

JOeSandbox Cloud BASIC



ID: 679145

Sample Name: JOB-in.line e.K. -
New Order 56899707.exe

Cookbook: default.jbs

Time: 10:47:06

Date: 05/08/2022

Version: 35.0.0 Citrine

Table of Contents

Table of Contents	2
Windows Analysis Report JOB-in.line e.K. - New Order 56899707.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: AveMaria	4
Yara Signatures	4
Memory Dumps	4
Unpacked PEs	5
Sigma Signatures	5
Snort Signatures	5
Joe Sandbox Signatures	6
AV Detection	6
Exploits	6
Networking	6
E-Banking Fraud	6
System Summary	6
Data Obfuscation	6
Boot Survival	6
Hooking and other Techniques for Hiding and Protection	6
Malware Analysis System Evasion	6
HIPS / PFW / Operating System Protection Evasion	6
Lowering of HIPS / PFW / Operating System Security Settings	7
Stealing of Sensitive Information	7
Remote Access Functionality	7
Mitre Att&ck Matrix	7
Behavior Graph	7
Screenshots	8
Thumbnails	8
Antivirus, Machine Learning and Genetic Malware Detection	9
Initial Sample	9
Dropped Files	9
Unpacked PE Files	9
Domains	10
URLs	10
Domains and IPs	10
Contacted Domains	10
Contacted URLs	10
URLs from Memory and Binaries	10
World Map of Contacted IPs	12
Public IPs	12
General Information	12
Warnings	13
Simulations	13
Behavior and APIs	13
Joe Sandbox View / Context	13
IPs	13
Domains	13
ASNs	13
JA3 Fingerprints	13
Dropped Files	13
Created / dropped Files	13
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\JOB-in.line e.K. - New Order 56899707.exe.log	13
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	14
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_evf3gbui.whq.psm1	14
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mkbfbupc.mhm.ps1	14
C:\Users\user\AppData\Local\Temp\tmpF006.tmp	15
C:\Users\user\AppData\Roaming\gATZIsOK.exe	15
C:\Users\user\AppData\Roaming\gATZIsOK.exe:Zone.Identifier	15
C:\Users\user\Documents\20220805\PowerShell_transcript.065367.PYT_AdW3.20220805104819.txt	16
Static File Info	16
General	16
File Icon	16
Static PE Info	16
General	16
Entrypoint Preview	17
Data Directories	18
Sections	19
Resources	19
Imports	19

Network Behavior	19
Snort IDS Alerts	19
TCP Packets	20
Statistics	20
Behavior	20
System Behavior	20
Analysis Process: JOB-in.line e.K. - New Order 56899707.exePID: 1700, Parent PID: 6108	21
General	21
File Activities	21
File Created	21
File Deleted	21
File Written	22
File Read	23
Analysis Process: powershell.exePID: 5000, Parent PID: 1700	23
General	23
File Activities	24
File Created	24
File Deleted	24
File Written	24
File Read	26
Analysis Process: conhost.exePID: 5064, Parent PID: 5000	30
General	30
Analysis Process: schtasks.exePID: 488, Parent PID: 1700	30
General	30
File Activities	30
File Read	30
Analysis Process: conhost.exePID: 4436, Parent PID: 488	30
General	30
Analysis Process: JOB-in.line e.K. - New Order 56899707.exePID: 396, Parent PID: 1700	31
General	31
File Activities	31
File Created	31
File Read	31
Registry Activities	31
Key Created	31
Key Value Created	32
Disassembly	32

Windows Analysis Report

JOB-in.line e.K. - New Order 56899707.exe

Overview

General Information

Sample Name:	JOB-in.line e.K. - New Order 56899707.exe
Analysis ID:	679145
MD5:	9e8d620f00f7988.
SHA1:	27e5c643563bfe..
SHA256:	7907827ba24412..
Tags:	exe
Infos:	

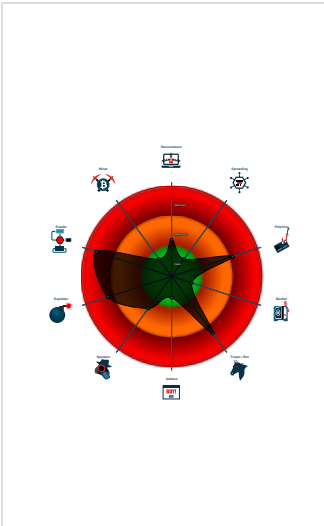
Detection

AveMaria, UACMe	
Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Multi AV Scanner detection for subm...
Malicious sample detected (through...
Yara detected AntiVM3
Yara detected UACMe UAC Bypass...
Yara detected AveMaria stealer
Multi AV Scanner detection for drop...
Snort IDS alert for network traffic
Initial sample is a PE file and has a...
Increases the number of concurrent...
Contains functionality to hide user a...
Tries to detect sandboxes and other...
Machine Learning detection for sam...

Classification



Process Tree

System is w10x64
JOB-in.line e.K. - New Order 56899707.exe (PID: 1700 cmdline: "C:\Users\user\Desktop\JOB-in.line e.K. - New Order 56899707.exe" MD5: 9E8D620F00F7988A79AE5C1228F37899) - powershell.exe (PID: 5000 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roamin glgATZIsOK.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10) - conhost.exe (PID: 5064 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496) - schtasks.exe (PID: 488 cmdline: C:\Windows\System32\schtasks.exe /Create /TN "Updates\lgATZIsOK" /XML "C:\Users\user\AppData\Local\Temp\tmpF006.tmp MD5: 15FF7D8324231381BAD48A052F85DF04) - conhost.exe (PID: 4436 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496) - JOB-in.line e.K. - New Order 56899707.exe (PID: 396 cmdline: C:\Users\user\Desktop\JOB-in.line e.K. - New Order 56899707.exe MD5: 9E8D620F00F7988A79AE5C1228F37899)
cleanup

Malware Configuration

Threatname: AveMaria

<pre>{ "C2 url": "20.91.187.223", "port": 5707 }</pre>
--

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
--------	------	-------------	--------	---------

Source	Rule	Description	Author	Strings
00000009.00000003.391271404.0000000000C88000.0000004.00000020.00020000.00000000.sdmp	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	0xa20:\$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} 0x3828:\$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} 0xa20:\$c1: Elevation:Administrator!new: 0x3828:\$c1: Elevation:Administrator!new:
00000009.00000003.391271404.0000000000C88000.0000004.00000020.00020000.00000000.sdmp	JoeSecurity_UAC Me	Yara detected UACMe UAC Bypass tool	Joe Security	
00000009.00000003.391610814.0000000000C87000.0000004.00000020.00020000.00000000.sdmp	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	0x1230:\$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} 0x1230:\$c1: Elevation:Administrator!new:
00000009.00000003.391610814.0000000000C87000.0000004.00000020.00020000.00000000.sdmp	JoeSecurity_UAC Me	Yara detected UACMe UAC Bypass tool	Joe Security	
00000009.00000000.385551724.000000000054F000.00000040.00000400.00020000.00000000.sdmp	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	0xdf0:\$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} 0xdf0:\$c1: Elevation:Administrator!new:
Click to see the 23 entries				

Unpacked PEs				
Source	Rule	Description	Author	Strings
9.3.JOB-in.line e.K. - New Order 56899707.exe.c8aa a8.1.raw.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	0xd80:\$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
9.3.JOB-in.line e.K. - New Order 56899707.exe.c8aa a8.1.raw.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	0xd80:\$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} 0xd80:\$c1: Elevation:Administrator!new:
9.3.JOB-in.line e.K. - New Order 56899707.exe.c8aa a8.1.raw.unpack	JoeSecurity_UAC Me	Yara detected UACMe UAC Bypass tool	Joe Security	
9.3.JOB-in.line e.K. - New Order 56899707.exe.c874 b0.4.unpack	Codoso_Gh0st_2	Detects Codoso APT Gh0st Malware	Florian Roth	0x970:\$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} 0x1b78:\$s13: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09}
9.3.JOB-in.line e.K. - New Order 56899707.exe.c874 b0.4.unpack	Codoso_Gh0st_1	Detects Codoso APT Gh0st Malware	Florian Roth	0x970:\$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} 0x1b78:\$x3: Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} 0x970:\$c1: Elevation:Administrator!new: 0x1b78:\$c1: Elevation:Administrator!new:
Click to see the 80 entries				

Sigma Signatures	
 No Sigma rule has matched	

Snort Signatures	
ET TROJAN Ave Maria/Warzone RAT Encrypted CnC Checkin (Inbound) - Source IP: 20.91.187.223 - Destination IP: 192.168.2.6	
Timestamp:	20.91.187.223192.168.2.65707497642036735 08/05/22-10:48:28.518524
SID:	2036735
Source Port:	5707
Destination Port:	49764
Protocol:	TCP
Classtype:	A Network Trojan was detected
ET TROJAN Ave Maria/Warzone RAT Encrypted CnC Checkin - Source IP: 192.168.2.6 - Destination IP: 20.91.187.223	
Timestamp:	192.168.2.620.91.187.2234976457072036734 08/05/22-10:48:28.721248
SID:	2036734
Source Port:	49764
Destination Port:	5707
Protocol:	TCP

Classtype:	A Network Trojan was detected
------------	-------------------------------

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Yara detected AveMaria stealer

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Exploits



Yara detected UACMe UAC Bypass tool

Networking



Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

E-Banking Fraud



Yara detected AveMaria stealer

System Summary



Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation



.NET source code contains potential unpacker

Boot Survival



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

Hooking and other Techniques for Hiding and Protection



Contains functionality to hide user accounts

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

Malware Analysis System Evasion



Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion



Adds a directory exclusion to Windows Defender

Lowering of HIPS / PFW / Operating System Security Settings



Increases the number of concurrent connection per server for Internet Explorer

Stealing of Sensitive Information



Yara detected AveMaria stealer

Remote Access Functionality

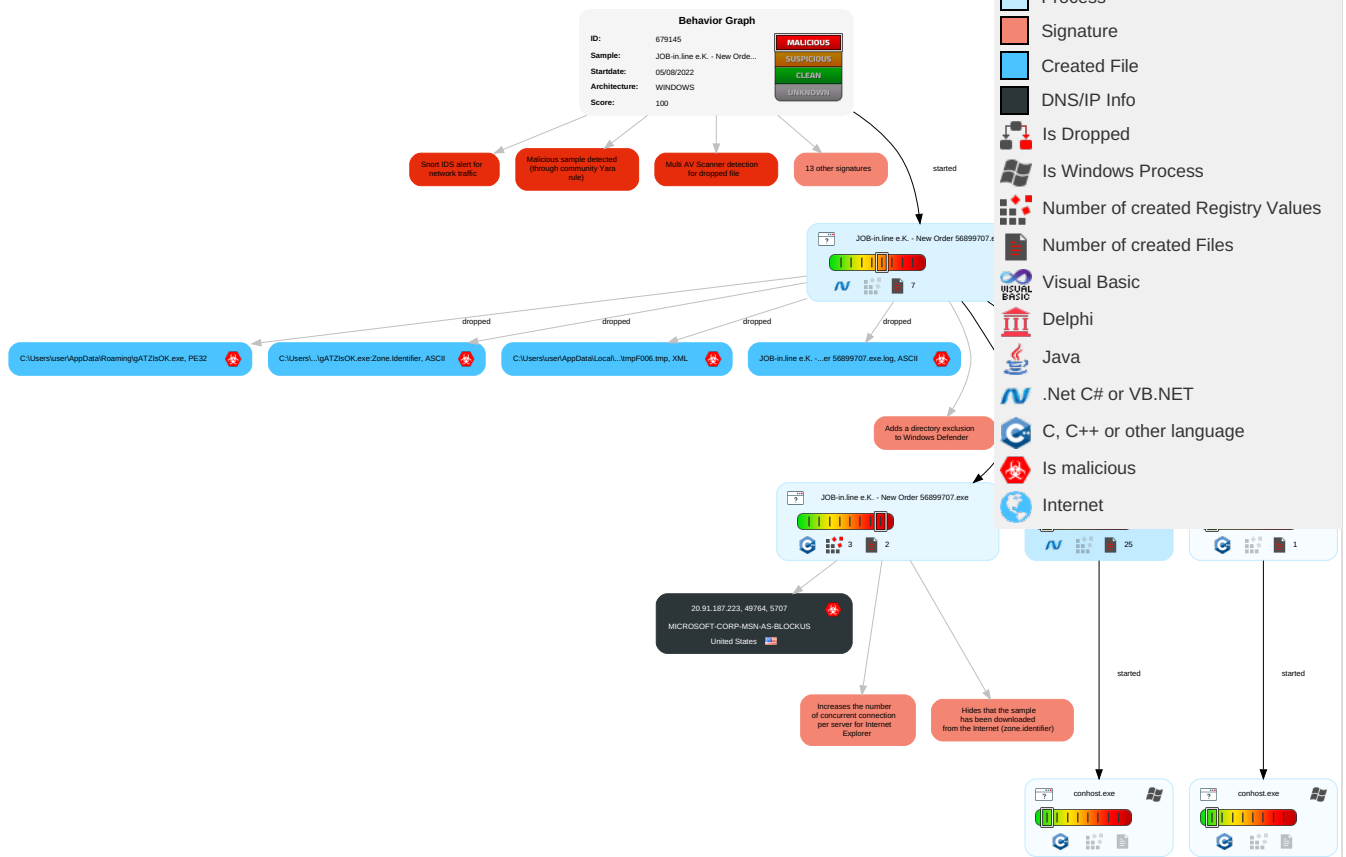


Yara detected AveMaria stealer

Mitre Att&ck Matrix

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

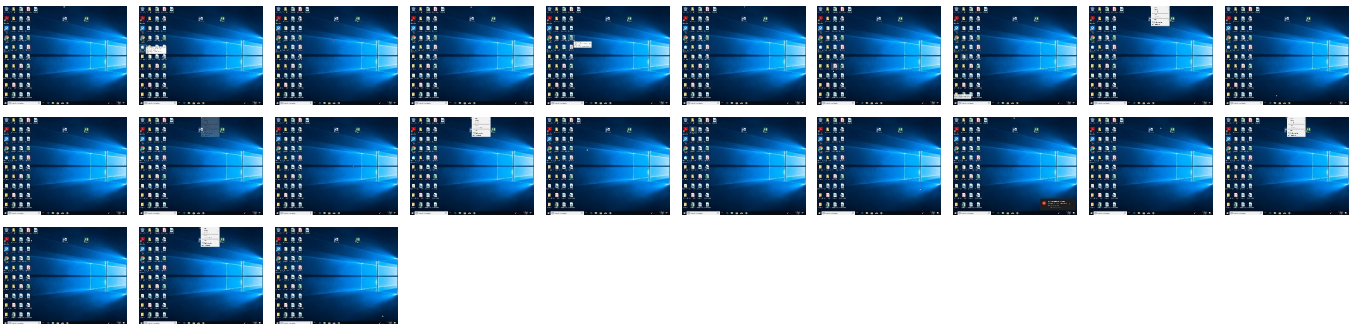
Behavior Graph



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
JOB-in.line e.K. - New Order 56899707.exe	36%	Virustotal		Browse
JOB-in.line e.K. - New Order 56899707.exe	26%	ReversingLabs	ByteCode-MSIL.Trojan.LokiBot	
JOB-in.line e.K. - New Order 56899707.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\gATZIsOK.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\gATZIsOK.exe	26%	ReversingLabs	ByteCode-MSIL.Trojan.LokiBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.JOB-in.line e.K. - New Order 56899707.exe.45e4a20.8.unpack	100%	Avira	TR/AD.MortyStaler.utbzg		Download File
9.0.JOB-in.line e.K. - New Order 56899707.exe.400000.0.unpack	100%	Avira	TR/Redcap.ghjpt		Download File

Domains
 No Antivirus matches

URLs				
Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
20.91.187.223	0%	Avira URL Cloud	safe	
http://www.fontbureau.comldva	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

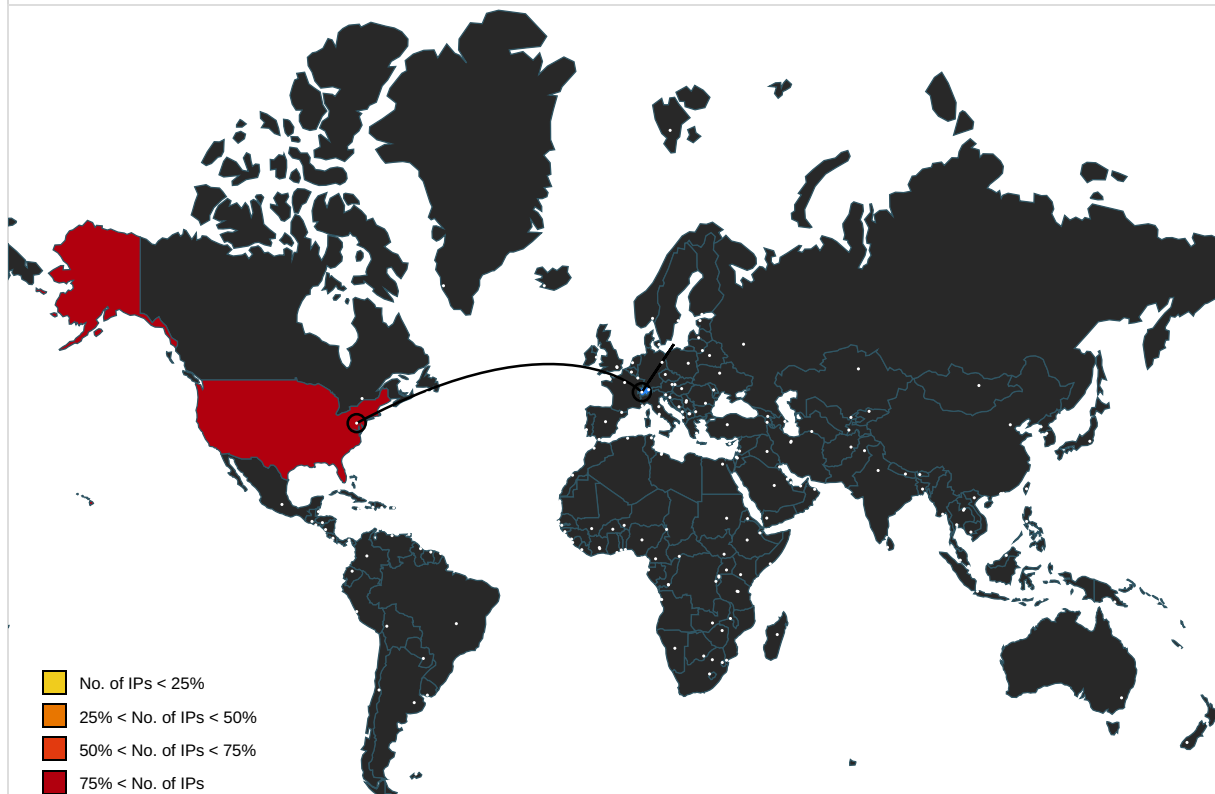
Domains and IPs
Contacted Domains
 No contacted domains info

Contacted URLs			
Name	Malicious	Antivirus Detection	Reputation
20.91.187.223	true	Avira URL Cloud: safe	unknown

URLs from Memory and Binaries				
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.396315425.00000000006B72000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.396315425.00000000006B72000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.396315425.00000000006B72000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.396315425.00000000006B72000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.396315425.00000000006B72000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.396315425.00000000006B72000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.396315425.00000000006B72000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.396315425.0000000006B72000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.396315425.0000000006B72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.396315425.0000000006B72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.396315425.0000000006B72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.396315425.0000000006B72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.396315425.0000000006B72000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.396315425.0000000006B72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.396315425.0000000006B72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.396315425.0000000006B72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.396315425.0000000006B72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.396315425.0000000006B72000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comldva	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.388743797.0000000000C07000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comm	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.388743797.0000000000C07000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.396315425.0000000006B72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.396315425.0000000006B72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.396315425.0000000006B72000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.396315425.0000000006B72000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.396315425.0000000006B72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.396315425.0000000006B72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.396315425.0000000006B72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://github.com/syohex/java-simple-mine-sweeperC:	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.394220155.00000000045C4000.00000004.00000800.00020000.00000000.sdmp, JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.392150523.0000000002D16000.00000004.00000800.00020000.00000000.sdmp, JOB-in.line e.K. - New Order 56899707.exe, 00000000.9.00000000.384273881.000000000414000.00000040.00000400.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nam e	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.392150523.0000000002D16000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	JOB-in.line e.K. - New Order 56899707.exe, 00000000.0.00000002.396315425.0000000006B72000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
20.91.187.223	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679145
Start date and time: 05/08/202210:47:06	2022-08-05 10:47:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	JOB-in.line e.K. - New Order 56899707.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:	26
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.phis.troj.expl.evad.winEXE@9/8@0/1
EGA Information:	Successful, ratio: 100%
HDC Information:	Failed

HCA Information:	• Successful, ratio: 90% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:48:14	API Interceptor	1x Sleep call for process: JOB-in.line e.K. - New Order 56899707.exe modified
10:48:21	API Interceptor	40x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

 No context
--

Domains

 No context
--

ASNs

 No context
--

JA3 Fingerprints

 No context
--

Dropped Files

 No context
--

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\JOB-in.line e.K. - New Order 56899707.exe.log 

Process:	C:\Users\user\Desktop\JOB-in.line e.K. - New Order 56899707.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1750

Entropy (8bit):	5.3375092442007315
Encrypted:	false
SSDEEP:	48:MIHK5HKXE1qHiYHKHqNoPtHoxHhAHKzvFHYHKIEHUzvAHj:Pq5qXEwCYqhQnoPtIxHeqzN4qm0z4D
MD5:	92FEE17DD9A6925BA2D1E5EF2CD6E5F2
SHA1:	4614AE0DD188A0FE1983C5A8D82A69AF5BD13039
SHA-256:	67351D6FA9F9E11FD21E72581AFDC8E63A284A6080D99A6390641FC11C667235
SHA-512:	C599C633D288B845A7FAA31FC0FA86EAB8585CC2C515D68CA0DFC6AB16B27515A5D729EF535109B2CDE29FF3CF4CF725F4F920858501A2421FC7D76C804F2A7
Malicious:	true
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni .dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a", "C:\Windows\assembly\NativeImages_v4.0.30319_32\S ystem.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b 77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\1b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22272
Entropy (8bit):	5.601254883343104
Encrypted:	false
SSDEEP:	384:BiCDA0e8ndTFv2qYSYJnsjsh77Y9g9SJ3xa1BMrm7Z1AV7xJZ664I+iyY:WdTd3YpJsohf9cBa4aA
MD5:	06205E11A9DF526F2FF7C403468FAEE6
SHA1:	904AA9587BD6994C944D823093E8F048B79A09EE
SHA-256:	0B6176302F9885786D720731275335DA302FE07154377C9D17DC0AADB50F420C
SHA-512:	CAAF33F6012E680E9F8D6C251459B24DE7A40DAE4DD1E7BB44DC126B9C77A58B38ED0B4BFAC41F40CA2A4B279821255E674671D4B38DEFC90BCA14B589A40 CCA
Malicious:	false
Reputation:	low
Preview:	@...e.....y.....R.U.I.(...@.c.....@.....H.....<@.^L."My...P.... .Microsoft.PowerShell.ConsoleHostD.....fZve...F....x.).....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o..A...4B.....System..4.....Zg5...:O..g..q.....System.Xml.L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'.....L..}).....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management..4.....].D.E..#.....System.Data.H..... ..H..m)aUu.....Microsoft.PowerShell.Security...<.....~..[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...\$.1.q.....System.ConfigurationP...../C..J..%...].....%Microsoft.PowerShell.Commands.Utility...D.....-D.F.<.;.nt.1System.Configuration.Ins

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_evf3gbiu.whq.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_mkbubpc.mhm.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0

Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmpF006.tmp 	
Process:	C:\Users\user\Desktop\JOB-in.line e.K. - New Order 56899707.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1607
Entropy (8bit):	5.115469344505131
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1K2ky1mo2dUnrKMhEMOFGpwOzNgU3ODOiQRvh7hwrgXuNtL6xvn:cgea6YrFdOFzOzN33ODOiDdKrsuT6v
MD5:	72EF6E87E7FD36C98FB3FCBDC5E917B1
SHA1:	A17031F96BEB591193C1DCE943DD756F10E10248
SHA-256:	300C48EBA80425F4A8FFFC85462E37CAFE816A8B8498DBFA4A0991F86C307419
SHA-512:	3D60068AD6982944419549B32D7FEC6F72A00DE1FA6688E72D3FE5936C58AF82C87B63692A391C4B89F058D6354D5A3493CACB285E1A5D681E8DE7FEB5C4E04
Malicious:	true
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailab

C:\Users\user\AppData\Roaming\gATZIsOK.exe  	
Process:	C:\Users\user\Desktop\JOB-in.line e.K. - New Order 56899707.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	862720
Entropy (8bit):	7.020056015678397
Encrypted:	false
SSDEEP:	12288:2k2oQCM0fSnakWL9Kh+gww5ysdG5Ggdy/hkKJg6SKlpxw8r:xtSWL Yh+geG5Gs2TnLlpxw8
MD5:	9E8D620F00F7988A79AE5C1228F37899
SHA1:	27E5C643563BFE8DBCCF7E26E9669C2CDDE8E767
SHA-256:	7907827BA244123DDC19A986203A2DF7F7B9E7D984FF8EFE6715372E2F431062
SHA-512:	39CD5593B238C32E0644448F6E1845760CE1A56F551A97217F2EA72C7AD72725564A2B568166B84712B12B5949A0146D7C355B4756E6985311E0451F5D09F2B0
Malicious:	true
Antivirus:	- Antivirus: Joe Sandbox ML, Detection: 100% - Antivirus: ReversingLabs, Detection: 26%
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.PE..L...t@.....0.....v.....@.....@.....\$.O.....H.....text......H......rsrc.....@.....@.reloc.....@.....@..B.....X.....H.....@..P.....\$.8.....}.....{.....0.....*.....0..W.....f..p..s.....~O.....o.....r\$.p..B.....(.....S.....o.....S.....o.....{.....&.....&.....0.....*.....Tc.....}k.....0.....0.....+..{.....0!...0"....0#...o\$.B.....(.....*...0..n.....f..p..s.....o.....f..p..B...(%).....(&.....B...(.....S.....o(f.....r..p()...&...&.....o.....*.....KZ..

C:\Users\user\AppData\Roaming\gATZIsOK.exe:Zone.Identifier 	
Process:	C:\Users\user\Desktop\JOB-in.line e.K. - New Order 56899707.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309

SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	true
Preview:	[ZoneTransfer]....Zoneld=0

C:\Users\user\Documents\20220805\PowerShell_transcript.065367.PYT_AdW3.20220805104819.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5811
Entropy (8bit):	5.370569364110241
Encrypted:	false
SSDEEP:	96:BZETLJNUc3qDo1ZjwZ+TLJNUc3qDo1Znf5njZ2TLJNUc3qDo1ZkeXXiZB:HAKIt
MD5:	2A825DC0186F01C76867E670AED74AF9
SHA1:	52C519B2EE900428B8D62828224132F13318020D
SHA-256:	3BFA4373B1F437FDA466ED109927F63B11806415ED8F9AA8A5D2076D87E5C769
SHA-512:	D9EAE585E8CBBDCB0243FAB70F45A5E65395AF4CC65B57727FFB988044A269C524AF80BA69BC3A07884E80103C47128EE8CD5C2FC920D47B4C3CA507E6250717
Malicious:	false
Preview:	.*****.Windows PowerShell transcript start..Start time: 20220805104820..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 065367 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\gATZIsOK.exe..Process ID: 5000..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..*****.*****.Command start time: 20220805104820..*****.PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\gATZIsOK.exe..*****.Windows PowerShell transcript start..Start time: 20220805105300..Username: computer\user..RunAs User: DESKTOP-7

Static File Info	
General	
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.020056015678397
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:	JOB-in.line e.K. - New Order 56899707.exe
File size:	862720
MD5:	9e8d620f00f7988a79ae5c1228f37899
SHA1:	27e5c643563bfe8dbccf7e26e9669c2cdde8e767
SHA256:	7907827ba24123ddc19a986203a2df7f7b9e7d984ff8efe6715372e2f431062
SHA512:	39cd5593b238c32e0644448f6e1845760ce1a56f551a97217f2ea72c7ad72725564a2b568166b84712b12b5949a0146d7c355b4756e6985311e0451f5d09f2b0
SSDEEP:	12288:2k2oQCM0fSNakWL9Kh+gww5ysdG5Ggdy/hkKJg6SKlpxw8r:xTSWLyh+geG5Gs2TnLlpxw8
TLSH:	DA05CF41B6BA9A12C5740FB0DBA181500F34AD1B7D71F6CEE85835A63B71BB78B106CE
File Content Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode....\$......PE..L....t@.....0.....v....@... ..@.....

File Icon	
	
Icon Hash:	30f0f8e4e0e0e060

Static PE Info	
General	
Entrypoint:	0x4ac276
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui

Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0xD34074E5 [Fri Apr 24 00:40:05 2082 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xac224	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xae000	0x28008	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xac208	0x1c	.text
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	0xaa294	0xaa400	False	0.8028577000734214	data	7.443954108514022	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xae000	0x28008	0x28200	False	0.1154047410436137	data	2.9852524877320703	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd8000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources					
Name	RVA	Size	Type	Language	Country
RT_ICON	0xae280	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xbeaa8	0x94a8	data		
RT_ICON	0xc7f50	0x5488	data		
RT_ICON	0xcd3d8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_ICON	0xd1600	0x25a8	data		
RT_ICON	0xd3ba8	0x10a8	data		
RT_ICON	0xd4c50	0x988	data		
RT_ICON	0xd55d8	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xd5a40	0x76	data		
RT_VERSION	0xd5ab8	0x364	data		
RT_MANIFEST	0xd5e1c	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports	
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior
Snort IDS Alerts

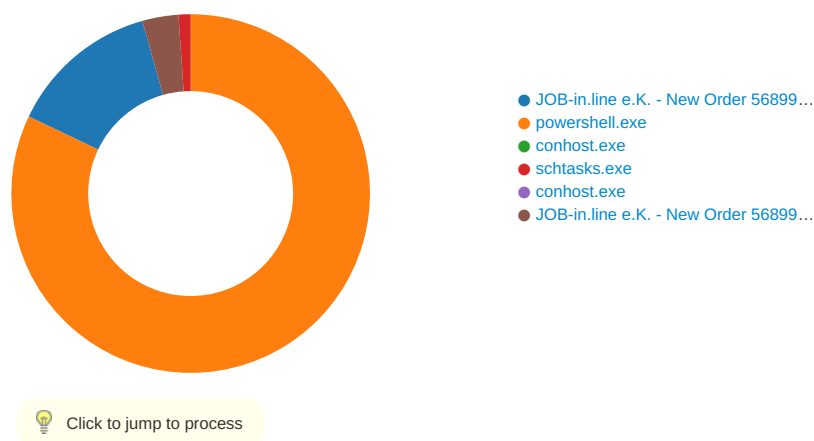
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
20.91.187.223192.168.2.6 5707497642036735 08/05/22- 10:48:28.518524	TCP	2036735	ET TROJAN Ave Maria/Warzone RAT Encrypted CnC Checkin (Inbound)	5707	49764	20.91.187.223	192.168.2.6
192.168.2.620.91.187.223 4976457072036734 08/05/22- 10:48:28.721248	TCP	2036734	ET TROJAN Ave Maria/Warzone RAT Encrypted CnC Checkin	49764	5707	192.168.2.6	20.91.187.223

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 5, 2022 10:48:28.439207077 CEST	49764	5707	192.168.2.6	20.91.187.223
Aug 5, 2022 10:48:28.478080034 CEST	5707	49764	20.91.187.223	192.168.2.6
Aug 5, 2022 10:48:28.478790045 CEST	49764	5707	192.168.2.6	20.91.187.223
Aug 5, 2022 10:48:28.518523932 CEST	5707	49764	20.91.187.223	192.168.2.6
Aug 5, 2022 10:48:28.721247911 CEST	49764	5707	192.168.2.6	20.91.187.223
Aug 5, 2022 10:48:28.810730934 CEST	5707	49764	20.91.187.223	192.168.2.6
Aug 5, 2022 10:48:48.518804073 CEST	5707	49764	20.91.187.223	192.168.2.6
Aug 5, 2022 10:48:48.519543886 CEST	49764	5707	192.168.2.6	20.91.187.223
Aug 5, 2022 10:48:48.607975960 CEST	5707	49764	20.91.187.223	192.168.2.6
Aug 5, 2022 10:49:08.521075010 CEST	5707	49764	20.91.187.223	192.168.2.6
Aug 5, 2022 10:49:08.524054050 CEST	49764	5707	192.168.2.6	20.91.187.223
Aug 5, 2022 10:49:08.603039980 CEST	5707	49764	20.91.187.223	192.168.2.6
Aug 5, 2022 10:49:28.520616055 CEST	5707	49764	20.91.187.223	192.168.2.6
Aug 5, 2022 10:49:28.521457911 CEST	49764	5707	192.168.2.6	20.91.187.223
Aug 5, 2022 10:49:28.605835915 CEST	5707	49764	20.91.187.223	192.168.2.6
Aug 5, 2022 10:49:48.533683062 CEST	5707	49764	20.91.187.223	192.168.2.6
Aug 5, 2022 10:49:48.534974098 CEST	49764	5707	192.168.2.6	20.91.187.223
Aug 5, 2022 10:49:48.622869015 CEST	5707	49764	20.91.187.223	192.168.2.6
Aug 5, 2022 10:50:08.534110069 CEST	5707	49764	20.91.187.223	192.168.2.6
Aug 5, 2022 10:50:08.534837008 CEST	49764	5707	192.168.2.6	20.91.187.223
Aug 5, 2022 10:50:08.623394966 CEST	5707	49764	20.91.187.223	192.168.2.6

Statistics

Behavior



System Behavior

General

Target ID:	0
Start time:	10:48:05
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\JOB-in.line e.K. - New Order 56899707.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\JOB-in.line e.K. - New Order 56899707.exe"
Imagebase:	0x6d0000
File size:	862720 bytes
MD5 hash:	9E8D620F00F7988A79AE5C1228F37899
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000000.00000002.394220155.00000000045C4000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000000.00000002.394220155.00000000045C4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.394220155.00000000045C4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000002.394220155.00000000045C4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AveMaria_31d2bce9, Description: unknown, Source: 00000000.00000002.394220155.00000000045C4000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000000.00000002.392150523.0000000002D16000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.392150523.0000000002D16000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000000.00000002.392150523.0000000002D16000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.392150523.0000000002D16000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000000.00000002.392150523.0000000002D16000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AveMaria_31d2bce9, Description: unknown, Source: 00000000.00000002.392150523.0000000002D16000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	6CE2CF06	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	6CE2CF06	unknown
C:\Users\user\AppData\Roaming\gATZIsOK.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	6BC7DD66	CopyFileW
C:\Users\user\AppData\Roaming\gATZIsOK.exe\Zone.Identifier:\$DATA	read data or list directory synchronize generic write	device	sequential only synchronous io non alert	success or wait	1	6BC7DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpF006.tmp	read attributes synchronize generic read	device	synchronous io non alert non directory file	success or wait	1	6BC77038	GetTempFile NameW
C:\Users\user\AppData\Local\Microsoft\CLR\v4.0_32\UsageLogs\JOB-in.line e.K. - New Order 56899707.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6D13C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF006.tmp	success or wait	1	6BC76A95	DeleteFileW

File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\gATZIsOK.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd 74 40 fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 0a 00 00 fd 02 00 00 00 00 00 76 fd 0a 00 00 20 00 00 00 fd 0a 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 0d 00 00 02 00 00 00 00 00 00 02 00 40 fd 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.\$PELt@0v @ @	success or wait	4	6BC7DD66	CopyFileW
C:\Users\user\AppData\Roaming\gATZIsOK.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	6BC7DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpF006.tmp	0	1607	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 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 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 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 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 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f	<?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	success or wait	1	6BC71B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0.32\UsageLogs\JOB-in.line e.K. - New Order 56899707.exe.log	0	1750	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","N otApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, Publ icKeyToken=b77a5c561934e089"," C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D13C907	WriteFile

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE05705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CE05705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD603DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE0CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD603DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD603DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD603DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD603DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE05705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CE05705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC71B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC71B4F	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentation5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6CD603DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6CD603DE	ReadFile	

Analysis Process: powershell.exe PID: 5000, Parent PID: 1700	
General	
Target ID:	5
Start time:	10:48:17
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\gATZIsOK.exe
Imagebase:	0xf10000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10

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

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	6CE2CF06	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	6CE2CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscripPolicyTest_mkbfbupc.mhm.ps1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6BC71E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscripPolicyTest_evf3gbui.whq.psm1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6BC71E60	CreateFileW
C:\Users\user\Documents\20220805	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6BC7BEFF	CreateDirectoryW
C:\Users\user\Documents\20220805\PowerShell_transcript.065367.PYT_AdW3.20220805104819.txt	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	6BC71E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mkbfbupc.mhm.ps1	success or wait	1	6BC76A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_evf3gbui.whq.psm1	success or wait	1	6BC76A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscripPolicyTest_mkbfbupc.mhm.ps1	0	1	31	1	success or wait	1	6BC71B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscripPolicyTest_evf3gbui.whq.psm1	0	1	31	1	success or wait	1	6BC71B4F	WriteFile
C:\Users\user\Documents\20220805\PowerShell_transcript.065367.PYT_AdW3.20220805104819.txt	0	3	ff		success or wait	1	6BC71B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StarterProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 16 3b 40 01 1b 3b 40 01 19 3b 40 01 fd 3c 40 01 fd 3c 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 fd 3c 40 01 57 03 40 01 4d 03 40 01 fd 45 40 01 38 4d 40 01 3f 4d 40 01 42 4d 00 01 fd 44 00 01 6d 45 00	T@>@@V@H@X@[@N T@HT@S@S@hT@S@ S@S@\\@T@T@X@? X@T@S@S@T@T@xT @zT@ T@=M@DM@:M@"M@ M@!M@;@;@;<@<@ ;M@D@D@M@<M@\$ M@<@W@M@E@8M@ ?M@BMDmE	success or wait	11	6D0F76FC	WriteFile

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CE05705	unknown	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CE05705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE05705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CE05705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae4ee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CD603DE	ReadFile	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CE0CA54	ReadFile	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CE0CA54	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE0CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\fd8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD603DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD603DE	ReadFile	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CE05705	unknown	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CE05705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD603DE	ReadFile	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CE05705	unknown	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CE05705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6CD603DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CE05705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CE05705	unknown	
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StarterProfileData-NonInteractive	unknown	64	success or wait	1	6CE11F73	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD603DE	ReadFile	
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile	
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6BC71B4F	ReadFile	
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile	
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile	

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6BC71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6BC71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6BC71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6BC71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6BC71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6BC71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6BC71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	110	6BC71B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTaskAppBackgroundTask.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTaskAppBackgroundTask.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6CD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CD603DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CD603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CD603DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CE05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CE05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	770	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	4	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6CE05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6CE05705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	4096	success or wait	3	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	770	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	74	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6BC71B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6BC71B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6BC71B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	2	6BC71B4F	ReadFile

Analysis Process: conhost.exe PID: 5064, Parent PID: 5000

General	
Target ID:	6
Start time:	10:48:17
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
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: 488, Parent PID: 1700

General	
Target ID:	7
Start time:	10:48:18
Start date:	05/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\gATZIsOK" /XML "C:\Users\user\AppData\Local\Temp\tmpF006.tmp
Imagebase:	0x10d0000
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\tmpF006.tmp	unknown	2	success or wait	1	10DAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpF006.tmp	unknown	1608	success or wait	1	10DABD9	ReadFile

Analysis Process: conhost.exe PID: 4436, Parent PID: 488

General	
Target ID:	8
Start time:	10:48:20
Start date:	05/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff6406f0000
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: JOB-in.line e.K. - New Order 56899707.exe PID: 396, Parent PID: 1700

General	
Target ID:	9
Start time:	10:48:22
Start date:	05/08/2022
Path:	C:\Users\user\Desktop\JOB-in.line e.K. - New Order 56899707.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\JOB-in.line e.K. - New Order 56899707.exe
Imagebase:	0x5e0000
File size:	862720 bytes
MD5 hash:	9E8D620F00F7988A79AE5C1228F37899
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	- Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000009.00000003.391271404.0000000000C88000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth - Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000009.00000003.391271404.0000000000C88000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000009.00000003.391610814.0000000000C87000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth - Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000009.00000003.391610814.0000000000C87000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: Codoso_Gh0st_1, Description: Detects Codoso APT Gh0st Malware, Source: 00000009.00000000.385551724.000000000054F000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth - Rule: JoeSecurity_UACMe, Description: Yara detected UACMe UAC Bypass tool, Source: 00000009.00000000.385551724.000000000054F000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000009.00000000.384273881.0000000000414000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000009.00000000.384273881.0000000000414000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security - Rule: Windows_Trojan_AveMaria_31d2bce9, Description: unknown, Source: 00000009.00000000.384273881.0000000000414000.00000040.00000400.00020000.00000000.sdmp, Author: unknown - Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000009.00000003.391249495.0000000000C98000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 00000009.00000003.391249495.0000000000C98000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security - Rule: Windows_Trojan_AveMaria_31d2bce9, Description: unknown, Source: 00000009.00000003.391249495.0000000000C98000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities							
File Created							
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft Vision\	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	4135ED	CreateDirectoryW

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Users\user\Desktop\JOB-in.line e.K. - New Order 56899707.exe	unknown	862720	success or wait	1	411E78	ReadFile	
C:\Users\user\Desktop\JOB-in.line e.K. - New Order 56899707.exe	unknown	862720	success or wait	1	411E78	ReadFile	

Registry Activities	
Key Created	

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\BS8JRXAM5E	success or wait	1	410F94	RegCreateKeyExW

Key Value Created							
Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings	MaxConnectionsPer1_0Server	dword	10	success or wait	1	413550	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings	MaxConnectionsPerServer	dword	10	success or wait	1	413565	RegSetValueExA

Disassembly

 No disassembly