ANY RUN
INTERACTIVE MALWARE ANALYSIS

General Info

File name:	DHL_11429040 영수증 문서, pdf.exe
Full analysis:	https://app.any.run/tasks/612b2704-20dc-4df1-b04d-4f00170a306c
Verdict:	Suspicious activity
Analysis date:	August 22, 2022 at 12:00:13
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Indicators:	
MIME:	application/x-dosexec
File info:	PE32 executable (GUI) Intel 80386, for MS Windows
MD5:	9D31002A80957FF0CC00FC9498A8D127
SHA1:	D57104AFA6C8A57E32A889873C40B30B40520C46
SHA256:	5BE5708B720B520F2292EC10196F47FF3A687843A529540D75C0D7621FAD247E
SSDEEP:	12288:fc+2ltCNEdmSene/lUrMP6PSzQbT7grJFcuHdl51T9u6mr:fMjdteed7qUflFcu9lyr

Software environment set and analysis options

Launch configuration

Task duration:	180 seconds	Heavy Evasion option:	off	Network geolocation:	off
Additional time used:	120 seconds	MITM proxy:	off	Privacy:	Public submission
Fakenet option:	on	Route via Tor:	off	Autoconfirmation of UAC:	on
Network:	on				

Software preset

- Internet Explorer 11.0.9600.19596 KB4534251
- Adobe Acrobat Reader DC (20.013.20064)
- Adobe Flash Player 32 ActiveX (32.0.0.453)
- Adobe Flash Player 32 NPAPI (32.0.0.453)
- Adobe Flash Player 32 PPAPI (32.0.0.453)
- Adobe Refresh Manager (1.8.0)
- CCleaner (5.74)
- FileZilla Client 3.51.0 (3.51.0)
- Google Chrome (86.0.4240.198)
- Google Update Helper (1.3.36.31)
- Java 8 Update 271 (8.0.2710.9)
- Java Auto Updater (2.8.271.9)
- Microsoft .NET Framework 4.5.2 (4.5.51209)
- Microsoft Office Access MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Access MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Access MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Access Setup Metadata MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Excel MUI (English) 2010 (14.0.6029.1000)
- Microsoft Office Excel MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Russian) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Spanish) 2010 (14.0.4763.1000)
- Microsoft Office Excel MUI (Turkish) 2010 (14.0.4763.1013)
- Microsoft Office Groove MUI (French) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (German) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Italian) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Japanese) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Korean) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)
- Microsoft Office Groove MUI (Russian) 2010 (14.0.4763.1000)

Hotfixes

- Client LanguagePack Package
- Client Refresh LanguagePack Package
- CodecPack Basic Package
- Foundation Package
- IE Hyphenation Parent Package English
- IE Spelling Parent Package English
- IE Troubleshooters Package
- InternetExplorer Optional Package
- InternetExplorer Package TopLevel
- KB2479943
- KB2491683
- KB2506212
- KB2506928
- KB2532531
- KB2533552
- KB2533623
- KB2534111
- KB2545698
- KB2547666
- KB2552343
- KB2560656
- KB2564958
- KB2574819
- KB2579686
- KB2585542
- KB2604115
- KB2620704
- KB2621440
- KB2631813
- KB2639308
- KB2640148
- KB2653956
- KB2654428
- KB2656356
- KB2660075
- KB2667402
- KB2676562
- KB2685811
- KB2685813
- KB2685939
- KB2690533

Microsoft Office Groove MUI (Spanish) 2010 (14.0.4763.1000)	KB2698365
Microsoft Office Groove MUI (Turkish) 2010 (14.0.4763.1013)	KB2705219
Microsoft Office IME (Japanese) 2010 (14.0.4763.1000)	KB2719857
Microsoft Office IME (Korean) 2010 (14.0.4763.1000)	KB2726535
Microsoft Office InfoPath MUI (French) 2010 (14.0.4763.1000)	KB2727528
Microsoft Office InfoPath MUI (German) 2010 (14.0.4763.1000)	KB2729094
Microsoft Office InfoPath MUI (Italian) 2010 (14.0.4763.1000)	KB2729452
Microsoft Office InfoPath MUI (Japanese) 2010 (14.0.4763.1000)	KB2731771
Microsoft Office InfoPath MUI (Korean) 2010 (14.0.4763.1000)	KB2732059
Microsoft Office InfoPath MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2736422
Microsoft Office InfoPath MUI (Russian) 2010 (14.0.4763.1000)	KB2742599
Microsoft Office InfoPath MUI (Spanish) 2010 (14.0.4763.1000)	KB2750841
Microsoft Office InfoPath MUI (Turkish) 2010 (14.0.4763.1013)	KB2758857
Microsoft Office Language Pack 2010 - French/Français (14.0.4763.1000)	KB2761217
Microsoft Office Language Pack 2010 - German/Deutsch (14.0.4763.1000)	KB2770660
Microsoft Office Language Pack 2010 - Italian/Italiano (14.0.4763.1000)	KB2773072
Microsoft Office Language Pack 2010 - Japanese/日本語 (14.0.4763.1000)	KB2786081
Microsoft Office Language Pack 2010 - Korean/한국어 (14.0.4763.1000)	KB2789645
Microsoft Office Language Pack 2010 - Portuguese/Português (Brasil) (14.0.4763.1000)	KB2799926
Microsoft Office Language Pack 2010 - Russian/русский (14.0.4763.1000)	KB2800095
Microsoft Office Language Pack 2010 - Spanish/Español (14.0.4763.1000)	KB2807986
Microsoft Office Language Pack 2010 - Turkish/Türkçe (14.0.4763.1013)	KB2808679
Microsoft Office O MUI (French) 2010 (14.0.4763.1000)	KB2813347
Microsoft Office O MUI (German) 2010 (14.0.4763.1000)	KB2813430
Microsoft Office O MUI (Italian) 2010 (14.0.4763.1000)	KB2820331
Microsoft Office O MUI (Japanese) 2010 (14.0.4763.1000)	KB2834140
Microsoft Office O MUI (Korean) 2010 (14.0.4763.1000)	KB2836942
Microsoft Office O MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2836943
Microsoft Office O MUI (Russian) 2010 (14.0.4763.1000)	KB2840631
Microsoft Office O MUI (Spanish) 2010 (14.0.4763.1000)	KB2843630
Microsoft Office O MUI (Turkish) 2010 (14.0.4763.1013)	KB2847927
Microsoft Office OneNote MUI (English) 2010 (14.0.6029.1000)	KB2852386
Microsoft Office OneNote MUI (French) 2010 (14.0.4763.1000)	KB2853952
Microsoft Office OneNote MUI (German) 2010 (14.0.4763.1000)	KB2857650
Microsoft Office OneNote MUI (Italian) 2010 (14.0.4763.1000)	KB2861698
Microsoft Office OneNote MUI (Japanese) 2010 (14.0.4763.1000)	KB2862152
Microsoft Office OneNote MUI (Korean) 2010 (14.0.4763.1000)	KB2862330
Microsoft Office OneNote MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2862335
Microsoft Office OneNote MUI (Russian) 2010 (14.0.4763.1000)	KB2864202
Microsoft Office OneNote MUI (Spanish) 2010 (14.0.4763.1000)	KB2868038
Microsoft Office OneNote MUI (Turkish) 2010 (14.0.4763.1013)	KB2871997
Microsoft Office Outlook MUI (English) 2010 (14.0.6029.1000)	KB2872035
Microsoft Office Outlook MUI (French) 2010 (14.0.4763.1000)	KB2884256
Microsoft Office Outlook MUI (German) 2010 (14.0.4763.1000)	KB2891804
Microsoft Office Outlook MUI (Italian) 2010 (14.0.4763.1000)	KB2893294
Microsoft Office Outlook MUI (Japanese) 2010 (14.0.4763.1000)	KB2893519
Microsoft Office Outlook MUI (Korean) 2010 (14.0.4763.1000)	KB2894844
Microsoft Office Outlook MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2900986
Microsoft Office Outlook MUI (Russian) 2010 (14.0.4763.1000)	KB2908783
Microsoft Office Outlook MUI (Spanish) 2010 (14.0.4763.1000)	KB2911501
Microsoft Office Outlook MUI (Turkish) 2010 (14.0.4763.1013)	KB2912390
Microsoft Office PowerPoint MUI (English) 2010 (14.0.6029.1000)	KB2918077
Microsoft Office PowerPoint MUI (French) 2010 (14.0.4763.1000)	KB2919469
Microsoft Office PowerPoint MUI (German) 2010 (14.0.4763.1000)	KB2923545
Microsoft Office PowerPoint MUI (Italian) 2010 (14.0.4763.1000)	KB2931356
Microsoft Office PowerPoint MUI (Japanese) 2010 (14.0.4763.1000)	KB2937610
Microsoft Office PowerPoint MUI (Korean) 2010 (14.0.4763.1000)	KB2943357
Microsoft Office PowerPoint MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2952664
Microsoft Office PowerPoint MUI (Russian) 2010 (14.0.4763.1000)	KB2968294
Microsoft Office PowerPoint MUI (Spanish) 2010 (14.0.4763.1000)	KB2970228
Microsoft Office PowerPoint MUI (Turkish) 2010 (14.0.4763.1013)	KB2972100
Microsoft Office Professional 2010 (14.0.6029.1000)	KB2972211
Microsoft Office Proof (Arabic) 2010 (14.0.4763.1000)	KB2973112
Microsoft Office Proof (Basque) 2010 (14.0.4763.1000)	KB2973201
Microsoft Office Proof (Catalan) 2010 (14.0.4763.1000)	KB2977292
Microsoft Office Proof (Dutch) 2010 (14.0.4763.1000)	KB2978120
Microsoft Office Proof (English) 2010 (14.0.6029.1000)	KB2978742
Microsoft Office Proof (French) 2010 (14.0.6029.1000)	KB2984972
Microsoft Office Proof (Galician) 2010 (14.0.4763.1000)	KB2984976
Microsoft Office Proof (German) 2010 (14.0.4763.1000)	KB2984976 SP1
Microsoft Office Proof (Italian) 2010 (14.0.4763.1000)	KB2985461

Microsoft Office Proof (Japanese) 2010 (14.0.4763.1000)	KB2991963
Microsoft Office Proof (Korean) 2010 (14.0.4763.1000)	KB2992611
Microsoft Office Proof (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB2999226
Microsoft Office Proof (Russian) 2010 (14.0.4763.1000)	KB3004375
Microsoft Office Proof (Spanish) 2010 (14.0.6029.1000)	KB3006121
Microsoft Office Proof (Turkish) 2010 (14.0.4763.1013)	KB3006137
Microsoft Office Proof (Ukrainian) 2010 (14.0.4763.1000)	KB3010788
Microsoft Office Proofing (English) 2010 (14.0.6029.1000)	KB3011780
Microsoft Office Proofing (French) 2010 (14.0.4763.1000)	KB3013531
Microsoft Office Proofing (German) 2010 (14.0.4763.1000)	KB3019978
Microsoft Office Proofing (Italian) 2010 (14.0.4763.1000)	KB3020370
Microsoft Office Proofing (Japanese) 2010 (14.0.4763.1000)	KB3020388
Microsoft Office Proofing (Korean) 2010 (14.0.4763.1000)	KB3021674
Microsoft Office Proofing (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3021917
Microsoft Office Proofing (Russian) 2010 (14.0.4763.1000)	KB3022777
Microsoft Office Proofing (Spanish) 2010 (14.0.4763.1000)	KB3023215
Microsoft Office Proofing (Turkish) 2010 (14.0.4763.1013)	KB3030377
Microsoft Office Publisher MUI (English) 2010 (14.0.6029.1000)	KB3031432
Microsoft Office Publisher MUI (French) 2010 (14.0.4763.1000)	KB3035126
Microsoft Office Publisher MUI (German) 2010 (14.0.4763.1000)	KB3037574
Microsoft Office Publisher MUI (Italian) 2010 (14.0.4763.1000)	KB3042058
Microsoft Office Publisher MUI (Japanese) 2010 (14.0.4763.1000)	KB3045685
Microsoft Office Publisher MUI (Korean) 2010 (14.0.4763.1000)	KB3046017
Microsoft Office Publisher MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3046269
Microsoft Office Publisher MUI (Russian) 2010 (14.0.4763.1000)	KB3054476
Microsoft Office Publisher MUI (Spanish) 2010 (14.0.4763.1000)	KB3055642
Microsoft Office Publisher MUI (Turkish) 2010 (14.0.4763.1013)	KB3059317
Microsoft Office SharePoint Designer MUI (French) 2010 (14.0.4763.1000)	KB3060716
Microsoft Office SharePoint Designer MUI (German) 2010 (14.0.4763.1000)	KB3061518
Microsoft Office SharePoint Designer MUI (Italian) 2010 (14.0.4763.1000)	KB3067903
Microsoft Office SharePoint Designer MUI (Japanese) 2010 (14.0.4763.1000)	KB3068708
Microsoft Office SharePoint Designer MUI (Korean) 2010 (14.0.4763.1000)	KB3071756
Microsoft Office SharePoint Designer MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3072305
Microsoft Office SharePoint Designer MUI (Russian) 2010 (14.0.4763.1000)	KB3074543
Microsoft Office SharePoint Designer MUI (Spanish) 2010 (14.0.4763.1000)	KB3075226
Microsoft Office SharePoint Designer MUI (Turkish) 2010 (14.0.4763.1013)	KB3078667
Microsoft Office Shared MUI (English) 2010 (14.0.6029.1000)	KB3080149
Microsoft Office Shared MUI (French) 2010 (14.0.4763.1000)	KB3086255
Microsoft Office Shared MUI (German) 2010 (14.0.4763.1000)	KB3092601
Microsoft Office Shared MUI (Italian) 2010 (14.0.4763.1000)	KB3093513
Microsoft Office Shared MUI (Japanese) 2010 (14.0.4763.1000)	KB3097989
Microsoft Office Shared MUI (Korean) 2010 (14.0.4763.1000)	KB3101722
Microsoft Office Shared MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3102429
Microsoft Office Shared MUI (Russian) 2010 (14.0.4763.1000)	KB3102810
Microsoft Office Shared MUI (Spanish) 2010 (14.0.4763.1000)	KB3107998
Microsoft Office Shared MUI (Turkish) 2010 (14.0.4763.1013)	KB3108371
Microsoft Office Shared Setup Metadata MUI (English) 2010 (14.0.6029.1000)	KB3108664
Microsoft Office Single Image 2010 (14.0.6029.1000)	KB3109103
Microsoft Office Word MUI (English) 2010 (14.0.6029.1000)	KB3109560
Microsoft Office Word MUI (French) 2010 (14.0.4763.1000)	KB3110329
Microsoft Office Word MUI (German) 2010 (14.0.4763.1000)	KB3115858
Microsoft Office Word MUI (Italian) 2010 (14.0.4763.1000)	KB3118401
Microsoft Office Word MUI (Japanese) 2010 (14.0.4763.1000)	KB3122648
Microsoft Office Word MUI (Korean) 2010 (14.0.4763.1000)	KB3123479
Microsoft Office Word MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3126587
Microsoft Office Word MUI (Russian) 2010 (14.0.4763.1000)	KB3127220
Microsoft Office Word MUI (Spanish) 2010 (14.0.4763.1000)	KB3133977
Microsoft Office Word MUI (Turkish) 2010 (14.0.4763.1013)	KB3137061
Microsoft Office X MUI (French) 2010 (14.0.4763.1000)	KB3138378
Microsoft Office X MUI (German) 2010 (14.0.4763.1000)	KB3138612
Microsoft Office X MUI (Italian) 2010 (14.0.4763.1000)	KB3138910
Microsoft Office X MUI (Japanese) 2010 (14.0.4763.1000)	KB3139398
Microsoft Office X MUI (Korean) 2010 (14.0.4763.1000)	KB3139914
Microsoft Office X MUI (Portuguese (Brazil)) 2010 (14.0.4763.1000)	KB3140245
Microsoft Office X MUI (Russian) 2010 (14.0.4763.1000)	KB3147071
Microsoft Office X MUI (Spanish) 2010 (14.0.4763.1000)	KB3150220
Microsoft Office X MUI (Turkish) 2010 (14.0.4763.1013)	KB3150513
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 (9.0.30729.6161)	KB3155178
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 (10.0.40219)	KB3156016
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 (12.0.30501.0)	KB3159398
Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 (12.0.21005)	KB3161102

Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 (12.0.21005)
Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.21.27702 (14.21.27702.2)
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.21.27702 (14.21.27702)
Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.21.27702 (14.21.27702)
Mozilla Firefox 83.0 (x86 en-US) (83.0)
Mozilla Maintenance Service (83.0.0.7621)
Notepad++ (32-bit x86) (7.9.1)
Opera 12.15 (12.15.1748)
QGA (2.14.33)
Skype version 8.29 (8.29)
VLC media player (3.0.11)
WinRAR 5.91 (32-bit) (5.91.0)

KB3161949
KB3170735
KB3172605
KB3179573
KB3184143
KB3185319
KB4019990
KB4040980
KB4474419
KB4490628
KB4524752
KB4532945
KB4536952
KB4567409
KB958488
KB976902
KB982018
LocalPack AU Package
LocalPack CA Package
LocalPack GB Package
LocalPack US Package
LocalPack ZA Package
Package 21 for KB2984976
Package 38 for KB2984976
Package 45 for KB2984976
Package 59 for KB2984976
Package 7 for KB2984976
Package 76 for KB2984976
PlatformUpdate Win7 SRV08R2 Package TopLevel
ProfessionalEdition
RDP BlueIP Package TopLevel
RDP WinIP Package TopLevel
RollupFix
UltimateEdition
WUClient SelfUpdate ActiveX
WUClient SelfUpdate Aux TopLevel
WUClient SelfUpdate Core TopLevel
WinMan WinIP Package TopLevel

Behavior activities

MALICIOUS

No malicious indicators.

SUSPICIOUS

Reads the computer name
DHL_11429040 영수증 문서, pdf.exe (PID: 2660)

Checks supported languages
DHL_11429040 영수증 문서, pdf.exe (PID: 2660)

INFO

No info indicators.

Static information

TRiD

.exe | Win32 Executable Borland Delphi 7 (68.8)
.exe | Win32 Executable Borland Delphi 6 (27.2)
.exe | Win32 Executable Delphi generic (1.4)
.scr | Windows screen saver (1.3)
.exe | Win32 Executable (generic) (0.4)

EXIF

EXE

Author:	WIxLife
HomePage:	
CompanyName:	
LegalCopyright:	Copyright ©2013 All Rights Reserved.
FileDescription:	Tec leader
Comments:	Tec leader
CharacterSet:	Unicode
LanguageCode:	English (British)
FileSubtype:	0
ObjectFileType:	Unknown
FileOS:	Win32
FileFlags:	(none)
FileFlagsMask:	0x003f
ProductVersionNumber:	0.0.0.0
FileVersionNumber:	0.0.0.0
Subsystem:	Windows GUI

SubsystemVersion:	4
ImageVersion:	0
OSVersion:	4
EntryPoint:	0x5e100
UninitializedDataSize:	0
InitializedDataSize:	304128
CodeSize:	381440
LinkerVersion:	2.25
PEType:	PE32
TimeStamp:	1992:06:20 00:22:17+02:00
MachineType:	Intel 386 or later, and compatibles

Summary

Architecture:	IMAGE_FILE_MACHINE_I386
Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI
Compilation Date:	19-Jun-1992 22:22:17
Detected languages:	English - United Kingdom
	English - United States
Comments:	Tec leader
FileDescription:	Tec leader
LegalCopyright:	Copyright ©2013 All Rights Reserved.
CompanyName:	
HomePage:	
Author:	WlxLife

DOS Header

Magic number:	MZ
Bytes on last page of file:	0x0050
Pages in file:	0x0002
Relocations:	0x0000
Size of header:	0x0004
Min extra paragraphs:	0x000F
Max extra paragraphs:	0xFFFF
Initial SS value:	0x0000
Initial SP value:	0x00B8
Checksum:	0x0000
Initial IP value:	0x0000
Initial CS value:	0x0000
Overlay number:	0x001A
OEM identifier:	0x0000
OEM information:	0x0000
Address of NE header:	0x00000100

PE Headers

Signature:	PE
Machine:	IMAGE_FILE_MACHINE_I386
Number of sections:	8
Time date stamp:	19-Jun-1992 22:22:17
Pointer to Symbol Table:	0x00000000
Number of symbols:	0
Size of Optional Header:	0x00E0
Characteristics:	IMAGE_FILE_32BIT_MACHINE
	IMAGE_FILE_BYTES_REVERSED_HI
	IMAGE_FILE_BYTES_REVERSED_LO
	IMAGE_FILE_EXECUTABLE_IMAGE
	IMAGE_FILE_LINE_NUMS_STRIPPED
	IMAGE_FILE_LOCAL_SYMS_STRIPPED

Sections

Name	Virtual Address	Virtual Size	Raw Size	Charateristics	Entropy
CODE	0x00001000	0x0005D13C	0x0005D200	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ	6.55532
DATA	0x0005F000	0x00001354	0x00001400	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	4.30445
BSS	0x00061000	0x00000DB9	0x00000000	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	0
.idata	0x00062000	0x00002264	0x00002400	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	4.88849
.tls	0x00065000	0x00000010	0x00000000	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE	0
.rdata	0x00066000	0x00000018	0x00000200	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_SHARED	0.20692
.reloc	0x00067000	0x00006938	0x00006A00	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_SHARED	6.66488
.rsrc	0x0006E000	0x00040000	0x00040000	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_SHARED	7.0208

Resources

Title	Entropy	Size	Codepage	Language	Type
1	3.24482	544	UNKNOWN	English - United Kingdom	RT_VERSION
2	2.80231	308	UNKNOWN	UNKNOWN	RT_CURSOR
3	3.00046	308	UNKNOWN	UNKNOWN	RT_CURSOR
4	2.56318	308	UNKNOWN	UNKNOWN	RT_CURSOR

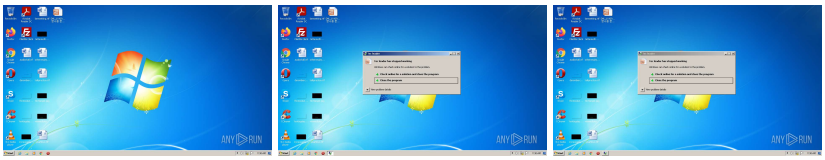
5	2.6949	308	UNKNOWN	UNKNOWN	RT_CURSOR
6	2.62527	308	UNKNOWN	UNKNOWN	RT_CURSOR
7	2.91604	308	UNKNOWN	UNKNOWN	RT_CURSOR
51	2.9114	1024	UNKNOWN	UNKNOWN	RT_ICON
53	5.06437	4096	UNKNOWN	UNKNOWN	RT_ICON
55	4.66504	2048	UNKNOWN	UNKNOWN	RT_ICON
57	4.53279	17408	UNKNOWN	UNKNOWN	RT_ICON
59	4.5687	4608	UNKNOWN	UNKNOWN	RT_ICON
61	4.08707	1536	UNKNOWN	UNKNOWN	RT_ICON
4081	3.31892	636	UNKNOWN	UNKNOWN	RT_STRING
4082	3.24878	504	UNKNOWN	UNKNOWN	RT_STRING
4083	3.16232	284	UNKNOWN	UNKNOWN	RT_STRING
4084	3.22813	768	UNKNOWN	UNKNOWN	RT_STRING
4085	2.99542	192	UNKNOWN	UNKNOWN	RT_STRING
4086	3.12805	252	UNKNOWN	UNKNOWN	RT_STRING
4087	3.25129	584	UNKNOWN	UNKNOWN	RT_STRING
4088	3.20722	1016	UNKNOWN	UNKNOWN	RT_STRING
4089	3.18654	864	UNKNOWN	UNKNOWN	RT_STRING
4090	3.23478	996	UNKNOWN	UNKNOWN	RT_STRING
4091	3.23259	564	UNKNOWN	UNKNOWN	RT_STRING
4092	3.00616	236	UNKNOWN	UNKNOWN	RT_STRING
4093	3.22288	436	UNKNOWN	UNKNOWN	RT_STRING
4094	3.19757	996	UNKNOWN	UNKNOWN	RT_STRING
4095	3.26686	856	UNKNOWN	UNKNOWN	RT_STRING
4096	3.18591	692	UNKNOWN	UNKNOWN	RT_STRING
32761	1.83876	20	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR
32762	1.91924	20	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR
32763	2.01924	20	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR
32764	2.01924	20	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR
32765	2.01924	20	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR
32766	2.01924	20	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR
32767	2.01924	20	UNKNOWN	UNKNOWN	RT_GROUP_CURSOR
BBABORT	2.92079	464	UNKNOWN	UNKNOWN	RT_BITMAP
BBALL	3.16995	484	UNKNOWN	UNKNOWN	RT_BITMAP
BBCANCEL	2.92079	464	UNKNOWN	UNKNOWN	RT_BITMAP
BBCLOSE	3.68492	464	UNKNOWN	UNKNOWN	RT_BITMAP
BBHELP	2.88085	464	UNKNOWN	UNKNOWN	RT_BITMAP
BBIGNORE	3.29718	464	UNKNOWN	UNKNOWN	RT_BITMAP
BBNO	3.58804	464	UNKNOWN	UNKNOWN	RT_BITMAP
BBOK	2.67459	464	UNKNOWN	UNKNOWN	RT_BITMAP
BBRETRY	3.53344	464	UNKNOWN	UNKNOWN	RT_BITMAP
BBYES	2.67459	464	UNKNOWN	UNKNOWN	RT_BITMAP
PREVIEWGLYPH	2.85172	232	UNKNOWN	English - United States	RT_BITMAP
DLGTEMPLATE	2.5627	82	UNKNOWN	UNKNOWN	RT_DIALOG
ASS	7.13555	209583	UNKNOWN	English - United States	RT_RCDATA
DVCLAL	4	16	UNKNOWN	UNKNOWN	RT_RCDATA
PACKAGEINFO	5.26778	896	UNKNOWN	UNKNOWN	RT_RCDATA
MAINICON	2.58795	90	UNKNOWN	UNKNOWN	RT_GROUP_ICON

Imports

advapi32.dll

comctl32.dll
gdi32.dll
kernel32.dll
ole32.dll
oleaut32.dll
user32.dll
version.dll

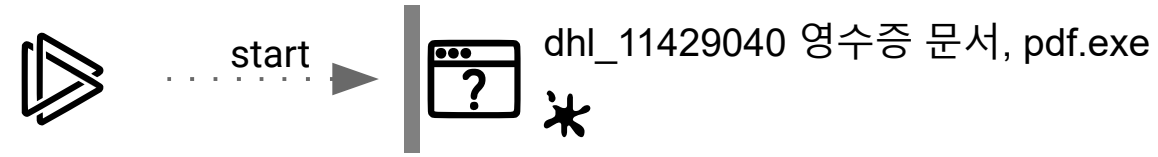
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
40	1	0	0

Behavior graph



Specs description

Program did not start	Low-level access to the HDD	Process was added to the startup	Debug information is available
Probably Tor was used	Behavior similar to spam	Task has injected processes	Executable file was dropped
Known threat	RAM overrun	Network attacks were detected	Integrity level elevation
Connects to the network	CPU overrun	Process starts the services	System was rebooted
Task contains several apps running	Application downloaded the executable file	Actions similar to stealing personal data	Task has apps ended with an error
File is detected by antivirus software	Inspected object has suspicious PE structure	Behavior similar to exploiting the vulnerability	Task contains an error or was rebooted
The process has the malware config			

Process information

PID	CMD	Path	Indicators	Parent process
2660	"C:\Users\admin\Desktop\DHL_11429040 영수증 문서, pdf.exe"	C:\Users\admin\Desktop\DHL_11429040 영수증 문서, pdf.exe		Explorer.EXE

Information

User: admin **Integrity Level:** MEDIUM
Description: Tec leader

Registry activity

Total events	Read events	Write events	Delete events
174	174	0	0

Modification events

No data

Files activity

Executable files	Suspicious files	Text files	Unknown types
0	0	0	0

Dropped files

No data

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
0	1	2	0

HTTP requests

No HTTP requests

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
–	–	192.168.100.2:53	–	–	–	whitelisted

DNS requests

Domain	IP	Reputation
www.microsoft.com	–	whitelisted
dns.msftncsi.com	131.107.255.255	shared

Threats

No threats detected

Debug output strings

No debug info