ID: 411850
Sample Name: PO #KV18RE001-A5491.exe
Cookbook: default.jbs
Time: 07:45:17
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

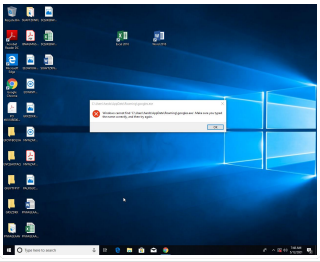
Analysis Report PO #KV18RE001-A5491.exe

Overview

General Information

Sample Name:	PO #KV18RE001-A5491.exe
Analysis ID:	411850
MD5:	9d9cb0f32a77d7d.
SHA1:	8386cdbc85faede..
SHA256:	0cbbdd2c9615f4d..
Tags:	exe NanoCore
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

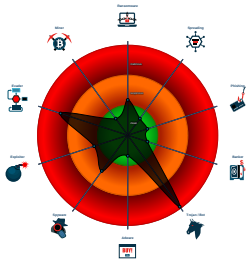
Nanocore AgentTesla

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

Signatures

- Antivirus detection for dropped file
- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected Nanocore RAT
- .NET source code contains very larg…
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…

Classification



Startup

- **System is w10x64**
- PO #KV18RE001-A5491.exe (PID: 5580 cmdline: 'C:\Users\user\Desktop\PO #KV18RE001-A5491.exe' MD5: 9D9CB0F32A77D7D81296095768D3583E)
  - cmd.exe (PID: 4064 cmdline: 'cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'googles' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\googles.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 3864 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - reg.exe (PID: 2416 cmdline: REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'googles' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\googles.exe' MD5: CEE2A7E57DF2A159A065A34913A055C2)
  - googles.exe (PID: 1196 cmdline: 'C:\Users\user\AppData\Roaming\googles.exe' MD5: 9D9CB0F32A77D7D81296095768D3583E)
- googles.exe (PID: 6120 cmdline: 'C:\Users\user\AppData\Roaming\googles.exe' MD5: 9D9CB0F32A77D7D81296095768D3583E)
  - ammero.exe (PID: 1784 cmdline: 'C:\Users\user\AppData\Roaming\ammero.exe' MD5: 605E939E44CD9B02C55CE0A09019AD47)
  - InstallUtil.exe (PID: 5476 cmdline: C:\Users\user\AppData\Local\Temp\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
    - schtasks.exe (PID: 3596 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp460B.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 1048 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5544 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp48BB.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 2428 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- InstallUtil.exe (PID: 632 cmdline: C:\Users\user\AppData\Local\Temp\InstallUtil.exe 0 MD5: EFEC8C379D165E3F33B536739AEE26A3)
  - conhost.exe (PID: 492 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 5268 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: EFEC8C379D165E3F33B536739AEE26A3)
  - conhost.exe (PID: 5284 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 5596 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: EFEC8C379D165E3F33B536739AEE26A3)
  - conhost.exe (PID: 5656 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "ed3103ae-73a9-4ea2-b0ca-9ce4d3e3",
  "Group": "POOKIE",
  "Domain1": "79.134.225.91",
  "Domain2": "",
  "Port": 4488,
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "aammorris@askoblue.comoffice12#smtp.privateemail.com"
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Roaming\ammero.exe	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
C:\Users\user\AppData\Roaming\ammero.exe	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.502894900.000000000447A000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1035f:$x1: NanoCore.ClientPluginHost • 0x793ed:$x1: NanoCore.ClientPluginHost • 0x1039c:$x2: IClientNetworkHost • 0x7942a:$x2: IClientNetworkHost • 0x13ecf:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x7cf5d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000007.00000002.502894900.000000000447A000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.502894900.000000000447A000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000007.00000002.502894900.000000000447A000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.502894900.000000000447A000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x100c7:$a: NanoCore • 0x100d7:$a: NanoCore • 0x1030b:$a: NanoCore • 0x1031f:$a: NanoCore • 0x1035f:$a: NanoCore • 0x79155:$a: NanoCore • 0x79165:$a: NanoCore • 0x79399:$a: NanoCore • 0x793ad:$a: NanoCore • 0x793ed:$a: NanoCore • 0x10126:$b: ClientPlugin • 0x10328:$b: ClientPlugin • 0x10368:$b: ClientPlugin • 0x791b4:$b: ClientPlugin • 0x793b6:$b: ClientPlugin • 0x793f6:$b: ClientPlugin • 0x1024d:$c: ProjectData • 0x62a87:$c: ProjectData • 0x792db:$c: ProjectData • 0xcbb06:$c: ProjectData • 0x10c54:$d: DESCrypto
Click to see the 44 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
17.2.InstallUtil.exe.371b78e.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0x145e3:$x1: NanoCore.ClientPluginHost • 0x2d5a7:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost • 0x14610:$x2: IClientNetworkHost • 0x2d5d4:$x2: IClientNetworkHost
17.2.InstallUtil.exe.371b78e.5.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x145e3:$x2: NanoCore.ClientPluginHost • 0x2d5a7:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0x156be:$s4: PipeCreated • 0x2e682:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost • 0x145fd:$s5: IClientLoggingHost • 0x2d5c1:$s5: IClientLoggingHost
17.2.InstallUtil.exe.371b78e.5.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
17.2.InstallUtil.exe.371b78e.5.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xddf:$a: NanoCore • 0xe38:$a: NanoCore • 0xe75:$a: NanoCore • 0xeee:$a: NanoCore • 0x14599:$a: NanoCore • 0x145ae:$a: NanoCore • 0x145e3:$a: NanoCore • 0x2d55d:$a: NanoCore • 0x2d572:$a: NanoCore • 0x2d5a7:$a: NanoCore • 0xe41:$b: ClientPlugin • 0xe7e:$b: ClientPlugin • 0x177c:$b: ClientPlugin • 0x1789:$b: ClientPlugin • 0x14355:$b: ClientPlugin • 0x14370:$b: ClientPlugin • 0x143a0:$b: ClientPlugin • 0x145b7:$b: ClientPlugin • 0x145ec:$b: ClientPlugin • 0x2d319:$b: ClientPlugin • 0x2d334:$b: ClientPlugin
7.2.googles.exe.447a1d2.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 137 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Direct Autorun Keys Modification

Sigma detected: Possible Applocker Bypass

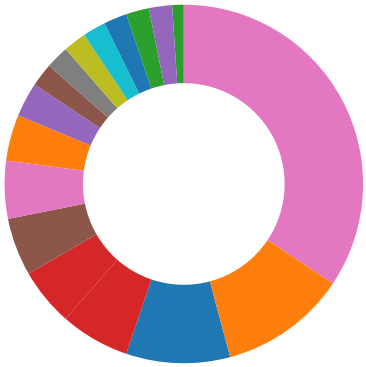
Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Signature Overview



- AV Detection
- Compliance
- 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:

Antivirus detection for dropped file

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

Yara detected AgentTesla

Yara detected AgentTesla

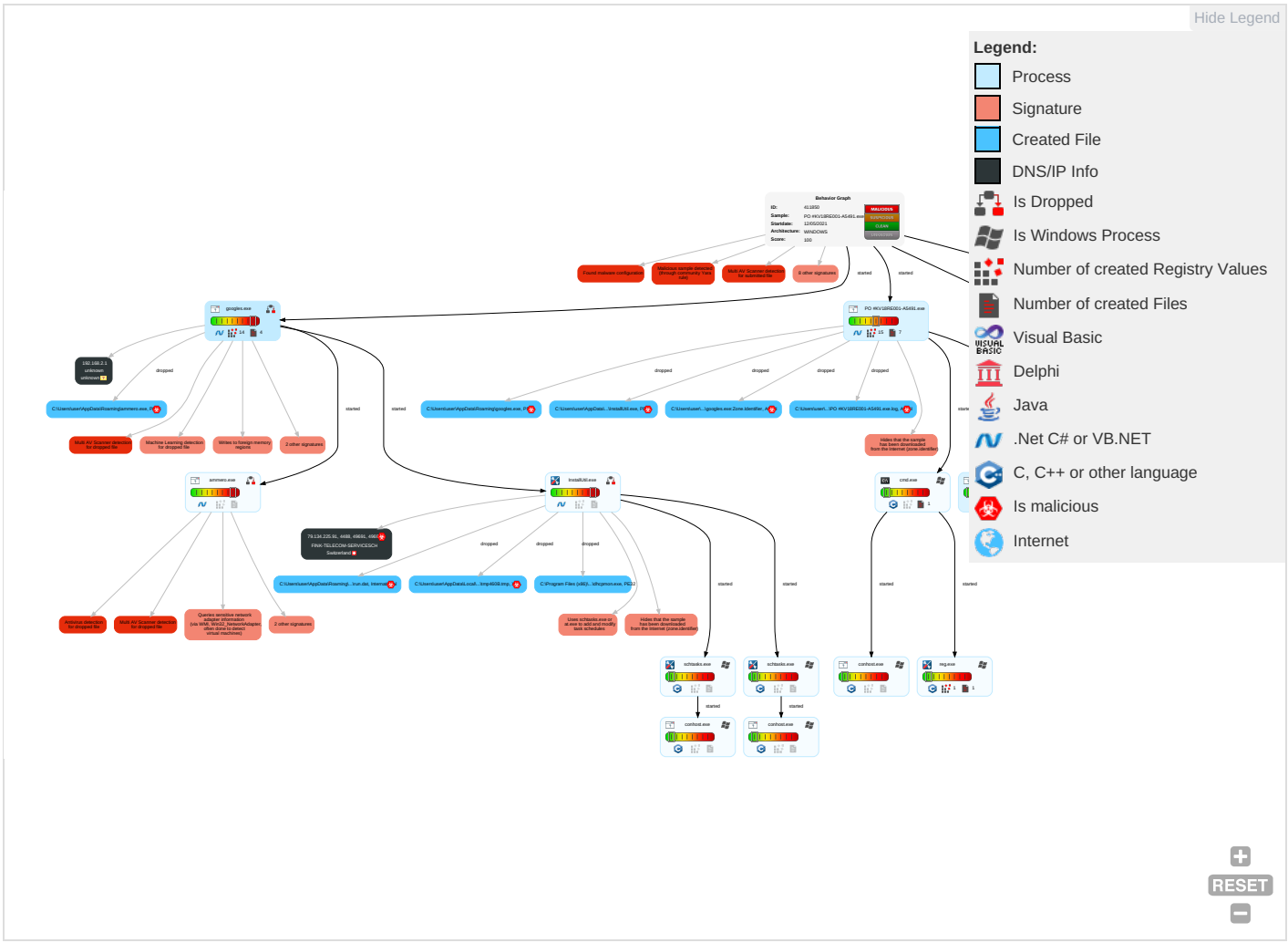
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts 1	Windows Management Instrumentation 2 1 1	Valid Accounts 1	Valid Accounts 1	Disable or Modify Tools 1	Input Capture 2 1	File and Directory Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium
Default Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Access Token Manipulation 1	Obfuscated Files or Information 2	LSASS Memory	System Information Discovery 1 1 3	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth
Domain Accounts	At (Linux)	Registry Run Keys / Startup Folder 1	Process Injection 3 1 2	Software Packing 1	Security Account Manager	Security Software Discovery 2 2 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Scheduled Task/Job 1	Masquerading 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Registry Run Keys / Startup Folder 1	Valid Accounts 1	LSA Secrets	Virtualization/Sandbox Evasion 1 4 1	SSH	Keylogging	Data Transfer Size Limits

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Modify Registry 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 1 4 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 3 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscate Non-C2 Protocol

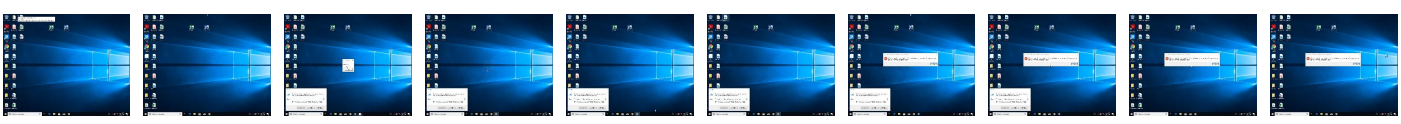
Behavior Graph

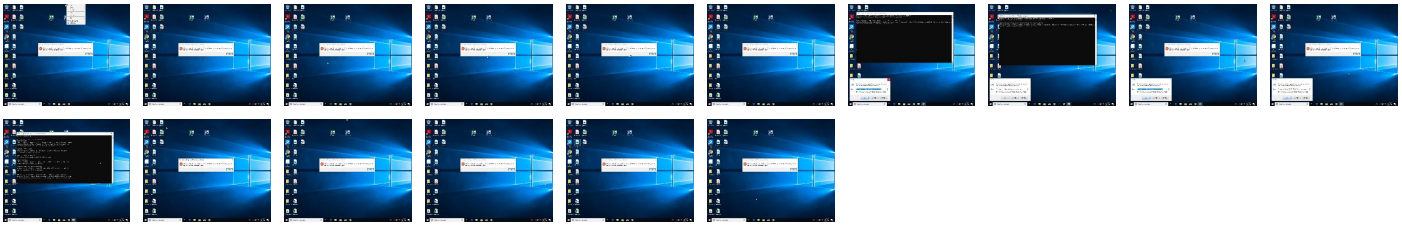


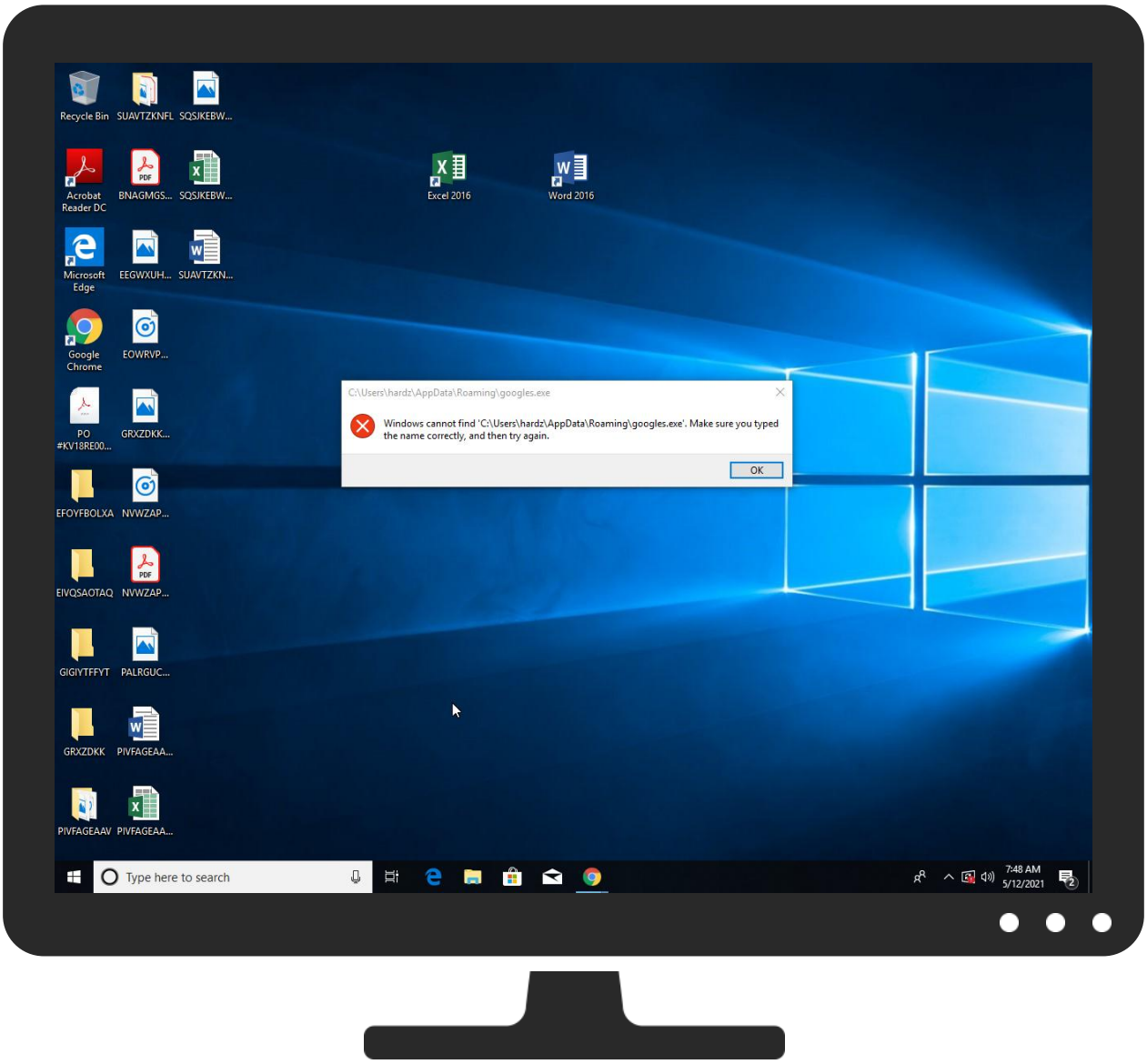
Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.







Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PO #KV18RE001-A5491.exe	33%	Virustotal		Browse
PO #KV18RE001-A5491.exe	26%	Metadefender		Browse
PO #KV18RE001-A5491.exe	38%	ReversingLabs	Win32.Trojan.Woreflint	
PO #KV18RE001-A5491.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\ammero.exe	100%	Avira	TR/Spy.Gen8	
C:\Users\user\AppData\Roaming\googles.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\ammero.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\ammero.exe	76%	ReversingLabs	ByteCode-MSIL.Infostealer.DarkStealer	
C:\Users\user\AppData\Roaming\googles.exe	26%	Metadefender		Browse
C:\Users\user\AppData\Roaming\googles.exe	38%	ReversingLabs	Win32.Trojan.Woreflint	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
16.2.ammero.exe.9e0000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
17.2.InstallUtil.exe.5dc0000.11.unpack	100%	Avira	TR/NanoCore.fadte		Download File
17.2.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.0.ammero.exe.9e0000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://ns.adobe.c/gj	0%	Avira URL Cloud	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://MFWCde.com	0%	Avira URL Cloud	safe	
http://ns.ado/1j	0%	Avira URL Cloud	safe	
http://ns.adobe.cobjj	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
79.134.225.91	0%	Avira URL Cloud	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://ns.ado/1	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

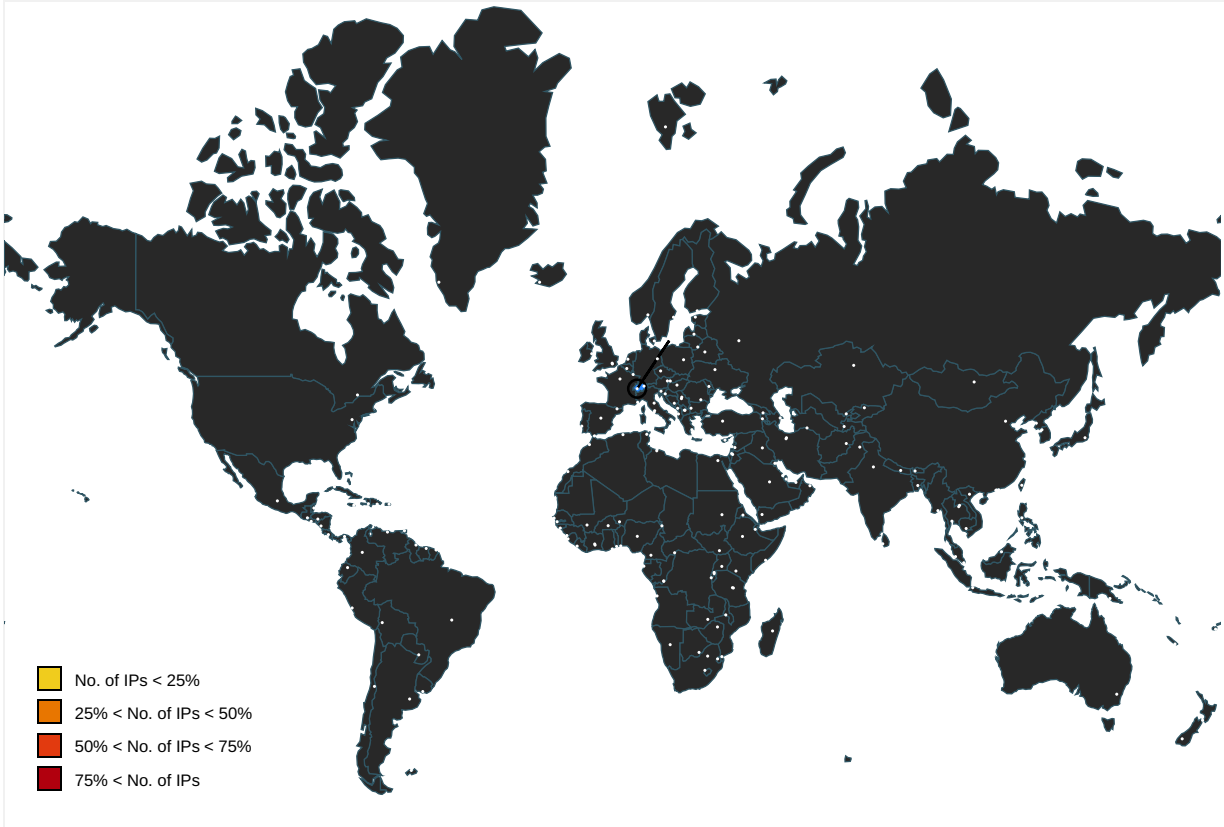
Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
79.134.225.91	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	ammero.exe, 00000010.00000002.489309809.0000000003011000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	ammero.exe, 00000010.00000002.489309809.0000000003011000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.c/gj	googles.exe, 00000007.00000003.296832321.00000000075FA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.adobe.cobj	PO #KV18RE001-A5491.exe, 00000000.00000003.232494092.00000000076DA000.00000004.00000001.sdmp, PO #KV18RE001-A5491.exe, 00000000.00000003.297857855.00000076E1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	ammero.exe, 00000010.00000002.489309809.0000000003011000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.goog/GTS1O1core.crl0	googles.exe, 00000007.00000002.488779548.00000000015C6000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	ammero.exe, 00000010.00000002.489309809.0000000003011000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://MFWCde.com	ammero.exe, 00000010.00000002.489309809.0000000003011000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.ado/1j	googles.exe, 00000007.00000003.296832321.00000000075FA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.adobe.cobjj	googles.exe, 00000007.00000003.296832321.00000000075FA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pki.goog/gsr2/GTS1O1.crt0	googles.exe, 00000007.00000002.488779548.00000000015C6000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.c/g	PO #KV18RE001-A5491.exe, 00000000.00000003.232494092.00000000076DA000.00000004.00000001.sdmp, PO #KV18RE001-A5491.exe, 00000000.00000003.297857855.00000076E1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.goog/gsr2/gsr2.crl0?	googles.exe, 00000007.00000002.489117933.0000000001603000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pki.goog/repository/0	googles.exe, 00000007.00000002.489117933.0000000001603000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	PO #KV18RE001-A5491.exe, 00000000.00000002.300286762.00000000033F1000.00000004.00000001.sdmp, googles.exe, 00000007.00000002.491630441.0000000003401000.00000004.00000001.sdmp, googles.exe, 0000000F.00000002.328020119.0000000003331000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	PO #KV18RE001-A5491.exe, 00000000.00000002.305699284.0000000004467000.00000004.00000001.sdmp, googles.exe, 00000007.00000002.502894900.000000000447A000.00000004.00000001.sdmp, ammero.exe, ammero.exe.7.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schema.org/WebPage	googles.exe, 0000000F.00000002.328049985.0000000003362000.00000004.00000001.sdmp, googles.exe, 0000000F.00000002.328086949.0000000003378000.00000004.00000001.sdmp	false		high
http://ns.ado/1	PO #KV18RE001-A5491.exe, 00000000.00000003.232494092.00000000076DA000.00000004.00000001.sdmp, PO #KV18RE001-A5491.exe, 00000000.00000003.297857855.00000000076E1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.91	unknown	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	411850
Start date:	12.05.2021
Start time:	07:45:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO #KV18RE001-A5491.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:	36
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@25/16@0/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.5% (good quality ratio 0.3%) • Quality average: 40.9% • Quality standard deviation: 34.2%
HCA Information:	• Successful, ratio: 96% • 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 • Excluded IPs from analysis (whitelisted): 172.217.168.68, 204.79.197.200, 13.107.21.200, 23.218.208.56, 131.253.33.200, 13.107.22.200, 2.20.142.209, 2.20.143.16, 40.88.32.150, 52.255.188.83, 168.61.161.212 • Excluded domains from analysis (whitelisted): www.bing.com, au.download.windowsupdate.com.edgesuite.net, fs.microsoft.com, dual-a-0001.a-msedge.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus17.cloudapp.net, a767.dscg3.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, dual-a-0001.dc-msedge.net, skypedataprdcoleus15.cloudapp.net, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, blobcollector.events.data.trafficmanager.net, www.google.com, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:46:22	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run googles C:\Users\user\AppData\Roaming\googles.exe
07:46:26	API Interceptor	46x Sleep call for process: PO #KV18RE001-A5491.exe modified
07:46:31	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run googles C:\Users\user\AppData\Roaming\googles.exe
07:46:53	API Interceptor	46x Sleep call for process: googles.exe modified
07:47:17	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\AppData\Local\Temp\InstallUtil.exe" s>$(Arg0)
07:47:17	API Interceptor	472x Sleep call for process: InstallUtil.exe modified
07:47:19	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
07:47:19	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
07:47:20	API Interceptor	382x Sleep call for process: ammero.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.91	PO#KV18RE001_A5491NGOCQUANGTRADEPRODUCTIONSERVICE5.exe	Get hash	malicious	Browse	
	UPSSHIPMENT_CONFIRMATION_CBJ19051700013_11Z35Q6Q80446518864888.doc	Get hash	malicious	Browse	
	ENrYP02wGO.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	UPSSHIPMENT_CONFIRMATION_CBJ19051700013_11Z35Q6Q80446518864.doc	Get hash	malicious	Browse	
	DHL file.exe	Get hash	malicious	Browse	
	Swift 5893038993.exe	Get hash	malicious	Browse	
	PO 67961.exe	Get hash	malicious	Browse	
	PO 77390029.exe	Get hash	malicious	Browse	
	SWIFT TT.exe	Get hash	malicious	Browse	
	Ugovor o prodajnom nalogu PO-0091870_25 Meka koza.exe	Get hash	malicious	Browse	
	51INVOICES.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	Devizni izvod za partiju 0050100073053.exe	Get hash	malicious	Browse	• 79.134.225.71
	QwUl4FaToe.exe	Get hash	malicious	Browse	• 79.134.225.71
	IMG_1035852_607.exe	Get hash	malicious	Browse	• 79.134.225.10
	RFQEMFA.Elektrik.exe	Get hash	malicious	Browse	• 79.134.225.17
	Waybill Document 22700456.exe	Get hash	malicious	Browse	• 79.134.225.7
	Give Offer CVE6535 _TVOP-MIO, pdf.exe	Get hash	malicious	Browse	• 79.134.225.8
	Waybill Document 22700456.exe	Get hash	malicious	Browse	• 79.134.225.7
	RFQEMFA.Elektrik.pdf.exe	Get hash	malicious	Browse	• 79.134.225.17
	w85rzxid7y.exe	Get hash	malicious	Browse	• 79.134.225.81
	Remittance E-MAIL Layout - 10_.jar	Get hash	malicious	Browse	• 79.134.225.106
	s65eJyjKga.exe	Get hash	malicious	Browse	• 79.134.225.47
	new order.xlsx	Get hash	malicious	Browse	• 79.134.225.47
	Ot3srIM10B.exe	Get hash	malicious	Browse	• 79.134.225.47
	Remittance E-MAIL Layout - 10_.jar	Get hash	malicious	Browse	• 79.134.225.106
	wnQXyfONbS.exe	Get hash	malicious	Browse	• 79.134.225.82
	kwK4iGa9DL.exe	Get hash	malicious	Browse	• 79.134.225.47
	Remittance E-MAIL Layout - 10_.jar	Get hash	malicious	Browse	• 79.134.225.106
	4z9Saf2vu3.exe	Get hash	malicious	Browse	• 79.134.225.47
	NewOrderSupplypdf.exe	Get hash	malicious	Browse	• 79.134.225.52
	Pu5UMH4fWK.exe	Get hash	malicious	Browse	• 79.134.225.14

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	contract_documents_993454938_pdf.exe	Get hash	malicious	Browse	
	DOCUMENTS_BY_FEDEX_JPG.exe	Get hash	malicious	Browse	
	mylvKlCNki.exe	Get hash	malicious	Browse	
	PptV7lNtMgTlPuO.exe	Get hash	malicious	Browse	
	6BD0F63D69EBAA8E28B21E9B0F5C02E05C1213535B288.exe	Get hash	malicious	Browse	
	PO#KV18RE001_A5491NGOCQUANGTRADEPRODUCTIONSERVICE5.exe	Get hash	malicious	Browse	
	M2Ia9NwhS0.exe	Get hash	malicious	Browse	
	Z1ZdFWqLdS.exe	Get hash	malicious	Browse	
	ENrYP02wGO.exe	Get hash	malicious	Browse	
	Quotation#73280126721_Oriental_Fastech_Manufacturing.exe	Get hash	malicious	Browse	
	Quotation#73280126721_Oriental_Fastech_Manufacturings.exe	Get hash	malicious	Browse	
	OFF8mgLVHc.exe	Get hash	malicious	Browse	
	06BUvGWk7B.exe	Get hash	malicious	Browse	
	4yO0B3vPLc.exe	Get hash	malicious	Browse	
	RWtutTA7Hl.exe	Get hash	malicious	Browse	
	APRILQUOTATIONS#QQO2103060_Hangzhou_Zhongniu_Import_Export_Co.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	QUOTATION#QQO2103060_Hangzhou_Zhongniu_Import_Export_Co.exe	Get hash	malicious	Browse	
	NEWQUOTATIONs#280321_RFQ_PRODUCTS_ENQUIRY_TRINITY_VIETNAM_CO.exe	Get hash	malicious	Browse	
	APRILQUOTATION#QQO2103060_Hangzhou_Zhongniu_Import_Export_Co.exe	Get hash	malicious	Browse	
	DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	41064
Entropy (8bit):	6.164873449128079
Encrypted:	false
SSDEEP:	384:FtpFVLK0MsihB9VKS7xdgE7KJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+sPZTd:ZBMs2SqdD86lq8gZZFyViML3an
MD5:	EFEC8C379D165E3F33B536739AEE26A3
SHA1:	C875908ACBA5CAC1E0B40F06A83F0F156A2640FA
SHA-256:	46DEE184523A584E56DF93389F81992911A1BA6B1F05AD7D803C6AB1450E18CB
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCFF
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: contract_documents_993454938_pdf.exe, Detection: malicious, Browse • Filename: DOCUMENTS_BY_FEDEX_JPG.exe, Detection: malicious, Browse • Filename: mylvKlCNki.exe, Detection: malicious, Browse • Filename: PptV7lNtMgTlPuO.exe, Detection: malicious, Browse • Filename: 6BD0F63D69EBAA8E28B21E9B0F5C02E05C1213535B288.exe, Detection: malicious, Browse • Filename: PO#KV18RE001_A5491NGOCQUANGTRADEPRODUCTIONSERVICE5.exe, Detection: malicious, Browse • Filename: M2Ia9NwhS0.exe, Detection: malicious, Browse • Filename: Z1ZdFWqLdS.exe, Detection: malicious, Browse • Filename: ENrYP02wGO.exe, Detection: malicious, Browse • Filename: Quotation#73280126721_Oriental_Fastech_Manufacturing.exe, Detection: malicious, Browse • Filename: Quotation#73280126721_Oriental_Fastech_Manufacturings.exe, Detection: malicious, Browse • Filename: OFF8mgLVHc.exe, Detection: malicious, Browse • Filename: 06BUvGWk7B.exe, Detection: malicious, Browse • Filename: 4yO0B3vPLc.exe, Detection: malicious, Browse • Filename: RWtutTA7HI.exe, Detection: malicious, Browse • Filename: APRILQUOTATIONS#QQO2103060_Hangzhou_Zhongniu_Import_Export_Co.exe, Detection: malicious, Browse • Filename: QUOTATION#QQO2103060_Hangzhou_Zhongniu_Import_Export_Co.exe, Detection: malicious, Browse • Filename: NEWQUOTATIONs#280321_RFQ_PRODUCTS_ENQUIRY_TRINITY_VIETNAM_CO.exe, Detection: malicious, Browse • Filename: APRILQUOTATION#QQO2103060_Hangzhou_Zhongniu_Import_Export_Co.exe, Detection: malicious, Browse • Filename: DHL_Express_Shipment_Invoice_Confirmation_CBJ190517000131_74700456XXXX.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....0..T.....r... .....@.. ....`.....4r..O.....b..h>.....p..... ..... ..H.....text....R... ...T..... ..`.rsrc.....V.....@..@.rel oc.....`.....@..B.....hr.....H.....".|J.....lm.....o.....2~.....o....*.r...p(....*VrK..p(....s.....*..0.....(....(....o....o....(....o.... .....T(....o....(....o....o ...o!....4(....o....(....o....o ...o".....(....rm..ps#...o....($.....(%....o&....ry..p.....%.r...p.%.(.....(....('....((.....o)...('.....*.*.....".(*...*..{Q...-...}Q.....(+...(....(,....(+...*".(- ...*..(....*..(.....r...p.(/...o0...s....}T...*....0.. .....~S...-.s

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\InstallUtil.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	329
Entropy (8bit):	5.324195011891804
Encrypted:	false
SSDEEP:	6:Q3La/xwc1K9rDLIP12MUAvvr3tDLIP12MUAvvR+uTL2LDY3U21v:Q3La/h1K9rDLI4M9tDLI4MWuPk21v
MD5:	0F3825E2D8885E05820523A5D8DFEF9C
SHA1:	E6AA2D5D00CE5F875C75B9490F21F2D6B3F0DED3
SHA-256:	2F3769543004FF49CB3B6EF06AC5FD6A402DB0C2546E365639338CA2F4049EBE
SHA-512:	D8FBAEEABF2D33EAF4FF5AADEBF86C233145502560A42B88EBDE455AE2B001F52728E4CE6C59DBCCA37CBF25BA485F5FC5527E992AB66957C6252CF1956F23 7C
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\InstallUtil.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Configuration.Install, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO #KV18RE001-A5491.exe.log	
Process:	C:\Users\user\Desktop\PO #KV18RE001-A5491.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1402
Entropy (8bit):	5.338819835253785
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4bE4Ko84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7csX3:MIHK5HKXE1qHbHKoviYHKhQnoPtHoxHH
MD5:	EB9F730FB5388BB883772033EA3CCE59
SHA1:	7DFF24FBD26D0ED7065882AE0A9A52E459D7F2A9
SHA-256:	B7192E58E5E91CF2CA113CA1C9575AADEAD3C417076AB83D8EF0720D5E473887
SHA-512:	1FB4FF9E7E85C4F4B2395B948A4B69180E602259FFC582A067B96420C60BA4B49D091F3D525333E07930AA21A8254AF1C9F90B29CCD31AA97C368CB1CB7EF322
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configu

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	329
Entropy (8bit):	5.324195011891804
Encrypted:	false
SSDEEP:	6:Q3La/xwc1K9rDLIP12MUAvvr3tDLIP12MUAvvR+uTL2LDY3U21v:Q3La/h1K9rDLI4M9tDLI4MWuPk21v
MD5:	0F3825E2D8885E05820523A5D8DFEF9C
SHA1:	E6AA2D5D00CE5F875C75B9490F21F2D6B3F0DED3
SHA-256:	2F3769543004FF49CB3B6EF06AC5FD6A402DB0C2546E365639338CA2F4049EBE
SHA-512:	D8FBAEEABF2D33EAF4FF5AADEBF86C233145502560A42B88EBDE455AE2B001F52728E4CE6C59DBCCA37CBF25BA485F5FC5527E992AB66957C6252CF1956F237C
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Configuration.Install, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\googles.exe.log	
Process:	C:\Users\user\AppData\Roaming\googles.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1402
Entropy (8bit):	5.338819835253785
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4bE4Ko84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7csX3:MIHK5HKXE1qHbHKoviYHKhQnoPtHoxHH
MD5:	EB9F730FB5388BB883772033EA3CCE59
SHA1:	7DFF24FBD26D0ED7065882AE0A9A52E459D7F2A9
SHA-256:	B7192E58E5E91CF2CA113CA1C9575AADEAD3C417076AB83D8EF0720D5E473887
SHA-512:	1FB4FF9E7E85C4F4B2395B948A4B69180E602259FFC582A067B96420C60BA4B49D091F3D525333E07930AA21A8254AF1C9F90B29CCD31AA97C368CB1CB7EF322
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configu

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
Process:	C:\Users\user\Desktop\PO #KV18RE001-A5491.exe

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	41064
Entropy (8bit):	6.164873449128079
Encrypted:	false
SSDEEP:	384:FtpFVLK0MsihB9VKS7xdgE7KJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+sPZTd:ZBMs2SqdD86lq8gZZFyViML3an
MD5:	EFEC8C379D165E3F33B536739AEE26A3
SHA1:	C875908ACBA5CAC1E0B40F06A83F0F156A2640FA
SHA-256:	46DEE184523A584E56DF93389F81992911A1BA6B1F05AD7D803C6AB1450E18CB
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCFF
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....0..T.....r... .....@.. ....`.....4r..O.....b..h>.....p..... ..... ..H.....text....R... ...T..... ..`.rsrc.....V.....@..@.rel oc.....`.....@..B.....hr.....H.....".|J.....lm.....o.....2~.....o....*.r...p(....*VrK..p(....s.....*..0.....(....(....o....o....(....o.... .....T(....o....(....o....o ...o!....4(....o....(....o....o ...o".....(....rm..ps#...o....($.....(%....o&....ry..p.....%.r...p.%.(.....('....((.....o)...('.....*.*.....".(*...*..{Q...-...}Q.....(+...(....(,....(+...*"..(- ...*..(....*..(.....r...p.(/...o0...s....}T...*....0.. .....~S...-.s

C:\Users\user\AppData\Local\Temp\tmp460B.tmp	
Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1312
Entropy (8bit):	5.101566624560937
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0aKxtn:cbk4oL600QydbQxIYODOLedq3BKj
MD5:	EC44C4BB6E92CFD7C187D5DD2AFB165C
SHA1:	51F8AAA4A9F14938B0B494ACAA514CDF06A83BE3
SHA-256:	CA07C8EB4087C95C4B991B4F791DD711E31A2D95F3E0AF0583B869A050488EB5
SHA-512:	A9419C23FD0F33C73CF2F48E19858E3E66301512DE44E7CCC83E48008644DFD8A1C12BB41812A2D69968EF78C9DA0DBC94947E6F55B20DD887E732DA8F3731E
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\tmp48BB.tmp	
Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <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\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
File Type:	International EBCDIC text, with NEL line terminators, with overstriking
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Encrypted:	false
SSDEEP:	3:X:X
MD5:	76090848624A5340999AFF25A07205A5
SHA1:	F40833A39981B70FE4ACCDA865372AE5A2F35A40
SHA-256:	1988DB99C7FCA406D763F07776718FC279709D2547920592F4C454EA8C1E636B
SHA-512:	582D7A76645C1E5B44862C22AE03FB1CA40AD146C0BBF668B5A0454A0BFAFE114F652F13D3F825F3F3251EE75A97809016FB343DD517F9EF4DAB4DA17E8F019
Malicious:	**true**
Preview:	....T..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	49
Entropy (8bit):	4.361973558701858
Encrypted:	false
SSDEEP:	3:oNWXp5cViE2J5xAIOWRxRI0dAn:oNWXp+N23f5RndA
MD5:	8069A620598F6D0795A045BC4C040FCE
SHA1:	BE6C7D1B6E3A49925674F335C601A53E985A2496
SHA-256:	85E54950497C2B5262439CC09BB7E0779225EAFF0C50B75D59DECE689F2B0625
SHA-512:	D9AB55D7A597CB3DB20E069AA4893654C7033E42738AD5CF3AA489C5745E3D85CBAD12530542241CD2133C52E108368AA5DB7255692177745A1EEAAFB339830
Malicious:	false
Preview:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe

C:\Users\user\AppData\Roaming\ammero.exe	
Process:	C:\Users\user\AppData\Roaming\googles.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	221696
Entropy (8bit):	6.062069753596832
Encrypted:	false
SSDEEP:	3072:Q9WEWiW0bRq1Do6UFJ7YjJhUi3EmkM7Gw+MevJgm3hHyT+rsXngL4J1tShtUh/q:Qoq6UoPU+n7AMOXBCXgC1EXU
MD5:	605E939E44CD9B02C55CE0A09019AD47
SHA1:	9AC8FF474631ED0C3D27A7290979B4880B9784F6
SHA-256:	5AB99263D0101E00809C2FE1F068BBCB601208C3FB0EFD753B36169A3A69C589
SHA-512:	5196B9B698A71DC4510A57ACABAEE22EC2CD3F35C7C82C0CCBC00673EE97B471019A79E4CDB1EC6B5765EF70F1B5AEBC19F56B0FA6A9932844C8AE07BA8B2B9D
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Roaming\ammero.exe, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Roaming\ammero.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 76%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...+L.`.....X.....v... .....@.. ..... ..@.....u..O.....@..... ..... ..H.....text...$V.. ...X..... ..`.rsrc...@.....Z.....@..@.rel oc.....`.....@..B.....v.....H.....@.....(....*..(....*.s.....s.....s.....s.....*...0..,.....+.....,.....,.....,.+.+.~.. ..o....*.0..,.....+.....,.....,.....,.+.+.~....o....*.0..,.....+.....,.....,.....,.+.+.~....o....*.0.....+.....,.....,.....,.+.+...(....(....*...0.. (.....+.....,.....,.....,.+.+..(....*.0..,.....

C:\Users\user\AppData\Roaming\googles.exe	
Process:	C:\Users\user\Desktop\PO #KV18RE001-A5491.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1270784
Entropy (8bit):	6.434519417949751
Encrypted:	false
SSDEEP:	24576:j0s3e0bj5uLJy3AmKANAlN8ek7CPWUli/v:I+OZlANAv8eb+Ul6
MD5:	9D9CB0F32A77D7D81296095768D3583E
SHA1:	8386CDBC85FAEDE7527AA83B4646DFF3F9EDC910
SHA-256:	0CBBDD2C9615F4D2DE4E0232ACE6B69889A54538444838AC6616A5AA39109C98
SHA-512:	1438EAB7E432FE118437CE17EE9459605FCC8758658F6BAE7C1081967BF7A446C3C015093EE51EBFEEA221A6FF76839F934644B0AF53D78DC8001D08B74A810E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 26%, Browse • Antivirus: ReversingLabs, Detection: 38%

C:\Users\user\AppData\Roaming\googles.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....m.,.....R.....q... .....@.. ....`.....tq..W..... ..... ..H.....text....Q... ...R..... ..`.rsrc.....T.....@..@.reloc..... .....b.....@..B.....q.....H.....|.....t.....(.$.('...9...m.>.... ...=..q.w.p...A.v.K...9.qHwHsH.p.yHG}KH].D.T.T.T.e.[.W.A4X.r.Ssl.e. [.W.A/X.r.Stl.e.[.W.A5X.r.Snl>e.[.W.A0.$.4...7....A.....>.|.$..w.4....9...-..{.k.~.L..#.*F.I.W....=Y..#.*B.u.A...+=.....9.....x.0....*...(...i.....7.*._.Q.X.|..:.3f.O.r...8$m..:.3d.R .K..W.W.W.BA[.q.P.oqf.X.T.B^[.q.P.opf.X.T.....g..0.....'.....f..0....*5&5 5@..2.....:-6$ .9K..2....1.6.:.....\.....

C:\Users\user\AppData\Roaming\googles.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\PO #KV18RE001-A5491.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2017
Entropy (8bit):	4.663189584482275
Encrypted:	false
SSDEEP:	48:zK4Qu4D4ql0+1AcJRy0EJP64gFljVlWo3ggxUnQK2qmBvgw1+5:zKJDEcTytNe3Wo3uQVBIe+5
MD5:	9C305D95E7DA8FCA9651F7F426BB25BC
SHA1:	FDB5C18C26CF5B83EF5DC297C0F9CEBEF6A97FFC
SHA-256:	444F71CF504D22F0EE88024D61501D3B79AE5D1AFD521E72499F325F6B0B82BE
SHA-512:	F2829518AE0F6DD35C1DE1175FC8BE3E52EDCAFAD0B2455AC593F5E5D4BD480B014F52C3AE24E742B914685513BE5DF862373E75C45BB7908C775D7E2E404D3
Malicious:	false
Preview:	Microsoft (R) .NET Framework Installation utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....Usage: InstallUtil [/u | /uninstall] [option [...]] assembly [[option [...]] assembly] [...]]....InstallUtil executes the installers in each given assembly...If the /u or /uninstall switch is specified, it uninstalls..the assemblies, otherwise it installs them. Unlike other..options, /u applies to all assemblies, regardless of where it..appears on the command line.....Installation is done in a transactioned way: If one of the..assemblies fails to install, the installations of all other..assemblies are rolled back. Uninstall is not transactioned.....Options take the form /switch=[value]. Any option that occurs..before the name of an assembly will apply to that assembly's..installation. Options are cumulative but overridable - options..specified for one assembly will apply to the next as well unless..the option is specified with a new value. The default for

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.434519417949751
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	PO #KV18RE001-A5491.exe
File size:	1270784
MD5:	9d9cb0f32a77d7d81296095768d3583e
SHA1:	8386cdbc85faede7527aa83b4646dff3f9edc910
SHA256:	0cbbdd2c9615f4d2de4e0232ace6b69889a54538444838ac6616a5aa39109c98
SHA512:	1438eab7e432fe118437ce17ee9459605fcc8758658f6bae7c1081967bf7a446c3c015093ee51ebfeea221a6ff76839f934644b0af53d78dc8001d08b74a810e

General

SSDEEP:	24576:j0s3e0bj5uLJy3AmKANAlN8ek7CPWUli/v:I+OZlANAv8eb+Ul6
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....m.,.................R...........q... ....@.. ....``...`.................................

File Icon

	
Icon Hash:	d0c0ecccd4c4c454

Static PE Info

General

Entrypoint:	0x5271ce
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x2CDB6D86 [Sat Nov 6 09:25:26 1993 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x127174	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x128000	0x10ca8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x13a000	0xc	.reloc
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	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1251d4	0x125200	False	0.591487040245	data	6.4539132428	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x128000	0x10ca8	0x10e00	False	0.141941550926	data	3.7071684256	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x13a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1280e8	0x10828	data		
RT_GROUP_ICON	0x138910	0x14	data		
RT_VERSION	0x138924	0x384	data		

Imports

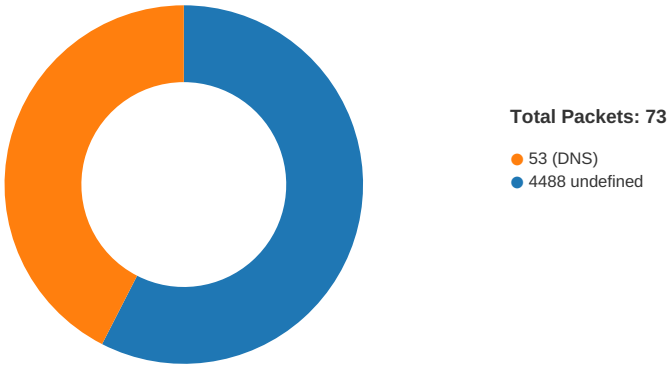
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 1999 <7DD5;=J3<E?J;H>9=B
Assembly Version	1.0.0.0
InternalName	AABBA.exe
FileVersion	7.10.13.17
CompanyName	<7DD5;=J3<E?J;H>9=B
Comments	A:C>4:G6CE47?=?D56=AD9J7
ProductName	65JGE8@H93FJ335
ProductVersion	7.10.13.17
FileDescription	65JGE8@H93FJ335
OriginalFilename	AABBA.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 07:47:19.134324074 CEST	49691	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:47:19.215867043 CEST	4488	49691	79.134.225.91	192.168.2.3
May 12, 2021 07:47:19.716223001 CEST	49691	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:47:19.796866894 CEST	4488	49691	79.134.225.91	192.168.2.3
May 12, 2021 07:47:20.310082912 CEST	49691	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:47:20.391540051 CEST	4488	49691	79.134.225.91	192.168.2.3
May 12, 2021 07:47:24.968660116 CEST	49692	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:47:25.049097061 CEST	4488	49692	79.134.225.91	192.168.2.3
May 12, 2021 07:47:25.560457945 CEST	49692	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:47:25.641999960 CEST	4488	49692	79.134.225.91	192.168.2.3
May 12, 2021 07:47:26.154200077 CEST	49692	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:47:26.234621048 CEST	4488	49692	79.134.225.91	192.168.2.3
May 12, 2021 07:47:30.274878025 CEST	49693	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:47:30.359219074 CEST	4488	49693	79.134.225.91	192.168.2.3
May 12, 2021 07:47:30.873501062 CEST	49693	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:47:30.956877947 CEST	4488	49693	79.134.225.91	192.168.2.3
May 12, 2021 07:47:31.467262983 CEST	49693	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:47:31.550713062 CEST	4488	49693	79.134.225.91	192.168.2.3
May 12, 2021 07:47:35.562935114 CEST	49694	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:47:35.645302057 CEST	4488	49694	79.134.225.91	192.168.2.3
May 12, 2021 07:47:36.155051947 CEST	49694	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:47:36.240921974 CEST	4488	49694	79.134.225.91	192.168.2.3
May 12, 2021 07:47:36.748944998 CEST	49694	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:47:36.832464933 CEST	4488	49694	79.134.225.91	192.168.2.3
May 12, 2021 07:47:40.845041037 CEST	49695	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:47:40.928467989 CEST	4488	49695	79.134.225.91	192.168.2.3
May 12, 2021 07:47:41.436881065 CEST	49695	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:47:41.520199060 CEST	4488	49695	79.134.225.91	192.168.2.3
May 12, 2021 07:47:42.030592918 CEST	49695	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:47:42.113818884 CEST	4488	49695	79.134.225.91	192.168.2.3
May 12, 2021 07:47:46.126332998 CEST	49698	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:47:46.209604979 CEST	4488	49698	79.134.225.91	192.168.2.3
May 12, 2021 07:47:46.718466997 CEST	49698	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:47:46.801826954 CEST	4488	49698	79.134.225.91	192.168.2.3
May 12, 2021 07:47:47.312284946 CEST	49698	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:47:47.395411968 CEST	4488	49698	79.134.225.91	192.168.2.3
May 12, 2021 07:47:51.459636927 CEST	49703	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:47:51.542972088 CEST	4488	49703	79.134.225.91	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 07:47:52.047068119 CEST	49703	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:47:52.132709980 CEST	4488	49703	79.134.225.91	192.168.2.3
May 12, 2021 07:47:52.640842915 CEST	49703	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:47:52.725085974 CEST	4488	49703	79.134.225.91	192.168.2.3
May 12, 2021 07:47:57.006196976 CEST	49707	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:47:57.086376905 CEST	4488	49707	79.134.225.91	192.168.2.3
May 12, 2021 07:47:57.594396114 CEST	49707	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:47:57.674560070 CEST	4488	49707	79.134.225.91	192.168.2.3
May 12, 2021 07:47:58.188213110 CEST	49707	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:47:58.268560886 CEST	4488	49707	79.134.225.91	192.168.2.3
May 12, 2021 07:48:02.402754068 CEST	49711	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:48:02.483135939 CEST	4488	49711	79.134.225.91	192.168.2.3
May 12, 2021 07:48:02.985466003 CEST	49711	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:48:03.066778898 CEST	4488	49711	79.134.225.91	192.168.2.3
May 12, 2021 07:48:03.579226971 CEST	49711	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:48:03.659740925 CEST	4488	49711	79.134.225.91	192.168.2.3
May 12, 2021 07:48:07.679939032 CEST	49716	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:48:07.761409998 CEST	4488	49716	79.134.225.91	192.168.2.3
May 12, 2021 07:48:08.267137051 CEST	49716	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:48:08.347863913 CEST	4488	49716	79.134.225.91	192.168.2.3
May 12, 2021 07:48:08.860995054 CEST	49716	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:48:08.942778111 CEST	4488	49716	79.134.225.91	192.168.2.3
May 12, 2021 07:48:12.956504107 CEST	49721	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:48:13.036941051 CEST	4488	49721	79.134.225.91	192.168.2.3
May 12, 2021 07:48:13.548749924 CEST	49721	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:48:13.630450010 CEST	4488	49721	79.134.225.91	192.168.2.3
May 12, 2021 07:48:14.142591953 CEST	49721	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:48:14.223201036 CEST	4488	49721	79.134.225.91	192.168.2.3
May 12, 2021 07:48:18.239823103 CEST	49722	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:48:18.320306063 CEST	4488	49722	79.134.225.91	192.168.2.3
May 12, 2021 07:48:18.823184013 CEST	49722	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:48:18.903579950 CEST	4488	49722	79.134.225.91	192.168.2.3
May 12, 2021 07:48:19.408647060 CEST	49722	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:48:19.490019083 CEST	4488	49722	79.134.225.91	192.168.2.3
May 12, 2021 07:48:23.506278992 CEST	49723	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:48:23.587838888 CEST	4488	49723	79.134.225.91	192.168.2.3
May 12, 2021 07:48:24.096506119 CEST	49723	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:48:24.177037954 CEST	4488	49723	79.134.225.91	192.168.2.3
May 12, 2021 07:48:24.690360069 CEST	49723	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:48:24.770771980 CEST	4488	49723	79.134.225.91	192.168.2.3
May 12, 2021 07:48:28.785541058 CEST	49724	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:48:28.870794058 CEST	4488	49724	79.134.225.91	192.168.2.3
May 12, 2021 07:48:29.378220081 CEST	49724	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:48:29.461577892 CEST	4488	49724	79.134.225.91	192.168.2.3
May 12, 2021 07:48:29.972134113 CEST	49724	4488	192.168.2.3	79.134.225.91
May 12, 2021 07:48:30.055479050 CEST	4488	49724	79.134.225.91	192.168.2.3

UDP Packets

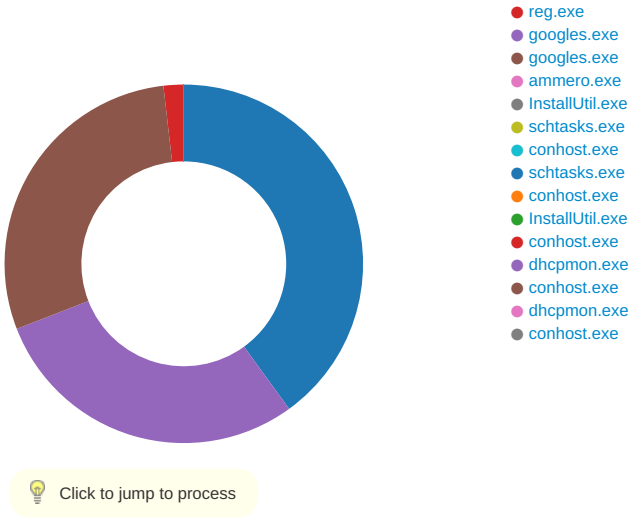
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 07:46:10.207685947 CEST	54260	53	192.168.2.3	8.8.8.8
May 12, 2021 07:46:10.265038967 CEST	53	54260	8.8.8.8	192.168.2.3
May 12, 2021 07:46:10.681350946 CEST	51904	53	192.168.2.3	8.8.8.8
May 12, 2021 07:46:10.741502047 CEST	53	51904	8.8.8.8	192.168.2.3
May 12, 2021 07:46:10.751137018 CEST	61328	53	192.168.2.3	8.8.8.8
May 12, 2021 07:46:10.808197021 CEST	53	61328	8.8.8.8	192.168.2.3
May 12, 2021 07:46:34.891448975 CEST	54130	53	192.168.2.3	8.8.8.8
May 12, 2021 07:46:34.953044891 CEST	53	54130	8.8.8.8	192.168.2.3
May 12, 2021 07:46:41.455427885 CEST	56961	53	192.168.2.3	8.8.8.8
May 12, 2021 07:46:41.515317917 CEST	53	56961	8.8.8.8	192.168.2.3
May 12, 2021 07:46:42.179349899 CEST	59353	53	192.168.2.3	8.8.8.8
May 12, 2021 07:46:42.236339092 CEST	53	59353	8.8.8.8	192.168.2.3
May 12, 2021 07:46:42.248321056 CEST	52238	53	192.168.2.3	8.8.8.8
May 12, 2021 07:46:42.308249950 CEST	53	52238	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 07:46:54.633949041 CEST	49873	53	192.168.2.3	8.8.8.8
May 12, 2021 07:46:54.696114063 CEST	53	49873	8.8.8.8	192.168.2.3
May 12, 2021 07:46:55.204524040 CEST	53196	53	192.168.2.3	8.8.8.8
May 12, 2021 07:46:55.264524937 CEST	53	53196	8.8.8.8	192.168.2.3
May 12, 2021 07:46:55.305525064 CEST	56777	53	192.168.2.3	8.8.8.8
May 12, 2021 07:46:55.354331017 CEST	53	56777	8.8.8.8	192.168.2.3
May 12, 2021 07:46:56.623327971 CEST	58643	53	192.168.2.3	8.8.8.8
May 12, 2021 07:46:56.680459976 CEST	53	58643	8.8.8.8	192.168.2.3
May 12, 2021 07:47:44.146961927 CEST	60985	53	192.168.2.3	8.8.8.8
May 12, 2021 07:47:44.196902990 CEST	53	60985	8.8.8.8	192.168.2.3
May 12, 2021 07:47:45.599400043 CEST	50200	53	192.168.2.3	8.8.8.8
May 12, 2021 07:47:45.648654938 CEST	53	50200	8.8.8.8	192.168.2.3
May 12, 2021 07:47:46.736840010 CEST	51281	53	192.168.2.3	8.8.8.8
May 12, 2021 07:47:46.785608053 CEST	53	51281	8.8.8.8	192.168.2.3
May 12, 2021 07:47:48.368988991 CEST	49199	53	192.168.2.3	8.8.8.8
May 12, 2021 07:47:48.417994022 CEST	53	49199	8.8.8.8	192.168.2.3
May 12, 2021 07:47:49.777586937 CEST	50620	53	192.168.2.3	8.8.8.8
May 12, 2021 07:47:49.830431938 CEST	53	50620	8.8.8.8	192.168.2.3
May 12, 2021 07:47:51.119570971 CEST	64938	53	192.168.2.3	8.8.8.8
May 12, 2021 07:47:51.168591976 CEST	53	64938	8.8.8.8	192.168.2.3
May 12, 2021 07:47:52.200820923 CEST	60152	53	192.168.2.3	8.8.8.8
May 12, 2021 07:47:52.251086950 CEST	53	60152	8.8.8.8	192.168.2.3
May 12, 2021 07:47:53.336946011 CEST	57544	53	192.168.2.3	8.8.8.8
May 12, 2021 07:47:53.389000893 CEST	53	57544	8.8.8.8	192.168.2.3
May 12, 2021 07:47:55.208327055 CEST	55984	53	192.168.2.3	8.8.8.8
May 12, 2021 07:47:55.271629095 CEST	53	55984	8.8.8.8	192.168.2.3
May 12, 2021 07:47:59.463005066 CEST	64185	53	192.168.2.3	8.8.8.8
May 12, 2021 07:47:59.511868954 CEST	53	64185	8.8.8.8	192.168.2.3
May 12, 2021 07:48:00.798407078 CEST	65110	53	192.168.2.3	8.8.8.8
May 12, 2021 07:48:00.857759953 CEST	53	65110	8.8.8.8	192.168.2.3
May 12, 2021 07:48:02.101973057 CEST	58361	53	192.168.2.3	8.8.8.8
May 12, 2021 07:48:02.153584957 CEST	53	58361	8.8.8.8	192.168.2.3
May 12, 2021 07:48:03.620207071 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 07:48:03.669038057 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 07:48:04.713371992 CEST	60831	53	192.168.2.3	8.8.8.8
May 12, 2021 07:48:04.765901089 CEST	53	60831	8.8.8.8	192.168.2.3
May 12, 2021 07:48:06.128130913 CEST	60100	53	192.168.2.3	8.8.8.8
May 12, 2021 07:48:06.187184095 CEST	53	60100	8.8.8.8	192.168.2.3
May 12, 2021 07:48:07.357901096 CEST	53195	53	192.168.2.3	8.8.8.8
May 12, 2021 07:48:07.409833908 CEST	53	53195	8.8.8.8	192.168.2.3
May 12, 2021 07:48:08.479552984 CEST	50141	53	192.168.2.3	8.8.8.8
May 12, 2021 07:48:08.528301954 CEST	53	50141	8.8.8.8	192.168.2.3
May 12, 2021 07:48:09.711353064 CEST	53023	53	192.168.2.3	8.8.8.8
May 12, 2021 07:48:09.760333061 CEST	53	53023	8.8.8.8	192.168.2.3
May 12, 2021 07:48:10.804955006 CEST	49563	53	192.168.2.3	8.8.8.8
May 12, 2021 07:48:10.853780985 CEST	53	49563	8.8.8.8	192.168.2.3
May 12, 2021 07:48:12.054651976 CEST	51352	53	192.168.2.3	8.8.8.8
May 12, 2021 07:48:12.103460073 CEST	53	51352	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: PO #KV18RE001-A5491.exe PID: 5580 Parent PID: 5644

General

Start time:	07:46:08
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\PO #KV18RE001-A5491.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO #KV18RE001-A5491.exe'
Imagebase:	0xfe0000
File size:	1270784 bytes
MD5 hash:	9D9CB0F32A77D7D81296095768D3583E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.306129386.000000000454E000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.306129386.000000000454E000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.306129386.000000000454E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.305699284.0000000004467000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.305699284.0000000004467000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.305699284.0000000004467000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.305699284.0000000004467000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.305699284.0000000004467000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.271257920.00000000045D8000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000003.271257920.00000000045D8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000003.271257920.00000000045D8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.271257920.00000000045D8000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.271257920.00000000045D8000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	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	6E0ACF06	unknown
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6F569BA	CopyFileExW
C:\Users\user\AppData\Roaming\googles.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	6F569BA	CopyFileExW
C:\Users\user\AppData\Roaming\googles.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6F569BA	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO #KV18RE001-A5491.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3BC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0	41064	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 00 00 00 00 00 80 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 50 45 00 00 4c 01 03 00 07 5a 8e 5a 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 54 00 00 00 0c 00 00 00 00 00 00 86 72 00 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 c0 00 00 00 02 00 00 9a 80 01 00 03 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....PE..L....Z.Z..... ....0..T.....r... .....@.. ....`.....	success or wait	1	6F569BA	CopyFileExW
C:\Users\user\AppData\Roaming\googles.exe	0	262144	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 00 00 00 00 00 80 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 50 45 00 00 4c 01 03 00 86 6d db 2c 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 52 12 00 00 10 01 00 00 00 00 00 ce 71 12 00 00 20 00 00 00 80 12 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 13 00 00 02 00 00 00 00 00 00 02 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....PE..L....m.,..... .....R.....q... .....@.. ....`.....	success or wait	5	6F569BA	CopyFileExW
C:\Users\user\AppData\Roaming\googles.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6F569BA	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO #KV18RE001-A5491.exe.log	unknown	1402	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 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 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 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 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 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 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E3BC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 4064 Parent PID: 5580

General

Start time:	07:46:21

Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'googles' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\googles.exe'
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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

Analysis Process: conhost.exe PID: 3864 Parent PID: 4064

General

Start time:	07:46:21
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: reg.exe PID: 2416 Parent PID: 4064

General

Start time:	07:46:21
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'googles' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\googles.exe'
Imagebase:	0x1380000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
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

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	googles	unicode	C:\Users\user\AppData\Roaming\googles.exe	success or wait	1	1385A1D	RegSetValueExW

Analysis Process: googles.exe PID: 6120 Parent PID: 3388

General

Start time:	07:46:39
Start date:	12/05/2021
Path:	C:\Users\user\AppData\Roaming\googles.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\googles.exe'
Imagebase:	0xe00000
File size:	1270784 bytes
MD5 hash:	9D9CB0F32A77D7D81296095768D3583E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.502894900.000000000447A000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.502894900.000000000447A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000002.502894900.000000000447A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.502894900.000000000447A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.502894900.000000000447A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.502994681.0000000004561000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.502994681.0000000004561000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000002.502994681.0000000004561000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.502994681.0000000004561000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.502994681.0000000004561000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.502813497.0000000004407000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.502813497.0000000004407000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.502813497.0000000004407000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 26%, Metadefender, Browse • Detection: 38%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6E0ACF06	unknown
C:\Users\user\AppData\Roaming\ammero.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CEF1E60	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ammero.exe	unknown	221696	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 80 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 50 45 00 00 4c 01 03 00 2b 4c 98 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0b 00 00 58 03 00 00 08 00 00 00 00 00 00 1e 76 03 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 c0 03 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ.....................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...+L.`.......... ....X...........v... ....@.. ....@................	success or wait	1	6CEF1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: googles.exe PID: 1196 Parent PID: 5580

General

Start time:	07:46:49
Start date:	12/05/2021
Path:	C:\Users\user\AppData\Roaming\googles.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\googles.exe'
Imagebase:	0xd60000
File size:	1270784 bytes
MD5 hash:	9D9CB0F32A77D7D81296095768D3583E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	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	6E0ACF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ googles.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3BC78D	CreateFileW

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\Microsoft\CLR_v4.0_32\UsageLogs\googles.exe.log	unknown	1402	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 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 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 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 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 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 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E3BC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile

Analysis Process: ammero.exe PID: 1784 Parent PID: 6120

General

Start time:	07:47:09
Start date:	12/05/2021
Path:	C:\Users\user\AppData\Roaming\ammero.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\ammero.exe'
Imagebase:	0x9e0000
File size:	221696 bytes
MD5 hash:	605E939E44CD9B02C55CE0A09019AD47
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000000.340634193.00000000009E2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000010.00000000.340634193.00000000009E2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000002.477797620.00000000009E2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000010.00000002.477797620.00000000009E2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000002.489309809.0000000003011000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000010.00000002.489309809.0000000003011000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Roaming\ammero.exe, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Roaming\ammero.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 76%, ReversingLabs
Reputation:	low

Analysis Process: InstallUtil.exe PID: 5476 Parent PID: 6120

General

Start time:	07:47:10
Start date:	12/05/2021
Path:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Imagebase:	0x480000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000002.477862066.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.477862066.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.477862066.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.495140225.0000000003719000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.495140225.0000000003719000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000002.500714113.0000000005020000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000011.00000002.500714113.0000000005020000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000002.501438329.0000000005DC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000011.00000002.501438329.0000000005DC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.501438329.0000000005DC0000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

Analysis Process: schtasks.exe PID: 3596 Parent PID: 5476

General

Start time:	07:47:15
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\tmp460B.tmp'
Imagebase:	0xcd0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 1048 Parent PID: 3596

General

Start time:	07:47:16
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 5544 Parent PID: 5476

General

Start time:	07:47:16
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp48BB.tmp'
Imagebase:	0xcd0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 2428 Parent PID: 5544

General

Start time:	07:47:16
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: InstallUtil.exe PID: 632 Parent PID: 528

General

Start time:	07:47:17
Start date:	12/05/2021
Path:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe 0
Imagebase:	0x5f0000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: conhost.exe PID: 492 Parent PID: 632

General

Start time:	07:47:17
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 5268 Parent PID: 528

General

Start time:	07:47:19
Start date:	12/05/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x7a0000
File size:	41064 bytes

MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

Analysis Process: conhost.exe PID: 5284 Parent PID: 5268

General

Start time:	07:47:20
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 5596 Parent PID: 3388

General

Start time:	07:47:27
Start date:	12/05/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x9d0000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: conhost.exe PID: 5656 Parent PID: 5596

General

Start time:	07:47:27
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis