ID: 357424
Sample Name:
Y5XyMnx8Ng.exe
Cookbook: default.jbs
Time: 16:08:49
Date: 24/02/2021
Version: 31.0.0 Emerald

Table of Contents

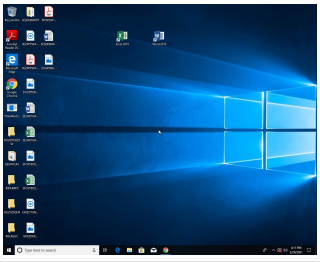
Analysis Report Y5XyMnx8Ng.exe

Overview

General Information

Sample Name:	Y5XyMnx8Ng.exe
Analysis ID:	357424
MD5:	5bd6a6dbda26ad..
SHA1:	20d05385be3621..
SHA256:	205f2ef71a4a099..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

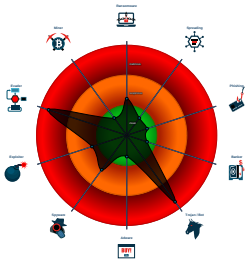
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Connects to many ports of the same…
- Hides that the sample has been dow…

Classification



Startup

- **System is w10x64**
- Y5XyMnx8Ng.exe (PID: 6372 cmdline: 'C:\Users\user\Desktop\Y5XyMnx8Ng.exe' MD5: 5BD6A6DBDA26ADA813C6F60FDFC7BA70)
  - schtasks.exe (PID: 5812 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\LbSNAHQmeXYAoG' /XML 'C:\Users\user\AppData\Local\Temp\tmp8EF2.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3180 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 5464 cmdline: {path} MD5: 71369277D09DA0830C8C59F9E22BB23A)
    - schtasks.exe (PID: 6292 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp3911.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6036 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6352 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp3C8D.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 1968 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegSvcs.exe (PID: 6384 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe 0 MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 2172 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 6200 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 5828 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 6404 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 5680 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "572eb7a9-aedf-4b39-8669-f7563dab8a38",
  "Group": "GREAT",
  "Domain1": "strongodss.ddns.net",
  "Domain2": "79.134.225.43",
  "Port": 58103,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Enable",
  "SetCriticalProcess": "Enable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Enable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8009,
  "BufferSize": "02000100",
  "MaxPacketSize": "",
  "GCThreshold": "",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.494335612.000000000571 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
00000008.00000002.494335612.000000000571 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
00000008.00000002.494335612.000000000571 0000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000008.00000002.483906093.000000000040 2000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000008.00000002.483906093.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 20 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.RegSvcs.exe.3bcec9e.5.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x4083:$x1: NanoCore.ClientPluginHost
8.2.RegSvcs.exe.3bcec9e.5.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x4083:$x2: NanoCore.ClientPluginHost • 0x4161:$s4: PipeCreated • 0x409d:$s5: IClientLoggingHost
8.2.RegSvcs.exe.2b91488.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x40c2:$x1: NanoCore.ClientPluginHost
8.2.RegSvcs.exe.2b91488.3.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x40c2:$x2: NanoCore.ClientPluginHost • 0x41a0:$s4: PipeCreated • 0x40dc:$s5: IClientLoggingHost
8.2.RegSvcs.exe.5700000.9.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1646:$x1: NanoCore.ClientPluginHost

Click to see the 42 entries

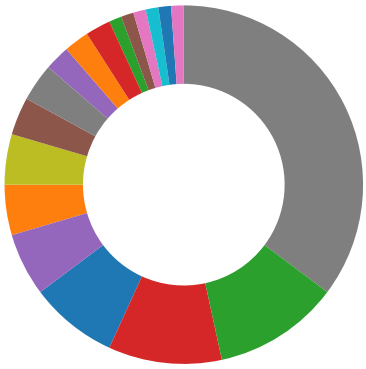
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Uses new MSVCR Dlls

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

Networking:

C2 URLs / IPs found in malware configuration

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

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

Operating System Destruction:

Protects its processes via BreakOnTermination flag

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM_3

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

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

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

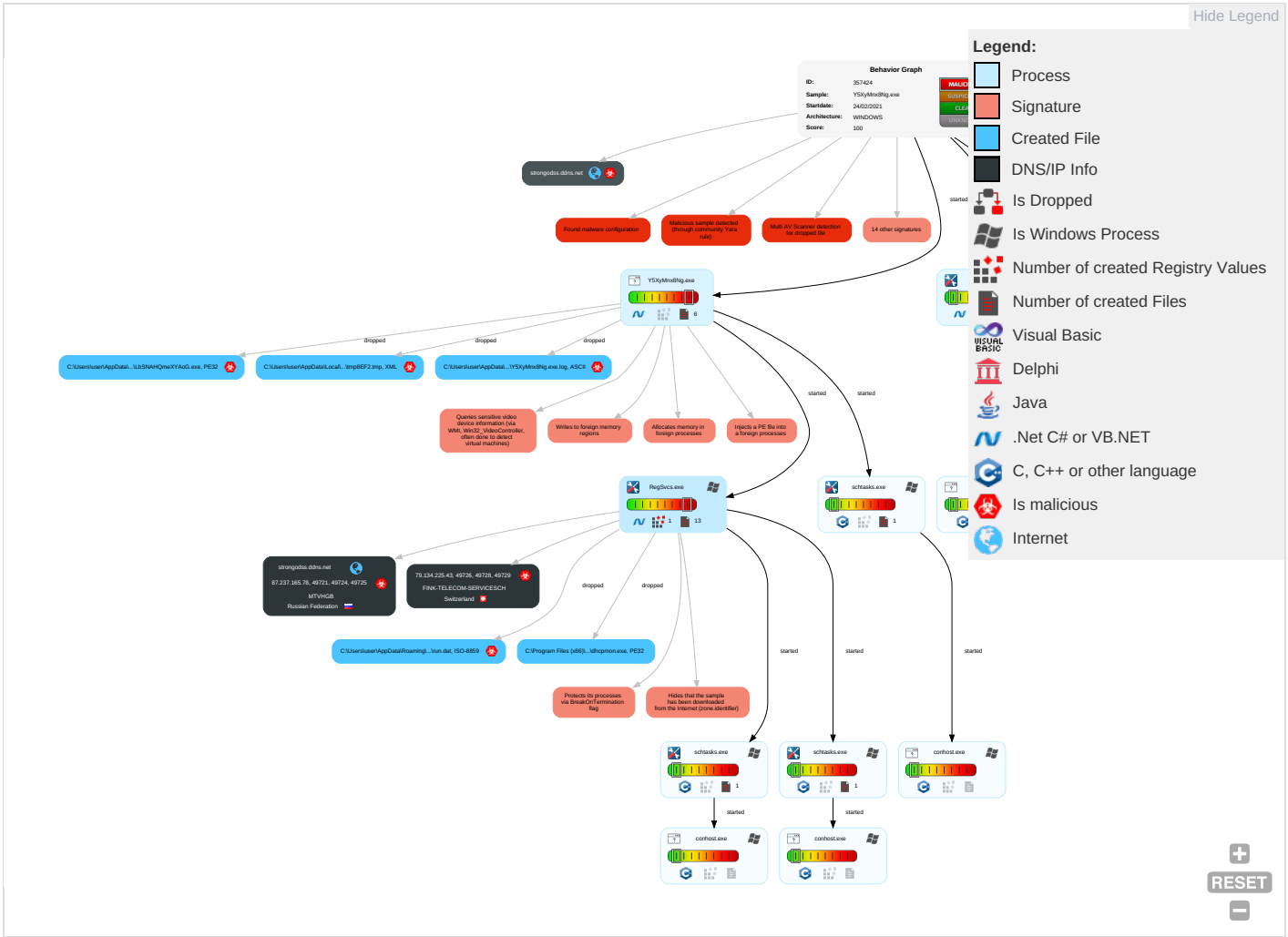
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1	Input Capture 2 1	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Process Injection 3 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 3	Security Account Manager	System Information Discovery 1 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Security Software Discovery 3 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 2	LSA Secrets	Virtualization/Sandbox Evasion 1 3	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3	Cached Domain Credentials	Process Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 3 1 2	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

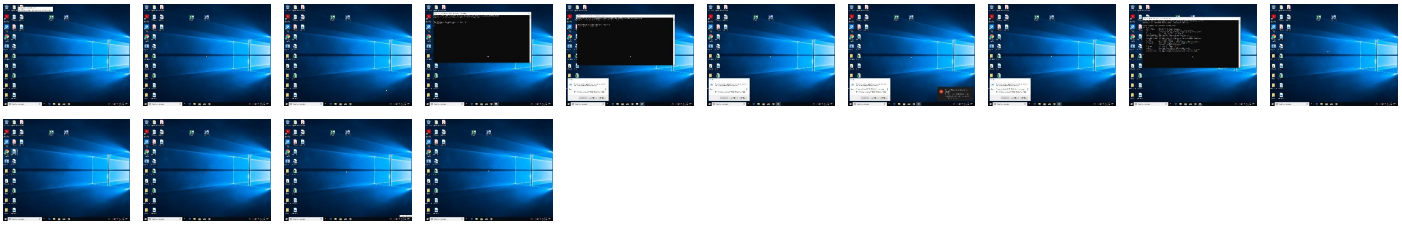
Behavior Graph



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
Y5XyMnx8Ng.exe	25%	Virustotal		Browse
Y5XyMnx8Ng.exe	38%	ReversingLabs	Win32.Trojan.Wacatac	
Y5XyMnx8Ng.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\LbSNAHQmeXYAoG.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\LbSNAHQmeXYAoG.exe	38%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.2.RegSvcs.exe.5710000.11.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/staff/dennis.htm:	0%	Avira URL Cloud	safe	
79.134.225.43	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.urwpp.de.h	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htmA	0%	Avira URL Cloud	safe	
http://www.fontbureau.comtu9	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comafV	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/8V	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ch	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.com.TTFt	0%	Avira URL Cloud	safe	
http://www.urwpp.delarKh	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdoVu	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/)	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.fontbureau.comalsdpV	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/u:	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/u9	0%	Avira URL Cloud	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/nt	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.tiro.como	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/3VY	0%	Avira URL Cloud	safe	
http://www.fontbureau.co	0%	Avira URL Cloud	safe	
http://www.urwpp.deF	0%	Avira URL Cloud	safe	
http://www.fontbureau.comJVR	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdaJVR	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.comTTFd	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
strongodss.ddns.net	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.fontbureau.comoVu	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comoitu	0%	URL Reputation	safe	
http://www.fontbureau.comoitu	0%	URL Reputation	safe	
http://www.fontbureau.comoitu	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/oVu	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
strongodss.ddns.net	87.237.165.78	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
79.134.225.43	true	• Avira URL Cloud: safe	unknown
strongodss.ddns.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

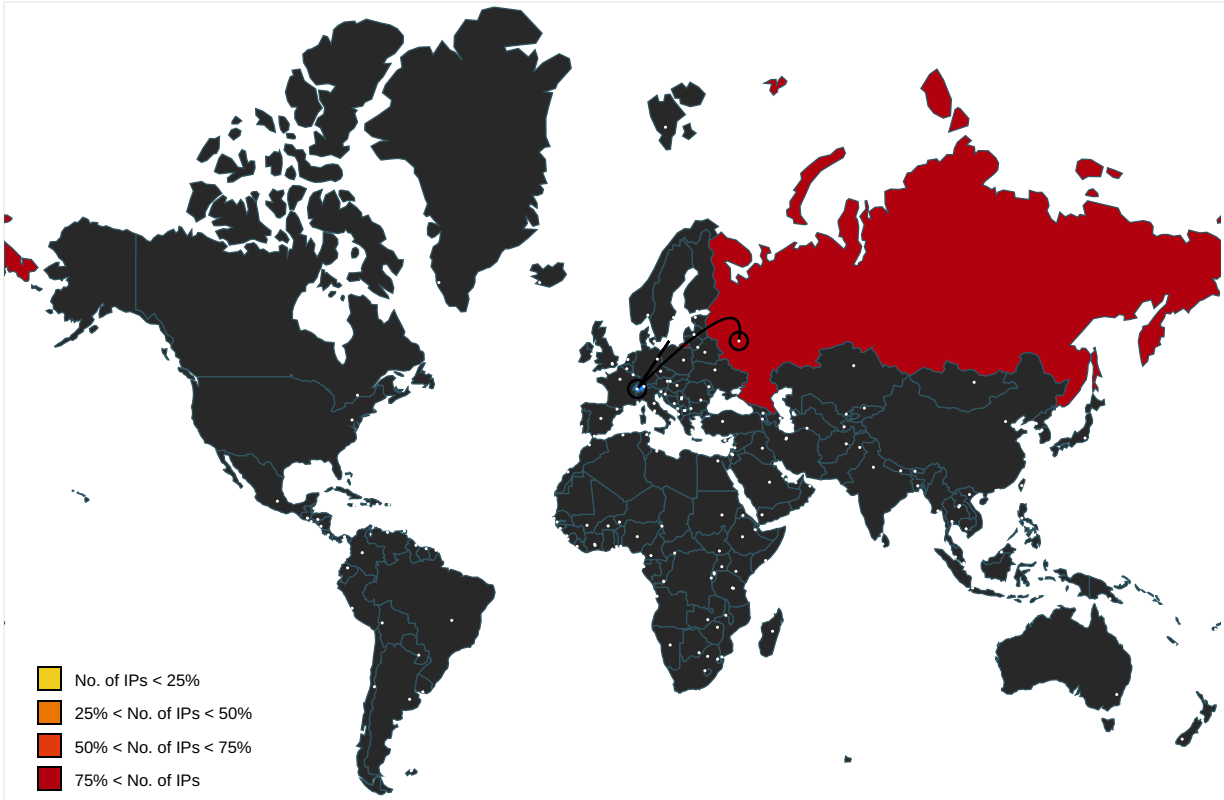
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm:	Y5XyMnx8Ng.exe, 00000000.00000003.226090976.0000000004FBA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	Y5XyMnx8Ng.exe, 00000000.00000003.221121855.0000000004FD9000.00000004.00000001.sdmp, Y5XyMnx8Ng.exe, 00000000.00000002.275100610.0000000005290000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	Y5XyMnx8Ng.exe, 00000000.00000002.275100610.0000000005290000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Y5XyMnx8Ng.exe, 00000000.00000002.275100610.0000000005290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.de.h	Y5XyMnx8Ng.exe, 00000000.00000003.222528263.0000000004FAE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htmA	Y5XyMnx8Ng.exe, 00000000.00000003.225264485.0000000004FD9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	Y5XyMnx8Ng.exe, 00000000.00000002.275100610.0000000005290000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comtu9	Y5XyMnx8Ng.exe, 00000000.00000003.222028980.0000000004FAC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html.	Y5XyMnx8Ng.exe, 00000000.00000003.221561815.0000000004FAF000.00000004.00000001.sdmp	false		high
http://www.tiro.com	Y5XyMnx8Ng.exe, 00000000.00000002.275100610.0000000005290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Y5XyMnx8Ng.exe, 00000000.00000002.275100610.0000000005290000.00000002.00000001.sdmp, Y5XyMnx8Ng.exe, 00000000.00000003.222322158.0000000004FD9000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	Y5XyMnx8Ng.exe, 00000000.00000002.275100610.0000000005290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersP	Y5XyMnx8Ng.exe, 00000000.00000003.221047138.0000000004FD9000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comafV	Y5XyMnx8Ng.exe, 00000000.00000002.274744752.0000000004FAA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/8V	Y5XyMnx8Ng.exe, 00000000.00000003.218561435.0000000004FA3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	Y5XyMnx8Ng.exe, 00000000.00000002.275100610.0000000005290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersi	Y5XyMnx8Ng.exe, 00000000.00000003.230715828.0000000004FD9000.00000004.00000001.sdmp	false		high
http://www.typography.netD	Y5XyMnx8Ng.exe, 00000000.00000002.275100610.0000000005290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Y5XyMnx8Ng.exe, 00000000.00000002.275100610.0000000005290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Y5XyMnx8Ng.exe, 00000000.00000002.275100610.0000000005290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/ch	Y5XyMnx8Ng.exe, 00000000.00000003.218060578.0000000004FAD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	Y5XyMnx8Ng.exe, 00000000.00000002.275100610.0000000005290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com.TTFt	Y5XyMnx8Ng.exe, 00000000.00000003.222347558.0000000004FAF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.delarKh	Y5XyMnx8Ng.exe, 00000000.00000003.222528263.0000000004FAE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersb	Y5XyMnx8Ng.exe, 00000000.00000003.222477602.0000000004FD9000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comdoVu	Y5XyMnx8Ng.exe, 00000000.00000003.221561815.0000000004FAF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	Y5XyMnx8Ng.exe, 00000000.00000002.275100610.0000000005290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/)	Y5XyMnx8Ng.exe, 00000000.00000003.218060578.0000000004FAD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	Y5XyMnx8Ng.exe, 00000000.00000003.218561435.0000000004FA3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comalsdpV	Y5XyMnx8Ng.exe, 00000000.00000003.222347558.0000000004FAF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	Y5XyMnx8Ng.exe, 00000000.00000002.275100610.0000000005290000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/u:	Y5XyMnx8Ng.exe, 00000000.00000003.216954032.0000000004FD9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kr	Y5XyMnx8Ng.exe, 00000000.00000002.275100610.0000000005290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Y5XyMnx8Ng.exe, 00000000.00000002.275100610.0000000005290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/u9	Y5XyMnx8Ng.exe, 00000000.00000003.216885369.0000000004FDF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.de	Y5XyMnx8Ng.exe, 00000000.00000003.222528263.0000000004FAE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Y5XyMnx8Ng.exe, 00000000.00000002.275100610.0000000005290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersp	Y5XyMnx8Ng.exe, 00000000.00000003.220778598.0000000004FD9000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	Y5XyMnx8Ng.exe, 00000000.00000002.275100610.0000000005290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Y5XyMnx8Ng.exe, 00000000.00000002.275100610.0000000005290000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	Y5XyMnx8Ng.exe, 00000000.00000002.275100610.0000000005290000.00000002.00000001.sdmp	false		high
http://www.galapagosdesign.com/	Y5XyMnx8Ng.exe, 00000000.00000003.225264485.0000000004FD9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/nt	Y5XyMnx8Ng.exe, 00000000.00000003.218060578.0000000004FAD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comF	Y5XyMnx8Ng.exe, 00000000.00000003.222028980.0000000004FAC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlo	Y5XyMnx8Ng.exe, 00000000.00000003.222028980.0000000004FAC000.00000004.00000001.sdmp	false		high
http://www.tiro.como	Y5XyMnx8Ng.exe, 00000000.00000003.216954032.0000000004FD9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/3VY	Y5XyMnx8Ng.exe, 00000000.00000003.218142700.0000000004FAD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.co	Y5XyMnx8Ng.exe, 00000000.00000003.221812778.0000000004FD9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deF	Y5XyMnx8Ng.exe, 00000000.00000003.222528263.0000000004FAE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comJVR	Y5XyMnx8Ng.exe, 00000000.00000003.222347558.0000000004FAF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comdaJVR	Y5XyMnx8Ng.exe, 00000000.00000003.221561815.0000000004FAF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	Y5XyMnx8Ng.exe, 00000000.00000003.218561435.0000000004FA3000.00000004.00000001.sdmp, Y5XyMnx8Ng.exe, 00000000.00000003.218681710.0000000004FAC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comTTFd	Y5XyMnx8Ng.exe, 00000000.00000003.222528263.0000000004FAE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comd	Y5XyMnx8Ng.exe, 00000000.00000003.221561815.0000000004FAF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	Y5XyMnx8Ng.exe, 00000000.00000002.275100610.0000000005290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comoVu	Y5XyMnx8Ng.exe, 00000000.00000003.222347558.0000000004FAF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/	Y5XyMnx8Ng.exe, 00000000.00000003.217090225.0000000004FE0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Y5XyMnx8Ng.exe, 00000000.00000002.275100610.0000000005290000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	Y5XyMnx8Ng.exe, 00000000.00000002.275100610.0000000005290000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Y5XyMnx8Ng.exe, 00000000.00000002.275100610.0000000005290000.00000002.00000001.sdmp, Y5XyMnx8Ng.exe, 00000000.00000003.221423345.0000000004FD9000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comoitu	Y5XyMnx8Ng.exe, 00000000.00000003.222347558.0000000004FAF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/oVu	Y5XyMnx8Ng.exe, 00000000.00000003.217807198.0000000004FA3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/s	Y5XyMnx8Ng.exe, 00000000.00000003.218171595.0000000004FA8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	Y5XyMnx8Ng.exe, 00000000.00000003.222028980.0000000004FAC000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers$	Y5XyMnx8Ng.exe, 00000000.00000003.221812778.0000000004FD9000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comm	Y5XyMnx8Ng.exe, 00000000.00000003.222347558.0000000004FAF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	Y5XyMnx8Ng.exe, 00000000.00000002.275100610.0000000005290000.00000002.00000001.sdmp, Y5XyMnx8Ng.exe, 00000000.00000003.218060578.0000000004FAD000.00000004.00000001.sdmp, Y5XyMnx8Ng.exe, 00000000.00000003.218561435.0000000004FA3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers9	Y5XyMnx8Ng.exe, 00000000.00000003.230809390.0000000004FD9000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers8	Y5XyMnx8Ng.exe, 00000000.00000002.275100610.0000000005290000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comdsed	Y5XyMnx8Ng.exe, 00000000.00000003.222028980.0000000004FAC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/nly	Y5XyMnx8Ng.exe, 00000000.00000003.218060578.0000000004FAD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/	Y5XyMnx8Ng.exe, 00000000.00000003.220682724.0000000004FD9000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/JVR	Y5XyMnx8Ng.exe, 00000000.00000003.218171595.0000000004FA8000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers2	Y5XyMnx8Ng.exe, 00000000.00000003.221121855.0000000004FD9000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
87.237.165.78	unknown	Russian Federation		49967	MTVHGB	true
79.134.225.43	unknown	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	357424
Start date:	24.02.2021
Start time:	16:08:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Y5XyMnx8Ng.exe

Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	40
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@18/13@11/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.1% (good quality ratio 1.5%) • Quality average: 51.1% • Quality standard deviation: 38%
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 2.22.152.11, 52.147.198.201, 204.79.197.200, 13.107.21.200, 104.42.151.234, 13.88.21.125, 23.54.113.53, 23.54.113.104, 51.104.139.180, 23.0.174.187, 23.0.174.185, 51.11.168.160, 23.10.249.25, 23.10.249.26, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, storeedgefd.xbetservices.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, storeedgefd.dsx.mp.microsoft.com, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, e16646.dscg.akamaiedge.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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
16:09:50	API Interceptor	1x Sleep call for process: Y5XyMnx8Ng.exe modified
16:10:10	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe" s>$(Arg0)
16:10:11	API Interceptor	811x Sleep call for process: RegSvcs.exe modified
16:10:13	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
16:10:13	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
87.237.165.78	YoWPu2BQzA9FeDd.exe	Get hash	malicious	Browse	
	M5QDAaK9yM.exe	Get hash	malicious	Browse	
	TdX45jQWjj.exe	Get hash	malicious	Browse	
79.134.225.43	YoWPu2BQzA9FeDd.exe	Get hash	malicious	Browse	
	TdX45jQWjj.exe	Get hash	malicious	Browse	
	JfRbEbUkpV39K4L.exe	Get hash	malicious	Browse	
	Dachser Consulta de cliente saliente no. 000150849 - SKBMT03082020-0012-IMG0149.exe	Get hash	malicious	Browse	
	290453721.xls	Get hash	malicious	Browse	
	nUo0FukkVO.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
strongodss.ddns.net	YoWPu2BQzA9FeDd.exe	Get hash	malicious	Browse	• 87.237.165.78
	M5QDAaK9yM.exe	Get hash	malicious	Browse	• 87.237.165.78
	TdX45jQWjj.exe	Get hash	malicious	Browse	• 87.237.165.78

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MTVHGB	YoWPu2BQzA9FeDd.exe	Get hash	malicious	Browse	• 87.237.165.78
	M5QDAaK9yM.exe	Get hash	malicious	Browse	• 87.237.165.78
	TdX45jQWjj.exe	Get hash	malicious	Browse	• 87.237.165.78
	QUOTATION 19 01 2021.exe	Get hash	malicious	Browse	• 87.237.165.162
FINK-TELECOM-SERVICESCH	YoWPu2BQzA9FeDd.exe	Get hash	malicious	Browse	• 79.134.225.43
	xF7GogN7tM.exe	Get hash	malicious	Browse	• 79.134.225.120
	TZgGVyMJYF.exe	Get hash	malicious	Browse	• 79.134.225.74
	ilpbALnKbE.exe	Get hash	malicious	Browse	• 79.134.225.103
	Documents.exe	Get hash	malicious	Browse	• 79.134.225.87
	SWcNyi2YBj.exe	Get hash	malicious	Browse	• 79.134.225.103
	Confirmation Transfer Note Ref Number0002636.exe	Get hash	malicious	Browse	• 79.134.225.8
	TdX45jQWjj.exe	Get hash	malicious	Browse	• 79.134.225.43
	e92b274943f4a3a557881ee0dd57772d.exe	Get hash	malicious	Browse	• 79.134.225.105
	WxTm2cWLHF.exe	Get hash	malicious	Browse	• 79.134.225.71
	Payment Confirmation.exe	Get hash	malicious	Browse	• 79.134.225.30
	rjHlt1zz28.exe	Get hash	malicious	Browse	• 79.134.225.49
	Deadly Variants of Covid 19.doc	Get hash	malicious	Browse	• 79.134.225.49
	document.exe	Get hash	malicious	Browse	• 79.134.225.122
	5293ea9467ea45e928620a5ed74440f5.exe	Get hash	malicious	Browse	• 79.134.225.105
	f1a14e6352036833f1c109e1bb2934f2.exe	Get hash	malicious	Browse	• 79.134.225.105
	256ec8f8f67b59c5e085b0bb63afcd13.exe	Get hash	malicious	Browse	• 79.134.225.105
	JOIN.exe	Get hash	malicious	Browse	• 79.134.225.30
	Delivery pdf.exe	Get hash	malicious	Browse	• 79.134.225.25
	d88e07467ddcf9e3b19fa972b9f000d1.exe	Get hash	malicious	Browse	• 79.134.225.105

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	receipt.exe	Get hash	malicious	Browse	
	YoWPu2BQzA9FeDd.exe	Get hash	malicious	Browse	
	M5QDAaK9yM.exe	Get hash	malicious	Browse	
	oMWv1Zof2y.exe	Get hash	malicious	Browse	
	TdX45jQWjj.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	QTxFuxF5NQ.exe	Get hash	malicious	Browse	
	a34b93ef-dea2-45f8-a5bf-4f6b0b5291c7.exe	Get hash	malicious	Browse	
	3fcd8c19-af88-4cd9-87e7-0bfea1de01a1.exe	Get hash	malicious	Browse	
	Vietnam Order.exe	Get hash	malicious	Browse	
	Dhl Shipping Document.exe	Get hash	malicious	Browse	
	PO-WJO-001, pdf.exe	Get hash	malicious	Browse	
	byWuWAR5FD.exe	Get hash	malicious	Browse	
	parcel_images.exe	Get hash	malicious	Browse	
	0712020.exe	Get hash	malicious	Browse	
	JfRbEbUkpV39K4L.exe	Get hash	malicious	Browse	
	DECEMBER QUOTATION REQUEST FOR FR12007POH0008_PO0000143_ETQ.exe	Get hash	malicious	Browse	
	DECEMBER QUOTATION REQUEST FOR FR12007POH0008_PO0000143_ETQ.exe	Get hash	malicious	Browse	
	zC3edqmNNt.exe	Get hash	malicious	Browse	
	Shipping Document.pdf..exe	Get hash	malicious	Browse	
	PPR & CPR_HEA_DECEMBER 4 2020.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	3.7515815714465193
Encrypted:	false
SSDEEP:	384:BOj9Y8/gS7SDriLGKq1MHR5U4Ag6ihJSxUCR1rgCPKabK2t0X5P7DZ+JgWSW72uw:B+gSAdN1MH3HAFRJngW2u
MD5:	71369277D09DA0830C8C59F9E22BB23A
SHA1:	37F9781314F0F6B7E9CB529A573F2B1C8DE9E93F
SHA-256:	D4527B7AD2FC4778CC5BE8709C95AEA44EAC0568B367EE14F7357D72898C3698
SHA-512:	2F470383E3C796C4CF212EC280854DBB9E7E8C8010CE6857E58F8E7066D7516B7CD7039BC5C0F547E1F5C7F9F2287869ADFFB2869800B08B2982A88BE96E9FB
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: receipt.exe, Detection: malicious, Browse • Filename: YoWPu2BQzA9FeDd.exe, Detection: malicious, Browse • Filename: M5QDAaK9yM.exe, Detection: malicious, Browse • Filename: oMWv1Zof2y.exe, Detection: malicious, Browse • Filename: TdX45jQWjj.exe, Detection: malicious, Browse • Filename: QTxFuxF5NQ.exe, Detection: malicious, Browse • Filename: a34b93ef-dea2-45f8-a5bf-4f6b0b5291c7.exe, Detection: malicious, Browse • Filename: 3fcd8c19-af88-4cd9-87e7-0bfea1de01a1.exe, Detection: malicious, Browse • Filename: Vietnam Order.exe, Detection: malicious, Browse • Filename: Dhl Shipping Document.exe, Detection: malicious, Browse • Filename: PO-WJO-001, pdf.exe, Detection: malicious, Browse • Filename: byWuWAR5FD.exe, Detection: malicious, Browse • Filename: parcel_images.exe, Detection: malicious, Browse • Filename: 0712020.exe, Detection: malicious, Browse • Filename: JfRbEbUkpV39K4L.exe, Detection: malicious, Browse • Filename: DECEMBER QUOTATION REQUEST FOR FR12007POH0008_PO0000143_ETQ.exe, Detection: malicious, Browse • Filename: DECEMBER QUOTATION REQUEST FOR FR12007POH0008_PO0000143_ETQ.exe, Detection: malicious, Browse • Filename: zC3edqmNNt.exe, Detection: malicious, Browse • Filename: Shipping Document.pdf..exe, Detection: malicious, Browse • Filename: PPR & CPR_HEA_DECEMBER 4 2020.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....{Z.....P... .....k... .....@.. .....[.. ..@.....k..K..... k..... ....H.....text....K... ...P..... ..`.rsrc.....`.....@..@.rel oc.....p.....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RegSvcs.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	120
Entropy (8bit):	5.016405576253028
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RegSvcs.exe.log	
SSDEEP:	3:QHXMKaoWglAFXMWA2yTMGfsbNXLVd49Am12MFuAvOAsDeieVyn:Q3LawlAFXMWTyAGCFLIP12MUAvvrs
MD5:	50DEC1858E13F033E6DCA3CBFAD5E8DE
SHA1:	79AE1E9131B0FAF215B499D2F7B4C595AA120925
SHA-256:	14A557E226E3BA8620BB3A70035E1E316F1E9FB5C9E8F74C07110EE90B8D8AE4
SHA-512:	1BD73338DF685A5B57B0546E102ECFDEE65800410D6F77845E50456AC70DE72929088AF19B59647F01CBA7A5ACFB399C52D9EF2402A9451366586862EF88E7BF
Malicious:	false
Preview:	1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Y5XyMnx8Ng.exe.log	
Process:	C:\Users\user\Desktop\Y5XyMnx8Ng.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	655
Entropy (8bit):	5.273171405160065
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9t0U2WUXBQav:MLF20NaL329hJ5g522rWz2p29XBT
MD5:	2703120C370FBB4A8BA08C6D1754039E
SHA1:	EC0DB47BF00A4A828F796147619386C0BBEA66A1
SHA-256:	F95566974BC44F3A757CAFB1456D185D8F333AC84775089DE18310B90C18B1BC
SHA-512:	BC05A2A1BE5B122FC6D3DEA66EF4258522F13351B9754378395AAD019631E312CFD3BC990F3E3D5C7BB0BDBA1EAD54A2B34A96DEE2FCCD703721E98F6192EE48
Malicious:	**true**
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Management\4de99804c29261edb63c93616550f034\System.Management.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	120
Entropy (8bit):	5.016405576253028
Encrypted:	false
SSDEEP:	3:QHXMKaoWglAFXMWA2yTMGfsbNXLVd49Am12MFuAvOAsDeieVyn:Q3LawlAFXMWTyAGCFLIP12MUAvvrs
MD5:	50DEC1858E13F033E6DCA3CBFAD5E8DE
SHA1:	79AE1E9131B0FAF215B499D2F7B4C595AA120925
SHA-256:	14A557E226E3BA8620BB3A70035E1E316F1E9FB5C9E8F74C07110EE90B8D8AE4
SHA-512:	1BD73338DF685A5B57B0546E102ECFDEE65800410D6F77845E50456AC70DE72929088AF19B59647F01CBA7A5ACFB399C52D9EF2402A9451366586862EF88E7BF
Malicious:	false
Preview:	1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\tmp3911.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	5.135021273392143
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mn4xtn:cbk4oL600QydbQxlYODOLedq3Z4j
MD5:	40B11EF601FB28F9B2E69D36857BF2EC
SHA1:	B6454020AD2CEED193F4792B77001D0BD741B370
SHA-256:	C51E12D18CC664425F6711D8AE2507068884C7057092CFA11884100E1E9D49E1
SHA-512:	E3C5BCC714CBFCA4B8058DDCDDF231DCEFA69C15881CE3F8123E59ED45CFB5DA052B56E1945DCF8DC7F800D62F9A4EECB82BCA69A66A1530787AEFFEB15B2BD5
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\tmp3C8D.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <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\tmp8EF2.tmp	
Process:	C:\Users\user\Desktop\Y5XyMnx8Ng.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1647
Entropy (8bit):	5.20290519634611
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBwtn:cbh47TlNQ//rydbz9l3YODOLNdq3k
MD5:	E61FE83EB8C07A1076C95D63A2E9C7E8
SHA1:	C45541423ECB8762EE2F8DAAF34BABA2E9932BE0
SHA-256:	8B817FAE8E4FD7B9A5D2604048DC837FE26167B6E8C58EA18F7EF3F43BA638CF
SHA-512:	C405B90523CDCB4624D47DDEF092321756983C3FD14472E1F74509A1CCDB670925B1F8179021CCB6FCBF4FF0848E713347F7D58CE94C888F545D961E627F7777
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:TuXt:U
MD5:	CF402C854B880FB79472DA48A88A3E43
SHA1:	C8A90AC6594C04B69F33AF27F72CE9A150C3203D
SHA-256:	8221288A0BD2019F58D6583BADF7C0E3C921078EB6D9C7F5A35FD39A40FC0699
SHA-512:	D135A204BCD0303455CF17FA1CA13880E47011B793F80263164DABAC29F95537C409263AA2A1E57D8C2862F083CA52D4608852D3F2E08D9D2142A7EB2A7451A2
Malicious:	**true**
Preview:	..m.!..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.795707286467131
Encrypted:	false
SSDEEP:	3:oMty8WbSX/MNn:oMLWus
MD5:	D685103573539B7E9FDBF5F1D7DD96CE
SHA1:	4B2FE6B5C0B37954B314FCAEE1F12237A9B02D07

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
SHA-256:	D78BC23B0CA3EDDF52D56AB85CDC30A71B3756569CB32AA2F6C28DBC23C76E8E
SHA-512:	17769A5944E8929323A34269ABEEF0861D5C6799B0A27F5545FBFADC80E5AB684A471AD6F6A7FC623002385154EA89DE94013051E09120AB94362E542AB0F1DD
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe

C:\Users\user\AppData\Roaming\LbSNAHQmeXYAoG.exe	
Process:	C:\Users\user\Desktop\Y5XyMnx8Ng.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	790016
Entropy (8bit):	7.9432068049127045
Encrypted:	false
SSDEEP:	12288:wEd3LLUEMjhvUbJG16Kfd/b2ze6Mg5saYrwOnkG4WuCmcoevatwmWFoH8l/MM:3L0iG16KfdD6zsaykItmcoQatwmY8qr
MD5:	5BD6A6DBDA26ADA813C6F60FDFC7BA70
SHA1:	20D05385BE36213404CA178BF15E39D0587DD73F
SHA-256:	205F2EF71A4A099B8CAC6B0DF7BE7D04F5CA0C65E31FB1C00158F656CF2785C3
SHA-512:	DF3E138E62994C2E640EC4C2B4DDE795512D3D23ECFB49B932EED2DDC451A96447A9C9435E0C1E38D567B9523C02D906E20208DD49AC7D66C456701620362E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 38%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...4.5`.....0.....F''... ...@....@.. ..... ..@.....I..O....@.....`..... ....H.....text...L.... ....`.rsrc.....@.....@..@.rel oc.....`.....@..B.....("......H.....Ho...2.....4...,.....&.(.....*...0..9.....~.....,''.r...p.....(....o....s.....~.....+..*....0.....~.....+..*'' .....*.0..!.....(....rI..p~....o.....t.....+..*....0..!.....(....r1..p~....o.....t.....+..*....0.....r5..p.+..*..0.....rA..p.+..*''.(....*^..}.....(.....(%....**...(.....*..0..;.....rQ..pr...p.(.....,.. (.....+..s.....o.....(....*..0..I.....r...pr...p.(.....

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1145
Entropy (8bit):	4.462201512373672
Encrypted:	false
SSDEEP:	24:zKLXkzPDObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0zPDQntKKH1MqJC
MD5:	46EBEB88876A00A52CC37B1F8E0D0438
SHA1:	5E5DB352F964E5F398301662FF558BD905798A65
SHA-256:	D65BD5A6CC112838AFE8FA70BF61FD13C1313BCE3EE3E76C50E454D7B581238B
SHA-512:	E713E6F304A469FB71235C598BC7E2C6F8458ABC61DAF3D1F364F66579CAFA4A7F3023E585BDA552FB400009E7805A8CA0311A50D5EDC9C2AD2D067772A071E E
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 2.0.50727.8922..Copyright (c) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [optio ns] AssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target app lication, error if it already exists... /exapp Expect an existing application... /tlb:<tlbfile> Filename for the exported type library... /appname:<name> Use the specified name for the target application... /parname:<name> Use the specified name or id for the target partition... /extlb Use an existing type library... /rec onfig Reconfigure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /no logo Suppress logo output... /quiet Suppress logo output and success output...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.9432068049127045
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:	Y5XyMnx8Ng.exe
File size:	790016
MD5:	5bd6a6dbda26ada813c6f60fdfc7ba70

General

SHA1:	20d05385be36213404ca178bf15e39d0587dd73f
SHA256:	205f2ef71a4a099b8cac6b0df7be7d04f5ca0c65e31fb1c00158f656cf2785c3
SHA512:	df3e138e62994c2e640ec4c2b4dde795512d3d23ecfb49b 932eed2ddc451a96447a9c9435e0c1e38d567b9523c02 906e20208dd49ac7d66c456701620362e28
SSDEEP:	12288:wEd3LLUEMjhvUbJG16Kfd/b2ze6Mg5saYrwOnkG4WuCmcoevatwmWFoH8l/MM:3L0iG16KfdD6zsaykItmcoQatwmY8qr
File Content Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L...4.5`..............0.............F"... ...@....@.. ....@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4c2246
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6035AE34 [Wed Feb 24 01:39:00 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc21f4	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc4000	0x5b4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc6000	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	0xc024c	0xc0400	False	0.935183680104	data	7.94843846597	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc4000	0x5b4	0x600	False	0.431640625	data	4.21916130547	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc6000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xc4090	0x324	data		
RT_MANIFEST	0xc43c4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

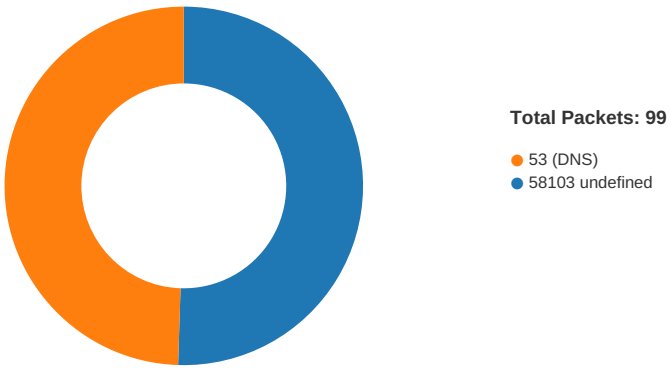
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2016
Assembly Version	4.0.0.0
InternalName	vSI.exe
FileVersion	4.0.0.0
CompanyName	
LegalTrademarks	

Description	Data
Comments	
ProductName	ITP_RMSS
ProductVersion	4.0.0.0
FileDescription	ITP_RMSS
OriginalFilename	vSI.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 16:10:12.533143997 CET	49721	58103	192.168.2.3	87.237.165.78
Feb 24, 2021 16:10:12.560343981 CET	58103	49721	87.237.165.78	192.168.2.3
Feb 24, 2021 16:10:13.123317957 CET	49721	58103	192.168.2.3	87.237.165.78
Feb 24, 2021 16:10:13.150600910 CET	58103	49721	87.237.165.78	192.168.2.3
Feb 24, 2021 16:10:13.757090092 CET	49721	58103	192.168.2.3	87.237.165.78
Feb 24, 2021 16:10:13.785631895 CET	58103	49721	87.237.165.78	192.168.2.3
Feb 24, 2021 16:10:19.076946020 CET	49724	58103	192.168.2.3	87.237.165.78
Feb 24, 2021 16:10:19.107546091 CET	58103	49724	87.237.165.78	192.168.2.3
Feb 24, 2021 16:10:19.651211023 CET	49724	58103	192.168.2.3	87.237.165.78
Feb 24, 2021 16:10:19.678690910 CET	58103	49724	87.237.165.78	192.168.2.3
Feb 24, 2021 16:10:20.257462025 CET	49724	58103	192.168.2.3	87.237.165.78
Feb 24, 2021 16:10:20.284785032 CET	58103	49724	87.237.165.78	192.168.2.3
Feb 24, 2021 16:10:24.380441904 CET	49725	58103	192.168.2.3	87.237.165.78
Feb 24, 2021 16:10:24.409280062 CET	58103	49725	87.237.165.78	192.168.2.3
Feb 24, 2021 16:10:25.047492027 CET	49725	58103	192.168.2.3	87.237.165.78
Feb 24, 2021 16:10:25.074667931 CET	58103	49725	87.237.165.78	192.168.2.3
Feb 24, 2021 16:10:25.656824112 CET	49725	58103	192.168.2.3	87.237.165.78
Feb 24, 2021 16:10:25.684272051 CET	58103	49725	87.237.165.78	192.168.2.3
Feb 24, 2021 16:10:29.727997065 CET	49726	58103	192.168.2.3	79.134.225.43
Feb 24, 2021 16:10:29.760649920 CET	58103	49726	79.134.225.43	192.168.2.3
Feb 24, 2021 16:10:30.268054962 CET	49726	58103	192.168.2.3	79.134.225.43
Feb 24, 2021 16:10:30.301914930 CET	58103	49726	79.134.225.43	192.168.2.3
Feb 24, 2021 16:10:30.813908100 CET	49726	58103	192.168.2.3	79.134.225.43
Feb 24, 2021 16:10:30.846590996 CET	58103	49726	79.134.225.43	192.168.2.3
Feb 24, 2021 16:10:34.955918074 CET	49728	58103	192.168.2.3	79.134.225.43
Feb 24, 2021 16:10:34.988707066 CET	58103	49728	79.134.225.43	192.168.2.3
Feb 24, 2021 16:10:35.579500914 CET	49728	58103	192.168.2.3	79.134.225.43
Feb 24, 2021 16:10:35.612328053 CET	58103	49728	79.134.225.43	192.168.2.3
Feb 24, 2021 16:10:36.282670975 CET	49728	58103	192.168.2.3	79.134.225.43
Feb 24, 2021 16:10:36.315766096 CET	58103	49728	79.134.225.43	192.168.2.3
Feb 24, 2021 16:10:40.331837893 CET	49729	58103	192.168.2.3	79.134.225.43

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 16:10:40.364761114 CET	58103	49729	79.134.225.43	192.168.2.3
Feb 24, 2021 16:10:40.876931906 CET	49729	58103	192.168.2.3	79.134.225.43
Feb 24, 2021 16:10:40.914079905 CET	58103	49729	79.134.225.43	192.168.2.3
Feb 24, 2021 16:10:41.423758984 CET	49729	58103	192.168.2.3	79.134.225.43
Feb 24, 2021 16:10:41.456362009 CET	58103	49729	79.134.225.43	192.168.2.3
Feb 24, 2021 16:10:45.681472063 CET	49730	58103	192.168.2.3	87.237.165.78
Feb 24, 2021 16:10:45.710315943 CET	58103	49730	87.237.165.78	192.168.2.3
Feb 24, 2021 16:10:46.221097946 CET	49730	58103	192.168.2.3	87.237.165.78
Feb 24, 2021 16:10:46.248971939 CET	58103	49730	87.237.165.78	192.168.2.3
Feb 24, 2021 16:10:46.752454042 CET	49730	58103	192.168.2.3	87.237.165.78
Feb 24, 2021 16:10:46.782939911 CET	58103	49730	87.237.165.78	192.168.2.3
Feb 24, 2021 16:10:50.995347977 CET	49731	58103	192.168.2.3	87.237.165.78
Feb 24, 2021 16:10:51.022494078 CET	58103	49731	87.237.165.78	192.168.2.3
Feb 24, 2021 16:10:51.533984900 CET	49731	58103	192.168.2.3	87.237.165.78
Feb 24, 2021 16:10:51.561500072 CET	58103	49731	87.237.165.78	192.168.2.3
Feb 24, 2021 16:10:52.065284967 CET	49731	58103	192.168.2.3	87.237.165.78
Feb 24, 2021 16:10:52.093585014 CET	58103	49731	87.237.165.78	192.168.2.3
Feb 24, 2021 16:10:56.166809082 CET	49732	58103	192.168.2.3	87.237.165.78
Feb 24, 2021 16:10:56.195791960 CET	58103	49732	87.237.165.78	192.168.2.3
Feb 24, 2021 16:10:56.706290960 CET	49732	58103	192.168.2.3	87.237.165.78
Feb 24, 2021 16:10:56.736602068 CET	58103	49732	87.237.165.78	192.168.2.3
Feb 24, 2021 16:10:57.237741947 CET	49732	58103	192.168.2.3	87.237.165.78
Feb 24, 2021 16:10:57.264682055 CET	58103	49732	87.237.165.78	192.168.2.3
Feb 24, 2021 16:11:01.270438910 CET	49739	58103	192.168.2.3	79.134.225.43
Feb 24, 2021 16:11:01.303239107 CET	58103	49739	79.134.225.43	192.168.2.3
Feb 24, 2021 16:11:01.816044092 CET	49739	58103	192.168.2.3	79.134.225.43
Feb 24, 2021 16:11:01.848630905 CET	58103	49739	79.134.225.43	192.168.2.3
Feb 24, 2021 16:11:02.362986088 CET	49739	58103	192.168.2.3	79.134.225.43
Feb 24, 2021 16:11:02.396814108 CET	58103	49739	79.134.225.43	192.168.2.3
Feb 24, 2021 16:11:06.429452896 CET	49740	58103	192.168.2.3	79.134.225.43
Feb 24, 2021 16:11:06.463603020 CET	58103	49740	79.134.225.43	192.168.2.3
Feb 24, 2021 16:11:06.972877026 CET	49740	58103	192.168.2.3	79.134.225.43
Feb 24, 2021 16:11:07.007544994 CET	58103	49740	79.134.225.43	192.168.2.3
Feb 24, 2021 16:11:07.519614935 CET	49740	58103	192.168.2.3	79.134.225.43
Feb 24, 2021 16:11:07.552390099 CET	58103	49740	79.134.225.43	192.168.2.3
Feb 24, 2021 16:11:11.568758011 CET	49746	58103	192.168.2.3	79.134.225.43
Feb 24, 2021 16:11:11.601488113 CET	58103	49746	79.134.225.43	192.168.2.3
Feb 24, 2021 16:11:12.114870071 CET	49746	58103	192.168.2.3	79.134.225.43
Feb 24, 2021 16:11:12.147849083 CET	58103	49746	79.134.225.43	192.168.2.3
Feb 24, 2021 16:11:12.662959099 CET	49746	58103	192.168.2.3	79.134.225.43
Feb 24, 2021 16:11:12.696906090 CET	58103	49746	79.134.225.43	192.168.2.3
Feb 24, 2021 16:11:16.757277012 CET	49747	58103	192.168.2.3	87.237.165.78
Feb 24, 2021 16:11:16.785811901 CET	58103	49747	87.237.165.78	192.168.2.3
Feb 24, 2021 16:11:17.302103043 CET	49747	58103	192.168.2.3	87.237.165.78
Feb 24, 2021 16:11:17.331185102 CET	58103	49747	87.237.165.78	192.168.2.3
Feb 24, 2021 16:11:17.833460093 CET	49747	58103	192.168.2.3	87.237.165.78
Feb 24, 2021 16:11:17.860521078 CET	58103	49747	87.237.165.78	192.168.2.3
Feb 24, 2021 16:11:21.924900055 CET	49748	58103	192.168.2.3	87.237.165.78
Feb 24, 2021 16:11:21.952218056 CET	58103	49748	87.237.165.78	192.168.2.3
Feb 24, 2021 16:11:22.458440065 CET	49748	58103	192.168.2.3	87.237.165.78
Feb 24, 2021 16:11:22.485619068 CET	58103	49748	87.237.165.78	192.168.2.3
Feb 24, 2021 16:11:22.989789009 CET	49748	58103	192.168.2.3	87.237.165.78
Feb 24, 2021 16:11:23.018168926 CET	58103	49748	87.237.165.78	192.168.2.3
Feb 24, 2021 16:11:27.147738934 CET	49756	58103	192.168.2.3	87.237.165.78
Feb 24, 2021 16:11:27.175889969 CET	58103	49756	87.237.165.78	192.168.2.3
Feb 24, 2021 16:11:27.677603006 CET	49756	58103	192.168.2.3	87.237.165.78
Feb 24, 2021 16:11:27.705015898 CET	58103	49756	87.237.165.78	192.168.2.3
Feb 24, 2021 16:11:28.208844900 CET	49756	58103	192.168.2.3	87.237.165.78
Feb 24, 2021 16:11:28.237665892 CET	58103	49756	87.237.165.78	192.168.2.3
Feb 24, 2021 16:11:32.268532038 CET	49761	58103	192.168.2.3	79.134.225.43
Feb 24, 2021 16:11:32.301124096 CET	58103	49761	79.134.225.43	192.168.2.3
Feb 24, 2021 16:11:32.803134918 CET	49761	58103	192.168.2.3	79.134.225.43
Feb 24, 2021 16:11:32.835714102 CET	58103	49761	79.134.225.43	192.168.2.3
Feb 24, 2021 16:11:33.350023985 CET	49761	58103	192.168.2.3	79.134.225.43

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 16:11:33.382822990 CET	58103	49761	79.134.225.43	192.168.2.3
Feb 24, 2021 16:11:37.758483887 CET	49762	58103	192.168.2.3	79.134.225.43
Feb 24, 2021 16:11:37.791282892 CET	58103	49762	79.134.225.43	192.168.2.3
Feb 24, 2021 16:11:38.303525925 CET	49762	58103	192.168.2.3	79.134.225.43
Feb 24, 2021 16:11:38.336097002 CET	58103	49762	79.134.225.43	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 16:09:34.962903023 CET	58643	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:09:35.001048088 CET	53	58643	8.8.8.8	192.168.2.3
Feb 24, 2021 16:09:35.563812017 CET	60985	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:09:35.576246977 CET	53	60985	8.8.8.8	192.168.2.3
Feb 24, 2021 16:09:35.645147085 CET	56777	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:09:35.657057047 CET	53	56777	8.8.8.8	192.168.2.3
Feb 24, 2021 16:09:36.236988068 CET	50200	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:09:36.249538898 CET	53	50200	8.8.8.8	192.168.2.3
Feb 24, 2021 16:09:37.237097979 CET	51281	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:09:37.249413013 CET	53	51281	8.8.8.8	192.168.2.3
Feb 24, 2021 16:09:38.251844883 CET	49199	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:09:38.264933109 CET	53	49199	8.8.8.8	192.168.2.3
Feb 24, 2021 16:09:38.662730932 CET	50620	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:09:38.680517912 CET	53	50620	8.8.8.8	192.168.2.3
Feb 24, 2021 16:09:39.442451954 CET	64938	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:09:39.455857038 CET	53	64938	8.8.8.8	192.168.2.3
Feb 24, 2021 16:09:40.795653105 CET	60152	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:09:40.808948040 CET	53	60152	8.8.8.8	192.168.2.3
Feb 24, 2021 16:09:41.904604912 CET	57544	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:09:41.919425964 CET	53	57544	8.8.8.8	192.168.2.3
Feb 24, 2021 16:09:43.047470093 CET	55984	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:09:43.059814930 CET	53	55984	8.8.8.8	192.168.2.3
Feb 24, 2021 16:09:44.306821108 CET	64185	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:09:44.319124937 CET	53	64185	8.8.8.8	192.168.2.3
Feb 24, 2021 16:09:45.135375977 CET	65110	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:09:45.148333073 CET	53	65110	8.8.8.8	192.168.2.3
Feb 24, 2021 16:09:48.856286049 CET	58361	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:09:48.868217945 CET	53	58361	8.8.8.8	192.168.2.3
Feb 24, 2021 16:09:53.001827002 CET	63492	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:09:53.044313908 CET	53	63492	8.8.8.8	192.168.2.3
Feb 24, 2021 16:09:54.032480955 CET	60831	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:09:54.046848059 CET	53	60831	8.8.8.8	192.168.2.3
Feb 24, 2021 16:09:54.677936077 CET	60100	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:09:54.690352917 CET	53	60100	8.8.8.8	192.168.2.3
Feb 24, 2021 16:09:55.502053022 CET	53195	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:09:55.514400005 CET	53	53195	8.8.8.8	192.168.2.3
Feb 24, 2021 16:09:56.381470919 CET	50141	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:09:56.393313885 CET	53	50141	8.8.8.8	192.168.2.3
Feb 24, 2021 16:10:02.328959942 CET	53023	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:10:02.341932058 CET	53	53023	8.8.8.8	192.168.2.3
Feb 24, 2021 16:10:04.517302036 CET	49563	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:10:04.529119968 CET	53	49563	8.8.8.8	192.168.2.3
Feb 24, 2021 16:10:06.100166082 CET	51352	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:10:06.112436056 CET	53	51352	8.8.8.8	192.168.2.3
Feb 24, 2021 16:10:06.430387020 CET	59349	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:10:06.448478937 CET	53	59349	8.8.8.8	192.168.2.3
Feb 24, 2021 16:10:12.494995117 CET	57084	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:10:12.515024900 CET	53	57084	8.8.8.8	192.168.2.3
Feb 24, 2021 16:10:17.301676989 CET	58823	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:10:17.313827038 CET	53	58823	8.8.8.8	192.168.2.3
Feb 24, 2021 16:10:19.046977043 CET	57568	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:10:19.069571018 CET	53	57568	8.8.8.8	192.168.2.3
Feb 24, 2021 16:10:24.355799913 CET	50540	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:10:24.378185987 CET	53	50540	8.8.8.8	192.168.2.3
Feb 24, 2021 16:10:31.779824018 CET	54366	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 16:10:31.798311949 CET	53	54366	8.8.8.8	192.168.2.3
Feb 24, 2021 16:10:45.665477037 CET	53034	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:10:45.679471970 CET	53	53034	8.8.8.8	192.168.2.3
Feb 24, 2021 16:10:50.969990969 CET	57762	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:10:50.982461929 CET	53	57762	8.8.8.8	192.168.2.3
Feb 24, 2021 16:10:56.150626898 CET	55435	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:10:56.164819956 CET	53	55435	8.8.8.8	192.168.2.3
Feb 24, 2021 16:11:00.175910950 CET	50713	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:11:00.188209057 CET	53	50713	8.8.8.8	192.168.2.3
Feb 24, 2021 16:11:10.023477077 CET	56132	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:11:10.036223888 CET	53	56132	8.8.8.8	192.168.2.3
Feb 24, 2021 16:11:16.742165089 CET	58987	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:11:16.755805969 CET	53	58987	8.8.8.8	192.168.2.3
Feb 24, 2021 16:11:21.909015894 CET	56579	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:11:21.921886921 CET	53	56579	8.8.8.8	192.168.2.3
Feb 24, 2021 16:11:24.093780994 CET	60633	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:11:24.106976032 CET	53	60633	8.8.8.8	192.168.2.3
Feb 24, 2021 16:11:24.641074896 CET	61292	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:11:24.653902054 CET	53	61292	8.8.8.8	192.168.2.3
Feb 24, 2021 16:11:25.124650955 CET	63619	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:11:25.137247086 CET	53	63619	8.8.8.8	192.168.2.3
Feb 24, 2021 16:11:25.476217985 CET	64938	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:11:25.488652945 CET	53	64938	8.8.8.8	192.168.2.3
Feb 24, 2021 16:11:25.934799910 CET	61946	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:11:25.942636967 CET	64910	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:11:25.955234051 CET	53	64910	8.8.8.8	192.168.2.3
Feb 24, 2021 16:11:25.967046022 CET	53	61946	8.8.8.8	192.168.2.3
Feb 24, 2021 16:11:26.422049999 CET	52123	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:11:26.435072899 CET	53	52123	8.8.8.8	192.168.2.3
Feb 24, 2021 16:11:27.133759022 CET	56130	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:11:27.143636942 CET	56338	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:11:27.146339893 CET	53	56130	8.8.8.8	192.168.2.3
Feb 24, 2021 16:11:27.158008099 CET	53	56338	8.8.8.8	192.168.2.3
Feb 24, 2021 16:11:27.831820011 CET	59420	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:11:27.844815969 CET	53	59420	8.8.8.8	192.168.2.3
Feb 24, 2021 16:11:28.594331026 CET	58784	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:11:28.609221935 CET	53	58784	8.8.8.8	192.168.2.3
Feb 24, 2021 16:11:29.027743101 CET	63978	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:11:29.042020082 CET	53	63978	8.8.8.8	192.168.2.3
Feb 24, 2021 16:11:48.078160048 CET	62938	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:11:48.098563910 CET	53	62938	8.8.8.8	192.168.2.3
Feb 24, 2021 16:11:53.198249102 CET	55708	53	192.168.2.3	8.8.8.8
Feb 24, 2021 16:11:53.212601900 CET	53	55708	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 24, 2021 16:10:12.494995117 CET	192.168.2.3	8.8.8.8	0x827b	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 16:10:19.046977043 CET	192.168.2.3	8.8.8.8	0xb011	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 16:10:24.355799913 CET	192.168.2.3	8.8.8.8	0x7a43	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 16:10:45.665477037 CET	192.168.2.3	8.8.8.8	0x4f9	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 16:10:50.969990969 CET	192.168.2.3	8.8.8.8	0x2628	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 16:10:56.150626898 CET	192.168.2.3	8.8.8.8	0xe64d	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 16:11:16.742165089 CET	192.168.2.3	8.8.8.8	0x9cbe	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 16:11:21.909015894 CET	192.168.2.3	8.8.8.8	0x9e7d	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 16:11:27.133759022 CET	192.168.2.3	8.8.8.8	0xec71	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 16:11:48.078160048 CET	192.168.2.3	8.8.8.8	0x427d	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 24, 2021 16:11:53.198249102 CET	192.168.2.3	8.8.8.8	0x28a1	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)

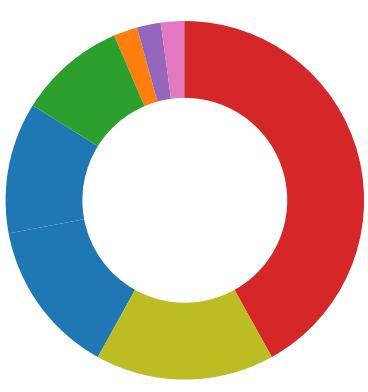
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 24, 2021 16:10:12.515024900 CET	8.8.8.8	192.168.2.3	0x827b	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 16:10:19.069571018 CET	8.8.8.8	192.168.2.3	0xb011	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 16:10:24.378185987 CET	8.8.8.8	192.168.2.3	0x7a43	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 16:10:45.679471970 CET	8.8.8.8	192.168.2.3	0x4f9	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 16:10:50.982461929 CET	8.8.8.8	192.168.2.3	0x2628	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 16:10:56.164819956 CET	8.8.8.8	192.168.2.3	0xe64d	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 16:11:16.755805969 CET	8.8.8.8	192.168.2.3	0x9cbe	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 16:11:21.921886921 CET	8.8.8.8	192.168.2.3	0x9e7d	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 16:11:27.146339893 CET	8.8.8.8	192.168.2.3	0xec71	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 16:11:48.098563910 CET	8.8.8.8	192.168.2.3	0x427d	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 16:11:53.212601900 CET	8.8.8.8	192.168.2.3	0x28a1	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Y5XyMnx8Ng.exe PID: 6372 Parent PID: 5716

General

Start time:	16:09:42
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\Y5XyMnx8Ng.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Y5XyMnx8Ng.exe'
Imagebase:	0x530000
File size:	790016 bytes
MD5 hash:	5BD6A6DBDA26ADA813C6F60FDFC7BA70
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: 00000000.00000002.273575013.0000000003C11000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.273575013.0000000003C11000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.273575013.0000000003C11000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.274362960.00000000040F1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.274362960.00000000040F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.274362960.00000000040F1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming\LbSNAHQmeXYAoG.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	70C131B	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp8EF2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	D8B2B8	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Y5XyMnx8Ng.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8EF2.tmp	success or wait	1	70C1F92	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\LbSNAHQmeXYAoG.exe	unknown	790016	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 34 ae 35 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 04 0c 00 00 08 00 00 00 00 00 00 46 22 0c 00 00 20 00 00 00 40 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 80 0c 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...4.5`.......... ....0.............F"... ...@....@.. ....@................	success or wait	1	70C15A3	WriteFile
C:\Users\user\AppData\Local\Temp\tmp8EF2.tmp	unknown	1647	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 68 61 72 64 7a 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.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	70C15A3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Y5XyMnx8Ng.exe.log	unknown	655	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Users\user\Desktop\Y5XyMnx8Ng.exe	unknown	790016	success or wait	1	70C15A3	ReadFile

Analysis Process: schtasks.exe PID: 5812 Parent PID: 6372

General

Start time:	16:10:06
Start date:	24/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\LbSNAHQmeXYAoG' /XML 'C:\Users\user\AppData\Local\Temp\tmp8EF2.tmp'
Imagebase:	0x320000
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\tmp8EF2.tmp	unknown	2	success or wait	1	32AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp8EF2.tmp	unknown	1648	success or wait	1	32ABD9	ReadFile

Analysis Process: conhost.exe PID: 3180 Parent PID: 5812

General

Start time:	16:10:06
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 5464 Parent PID: 6372

General

Start time:	16:10:07
Start date:	24/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x440000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.494335612.0000000005710000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.494335612.0000000005710000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.494335612.0000000005710000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.483906093.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.483906093.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.483906093.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.492975177.0000000003BBB000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.492975177.0000000003BBB000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.494301167.0000000005700000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.494301167.0000000005700000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.493799082.0000000004E80000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.493799082.0000000004E80000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming\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	27207A1	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	272089B	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	27207A1	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	2720B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp3911.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	2720D1C	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	272089B	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp3C8D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	2720D1C	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	27207A1	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	27207A1	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp3911.tmp	success or wait	1	C2BF0E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp3C8D.tmp	success or wait	1	C2BF0E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	b1 ef 6d b6 21 d9 d8 48	..m.!..H	success or wait	1	2720A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	32768	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 cf ce 7b 5a 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 08 00 00 50 00 00 00 20 00 00 00 00 00 00 de 6b 00 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 00 00 00 10 00 00 b1 5b 01 00 03 00 40 05 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......PE..L..... {Z.................P... ....k... ....@.. ....[....@................	success or wait	1	2720B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp3911.tmp	unknown	1320	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	2720A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	57	43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 5c 76 32 2e 30 2e 35 30 37 32 37 5c 52 65 67 53 76 63 73 2e 65 78 65	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	success or wait	1	2720A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp3C8D.tmp	unknown	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	2720A53	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	2720A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	success or wait	1	2720A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	end of file	1	2720A53	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	2720C12	RegSetValueExW

Analysis Process: schtasks.exe PID: 6292 Parent PID: 5464

General

Start time:	16:10:09
Start date:	24/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp3911.tmp'
Imagebase:	0x320000
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\tmp3911.tmp	unknown	2	success or wait	1	32AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp3911.tmp	unknown	1321	success or wait	1	32ABD9	ReadFile

Analysis Process: conhost.exe PID: 6036 Parent PID: 6292

General

Start time:	16:10:09
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6352 Parent PID: 5464

General

Start time:	16:10:10
Start date:	24/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp3C8D.tmp'
Imagebase:	0x320000
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\tmp3C8D.tmp	unknown	2	success or wait	1	32AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp3C8D.tmp	unknown	1311	success or wait	1	32ABD9	ReadFile

Analysis Process: conhost.exe PID: 1968 Parent PID: 6352

General

Start time:	16:10:10
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 6384 Parent PID: 528

General

Start time:	16:10:10
Start date:	24/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe 0
Imagebase:	0x7d0000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

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

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	7266DCB3	unknown
\Device\ConDrv	unknown	145	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 53 65 72 76 69 63 65 73 20 49 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) .NET Framework Services Installation Utility Version 2.0.50727.8922..Copyright (c) Microsoft Corporation. All rights reserved.....	success or wait	1	7266DFAB	unknown
\Device\ConDrv	unknown	45	0a 54 68 65 20 66 6f 6c 6c 6f 77 69 6e 67 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 65 72 72 6f 72 20 6f 63 63 75 72 72 65 64 3a 0d 0a	.The following installation error occurred:..	success or wait	1	7266DFAB	unknown
\Device\ConDrv	unknown	29	31 3a 20 41 73 73 65 6d 62 6c 79 20 6e 6f 74 20 66 6f 75 6e 64 3a 20 27 30 27 2e 0d 0a	1: Assembly not found: '0'...	success or wait	1	7266DFAB	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RegSvcs.exe.log	unknown	120	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 45 6e 74 65 72 70 72 69 73 65 53 65 72 76 69 63 65 73 2c 20 56 65 72 73 69 6f 6e 3d 32 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: conhost.exe PID: 2172 Parent PID: 6384

General

Start time:	16:10:11
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 6200 Parent PID: 528

General

Start time:	16:10:13
Start date:	24/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x8c0000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Created

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

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	7266DCB3	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	145	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 53 65 72 76 69 63 65 73 20 49 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) .NET Framework Services Installation Utility Version 2.0.50727.8922..Copyright (c) Microsoft Corporation. All rights reserved.....	success or wait	1	7266DFAB	unknown
\Device\ConDrv	unknown	45	0a 54 68 65 20 66 6f 6c 6c 6f 77 69 6e 67 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 65 72 72 6f 72 20 6f 63 63 75 72 72 65 64 3a 0d 0a	.The following installation error occurred:..	success or wait	1	7266DFAB	unknown
\Device\ConDrv	unknown	29	31 3a 20 41 73 73 65 6d 62 6c 79 20 6e 6f 74 20 66 6f 75 6e 64 3a 20 27 30 27 2e 0d 0a	1: Assembly not found: '0'...	success or wait	1	7266DFAB	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	unknown	120	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 45 6e 74 65 72 70 72 69 73 65 53 65 72 76 69 63 65 73 2c 20 56 65 72 73 69 6f 6e 3d 32 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..	success or wait	1	7328A33A	WriteFile

File Read

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

Analysis Process: conhost.exe PID: 5828 Parent PID: 6200

General

Start time:	16:10:13
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 6404 Parent PID: 3388

General

Start time:	16:10:22
Start date:	24/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x760000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

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

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	293A53F	WriteFile
\Device\ConDrv	unknown	145	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 53 65 72 76 69 63 65 73 20 49 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) .NET Framework Services Installation Utility Version 2.0.50727.8922..Copyright (c) Microsoft Corporation. All rights reserved.....	success or wait	1	293A53F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	256	55 53 41 47 45 3a 20 72 65 67 73 76 63 73 2e 65 78 65 20 5b 6f 70 74 69 6f 6e 73 5d 20 41 73 73 65 6d 62 6c 79 4e 61 6d 65 0d 0a 4f 70 74 69 6f 6e 73 3a 0d 0a 20 20 20 20 2f 3f 20 6f 72 20 2f 68 65 6c 70 20 20 20 20 20 44 69 73 70 6c 61 79 20 74 68 69 73 20 75 73 61 67 65 20 6d 65 73 73 61 67 65 2e 0d 0a 20 20 20 20 2f 66 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 46 69 6e 64 20 6f 72 20 63 72 65 61 74 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 28 64 65 66 61 75 6c 74 29 2e 0d 0a 20 20 20 20 2f 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 43 72 65 61 74 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 2c 20 65 72 72 6f 72 20 69 66 20 69 74 20 61 6c 72 65 61 64 79 20 65 78 69 73 74 73 2e 0d 0a 20 20 20 20 2f 65 78 61 70 70 20	USAGE: regsvcs.exe [options] A ssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp	success or wait	3	293A53F	WriteFile
\Device\ConDrv	unknown	232	53 75 70 70 72 65 73 73 20 6c 6f 67 6f 20 6f 75 74 70 75 74 2e 0d 0a 20 20 20 20 2f 71 75 69 65 74 20 20 20 20 20 20 20 20 20 20 20 53 75 70 70 72 65 73 73 20 6c 6f 67 6f 20 6f 75 74 70 75 74 20 61 6e 64 20 73 75 63 63 65 73 73 20 6f 75 74 70 75 74 2e 0d 0a 20 20 20 20 2f 63 6f 6d 70 6f 6e 6c 79 20 20 20 20 20 20 20 20 43 6f 6e 66 69 67 75 72 65 20 63 6f 6d 70 6f 6e 65 6e 74 73 20 6f 6e 6c 79 2c 20 6e 6f 20 6d 65 74 68 6f 64 73 20 6f 72 20 69 6e 74 65 72 66 61 63 65 73 2e 0d 0a 20 20 20 20 2f 61 70 70 64 69 72 3a 3c 70 61 74 68 3e 20 20 53 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 72 6f 6f 74 20 64 69 72 65 63 74 6f 72 79 20 74 6f 20 73 70 65 63 69 66 69 65 64 20 70 61 74 68 2e 0d 0a 0d 0a	Suppress logo output... /quiet Suppress logo output and success output... /componly Configure components only, no methods or inte rfaces... /appdir:<path> Set application root directory to specified path.....	success or wait	1	293A53F	WriteFile

File Read

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

Analysis Process: conhost.exe PID: 5680 Parent PID: 6404

General

Start time:	16:10:22
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis