



ID: 714049
Sample Name: APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe
Cookbook: default.jbs
Time: 12:41:07
Date: 01/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Process Tree 5
Malware Configuration 5
Threatname: NanoCore 6
Yara Signatures 6
Memory Dumps 6
Unpacked PEs 6
Sigma Signatures 7
AV Detection 7
E-Banking Fraud 7
Persistence and Installation Behavior 7
Stealing of Sensitive Information 7
Remote Access Functionality 7
Snort Signatures 7
Joe Sandbox Signatures 8
AV Detection 8
Networking 8
E-Banking Fraud 8
System Summary 8
Data Obfuscation 8
Boot Survival 8
Hooking and other Techniques for Hiding and Protection 8
Malware Analysis System Evasion 9
HIPS / PFW / Operating System Protection Evasion 9
Stealing of Sensitive Information 9
Remote Access Functionality 9
Mitre Att&ck Matrix 9
Behavior Graph 10
Screenshots 10
Thumbnails 10
Antivirus, Machine Learning and Genetic Malware Detection 11
Initial Sample 11
Dropped Files 11
Unpacked PE Files 11
Domains 12
URLs 12
Domains and IPs 13
Contacted Domains 13
Contacted URLs 13
URLs from Memory and Binaries 13
World Map of Contacted IPs 18
Public IPs 19
General Information 19
Warnings 20
Simulations 20
Behavior and APIs 20
Joe Sandbox View / Context 20
IPs 20
Domains 20
ASNs 20
JA3 Fingerprints 20
Dropped Files 20
Created / dropped Files 20
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe 20
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier 21
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe.log 21
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log 21
C:\Users\user\AppData\Local\Temp\tmp2889.tmp 22
C:\Users\user\AppData\Local\Temp\tmp2B48.tmp 22
C:\Users\user\AppData\Local\Temp\tmp63CD.tmp 22
C:\Users\user\AppData\Local\Temp\tmp690.tmp 23
C:\Users\user\AppData\Local\Temp\tmp8832.tmp 23
C:\Users\user\AppData\Local\Temp\tmpA4B.tmp 23
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat 24

Copyright Joe Security LLC 2022

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat 24
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat 24
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat 24
C:\Users\user\AppData\Roaming\JLsbuY.exe 25
Static File Info 25
General 25
File Icon 25
Static PE Info 26
General 26
Entrypoint Preview 26
Data Directories 28
Sections 28
Resources 28
Imports 28
Network Behavior 28
Snort IDS Alerts 28
Network Port Distribution 29
TCP Packets 29
UDP Packets 31
DNS Queries 31
DNS Answers 31
Statistics 31
Behavior 31
System Behavior 32
Analysis Process: APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exePID: 3256, Parent PID: 6028 32
General 32
File Activities 32
File Created 32
File Deleted 33
File Written 33
File Read 34
Analysis Process: schtasks.exePID: 1592, Parent PID: 3256 35
General 35
File Activities 35
File Read 35
Analysis Process: conhost.exePID: 2188, Parent PID: 1592 35
General 35
Analysis Process: APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exePID: 4128, Parent PID: 3256 35
General 35
File Activities 37
File Created 37
File Deleted 38
File Written 38
File Read 41
Registry Activities 41
Key Value Created 41
Analysis Process: schtasks.exePID: 5176, Parent PID: 4128 41
General 41
File Activities 41
File Read 41
Analysis Process: conhost.exePID: 5000, Parent PID: 5176 42
General 42
Analysis Process: APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exePID: 3260, Parent PID: 1088 42
General 42
File Activities 42
File Created 42
File Deleted 42
File Written 42
File Read 43
Analysis Process: schtasks.exePID: 2264, Parent PID: 4128 43
General 43
File Activities 44
File Read 44
Analysis Process: conhost.exePID: 6052, Parent PID: 2264 44
General 44
Analysis Process: dhcpmon.exePID: 1680, Parent PID: 1088 44
General 44
File Activities 44
File Created 44
File Deleted 45
File Written 45
File Read 46
Analysis Process: dhcpmon.exePID: 2068, Parent PID: 3528 46
General 46
Analysis Process: schtasks.exePID: 3736, Parent PID: 3260 47
General 47
Analysis Process: schtasks.exePID: 920, Parent PID: 1680 47
General 47
Analysis Process: conhost.exePID: 4748, Parent PID: 3736 47
General 47
Analysis Process: conhost.exePID: 2220, Parent PID: 920 47
General 47
Analysis Process: APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exePID: 5000, Parent PID: 3260 48
General 48
Analysis Process: dhcpmon.exePID: 1276, Parent PID: 1680 48
General 48
Analysis Process: schtasks.exePID: 5716, Parent PID: 2068 49
General 49
Analysis Process: conhost.exePID: 4616, Parent PID: 5716 49
General 49
Analysis Process: dhcpmon.exePID: 2760, Parent PID: 2068 49

Disassembly 49

Copyright Joe Security LLC 2022

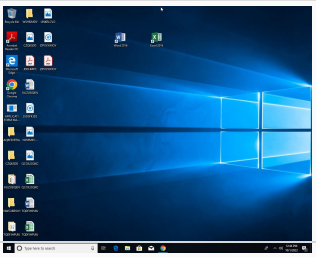
Windows Analysis Report

APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe

Overview

General Information

Sample Name:	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe
Analysis ID:	714049
MD5:	c5ca6bf1a4d668...
SHA1:	1fb0c57d1ea566..
SHA256:	f360431bc55ce6...
Tags:	exe NanoCore RAT
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

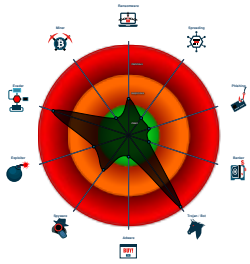
Nanocore

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

Signatures

- Multi AV Scanner detection for subm...
- Malicious sample detected (through...
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Sigma detected: Scheduled temp fil...
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom...
- Multi AV Scanner detection for drop...
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Tries to detect sandboxes and other...

Classification



Process Tree

- **System is w10x64**
- APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe (PID: 3256 cmdline: "C:\Users\user\Desktop\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe" MD5: C5CA6BF1A4D668ABAE8A1BD58DA7FA89)
  - schtasks.exe (PID: 1592 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\JLsbuY" /XML "C:\Users\user\AppData\Local\Temp\tmp8832.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 2188 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe (PID: 4128 cmdline: {path} MD5: C5CA6BF1A4D668ABAE8A1BD58DA7FA89)
    - schtasks.exe (PID: 5176 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp690.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5000 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 2264 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" / xml "C:\Users\user\AppData\Local\Temp\tmpA4B.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6052 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe (PID: 3260 cmdline: "C:\Users\user\Desktop\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe" 0 MD5: C5CA6BF1A4D668ABAE8A1BD58DA7FA89)
  - schtasks.exe (PID: 3736 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\JLsbuY" /XML "C:\Users\user\AppData\Local\Temp\tmp2889.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4748 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe (PID: 5000 cmdline: {path} MD5: C5CA6BF1A4D668ABAE8A1BD58DA7FA89)
- dhcpmon.exe (PID: 1680 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: C5CA6BF1A4D668ABAE8A1BD58DA7FA89)
  - schtasks.exe (PID: 920 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\JLsbuY" /XML "C:\Users\user\AppData\Local\Temp\tmp2B48.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 2220 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 1276 cmdline: {path} MD5: C5CA6BF1A4D668ABAE8A1BD58DA7FA89)
- dhcpmon.exe (PID: 2068 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: C5CA6BF1A4D668ABAE8A1BD58DA7FA89)
  - schtasks.exe (PID: 5716 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\JLsbuY" /XML "C:\Users\user\AppData\Local\Temp\tmp63CD.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4616 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 2760 cmdline: {path} MD5: C5CA6BF1A4D668ABAE8A1BD58DA7FA89)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "bcd7727e-ef56-4958-8ed9-949f5c5e",
  "Group": "Default",
  "Domain1": "godisgood1.hopto.org",
  "Domain2": "185.225.73.164",
  "Port": 7712,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.594571838.00000000072D0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1f1db:$x1: NanoCore.ClientPluginHost • 0x1f1f5:$x2: IClientNetworkHost
00000003.00000002.594571838.00000000072D0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1f1db:$x2: NanoCore.ClientPluginHost • 0x22518:$s4: PipeCreated • 0x1f1c8:$s5: IClientLoggingHost
00000003.00000002.594571838.00000000072D0000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x1f1b2:$x2: NanoCore.ClientPlugin • 0x1f1db:$x3: NanoCore.ClientPluginHost • 0x1f1a3:$i3: IClientNetwork • 0x1f1c8:$i6: IClientLoggingHost • 0x1f1f5:$i7: IClientNetworkHost • 0x1f208:$i8: IClientUIHost • 0x1ef12:$s1: ClientPlugin • 0x1f1bb:$s1: ClientPlugin
00000003.00000002.594571838.00000000072D0000.00000004.08000000.00040000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x1f1db:$a1: NanoCore.ClientPluginHost • 0x1f1b2:$a2: NanoCore.ClientPlugin • 0x24206:$b7: LogClientException • 0x1f1c8:$b9: IClientLoggingHost
00000003.00000002.594469574.00000000072C0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x350b:$x1: NanoCore.ClientPluginHost • 0x3525:$x2: IClientNetworkHost

Click to see the 107 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe.2a6dde4.5.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x3f0b:$x1: NanoCore.ClientPluginHost • 0x921c:$x1: NanoCore.ClientPluginHost • 0x3f44:$x2: IClientNetworkHost

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
3.2.APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe.2a6dde4.5.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x3f0b:$x2: NanoCore.ClientPluginHost • 0x921c:$x2: NanoCore.ClientPluginHost • 0x400f:$s4: PipeCreated • 0x92fa:$s4: PipeCreated • 0x3f25:$s5: IClientLoggingHost • 0x9236:$s5: IClientLoggingHost
3.2.APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe.2a6dde4.5.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x3f87:$x2: NanoCore.ClientPlugin • 0x9266:$x2: NanoCore.ClientPlugin • 0x3f0b:$x3: NanoCore.ClientPluginHost • 0x921c:$x3: NanoCore.ClientPluginHost • 0x3f9d:$i3: IClientNetwork • 0x927c:$i3: IClientNetwork • 0x3f25:$i6: IClientLoggingHost • 0x9236:$i6: IClientLoggingHost • 0x3f44:$i7: IClientNetworkHost • 0x3bfb:$s1: ClientPlugin • 0x3f90:$s1: ClientPlugin • 0x8ff9:$s1: ClientPlugin • 0x926f:$s1: ClientPlugin • 0x50f4:$s3: IPAddress
3.2.APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe.2a6dde4.5.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x3f0b:$a1: NanoCore.ClientPluginHost • 0x921c:$a1: NanoCore.ClientPluginHost • 0x3f87:$a2: NanoCore.ClientPlugin • 0x9266:$a2: NanoCore.ClientPlugin • 0x4b10:$b7: LogClientException • 0x3f25:$b9: IClientLoggingHost • 0x9236:$b9: IClientLoggingHost
17.2.APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe.2eb9838.0.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
Click to see the 267 entries				

Sigma Signatures

AV Detection



Sigma detected: NanoCore

E-Banking Fraud



Sigma detected: NanoCore

Persistence and Installation Behavior



Sigma detected: Scheduled temp file as task from temp location

Stealing of Sensitive Information



Sigma detected: NanoCore

Remote Access Functionality



Sigma detected: NanoCore

Snort Signatures

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 37.139.129.71 - Destination IP: 192.168.2.4 −

Timestamp:	37.139.129.71192.168.2.47712496982841753 10/01/22-12:42:35.121312
SID:	2841753
Source Port:	7712
Destination Port:	49698
Protocol:	TCP

Copyright Joe Security LLC 2022

Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 37.139.129.71	
Timestamp:	192.168.2.437.139.129.714969877122025019 10/01/22-12:42:30.424505
SID:	2025019
Source Port:	49698
Destination Port:	7712
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 37.139.129.71	
Timestamp:	192.168.2.437.139.129.714969877122816766 10/01/22-12:42:35.951752
SID:	2816766
Source Port:	49698
Destination Port:	7712
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection



- Multi AV Scanner detection for submitted file
- Antivirus detection for URL or domain
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Yara detected Nanocore RAT
- Machine Learning detection for sample
- Machine Learning detection for dropped file

Networking



- Snort IDS alert for network traffic
- 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 strings

Data Obfuscation



- .NET source code contains potential unpacker

Boot Survival



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

Hooking and other Techniques for Hiding and Protection



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

Malware Analysis System Evasion



Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion



Injects a PE file into a foreign processes

Stealing of Sensitive Information



Yara detected Nanocore RAT

Remote Access Functionality



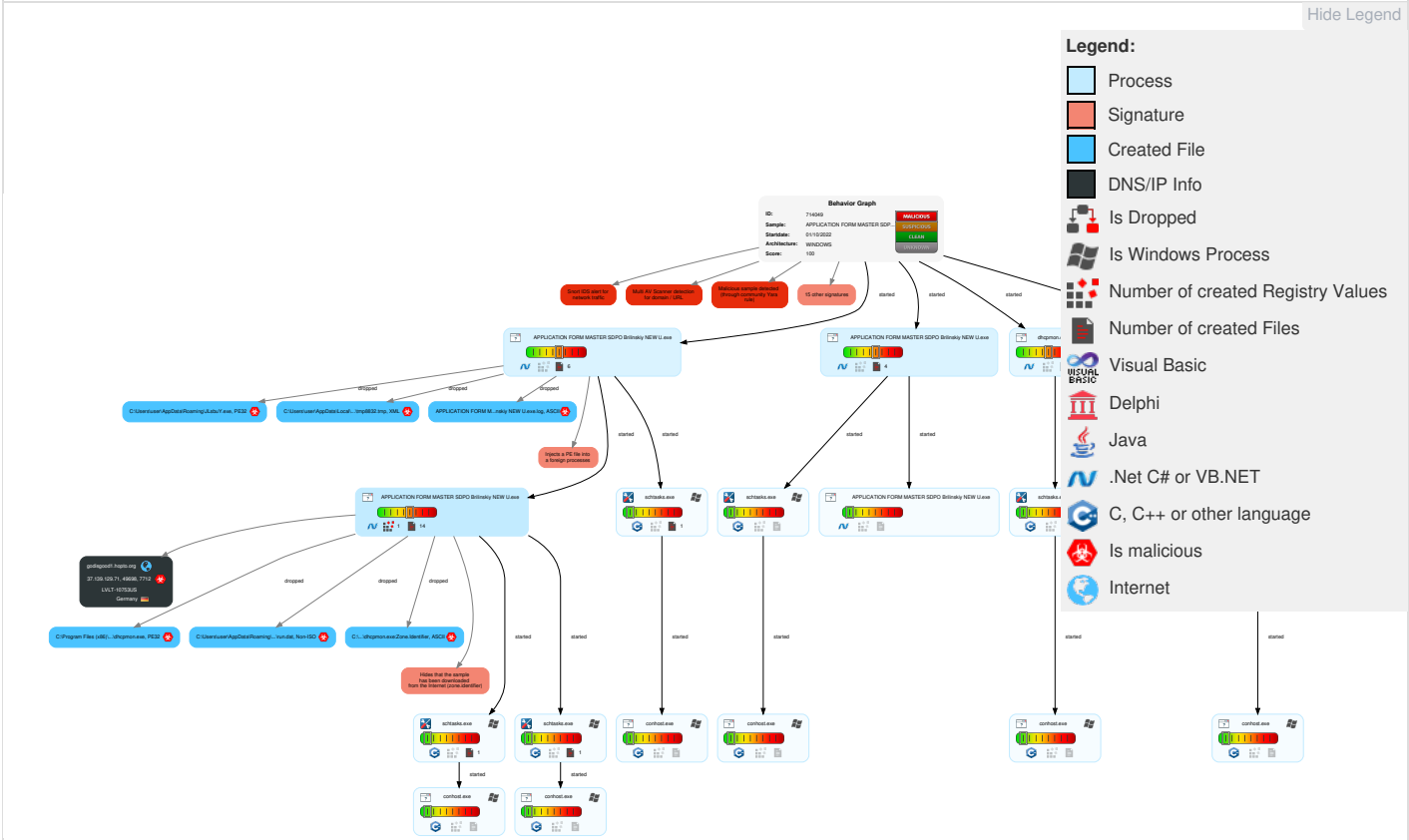
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

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

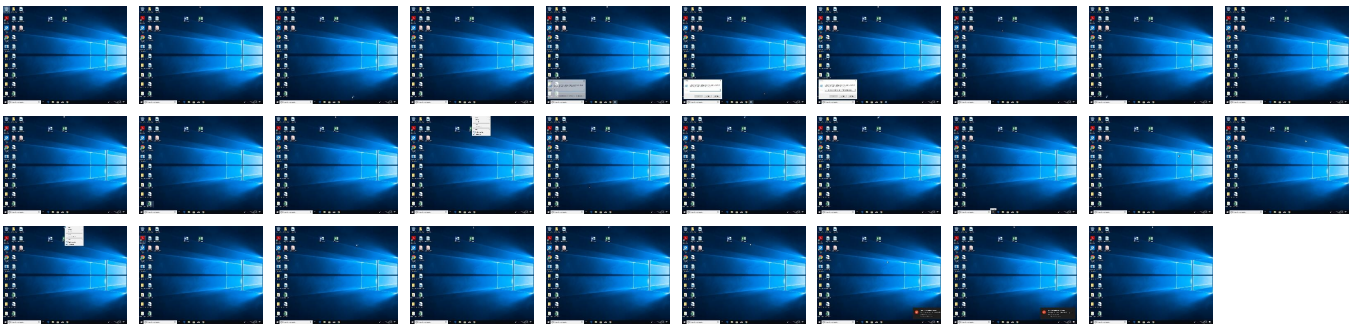
Behavior Graph



Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe	34%	ReversingLabs	ByteCode-MSIL.Trojan.Worefiint	
APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe	31%	Virustotal		Browse
APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\JLsbuY.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	37%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\JLsbuY.exe	37%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link	Download
3.2.APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe.5280000.17.unpack	100%	Avira	TR/NanoCore.fadte		Download File
3.0.APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
godisgood1.hopto.org	14%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.sajatypeworks.comn-u	0%	URL Reputation	safe	
http://www.founder.com.cn/cnT	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comiona	0%	URL Reputation	safe	
http://www.fontbureau.comiona	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnr-f	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.founder.com.c	0%	URL Reputation	safe	
http://www.tiro.comn	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.fontbureau.comituF	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.tiro.comc	0%	URL Reputation	safe	
godisgood1.hopto.org	14%	Virustotal		Browse
http://www.fontbureau.comFV	0%	Avira URL Cloud	safe	
http://www.fonts.comibi	0%	Avira URL Cloud	safe	
http://www.fontbureau.comepkoH	0%	Avira URL Cloud	safe	
godisgood1.hopto.org	100%	Avira URL Cloud	malware	
http://www.founder.com.cn/cnsH	0%	Avira URL Cloud	safe	
http://www.agfamonotype.~SBIm	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn#H4	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcomFH	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdd	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/om	0%	Avira URL Cloud	safe	
http://www.fonts.comS	0%	Avira URL Cloud	safe	
185.225.73.164	100%	Avira URL Cloud	malware	
http://www.urwpp.derT	0%	Avira URL Cloud	safe	
http://www.urwpp.deJ(	0%	Avira URL Cloud	safe	
http://www.fonts.comical	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krXH.	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krend	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnoH%	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
godisgood1.hopto.org	37.139.129.71	true	true	• 14%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
godisgood1.hopto.org	true	• 14%, Virustotal, Browse • Avira URL Cloud: malware	unknown
185.225.73.164	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.367334351.00000000067 22000.00000004.00000800.00020000.0000000 0.sdmp	false		high
http://www.fontbureau.comFV	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.311980649.00000000055 19000.00000004.00000800.00020000.0000000 0.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.367334351.00000000067 22000.00000004.00000800.00020000.0000000 0.sdmp	false		high
http://www.founder.com.cn/cn/bThe	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.367334351.00000000067 22000.00000004.00000800.00020000.0000000 0.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnsH	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.307170791.00000000055 4D000.00000004.00000800.00020000.0000000 0.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.367334351.00000000067 22000.00000004.00000800.00020000.0000000 0.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.comn-u	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303377395.000000000552B000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303559071.0000000005533000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303820040.000000000553300.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303774139.0000000005533000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303418482.0000000005533000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303640331.0000000005532000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnT	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.307170791.000000000554D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.367334351.0000000006722000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.367334351.0000000006722000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comessed	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.312292131.000000000551A000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.311980649.0000000005519000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.goodfont.co.kr	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.367334351.0000000006722000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://google.com	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000003.00000002.581612836.0000000003A90000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000003.00000002.574094218.0000000002A5D000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000003.00000002.584965011.0000000003CAE000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000003.00000002.593962047.0000000007000000.00000004.08000000.00040000.00000000.sdmp	false		high
http://www.fontbureau.comepkoH	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.344604107.0000000005510000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.365697319.000000000551A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comiona	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.344604107.0000000005510000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.365697319.000000000551A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown

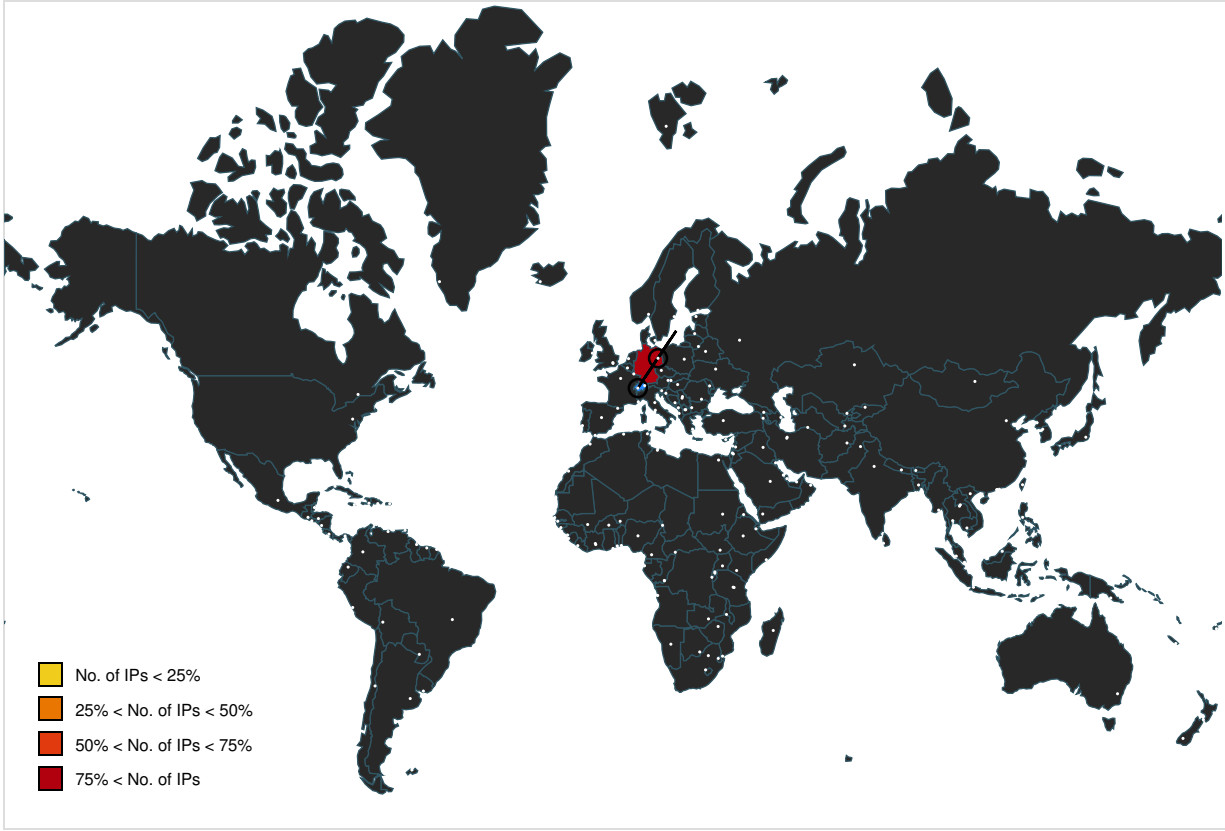
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303377395.000000005552B000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303559071.0000000005533000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303715113.000000005534000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303685970.000000005534000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303820040.0000000005533000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303588332.000000005534000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303452217.0000000005534000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303515704.000000005534000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303774139.000000005533000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.367334351.0000000006722000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303418482.000000005533000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303640331.0000000005532000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.367334351.0000000006722000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.367334351.0000000006722000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.367334351.0000000006722000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.367334351.0000000006722000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comic	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303762586.000000005552B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.comibi	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303685970.000000005534000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303640331.0000000005532000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comcom	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.313059366.000000005519000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.367334351.0000000006722000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.agfamonotype.~SBIm	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.317352691.000000005522000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303685970.0000000005534000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303762586.000000000552B000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.367334351.000000000672200.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303640331.0000000005532000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303671777.000000000552B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.367334351.0000000006722000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.367334351.0000000006722000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.313059366.0000000005519000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.367334351.0000000006722000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.346550034.00000000024A1000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000003.00000002.572765724.00000000029C1000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000006.00000002.453978396.00000000031B500.00000004.00000800.00020000.00000000.sdmp, dhcpmon.exe, 00000009.00000002.455600928.0000000002DA1000.00000004.00000800.00020000.00000000.sdmp, dhcpmon.exe, 0000000A.00000002.480986509.0000000002974000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.367334351.0000000006722000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn#H4	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.307170791.0000000005544D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/om	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.307564401.0000000005514000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnr-f	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.307170791.0000000005544D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.367334351.0000000006722000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.367334351.0000000006722000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comF	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.312292131.000000000551A000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.311980649.0000000005519000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.313059366.000000000551900 0.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.311387611.0000000005518000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.agfamonotype.	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.317352691.0000000005522000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.c	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.307239153.0000000005514000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comn	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.304268623.000000000552B000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.304289380.000000000552B000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.304202190.000000000552B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comdd	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.311980649.0000000005519000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comcomFH	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.313059366.0000000005519000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comS	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303685970.0000000005534000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comd	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.311980649.0000000005519000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.w	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303119536.0000000000BCD000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.367334351.0000000006722000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.derT	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.313059366.0000000005519000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.367334351.0000000006722000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comituF	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.313059366.0000000005519000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.307654597.0000000005521B000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.307572542.0000000005519000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.307239153.0000000005514000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.367334351.0000000006722000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deJ(	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.313059366.00000000551900 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designers/frere-user.html	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.367334351.0000000006722000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.comical	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303629841.000000005552B000.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.303671777.000000000552B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.312451749.000000005554D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.krXH.	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.306187785.00000000551900 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comm	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.344604107.00000000551000 0.00000004.00000800.00020000.00000000.sdmp, APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.365697319.000000000551A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.367334351.0000000006722000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000002.367334351.0000000006722000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.krend	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.306187785.00000000551900 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comc	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.304289380.000000005552B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnoH%	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe, 00000000.00000003.307170791.000000005554D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
37.139.129.71	godisgood1.hopto.org	Germany		10753	LVLT-10753US	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	714049
Start date and time:	2022-10-01 12:41:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
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@30/15@3/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Copyright Joe Security LLC 2022

Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size 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.

Simulations

Behavior and APIs

Time	Type	Description
12:42:11	API Interceptor	724x Sleep call for process: APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe modified
12:42:23	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe" s>$(Arg0)
12:42:24	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
12:42:26	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
12:42:54	API Interceptor	2x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1189376
Entropy (8bit):	6.94809823392214

Encrypted:	false
SSDEEP:	24576:LrArSrrSV1DCOzMFd1bFfxR6ImZlNRU3jrx:OV/+9fxAXU
MD5:	C5CA6BF1A4D668ABAE8A1BD58DA7FA89
SHA1:	1FB0C57D1EA566B703BE21A5DD2334166F5A918E
SHA-256:	F360431BC55CE6BBBD77F26A9BCB86B6267C3B82220D06EE4C67B44BE2273735
SHA-512:	18401E658D3D97A845D8ED05A750EB702337D9C4E1D25CCEDC5A6024BEB09CC333668C6F16A60E11523E79908DCD5D7D439A396724B9D5329D44648F6996FD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 37%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....7c.....P...../.. ...@....@.. ....@.....O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....$.....@..B.....H.....Q..dq.....B.....k.....(....*&..(....*.s .....s!.....s".....s#.....s$.....*...0.....~....o%....+. .*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....(*.....,r...p.....(+...o,...s-.....~.....+..*.0.....~....+..*".....*.0..&..... (....r#..p~....o....(/.....t$....+..*...0..&.....(....r5..p~....o....(/.....

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

Process:	C:\Users\user\Desktop\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.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 E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe.log

Process:	C:\Users\user\Desktop\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
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, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Cultur e=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.Con figuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

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:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF

SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
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, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Cultur e=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.Con figuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp2889.tmp

Process:	C:\Users\user\Desktop\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1639
Entropy (8bit):	5.179579532436944
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGc6Ptn:cbhK79lNQR/rydbz9I3YODOLNdq3ho
MD5:	434B39DEA1D167EF66A3D88C5E1B052F
SHA1:	3850962A4E0064FC0568C51DFA5B7EA3A7859DDC
SHA-256:	8263E5BEE3F8FC17EF42C4A860499EA8F05D83C17FE7F6099846085B49D85279
SHA-512:	17429C9AAE656E636CD928FA5D4E5672C12458C740A292852E5D3F18AE4817ECFB85F9BA96376ED97455570EA22A0D2E02A846311D7E1D55D24E60A0D30F157
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>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Pri ncipal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatte ries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmp2B48.tmp

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1639
Entropy (8bit):	5.179579532436944
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGc6Ptn:cbhK79lNQR/rydbz9I3YODOLNdq3ho
MD5:	434B39DEA1D167EF66A3D88C5E1B052F
SHA1:	3850962A4E0064FC0568C51DFA5B7EA3A7859DDC
SHA-256:	8263E5BEE3F8FC17EF42C4A860499EA8F05D83C17FE7F6099846085B49D85279
SHA-512:	17429C9AAE656E636CD928FA5D4E5672C12458C740A292852E5D3F18AE4817ECFB85F9BA96376ED97455570EA22A0D2E02A846311D7E1D55D24E60A0D30F157
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>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Pri ncipal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatte ries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmp63CD.tmp

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1639
Entropy (8bit):	5.179579532436944
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGc6Ptn:cbhK79lNQR/rydbz9I3YODOLNdq3ho
MD5:	434B39DEA1D167EF66A3D88C5E1B052F
SHA1:	3850962A4E0064FC0568C51DFA5B7EA3A7859DDC
SHA-256:	8263E5BEE3F8FC17EF42C4A860499EA8F05D83C17FE7F6099846085B49D85279
SHA-512:	17429C9AAE656E636CD928FA5D4E5672C12458C740A292852E5D3F18AE4817ECFB85F9BA96376ED97455570EA22A0D2E02A846311D7E1D55D24E60A0D30F157

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>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmp690.tmp

Process:	C:\Users\user\Desktop\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1335
Entropy (8bit):	5.131538419856332
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Y8dxtn:cbk4oL600QydbQxIYODOLedq3odj
MD5:	B9DEE575F2B0ACDC2037D92C74DC29BB
SHA1:	037CA9A5B3612ADEB251AE4D780CD0D0C5053DCB
SHA-256:	8036080B940A7BD8C425649914CCBBA4A4DCF3AABA3023DFAD249BD89F36F4F7
SHA-512:	3970ADE224745201DC6C3FB65E57083B136C53088B212FF1F801388876BB7A3B744B777A1138673BC294614244BA564F39499C865F437221293085BBA334C4C4
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp8832.tmp

Process:	C:\Users\user\Desktop\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1639
Entropy (8bit):	5.179579532436944
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGc6Ptn:cbhK79lNQR/rydbz9I3YODOLNdq3ho
MD5:	434B39DEA1D167EF66A3D88C5E1B052F
SHA1:	3850962A4E0064FC0568C51DFA5B7EA3A7859DDC
SHA-256:	8263E5BEE3F8FC17EF42C4A860499EA8F05D83C17FE7F6099846085B49D85279
SHA-512:	17429C9AAE656E636CD928FA5D4E5672C12458C740A292852E5D3F18AE4817ECFB85F9BA96376ED97455570EA22A0D2E02A846311D7E1D55D24E60A0D30F157
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmpA4B.tmp

Process:	C:\Users\user\Desktop\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.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:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755734
Malicious:	false

Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

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

Process:	C:\Users\user\Desktop\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	3:XrURGizD7cnRNGbgCFKRNX/pBK0jCV83ne+VdWPiKgmR7kkmefoeLBizbCuVkqYM:X4LDAnybgCFcps0OafmCYDlizZr/i/Oh
MD5:	9E7D0351E4DF94A9B0BADCEB6A9DB963
SHA1:	76C6A69B1C31CEA2014D1FD1E222A3DD1E433005
SHA-256:	AAFC7B40C5FE680A2BB549C3B90AABAAC63163F74FFFC0B00277C6BBFF88B757
SHA-512:	93CCF7E046A3C403ECF8BC4F1A8850BA0180FE18926C98B297C5214EB77BC212C8FBCC58412D0307840CF2715B63BE68BACDA95AA98E82835C5C53F17EF3851
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?...A.K...J.=8x!....+.2e'..E?.G.....[.&

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

Process:	C:\Users\user\Desktop\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:DCg:z
MD5:	5A6FF3DF7B2CB03AA295AE6A3C2728C6
SHA1:	656CE7D1794A14D6E749316CBD0BD00AA2DF9D8F
SHA-256:	08F3C75923C4CC4BD40D01FB1D98198307914B0841B9CBD4008F21E4BE5323A2
SHA-512:	D55DF6007CDE0465EB462FDE244FC7707D640179C42499CC20737402E2EE19D50CC12C875531977894F403478024E15EE086FA9ECBC5A827E9378BCC43C873E
Malicious:	**true**
Preview:	.;g....H

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

Process:	C:\Users\user\Desktop\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe
File Type:	data
Category:	modified
Size (bytes):	327768
Entropy (8bit):	**7.999367066417797**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3PlZmqze1d1wI8lkWmtjJ/3Exi:LkjbU7LjGxi
MD5:	2E52F446105FBF828E63CF808B721F9C
SHA1:	5330E54F238F46DC04C1AC62B051DB4FCD7416FB
SHA-256:	2F7479AA2661BD259747BC89106031C11B3A3F79F12190E7F19F5DF65B7C15C8
SHA-512:	C08BA0E3315E2314ECBEF38722DF834C2CB8412446A9A310F41A8F83B4AC5984FCC1B26A1D8B0D58A730FDBDD885714854BDFD04DCDF7F582FC125F552D5C3CA
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV...,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n..._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&.jm.#u..1..Mg!.E..U.T.....6.2>...6.I.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC.....O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$.. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. I..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

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

Process:	C:\Users\user\Desktop\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe

File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	72
Entropy (8bit):	4.867861029749889
Encrypted:	false
SSDEEP:	3:oNt+WfWk1Q9PFB8j+nXIMLWA2LN:oNwvk1QRsj+nXxix
MD5:	2D2969AF6342D4C42632BBEA0FAAB3C1
SHA1:	533268FF8603A9705BDB38DB60CB2D795E754A30
SHA-256:	B2ACA0EE9C8564A59BF6F15F82FDD183486916F18F1E333243E285A8E9957F47
SHA-512:	4C0B9ED26CBD070D9542F258957F4436F0CEECD032D3A8582708B97DF53AB536AD664195C1AAA5D24EDD983ABFA135AD90C0535C99EDFC174274F5569CFDDE5
Malicious:	false
Preview:	C:\Users\user\Desktop\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe

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

Process:	C:\Users\user\Desktop\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1189376
Entropy (8bit):	6.94809823392214
Encrypted:	false
SSDEEP:	24576:LrArSrrSV1DCOzMFd1bFfxR6ImZlNRU3jrx:OV/+9fxAXU
MD5:	C5CA6BF1A4D668ABAE8A1BD58DA7FA89
SHA1:	1FB0C57D1EA566B703BE21A5DD2334166F5A918E
SHA-256:	F360431BC55CE6BBBD77F26A9BCB86B6267C3B82220D06EE4C67B44BE2273735
SHA-512:	18401E658D3D97A845D8ED05A750EB702337D9C4E1D25CCEDC5A6024BEB09CC333668C6F16A60E11523E79908DCD5D7D439A396724B9D5329D44648F6996FD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 37%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....7c.....P...../... ...@....@.. ....@.....O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....$.....@..B.....H.....Q..dq.....B.....k.....(....*&..(.....*.s .....s!.....s".....s#.....s$.....*...0.....~....o%....+. .*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....(*.....,lr...p.....(+...o,...s-.....~.....+..*.0.....~.....+..*"".....*.0..&..... (....r#..p~....o....(/.....t$....+..*...0..&.....(....r5..p~....o....(/.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.94809823392214
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:	APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe
File size:	1189376
MD5:	c5ca6bf1a4d668abae8a1bd58da7fa89
SHA1:	1fb0c57d1ea566b703be21a5dd2334166f5a918e
SHA256:	f360431bc55ce6bbbd77f26a9bcb86b6267c3b82220d06ee4c67b44be2273735
SHA512:	18401e658d3d97a845d8ed05a750eb702337d9c4e1d25ccedc5a6024beb09cc333668c6f16a60e11523e79908dcd5d7d439a396724b9d5329d44648f6996fdc7
SSDEEP:	24576:LrArSrrSV1DCOzMFd1bFfxR6ImZlNRU3jrx:OV/+9fxAXU
TLSH:	AA453A1425DA4B1EF07E8BF91BD4A4E54BFAE622A329E5FA3DE043850722F01CDC1576
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....7c.....P...../... ...@....@.. .....@.....

File Icon



Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x522f16
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x6337A6B5 [Sat Oct 1 02:32:21 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
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

Instruction
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	0x122ec4	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x124000	0x11c8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x126000	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	0x120f1c	0x121000	False	0.6100981293252595	data	6.951369793482402	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x124000	0x11c8	0x1200	False	0.3919270833333333	data	5.051703971077691	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x126000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x124090	0x30c	data		
RT_MANIFEST	0x1243ac	0xe15	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF, LF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

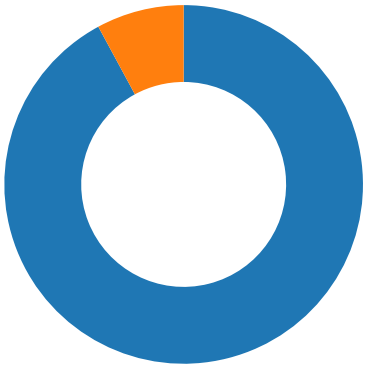
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
37.139.129.71192.168.2.47712496982841753 10/01/22-12:42:35.121312	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	7712	49698	37.139.129.71	192.168.2.4

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.437.139.129.71 4969877122025019 10/01/22-12:42:30.424505	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49698	7712	192.168.2.4	37.139.129.71
192.168.2.437.139.129.71 4969877122816766 10/01/22-12:42:35.951752	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49698	7712	192.168.2.4	37.139.129.71

Network Port Distribution



Total Packets: 38

- 53 (DNS)
- 7712 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 1, 2022 12:42:30.048540115 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:30.076286077 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:30.076489925 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:30.424504995 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:30.472449064 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:30.546344995 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:30.588115931 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:30.755649090 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:30.817027092 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:30.916877985 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:30.944308996 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:30.950195074 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:30.950231075 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:30.950248957 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:30.950268984 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:30.950289011 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:30.950340033 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:30.979064941 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:30.979098082 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:30.979115009 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:30.979135990 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:30.979155064 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:30.979173899 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:30.979190111 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:30.979191065 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:30.979211092 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:30.979238033 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:30.979262114 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:31.006762028 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.006822109 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.006844997 CEST	7712	49698	37.139.129.71	192.168.2.4

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 1, 2022 12:42:31.006867886 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.006910086 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.006932974 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.006952047 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:31.006956100 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.006979942 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.007011890 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.007013083 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:31.007030964 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:31.007036924 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.007062912 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.007081032 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:31.007086992 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.007117033 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.007127047 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:31.007141113 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.007163048 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.007180929 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:31.034719944 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.034754038 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.034774065 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.034780979 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:31.034794092 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.034815073 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.034821987 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:31.034836054 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.034854889 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.034854889 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:31.034888029 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.034893036 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:31.034914017 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.034933090 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.034945011 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:31.034950972 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.034970045 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.034981012 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:31.034990072 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.035008907 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.035027027 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.035031080 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:31.035058022 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:31.035059929 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.035080910 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.035098076 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.035113096 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:31.035115957 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.035135984 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.035150051 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:31.035155058 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.035173893 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.035188913 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:31.035192966 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.035211086 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.035223007 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:31.035229921 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.035248995 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.035268068 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.035273075 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:31.035300016 CEST	49698	7712	192.168.2.4	37.139.129.71

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 1, 2022 12:42:31.063040972 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.063081980 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.063107967 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.063133001 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.063141108 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:31.063160896 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.063178062 CEST	49698	7712	192.168.2.4	37.139.129.71
Oct 1, 2022 12:42:31.063193083 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.063220024 CEST	7712	49698	37.139.129.71	192.168.2.4
Oct 1, 2022 12:42:31.063230038 CEST	49698	7712	192.168.2.4	37.139.129.71

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 1, 2022 12:42:30.000255108 CEST	56572	53	192.168.2.4	8.8.8.8
Oct 1, 2022 12:42:30.021872997 CEST	53	56572	8.8.8.8	192.168.2.4
Oct 1, 2022 12:42:43.918507099 CEST	50911	53	192.168.2.4	8.8.8.8
Oct 1, 2022 12:42:43.938385010 CEST	53	50911	8.8.8.8	192.168.2.4
Oct 1, 2022 12:42:47.465024948 CEST	59683	53	192.168.2.4	8.8.8.8
Oct 1, 2022 12:42:47.486771107 CEST	53	59683	8.8.8.8	192.168.2.4

DNS Queries

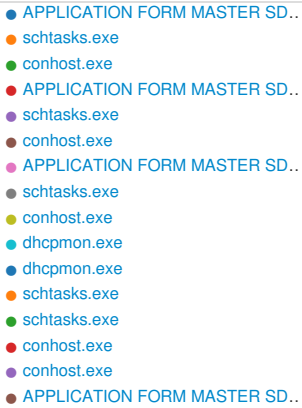
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 1, 2022 12:42:30.000255108 CEST	192.168.2.4	8.8.8.8	0xa928	Standard query (0)	godisgood1 .hopto.org	A (IP address)	IN (0x0001)	false
Oct 1, 2022 12:42:43.918507099 CEST	192.168.2.4	8.8.8.8	0xa723	Standard query (0)	godisgood1 .hopto.org	A (IP address)	IN (0x0001)	false
Oct 1, 2022 12:42:47.465024948 CEST	192.168.2.4	8.8.8.8	0x2be2	Standard query (0)	godisgood1 .hopto.org	A (IP address)	IN (0x0001)	false

DNS Answers

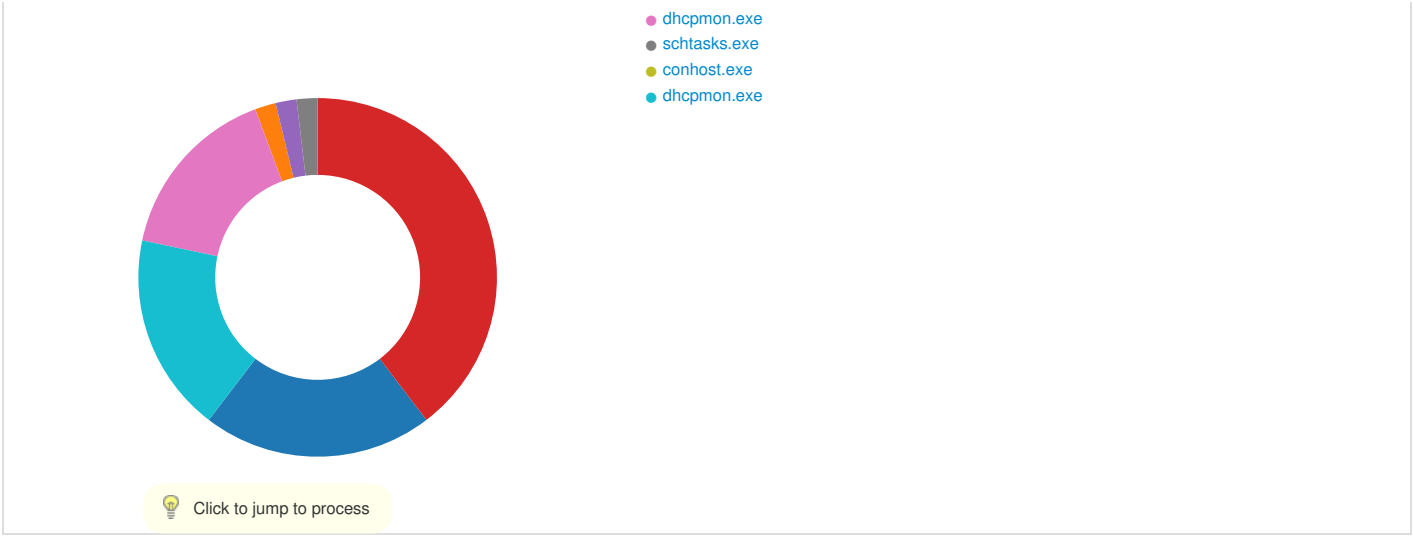
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 1, 2022 12:42:30.021872997 CEST	8.8.8.8	192.168.2.4	0xa928	No error (0)	godisgood1 .hopto.org		37.139.129.71	A (IP address)	IN (0x0001)	false
Oct 1, 2022 12:42:43.938385010 CEST	8.8.8.8	192.168.2.4	0xa723	No error (0)	godisgood1 .hopto.org		37.139.129.71	A (IP address)	IN (0x0001)	false
Oct 1, 2022 12:42:47.486771107 CEST	8.8.8.8	192.168.2.4	0x2be2	No error (0)	godisgood1 .hopto.org		37.139.129.71	A (IP address)	IN (0x0001)	false

Statistics

Behavior



Copyright Joe Security LLC 2022



System Behavior

Analysis Process: APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe PID: 3256, Parent PID: 6028

General

Target ID:	0
Start time:	12:41:58
Start date:	01/10/2022
Path:	C:\Users\user\Desktop\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe"
Imagebase:	0x110000
File size:	1189376 bytes
MD5 hash:	C5CA6BF1A4D668ABAE8A1BD58DA7FA89
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: 00000000.00000002.351210930.00000000034A9000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.351210930.00000000034A9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.351210930.00000000034A9000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.351210930.00000000034A9000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.352245428.00000000035EE000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.352245428.00000000035EE000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.352245428.00000000035EE000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.352245428.00000000035EE000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
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	6D64CF06	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	6D64CF06	unknown
C:\Users\user\AppData\Roaming\JLsbuY.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C491E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp8832.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C497038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D95C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8832.tmp	success or wait	1	6C496A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\JLsbuY.exe	0	1189376	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8832.tmp	0	1639	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationIn	success or wait	1	6C491B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe.log	0	1216	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",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D95C907	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	6D625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D625705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D62CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D625705	unknown

Copyright Joe Security LLC 2022

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C491B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C491B4F	ReadFile
C:\Users\user\Desktop\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe	unknown	1189376	success or wait	1	6C491B4F	ReadFile

Analysis Process: schtasks.exe PID: **1592**, Parent PID: **3256**

General

Target ID:	1
Start time:	12:42:18
Start date:	01/10/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\JLsbuY" /XML "C:\Users\user\AppData\Local\Temp\tmp8832.tmp
Imagebase:	0x10a0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8832.tmp	unknown	2	success or wait	1	10AAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp8832.tmp	unknown	1640	success or wait	1	10AABD9	ReadFile

Analysis Process: conhost.exe PID: **2188**, Parent PID: **1592**

General

Target ID:	2
Start time:	12:42:18
Start date:	01/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
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: APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe PID: **4128**, Parent PID: **3256**

General

Target ID:	3
Start time:	12:42:19
Start date:	01/10/2022

Path:	C:\Users\user\Desktop\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x530000
File size:	1189376 bytes
MD5 hash:	C5CA6BF1A4D668ABAE8A1BD58DA7FA89
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: 00000003.00000002.594571838.00000000072D0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.594571838.00000000072D0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.594571838.00000000072D0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.594571838.00000000072D0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.594469574.00000000072C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.594469574.00000000072C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.594469574.00000000072C0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.594469574.00000000072C0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.593893494.0000000006FF0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.593893494.0000000006FF0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.593893494.0000000006FF0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.593893494.0000000006FF0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.590737920.0000000005CC0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.590737920.0000000005CC0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.590737920.0000000005CC0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.590737920.0000000005CC0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.593817105.0000000006FE0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.593817105.0000000006FE0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.593817105.0000000006FE0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.593817105.0000000006FE0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000003.376885871.0000000006301000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.590108854.0000000005280000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.590108854.0000000005280000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.590108854.0000000005280000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.590108854.0000000005280000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.590108854.0000000005280000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.594220234.00000000072A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.594220234.00000000072A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.594220234.00000000072A0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.594220234.00000000072A0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.574094218.0000000002A5D000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.574094218.0000000002A5D000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.581612836.0000000003A90000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.581612836.0000000003A90000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.581612836.0000000003A90000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.584965011.0000000003CAE000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.584965011.0000000003CAE000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.590874533.0000000005CD0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth

- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.590874533.0000000005CD0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.590874533.0000000005CD0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.590874533.0000000005CD0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.593962047.0000000007000000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.593962047.0000000007000000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.593962047.0000000007000000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.593962047.0000000007000000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.594928792.0000000007310000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.594928792.0000000007310000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.594928792.0000000007310000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.594928792.0000000007310000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.594066194.0000000007010000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.594066194.0000000007010000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.594066194.0000000007010000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.594066194.0000000007010000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000000.343643595.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.343643595.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000003.00000000.343643595.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000000.343643595.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.593436718.0000000006E80000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.593436718.0000000006E80000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.593436718.0000000006E80000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.593436718.0000000006E80000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.592602875.0000000006540000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.592602875.0000000006540000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.592602875.0000000006540000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.592602875.0000000006540000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.589979363.0000000005050000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.589979363.0000000005050000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.589979363.0000000005050000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.589979363.0000000005050000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.580783944.00000000039C1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.572765724.00000000029C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000003.00000002.572765724.00000000029C1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.572765724.00000000029C1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

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	6D64CF06	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	6D64CF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C49BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C491E60	CreateFileW
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C49BEFF	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C49DD66	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C49DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp690.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C497038	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C491E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpA4B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C497038	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C49BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C49BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C491E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C491E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp690.tmp	success or wait	1	6C496A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpA4B.tmp	success or wait	1	6C496A95	DeleteFileW
C:\Users\user\Desktop\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe:Zone.Identifier	success or wait	1	6C412935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	fd 3b 67 fd fd fd fd 48	;gH	success or wait	1	6C491B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA4B.tmp	0	1310	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	6C491B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	0	232	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd fd 26 15 fd fd 69 2b fd 49 63 28 31 fd 50 fd fd 50 fd 63 4c 54 fd fd 42 41 fd 62 fd fd 1b fd fd fd fd fd 34 68 fd 12 fd 74 fd 2b fd 07 5a 5c fd fd 20 fd 69 3b fd fd 04 20 53 fd 12 1c fd 7d 46 46 fd 32 fd fd fd 68 fd 4d 2b fd 39 fd fd 4c fd 23 fd 58 fd fd 2b fd fd fd 01 fd fd 2a fd fd 1e fd 7e 66 1e 47 30 5e e9 56 3b fd 2e fd fd 57 32 fd 3d 10 fd fd 4b fd 7e fd 4c 1f 15 26 66 fd fd 2e 70 fd 04 1b fd fd fd 0f fd fd fd 0b 10 3a 37 72 48 7d fd fd fd 0d 2f 48 16 fd fd 06 17 fd 4c fd fd 04 3f fd fd 04 41 08 4b 07 fd fd 4a 17 3d 38 78 21 19 fd fd fd 2b fd 32 65 27 fd 1f 45 3f fd 47 11 fd fd fd 01 fd 5b 00 26	Gjh\3A5x&i+c(1PPcLTAb 4ht+Z\ i S}FF2hM+L#X+*~fG0^;. W2=K~L&f.p:7rH}/HL? AKJ=8x!+2e'E?G[&	success or wait	1	6C491B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	0	327768	70 54 eb fd 21 fd 08 57 fd fd 47 14 4a fd fd 61 60 29 17 40 8b 69 fd fd 77 70 4b fd 73 6f 40 fd 06 fd 35 fd 3d 10 5e fd 1d 51 fd 6f 79 fd 3d 65 40 39 fd 42 fd fd fd 46 fd fd 30 39 75 22 33 fd fd 20 30 74 fd 19 52 44 6e 5f 34 64 fd fd 17 02 fd 45 fd fd 06 69 fd 08 fd fd fd fd 7e 0c fd fd 7c fd fd 66 58 5f 0e fd fd 58 66 fd 70 5e fd fd fd fd 03 fd 3e 61 cb fd 24 fd fd fd 65 05 36 3a 37 64 fd 28 61 05 41 fd fd fd 3d fd 29 2a 0d fd fd fd fd 7b 42 1c 5b fd fd fd 79 25 fd 2a 31 fd 69 fd 51 fd 3c 12 90 78 74 29 58 13 11 48 09 fd 20 fd 24 48 46 37 67 0f fd fd 49 fd 2a 33 03 7b 0c 6e fd fd fd fd 4c 5b 79 3b 69 fd fd 73 2d 1e fd fd fd 28 35 69 8b fd fd 10 fd fd 02 fd fd 08 17 4a 09 35 62 37 7d fd fd 66 4b fd fd 48 56	pT!WGJa)@iwpKso@5=^ Qoy=e@9BF09u"3 0tRDn_4dEi~|fX_Xfp^>a$ e6:7d(aA=)* {B[y%*iQ<xtXH HF7gI*3{nLy;is- (5iJ5b7}fKHV	success or wait	1	6C491B4F	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	6D625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D625705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D62CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C491B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C491B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D60D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D60D72F	unknown
C:\Users\user\Desktop\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe	unknown	4096	success or wait	1	6D60D72F	unknown
C:\Users\user\Desktop\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe	unknown	512	success or wait	1	6D60D72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	6C49646A	RegSetValueExW

Analysis Process: schtasks.exe PID: **5176**, Parent PID: **4128**

General

Target ID:	4
Start time:	12:42:23
Start date:	01/10/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp690.tmp
Imagebase:	0x10a0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp690.tmp	unknown	2	success or wait	1	10AAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp690.tmp	unknown	1336	success or wait	1	10AABD9	ReadFile

Analysis Process: conhost.exe PID: **5000**, Parent PID: **5176**

General

Target ID:	5
Start time:	12:42:23
Start date:	01/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
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: APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe PID: **3260**, Parent PID: **1088**

General

Target ID:	6
Start time:	12:42:23
Start date:	01/10/2022
Path:	C:\Users\user\Desktop\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe" 0
Imagebase:	0xcf0000
File size:	1189376 bytes
MD5 hash:	C5CA6BF1A4D668ABAE8A1BD58DA7FA89
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	6D64CF06	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	6D64CF06	unknown
C:\Users\user\AppData\Local\Temp\tmp2889.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C497038	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2889.tmp	success or wait	1	6C496A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2889.tmp	0	1639	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationIn	success or wait	1	6C491B4F	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	6D625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D625705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D62CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C491B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C491B4F	ReadFile

Analysis Process: schtasks.exe PID: **2264**, Parent PID: **4128**

General

Target ID:	7
Start time:	12:42:24
Start date:	01/10/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmpA4B.tmp
Imagebase:	0x10a0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA4B.tmp	unknown	2	success or wait	1	10AAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA4B.tmp	unknown	1311	success or wait	1	10AABD9	ReadFile

Analysis Process: conhost.exe PID: **6052**, Parent PID: **2264**

General

Target ID:	8
Start time:	12:42:25
Start date:	01/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
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: **1680**, Parent PID: **1088**

General

Target ID:	9
Start time:	12:42:26
Start date:	01/10/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0x9a0000
File size:	1189376 bytes
MD5 hash:	C5CA6BF1A4D668ABAE8A1BD58DA7FA89
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 37%, 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	6D64CF06	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	6D64CF06	unknown
C:\Users\user\AppData\Local\Temp\tmp2B48.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C497038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D95C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2B48.tmp	success or wait	1	6C496A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2B48.tmp	0	1639	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationIn	success or wait	1	6C491B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	0	1216	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",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089"," C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D95C907	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

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	6D625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D625705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D62CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5803DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5803DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D625705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C491B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C491B4F	ReadFile

Analysis Process: dhcpmon.exe PID: **2068**, Parent PID: **3528**

General

Target ID:	10
Start time:	12:42:34
Start date:	01/10/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0x4b0000
File size:	1189376 bytes
MD5 hash:	C5CA6BF1A4D668ABAE8A1BD58DA7FA89
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Reputation:	low

Analysis Process: schtasks.exe PID: **3736**, Parent PID: **3260**

General	
Target ID:	13
Start time:	12:43:00
Start date:	01/10/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\JLsbuY" /XML "C:\Users\user\AppData\Local\Temp\tmp2889.tmp
Imagebase:	0x10a0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **920**, Parent PID: **1680**

General	
Target ID:	14
Start time:	12:43:01
Start date:	01/10/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\JLsbuY" /XML "C:\Users\user\AppData\Local\Temp\tmp2B48.tmp
Imagebase:	0x10a0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **4748**, Parent PID: **3736**

General	
Target ID:	15
Start time:	12:43:01
Start date:	01/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **2220**, Parent PID: **920**

General	
Target ID:	16
Start time:	12:43:01

Start date:	01/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe PID: **5000**, Parent PID: **3260**

General

Target ID:	17
Start time:	12:43:02
Start date:	01/10/2022
Path:	C:\Users\user\Desktop\APPLICATION FORM MASTER SDPO Brilinskiy NEW U.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x9c0000
File size:	1189376 bytes
MD5 hash:	C5CA6BF1A4D668ABAE8A1BD58DA7FA89
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.500556457.0000000003E59000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.500556457.0000000003E59000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000011.00000002.500556457.0000000003E59000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.497822993.0000000002E51000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.497822993.0000000002E51000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000011.00000002.497822993.0000000002E51000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Analysis Process: dhcpmon.exe PID: **1276**, Parent PID: **1680**

General

Target ID:	18
Start time:	12:43:02
Start date:	01/10/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xce0000
File size:	1189376 bytes
MD5 hash:	C5CA6BF1A4D668ABAE8A1BD58DA7FA89
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.502379246.0000000003271000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.502379246.0000000003271000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000012.00000002.502379246.0000000003271000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Analysis Process: schtasks.exe PID: **5716**, Parent PID: **2068**

General	
Target ID:	19
Start time:	12:43:15
Start date:	01/10/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\JLsbuY" /XML "C:\Users\user\AppData\Local\Temp\tmp63CD.tmp
Imagebase:	0x10a0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **4616**, Parent PID: **5716**

General	
Target ID:	20
Start time:	12:43:16
Start date:	01/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: **2760**, Parent PID: **2068**

General	
Target ID:	21
Start time:	12:43:18
Start date:	01/10/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x4f0000
File size:	1189376 bytes
MD5 hash:	C5CA6BF1A4D668ABAE8A1BD58DA7FA89
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Disassembly

No disassembly

Copyright Joe Security LLC 2022