytes):	227087
Entropy (8bit):	7.939223952673508
Encrypted:	false
SSDEEP:	6144:J7lDzCvnAXYv/i/8bA7r8ePZFz1Yxp1T:qOnSY3A807r8AZFz1UN
MD5:	DC0CB7051E536384DE28ED52AB92EA19
SHA1:	D145293DEE4F6A963FE964B44CB791F599265B52
SHA-256:	7180220E08967228A453E1076EFDEB42589456E4CB6F1D5C8F5765F1994A179C
SHA-512:	DD189821102FE517D24541F9D34C77F4210802B7B3FD089D0AA28090DFF719676325A8F886209B3CEE48AEA6149A67A4EC4C3C97E252EA7336F9E8EF4E36CD5E
Malicious:	false
Preview:	.....,.....d.....4..... .....G.....j..... ....

C:\Users\user\AppData\Local\Temp\nshD279.tmp\qm1tw12xr.dll	
Process:	C:\Users\user\Desktop\PAYMENT SLIP.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	3.7496483038392974
Encrypted:	false
SSDEEP:	48:Sa/T+kBvwunRLZ6AL0rpRVaS53RS9BNZYWrTZxZ4Vo:+kBvFLgALER8S53RS9dtng
MD5:	EE2F349BA112FE569BD9AB1368E65791
SHA1:	9CEB495D81A804E604111D98C1169B4A9B640510
SHA-256:	5A97B6F5313D875AE40429BB27D486F7B745EEFDF5C116E434DC08770923FA9F
SHA-512:	D4CD1A797307B4FC4D9C3E80979BDDE682F64931FCF6D9CFCAE333646A242C143C2F77D2D6A80E01452A614E7981339E7E17580871B48518DC71A58339970B64
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....!..... .....@.....%..K.... ..... .....text..... ..... ..`.rdata..+.... .....@..@.data...&....0.....@..... .....

C:\Users\user\AppData\Local\Temp\nsiFB00.tmp\qm1tw12xr.dll	
Process:	C:\Users\user\Desktop\PAYMENT SLIP.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	3.7496483038392974
Encrypted:	false

C:\Users\user\AppData\Local\Temp\nsiFB00.tmp\qm1tw12xr.dll	
SSDEEP:	48:Sa/T+kBvwunRLZ6AL0rpRVaS53RS9BNZYWrTZxZ4Vo:+kBvFLgALER8S53RS9dtng
MD5:	EE2F349BA112FE569BD9AB1368E65791
SHA1:	9CEB495D81A804E604111D98C1169B4A9B640510
SHA-256:	5A97B6F5313D875AE40429BB27D486F7B745EEFDF5C116E434DC08770923FA9F
SHA-512:	D4CD1A797307B4FC4D9C3E80979BDDE682F64931FCF6D9CFCAE333646A242C143C2F77D2D6A80E01452A614E7981339E7E17580871B48518DC71A58339970B64
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....!..... .....@.....%..K.... ..... .....text..... ..... ..`.rdata..+.... .....@..@.data...&....0.....@..... .....

C:\Users\user\AppData\Local\Temp\nsj3D87.tmp\qm1tw12xr.dll	
Process:	C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	3.7496483038392974
Encrypted:	false
SSDEEP:	48:Sa/T+kBvwunRLZ6AL0rpRVaS53RS9BNZYWrTZxZ4Vo:+kBvFLgALER8S53RS9dtng
MD5:	EE2F349BA112FE569BD9AB1368E65791
SHA1:	9CEB495D81A804E604111D98C1169B4A9B640510
SHA-256:	5A97B6F5313D875AE40429BB27D486F7B745EEFDF5C116E434DC08770923FA9F
SHA-512:	D4CD1A797307B4FC4D9C3E80979BDDE682F64931FCF6D9CFCAE333646A242C143C2F77D2D6A80E01452A614E7981339E7E17580871B48518DC71A58339970B64
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....!..... .....@.....%..K.... ..... .....text..... ..... ..`.rdata..+.... .....@..@.data...&....0.....@..... .....

C:\Users\user\AppData\Local\Temp\nsj62B2.tmp	
Process:	C:\Users\user\Desktop\PAYMENT SLIP.exe
File Type:	data
Category:	dropped
Size (bytes):	227087
Entropy (8bit):	7.939223952673508
Encrypted:	false
SSDEEP:	6144:J7IDzCvnAXYv/i/8bA7r8ePZFz1Yxp1T:qOnSY3A807r8AZFz1UN
MD5:	DC0CB7051E536384DE28ED52AB92EA19
SHA1:	D145293DEE4F6A963FE964B44CB791F599265B52
SHA-256:	7180220E08967228A453E1076EFDEB42589456E4CB6F1D5C8F5765F1994A179C
SHA-512:	DD189821102FE517D24541F9D34C77F4210802B7B3FD089D0AA28090DFF719676325A8F886209B3CEE48AEA6149A67A4EC4C3C97E252EA7336F9E8EF4E36CD5E
Malicious:	false
Preview:	.....,.....d.....4..... .....G.....j..... ....

C:\Users\user\AppData\Local\Temp\nsmD249.tmp	
Process:	C:\Users\user\Desktop\PAYMENT SLIP.exe
File Type:	data
Category:	dropped
Size (bytes):	227087
Entropy (8bit):	7.939223952673508
Encrypted:	false
SSDEEP:	6144:J7IDzCvnAXYv/i/8bA7r8ePZFz1Yxp1T:qOnSY3A807r8AZFz1UN
MD5:	DC0CB7051E536384DE28ED52AB92EA19
SHA1:	D145293DEE4F6A963FE964B44CB791F599265B52
SHA-256:	7180220E08967228A453E1076EFDEB42589456E4CB6F1D5C8F5765F1994A179C
SHA-512:	DD189821102FE517D24541F9D34C77F4210802B7B3FD089D0AA28090DFF719676325A8F886209B3CEE48AEA6149A67A4EC4C3C97E252EA7336F9E8EF4E36CD5E
Malicious:	false
Preview:	.....,.....d.....4..... .....G.....j..... ....

C:\Users\user\AppData\Local\Temp\nsnFAD0.tmp	
Process:	C:\Users\user\Desktop\PAYMENT SLIP.exe
File Type:	data
Category:	dropped
Size (bytes):	227087
Entropy (8bit):	7.939223952673508
Encrypted:	false
SSDEEP:	6144:J7IDzCvnAXYv/i/8bA7r8ePZFz1Yxp1T:qOnSY3A807r8AZFz1UN
MD5:	DC0CB7051E536384DE28ED52AB92EA19
SHA1:	D145293DEE4F6A963FE964B44CB791F599265B52
SHA-256:	7180220E08967228A453E1076EFDEB42589456E4CB6F1D5C8F5765F1994A179C
SHA-512:	DD189821102FE517D24541F9D34C77F4210802B7B3FD089D0AA28090DFF719676325A8F886209B3CEE48AEA6149A67A4EC4C3C97E252EA7336F9E8EF4E36CD5E
Malicious:	false
Preview:	.....,.....d.....4..... .....G.....j..... ....

C:\Users\user\AppData\Local\Temp\nsq1C23.tmp	
Process:	C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe
File Type:	data
Category:	dropped
Size (bytes):	227087
Entropy (8bit):	7.939223952673508
Encrypted:	false
SSDEEP:	6144:J7IDzCvnAXYv/i/8bA7r8ePZFz1Yxp1T:qOnSY3A807r8AZFz1UN
MD5:	DC0CB7051E536384DE28ED52AB92EA19
SHA1:	D145293DEE4F6A963FE964B44CB791F599265B52
SHA-256:	7180220E08967228A453E1076EFDEB42589456E4CB6F1D5C8F5765F1994A179C
SHA-512:	DD189821102FE517D24541F9D34C77F4210802B7B3FD089D0AA28090DFF719676325A8F886209B3CEE48AEA6149A67A4EC4C3C97E252EA7336F9E8EF4E36CD5E
Malicious:	false
Preview:	.....,.....d.....4..... .....G.....j..... ....

C:\Users\user\AppData\Local\Temp\nsy2D8A.tmp\qm1tw12xr.dll	
Process:	C:\Users\user\Desktop\PAYMENT SLIP.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	3.7496483038392974
Encrypted:	false
SSDEEP:	48:Sa/T+kBvwunRLZ6AL0rpRVaS53RS9BNZYWrTZxZ4Vo:+kBvFLgALER8S53RS9dtng
MD5:	EE2F349BA112FE569BD9AB1368E65791
SHA1:	9CEB495D81A804E604111D98C1169B4A9B640510
SHA-256:	5A97B6F5313D875AE40429BB27D486F7B745EEFDF5C116E434DC08770923FA9F
SHA-512:	D4CD1A797307B4FC4D9C3E80979BDDE682F64931FCF6D9CFCAE333646A242C143C2F77D2D6A80E01452A614E7981339E7E17580871B48518DC71A58339970B64
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`... .....!..... ..... .....@.....%..K.... ..... ..... .....text..... ..... ..`.rdata..+.... .....@..@.data...&....0.....@..... .....

C:\Users\user\AppData\Local\Temp\nsz3D48.tmp	
Process:	C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe
File Type:	data
Category:	dropped
Size (bytes):	227087
Entropy (8bit):	7.939223952673508
Encrypted:	false
SSDEEP:	6144:J7IDzCvnAXYv/i/8bA7r8ePZFz1Yxp1T:qOnSY3A807r8AZFz1UN
MD5:	DC0CB7051E536384DE28ED52AB92EA19
SHA1:	D145293DEE4F6A963FE964B44CB791F599265B52
SHA-256:	7180220E08967228A453E1076EFDEB42589456E4CB6F1D5C8F5765F1994A179C
SHA-512:	DD189821102FE517D24541F9D34C77F4210802B7B3FD089D0AA28090DFF719676325A8F886209B3CEE48AEA6149A67A4EC4C3C97E252EA7336F9E8EF4E36CD5E

C:\Users\user\AppData\Local\Temp\nsz3D48.tmp	
Malicious:	false
Preview:	.....,.....d.....4..... .....G.....j..... ....

C:\Users\user\AppData\Local\Temp\nsz6311.tmp\qm1tw12xr.dll	
Process:	C:\Users\user\Desktop\PAYMENT SLIP.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4608
Entropy (8bit):	3.7496483038392974
Encrypted:	false
SSDEEP:	48:Sa/T+kBvwunRLZ6AL0rpRVaS53RS9BNZYWrTZxZ4Vo:+kBvFLgALER8S53RS9dtng
MD5:	EE2F349BA112FE569BD9AB1368E65791
SHA1:	9CEB495D81A804E604111D98C1169B4A9B640510
SHA-256:	5A97B6F5313D875AE40429BB27D486F7B745EEFDF5C116E434DC08770923FA9F
SHA-512:	D4CD1A797307B4FC4D9C3E80979BDDE682F64931FCF6D9CFCAE333646A242C143C2F77D2D6A80E01452A614E7981339E7E17580871B48518DC71A58339970B64
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`... .....!..... .....@.....%..K.... ..... .....text..... ..... ..`.rdata..+.... .....@..@.data...&....0.....@..... .....

C:\Users\user\AppData\Local\Temp\p7nih0ok4yeyw5j9l	
Process:	C:\Users\user\Desktop\PAYMENT SLIP.exe
File Type:	data
Category:	dropped
Size (bytes):	9733
Entropy (8bit):	7.976610510872038
Encrypted:	false
SSDEEP:	192:ttSk8it38myV0RlyqF61GDX8uuU078l07Ie73nOblxXLz7gUZW3E:/+UMmlzdjsv7CMz3ALzUl0
MD5:	B312481DDB4D93F427F4BFE952EC032F
SHA1:	A035A4ABF6D941F61F1427791B0121A4B400DB20
SHA-256:	E49684274A30B245C813044704EC5E9F4EB63163B6F0D18A969F5EC455240A2E
SHA-512:	E7697534D567B978BF4AD8AB015B3EA0CD39DC9A7EBF0DC77AF01075B797696895A8A4D5D52F834EC60DB877230353C99A7CD732AF023120079F1D3A889F513
Malicious:	false
Preview:	)..... ....=...A.*.....itE eJyOy....1..q.n.*...u..=!{~.....Z#..R....{..Up....54o.....$.../2e..<._j....0.J1m.z;>.N....t...\ev....FI.....x.t7.....!b.....[!$'....1,U..T.g.cP[.... ..!^.I.-...8...Dx{~..e. ~69.J...w...w..x..2..X...&._+...#.~...%.....S._=@.....z'.K..hkn.z.\zu....9.3j."G.z...%..svIE.?..N.....Hmt..6...QN...0-0S.|...X.a../;f....,5.M.....=.[G..DG*..r..q.be...0.T..psv....B}. ..%B....*...B.:..-I...P.t..W.....f6.....|....8..4..H.al....._.vD.....s.....^a..*l".....Oz.....~.....9<?..%.ID...l.|C..s....7..8v.r...Uj...k....=D..eOR...[.....O.iP..Y[^.mz.>.7SBY....4....5.e..+. c./.....:&^...)*m.hu..t..8^3*..buvy.C.8%..$%(E....-.ABE...d0L.OPS..._ZK.....9...{|.....K.d.....T....2...v.....l...#o%c.....}T!.....>?B..(..GUklo....v...:7.ky.....4=D.\ .H.B9V.Z=..N[.[R.I.,.....sG}.....<._.o...(T..,K.M.eAQP.....%.....,..K.2.....<.$....:.....&'*.F.../`ST....f.....a.....;....}~...h@-.H...M...;.

C:\Users\user\AppData\Local\Temp\tmp3E70.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	5.136963558289723
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mnc2xtn:cbk4oL600QydbQxIYODOLedq3ZLj
MD5:	AE766004C0D8792953BAFFFE8F6A2E3B
SHA1:	14B12F27543A401E2FE0AF8052E116CAB0032426
SHA-256:	1ABDD9B6A6B84E4BA1AF1282DC84CE276C59BA253F4C4AF05FEA498A4FD99540
SHA-512:	E530DA4A5D4336FC37838D0E93B5EB3804B9C489C71F6954A47FC81A4C655BB72EC493E109CF96E6E3617D7623AC80697AD3BBD5FFC6281BAFC8B34DCA5E65 7
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 />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatterie s>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAv ailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </Idl eSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\yj86kat5ru4v3qtvudmb	
Process:	C:\Users\user\Desktop\PAYMENT SLIP.exe
File Type:	data
Category:	dropped
Size (bytes):	207872
Entropy (8bit):	**7.998917498661265**
Encrypted:	**true**
SSDEEP:	6144:j7IDzCvnAXYv/i/8bA7r8ePZFz1Yxp1TN:cOnSY3A807r8AZFz1UNN
MD5:	C9F8BAE9DBB880A3C8D3100855E94065
SHA1:	2F66D8691CD7E33C7F5026DD7DB102FAFD664C7B
SHA-256:	913B0E52C651B9BE1F4FA52EFCBC9FBE6471B805A9AD27D8DDC6FB5286D330E6
SHA-512:	797E0D7E5D502332A049816F1AAE2C17060698C11432C0639079D0F16C7C2DB3F9B3A9F07A101729723C621A8A3D96972A164768126990A73FF0D01DC255EA6C
Malicious:	false
Preview:	VG$....(.Y..e.C.6J.........Q..=.42..(..| >.`4...d.....S+v._."......o./e.S.....y7....J.Y.n3.?..hu..n.GB3.5YND...1.Z..p.h5.5...or."R..:;.o.-.&5.W...VG.yX.+.PM...J....B....R.b....H?.I..... {.....N*.v..... .....o:.....qr...y....p~....yP.Y..d\.n..._..!...IE.VI*.....{v..>.%%...L..;^.(l8.....jY..)..9Gw...S...7e.....JLC...{...|XA.u.|.....I..\T.#.....Zq..=.z.w.L;...../..R.%%7.jl.|C.. jb..;ZcS..t..Gv..0.BK.|H.....q...7j..C.3?.6..b.....D...G>...\FSX,.\9.|=.....AY..N.....Ir.R....9...K...,.<....;@aQpL....V.#.iU.....q.z..F8.p5E..8.i.....z%.T.P....,xv....z..WV..e. .s....WB....B5....[....:d.=.V.P&7:....E.....N.?.-..OI..E....k.....j.[v..[..i..<3.A.....(-.a..Tq&..b.c)..=wFim..r.a.h.<..~..@P....4.t....5n..>...8....1.....q.P .....6..w..2.Z~.vv.....:.I_m~V $..8S..Ce.g.$z.n....y... &.%'J.....A.....m.=:D[L..O..7....o.....N...b..F.P@.'..Mq@....].A"','.zyP=....o.v.S.....`;.4.xZH.-7..h.J/....Pt.....qT...

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	1856
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	48:IknjhUknjhUknjhUknjhUknjhUknjhUknjhL:HjhDjhDjhDjhDjhDjhDjhL
MD5:	30D23CC577A89146961915B57F408623
SHA1:	9B5709D6081D8E0A570511E6E0AAE96FA041964F
SHA-256:	E2130A72E55193D402B5F43F7F3584ECF6B423F8EC4B1B1B69AD693C7E0E5A9E
SHA-512:	2D5C5747FD04F8326C2CC1FB313925070BC01D3352AFA6C36C167B72757A15F58B6263D96BD606338DA055812E69DDB628A6E18D64DD59697C2F42D1C58CC68
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?...A.K...J.=8x!....+ .2e'..E?.G.....[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?. ..A.K...J.=8x!....+.2e'..E?.G.....[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH }..../H.....L...?...A.K...J.=8x!....+.2e'..E?.G.....[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f. ..p.....:7rH}..../H.....L...?...A.K...J.=8x!....+.2e'..E?.G.....[.&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\v2.0.50727\MSBuild.exe
File Type:	International EBCDIC text, with NEL line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:bAt:U
MD5:	C2A50EDC6F6D3A2C5183544FFC6B36FE
SHA1:	41213577BDE2E7AD795F79D2747EA7B4FEBE44B7
SHA-256:	1105EDFF279035C252F149FAD0058E533177E1C4CD1525278187C168572D8A9B
SHA-512:	01C57FEEAE764B4541AF6078BFDB3C2C4599DC2E2063279507AA84B7C0DB11771E504A6437A8848B0EF30AB8BA3D2A10A4E06C4354DF8184BD8C6156E1413FC C
Malicious:	**true**
Preview:	\N..K..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.85263908467479
Encrypted:	false
SSDEEP:	3:oMty8WbSl1u:oMLWul1u
MD5:	A35128E4E28B27328F70E4E8FF482443
SHA1:	B89066B2F8DB34299AABFD7ABEE402D5444DD079
SHA-256:	88AEA00733DC4B570A29D56A423CC5BF163E5ACE7AF349972EB0BBA8D9AD06E1

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
SHA-512:	F098E844B5373B34642B49B6E0F2E15CFDAA1A8B6CABC2196CEC0F3765289E5B1FD4AB588DD65F97C8E51FA9A81077621E9A06946859F296904C646906A70F33
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe

C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe	
Process:	C:\Users\user\Desktop\PAYMENT SLIP.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	259286
Entropy (8bit):	7.914777825531565
Encrypted:	false
SSDEEP:	6144:kgORaiLT/dr9odWD2AHR5onxnn/UHDV8m0RjPwCytV:kgmLT/vodYR5gnn/i0RjPjc
MD5:	50C9D58F61950484825D85A9A1372A7D
SHA1:	79DF49A23AF28B6322F1FA461167B1145FC927DE
SHA-256:	80726D3E380E4A7D0D1EEE7F352C4A319E70DD4355A1A4F02AB27BABC1A13D15
SHA-512:	AC470694F9CA70CF8EB1A87604AE03E9F521FA413AA2D78F411AF4B7F60BC8CF346C2C69F30E083AA6F34E32041012F295DCF6BDAD378E1A2A8CD6D2E9FC06D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 43%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf.sV..Pf..V`..Pf.Rich.Pf..... .....PE..L.....$_.....f...*.....5.....@.....@.....P..... .....text...re.....f..... ..`.rdata.....j.....@..@.data...x.....~.....@....ndata.....rsrc...P.....@..@..... ....

\Device\ConDrv	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.107306146099542
Encrypted:	false
SSDEEP:	6:zx3M1tlAX8bSWR30qysGMQbSVRRZBXVRbJ0fFPRAgRYan:zK1XnV30ZsGMIG9BFRbQ5AUYan
MD5:	67DDD8252A246E7B14649B0063E351C0
SHA1:	AAE1C6839D1CC4A626D0FB2D4773823AD209FA17
SHA-256:	24C8283BA3F7FCA2E4CEF6F141263DD1E8A36E5A5CD96A97BFE83525D7663116
SHA-512:	326A5E0A440F60D4808C91499F1F3616C496B67DC053B4A2A40B0FE09002074AE5365018781F8746E98E7E3CFCD35F1310D17FB7C2138A8157318E6791987025
Malicious:	false
Preview:	Microsoft (R) Build Engine Version 2.0.50727.8922..[Microsoft .NET Framework, Version 2.0.50727.8922]..Copyright (C) Microsoft Corporation 2005. All rights reserved.....MSBUILD : error MSB1009: Project file does not exist...Switch: 0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.914777825531565
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	PAYMENT SLIP.exe
File size:	259286
MD5:	50c9d58f61950484825d85a9a1372a7d
SHA1:	79df49a23af28b6322f1fa461167b1145fc927de
SHA256:	80726d3e380e4a7d0d1eee7f352c4a319e70dd4355a1a402ab27babc1a13d15
SHA512:	ac470694f9ca70cf8eb1a87604ae03e9f521fa413aa2d78f411af4b7f60bc8cf346c2c69f30e083aa6f34e32041012f295dcf6bdad378e1a2a8cd6d2e9fc066d

General

SSDEEP:	6144:kgORaiLT/dr9odWD2AHR5onxnn/UHDV8m0RjPwCytV:kgmLT/vodYR5gnn/i0RjPjc
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....$_.....f...*.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x4035d8
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F24D702 [Sat Aug 1 02:44:18 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	c05041e01f84e1ccca9c4451f3b6a383

Entrypoint Preview

Instruction
sub esp, 000002D4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+14h], ebx
mov dword ptr [esp+10h], 0040A230h
mov dword ptr [esp+1Ch], ebx
call dword ptr [004080C8h]
call dword ptr [004080CCh]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042A26Ch], eax
je 00007FBFD4F753F3h
push ebx
call 00007FBFD4F786F9h
cmp eax, ebx
je 00007FBFD4F753E9h
push 00000C00h
call eax
mov esi, 004082B0h
push esi
call 00007FBFD4F78673h
push esi

Instruction
call dword ptr [00408154h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007FBFD4F753CCh
push 0000000Bh
call 00007FBFD4F786CCh
push 00000009h
call 00007FBFD4F786C5h
push 00000007h
mov dword ptr [0042A264h], eax
call 00007FBFD4F786B9h
cmp eax, ebx
je 00007FBFD4F753F1h
push 0000001Eh
call eax
test eax, eax
je 00007FBFD4F753E9h
or byte ptr [0042A26Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx
call dword ptr [00408298h]
mov dword ptr [0042A338h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 000002B4h
push eax
push ebx
push 00421708h
call dword ptr [0040818Ch]
push 0040A384h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3b000	0xa50	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
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	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6572	0x6600	False	0.662300857843	data	6.45391938596	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1398	0x1400	False	0.449609375	data	5.13671758274	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20378	0x600	False	0.5078125	data	4.09680908363	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.ndata	0x2b000	0x10000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3b000	0xa50	0xc00	False	0.402994791667	data	4.18988587465	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3b190	0x2e8	data	English	United States
RT_DIALOG	0x3b478	0x100	data	English	United States
RT_DIALOG	0x3b578	0x11c	data	English	United States
RT_DIALOG	0x3b698	0x60	data	English	United States
RT_GROUP_ICON	0x3b6f8	0x14	data	English	United States
RT_MANIFEST	0x3b710	0x340	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetWindowLongW, GetSysColor, SetWindowPos, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersion, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, ExitProcess, CopyFileW, GetCurrentProcess, GetModuleFileNameW, GetFileSize, CreateFileW, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Possible Origin

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

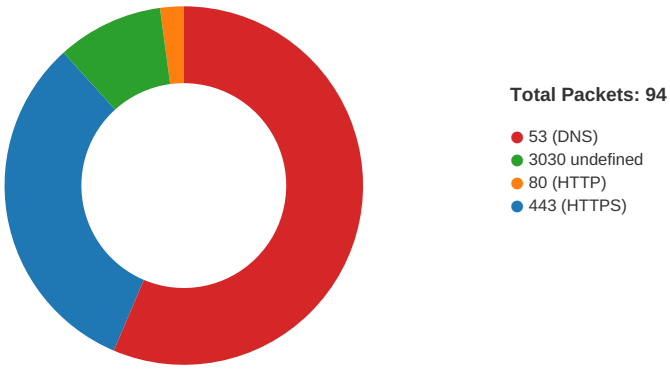
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-15:41:34.548350	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	3030	192.168.2.4	23.254.130.71
05/12/21-15:41:41.843567	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49746	3030	192.168.2.4	23.254.130.71
05/12/21-15:41:46.571158	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49747	3030	192.168.2.4	23.254.130.71

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-15:41:51.395995	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49748	3030	192.168.2.4	23.254.130.71
05/12/21-15:41:56.069794	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49750	3030	192.168.2.4	23.254.130.71
05/12/21-15:42:00.757206	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49755	3030	192.168.2.4	23.254.130.71
05/12/21-15:42:05.426115	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49763	3030	192.168.2.4	23.254.130.71
05/12/21-15:42:11.653205	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49769	3030	192.168.2.4	23.254.130.71
05/12/21-15:42:19.087468	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49770	3030	192.168.2.4	23.254.130.71
05/12/21-15:42:25.331297	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49771	3030	192.168.2.4	23.254.130.71
05/12/21-15:42:31.561598	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49772	3030	192.168.2.4	23.254.130.71
05/12/21-15:42:38.561876	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49773	3030	192.168.2.4	23.254.130.71
05/12/21-15:42:44.823846	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49777	3030	192.168.2.4	23.254.130.71
05/12/21-15:42:49.508873	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49778	3030	192.168.2.4	23.254.130.71
05/12/21-15:42:54.396373	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49779	3030	192.168.2.4	23.254.130.71
05/12/21-15:43:02.640724	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49780	3030	192.168.2.4	23.254.130.71
05/12/21-15:43:07.360825	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49781	3030	192.168.2.4	23.254.130.71

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 15:40:56.026963949 CEST	49717	443	192.168.2.4	204.79.197.200
May 12, 2021 15:40:56.064064026 CEST	443	49717	204.79.197.200	192.168.2.4
May 12, 2021 15:40:56.065521002 CEST	443	49717	204.79.197.200	192.168.2.4
May 12, 2021 15:40:56.065541983 CEST	443	49717	204.79.197.200	192.168.2.4
May 12, 2021 15:40:56.065642118 CEST	443	49717	204.79.197.200	192.168.2.4
May 12, 2021 15:40:56.065640926 CEST	49717	443	192.168.2.4	204.79.197.200
May 12, 2021 15:40:56.065661907 CEST	443	49717	204.79.197.200	192.168.2.4
May 12, 2021 15:40:56.065673113 CEST	49717	443	192.168.2.4	204.79.197.200
May 12, 2021 15:40:56.065677881 CEST	443	49717	204.79.197.200	192.168.2.4
May 12, 2021 15:40:56.065696001 CEST	443	49717	204.79.197.200	192.168.2.4
May 12, 2021 15:40:56.065700054 CEST	49717	443	192.168.2.4	204.79.197.200
May 12, 2021 15:40:56.065723896 CEST	49717	443	192.168.2.4	204.79.197.200
May 12, 2021 15:40:56.065773010 CEST	49717	443	192.168.2.4	204.79.197.200
May 12, 2021 15:40:56.376399994 CEST	49717	443	192.168.2.4	204.79.197.200
May 12, 2021 15:40:56.379153013 CEST	49717	443	192.168.2.4	204.79.197.200
May 12, 2021 15:40:56.379416943 CEST	49717	443	192.168.2.4	204.79.197.200

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 15:40:56.411833048 CEST	443	49717	204.79.197.200	192.168.2.4
May 12, 2021 15:40:56.413743019 CEST	443	49717	204.79.197.200	192.168.2.4
May 12, 2021 15:40:56.413815022 CEST	443	49717	204.79.197.200	192.168.2.4
May 12, 2021 15:40:56.413839102 CEST	49717	443	192.168.2.4	204.79.197.200
May 12, 2021 15:40:56.413873911 CEST	49717	443	192.168.2.4	204.79.197.200
May 12, 2021 15:40:56.414469004 CEST	443	49717	204.79.197.200	192.168.2.4
May 12, 2021 15:40:56.414696932 CEST	443	49717	204.79.197.200	192.168.2.4
May 12, 2021 15:40:56.414761066 CEST	49717	443	192.168.2.4	204.79.197.200
May 12, 2021 15:40:56.414896965 CEST	443	49717	204.79.197.200	192.168.2.4
May 12, 2021 15:40:56.449836969 CEST	49717	443	192.168.2.4	204.79.197.200
May 12, 2021 15:40:56.460462093 CEST	443	49717	204.79.197.200	192.168.2.4
May 12, 2021 15:40:56.460480928 CEST	443	49717	204.79.197.200	192.168.2.4
May 12, 2021 15:40:56.460618019 CEST	49717	443	192.168.2.4	204.79.197.200
May 12, 2021 15:40:56.485332012 CEST	443	49717	204.79.197.200	192.168.2.4
May 12, 2021 15:40:58.139776945 CEST	49708	80	192.168.2.4	93.184.220.29
May 12, 2021 15:41:20.264144897 CEST	80	49743	13.224.186.242	192.168.2.4
May 12, 2021 15:41:20.264288902 CEST	49743	80	192.168.2.4	13.224.186.242
May 12, 2021 15:41:20.815228939 CEST	443	49745	216.58.215.238	192.168.2.4
May 12, 2021 15:41:20.815392017 CEST	49745	443	192.168.2.4	216.58.215.238
May 12, 2021 15:41:20.819276094 CEST	443	49741	142.250.185.205	192.168.2.4
May 12, 2021 15:41:20.819477081 CEST	49741	443	192.168.2.4	142.250.185.205
May 12, 2021 15:41:20.842755079 CEST	443	49742	172.217.168.67	192.168.2.4
May 12, 2021 15:41:20.842927933 CEST	49742	443	192.168.2.4	172.217.168.67
May 12, 2021 15:41:26.463403940 CEST	443	49758	142.250.185.225	192.168.2.4
May 12, 2021 15:41:26.463473082 CEST	49758	443	192.168.2.4	142.250.185.225
May 12, 2021 15:41:27.048073053 CEST	49683	443	192.168.2.4	20.190.159.138
May 12, 2021 15:41:27.048115969 CEST	49683	443	192.168.2.4	20.190.159.138
May 12, 2021 15:41:27.051733017 CEST	49682	443	192.168.2.4	20.190.159.138
May 12, 2021 15:41:27.051822901 CEST	49682	443	192.168.2.4	20.190.159.138
May 12, 2021 15:41:27.110873938 CEST	443	49683	20.190.159.138	192.168.2.4
May 12, 2021 15:41:27.110907078 CEST	443	49683	20.190.159.138	192.168.2.4
May 12, 2021 15:41:27.114084959 CEST	443	49682	20.190.159.138	192.168.2.4
May 12, 2021 15:41:27.114109039 CEST	443	49682	20.190.159.138	192.168.2.4
May 12, 2021 15:41:27.154938936 CEST	443	49682	20.190.159.138	192.168.2.4
May 12, 2021 15:41:27.258677959 CEST	443	49682	20.190.159.138	192.168.2.4
May 12, 2021 15:41:27.258714914 CEST	443	49682	20.190.159.138	192.168.2.4
May 12, 2021 15:41:27.258738041 CEST	443	49682	20.190.159.138	192.168.2.4
May 12, 2021 15:41:27.258750916 CEST	49682	443	192.168.2.4	20.190.159.138
May 12, 2021 15:41:27.258759975 CEST	443	49682	20.190.159.138	192.168.2.4
May 12, 2021 15:41:27.258780003 CEST	443	49682	20.190.159.138	192.168.2.4
May 12, 2021 15:41:27.258791924 CEST	49682	443	192.168.2.4	20.190.159.138
May 12, 2021 15:41:27.258802891 CEST	443	49682	20.190.159.138	192.168.2.4
May 12, 2021 15:41:27.258830070 CEST	443	49682	20.190.159.138	192.168.2.4
May 12, 2021 15:41:27.258837938 CEST	49682	443	192.168.2.4	20.190.159.138
May 12, 2021 15:41:27.258855104 CEST	443	49682	20.190.159.138	192.168.2.4
May 12, 2021 15:41:27.258876085 CEST	443	49682	20.190.159.138	192.168.2.4
May 12, 2021 15:41:27.258924007 CEST	49682	443	192.168.2.4	20.190.159.138
May 12, 2021 15:41:27.264658928 CEST	443	49683	20.190.159.138	192.168.2.4
May 12, 2021 15:41:27.264698029 CEST	443	49683	20.190.159.138	192.168.2.4
May 12, 2021 15:41:27.264713049 CEST	443	49683	20.190.159.138	192.168.2.4
May 12, 2021 15:41:27.264730930 CEST	443	49683	20.190.159.138	192.168.2.4
May 12, 2021 15:41:27.264749050 CEST	443	49683	20.190.159.138	192.168.2.4
May 12, 2021 15:41:27.264765024 CEST	443	49683	20.190.159.138	192.168.2.4
May 12, 2021 15:41:27.264785051 CEST	443	49683	20.190.159.138	192.168.2.4
May 12, 2021 15:41:27.264802933 CEST	443	49683	20.190.159.138	192.168.2.4
May 12, 2021 15:41:27.264818907 CEST	443	49683	20.190.159.138	192.168.2.4
May 12, 2021 15:41:27.264822006 CEST	49683	443	192.168.2.4	20.190.159.138
May 12, 2021 15:41:27.264858007 CEST	49683	443	192.168.2.4	20.190.159.138
May 12, 2021 15:41:27.307136059 CEST	49683	443	192.168.2.4	20.190.159.138
May 12, 2021 15:41:27.913104057 CEST	443	49763	172.217.23.42	192.168.2.4
May 12, 2021 15:41:27.913273096 CEST	49763	443	192.168.2.4	172.217.23.42
May 12, 2021 15:41:34.330414057 CEST	49745	3030	192.168.2.4	23.254.130.71
May 12, 2021 15:41:34.497849941 CEST	3030	49745	23.254.130.71	192.168.2.4
May 12, 2021 15:41:34.498466969 CEST	49745	3030	192.168.2.4	23.254.130.71

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 15:41:34.548350096 CEST	49745	3030	192.168.2.4	23.254.130.71
May 12, 2021 15:41:34.735836029 CEST	3030	49745	23.254.130.71	192.168.2.4
May 12, 2021 15:41:34.736342907 CEST	49745	3030	192.168.2.4	23.254.130.71
May 12, 2021 15:41:34.945247889 CEST	3030	49745	23.254.130.71	192.168.2.4
May 12, 2021 15:41:34.949302912 CEST	49745	3030	192.168.2.4	23.254.130.71
May 12, 2021 15:41:35.118865967 CEST	3030	49745	23.254.130.71	192.168.2.4
May 12, 2021 15:41:35.119357109 CEST	49745	3030	192.168.2.4	23.254.130.71
May 12, 2021 15:41:35.347301006 CEST	3030	49745	23.254.130.71	192.168.2.4
May 12, 2021 15:41:35.347610950 CEST	49745	3030	192.168.2.4	23.254.130.71
May 12, 2021 15:41:35.570543051 CEST	3030	49745	23.254.130.71	192.168.2.4
May 12, 2021 15:41:35.570683002 CEST	49745	3030	192.168.2.4	23.254.130.71
May 12, 2021 15:41:35.787461042 CEST	3030	49745	23.254.130.71	192.168.2.4
May 12, 2021 15:41:35.787610054 CEST	49745	3030	192.168.2.4	23.254.130.71
May 12, 2021 15:41:35.840923071 CEST	3030	49745	23.254.130.71	192.168.2.4
May 12, 2021 15:41:35.840960026 CEST	3030	49745	23.254.130.71	192.168.2.4
May 12, 2021 15:41:35.840970993 CEST	3030	49745	23.254.130.71	192.168.2.4
May 12, 2021 15:41:35.840996027 CEST	3030	49745	23.254.130.71	192.168.2.4
May 12, 2021 15:41:35.841013908 CEST	3030	49745	23.254.130.71	192.168.2.4
May 12, 2021 15:41:35.841029882 CEST	3030	49745	23.254.130.71	192.168.2.4
May 12, 2021 15:41:35.841052055 CEST	3030	49745	23.254.130.71	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 15:40:56.365001917 CEST	54531	53	192.168.2.4	8.8.8.8
May 12, 2021 15:40:56.413590908 CEST	53	54531	8.8.8.8	192.168.2.4
May 12, 2021 15:40:57.462188005 CEST	49714	53	192.168.2.4	8.8.8.8
May 12, 2021 15:40:57.510945082 CEST	53	49714	8.8.8.8	192.168.2.4
May 12, 2021 15:40:58.096000910 CEST	58028	53	192.168.2.4	8.8.8.8
May 12, 2021 15:40:58.155076981 CEST	53	58028	8.8.8.8	192.168.2.4
May 12, 2021 15:40:58.895443916 CEST	53097	53	192.168.2.4	8.8.8.8
May 12, 2021 15:40:58.944289923 CEST	53	53097	8.8.8.8	192.168.2.4
May 12, 2021 15:40:59.821526051 CEST	49257	53	192.168.2.4	8.8.8.8
May 12, 2021 15:40:59.873083115 CEST	53	49257	8.8.8.8	192.168.2.4
May 12, 2021 15:41:01.446532011 CEST	62389	53	192.168.2.4	8.8.8.8
May 12, 2021 15:41:01.498163939 CEST	53	62389	8.8.8.8	192.168.2.4
May 12, 2021 15:41:02.455862045 CEST	49910	53	192.168.2.4	8.8.8.8
May 12, 2021 15:41:02.507606030 CEST	53	49910	8.8.8.8	192.168.2.4
May 12, 2021 15:41:03.504097939 CEST	55854	53	192.168.2.4	8.8.8.8
May 12, 2021 15:41:03.556497097 CEST	53	55854	8.8.8.8	192.168.2.4
May 12, 2021 15:41:08.438261032 CEST	64549	53	192.168.2.4	8.8.8.8
May 12, 2021 15:41:08.490040064 CEST	53	64549	8.8.8.8	192.168.2.4
May 12, 2021 15:41:09.995616913 CEST	63153	53	192.168.2.4	8.8.8.8
May 12, 2021 15:41:10.046076059 CEST	53	63153	8.8.8.8	192.168.2.4
May 12, 2021 15:41:11.000562906 CEST	52991	53	192.168.2.4	8.8.8.8
May 12, 2021 15:41:11.078963041 CEST	53	52991	8.8.8.8	192.168.2.4
May 12, 2021 15:41:12.131509066 CEST	53700	53	192.168.2.4	8.8.8.8
May 12, 2021 15:41:12.180249929 CEST	53	53700	8.8.8.8	192.168.2.4
May 12, 2021 15:41:13.211496115 CEST	51726	53	192.168.2.4	8.8.8.8
May 12, 2021 15:41:13.260318995 CEST	53	51726	8.8.8.8	192.168.2.4
May 12, 2021 15:41:14.317698002 CEST	56794	53	192.168.2.4	8.8.8.8
May 12, 2021 15:41:14.366503000 CEST	53	56794	8.8.8.8	192.168.2.4
May 12, 2021 15:41:23.708602905 CEST	56534	53	192.168.2.4	8.8.8.8
May 12, 2021 15:41:23.762186050 CEST	53	56534	8.8.8.8	192.168.2.4
May 12, 2021 15:41:24.810179949 CEST	56627	53	192.168.2.4	8.8.8.8
May 12, 2021 15:41:24.858977079 CEST	53	56627	8.8.8.8	192.168.2.4
May 12, 2021 15:41:26.637279987 CEST	56621	53	192.168.2.4	8.8.8.8
May 12, 2021 15:41:26.686199903 CEST	53	56621	8.8.8.8	192.168.2.4
May 12, 2021 15:41:27.852693081 CEST	63116	53	192.168.2.4	8.8.8.8
May 12, 2021 15:41:27.904263973 CEST	53	63116	8.8.8.8	192.168.2.4
May 12, 2021 15:41:27.915894985 CEST	64078	53	192.168.2.4	8.8.8.8
May 12, 2021 15:41:27.975853920 CEST	53	64078	8.8.8.8	192.168.2.4
May 12, 2021 15:41:29.517250061 CEST	64801	53	192.168.2.4	8.8.8.8
May 12, 2021 15:41:29.566082001 CEST	53	64801	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 15:41:30.614928961 CEST	61721	53	192.168.2.4	8.8.8.8
May 12, 2021 15:41:30.665735960 CEST	53	61721	8.8.8.8	192.168.2.4
May 12, 2021 15:41:34.259408951 CEST	51255	53	192.168.2.4	8.8.8.8
May 12, 2021 15:41:34.319515944 CEST	53	51255	8.8.8.8	192.168.2.4
May 12, 2021 15:41:41.593622923 CEST	61522	53	192.168.2.4	8.8.8.8
May 12, 2021 15:41:41.655122995 CEST	53	61522	8.8.8.8	192.168.2.4
May 12, 2021 15:41:46.336102009 CEST	52337	53	192.168.2.4	8.8.8.8
May 12, 2021 15:41:46.398098946 CEST	53	52337	8.8.8.8	192.168.2.4
May 12, 2021 15:41:51.142338037 CEST	55046	53	192.168.2.4	8.8.8.8
May 12, 2021 15:41:51.202563047 CEST	53	55046	8.8.8.8	192.168.2.4
May 12, 2021 15:41:51.428154945 CEST	49612	53	192.168.2.4	8.8.8.8
May 12, 2021 15:41:51.485519886 CEST	53	49612	8.8.8.8	192.168.2.4
May 12, 2021 15:41:55.850594044 CEST	49285	53	192.168.2.4	8.8.8.8
May 12, 2021 15:41:55.899343967 CEST	53	49285	8.8.8.8	192.168.2.4
May 12, 2021 15:41:56.742501020 CEST	50601	53	192.168.2.4	8.8.8.8
May 12, 2021 15:41:56.845690012 CEST	53	50601	8.8.8.8	192.168.2.4
May 12, 2021 15:41:57.624161005 CEST	60875	53	192.168.2.4	8.8.8.8
May 12, 2021 15:41:57.684287071 CEST	53	60875	8.8.8.8	192.168.2.4
May 12, 2021 15:41:58.659828901 CEST	56448	53	192.168.2.4	8.8.8.8
May 12, 2021 15:41:58.826293945 CEST	53	56448	8.8.8.8	192.168.2.4
May 12, 2021 15:42:00.020754099 CEST	59172	53	192.168.2.4	8.8.8.8
May 12, 2021 15:42:00.071636915 CEST	53	59172	8.8.8.8	192.168.2.4
May 12, 2021 15:42:00.509931087 CEST	62420	53	192.168.2.4	8.8.8.8
May 12, 2021 15:42:00.569497108 CEST	53	62420	8.8.8.8	192.168.2.4
May 12, 2021 15:42:00.671063900 CEST	60579	53	192.168.2.4	8.8.8.8
May 12, 2021 15:42:00.731378078 CEST	53	60579	8.8.8.8	192.168.2.4
May 12, 2021 15:42:01.064954042 CEST	50183	53	192.168.2.4	8.8.8.8
May 12, 2021 15:42:01.132759094 CEST	53	50183	8.8.8.8	192.168.2.4
May 12, 2021 15:42:01.307965994 CEST	61531	53	192.168.2.4	8.8.8.8
May 12, 2021 15:42:01.365118027 CEST	53	61531	8.8.8.8	192.168.2.4
May 12, 2021 15:42:01.830445051 CEST	49228	53	192.168.2.4	8.8.8.8
May 12, 2021 15:42:01.887847900 CEST	53	49228	8.8.8.8	192.168.2.4
May 12, 2021 15:42:02.659746885 CEST	59794	53	192.168.2.4	8.8.8.8
May 12, 2021 15:42:02.708405018 CEST	53	59794	8.8.8.8	192.168.2.4
May 12, 2021 15:42:03.681365013 CEST	55916	53	192.168.2.4	8.8.8.8
May 12, 2021 15:42:03.738527060 CEST	53	55916	8.8.8.8	192.168.2.4
May 12, 2021 15:42:04.213337898 CEST	52752	53	192.168.2.4	8.8.8.8
May 12, 2021 15:42:04.275392056 CEST	53	52752	8.8.8.8	192.168.2.4
May 12, 2021 15:42:05.186784983 CEST	60542	53	192.168.2.4	8.8.8.8
May 12, 2021 15:42:05.250067949 CEST	53	60542	8.8.8.8	192.168.2.4
May 12, 2021 15:42:08.201644897 CEST	60689	53	192.168.2.4	8.8.8.8
May 12, 2021 15:42:08.252142906 CEST	53	60689	8.8.8.8	192.168.2.4
May 12, 2021 15:42:11.425129890 CEST	64206	53	192.168.2.4	8.8.8.8
May 12, 2021 15:42:11.482409954 CEST	53	64206	8.8.8.8	192.168.2.4
May 12, 2021 15:42:18.821676016 CEST	50904	53	192.168.2.4	8.8.8.8
May 12, 2021 15:42:18.879184008 CEST	53	50904	8.8.8.8	192.168.2.4
May 12, 2021 15:42:25.091231108 CEST	57525	53	192.168.2.4	8.8.8.8
May 12, 2021 15:42:25.154309034 CEST	53	57525	8.8.8.8	192.168.2.4
May 12, 2021 15:42:31.332638025 CEST	53814	53	192.168.2.4	8.8.8.8
May 12, 2021 15:42:31.389828920 CEST	53	53814	8.8.8.8	192.168.2.4
May 12, 2021 15:42:38.191953897 CEST	53418	53	192.168.2.4	8.8.8.8
May 12, 2021 15:42:38.251568079 CEST	53	53418	8.8.8.8	192.168.2.4
May 12, 2021 15:42:39.914653063 CEST	62833	53	192.168.2.4	8.8.8.8
May 12, 2021 15:42:39.990272045 CEST	53	62833	8.8.8.8	192.168.2.4
May 12, 2021 15:42:41.877824068 CEST	59260	53	192.168.2.4	8.8.8.8
May 12, 2021 15:42:41.934930086 CEST	53	59260	8.8.8.8	192.168.2.4
May 12, 2021 15:42:44.560812950 CEST	49944	53	192.168.2.4	8.8.8.8
May 12, 2021 15:42:44.619924068 CEST	53	49944	8.8.8.8	192.168.2.4
May 12, 2021 15:42:49.266288042 CEST	63300	53	192.168.2.4	8.8.8.8
May 12, 2021 15:42:49.323539972 CEST	53	63300	8.8.8.8	192.168.2.4
May 12, 2021 15:42:54.101478100 CEST	61449	53	192.168.2.4	8.8.8.8
May 12, 2021 15:42:54.160172939 CEST	53	61449	8.8.8.8	192.168.2.4
May 12, 2021 15:43:02.405359030 CEST	51275	53	192.168.2.4	8.8.8.8
May 12, 2021 15:43:02.468023062 CEST	53	51275	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 15:43:07.135113955 CEST	63492	53	192.168.2.4	8.8.8.8
May 12, 2021 15:43:07.192173004 CEST	53	63492	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 15:41:34.259408951 CEST	192.168.2.4	8.8.8.8	0xaa10	Standard query (0)	seaudo.hopto.org	A (IP address)	IN (0x0001)
May 12, 2021 15:41:41.593622923 CEST	192.168.2.4	8.8.8.8	0x15dd	Standard query (0)	seaudo.hopto.org	A (IP address)	IN (0x0001)
May 12, 2021 15:41:46.336102009 CEST	192.168.2.4	8.8.8.8	0x49fd	Standard query (0)	seaudo.hopto.org	A (IP address)	IN (0x0001)
May 12, 2021 15:41:51.142338037 CEST	192.168.2.4	8.8.8.8	0x7b21	Standard query (0)	seaudo.hopto.org	A (IP address)	IN (0x0001)
May 12, 2021 15:41:55.850594044 CEST	192.168.2.4	8.8.8.8	0x1687	Standard query (0)	seaudo.hopto.org	A (IP address)	IN (0x0001)
May 12, 2021 15:42:00.509931087 CEST	192.168.2.4	8.8.8.8	0x958c	Standard query (0)	seaudo.hopto.org	A (IP address)	IN (0x0001)
May 12, 2021 15:42:05.186784983 CEST	192.168.2.4	8.8.8.8	0x1b63	Standard query (0)	seaudo.hopto.org	A (IP address)	IN (0x0001)
May 12, 2021 15:42:11.425129890 CEST	192.168.2.4	8.8.8.8	0x6ee1	Standard query (0)	seaudo.hopto.org	A (IP address)	IN (0x0001)
May 12, 2021 15:42:18.821676016 CEST	192.168.2.4	8.8.8.8	0x780a	Standard query (0)	seaudo.hopto.org	A (IP address)	IN (0x0001)
May 12, 2021 15:42:25.091231108 CEST	192.168.2.4	8.8.8.8	0x4ab5	Standard query (0)	seaudo.hopto.org	A (IP address)	IN (0x0001)
May 12, 2021 15:42:31.332638025 CEST	192.168.2.4	8.8.8.8	0xcf2f	Standard query (0)	seaudo.hopto.org	A (IP address)	IN (0x0001)
May 12, 2021 15:42:38.191953897 CEST	192.168.2.4	8.8.8.8	0x9831	Standard query (0)	seaudo.hopto.org	A (IP address)	IN (0x0001)
May 12, 2021 15:42:44.560812950 CEST	192.168.2.4	8.8.8.8	0xb990	Standard query (0)	seaudo.hopto.org	A (IP address)	IN (0x0001)
May 12, 2021 15:42:49.266288042 CEST	192.168.2.4	8.8.8.8	0xdd77	Standard query (0)	seaudo.hopto.org	A (IP address)	IN (0x0001)
May 12, 2021 15:42:54.101478100 CEST	192.168.2.4	8.8.8.8	0x5c0f	Standard query (0)	seaudo.hopto.org	A (IP address)	IN (0x0001)
May 12, 2021 15:43:02.405359030 CEST	192.168.2.4	8.8.8.8	0x28cd	Standard query (0)	seaudo.hopto.org	A (IP address)	IN (0x0001)
May 12, 2021 15:43:07.135113955 CEST	192.168.2.4	8.8.8.8	0xaa22	Standard query (0)	seaudo.hopto.org	A (IP address)	IN (0x0001)

DNS Answers

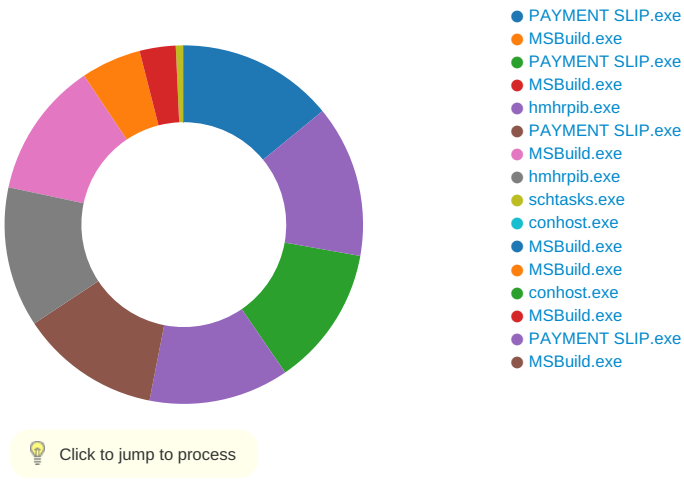
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 15:41:34.319515944 CEST	8.8.8.8	192.168.2.4	0xaa10	No error (0)	seaudo.hopto.org		23.254.130.71	A (IP address)	IN (0x0001)
May 12, 2021 15:41:41.655122995 CEST	8.8.8.8	192.168.2.4	0x15dd	No error (0)	seaudo.hopto.org		23.254.130.71	A (IP address)	IN (0x0001)
May 12, 2021 15:41:46.398098946 CEST	8.8.8.8	192.168.2.4	0x49fd	No error (0)	seaudo.hopto.org		23.254.130.71	A (IP address)	IN (0x0001)
May 12, 2021 15:41:51.202563047 CEST	8.8.8.8	192.168.2.4	0x7b21	No error (0)	seaudo.hopto.org		23.254.130.71	A (IP address)	IN (0x0001)
May 12, 2021 15:41:55.899343967 CEST	8.8.8.8	192.168.2.4	0x1687	No error (0)	seaudo.hopto.org		23.254.130.71	A (IP address)	IN (0x0001)
May 12, 2021 15:42:00.569497108 CEST	8.8.8.8	192.168.2.4	0x958c	No error (0)	seaudo.hopto.org		23.254.130.71	A (IP address)	IN (0x0001)
May 12, 2021 15:42:05.250067949 CEST	8.8.8.8	192.168.2.4	0x1b63	No error (0)	seaudo.hopto.org		23.254.130.71	A (IP address)	IN (0x0001)
May 12, 2021 15:42:11.482409954 CEST	8.8.8.8	192.168.2.4	0x6ee1	No error (0)	seaudo.hopto.org		23.254.130.71	A (IP address)	IN (0x0001)
May 12, 2021 15:42:18.879184008 CEST	8.8.8.8	192.168.2.4	0x780a	No error (0)	seaudo.hopto.org		23.254.130.71	A (IP address)	IN (0x0001)
May 12, 2021 15:42:25.154309034 CEST	8.8.8.8	192.168.2.4	0x4ab5	No error (0)	seaudo.hopto.org		23.254.130.71	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 15:42:31.389828920 CEST	8.8.8.8	192.168.2.4	0xcf2f	No error (0)	seaudo.hopto.org		23.254.130.71	A (IP address)	IN (0x0001)
May 12, 2021 15:42:38.251568079 CEST	8.8.8.8	192.168.2.4	0x9831	No error (0)	seaudo.hopto.org		23.254.130.71	A (IP address)	IN (0x0001)
May 12, 2021 15:42:44.619924068 CEST	8.8.8.8	192.168.2.4	0xb990	No error (0)	seaudo.hopto.org		23.254.130.71	A (IP address)	IN (0x0001)
May 12, 2021 15:42:49.323539972 CEST	8.8.8.8	192.168.2.4	0xdd77	No error (0)	seaudo.hopto.org		23.254.130.71	A (IP address)	IN (0x0001)
May 12, 2021 15:42:54.160172939 CEST	8.8.8.8	192.168.2.4	0x5c0f	No error (0)	seaudo.hopto.org		23.254.130.71	A (IP address)	IN (0x0001)
May 12, 2021 15:43:02.468023062 CEST	8.8.8.8	192.168.2.4	0x28cd	No error (0)	seaudo.hopto.org		23.254.130.71	A (IP address)	IN (0x0001)
May 12, 2021 15:43:07.192173004 CEST	8.8.8.8	192.168.2.4	0xaa22	No error (0)	seaudo.hopto.org		23.254.130.71	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: PAYMENT SLIP.exe PID: 6804 Parent PID: 6052

General

Start time:	15:41:03
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\PAYMENT SLIP.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PAYMENT SLIP.exe'
Imagebase:	0x400000
File size:	259286 bytes

MD5 hash:	50C9D58F61950484825D85A9A1372A7D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.665787151.0000000002400000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.665787151.0000000002400000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.665787151.0000000002400000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.665787151.0000000002400000.00000004.00000001.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\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsmD248.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4060A0	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsmD249.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4060A0	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	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	405AFC	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\p7nih0ok4yeyw5j9l	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40605E	CreateFileW
C:\Users\user\AppData\Local\Temp\yj86kat5ru4v3qtvudmb	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40605E	CreateFileW
C:\Users\user\AppData\Local\Temp\nshD279.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4060A0	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW

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	405AFC	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nshD279.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405ABC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nshD279.tmp\qm1tw12xr.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40605E	CreateFileW
C:\Users\user\AppData\Roaming\tteegmiuoefs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	B11C62	CreateDirectoryW
C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	B11BAC	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsmD248.tmp	success or wait	1	403887	DeleteFileW
C:\Users\user\AppData\Local\Temp\nshD279.tmp	success or wait	1	405C7D	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\nsmD249.tmp	unknown	20692	fa 12 00 00 80 00 00 00 2c 01 00 00 02 00 00 00 ac 01 00 00 01 00 00 00 c4 09 00 00 18 00 00 00 64 0c 00 00 00 00 00 00 34 12 00 00 01 00 00 00 fa 12 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 ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 ff 00 00 c6 00 00 00 f1 ff ff ff 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 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 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 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	.......,.................... ..d.......4..................	success or wait	14	4060FE	WriteFile
C:\Users\user\AppData\Local\Temp\p7nih0ok4yeyw5j9l	unknown	9733	29 e7 f8 b4 b7 80 c7 88 f0 20 0e bc bc 17 3d f1 e0 96 41 eb 2a d3 c2 98 c7 f6 b9 d5 c4 69 74 45 20 65 4a 79 4f 79 fa f5 ab c0 31 05 f4 71 9f 6e 80 2a b0 c4 8c b4 75 1d 9b 3d 21 7b 7e 9c 9a 0f db e9 5a 23 9a 88 52 d8 85 88 ab 17 7b b1 18 55 70 91 a3 a6 f9 35 34 6f c6 93 fe 8c b1 b4 b7 c3 1d 1e 24 81 bc c6 2f 32 65 81 f7 3c f3 5f 6a c0 dd e0 83 30 fb 4a 31 6d 88 7a 3b 3e 91 4e 1d c7 1f eb 96 74 08 0b 0e 5c 65 76 fc 1a 15 ae 46 49 bc d9 13 d3 0a 78 c3 a8 74 37 1a 88 18 a2 89 c6 21 62 13 16 e9 e5 e5 e0 b7 84 ee 5b 21 24 27 b4 a1 0e 15 31 2c 55 9e a1 54 f2 67 ac 63 50 5b 8f cc cf f2 20 91 ba 21 5e f9 49 ea 2d 00 be d1 38 cf dc 07 44 78 7b 7e cc d5 65 ed 8a 85 7e 36 39 ac 4a db 83 fb e8 b3 77 e4 e7 ca 77 01 11 78 b6 11 32 02 05 58 95 b0 cf 26 f4 5f 2b 10 13 16	)........ ....=...A.*........itE eJyOy....1..q.n.*....u..=!{ ~.....Z#..R.....{..Up....54o.. ....$.../2e..<._j....0.J1m .z;>.N.....t...\ev....FI.....x ..t7......!b.........[!$'....1 ,U..T.g.cP[.... ..!^.I.-...8.. .Dx{~..e...~69.J.....w...w..x. .2..X...&._+...	success or wait	1	4060FE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\yj86kat5ru4v3qtvudmb	unknown	16384	56 47 24 10 cb 2e 80 28 10 59 be a6 65 81 43 bc 36 4a 9c 1c c3 b1 ac d9 a5 0c 02 ac 11 51 e1 e4 3d a9 34 32 04 b5 28 8e ff 7c 20 3e de 60 34 0c a2 8e 64 1d 1a f7 f5 bb de 53 2b 76 bd 5f ef b7 22 a2 83 b8 a2 94 9f 6f 2e 2f 65 9e 53 a5 18 93 e2 a8 f9 eb 79 37 9b 8d d1 14 4a 14 59 e7 6e 33 ef 3f 9b ba 68 75 09 d5 6e de 47 42 33 c3 b0 35 59 4e 44 8a d7 a7 08 31 d3 a6 5a 11 b5 70 97 68 35 ee 35 a2 9c b0 6f 72 dd 22 52 ff 98 3a b4 3b 94 6f 1e 2d ea 9c 26 35 e0 57 82 a6 16 56 47 f8 79 58 1e 2b be 50 4d 8c 94 eb 4a 89 9e fc de 42 cd c7 cb 1c 52 c0 62 bf a7 b3 c7 bf 48 3f 96 6c 0a 10 8f 86 8a 99 dd 7b ac 0a 1f cb f8 86 af 4e 2a e4 76 f5 82 e9 f1 fa 15 20 92 eb b7 af e0 94 9a 6f 3a c8 e6 1b 85 80 a2 df ec eb f9 71 72 d5 d6 cb 79 bd a4 d6 f8 70 7e 1e ac a5 e6 ad 79	VG$....(.Y..e.C.6J...........Q ..=.42..(..| >.`4...d......S+v ._..".......o./e.S.......y7.... J.Y.n3.?..hu..n.GB3..5YND ....1 ..Z..p.h5.5...or."R..:.;.o.-.. &5.W...VG.yX.+.PM...J....B ....R.b.....H?.l.......{.......N*. v...... ....o:..........qr. ..y....p~.....y	success or wait	13	4060FE	WriteFile
C:\Users\user\AppData\Local\Temp\nshD279.tmp\qm1tw12xr.dll	unknown	4608	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 80 d2 9b 60 00 00 00 00 00 00 00 00 e0 00 03 21 0b 01 0b 00 00 04 00 00 00 0a 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $............................ ....PE..L......`...........!	success or wait	1	4060FE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe	unknown	259286	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 ad 31 08 81 e9 50 66 d2 e9 50 66 d2 e9 50 66 d2 2a 5f 39 d2 eb 50 66 d2 e9 50 67 d2 4c 50 66 d2 2a 5f 3b d2 e6 50 66 d2 bd 73 56 d2 e3 50 66 d2 2e 56 60 d2 e8 50 66 d2 52 69 63 68 e9 50 66 d2 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 50 45 00 00 4c 01 05 00 02 d7 24 5f 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 66 00 00 00 2a 02 00 00 08 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........1...Pf..Pf..Pf.*_9..P f..Pg.LPf.*_;..Pf..sV..Pf..V`. .Pf.Rich.Pf.................. ......PE..L.....$_........... .....f...*.....	success or wait	1	B11BC1	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PAYMENT SLIP.exe	unknown	512	success or wait	81	4060CF	ReadFile
C:\Users\user\Desktop\PAYMENT SLIP.exe	unknown	16384	success or wait	14	4060CF	ReadFile
C:\Users\user\AppData\Local\Temp\nsmD249.tmp	unknown	4	success or wait	1	4060CF	ReadFile
C:\Users\user\AppData\Local\Temp\nsmD249.tmp	unknown	4858	success or wait	1	4033F7	ReadFile
C:\Users\user\AppData\Local\Temp\nsmD249.tmp	unknown	4	success or wait	3	4060CF	ReadFile
C:\Users\user\AppData\Local\Temp\p7nih0ok4yeyw5j9l	unknown	9733	success or wait	1	100010CB	ReadFile
C:\Users\user\Desktop\PAYMENT SLIP.exe	unknown	259286	success or wait	1	B11B82	ReadFile
C:\Users\user\AppData\Local\Temp\yj86kat5ru4v3qtvudmb	unknown	207872	success or wait	1	B119C2	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	B10AA8	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	B10AA8	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	B10AA8	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	jnckjcfx	unicode	C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe"......u. ......HA$.D\.D.........B....''..D...uD.DD	success or wait	1	B12170	RegSetValueExW

Analysis Process: MSBuild.exe PID: 7012 Parent PID: 6804

General

Start time:	15:41:09
Start date:	12/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Wow64 process (32bit):	false

Commandline:	'C:\Users\user\Desktop\PAYMENT SLIP.exe'
Imagebase:	0x70000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: PAYMENT SLIP.exe PID: 7116 Parent PID: 6804

General

Start time:	15:41:13
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\PAYMENT SLIP.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PAYMENT SLIP.exe'
Imagebase:	0x400000
File size:	259286 bytes
MD5 hash:	50C9D58F61950484825D85A9A1372A7D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.693808017.0000000003160000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.693808017.0000000003160000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.693808017.0000000003160000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.693808017.0000000003160000.00000004.00000001.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\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nssFAA0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4060A0	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsnFAD0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4060A0	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	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	405AFC	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsiFB00.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4060A0	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	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	405AFC	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsiFB00.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405ABC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsiFB00.tmp\qm1tw12xr.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40605E	CreateFileW
C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	1	3051BAC	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nssFAA0.tmp	success or wait	1	403887	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsiFB00.tmp	success or wait	1	405C7D	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\nsnFAD0.tmp	unknown	20692	fa 12 00 00 80 00 00 00 2c 01 00 00 02 00 00 00 ac 01 00 00 01 00 00 00 c4 09 00 00 18 00 00 00 64 0c 00 00 00 00 00 00 34 12 00 00 01 00 00 00 fa 12 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 ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 ff 00 00 c6 00 00 00 f1 ff ff ff 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 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 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 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	.......,..................... ..d.......4...................	success or wait	14	4060FE	WriteFile
C:\Users\user\AppData\Local\Temp\p7nih0ok4yeyw5j9l	unknown	9733	29 e7 f8 b4 b7 80 c7 88 f0 20 0e bc bc 17 3d f1 e0 96 41 eb 2a d3 c2 98 c7 f6 b9 d5 c4 69 74 45 20 65 4a 79 4f 79 fa f5 ab c0 31 05 f4 71 9f 6e 80 2a b0 c4 8c b4 75 1d 9b 3d 21 7b 7e 9c 9a 0f db e9 5a 23 9a 88 52 d8 85 88 ab 17 7b b1 18 55 70 91 a3 a6 f9 35 34 6f c6 93 fe 8c b1 b4 b7 c3 1d 1e 24 81 bc c6 2f 32 65 81 f7 3c f3 5f 6a c0 dd e0 83 30 fb 4a 31 6d 88 7a 3b 3e 91 4e 1d c7 1f eb 96 74 08 0b 0e 5c 65 76 fc 1a 15 ae 46 49 bc d9 13 d3 0a 78 c3 a8 74 37 1a 88 18 a2 89 c6 21 62 13 16 e9 e5 e5 e0 b7 84 ee 5b 21 24 27 b4 a1 0e 15 31 2c 55 9e a1 54 f2 67 ac 63 50 5b 8f cc cf f2 20 91 ba 21 5e f9 49 ea 2d 00 be d1 38 cf dc 07 44 78 7b 7e cc d5 65 ed 8a 85 7e 36 39 ac 4a db 83 fb e8 b3 77 e4 e7 ca 77 01 11 78 b6 11 32 02 05 58 95 b0 cf 26 f4 5f 2b 10 13 16	)........ ....=...A.*........itE eJyOy....1..q.n.*....u..=!{ ~.....Z#..R.....{..Up....54o.. ....$.../2e..<._j....0.J1m .z;>.N.....t...\ev....FI.....x ..t7......!b.........[!$'....1 ,U..T.g.cP[.... ..!^.I.-...8.. .Dx{~..e...~69.J.....w...w..x. .2..X...&._+...	success or wait	1	4060FE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\yj86kat5ru4v3qtvudmb	unknown	16384	56 47 24 10 cb 2e 80 28 10 59 be a6 65 81 43 bc 36 4a 9c 1c c3 b1 ac d9 a5 0c 02 ac 11 51 e1 e4 3d a9 34 32 04 b5 28 8e ff 7c 20 3e de 60 34 0c a2 8e 64 1d 1a f7 f5 bb de 53 2b 76 bd 5f ef b7 22 a2 83 b8 a2 94 9f 6f 2e 2f 65 9e 53 a5 18 93 e2 a8 f9 eb 79 37 9b 8d d1 14 4a 14 59 e7 6e 33 ef 3f 9b ba 68 75 09 d5 6e de 47 42 33 c3 b0 35 59 4e 44 8a d7 a7 08 31 d3 a6 5a 11 b5 70 97 68 35 ee 35 a2 9c b0 6f 72 dd 22 52 ff 98 3a b4 3b 94 6f 1e 2d ea 9c 26 35 e0 57 82 a6 16 56 47 f8 79 58 1e 2b be 50 4d 8c 94 eb 4a 89 9e fc de 42 cd c7 cb 1c 52 c0 62 bf a7 b3 c7 bf 48 3f 96 6c 0a 10 8f 86 8a 99 dd 7b ac 0a 1f cb f8 86 af 4e 2a e4 76 f5 82 e9 f1 fa 15 20 92 eb b7 af e0 94 9a 6f 3a c8 e6 1b 85 80 a2 df ec eb f9 71 72 d5 d6 cb 79 bd a4 d6 f8 70 7e 1e ac a5 e6 ad 79	VG$....(.Y..e.C.6J...........Q ..=.42..(..| >.`4...d......S+v ._..".......o./e.S.......y7.... J.Y.n3.?..hu..n.GB3..5YND ....1 ..Z..p.h5.5...or."R..:.;.o.-.. &5.W...VG.yX.+.PM...J....B ....R.b.....H?.I.......{.......N*. v...... ....o:..........qr. ..y....p~.....y	success or wait	13	4060FE	WriteFile
C:\Users\user\AppData\Local\Temp\nsiFB00.tmp\qm1tw12xr.dll	unknown	4608	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 80 d2 9b 60 00 00 00 00 00 00 00 00 e0 00 03 21 0b 01 0b 00 00 04 00 00 00 0a 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $............................ ....PE..L......`...........!	success or wait	1	4060FE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	259286	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 ad 31 08 81 e9 50 66 d2 e9 50 66 d2 e9 50 66 d2 2a 5f 39 d2 eb 50 66 d2 e9 50 67 d2 4c 50 66 d2 2a 5f 3b d2 e6 50 66 d2 bd 73 56 d2 e3 50 66 d2 2e 56 60 d2 e8 50 66 d2 52 69 63 68 e9 50 66 d2 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 50 45 00 00 4c 01 05 00 02 d7 24 5f 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 66 00 00 00 2a 02 00 00 08 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........1...Pf..Pf..Pf.*_9..P f..Pg.LPf.*_;..Pf..sV..Pf..V`. .Pf.Rich.Pf.................. ......PE..L.....$_........... .....f...*.....	invalid handle	1	3051BC1	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PAYMENT SLIP.exe	unknown	512	success or wait	81	4060CF	ReadFile
C:\Users\user\Desktop\PAYMENT SLIP.exe	unknown	16384	success or wait	14	4060CF	ReadFile
C:\Users\user\AppData\Local\Temp\nsnFAD0.tmp	unknown	4	success or wait	1	4060CF	ReadFile
C:\Users\user\AppData\Local\Temp\nsnFAD0.tmp	unknown	4858	success or wait	1	4033F7	ReadFile
C:\Users\user\AppData\Local\Temp\nsnFAD0.tmp	unknown	4	success or wait	3	4060CF	ReadFile
C:\Users\user\AppData\Local\Temp\p7nih0ok4yeyw5j9l	unknown	9733	success or wait	1	100010CB	ReadFile
C:\Users\user\Desktop\PAYMENT SLIP.exe	unknown	259286	success or wait	1	3051B82	ReadFile
C:\Users\user\AppData\Local\Temp\yj86kat5ru4v3qtvudmb	unknown	207872	success or wait	1	30519C2	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	3050AA8	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	3050AA8	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	3050AA8	ReadFile

Analysis Process: MSBuild.exe PID: 4228 Parent PID: 7116

General

Start time:	15:41:20
Start date:	12/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\PAYMENT SLIP.exe'
Imagebase:	0x1f0000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: hmhrpib.exe PID: 6024 Parent PID: 3424

General

Start time:	15:41:21
Start date:	12/05/2021
Path:	C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe'
Imagebase:	0x400000
File size:	259286 bytes
MD5 hash:	50C9D58F61950484825D85A9A1372A7D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.706739434.0000000002F30000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.706739434.0000000002F30000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.706739434.0000000002F30000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.706739434.0000000002F30000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 43%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsq1C22.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4060A0	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsq1C23.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4060A0	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	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	405AFC	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsb1C63.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4060A0	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	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	405AFC	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsb1C63.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405ABC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsb1C63.tmp\qm1tw12xr.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40605E	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsq1C22.tmp	success or wait	1	403887	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsb1C63.tmp	success or wait	1	405C7D	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\nsq1C23.tmp	unknown	20692	fa 12 00 00 80 00 00 00 2c 01 00 00 02 00 00 00 ac 01 00 00 01 00 00 00 c4 09 00 00 18 00 00 00 64 0c 00 00 00 00 00 00 34 12 00 00 01 00 00 00 fa 12 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 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 ff 00 00 c6 00 00 00 f1 ff ff ff 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 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 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 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 00 00 00 00 00 00 00 00	........,...................... ..d.......4..................	success or wait	14	4060FE	WriteFile
C:\Users\user\AppData\Local\Temp\p7nih0ok4yeyw5j9l	unknown	9733	29 e7 f8 b4 b7 80 c7 88 f0 20 0e bc bc 17 3d f1 e0 96 41 eb 2a d3 c2 98 c7 f6 b9 d5 c4 69 74 45 20 65 4a 79 4f 79 fa f5 ab c0 31 05 f4 71 9f 6e 80 2a b0 c4 8c b4 75 1d 9b 3d 21 7b 7e 9c 9a 0f db e9 5a 23 9a 88 52 d8 85 88 ab 17 7b b1 18 55 70 91 a3 a6 f9 35 34 6f c6 93 fe 8c b1 b4 b7 c3 1d 1e 24 81 bc c6 2f 32 65 81 f7 3c f3 5f 6a c0 dd e0 83 30 fb 4a 31 6d 88 7a 3b 3e 91 4e 1d c7 1f eb 96 74 08 0b 0e 5c 65 76 fc 1a 15 ae 46 49 bc d9 13 d3 0a 78 c3 a8 74 37 1a 88 18 a2 89 c6 21 62 13 16 e9 e5 e5 e0 b7 84 ee 5b 21 24 27 b4 a1 0e 15 31 2c 55 9e a1 54 f2 67 ac 63 50 5b 8f cc cf f2 20 91 ba 21 5e f9 49 ea 2d 00 be d1 38 cf dc 07 44 78 7b 7e cc d5 65 ed 8a 85 7e 36 39 ac 4a db 83 fb e8 b3 77 e4 e7 ca 77 01 11 78 b6 11 32 02 05 58 95 b0 cf 26 f4 5f 2b 10 13 16	)........ ....=...A.*........itE eJyOy....1..q.n.*....u..=!{ ~.....Z#..R.....{..Up....54o.. ....$.../2e..<._j....0.J1m .z;>.N.....t...\ev....FI.....x ..t7......!b.........[!$'....1 ,U..T.g.cP[.... ..!^.I.-...8.. .Dx{~..e...~69.J.....w...w..x. .2..X...&._+...	success or wait	1	4060FE	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\yj86kat5ru4v3qtvudmb</td><td>unknown</td><td>16384</td><td>56 47 24 10 cb 2e 80 28 10 59 be a6 65 81 43 bc 36 4a 9c 1c c3 b1 ac d9 a5 0c 02 ac 11 51 e1 e4 3d a9 34 32 04 b5 28 8e ff 7c 20 3e de 60 34 0c a2 8e 64 1d 1a f7 f5 bb de 53 2b 76 bd 5f ef b7 22 a2 83 b8 a2 94 9f 6f 2e 2f 65 9e 53 a5 18 93 e2 a8 f9 eb 79 37 9b 8d d1 14 4a 14 59 e7 6e 33 ef 3f 9b ba 68 75 09 d5 6e de 47 42 33 c3 b0 35 59 4e 44 8a d7 a7 08 31 d3 a6 5a 11 b5 70 97 68 35 ee 35 a2 9c b0 6f 72 dd 22 52 ff 98 3a b4 3b 94 6f 1e 2d ea 9c 26 35 e0 57 82 a6 16 56 47 f8 79 58 1e 2b be 50 4d 8c 94 eb 4a 89 9e fc de 42 cd c7 cb 1c 52 c0 62 bf a7 b3 c7 bf 48 3f 96 6c 0a 10 8f 86 8a 99 dd 7b ac 0a 1f cb f8 86 af 4e 2a e4 76 f5 82 e9 f1 fa 15 20 92 eb b7 af e0 94 9a 6f 3a c8 e6 1b 85 80 a2 df ec eb f9 71 72 d5 d6 cb 79 bd a4 d6 f8 70 7e 1e ac a5 e6 ad 79</td><td>VG$....(.Y..e.C.6J...........Q ..=.42..(..| >.`4...d......S+v ._..".......o./e.S.......y7.... J.Y.n3.?..hu..n.GB3..5YND ....1 ..Z..p.h5.5...or."R..:.;.o.-.. &5.W...VG.yX.+.PM...J....B ....R.b.....H?.I.......{.......N*. v...... ....o:..........qr. ..y....p~.....y</td><td>success or wait</td><td>13</td><td>4060FE</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\nsb1C63.tmp\qm1tw12xr.dll</td><td>unknown</td><td>4608</td><td>4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 80 d2 9b 60 00 00 00 00 00 00 00 00 e0 00 03 21 0b 01 0b 00 00 04 00 00 00 0a 00 00 00 00 00</td><td>MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $............................ ....PE..L......`...........! ....</td><td>success or wait</td><td>1</td><td>4060FE</td><td>WriteFile</td></tr>
</table>

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe	unknown	512	success or wait	81	4060CF	ReadFile
C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe	unknown	16384	success or wait	14	4060CF	ReadFile
C:\Users\user\AppData\Local\Temp\nsq1C23.tmp	unknown	4	success or wait	1	4060CF	ReadFile
C:\Users\user\AppData\Local\Temp\nsq1C23.tmp	unknown	4858	success or wait	1	4033F7	ReadFile
C:\Users\user\AppData\Local\Temp\nsq1C23.tmp	unknown	4	success or wait	3	4060CF	ReadFile
C:\Users\user\AppData\Local\Temp\p7nih0ok4yeyw5j9l	unknown	9733	success or wait	1	100010CB	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\yj86kat5ru4v3qtvudmb	unknown	207872	success or wait	1	2F119C2	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2F10AA8	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2F10AA8	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2F10AA8	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2F10AA8	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2F10AA8	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2F10AA8	ReadFile

Analysis Process: PAYMENT SLIP.exe PID: 5704 Parent PID: 7116

General

Start time:	15:41:26
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\PAYMENT SLIP.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PAYMENT SLIP.exe'
Imagebase:	0x400000
File size:	259286 bytes
MD5 hash:	50C9D58F61950484825D85A9A1372A7D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.723894048.00000000024E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.723894048.00000000024E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.723894048.00000000024E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.723894048.00000000024E0000.00000004.00000001.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\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsi2D2A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4060A0	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsd2D5A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4060A0	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	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	405AFC	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsy2D8A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4060A0	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	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	405AFC	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsy2D8A.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405ABC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsy2D8A.tmp\qm1tw12xr.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40605E	CreateFileW
C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	1	23A1BAC	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsi2D2A.tmp	success or wait	1	403887	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsy2D8A.tmp	success or wait	1	405C7D	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\nsd2D5A.tmp	unknown	20692	fa 12 00 00 80 00 00 00 2c 01 00 00 02 00 00 00 ac 01 00 00 01 00 00 00 c4 09 00 00 18 00 00 00 64 0c 00 00 00 00 00 00 34 12 00 00 01 00 00 00 fa 12 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 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 ff 00 00 c6 00 00 00 f1 ff ff ff 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 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 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 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	.......,...................... ..d.......4...................	success or wait	14	4060FE	WriteFile
C:\Users\user\AppData\Local\Temp\p7nih0ok4yeyw5j9l	unknown	9733	29 e7 f8 b4 b7 80 c7 88 f0 20 0e bc bc 17 3d f1 e0 96 41 eb 2a d3 c2 98 c7 f6 b9 d5 c4 69 74 45 20 65 4a 79 4f 79 fa f5 ab c0 31 05 f4 71 9f 6e 80 2a b0 c4 8c b4 75 1d 9b 3d 21 7b 7e 9c 9a 0f db e9 5a 23 9a 88 52 d8 85 88 ab 17 7b b1 18 55 70 91 a3 a6 f9 35 34 6f c6 93 fe 8c b1 b4 b7 c3 1d 1e 24 81 bc c6 2f 32 65 81 f7 3c f3 5f 6a c0 dd e0 83 30 fb 4a 31 6d 88 7a 3b 3e 91 4e 1d c7 1f eb 96 74 08 0b 0e 5c 65 76 fc 1a 15 ae 46 49 bc d9 13 d3 0a 78 c3 a8 74 37 1a 88 18 a2 89 c6 21 62 13 16 e9 e5 e5 e0 b7 84 ee 5b 21 24 27 b4 a1 0e 15 31 2c 55 9e a1 54 f2 67 ac 63 50 5b 8f cc cf f2 20 91 ba 21 5e f9 49 ea 2d 00 be d1 38 cf dc 07 44 78 7b 7e cc d5 65 ed 8a 85 7e 36 39 ac 4a db 83 fb e8 b3 77 e4 e7 ca 77 01 11 78 b6 11 32 02 05 58 95 b0 cf 26 f4 5f 2b 10 13 16	)........ ....=...A.*........itE eJyOy....1..q.n.*....u..=!{ ~.....Z#..R.....{..Up....54o.. ....$.../2e..<._j....0.J1m .z;>.N.....t...\ev....FI.....x ..t7......!b.........[!$'....1 ,U..T.g.cP[.... ..!^.I.-...8.. .Dx{~..e...~69.J.....w...w..x. .2..X...&._+...	success or wait	1	4060FE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\yj86kat5ru4v3qtvudmb	unknown	16384	56 47 24 10 cb 2e 80 28 10 59 be a6 65 81 43 bc 36 4a 9c 1c c3 b1 ac d9 a5 0c 02 ac 11 51 e1 e4 3d a9 34 32 04 b5 28 8e ff 7c 20 3e de 60 34 0c a2 8e 64 1d 1a f7 f5 bb de 53 2b 76 bd 5f ef b7 22 a2 83 b8 a2 94 9f 6f 2e 2f 65 9e 53 a5 18 93 e2 a8 f9 eb 79 37 9b 8d d1 14 4a 14 59 e7 6e 33 ef 3f 9b ba 68 75 09 d5 6e de 47 42 33 c3 b0 35 59 4e 44 8a d7 a7 08 31 d3 a6 5a 11 b5 70 97 68 35 ee 35 a2 9c b0 6f 72 dd 22 52 ff 98 3a b4 3b 94 6f 1e 2d ea 9c 26 35 e0 57 82 a6 16 56 47 f8 79 58 1e 2b be 50 4d 8c 94 eb 4a 89 9e fc de 42 cd c7 cb 1c 52 c0 62 bf a7 b3 c7 bf 48 3f 96 6c 0a 10 8f 86 8a 99 dd 7b ac 0a 1f cb f8 86 af 4e 2a e4 76 f5 82 e9 f1 fa 15 20 92 eb b7 af e0 94 9a 6f 3a c8 e6 1b 85 80 a2 df ec eb f9 71 72 d5 d6 cb 79 bd a4 d6 f8 70 7e 1e ac a5 e6 ad 79	VG$....(.Y..e.C.6J...........Q ..=.42..(..| >.`4...d......S+v ._..''......o./e.S.......y7.... J.Y.n3.?..hu..n.GB3..5YND ....1 ..Z..p.h5.5...or."R..:.;.o.-.. &5.W...VG.yX.+.PM...J....B ....R.b.....H?.l.......{.......N*. v...... ....o:..........qr. ..y....p~.....y	success or wait	13	4060FE	WriteFile
C:\Users\user\AppData\Local\Temp\nsy2D8A.tmp\qm1tw12xr.dll	unknown	4608	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 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 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 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 50 45 00 00 4c 01 03 00 80 d2 9b 60 00 00 00 00 00 00 00 00 e0 00 03 21 0b 01 0b 00 00 04 00 00 00 0a 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.............................. ....PE..L......`...........!	success or wait	1	4060FE	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	259286	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 ad 31 08 81 e9 50 66 d2 e9 50 66 d2 e9 50 66 d2 2a 5f 39 d2 eb 50 66 d2 e9 50 67 d2 4c 50 66 d2 2a 5f 3b d2 e6 50 66 d2 bd 73 56 d2 e3 50 66 d2 2e 56 60 d2 e8 50 66 d2 52 69 63 68 e9 50 66 d2 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 50 45 00 00 4c 01 05 00 02 d7 24 5f 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 66 00 00 00 2a 02 00 00 08 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........1...Pf..Pf..Pf.*_9..P f..Pg.LPf.*_;..Pf..sV..Pf..V`. .Pf.Rich.Pf.................. ......PE..L.....$_........... .....f...*.....	invalid handle	1	23A1BC1	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PAYMENT SLIP.exe	unknown	512	success or wait	81	4060CF	ReadFile
C:\Users\user\Desktop\PAYMENT SLIP.exe	unknown	16384	success or wait	14	4060CF	ReadFile
C:\Users\user\AppData\Local\Temp\nsd2D5A.tmp	unknown	4	success or wait	1	4060CF	ReadFile
C:\Users\user\AppData\Local\Temp\nsd2D5A.tmp	unknown	4858	success or wait	1	4033F7	ReadFile
C:\Users\user\AppData\Local\Temp\nsd2D5A.tmp	unknown	4	success or wait	3	4060CF	ReadFile
C:\Users\user\AppData\Local\Temp\p7nih0ok4yeyw5j9l	unknown	9733	success or wait	1	100010CB	ReadFile
C:\Users\user\Desktop\PAYMENT SLIP.exe	unknown	259286	success or wait	1	23A1B82	ReadFile
C:\Users\user\AppData\Local\Temp\yj86kat5ru4v3qtvudmb	unknown	207872	success or wait	1	23A19C2	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	23A0AA8	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	23A0AA8	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	23A0AA8	ReadFile

Analysis Process: MSBuild.exe PID: 6372 Parent PID: 6024

General

Start time:	15:41:28
Start date:	12/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe'
Imagebase:	0xec0000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.911350836.00000000044FF000.00000004.00000001.sdmp, Author: Joe Security

- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.910500149.0000000001830000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.910500149.0000000001830000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.909856080.0000000001450000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.909856080.0000000001450000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.910512551.0000000001840000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.910512551.0000000001840000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.909818098.0000000001420000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.909818098.0000000001420000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.910417181.00000000017D0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.910417181.00000000017D0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.914312313.00000000061A0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.914312313.00000000061A0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.914312313.00000000061A0000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.910472948.0000000001810000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.910472948.0000000001810000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.909835016.0000000001430000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.909835016.0000000001430000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.911646592.000000000485A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.910378079.00000000017A0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.910378079.00000000017A0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.910442224.00000000017F0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.910442224.00000000017F0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.910984817.00000000034F4000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.910406423.00000000017C0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.910406423.00000000017C0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.910536260.0000000001870000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.910536260.0000000001870000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.912631638.0000000005810000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.912631638.0000000005810000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.910428872.00000000017E0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source:

	0000000C.00000002.910428872.00000000017E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.909543177.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.909543177.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.909543177.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	moderate

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	722760AC	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	722760AC	unknown
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	57D07A1	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	57D089B	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp3E70.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	57D0B6C	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	57D089B	CreateFileW
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	57D07A1	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	57D07A1	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	722760AC	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	722760AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	7	57D089B	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp3E70.tmp	success or wait	1	14BBF0E	DeleteFileW

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	unknown	8	5c 4e f4 a6 4b 15 d9 48	\N..K..H	success or wait	1	57D0A53	WriteFile
C:\Users\user\AppData\Local\Temp\tmp3E70.tmp	unknown	1320	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	57D0A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	57	43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 5c 76 32 2e 30 2e 35 30 37 32 37 5c 4d 53 42 75 69 6c 64 2e 65 78 65	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe	success or wait	1	57D0A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc bb 8e f9 04 20 53 f0 bc 12 1c d2 7d 46 46 d4 32 d7 fe a4 68 e2 b4 4d 2b cf cc b9 c1 ec 4c bb 23 8c 58 cb ee 2b 8b b7 cd 01 a9 c0 2a c7 f9 1e d1 7e 66 1e 47 30 5e c3 a9 dd 96 3b b4 2e 95 a2 57 32 c2 3d 10 b3 ce 4b ca 7e c7 4c cc 9f 15 26 66 8d bb 2e 70 c8 04 1b f8 b7 c2 0f e9 ff e7 0b 10 3a 37 72 48 7d bd be f1 88 0d 2f 48 16 b2 87 06 17 96 4c 8c b6 04 3f b5 f3 04 41 08 4b 07 d1 e5 84 4a 17 3d 38 78 21 19 a1 e1 e4 2b fa 32 65 27 d7 1f 45 3f d9 47 11 9e a7 e7 a8 01 f0 5b 00 26	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i..... S.....}FF.2.. .h..M+.....L.#.X..+.....*.... ~f.G0^...;....W2.=...K.~.L... &f...p.....:7rH}...../H .....L...?...A.K....J.=8x!... .+.2e'..E?.G.....[.&	success or wait	8	57D0A53	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	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe	unknown	4096	success or wait	1	7234BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe	unknown	512	success or wait	1	7234BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	57D0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4096	success or wait	1	57D0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4096	end of file	1	57D0A53	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7234BF06	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7234BF06	unknown

Analysis Process: hmhrpib.exe PID: 6376 Parent PID: 3424

General

Start time:	15:41:30
Start date:	12/05/2021
Path:	C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe'
Imagebase:	0x400000
File size:	259286 bytes
MD5 hash:	50C9D58F61950484825D85A9A1372A7D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.732908055.0000000002F30000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.732908055.0000000002F30000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.732908055.0000000002F30000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.732908055.0000000002F30000.00000004.00000001.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\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsz3D47.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4060A0	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsz3D48.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4060A0	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	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	405AFC	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsj3D87.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4060A0	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	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	405AFC	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsj3D87.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405ABC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsj3D87.tmp\qm1tw12xr.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40605E	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsz3D47.tmp	success or wait	1	403887	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsj3D87.tmp	success or wait	1	405C7D	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsz3D48.tmp	unknown	20692	fa 12 00 00 80 00 00 00 2c 01 00 00 02 00 00 00 ac 01 00 00 01 00 00 00 c4 09 00 00 18 00 00 00 64 0c 00 00 00 00 00 00 34 12 00 00 01 00 00 00 fa 12 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 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 ff 00 00 c6 00 00 00 f1 ff ff 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 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 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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	........,..................... ..d.......4..................	success or wait	14	4060FE	WriteFile
C:\Users\user\AppData\Local\Temp\p7nih0ok4yeyw5j9l	unknown	9733	29 e7 f8 b4 b7 80 c7 88 f0 20 0e bc bc 17 3d f1 e0 96 41 eb 2a d3 c2 98 c7 f6 b9 d5 c4 69 74 45 20 65 4a 79 4f 79 fa f5 ab c0 31 05 f4 71 9f 6e 80 2a b0 c4 8c b4 75 1d 9b 3d 21 7b 7e 9c 9a 0f db e9 5a 23 9a 88 52 d8 85 88 ab 17 7b b1 18 55 70 91 a3 a6 f9 35 34 6f c6 93 fe 8c b1 b4 b7 c3 1d 1e 24 81 bc c6 2f 32 65 81 f7 3c f3 5f 6a c0 dd e0 83 30 fb 4a 31 6d 88 7a 3b 3e 91 4e 1d c7 1f eb 96 74 08 0b 0e 5c 65 76 fc 1a 15 ae 46 49 bc d9 13 d3 0a 78 c3 a8 74 37 1a 88 18 a2 89 c6 21 62 13 16 e9 e5 e5 e0 b7 84 ee 5b 21 24 27 b4 a1 0e 15 31 2c 55 9e a1 54 f2 67 ac 63 50 5b 8f cc cf f2 20 91 ba 21 5e f9 49 ea 2d 00 be d1 38 cf dc 07 44 78 7b 7e cc d5 65 ed 8a 85 7e 36 39 ac 4a db 83 fb e8 b3 77 e4 e7 ca 77 01 11 78 b6 11 32 02 05 58 95 b0 cf 26 f4 5f 2b 10 13 16	)........ ....=...A.*........itE eJyOy....1..q.n.*....u..=!{ ~.....Z#..R.....{..Up....54o.. ....$.../2e..<._j....0.J1m .z;>.N.....t...\ev....FI.....x ..t7......!b.........[!$'....1 ,U..T.g.cP[.... ..!^.I.-...8.. .Dx{~..e...~69.J.....w...w..x. .2..X...&._+...	success or wait	1	4060FE	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\yj86kat5ru4v3qtvudmb</td><td>unknown</td><td>16384</td><td>56 47 24 10 cb 2e 80
28 10 59 be a6 65 81
43 bc 36 4a 9c 1c c3
b1 ac d9 a5 0c 02 ac
11 51 e1 e4 3d a9 34
32 04 b5 28 8e ff 7c 20
3e de 60 34 0c a2 8e
64 1d 1a f7 f5 bb de 53
2b 76 bd 5f ef b7 22 a2
83 b8 a2 94 9f 6f 2e 2f
65 9e 53 a5 18 93 e2
a8 f9 eb 79 37 9b 8d
d1 14 4a 14 59 e7 6e
33 ef 3f 9b ba 68 75 09
d5 6e de 47 42 33 c3
b0 35 59 4e 44 8a d7
a7 08 31 d3 a6 5a 11
b5 70 97 68 35 ee 35
a2 9c b0 6f 72 dd 22
52 ff 98 3a b4 3b 94 6f
1e 2d ea 9c 26 35 e0
57 82 a6 16 56 47 f8
79 58 1e 2b be 50 4d
8c 94 eb 4a 89 9e fc
de 42 cd c7 cb 1c 52
c0 62 bf a7 b3 c7 bf 48
3f 96 6c 0a 10 8f 86 8a
99 dd 7b ac 0a 1f cb f8
86 af 4e 2a e4 76 f5 82
e9 f1 fa 15 20 92 eb b7
af e0 94 9a 6f 3a c8 e6
1b 85 80 a2 df ec eb f9
71 72 d5 d6 cb 79 bd
a4 d6 f8 70 7e 1e ac
a5 e6 ad 79</td><td>VG$....(.Y..e.C.6J..........Q
..=.42..(..| >.`4...d......S+v
._..".......o./e.S.......y7....
J.Y.n3.?..hu..n.GB3..5YND
....1
..Z..p.h5.5...or."R..:.;.o.-..
&5.W...VG.yX.+.PM...J....B
....R.b.....H?.I.......{.......N*.
v...... ....o:..........qr.
..y....p~.....y</td><td>success or wait</td><td>13</td><td>4060FE</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\nsj3D87.tmp\qm1tw12xr.dll</td><td>unknown</td><td>4608</td><td>4d 5a 90 00 03 00 00
00 04 00 00 00 ff ff 00
00 b8 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 d8 00 00 00
0e 1f ba 0e 00 b4 09
cd 21 b8 01 4c cd 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
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
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
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 50 45 00
00 4c 01 03 00 80 d2
9b 60 00 00 00 00 00
00 00 00 e0 00 03 21
0b 01 0b 00 00 04 00
00 00 0a 00 00 00 00
00</td><td>MZ......................@.....
....
............!..L.!This program
cannot be run in DOS
mode....
$............................
....
....
......PE..L......`...........!
..............</td><td>success or wait</td><td>1</td><td>4060FE</td><td>WriteFile</td></tr>
</table>

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe	unknown	512	success or wait	81	4060CF	ReadFile
C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe	unknown	16384	success or wait	14	4060CF	ReadFile
C:\Users\user\AppData\Local\Temp\nsz3D48.tmp	unknown	4	success or wait	1	4060CF	ReadFile
C:\Users\user\AppData\Local\Temp\nsz3D48.tmp	unknown	4858	success or wait	1	4033F7	ReadFile
C:\Users\user\AppData\Local\Temp\nsz3D48.tmp	unknown	4	success or wait	3	4060CF	ReadFile
C:\Users\user\AppData\Local\Temp\p7nih0ok4yeyw5j9l	unknown	9733	success or wait	1	100010CB	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\yj86kat5ru4v3qtvudmb	unknown	207872	success or wait	1	2F119C2	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2F10AA8	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2F10AA8	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2F10AA8	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2F10AA8	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2F10AA8	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2F10AA8	ReadFile

Analysis Process: schtasks.exe PID: 6508 Parent PID: 6372

General

Start time:	15:41:31
Start date:	12/05/2021
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\tmp3E70.tmp'
Imagebase:	0x1390000
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\tmp3E70.tmp	unknown	2	success or wait	1	139AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp3E70.tmp	unknown	1321	success or wait	1	139ABD9	ReadFile

Analysis Process: conhost.exe PID: 6608 Parent PID: 6508

General

Start time:	15:41:32
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: MSBuild.exe PID: 6504 Parent PID: 5704

General

Start time:	15:41:32
Start date:	12/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\PAYMENT SLIP.exe'
Imagebase:	0x120000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: MSBuild.exe PID: 6800 Parent PID: 968

General

Start time:	15:41:34
Start date:	12/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe 0
Imagebase:	0x870000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

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	722760AC	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	722760AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\MSBuild.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	722634A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	E5A7A3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	169	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 42 75 69 6c 64 20 45 6e 67 69 6e 65 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 0d 0a 5b 4d 69 63 72 6f 73 6f 66 74 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 2c 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 5d 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 20 32 30 30 35 2e 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) Build Engine Version 2.0.50727.8922.. [Microsoft .NET Framework, Version 2.0. 50727.8922]..Copyright (C) Microsoft Corporation 2005. All rights reserved.....	success or wait	1	E5A7A3	WriteFile
\Device\ConDrv	unknown	66	4d 53 42 55 49 4c 44 20 3a 20 65 72 72 6f 72 20 4d 53 42 31 30 30 39 3a 20 50 72 6f 6a 65 63 74 20 66 69 6c 65 20 64 6f 65 73 20 6e 6f 74 20 65 78 69 73 74 2e 0d 0a 53 77 69 74 63 68 3a 20 30 0d 0a	MSBUILD : error MSB1009: Project file does not exist...Switch: 0..	success or wait	1	E5A7A3	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\MSBuild.exe.log	unknown	325	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 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 42 75 69 6c 64 2e 45 6e 67 69 6e 65 2c 20 56 65 72 73 69 6f 6e 3d 32 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 42 75 69 6c 64 2e 46 72 61 6d 65 77 6f 72 6b 2c 20	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..2,"Microsoft.Build.Engine, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.Build.Framework,	success or wait	1	7254A33A	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	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	722A8738	ReadFile

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	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.rsp	unknown	4096	success or wait	1	E5A7A3	ReadFile

Analysis Process: conhost.exe PID: 6876 Parent PID: 6800

General

Start time:	15:41:35
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: MSBuild.exe PID: 6940 Parent PID: 6376

General

Start time:	15:41:37
Start date:	12/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe'
Imagebase:	0xa30000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.745550001.00000000040B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.745550001.00000000040B1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.745514113.00000000030B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.745514113.00000000030B1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.744233608.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.744233608.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.744233608.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	moderate

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	722760AC	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	722760AC	unknown

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	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile

Analysis Process: PAYMENT SLIP.exe PID: 6900 Parent PID: 5704

General

Start time:	15:41:38
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\PAYMENT SLIP.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PAYMENT SLIP.exe'
Imagebase:	0x400000
File size:	259286 bytes
MD5 hash:	50C9D58F61950484825D85A9A1372A7D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.745571478.0000000003050000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000014.00000002.745571478.0000000003050000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.745571478.0000000003050000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.745571478.0000000003050000.00000004.00000001.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\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsy6272.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4060A0	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsj62B2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4060A0	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	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	405AFC	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsz6311.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4060A0	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	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	405AFC	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AFC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsz6311.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405ABC	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsz6311.tmp\qm1tw12xr.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	40605E	CreateFileW
C:\Users\user\AppData\Roaming\tteegmiuoefs\hmhrpib.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	1	22B1BAC	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsy6272.tmp	success or wait	1	403887	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsz6311.tmp	success or wait	1	405C7D	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsj62B2.tmp	unknown	20692	fa 12 00 00 80 00 00 00 2c 01 00 00 02 00 00 00 ac 01 00 00 01 00 00 00 c4 09 00 00 18 00 00 00 64 0c 00 00 00 00 00 00 34 12 00 00 01 00 00 00 fa 12 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 ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 ff 00 00 c6 00 00 00 f1 ff ff ff 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 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 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 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	.......,..................... ..d.......4..................	success or wait	14	4060FE	WriteFile
C:\Users\user\AppData\Local\Temp\p7nih0ok4yeyw5j9l	unknown	9733	29 e7 f8 b4 b7 80 c7 88 f0 20 0e bc bc 17 3d f1 e0 96 41 eb 2a d3 c2 98 c7 f6 b9 d5 c4 69 74 45 20 65 4a 79 4f 79 fa f5 ab c0 31 05 f4 71 9f 6e 80 2a b0 c4 8c b4 75 1d 9b 3d 21 7b 7e 9c 9a 0f db e9 5a 23 9a 88 52 d8 85 88 ab 17 7b b1 18 55 70 91 a3 a6 f9 35 34 6f c6 93 fe 8c b1 b4 b7 c3 1d 1e 24 81 bc c6 2f 32 65 81 f7 3c f3 5f 6a c0 dd e0 83 30 fb 4a 31 6d 88 7a 3b 3e 91 4e 1d c7 1f eb 96 74 08 0b 0e 5c 65 76 fc 1a 15 ae 46 49 bc d9 13 d3 0a 78 c3 a8 74 37 1a 88 18 a2 89 c6 21 62 13 16 e9 e5 e5 e0 b7 84 ee 5b 21 24 27 b4 a1 0e 15 31 2c 55 9e a1 54 f2 67 ac 63 50 5b 8f cc cf f2 20 91 ba 21 5e f9 49 ea 2d 00 be d1 38 cf dc 07 44 78 7b 7e cc d5 65 ed 8a 85 7e 36 39 ac 4a db 83 fb e8 b3 77 e4 e7 ca 77 01 11 78 b6 11 32 02 05 58 95 b0 cf 26 f4 5f 2b 10 13 16	)........ ....=...A.*........itE eJyOy....1..q.n.*....u..=!{ ~.....Z#..R.....{..Up....54o.. ....$.../2e..<._j....0.J1m .z;>.N.....t...\ev....FI.....x ..t7......!b.........[!$'....1 ,U..T.g.cP[.... ..!^.I.-...8.. .Dx{~..e...~69.J.....w...w..x. .2..X...&._+...	success or wait	1	4060FE	WriteFile

<table>
<thead>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
</thead>
<tbody>
<tr><td>C:\Users\user\AppData\Local\Temp\yj86kat5ru4v3qtvudmb</td><td>unknown</td><td>16384</td><td>56 47 24 10 cb 2e 80 28 10 59 be a6 65 81 43 bc 36 4a 9c 1c c3 b1 ac d9 a5 0c 02 ac 11 51 e1 e4 3d a9 34 32 04 b5 28 8e ff 7c 20 3e de 60 34 0c a2 8e 64 1d 1a f7 f5 bb de 53 2b 76 bd 5f ef b7 22 a2 83 b8 a2 94 9f 6f 2e 2f 65 9e 53 a5 18 93 e2 a8 f9 eb 79 37 9b 8d d1 14 4a 14 59 e7 6e 33 ef 3f 9b ba 68 75 09 d5 6e de 47 42 33 c3 b0 35 59 4e 44 8a d7 a7 08 31 d3 a6 5a 11 b5 70 97 68 35 ee 35 a2 9c b0 6f 72 dd 22 52 ff 98 3a b4 3b 94 6f 1e 2d ea 9c 26 35 e0 57 82 a6 16 56 47 f8 79 58 1e 2b be 50 4d 8c 94 eb 4a 89 9e fc de 42 cd c7 cb 1c 52 c0 62 bf a7 b3 c7 bf 48 3f 96 6c 0a 10 8f 86 8a 99 dd 7b ac 0a 1f cb f8 86 af 4e 2a e4 76 f5 82 e9 f1 fa 15 20 92 eb b7 af e0 94 9a 6f 3a c8 e6 1b 85 80 a2 df ec eb f9 71 72 d5 d6 cb 79 bd a4 d6 f8 70 7e 1e ac a5 e6 ad 79</td><td>VG$....(.Y..e.C.6J...........Q
..=.42..(..| >.`4...d......S+v
._..".......o./e.S.......y7....
J.Y.n3.?..hu..n.GB3..5YND
....1
..Z..p.h5.5...or."R..:.;.o.-..
&5.W...VG.yX.+.PM...J....B
....R.b.....H?.l.......{.......N*.
v...... ....o:..........qr.
..y....p~.....y</td><td>success or wait</td><td>13</td><td>4060FE</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\nsz6311.tmp\qm1tw12xr.dll</td><td>unknown</td><td>4608</td><td>4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 80 d2 9b 60 00 00 00 00 00 00 00 00 e0 00 03 21 0b 01 0b 00 00 04 00 00 00 0a 00 00 00 00 00</td><td>MZ......................@.....
....
............!..L.!This program
cannot be run in DOS
mode....
$............................
....
....
......PE..L......`...........!
..............</td><td>success or wait</td><td>1</td><td>4060FE</td><td>WriteFile</td></tr>
</tbody>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	259286	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 ad 31 08 81 e9 50 66 d2 e9 50 66 d2 e9 50 66 d2 2a 5f 39 d2 eb 50 66 d2 e9 50 67 d2 4c 50 66 d2 2a 5f 3b d2 e6 50 66 d2 bd 73 56 d2 e3 50 66 d2 2e 56 60 d2 e8 50 66 d2 52 69 63 68 e9 50 66 d2 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 50 45 00 00 4c 01 05 00 02 d7 24 5f 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 66 00 00 00 2a 02 00 00 08 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........1...Pf..Pf..Pf.*_9..P f..Pg.LPf.*_;..Pf..sV..Pf..V`. .Pf.Rich.Pf.................. ......PE..L.....$_........... .....f...*.....	invalid handle	1	22B1BC1	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PAYMENT SLIP.exe	unknown	512	success or wait	81	4060CF	ReadFile
C:\Users\user\Desktop\PAYMENT SLIP.exe	unknown	16384	success or wait	14	4060CF	ReadFile
C:\Users\user\AppData\Local\Temp\nsj62B2.tmp	unknown	4	success or wait	1	4060CF	ReadFile
C:\Users\user\AppData\Local\Temp\nsj62B2.tmp	unknown	4858	success or wait	1	4033F7	ReadFile
C:\Users\user\AppData\Local\Temp\nsj62B2.tmp	unknown	4	success or wait	3	4060CF	ReadFile
C:\Users\user\AppData\Local\Temp\p7nih0ok4yeyw5j9l	unknown	9733	success or wait	1	100010CB	ReadFile
C:\Users\user\Desktop\PAYMENT SLIP.exe	unknown	259286	success or wait	1	22B1B82	ReadFile
C:\Users\user\AppData\Local\Temp\yj86kat5ru4v3qtvudmb	unknown	207872	success or wait	1	22B19C2	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	22B0AA8	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	22B0AA8	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	22B0AA8	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	22B0AA8	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	22B0AA8	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	22B0AA8	ReadFile

Analysis Process: MSBuild.exe PID: 6948 Parent PID: 6900

General

Start time:	15:41:46
Start date:	12/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PAYMENT SLIP.exe'
Imagebase:	0x910000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.762297835.0000000002F11000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.762297835.0000000002F11000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.762317389.0000000003F11000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.762317389.0000000003F11000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000002.753927401.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.753927401.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.753927401.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	moderate

Disassembly

Code Analysis