ID: 830334
Sample Name: AEAT-Notificaci#U00f3n..rar
Cookbook: defaultwindowsinteractivecookbook.jbs
Time: 09:20:30
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

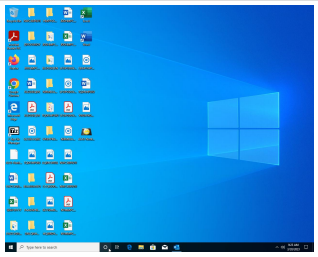
Windows Analysis Report

AEAT-Notificaci#U00f3n..rar

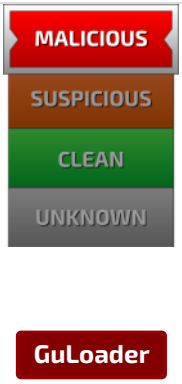
Overview

General Information

Sample Name:	AEAT-Notificaci#U00f3n..rar
Analysis ID:	830334
MD5:	dd05bf773b3d2..
SHA1:	a26d39292e8d...
SHA256:	c00e9a2a34c6...
Infos:	



Detection



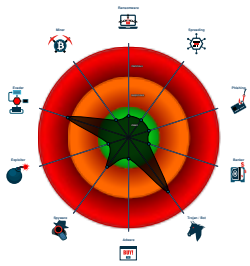
GuLoader

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

Signatures

- Yara detected GuLoader
- Tries to detect virtualization through…
- Queries the volume information (nam…
- Found dropped PE file which has no…
- Drops PE files

Classification



Process Tree

- **System is w10x64_ra**
- OUTLOOK.EXE (PID: 4560 cmdline: "C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE" /PIM NoEmail MD5: CA3FDE8329DE07C95897DB0D828545CD)
- OpenWith.exe (PID: 6736 cmdline: C:\Windows\system32\OpenWith.exe -Embedding MD5: 5D37A62943F1071FFFFE1DE74B8F2778)
- 7zG.exe (PID: 6944 cmdline: "C:\Program Files\7-Zip\7zG.exe" x -o"C:\Users\alfredo\Desktop\" -an -ai#7zMap6823:108:7zEvent2591 MD5: 04FB3AE7F05C8BC333125972BA907398)
- AEAT-Notificaci n..exe (PID: 7024 cmdline: "C:\Users\alfredo\Desktop\AEAT-Notificaci n..exe" MD5: FE2CE03E16418D24EEA8A3EB5CFE1DD5)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
CloudEyE, GuLoader	CloudEyE (initially named GuLoader) is a small VB5/6 downloader. It typically downloads RATs/Stealers, such as Agent Tesla, Arkei/Vidar, Formbook, Lokibot, Netwire and Remcos, often but not always from Google Drive. The downloaded payload is xored.	No Attribution	• https://0x00sec.org/t/ana… • https://blog.malwarebytes… • https://blog.morphisec.co… • https://blog.vincss.net/20… • https://cert-agid.gov.it/ne…	https://malpedia.caad.fkie.…

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.2683502888.0000000004633000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Data Obfuscation

Yara detected GuLoader

Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

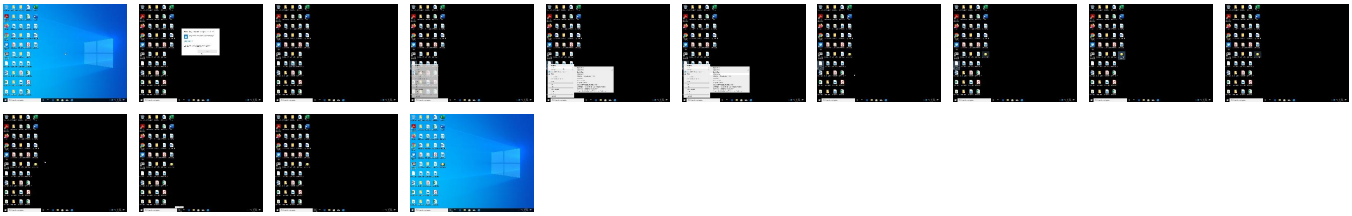
Mitre Att&ck Matrix

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	Windows Management Instrumentation	1 Windows Service	1 Windows Service	1 Masquerading	OS Credential Dumping	1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Process Injection	1 Virtualization/Sandbox Evasion	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Process Injection	Security Account Manager	1 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	1 1 1 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

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
AEAT-Notificaci#U00f3n..rar	3%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\alfredo\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\ftre\Peroba\Udviklers\Unsingableness\System.Reflection.Primitives.dll	0%	ReversingLabs		
C:\Users\alfredo\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\ftre\Peroba\Udviklers\Unsingableness\System.Reflection.Primitives.dll	0%	Virustotal		Browse
C:\Users\alfredo\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\ftre\Peroba\Udviklers\Unsingableness\System.Reflection.TypeExtensions.dll	0%	ReversingLabs		
C:\Users\alfredo\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\ftre\Peroba\Udviklers\Unsingableness\System.Reflection.TypeExtensions.dll	0%	Virustotal		Browse
C:\Users\alfredo\AppData\Local\Temp\nsICA0A.tmp\AdvSplash.dll	0%	ReversingLabs		
C:\Users\alfredo\AppData\Local\Temp\nsICA0A.tmp\AdvSplash.dll	3%	Virustotal		Browse
C:\Users\alfredo\AppData\Local\Temp\nsICA0A.tmp\System.dll	0%	ReversingLabs		
C:\Users\alfredo\Desktop\AEAT-Notificaci n..exe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

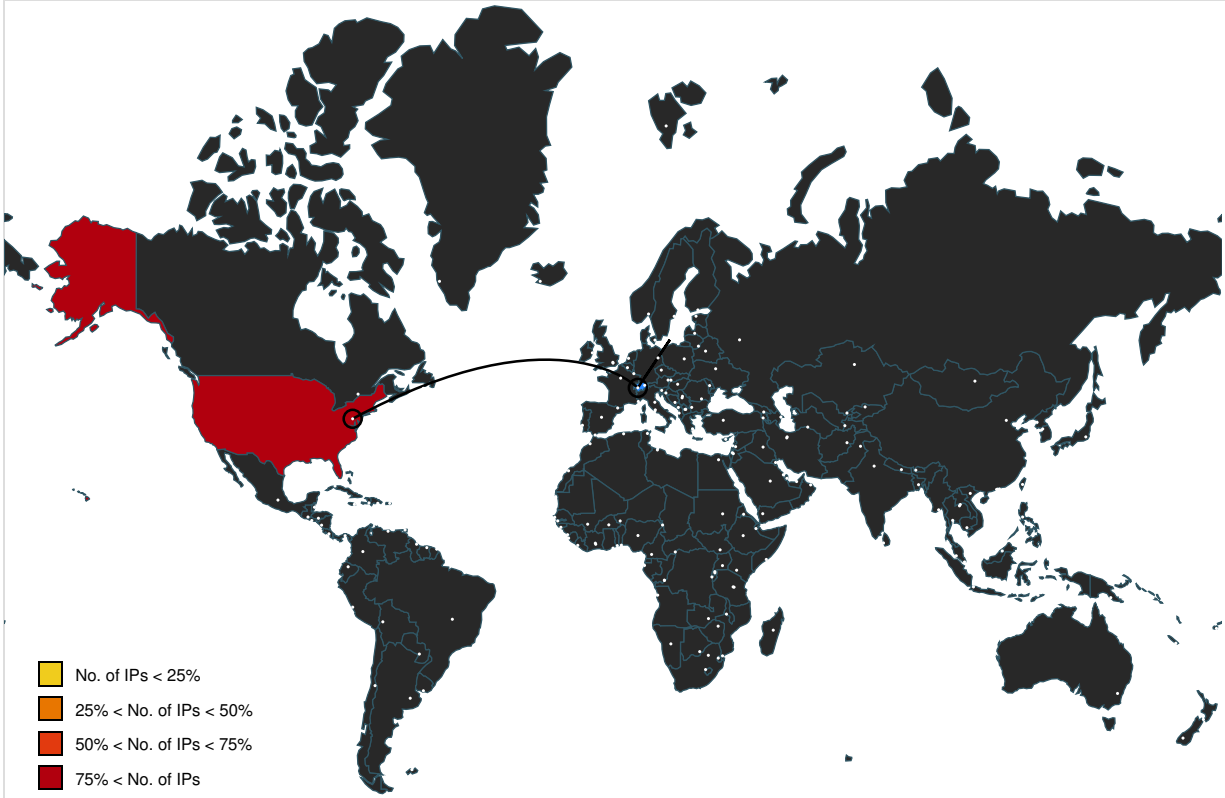
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.109.8.45	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
192.229.221.95	unknown	United States		15133	EDGECASTUS	false
52.109.88.191	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830334
Start date and time:	2023-03-20 09:20:30 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	

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:	10
Number of new started drivers analysed:	0
Number of existing processes analysed:	1
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• EGA enabled
Analysis Mode:	stream
Analysis stop reason:	Timeout
Sample file name:	AEAT-Notificaci#U00f3n..rar
Detection:	MAL
Classification:	mal52.troj.evad.winRAR@3/16@0/19

Warnings

- Exclude process from analysis (whitelisted): SIHClient.exe, usocoreworker.exe, svchost.exe
- Excluded domains from analysis (whitelisted): login.live.com
- 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.
- Report size getting too big, too many NtSetInformationFile calls found.
- VT rate limit hit for: C:\Users\alfredo\AppData\Local\Temp\nsiCA0A.tmp\System.dll

Created / dropped Files

C:\Users\alfredo\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\Melaenic.mil

Process:	C:\Users\alfredo\Desktop\AEAT-Notificaci n..exe
File Type:	data
Category:	dropped
Size (bytes):	225254
Entropy (8bit):	7.359675827547892
Encrypted:	false
SSDEEP:	
MD5:	5674661083BA2E6903DB69C253682AD0
SHA1:	75C8C397677A778AA479B699F9F94F9299635561
SHA-256:	14422C6CFC0B73AC9B882D9471F81FAD84FB8ADCA9F6AE26E5197AD96CA7D90F
SHA-512:	A8009AB181CAE3753DDC9868032CF0B791BC57D2E17CB17F091ABD1F86A17D67AA2367A47FE31A518191EFC3F399E67462DE3F8EC63C0CAD9E09AF9BE0D34F C6
Malicious:	false
Reputation:	low
Preview:	..........pppp...pp....4.....ii....PP..L.....MMMMM.....i.....A.d....(.....W.222.ss.....PPPPPPP.....a.....PP.....DD.....11111..... ....DD..]..... =..<.!..7777..;.....p...###..V.....&..V.....M...L.6.....~.....B.....%.Z.....]]..... J.....X...A.....:.,.Y..... .....{.....ss.....%%.....mm.....444444....I.....|.....7.....ppp.....].||.....ww.9...II....9....z.....!!.....XX.&&...RR.....f. F..>.....E.a.....=.....LLLL.....s.....---.9.....$$...J...:KK.<.....??..Z.,.....v...!.....+++++.....L.....; ;;;;..d..D..L..... ..*.....ttt....i.....KK.....#.....M.....n...

C:\Users\alfredo\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\ftre\Peroba\Udviklers\Unsingableness\Oversaturated.Bil

Process:	C:\Users\alfredo\Desktop\AEAT-Notificaci n..exe
File Type:	ASCII text, with very long lines (26818), with no line terminators
Category:	dropped
Size (bytes):	26818
Entropy (8bit):	2.7236675414283296
Encrypted:	false
SSDEEP:	
MD5:	8F73411385AA2F4BF5CDF54248F86ABE
SHA1:	676D41087832C418180C206151601686AAEC6B55
SHA-256:	D76B20E8714264A7B1099E5386D6AA8D2486C162EA70C76F5C549143CDFF2E21

SHA-512:	28F17FFE463819ACCBBB8391A814591C351D4A6F103A53526EC1B5746C8CE8457B0B0D4A0CFC2EC05132FD305B1E4CA9A42FBBFB7FBA0D3614AFF9523ACB2AAA
Malicious:	false
Reputation:	low
Preview:	00AE00E400009A004200000000FEFEFE0000AC003F3F0000D6D600003A3A0000007A0035353500002E2E2E2E000000020000880084000FAFA00000000 00C7C7C7000800A7A70052520000ABABABAB0000AE005B5B0000CF0035353535350000D900535300004D0018004242000000D000DFDF007000AA00 006F000000000000A3A3A3A300E7E70000A4A4004400DCDCDC005C5C5C009D000000D200E7E7E70000060606060000600000000DD0000006B6B6B6B6B 003D3D0000E60000005252520000B1000000080808000FF006A00000000006B6B00002E000909000089000091919100000094008282828200007A002300BEBE00 00C200CACACACA00930000B500B300009F9F00000000002B000053535300008686860000D8D8D800001C1C1C000800080808008080000009400110000000011000 00004E000096960000000000570000000000000000D4D4D4D4D400323200F6005F000000A800000F00EB00004E000000003F00F100F800003A3A00005E5E5E0071 00F9F9F9006800A5A50000003C0000004D0000D2D2D200A7A7000000C7C7C7C7000000DFDFDF00FE007B006767000000002300430 0A5A50000E500BE 0000A5000000D8D80000D60000000500000007E000C0C0000003131006900680000C3C3C300FCFCFCFCFCFC0000006363636300E6E6E600A900C1002F 2F00002C2C

C:\Users\alfredo\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\ftre\Peroba\Udviklers\Unsingableness\System.Reflection.Primitives.dll

Process:	C:\Users\alfredo\Desktop\AEAT-Notificaci n..exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	14952
Entropy (8bit):	6.599053939997928
Encrypted:	false
SSDEEP:	
MD5:	EDA04E04EBC0EBF7F8BBF30C4DAE6DE3
SHA1:	7BC4D50E6EEC7F04A9272BFEE4E4DB6F278DBE63
SHA-256:	F3E55CB3ADFA93F563B09114D93062E680AB0864C220491458FBE151798B862F
SHA-512:	7027DA3404675596B71394B660E600DA12C0750895F624776362167869760555EE9990699FFC9E4407301FC9437B2F638E2734B8BDEF3C7054990FD5A9C86550
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....."!..0.....^+... .....@.. ....`.....+..K....@.....h$...`.....T*..8..... ....H.....text...d.... ....`.rsrc.....@.....@..@.rel oc.....`.....@..B.....@+.....H..... .....P .....H>.s..X.\...3V...?G../..3q..I.L.....qKy6b..u"HO...JmYQ.....J..,.*S..".R..=1RY. ....\?.&dM.....@'J.j.:.'.A.../.....I.BSJB.....v4.0.30319.....`.....#~.....#Strings.....#GUID.....#Blob.....3.....3.....@..... .Y.....`.....g...?.g.....g...y.g.....g.....g...`.g...m.g.....

C:\Users\alfredo\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\ftre\Peroba\Udviklers\Unsingableness\System.Reflection.TypeExtensions.dll

Process:	C:\Users\alfredo\Desktop\AEAT-Notificaci n..exe
File Type:	PE32+ executable (DLL) (console) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	32368
Entropy (8bit):	6.393948275188786
Encrypted:	false
SSDEEP:	
MD5:	F2A123183E106BB1CF19376A8079D171
SHA1:	2B96296BE92D5F2EF7C59A70858AF4CAABC99A9D
SHA-256:	896D4ED138C35ECF19AE432380096562872EAB103F7E352C15D214FD875B337A
SHA-512:	FCA6A89EFB16780A06CD25A55638882970F03E1535180A0E463AF9794184B04EB345CF29B12D4F261094E04A584E9225A7AD36A62631227451059F64A77B3C67
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....[....." .....P..... ..`...@.....@..... .....<.....Z..p$...p.....T.....H.....text....N.....P..... ..`.data.....`.....R..... .....@....reloc.....p.....X.....@..B.....0.....4...V.S._.V.E.R.S.I.O.N._.I.N.F.O.....y.....?.....D.....V.a.r.F. i.l.e.I.n.f.o.....$.....T.r.a.n.s.l.a.t.i.o.n.....S.t.r.i.n.g.F.i.l.e.I.n.f.o.....0.0.0.0.0.4.b.0...Z.!...C.o.m.m.e.n.t.s...S.y.s.t.e.m...R.e.f.l.e.c.t.i.o.n...T.y.p.e.E.x.t.e.n.s.i.o.n.s.....L... ..C.o.m.p.a.n.y.N.a.m.e.....M.i.c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n...j.!...F.i.l.e.D.e.s.c.r.i.p.

C:\Users\alfredo\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\ftre\Peroba\Udviklers\Unsingableness\battery-level-90-charging-symbolic.svg

Process:	C:\Users\alfredo\Desktop\AEAT-Notificaci n..exe
File Type:	SVG Scalable Vector Graphics image

Category:	dropped
Size (bytes):	6689
Entropy (8bit):	5.135211840989561
Encrypted:	false
SSDEEP:	
MD5:	C96D0DD361AFC6B812BDDD390B765A26
SHA1:	71081F096719CAA70B9BAEF86FE642635D8E2765
SHA-256:	6690799E5FA3FB0DD6CCE4BAC5AA1607C8A6BB16507854A87520C7DE53052E1B
SHA-512:	7C73BC880A9401C64AB0571957B414180C1B94137C7BC870BA602979E7A990640A37991CB87A40BC7E5942A37FDA25EFC58C759C00F4344BA3D88B9AA64182D
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="no"?>.<svg. xmlns:dc="http://purl.org/dc/elements/1.1/". xmlns:cc="http://creativecommons.org/ns#". xmlns :rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#". xmlns:svg="http://www.w3.org/2000/svg". xmlns="http://www.w3.org/2000/svg". width="16". version="1.1". style ="enable-background:new". id="svg7384". height="16.000036">. <metadata. id="metadata90">. <rdf:RDF>. <cc:Work. rdf:about="">. <dc:format>i mage/svg+xml</dc:format>. <dc:type. rdf:resource="http://purl.org/dc/dcmitype/StillImage" />. <dc:title>Gnome Symbolic Icons</dc:title>. <c c:license. rdf:resource="http://creativecommons.org/licenses/by-sa/4.0/" />. </cc:Work>. <cc:License. rdf:about="http://creativecommons.org/li censes/by-sa/4.0/">. <cc:permits. rdf:resource="http://creativecommons.org/ns#Reproduction" />. <cc:permits. rdf:resource="htt

C:\Users\alfredo\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\ftre\Peroba\Udviklers\Unsingableness\colorimeter-colorhug-sym bolic.symbolic.png

Process:	C:\Users\alfredo\Desktop\AEAT-Notificaci n..exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	227
Entropy (8bit):	6.604776901672149
Encrypted:	false
SSDEEP:	
MD5:	7843C38CC42C6786B3373F166AF10172
SHA1:	BA0163109D9B641B1312230B3F62E1E10A61AA5E
SHA-256:	E3AF1293F8E8AB5C81300196AF55A7C15D5608291D46A2B86D4255910A7D0E59
SHA-512:	B1D3DF6A0A8CACD729CD9A2FD5AB0F74ED611270FA172CDBEB13D46FA71DD5CC5540A2FBFDB6C3004E652D317C8FAD4EC3AE437DF1C082B629870A33CC6 D34F
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...1..P.....#.bae....^.^K/fek+.....X.....gfw....\.D/..b...a.4..$.....H#....o8...}..6.K.....Xc.$ ..'.1.2..vu.../O..>V.....CD....< ....w.....IEND.B`.

C:\Users\alfredo\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\ftre\Peroba\Udviklers\Unsingableness\media-playlist-consecutive-symbolic.svg

Process:	C:\Users\alfredo\Desktop\AEAT-Notificaci n..exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	1329
Entropy (8bit):	4.950241534342892
Encrypted:	false
SSDEEP:	
MD5:	021A9F00A28C9D496E490AE951E8EF12
SHA1:	F8A6392065D07BAC72E138B0E47A24FFDCCEE74B
SHA-256:	B420561770B77FCB47F69B6198B34B11155535F8A2E907BC4A0998CE74AFD340
SHA-512:	7F4F2D904EA968BF68E35E0D7F1EAE9718234757D1989879996BFB49D9C447F67544CB0E1C441FD6539D58B5F2C6ACA7E9E0208738C235D9AF0C093511760212
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g fill="#474747"><path d="M1.018 7v2H14V7z" style="line-height:normal;font-variant-ligatures:nor mal;font-variant-position:normal;font-variant-caps:normal;font-variant-numeric:normal;font-variant-alternates:normal;font-feature-settings:normal;text-indent:0;text-align :start;text-decoration-line:none;text-decoration-style:solid;text-decoration-color:#000;text-transform:none;text-orientation:mixed;shape-padding:0;isolation:auto;mix-blend-mode:normal;marker:none" color="#bebebe" font-weight="400" font-family="sans-serif" overflow="visible"/><path d="M11.99 4.99a1 1 0 00-.697 1.717L12.586 8l-1.293 1.293a1 1 0 101.414 1.414L15.414 8l-2.707-2.707a1 1 0 00-.717-.303z" style="line-height:normal;font-variant-ligatures:normal;font-variant-position:normal;font-variant-caps:normal;font-variant-numeric:normal;font-variant-alternates:normal;font-feature-settings:normal;text-indent:0;text-align:start;text-decoration-line:none;text-decorati

C:\Users\alfredo\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\ftre\Peroba\Udviklers\Unsingableness\network-offline-symbolic.svg

Process:	C:\Users\alfredo\Desktop\AEAT-Notificaci n..exe
File Type:	SVG Scalable Vector Graphics image

Category:	dropped
Size (bytes):	1155
Entropy (8bit):	5.154592341044034
Encrypted:	false
SSDEEP:	
MD5:	EFB3C780BC44B346B50B1F0DC6CF6D0F
SHA1:	472B0EDD1C4C3092BC7C4DF934ABE126885B1780
SHA-256:	990859D3B2C830E23EC276BF1D38A38EE1BA3D89BF04CB138107E4CDE31167B5
SHA-512:	5B9C96F146C6A065C89172D02BDE8020876DC9C78859AD2B8B9529C615215F88BA85C2789544F5C5A247C148BB52FE4B5FCA325E7EAC4826D31A0365A0B8BCE E
Malicious:	false
Reputation:	low
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><g fill="#474747"><path d="M5 7c-.31 0-.615.09-.812.281L.594 11l3.656 3.719c.198.19.44.281.75.281 h1v-1c0-.257-.13-.529-.312-.719L4.406 12H9s1 0 1-1c0 0 0-1-1-1H4.375l1.219-1.281C5.776 8.529 6 8.257 6 8V7z" style="line-height:normal;-inkscape-font-specificat ion:Sans;text-indent:0;text-align:start;text-decoration-line:none;text-transform:none;marker:none" color="#000" font-weight="400" font-family="Sans" overflow="visible" op acity=".35"/><path d="M11 11h1.375l1.125 1.094L14.594 11H16v1.469l-1.094 1.062L16 14.594V16h-1.438L13.5 14.937 12.437 16H11v-1.406l1.063-1.063L11 12.47z" style="marker:none" color="#bebebe" overflow="visible"/><path d="M11 9c.31 0 .615-.09.813-.281L15.406 5 11.75 1.281C11.552 1.091 11.31 1 11 1h-1v1c0 .257.13 .529.313.719L11.593 4H7c-.528-.007-1 .472-1 1s.472 1.007 1 1h4.625l-1.219 1.281c-.182.19-.406.462-.406.719v1z" style="line-height:normal;-inkscape-font-specific ation:Sans;text-indent:0;text-align:star

C:\Users\alfredo\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\ftre\Peroba\Udviklers\Unsingableness\network-wireless.png

Process:	C:\Users\alfredo\Desktop\AEAT-Notificaci n..exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	891
Entropy (8bit):	7.745720384539504
Encrypted:	false
SSDEEP:	
MD5:	5AF147D26AD399F83825377F04FD56A1
SHA1:	B378A498B0DB8114C794E21D533E80CEBE5DDE04
SHA-256:	6147A091847FCC9D9EDB22E655C4FC9DE6632C76D4252350400FA286F9791109
SHA-512:	EEC16DE49A4698FE4F03F841FBCF045FBBDC9D634EB73ED35DB544B6DB4BC0135CD8E1DF102FD1E8BDE9FC75380948B4C0459685EE2C21858D645B7973759I A6
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a...BIDATx.m.S.%9...$U.Fkl.y].m.6.m.F..5*g;k}.....P.....~u.....M.....M.q.....\|OM>....:?>.X7.U..j.v..?...e....>.Jk.&.{.[=.....t.d.....4.D... V....b..s.L.....Jg,..=V..@.n.....Rqv...._....B.h.;l....A....r.ap....N...1./.O.2.u7#.../.....o..*..O...[..X,<. .....@v.....t...H..Rf..C?q..8.HB.!{K..N.....t..5..1d.+.....).....pL.5.R..=....jC". ...t6.BA.)....xZ..d..^W~yU...ya.....U/...VA.r.....r.U....[".D.).8..iO<..[.....t.e9S...K8!....K..&p..Y2l.....".P8:..v..0....zd.."....O?+^.. =..b....t..K../.....?.?5...c.[.f.nP.P.o....7..k..t.?P(..O >.H~...n..jh.'..]..SC.5M.....'.}.n..'...t..9..c*...Ki...t..1z..N.q...w.w..y..W...K7x.^..p....j...%..3.\|.....x...G.\|~..a.o.N.<.....wK...]..u.....`...(z.B!.?q.b..u..$(.#1..N...b.u...@h...|.w..g.. ..}i....?~.....1~...l..]h.....IEND.B`.

C:\Users\alfredo\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\ftre\Peroba\Udviklers\Unsingableness\preferences-desktop-font-symbolic.symbolic.png

Process:	C:\Users\alfredo\Desktop\AEAT-Notificaci n..exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	225
Entropy (8bit):	6.596645802250635
Encrypted:	false
SSDEEP:	
MD5:	F894266AB6A933B2FDA751E6490C319A
SHA1:	2D2D3635198FEEFCB64D1D6B3CDCCDC4EA3DF4B0
SHA-256:	95F533585B4C61936C369557B3B7E397E56545A4C9DB9A5BDDD0E9ABB7A7F7E7
SHA-512:	977ED04753C3CB2B883D03A2A55001F6FCC8617DC3060B6C25AB7E5C691C3F76049E7DEADC7F6567AB7E8DC8492DE2874E8E632CF3EAD7B39ABC8CC98D331 42
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8..1..@.E...".u.`..#.v.,r.[..1$..]B.@6.,,.e.....fwg...._)9.....y..[n...t.$g..:...P....@k.q.....W.. .PY.$z..x....t..(-~!.0$:P.t.....`..... .Ba..Y.....IEND.B`.

C:\Users\alfredo\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\ftre\Peroba\Udviklers\Unsingableness\task-due-symbolic.symbolic.png

Process:	C:\Users\alfredo\Desktop\AEAT-Notificaci n..exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	263
Entropy (8bit):	6.731374842054556
Encrypted:	false
SSDEEP:	
MD5:	003B524806C1CA654CAC6ED2EB883E1B
SHA1:	F6F6ACA125DC4DB3B33378404017B5EE7D21D334
SHA-256:	2899E53769FA741E2C0675A2C69D2C246A8F34601BEE58DD66B16261005962A9
SHA-512:	AA905997F9CE39F039E33C4CCA167C0137775D91B4929D918528BA00B92737C448EC46D91A4221644CCC00D1FCAA403AFF83F07276BAB6FD80D4B9E88E652F8
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...K..1.D.....g.e=.x.....[]....Y$J'..`.@.S)R.4.q.D.K....x..%..0>~.;}..^.X....Lt.f!..K.....D.&,.7,..BM..t@..}N..o.?.....Hv.J...(..r.. ..)L... .&..dT<..1y...X..X.....q...p..p.....IEND.B`.

C:\Users\alfredo\AppData\Local\Temp\Musicalises34\Coleman\Biarcuated\ftre\Peroba\Udviklers\Unsingableness\window-close.png

Process:	C:\Users\alfredo\Desktop\AEAT-Notificaci n..exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	337
Entropy (8bit):	7.143668471552015
Encrypted:	false
SSDEEP:	
MD5:	7FBFE5B0A7AD2A67AACFD8481F8DCA01
SHA1:	21BABB6B7EC4746835DB43DC6A69A4AF0EFECA2D
SHA-256:	0B4CD789E087F712F131FACCD754DC461774498DF3CA19B346D461D18A0AE622
SHA-512:	3A8F0D9653301F789A0588E848C40FFC92394461BF70A3421ABC85647F2C115948134FE9E161D055A11D200536356A15677D9C0E645346D27E122001F67FE22B
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a....IDATx..S.r.P..=7.cw.....W.m...=.....V....I...K.?#@D.0G.....R.rF..^$....p..b..f.<.T.z..... +..3#.v.K...$....pT.j.....[.....r..p....O.2.Y.T.,.....==...9{/.. .T./....Qa...3%....5...xmkI.7.1..P,g.%y..J..#^.e..I(.%jzI..#../..49...*..?#..I. =~..E.,MN@.....`...../...=.-...1....IEND.B`.

C:\Users\alfredo\AppData\Local\Temp\nslCA0A.tmp\AdvSplash.dll

Process:	C:\Users\alfredo\Desktop\AEAT-Notificaci n..exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	6144
Entropy (8bit):	4.496995234059773
Encrypted:	false
SSDEEP:	
MD5:	E8B67A37FB41D54A7EDA453309D45D97
SHA1:	96BE9BF7A988D9CEA06150D57CD1DE19F1FEC19E
SHA-256:	2AD232BCCF4CA06CF13475AF87B510C5788AA790785FD50509BE483AFC0E0BCF
SHA-512:	20EFFAE18EEBB2DF90D3186A281FA9233A97998F226F7ADEAD0784FBC787FEEE419973962F8369D8822C1BBCDFB6E7948D9CA6086C9CF90190C8AB3EC97F4C 38
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 3%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....+.Y.o.7Eo.7Eo.7Eo.6EF.7E..jEf.7E;..Em.7E..3En.7ERicho.7E..... ..PE..L.....uY.....!.....`..... .....P.....`$..E.... ..d.....@..$..... ..... .text..... ..`.rdata..... .....@..@.data.....0.....@....reloc.....@.....@..B..... ....

C:\Users\alfredo\AppData\Local\Temp\nslCA0A.tmp\System.dll

Process:	C:\Users\alfredo\Desktop\AEAT-Notificaci n..exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776

Entropy (8bit):	5.659384359264642
Encrypted:	false
SSDEEP:	
MD5:	8B3830B9DBF87F84DDD3B26645FED3A0
SHA1:	223BEF1F19E644A610A0877D01EADC9E28299509
SHA-256:	F004C568D305CD95EDBD704166FCD2849D395B595DFF814BCC2012693527AC37
SHA-512:	D13CFD98DB5CA8DC9C15723EEE0E7454975078A776BCE26247228BE4603A0217E166058EBADC68090AFE988862B7514CB8CB84DE13B3DE35737412A6F0A8AC3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...u.u.u...s.u.a....r.!..q....t....t.Richu.....PE..L.....uY.. .....!..... .....'.....0.....`.....2.....0..P.....P.....0..X.....text..... ..... ..... ..`.rdata..S....0.....$.....@..@.data...x....@.....(.....@....reloc..`....P.....*.....@..B..... .....

C:\Users\alfredo\Desktop\AEAT-Notificaci n..exe

Process:	C:\Program Files\7-Zip\7zG.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	433776
Entropy (8bit):	7.034150239029318
Encrypted:	false
SSDEEP:	
MD5:	FE2CE03E16418D24EEA8A3EB5CFE1DD5
SHA1:	49E3AB955C0C92FEB101CD039BC1891F950457C6
SHA-256:	36279C5DB2A42FA7B963EE7E816AB366EA1AB370BF08C94AAFD1D0A826601C7D
SHA-512:	F51A3C180290D1D3A443D7534AF838DA0FAD553258EA698B53ACFF204E3C29DC626CE0583F89C4B29F87682D3E2916F645B0A1624588F013AE01C36F4A7882F4
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!`G.@...@...@../OQ..@...@..I@../OS..@...c>..@..+F...@..Rich.@ .....PE..L.....uY.....d....:.....P3.....@.....?.....@.....=.h.....X|..."..... .....text....c.....d..... ..`.rdata.....h.....@..@.data...8.9.....|.....@....ndata...p....:.....rsrc...h.....=.....@..@..... ....

C:\Users\alfredo\Documents\Outlook Files\Outlook Data File - NoEmail.pst

Process:	C:\Program Files\Microsoft Office\root\Office16\OUTLOOK.EXE
File Type:	data
Category:	dropped
Size (bytes):	576
Entropy (8bit):	5.060946394820425
Encrypted:	false
SSDEEP:	
MD5:	D3EB80964CF05083D399F33AAF886424
SHA1:	D25168E766196FFDF14821BDA3876EF8000527AF
SHA-256:	37F68D3C5C5626F5E023D16E9257A254EF0CA37775779F1B6B8A927F2B78FCA7
SHA-512:	9CD78E928BE932E798EAC2E8636D456AE040E7F6AEE162BEF8DC0E5C774CC9A4E3B85A23DDEEC0C824B50FBF802D0467ECACCEB2745477D46D982437073AC1A7
Malicious:	false
Reputation:	low
Preview:	.6...AAAAAAA...AAAAA...A.A.A/ALAAAAAAAAAAAbA5AtA.!.AGA.A.bbA.A`A.].A%A.A...A AHA...AVA.A.n.AKA.A6d.A.A.A6.A~AEA...6.A.A..Ab.A...A...A...An.LA..bA...A. .bA..#A..bA5..A...6#.qA.^tA..&A.5.6..A..bA..A...6`.~A.G.6N..A..bA2..A...A6#.A.-.A.#.A...A.#cA...6*#.A.*bA..A...An..A...A..A..bA..A. bA..A.tbA.SAA.AbA.S.A.6.AF..A.L.A`..A. ..AN.A...A..(A.}.A...A.1.A...A..A...A...AV..A..AQ.yA._.AE.MA...A|.A...AU..A...6...A...6...A.?.6...A.H.A..A.9bAK.XA...A...A...A..DA..A...A.%bAZ.A.;b.q..A.#b...7A...Aw..A68 .AAA.AtA.6.....

Static File Info

General

File type:	RAR archive data, v5
Entropy (8bit):	7.9992452622577
TrID:	• RAR Archive (5005/1) 100.00%
File name:	AEAT-Notificaci#U00f3n..rar
File size:	297518
MD5:	dd05bf773b3d290ef4925014d0bd6e12
SHA1:	a26d39292e8d88b4c3efc90ea759d8a68980847e
SHA256:	c00e9a2a34c6b7a69d2ed42b92f07bfcd35134dd39fd19334b233c23da3118c6
SHA512:	7bc5688a674811e9bf271581ab0d020cd74c3bbe2d54fd300bbfb118f990a56a6bef37354ca723e47a3943ca9ca1f6c5c9b6e337a9b246d68de5b9390ab1f675
SSDEEP:	6144:1fIwoLdfwiWDbfUcf0BHDucvPXMM3svJeamdo33J8kjGmJMUQ7flF:PoLdfRWPfUc26cMM8Uq3Z8FcMjflF
TLSH:	005423BC88A769183AF9AD0DA14FF159D33BA054F3ED0472A05681393A63578E6EFD04
File Content Preview:	Rar!.....:.....r.35..... .I^h....AEAT-Notificaci..n..exe...7....Z....,T`.DT23G`hg.xQ....`41...6H.d.....x$H1<.`6.c..,g.D.....%!....I5..v2.M6I.^...5.i.....I..3[Cd.a..1....'9.\|..f$G'.G}....~.....]]._9..-_.?..U].s.,.....$.....

File Icon

Icon Hash:	74f0e4e4e4e4e0e4