ID: 341479
Sample Name: Orden n.#U00ba STL21119, pdf.exe
Cookbook: default.jbs
Time: 13:00:14
Date: 19/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

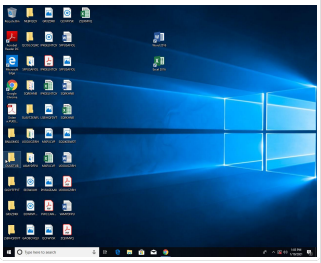
Analysis Report Orden n.#U00ba STL21119, pdf.exe

Overview

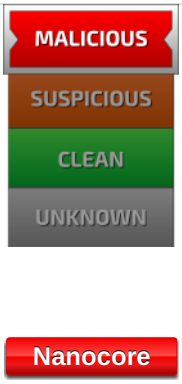
General Information

Sample Name:	Orden n.#U00ba STL21119, pdf.exe
Analysis ID:	341479
MD5:	35ac4ad018dc2b..
SHA1:	6dbe8e66f9e1c0f..
SHA256:	9a74f71ee76b365.
Tags:	exe NanoCore nVpn RAT

Most interesting Screenshot:



Detection

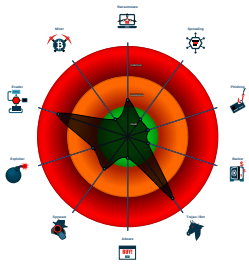


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Icon mismatch, binary includes an ic…
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- Allocates memory in foreign process…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**
- Orden n.#U00ba STL21119, pdf.exe (PID: 2160 cmdline: 'C:\Users\user\Desktop\Orden n.#U00ba STL21119, pdf.exe' MD5: 35AC4AD018DC2BCDFAEFF01DECD3E8FE)
  - schtasks.exe (PID: 6324 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\kSLtgWcvnYChD' /XML 'C:\Users\user\AppData\Local\Temp\tmp40AA.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6336 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - MSBuild.exe (PID: 6376 cmdline: {path} MD5: 88BBB7610152B48C2B3879473B17857E)
    - schtasks.exe (PID: 6424 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpD3F6.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6432 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6504 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpD714.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6512 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- MSBuild.exe (PID: 6556 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe 0 MD5: 88BBB7610152B48C2B3879473B17857E)
  - conhost.exe (PID: 6644 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 6652 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 88BBB7610152B48C2B3879473B17857E)
  - conhost.exe (PID: 6704 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 6948 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 88BBB7610152B48C2B3879473B17857E)
  - conhost.exe (PID: 6956 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
00000000.00000002.253789558.0000000003B41000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5eef5:$x1: NanoCore.ClientPluginHost • 0x5ef32:$x2: IClientNetworkHost • 0x62a65:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.253789558.0000000003B41000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.253789558.0000000003B41000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x5ec5d:$a: NanoCore • 0x5ec6d:$a: NanoCore • 0x5eea1:$a: NanoCore • 0x5eeb5:$a: NanoCore • 0x5eef5:$a: NanoCore • 0x5ecbc:$b: ClientPlugin • 0x5eebe:$b: ClientPlugin • 0x5eefe:$b: ClientPlugin • 0x5ede3:$c: ProjectData • 0x5f7ea:$d: DESCrypto • 0x671b6:$e: KeepAlive • 0x651a4:$g: LogClientMessage • 0x6139f:$i: get_Connected • 0x5fb20:$j: #=q • 0x5fb50:$j: #=q • 0x5fb6c:$j: #=q • 0x5fb9c:$j: #=q • 0x5fbb8:$j: #=q • 0x5fbd4:$j: #=q • 0x5fc04:$j: #=q • 0x5fc20:$j: #=q
00000000.00000002.251685714.0000000002B8B000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.254170099.0000000003C38000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1b64c5:$x1: NanoCore.ClientPluginHost • 0x1b6502:$x2: IClientNetworkHost • 0x1ba035:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 6 entries				

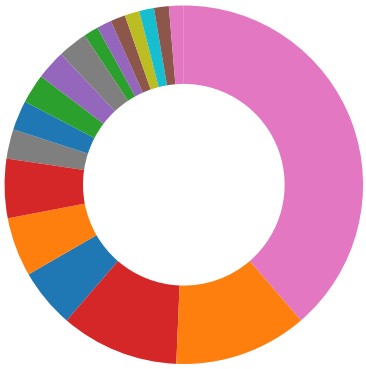
Sigma Overview

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
- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for domain / URL

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:

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

Icon mismatch, binary includes an icon from a different legit application in order to fool users

Malware Analysis System Evasion:

Yara detected AntiVM_3

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:

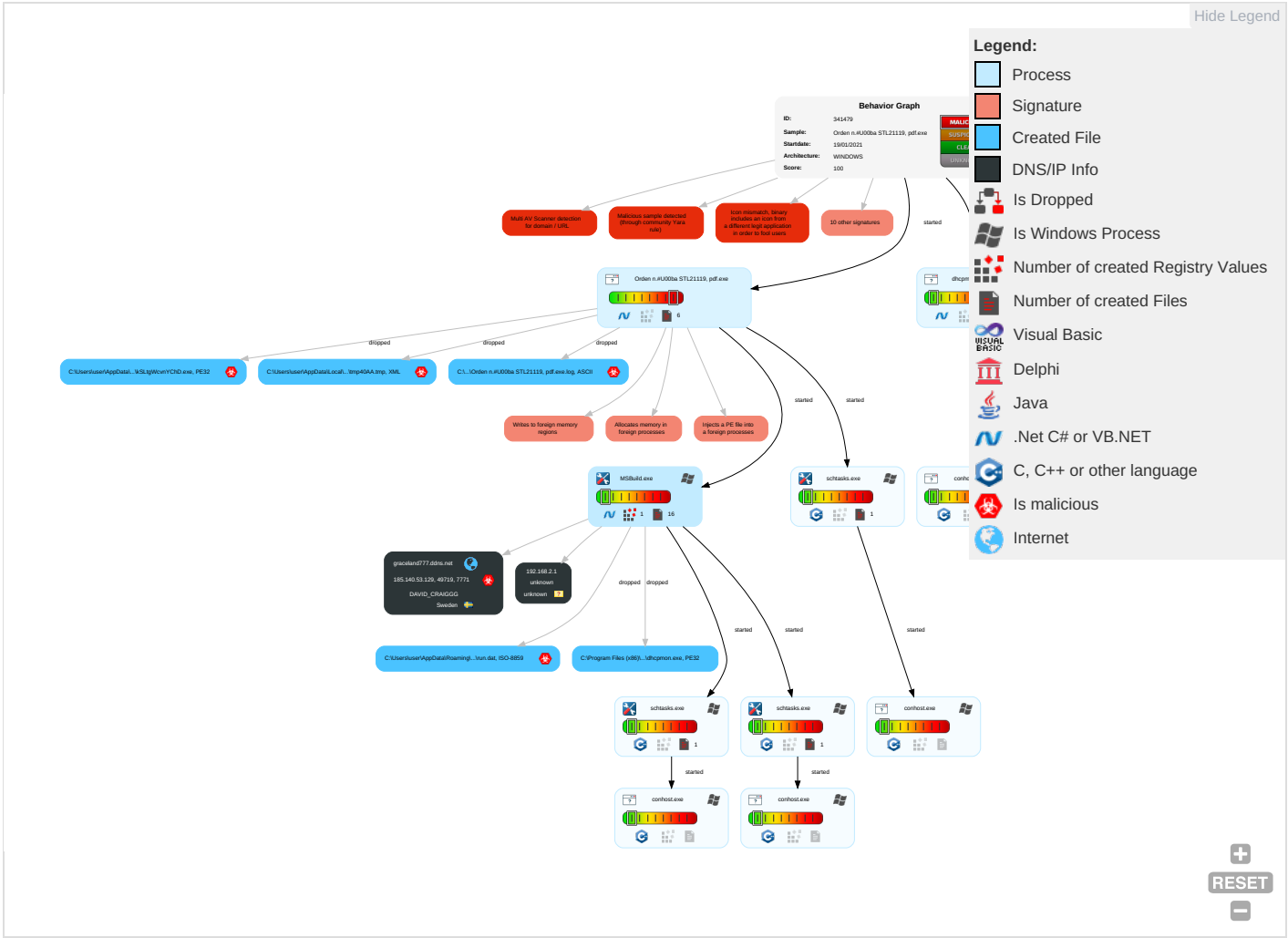
Detected Nanocore Rat

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	Networ Effects
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Access Token Manipulation 1	Masquerading 1 2	Input Capture 1	Security Software Discovery 1 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesc Insecu Networ Commu
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Process Injection 3 1 1	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Disable or Modify Tools 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 3 1 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 2	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

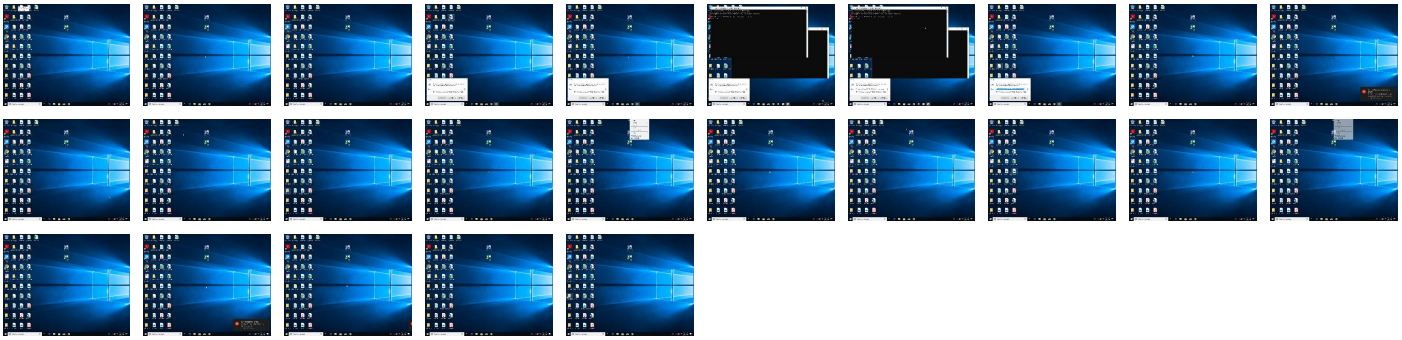
Behavior Graph



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
Orden n.#U00ba STL21119, pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\kSLtgWcvnYChD.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		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
graceland777.ddns.net	10%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/://w	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.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fontbureau.comueva	0%	Avira URL Cloud	safe	
http://www.fontbureau.comitu4	0%	Avira URL Cloud	safe	
http://www.fontbureau.comFE	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.fontbureau.comalsN	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.tiro.comH	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comJ	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/=	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://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.com4	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0p	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/k	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/l-b	0%	Avira URL Cloud	safe	
http://www.fontbureau.comrsiv	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/W	0%	Avira URL Cloud	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.fontbureau.comnc./	0%	Avira URL Cloud	safe	
http://www.fontbureau.come.com=	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/W	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/F	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/F	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/F	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.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/=	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.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.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.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/k	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/k	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/k	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
graceland777.ddns.net	185.140.53.129	true	true	• 10%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/://w	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000003.23432418 7.0000000004E61000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000002.25466732 3.0000000004F40000.00000002.00 000001.sdmp	false		high
http://www.fontbureau.com/designers/?	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000002.25466732 3.0000000004F40000.00000002.00 000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000002.25466732 3.0000000004F40000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comueva	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000003.25013956 7.0000000004E50000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000002.25466732 3.0000000004F40000.00000002.00 000001.sdmp	false		high
http://www.fontbureau.comitu4	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000003.23637839 3.0000000004E54000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comFE	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000003.23637839 3.0000000004E54000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000002.25466732 3.0000000004F40000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comalsN	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000003.23637839 3.0000000004E54000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000002.25466732 3.0000000004F40000.00000002.00 000001.sdmp	false		high
http://www.goodfont.co.kr	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000002.25466732 3.0000000004F40000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.comH	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000003.23265039 9.0000000004E54000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.comJ	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000003.23077559 2.0000000004E57000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/=	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000003.23432418 7.0000000004E61000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000002.25466732 3.0000000004F40000.00000002.00 000001.sdmp, Orden n.#U00ba ST L21119, pdf.exe, 00000000.0000 0003.230775592.0000000004E5700 0.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000002.25466732 3.0000000004F40000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000002.25466732 3.0000000004F40000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000002.25466732 3.0000000004F40000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000002.25466732 3.0000000004F40000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com4	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000003.23574412 9.0000000004E59000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Y0p	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000003.23413250 1.0000000004E61000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/k	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000003.23381336 2.0000000004E61000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000002.25466732 3.0000000004F40000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/l-b	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000003.23373185 1.0000000004E59000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comrsiv	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000003.23574412 9.0000000004E59000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000002.25466732 3.0000000004F40000.00000002.00 000001.sdmp	false		high
http://www.sandoll.co.kr	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000002.25466732 3.0000000004F40000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000002.25466732 3.0000000004F40000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000002.25466732 3.0000000004F40000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/W	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000003.23432418 7.0000000004E61000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000002.25466732 3.0000000004F40000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comnc./	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000003.23574412 9.0000000004E59000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.come.com=	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000003.25013956 7.0000000004E50000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000002.25466732 3.0000000004F40000.00000002.00 000001.sdmp	false		high
http://www.fontbureau.com	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000002.25466732 3.0000000004F40000.00000002.00 000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/W	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000003.23373185 1.0000000004E59000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/F	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000003.23432418 7.0000000004E61000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000003.23432418 7.0000000004E61000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.coma	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000003.25013956 7.0000000004E50000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/=	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000003.23391127 0.0000000004E61000.00000004.00 000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000002.25466732 3.0000000004F40000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000003.23247656 3.0000000004E8D000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000002.25466732 3.0000000004F40000.00000002.00 000001.sdmp	false		high
http://www.founder.com.cn/cn	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000002.25466732 3.0000000004F40000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000002.25466732 3.0000000004F40000.00000002.00 000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/Y0/	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000003.23391127 0.0000000004E61000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000003.23432418 7.0000000004E61000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/k	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000003.23432418 7.0000000004E61000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000002.25466732 3.0000000004F40000.00000002.00 000001.sdmp	false		high
http://www.fontbureau.comals	Orden n.#U00ba STL21119, pdf.exe, 00000000.00000003.23620718 0.0000000004E54000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.129	unknown	Sweden		209623	DAVID_CRAIGGG	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	341479
Start date:	19.01.2021
Start time:	13:00:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Orden n.#U00ba STL21119, pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	36
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@18/16@4/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.2% (good quality ratio 0%) • Quality average: 0% • Quality standard deviation: 0%
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): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 104.43.193.48, 104.84.56.60, 51.104.139.180, 13.88.21.125, 205.185.216.10, 205.185.216.42, 51.103.5.186, 92.122.213.247, 92.122.213.201, 52.254.96.93, 20.54.26.129, 52.255.188.83 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, bn2eap.displaycatalog.md.mp.microsoft.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.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, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, cds.d2s7q6s2.hwcdn.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, par02p.wns.notify.trafficmanager.net, skypedataprdcolwus15.cloudapp.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 NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:01:09	API Interceptor	1x Sleep call for process: Orden n.#U00ba STL21119, pdf.exe modified
13:01:16	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
13:01:18	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe" s>$(Arg0)
13:01:18	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.140.53.129	Orden n.#U00ba 21115, pdf.exe	Get hash	malicious	Browse	
	PO-WJO-001, pdf.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO-WJO-001, pdf.exe	Get hash	malicious	Browse	
	RFQPR2000293356.exe	Get hash	malicious	Browse	
	PO#4500139207.exe	Get hash	malicious	Browse	
	Shipping Documents Maersk Kleven.exe	Get hash	malicious	Browse	
	T2kRjvHnWc.exe	Get hash	malicious	Browse	
	NEW PO # 20001578.exe	Get hash	malicious	Browse	
	Ordine R20 T40567, pdf.exe	Get hash	malicious	Browse	
	Ordine R20 T4077 TBA 2020, pdf.exe	Get hash	malicious	Browse	
	Orden CW62175Q.exe	Get hash	malicious	Browse	
	Ordine R20-T4077, pdf.exe	Get hash	malicious	Browse	
	Importa ed esporta tariffa di spedizione.exe	Get hash	malicious	Browse	
	91HN20DCI100053,54,80.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
graceland777.ddns.net	Orden n.#U00ba 21115, pdf.exe	Get hash	malicious	Browse	• 185.140.53.129
	PO-WJO-001, pdf.exe	Get hash	malicious	Browse	• 185.140.53.129
	PO-WJO-001, pdf.exe	Get hash	malicious	Browse	• 185.140.53.129
	Ordine R20 T40567, pdf.exe	Get hash	malicious	Browse	• 185.140.53.129
	Ordine R20 T4077 TBA 2020, pdf.exe	Get hash	malicious	Browse	• 185.140.53.129
	Ordine R20-T4077, pdf.exe	Get hash	malicious	Browse	• 185.140.53.129
	Orden CW62175Q, pdf.exe	Get hash	malicious	Browse	• 185.244.30.19
	Orden CW62125Q, pdf.exe	Get hash	malicious	Browse	• 185.244.30.19
	Orden CW62125Q, pdf.exe	Get hash	malicious	Browse	• 185.244.30.19
	Orden CW62125Q, pdf.exe	Get hash	malicious	Browse	• 216.38.2.218
	DHL Shipping Documents Original BL, Inv, parking list, pdf.exe	Get hash	malicious	Browse	• 23.105.131.131

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	Proof of Payment.exe	Get hash	malicious	Browse	• 185.244.30.51
	DxCHoDnNLn.exe	Get hash	malicious	Browse	• 185.140.53.202
	T7gzTHDZ7g.rtf	Get hash	malicious	Browse	• 185.140.53.202
	PO - 2021-000511.exe	Get hash	malicious	Browse	• 185.244.30.69
	PO AR483-1590436 _ J-3000 PROJT.xlsx	Get hash	malicious	Browse	• 185.140.53.202
	Qotation.exe	Get hash	malicious	Browse	• 185.140.53.154
	PO - 2021-000511.exe	Get hash	malicious	Browse	• 185.244.30.69
	file.exe	Get hash	malicious	Browse	• 91.193.75.155
	Orden n.#U00ba 21115, pdf.exe	Get hash	malicious	Browse	• 185.140.53.129
	Lists.exe	Get hash	malicious	Browse	• 185.140.53.136
	Quotation Request.exe	Get hash	malicious	Browse	• 185.244.30.171
	PO-PDF_PDF.exe	Get hash	malicious	Browse	• 185.244.30.69
	Quiero hacer el pedido de su producto.exe	Get hash	malicious	Browse	• 185.244.30.18
	PO 047428.xlsx	Get hash	malicious	Browse	• 185.140.53.183
	SLIP.exe	Get hash	malicious	Browse	• 185.244.30.171
	2owa3HlP0V.exe	Get hash	malicious	Browse	• 185.140.53.183
	TAtAHTebr6.exe	Get hash	malicious	Browse	• 185.140.53.183
	Quotation.exe	Get hash	malicious	Browse	• 185.244.30.29
	Halkbank_Ekstre_20210118_162356_389771.exe	Get hash	malicious	Browse	• 91.193.75.189
	Urgent order 1812021-672 Q30721,pdf.exe	Get hash	malicious	Browse	• 185.140.53.131

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Orden n.#U00ba 21115, pdf.exe	Get hash	malicious	Browse	
	PO-WJO-001, pdf.exe	Get hash	malicious	Browse	
	DFR2154747.vbe	Get hash	malicious	Browse	
	SOA Dec2020.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Variant.Mikey.117100.12986.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.DownLoader36.7233.23906.exe	Get hash	malicious	Browse	
	Purchase Order PDF pdf.exe	Get hash	malicious	Browse	
	Orden CW62125Q, pdf.exe	Get hash	malicious	Browse	
	7444478441.js	Get hash	malicious	Browse	
	7444478441.js	Get hash	malicious	Browse	
	7444478441.js	Get hash	malicious	Browse	
	5HuSdWXs4n.exe	Get hash	malicious	Browse	
	ABU.exe	Get hash	malicious	Browse	
	LI-TAK P0 TVOP CK-20-08-30 203008,pdf.exe	Get hash	malicious	Browse	
	ppp.exe	Get hash	malicious	Browse	
	787774778.js	Get hash	malicious	Browse	
	12477123690.js	Get hash	malicious	Browse	
	12477123690.js	Get hash	malicious	Browse	
	order pdf.exe	Get hash	malicious	Browse	
	Documents RF V23665.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\MSBuild.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	69632
Entropy (8bit):	5.20894581699571
Encrypted:	false
SSDEEP:	768:NElGiBcBuiyFjUwF0wdP9/rJMDnRFRJfStGpwV3e3qtAcy:ilGBu7jjP9/tMDn9Jt+VO3GO
MD5:	88BBB7610152B48C2B3879473B17857E
SHA1:	0F6CF8DD66AA58CE31DA4E8AC0631600EF055636
SHA-256:	2C7ACC16D19D076D67E9F1F37984935899B79536C9AC6EEC8850C44D20F87616
SHA-512:	5BACDF6C190A76C2C6A9A3519936E08E898AC8A2B1384D60429DF850BE778860435BF9E5EB316517D2345A5AAE201F369863F7A242134253978BCB5B2179CA58
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: Orden n.#U00ba 21115, pdf.exe, Detection: malicious, Browse • Filename: PO-WJO-001, pdf.exe, Detection: malicious, Browse • Filename: DFR2154747.vbe, Detection: malicious, Browse • Filename: SOA Dec2020.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Variant.Mikey.117100.12986.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.DownLoader36.7233.23906.exe, Detection: malicious, Browse • Filename: Purchase Order PDF pdf.exe, Detection: malicious, Browse • Filename: Orden CW62125Q, pdf.exe, Detection: malicious, Browse • Filename: 7444478441.js, Detection: malicious, Browse • Filename: 7444478441.js, Detection: malicious, Browse • Filename: 7444478441.js, Detection: malicious, Browse • Filename: 5HuSdWXs4n.exe, Detection: malicious, Browse • Filename: ABU.exe, Detection: malicious, Browse • Filename: LI-TAK P0 TVOP CK-20-08-30 203008,pdf.exe, Detection: malicious, Browse • Filename: ppp.exe, Detection: malicious, Browse • Filename: 787774778.js, Detection: malicious, Browse • Filename: 12477123690.js, Detection: malicious, Browse • Filename: 12477123690.js, Detection: malicious, Browse • Filename: order pdf.exe, Detection: malicious, Browse • Filename: Documents RF V23665.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....{Z.....@..... .....@.. .....@.....99.. ..@.....S.....`/..... ..... ..... ..H.....text..... ..... ..`.rsrc...`/.....0.....@..@.reloc..... . ...

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\MSBuild.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	325
Entropy (8bit):	5.334380084018418
Encrypted:	false
SSDEEP:	6:Q3LadLCR22IAQykdL1tZbLsbFLIP12MUAvvro6ysGMFLIP12MUAvvrs:Q3LaJU20NaL1tZbgbe4MqJsGMe4M6

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\MSBuild.exe.log	
MD5:	65CE98936A67552310EFE2F0FF5BDF88
SHA1:	8133653A6B9A169C7496ADE315CED322CFC3613A
SHA-256:	682F7C55B1B6E189D17755F74959CD08762F91373203B3B982ACFFCADE2E871A
SHA-512:	2D00AC024267EC384720A400F6D0B4F7EDDF49FAF8AB3C9E6CBFBBAE90ECADACA9022B33E3E8EC92E4F57C7FC830299C8643235EB4AA7D8A6AFE9DD1775F57C3
Malicious:	false
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..2,"Microsoft.Build.Engine, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.Build.Framework, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Orden n.#U00ba STL21119, pdf.exe.log	
Process:	C:\Users\user\Desktop\Orden n.#U00ba STL21119, pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
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..

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):	441
Entropy (8bit):	5.388715099859351
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U2+gYhD5itZbgbe4MqJsGMe4M6:MLF20NaL32+g2OH4xvn4j
MD5:	88F0104DB9A3F9BC4F0FC3805F571B0D
SHA1:	CDD4F34385792F0CCE0A844F4ABB447C25AB4E73
SHA-256:	F6C11D3D078ED73F2640DA510E68DEEAA5F14F79CAE2E23A254B4E37C7D0230F
SHA-512:	04B977F63CAB8DE20EA7EFA9D4299C2E625D92FA6D54CA03EECD9F322E978326B353824F23BEC0E712083BDE0DBC5CC4EE90922137106B096050CA46A166DFE
Malicious:	false
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.Xml\527c933194f3a99a816d83c619a3e1d3\System.Xml.ni.dll",0..2,"Microsoft.Build.Engine, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.Build.Framework, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\tmp40AA.tmp	
Process:	C:\Users\user\Desktop\Orden n.#U00ba STL21119, pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1662
Entropy (8bit):	5.177106365791287
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB79tn:cbhH7MlNQ8/rydbz9I3YODOLNdq3h3
MD5:	8C39B8F056EDC5EE83D6EB5DCB1887DD
SHA1:	B45B25390914435C2653B427FF1C709FDCA4ED7D
SHA-256:	67D331680E679E2081D602E84CE2F256841D11FBCDB9A312828BD9ED3754B4A8
SHA-512:	52F002527995A7AB752A5B52B4AD349C6101BCDAEA57B5D82B760567EA51D78CF18892AC5C271512C42EAA07D81664F7FAD228D34E35D859209F4D37ADD18E0
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>.. <StartWhenAv

C:\Users\user\AppData\Local\Temp\tmpD3F6.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	5.136963558289723
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mnc2xtn:cbk4oL600QydbQxIYODOLedq3ZLj
MD5:	AE766004C0D8792953BAFFFE8F6A2E3B
SHA1:	14B12F27543A401E2FE0AF8052E116CAB0032426
SHA-256:	1ABDD9B6A6B84E4BA1AF1282DC84CE276C59BA253F4C4AF05FEA498A4FD99540
SHA-512:	E530DA4A5D4336FC37838D0E93B5EB3804B9C489C71F6954A47FC81A4C655BB72EC493E109CF96E6E3617D7623AC80697AD3BBD5FFC6281BAFC8B34DCA5E657
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\tmpD714.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	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\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	128
Entropy (8bit):	6.527114648336088
Encrypted:	false
SSDEEP:	3:XrURGizD7cnRH5/ljRAaTlKYrI1Sj9txROIsxcMek2:X4LDAn1rplKTYBROIsxek2
MD5:	0A9C5EAE8756D6FC90F59D8D71A79E1E
SHA1:	0F7D6AAED17CD18DC614535ED26335C147E29ED7
SHA-256:	B1921EA14C66927397BAF3FA456C22B93C30C3DE23546087C0B18551CE5001C5
SHA-512:	78C2F399AC49C78D89915DFF99AC955B5E0AB07BAAD61B07B0CE073C88C1D3A9F1D302C2413691B349DD34441B0FF909C08A4F71E2F1B73F46C1FF308BC7CFA
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P.OT....g.t.....'7.....)..8zII..K/....n3...3.5.....&.7].)..wL...:}g...@...mV.....JUP...w

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:HEn:kn

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
MD5:	574515807DB36F5348D3C83B852906BB
SHA1:	5A18634E11FC602F57987BFE4FA27BCAD6E5C507
SHA-256:	07994CBBA08913C70ECCB749D60E3D0FC87AA1C39759641C1D26F20EFFFAB284
SHA-512:	17496D4765A425ECB286DE50C026F4E53F4EDA580182FDCC8C6FFA5DAF6F9F7DCCC0908445E728814CDD9E9EDCDCCEC07B047931ACA9EB9D69530EF2B5FB F11
Malicious:	**true**
Preview:	..<\...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671E CB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	367496
Entropy (8bit):	**7.999535722214108**
Encrypted:	**true**
SSDEEP:	6144:3rv1Xjouu5ZMQajChQSE0Rp30gbdoh5Y2cmSPCqA9BCNHku9BdFqB3GbiCX:D1TousJSafd6imJd8EeBdF7biCX
MD5:	4D784935677AE26ACDC3FB84FA1E6CF8
SHA1:	4B143D26638C2BE44BE05D862E5CD1BEA3664825
SHA-256:	C77E2D82DB9066E4DBFDE3AE0461A4259505F435EC0DB2CE3BD005BE0E2DE67C
SHA-512:	193295AB3FBCE6BA4A563DD864839F5D7A3B8F351F576DE2C85E2F3978F3E33EF22299224DFD7D2F5506A2CAFB04656E19676F28B21F19C504B2D43921063554
Malicious:	false
Preview:	..m.....%.8C.....o`.M..d....mvW5].N ...c....m.b..1^J@....M.!.aq.f....<....._..;i.1-+.wZ..C@Z...> .P9.K..[~....1.....#.Djp...q..z..HoR/..8....k.....\.7..c..]_....._F.....3Z.9U.....r.. 8..]..%n..Q..^<s`L{. ..9.o..wU33z...hJG..!..a.?mI...}.H}...o.Zs`.....~..x....".7.{....k.>. @X.\j.....57..C..f.v...:..Q<.B.o..x..s}\.`....z..E@$.!.}}.&.VI.....Y.....gU..b.b..l..Bg....bh .$.....f.B...e.f...a.....v.....9..x.#.....*[.....=.T#.,.6.uN.....D.jdQ..go.T..+..N.U-.w.a..6 C.5.vMy....S...V...I..:..v2..V.....G..P K.{.&.....o...q.....`~.i8.....+k.F...o.$TP.... I.....;T..3.a.u.f..)...4b...-.r.&(<....'....n.[...b....k....W.Vp..G`..~..."k....Y../l3`....u_.L...#.....;....m.cV.|.:.....#..P9;....Q..*F.._%.f..0...'.z.i..#;.X=.utJ...)9".....k..E..K...\..cc-..8<..f.T!{ ..c....S`4{....D2..s.....)`.h.;.QQ^mP.M77.'M.....q C).l....<..]QA.,...p.....4..XQ.xu.w.z..g~.%M.....D...!.h.F.$~.....n%'.lt..E...h=.....).?.....N.K?.M.48..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.85263908467479
Encrypted:	false
SSDEEP:	3:oMty8WbSl1u:oMLWul1u
MD5:	A35128E4E28B27328F70E4E8FF482443
SHA1:	B89066B2F8DB34299AABFD7ABEE402D5444DD079
SHA-256:	88AEA00733DC4B570A29D56A423CC5BF163E5ACE7AF349972EB0BBA8D9AD06E1
SHA-512:	F098E844B5373B34642B49B6E0F2E15CFDAA1A8B6CABC2196CEC0F3765289E5B1FD4AB588DD65F97C8E51FA9A81077621E9A06946859F296904C646906A70F33
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe

C:\Users\user\AppData\Roaming\kSLtgWcvnYChD.exe	
Process:	C:\Users\user\Desktop\Orden n.#U00ba STL21119, pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1074176

C:\Users\user\AppData\Roaming\kSLtgWcvnYChD.exe	
Entropy (8bit):	6.8072726854936185
Encrypted:	false
SSDEEP:	12288:7Sh4DXUMmnrfhufp9sdKxU2QwGjmMMs0t22BWLXdkeA:eSpAKWrwkm1y2+keA
MD5:	35AC4AD018DC2BCDFAEFF01DECD3E8FE
SHA1:	6DBE8E66F9E1C0F59169B7C7AFF0BCDB9C789ECC
SHA-256:	9A74F71EE76B3652042A3F5E1F5E4A8BACC97A3C72B28BAA37008169170AB980
SHA-512:	259B55AB84D7088D58C1E4C8C819FA84EF7591BFA9F4F16F21B5471EBB69BB984521447428E41F26A3E51CACC540C63BEC1F39B126461AF2270D1974BAD5C49
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....0.....:.... .....@.. ..@.....O..... ..... ..H.....text...@.... ..... ..`.rsrc.....@..@.reloc..... .....b.....@..B.....H..... ....$.....k...(.....".(.....*Vr...p.....r...p.....*..0..L.....}.....(.....(.....(.....s .....(!....o".....(#....o$.....(%... .*.0..K.....}.....(&.....('.....5...(.....s .....(.....o".....(.....o$....8.....r...p.c...((...o)...tc.....(*.....9.....s.....s+...s,...o-.....o....(/.....o0...(1.....o2...(3.....o4...(5.....o6... (7.....o8...(9.....(:.....(.....+....s+...s,...(

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	306
Entropy (8bit):	4.969261552825097
Encrypted:	false
SSDEEP:	6:zx3M1tlAX8bSWR30qysGMQbSVRRZBXVRbJ0fFdCsq2UTiMdH8stCal+n:zK1XnV30ZsGMIG9BFRbQdCT2UftCM+
MD5:	F227448515085A647910907084E6728E
SHA1:	5FA1A8E28B084DA25A1BBC51A2D75810CEF57E2C
SHA-256:	662BA47D628FE8EBE95DD47B4482110A10B49AED09387BC0E028BB66E68E20BD
SHA-512:	6F6E5DFFF7B17C304FB19B0BA5466AF84EF98A5C2EFA573AF72CFD3ED6964E9FD7F8E4B79FCFFBEF87CE545418C69D4984F4DD60BBF457D0A3640950F8FC5A F0
Malicious:	false
Preview:	Microsoft (R) Build Engine Version 2.0.50727.8922..[Microsoft .NET Framework, Version 2.0.50727.8922]..Copyright (C) Microsoft Corporation 2005. All rights rese rved.....MSBUILD : error MSB1003: Specify a project or solution file. The current working directory does not contain a project or solution file...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assemb ly, for MS Windows
Entropy (8bit):	6.8072726854936185
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:	Orden n.#U00ba STL21119, pdf.exe
File size:	1074176
MD5:	35ac4ad018dc2bcdfaeff01decd3e8fe
SHA1:	6dbe8e66f9e1c0f59169b7c7aff0bcdb9c789ecc
SHA256:	9a74f71ee76b3652042a3f5e1f5e4a8bacc97a3c72b28ba a37008169170ab980
SHA512:	259b55ab84d7088d58c1e4c8c819fa84ef7591bfa9f4f16f 21b5471ebb69bb984521447428e41f26a3e51cacc540c6 3bec1f39b126461af2270d1974bad5c495
SSDEEP:	12288:7Sh4DXUMmnrfhufp9sdKxU2QwGjmMMs0t22B WLXdkeA:eSpAKWrwkm1y2+keA
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....PE..L..... .`.....0.....:.... .....@.. ..... @.....

File Icon

	
Icon Hash:	d4c6c4c8ccd4c0e4

Static PE Info

General	
Entrypoint:	0x4dc33a
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:	0x6006B60A [Tue Jan 19 10:35:54 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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xdc2e8	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xde000	0x2bb88	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x10a000	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	0xda340	0xda400	False	0.464727412658	data	7.08615591885	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xde000	0x2bb88	0x2bc00	False	0.145106026786	data	3.6125761847	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x10a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xde250	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0xeea78	0x2ad0	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xf1548	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 3892081920, next used block 3187504384		
RT_ICON	0xf3af0	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4294866176, next used block 4294866176		
RT_ICON	0xf4b98	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x1053c0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 670987520, next used block 0		
RT_GROUP_ICON	0x1095e8	0x14	data		
RT_GROUP_ICON	0x1095fc	0x5a	data		
RT_VERSION	0x109658	0x342	data		
RT_MANIFEST	0x10999c	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

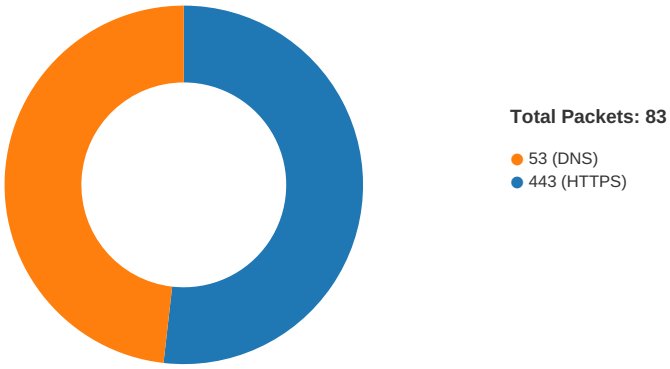
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Hewlett-Packard 2016
Assembly Version	46.3.0.0
InternalName	.exe
FileVersion	46.3.0.0
CompanyName	Hewlett-Packard
LegalTrademarks	
Comments	

Description	Data
ProductName	
ProductVersion	46.3.0.0
FileDescription	
OriginalFilename	.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 13:00:58.794450045 CET	49702	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.826157093 CET	443	49697	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.826179028 CET	443	49697	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.826332092 CET	49697	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.827991009 CET	443	49697	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.828012943 CET	443	49697	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.828125000 CET	49701	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.828207016 CET	49697	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.831935883 CET	443	49697	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.831957102 CET	443	49697	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.832664967 CET	49697	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.838604927 CET	443	49698	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.838644028 CET	443	49698	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.838769913 CET	49698	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.838831902 CET	49698	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.839159012 CET	443	49698	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.839190006 CET	443	49698	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.839260101 CET	49698	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.839293957 CET	49698	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.842629910 CET	49697	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.845474958 CET	443	49698	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.845504999 CET	443	49698	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.845521927 CET	443	49698	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.845537901 CET	443	49698	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.845556974 CET	443	49698	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.845575094 CET	443	49698	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.845591068 CET	443	49698	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.845607996 CET	443	49698	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.845627069 CET	443	49698	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.845642090 CET	443	49698	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.845659971 CET	49698	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.845843077 CET	49698	443	192.168.2.7	92.122.145.220

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 13:00:58.845870018 CET	49698	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.856807947 CET	443	49702	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.856836081 CET	443	49702	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.857081890 CET	49702	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.887295008 CET	443	49701	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.887334108 CET	443	49701	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.887447119 CET	49701	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.887650967 CET	443	49701	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.887681007 CET	443	49701	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.887713909 CET	49701	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.887775898 CET	49701	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.888638973 CET	443	49701	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.888670921 CET	443	49701	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.888745070 CET	49701	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.888788939 CET	49701	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.889475107 CET	443	49701	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.889508963 CET	443	49701	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.889568090 CET	49701	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.889704943 CET	49701	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.890306950 CET	443	49701	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.890330076 CET	443	49701	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.890381098 CET	49701	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.890434027 CET	49701	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.891285896 CET	443	49701	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.891319990 CET	443	49701	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.891377926 CET	49701	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.891438961 CET	49701	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.892086983 CET	443	49701	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.892111063 CET	443	49701	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.892174959 CET	49701	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.892224073 CET	49701	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.892985106 CET	443	49701	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.893014908 CET	443	49701	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.893075943 CET	49701	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.913619995 CET	443	49697	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.913686991 CET	443	49697	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.913849115 CET	49697	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.913873911 CET	49697	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.915568113 CET	443	49697	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.915608883 CET	443	49697	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.916007042 CET	49697	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.919421911 CET	443	49697	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.919465065 CET	443	49697	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.919588089 CET	49697	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.919606924 CET	49697	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.923290968 CET	443	49697	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.923317909 CET	443	49697	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.924442053 CET	49697	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.927139044 CET	443	49697	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:58.927251101 CET	49697	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:58.994102955 CET	443	49703	52.147.198.201	192.168.2.7
Jan 19, 2021 13:00:58.994981050 CET	49703	443	192.168.2.7	52.147.198.201
Jan 19, 2021 13:00:59.110119104 CET	49697	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:59.120718956 CET	443	49703	52.147.198.201	192.168.2.7
Jan 19, 2021 13:00:59.120909929 CET	49703	443	192.168.2.7	52.147.198.201
Jan 19, 2021 13:00:59.172729969 CET	443	49697	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:59.172759056 CET	443	49697	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:59.173068047 CET	49697	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:59.174572945 CET	443	49697	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:59.174597979 CET	443	49697	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:59.174858093 CET	49697	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:59.178553104 CET	443	49697	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:59.178591013 CET	443	49697	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:59.178956032 CET	49697	443	192.168.2.7	92.122.145.220

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 13:00:59.182414055 CET	443	49697	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:59.182557106 CET	49697	443	192.168.2.7	92.122.145.220
Jan 19, 2021 13:00:59.184472084 CET	443	49697	92.122.145.220	192.168.2.7
Jan 19, 2021 13:00:59.184591055 CET	49697	443	192.168.2.7	92.122.145.220

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 13:00:59.216551065 CET	54640	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:00:59.278104067 CET	53	54640	8.8.8.8	192.168.2.7
Jan 19, 2021 13:01:03.000880003 CET	58739	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:01:03.048883915 CET	53	58739	8.8.8.8	192.168.2.7
Jan 19, 2021 13:01:04.741123915 CET	60338	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:01:04.791841984 CET	53	60338	8.8.8.8	192.168.2.7
Jan 19, 2021 13:01:05.761414051 CET	58717	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:01:05.814177990 CET	53	58717	8.8.8.8	192.168.2.7
Jan 19, 2021 13:01:06.912892103 CET	59762	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:01:06.961415052 CET	53	59762	8.8.8.8	192.168.2.7
Jan 19, 2021 13:01:08.056766033 CET	54329	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:01:08.104758978 CET	53	54329	8.8.8.8	192.168.2.7
Jan 19, 2021 13:01:09.079817057 CET	58052	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:01:09.138430119 CET	53	58052	8.8.8.8	192.168.2.7
Jan 19, 2021 13:01:10.165616035 CET	54008	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:01:10.213527918 CET	53	54008	8.8.8.8	192.168.2.7
Jan 19, 2021 13:01:11.812091112 CET	59451	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:01:11.859911919 CET	53	59451	8.8.8.8	192.168.2.7
Jan 19, 2021 13:01:12.977188110 CET	52914	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:01:13.025719881 CET	53	52914	8.8.8.8	192.168.2.7
Jan 19, 2021 13:01:14.030255079 CET	64569	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:01:14.081110001 CET	53	64569	8.8.8.8	192.168.2.7
Jan 19, 2021 13:01:15.391658068 CET	52816	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:01:15.448194981 CET	53	52816	8.8.8.8	192.168.2.7
Jan 19, 2021 13:01:16.477684021 CET	50781	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:01:16.525547981 CET	53	50781	8.8.8.8	192.168.2.7
Jan 19, 2021 13:01:20.885052919 CET	54230	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:01:20.945959091 CET	53	54230	8.8.8.8	192.168.2.7
Jan 19, 2021 13:01:22.778745890 CET	54911	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:01:22.840121031 CET	53	54911	8.8.8.8	192.168.2.7
Jan 19, 2021 13:01:26.313744068 CET	49958	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:01:26.361865997 CET	53	49958	8.8.8.8	192.168.2.7
Jan 19, 2021 13:01:31.787610054 CET	50860	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:01:31.836179018 CET	53	50860	8.8.8.8	192.168.2.7
Jan 19, 2021 13:01:43.130891085 CET	50452	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:01:43.181907892 CET	53	50452	8.8.8.8	192.168.2.7
Jan 19, 2021 13:01:44.289680958 CET	59730	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:01:44.340419054 CET	53	59730	8.8.8.8	192.168.2.7
Jan 19, 2021 13:01:45.511645079 CET	59310	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:01:45.559434891 CET	53	59310	8.8.8.8	192.168.2.7
Jan 19, 2021 13:01:48.328197956 CET	51919	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:01:48.378981113 CET	53	51919	8.8.8.8	192.168.2.7
Jan 19, 2021 13:01:49.379774094 CET	64296	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:01:49.439013958 CET	53	64296	8.8.8.8	192.168.2.7
Jan 19, 2021 13:02:01.919405937 CET	56680	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:02:01.977049112 CET	53	56680	8.8.8.8	192.168.2.7
Jan 19, 2021 13:02:06.905705929 CET	58820	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:02:06.956756115 CET	53	58820	8.8.8.8	192.168.2.7
Jan 19, 2021 13:02:07.877549887 CET	60983	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:02:07.933974981 CET	53	60983	8.8.8.8	192.168.2.7
Jan 19, 2021 13:02:09.136959076 CET	49247	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:02:09.193193913 CET	53	49247	8.8.8.8	192.168.2.7
Jan 19, 2021 13:02:10.278424025 CET	52286	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:02:10.326281071 CET	53	52286	8.8.8.8	192.168.2.7
Jan 19, 2021 13:02:10.426754951 CET	56064	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:02:10.500736952 CET	53	56064	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 13:02:11.218262911 CET	63744	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:02:11.266000986 CET	53	63744	8.8.8.8	192.168.2.7
Jan 19, 2021 13:02:13.043951988 CET	61457	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:02:13.103302956 CET	53	61457	8.8.8.8	192.168.2.7
Jan 19, 2021 13:02:14.437928915 CET	58367	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:02:14.488084078 CET	53	58367	8.8.8.8	192.168.2.7
Jan 19, 2021 13:02:15.462379932 CET	60599	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:02:15.510675907 CET	53	60599	8.8.8.8	192.168.2.7
Jan 19, 2021 13:02:17.396972895 CET	59571	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:02:17.453497887 CET	53	59571	8.8.8.8	192.168.2.7
Jan 19, 2021 13:02:19.650741100 CET	52689	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:02:19.706891060 CET	53	52689	8.8.8.8	192.168.2.7
Jan 19, 2021 13:02:20.599031925 CET	50290	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:02:20.656295061 CET	53	50290	8.8.8.8	192.168.2.7
Jan 19, 2021 13:02:36.772881031 CET	60427	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:02:36.829235077 CET	53	60427	8.8.8.8	192.168.2.7
Jan 19, 2021 13:02:52.913959026 CET	56209	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:02:52.965224028 CET	53	56209	8.8.8.8	192.168.2.7
Jan 19, 2021 13:03:12.404690027 CET	59582	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:03:12.463337898 CET	53	59582	8.8.8.8	192.168.2.7
Jan 19, 2021 13:03:29.861680984 CET	60949	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:03:29.917964935 CET	53	60949	8.8.8.8	192.168.2.7
Jan 19, 2021 13:03:47.478713036 CET	58542	53	192.168.2.7	8.8.8.8
Jan 19, 2021 13:03:47.538125038 CET	53	58542	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 19, 2021 13:01:20.885052919 CET	192.168.2.7	8.8.8.8	0x4abd	Standard query (0)	graceland7 77.ddns.net	A (IP address)	IN (0x0001)
Jan 19, 2021 13:03:12.404690027 CET	192.168.2.7	8.8.8.8	0xc958	Standard query (0)	graceland7 77.ddns.net	A (IP address)	IN (0x0001)
Jan 19, 2021 13:03:29.861680984 CET	192.168.2.7	8.8.8.8	0x7333	Standard query (0)	graceland7 77.ddns.net	A (IP address)	IN (0x0001)
Jan 19, 2021 13:03:47.478713036 CET	192.168.2.7	8.8.8.8	0xfa40	Standard query (0)	graceland7 77.ddns.net	A (IP address)	IN (0x0001)

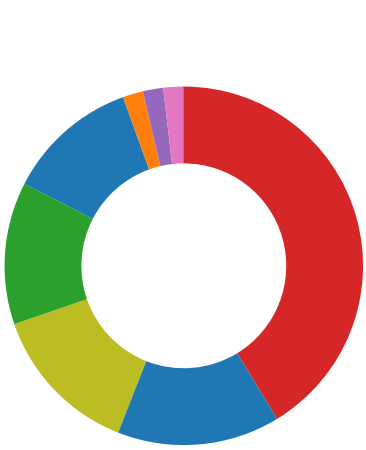
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 19, 2021 13:01:20.945959091 CET	8.8.8.8	192.168.2.7	0x4abd	No error (0)	graceland7 77.ddns.net		185.140.53.129	A (IP address)	IN (0x0001)
Jan 19, 2021 13:03:12.463337898 CET	8.8.8.8	192.168.2.7	0xc958	No error (0)	graceland7 77.ddns.net		185.140.53.129	A (IP address)	IN (0x0001)
Jan 19, 2021 13:03:29.917964935 CET	8.8.8.8	192.168.2.7	0x7333	No error (0)	graceland7 77.ddns.net		185.140.53.129	A (IP address)	IN (0x0001)
Jan 19, 2021 13:03:47.538125038 CET	8.8.8.8	192.168.2.7	0xfa40	No error (0)	graceland7 77.ddns.net		185.140.53.129	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Orden n.#U00ba STL21119, pdf.exe PID: 2160 Parent PID: 5712

General

Start time:	13:01:04
Start date:	19/01/2021
Path:	C:\Users\user\Desktop\Orden n.#U00ba STL21119, pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Orden n.#U00ba STL21119, pdf.exe'
Imagebase:	0x7fffae0c0000
File size:	1074176 bytes
MD5 hash:	35AC4AD018DC2BCDFAEFF01DECD3E8FE
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: 00000000.00000002.253789558.0000000003B41000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.253789558.0000000003B41000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.253789558.0000000003B41000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.251685714.0000000002B8B000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.254170099.0000000003C38000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.254170099.0000000003C38000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.254170099.0000000003C38000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	724660AC	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	724660AC	unknown
C:\Users\user\AppData\Roaming\kSLtgWcvnYChD.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6440357	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp40AA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	ADB2B8	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Orden n.#U00ba STL21119, pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	724534A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp40AA.tmp	success or wait	1	644107E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\kSLtgWcvnYChD.exe	unknown	1074176	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 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 0a b6 06 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 a4 0d 00 00 be 02 00 00 00 00 00 3a c3 0d 00 00 20 00 00 00 e0 0d 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 c0 10 00 00 02 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......`.......... ....0.............:.... ....@.. ....@................	success or wait	1	64405DF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp40AA.tmp	unknown	1662	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 66 72 6f 6e 74 64 65 73 6b 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	<?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>.. </Registrati	success or wait	1	64405DF	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Orden n.#U00ba STL21119, pdf.exe.log	unknown	525	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	7273A33A	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	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72498738	ReadFile
C:\Users\user\Desktop\Orden n.#U00ba STL21119, pdf.exe	unknown	1074176	success or wait	1	64405DF	ReadFile

Analysis Process: schtasks.exe PID: 6324 Parent PID: 2160

General

Start time:	13:01:12
Start date:	19/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\kSLtgWcvnYChD' /XML 'C:\Users\user\AppData\Local\Temp\tmp40AA.tmp'
Imagebase:	0x260000
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\tmp40AA.tmp	unknown	2	success or wait	1	26AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp40AA.tmp	unknown	1663	success or wait	1	26ABD9	ReadFile

Analysis Process: conhost.exe PID: 6336 Parent PID: 6324

General

Start time:	13:01:13
Start date:	19/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: MSBuild.exe PID: 6376 Parent PID: 2160

General

Start time:	13:01:14
Start date:	19/01/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x700000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	724660AC	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	724660AC	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	4F207A1	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	4F2089B	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	4F207A1	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	4F20B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpD3F6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4F20DCC	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	4F2089B	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpD714.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4F20DCC	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	4F207A1	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	4F207A1	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	724660AC	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	724660AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	4F2089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	4F2089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	4F2089B	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpD3F6.tmp	success or wait	1	DDBF0E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpD714.tmp	success or wait	1	DDBF0E	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	b2 d2 3c 5c bd bc d8 48	..<\...H	success or wait	1	4F20A53	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	69632	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 a9 d1 7b 5a 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 08 00 00 c0 00 00 00 40 00 00 00 00 00 00 de d2 00 00 00 20 00 00 00 e0 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 40 01 00 00 10 00 00 39 39 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.....................@........... ....@.. ....@ ......99....@................	success or wait	1	4F20B20	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpD3F6.tmp	unknown	1320	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	4F20A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	57	43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 5c 76 32 2e 30 2e 35 30 37 32 37 5c 4d 53 42 75 69 6c 64 2e 65 78 65	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe	success or wait	1	4F20A53	WriteFile
C:\Users\user\AppData\Local\Temp\tmpD714.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	4F20A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	128	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 f7 4f 54 9a 9e cd ce 67 b2 74 1d 8d f3 84 d5 c8 14 27 37 9d 1c 91 f7 de c0 29 c6 85 f2 9b 38 7a 49 49 d1 ba 8a 4b 2f 1e f9 0e c8 6e 33 10 b7 d5 33 90 35 c3 c9 07 e0 81 87 ea 26 b8 37 5d 98 29 bb eb 77 4c 93 d5 c0 3a 7d 67 09 96 2e 40 ce f9 f7 6d 56 d9 b2 fc bd 83 ad 4a 55 50 9c fa 96 77	Gj.h\.3..A...5.x..&...i+...c(1 .P.OT....g.t.....'7.....).. ..8zII...K/....n3...3.5..... &.7].)..wL...:}g...@...mV..... .JUP...w	success or wait	1	4F20A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	367496	1e 9f 6d a5 c0 de 11 eb 25 2e 38 43 8e cf 1f 13 a6 b8 6f 60 e9 4d c1 08 64 9a 8d ac ae 6d 76 57 35 5d ba 4e 20 c0 d2 d2 80 63 0a 09 1e d4 6d ff 62 11 05 31 5e 4a 40 97 bc ec c4 4d 8f 21 cb 91 61 71 a8 66 90 10 e6 cb 3c bb ed d1 be 8a fc 5f eb 0c 3b 69 fa 31 2d 2b ea 77 5a fb ef 43 40 5a 01 ba a1 3e 20 ce 50 39 f2 4b bd 10 5b 7e 9f e7 87 f6 df 31 f6 03 18 91 94 f9 13 23 a4 44 6a 70 99 89 80 71 e0 fc 7a 88 ec a7 94 48 6f 52 2f 19 ab 38 97 ba 95 d8 6b 9b 1f 87 bd f7 da 09 5c 80 37 a0 a6 63 1a c1 5d 5f 0e dd ea 8e e9 01 5f 46 90 d8 cc fb ab 33 5a 8d 39 55 83 c8 0e 99 95 0a 05 b0 72 0f b0 38 dc f5 5d aa c5 25 6e d1 d4 51 e5 dc 5e 3c 73 60 4c 7b 0b 20 9a 86 39 cf bd 6f f7 ba 77 55 33 33 7a cc fd 0c 68 4a 47 b6 c3 21 9a c5 97 61 f2 3f 6d 49 94 cb 09 7d 00 48 7d	..m.....%.8C.....o`.M..d....m vW5].N ....c....m.b..1^J@....M .!..aq.f....<....._..;i.1-+.w Z..C@Z...> .P9.K.. [~.....1.... ...#.Djp...q..z....HoR/..8.... k.....\.7..c..]_....._F.... .3Z.9U.....r..8..]..%n..Q.. ^<s`L{. ..9..o..wU33z...hJG..!...a.? mI...}.H}	success or wait	1	4F20A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 7e 61 d3 f8 a3 01 06 96 0c a9 7e ba 7e 86 90 d9 e5 05 8d ca 33 e7 55 0b	9iH....}Z..4..f.~a.....~.~. .....3.U.	success or wait	1	4F20A53	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	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	72498738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	72498738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72498738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7253BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7253BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe	unknown	4096	success or wait	1	7253BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe	unknown	512	success or wait	1	7253BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72495544	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	4F20A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4096	success or wait	1	4F20A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4096	end of file	1	4F20A53	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	4F20C12	RegSetValueExW

Analysis Process: schtasks.exe PID: 6424 Parent PID: 6376

General

Start time:	13:01:15
Start date:	19/01/2021
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\tmpD3F6.tmp'
Imagebase:	0x260000
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\tmpD3F6.tmp	unknown	2	success or wait	1	26AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpD3F6.tmp	unknown	1321	success or wait	1	26ABD9	ReadFile

Analysis Process: conhost.exe PID: 6432 Parent PID: 6424

General

Start time:	13:01:16
Start date:	19/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: 6504 Parent PID: 6376

General

Start time:	13:01:16
Start date:	19/01/2021
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\tmpD714.tmp'
Imagebase:	0x260000
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\tmpD714.tmp	unknown	2	success or wait	1	26AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpD714.tmp	unknown	1311	success or wait	1	26ABD9	ReadFile

Analysis Process: conhost.exe PID: 6512 Parent PID: 6504

General

Start time:	13:01:16
Start date:	19/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: MSBuild.exe PID: 6556 Parent PID: 1104

General

Start time:	13:01:18
Start date:	19/01/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe 0
Imagebase:	0x3b0000
File size:	69632 bytes

MD5 hash:	88BBB7610152B48C2B3879473B17857E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	724660AC	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	724660AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\MSBuild.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	724534A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	71B1DCB3	unknown
\Device\ConDrv	unknown	169	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 42 75 69 6c 64 20 45 6e 67 69 6e 65 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 0d 0a 5b 4d 69 63 72 6f 73 6f 66 74 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 2c 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 5d 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 20 32 30 30 35 2e 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) Build Engine Version 2.0.50727.8922.. [Microsoft .NET Framework, Version 2.0. 50727.8922]..Copyright (C) Microsoft Corporation 2005. All rights reserved.....	success or wait	1	71B1DFAB	unknown
\Device\ConDrv	unknown	66	4d 53 42 55 49 4c 44 20 3a 20 65 72 72 6f 72 20 4d 53 42 31 30 30 39 3a 20 50 72 6f 6a 65 63 74 20 66 69 6c 65 20 64 6f 65 73 20 6e 6f 74 20 65 78 69 73 74 2e 0d 0a 53 77 69 74 63 68 3a 20 30 0d 0a	MSBUILD : error MSB1009: Project file does not exist...Switch: 0..	success or wait	1	71B1DFAB	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\MSBuild.exe.log	unknown	325	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 42 75 69 6c 64 2e 45 6e 67 69 6e 65 2c 20 56 65 72 73 69 6f 6e 3d 32 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 42 75 69 6c 64 2e 46 72 61 6d 65 77 6f 72 6b 2c 20	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..2,"Microsoft.Build.Engine, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.Build.Framework,	success or wait	1	7273A33A	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	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	72498738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	72498738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72498738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.rsp	unknown	4096	success or wait	1	71B1C1B7	unknown

Analysis Process: conhost.exe PID: 6644 Parent PID: 6556

General

Start time:	13:01:18
Start date:	19/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: 6652 Parent PID: 1104

General

Start time:	13:01:18
Start date:	19/01/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x1f0000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
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	724660AC	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	724660AC	unknown
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	724660AC	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	724660AC	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	724534A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	8EA897	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	169	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 42 75 69 6c 64 20 45 6e 67 69 6e 65 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 0d 0a 5b 4d 69 63 72 6f 73 6f 66 74 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 2c 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 5d 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 20 32 30 30 35 2e 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) Build Engine Version 2.0.50727.8922.. [Microsoft .NET Framework, Version 2.0. 50727.8922]..Copyright (C) Microsoft Corporation 2005. All rights reserved.....	success or wait	1	8EA897	WriteFile
\Device\ConDrv	unknown	66	4d 53 42 55 49 4c 44 20 3a 20 65 72 72 6f 72 20 4d 53 42 31 30 30 39 3a 20 50 72 6f 6a 65 63 74 20 66 69 6c 65 20 64 6f 65 73 20 6e 6f 74 20 65 78 69 73 74 2e 0d 0a 53 77 69 74 63 68 3a 20 30 0d 0a	MSBUILD : error MSB1009: Project file does not exist...Switch: 0..	success or wait	1	8EA897	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	unknown	441	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 58 6d 6c 5c 35 32 37 63 39 33 33 31 39 34 66 33 61 39 39 61 38 31 36 64 38 33 63 36 31 39 61 33 65 31 64 33 5c 53 79 73 74 65 6d 2e 58 6d 6c 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0 .50727_32\System\1ffc437de59fb 69ba2b865ffdc98ffd1\System.ni. dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\System.Xml\527c933194f3a99a816d8 3c619a3e1d3\System.Xml.ni.dll",0..2,"Microsof	success or wait	1	7273A33A	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	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72498738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	8EA897	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	8EA897	ReadFile

Analysis Process: conhost.exe PID: 6704 Parent PID: 6652

General

Start time:	13:01:19
Start date:	19/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: 6948 Parent PID: 3292

General

Start time:	13:01:25
Start date:	19/01/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xcd0000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	724660AC	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	724660AC	unknown
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	724660AC	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	724660AC	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	15BA897	WriteFile
\Device\ConDrv	unknown	169	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 42 75 69 6c 64 20 45 6e 67 69 6e 65 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 0d 0a 5b 4d 69 63 72 6f 73 6f 66 74 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 2c 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 5d 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 20 32 30 30 35 2e 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) Build Engine Version 2.0.50727.8922.. [Microsoft .NET Framework, Version 2.0. 50727.8922]..Copyright (C) Microsoft Corporation 2005. All rights reserved.....	success or wait	1	15BA897	WriteFile
\Device\ConDrv	unknown	137	4d 53 42 55 49 4c 44 20 3a 20 65 72 72 6f 72 20 4d 53 42 31 30 30 33 3a 20 53 70 65 63 69 66 79 20 61 20 70 72 6f 6a 65 63 74 20 6f 72 20 73 6f 6c 75 74 69 6f 6e 20 66 69 6c 65 2e 20 54 68 65 20 63 75 72 72 65 6e 74 20 77 6f 72 6b 69 6e 67 20 64 69 72 65 63 74 6f 72 79 20 64 6f 65 73 20 6e 6f 74 20 63 6f 6e 74 61 69 6e 20 61 20 70 72 6f 6a 65 63 74 20 6f 72 20 73 6f 6c 75 74 69 6f 6e 20 66 69 6c 65 2e 0d 0a	MSBUILD : error MSB1003: Specify a project or solution file. The current working directory does not contain a project or solution file...	success or wait	1	15BA897	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	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72498738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	15BA897	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	15BA897	ReadFile

Analysis Process: conhost.exe PID: 6956 Parent PID: 6948

General

Start time:	13:01:25
Start date:	19/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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