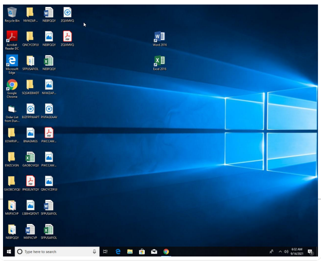
ID: 482788
Sample Name: Order List from Dunen Enterprise Corporation.exe
Cookbook: default.jbs
Time: 06:27:44
Date: 14/09/2021
Version: 33.0.0 White Diamond

Table of Contents

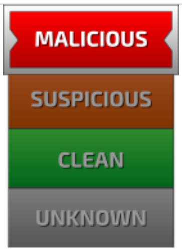
Windows Analysis Report Order List from Dunen Enterp…

Overview

General Information

Sample Name:	Order List from Dunen Enterprise Corporation.exe
Analysis ID:	482788
MD5:	744d8320069103..
SHA1:	b58f485d5153dc4.
SHA256:	e015835dd69bbd..
Tags:	exe guloader
Infos:	
Most interesting Screenshot: 	

Detection



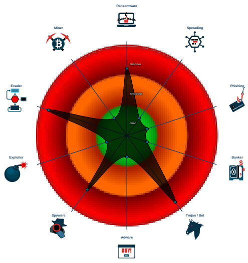
GuLoader FormBook

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

Signatures

- Found malware configuration
- Potential malicious icon found
- Yara detected Generic Dropper
- Yara detected FormBook
- Malicious sample detected (through …
- GuLoader behavior detected
- Yara detected GuLoader
- Hides threads from debuggers
- Maps a DLL or memory area into an…
- Initial sample is a PE file and has a …
- Tries to detect Any.run
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- Order List from Dunen Enterprise Corporation.exe (PID: 2968 cmdline: 'C:\Users\user\Desktop\Order List from Dunen Enterprise Corporation.exe' MD5: 744D832006910318B2826E4CC8DB4B11)
  - Order List from Dunen Enterprise Corporation.exe (PID: 5796 cmdline: 'C:\Users\user\Desktop\Order List from Dunen Enterprise Corporation.exe' MD5: 744D832006910318B2826E4CC8DB4B11)
    - explorer.exe (PID: 3292 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msdt.exe (PID: 4780 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.mx-online-service.xyz/hhse/"
  ],
  "decoy": [
    "gujranwala.city",
    "peinture-san-deco.com",
    "disvapes.com",
    "tekst-sanderlei.com",
    "veryfastsnail.com",
    "yaqiong.net",
    "onlinebingocenter.com",
    "kenttreesurgery.com",
    "berislavic.com",
    "ecomemailspack.com",
    "drgustavoteyssier.com",
    "mayfieldslodge.com",
    "qiubaolink.com",
    "kevinkensik.com",
    "boatmanagementexpert.com",
    "dbylkov.com",
    "griffin-designs.com",
    "glowlikethis.com",
    "fuckjules.com",
    "lxqc6688.com",
    "cduyechang.com",
    "jintelcare.com",
    "abdiscountplumbing.com",
    "merrilllynchph.com",
    "yuanxinlv.com",
    "chinapuma.com",
    "covertroyalty.com",
    "grouphall.net",
    "unikpixls.com",
    "rbainlaw.com",
    "bold2x.com",
    "eventosav.com",
    "copywritermeg.com",
    "geeeknozoid.com",
    "physio-schmid.com",
    "bankofsavings.com",
    "xzttzs.com",
    "water-note.com",
    "gutter-rutter.com",
    "wallis-applications.com",
    "aurora-graphics.com",
    "justindoorsoccer.com",
    "drivly.net",
    "allonot.com",
    "splashseltzer.com",
    "sanctuarymarbella.com",
    "fossickandfind.com",
    "sari-2.com",
    "luxedesignsinc.com",
    "cowlickgin.com",
    "anothergeorgia.life",
    "mainstreetmarketlillington.com",
    "vibe-communications.com",
    "nextgenrs.net",
    "kosurvival.com",
    "uvinq.com",
    "crenate-throe.info",
    "weazing.net",
    "mydreamit.world",
    "shortandsweetorganizing.com",
    "24bitpay-trade.com",
    "qianniaofan.com",
    "thepccafe.com",
    "solucionesautomotrices.info"
  ]
}
```

Threatname: GuLoader

```
{
  "Payload URL": "https://onedrive.live.com/download?cid=3B15BFABEF8C3B9%()"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001A.00000000.748909950.0000000006D25000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000001A.00000000.748909950.0000000006D25000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x5695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x5181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x5797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x590f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x43fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xb82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000001A.00000000.748909950.0000000006D25000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x76b9:$sqlite3step: 68 34 1C 7B E1 • 0x77cc:$sqlite3step: 68 34 1C 7B E1 • 0x76e8:$sqlite3text: 68 38 2A 90 C5 • 0x780d:$sqlite3text: 68 38 2A 90 C5 • 0x76fb:$sqlite3blob: 68 53 D8 7F 8C • 0x7823:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000002.473954904.0000000002880000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000016.00000002.768114646.000000001E3D0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 6 entries				

Sigma Overview

System Summary:

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected FormBook

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Potential malicious icon found

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information:

Yara detected Generic Dropper

Yara detected FormBook

GuLoader behavior detected

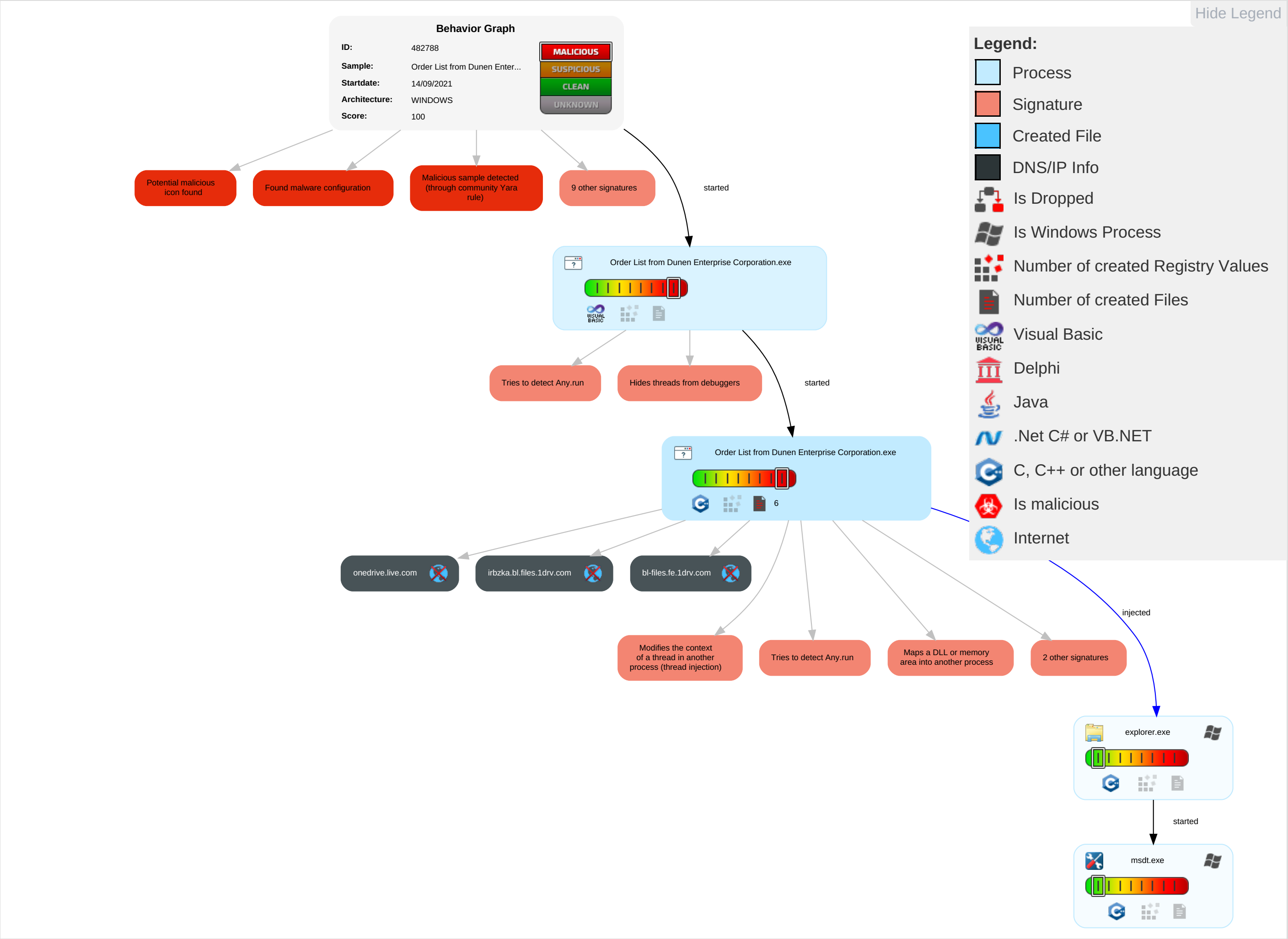
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 3 1 2	Virtualization/Sandbox Evasion 2 1	OS Credential Dumping	Security Software Discovery 4 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 3 1 2	LSASS Memory	Virtualization/Sandbox Evasion 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 1	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	System Information Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati

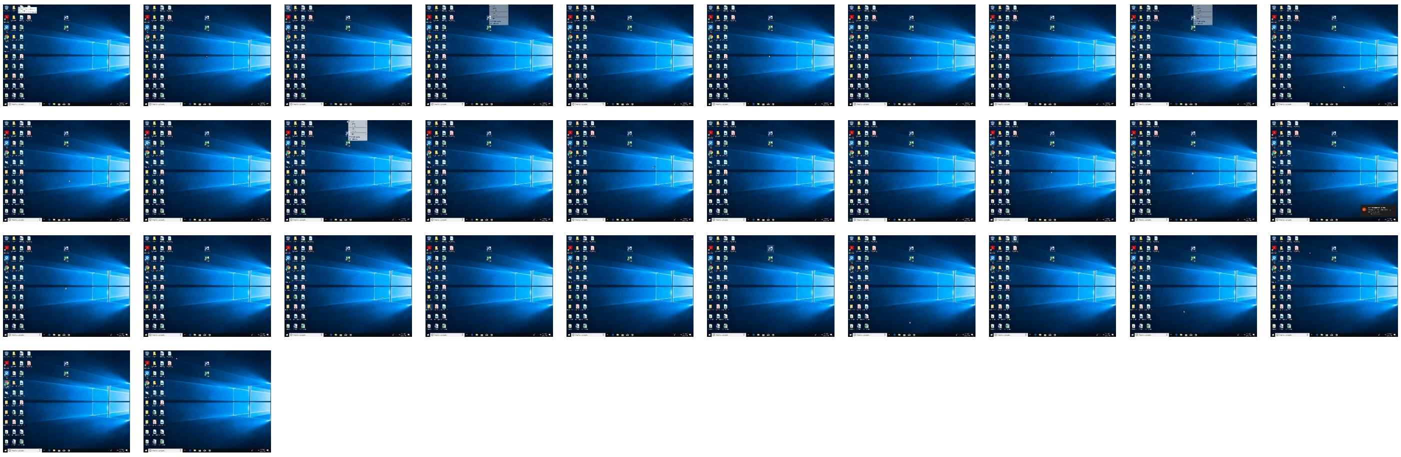
Behavior Graph

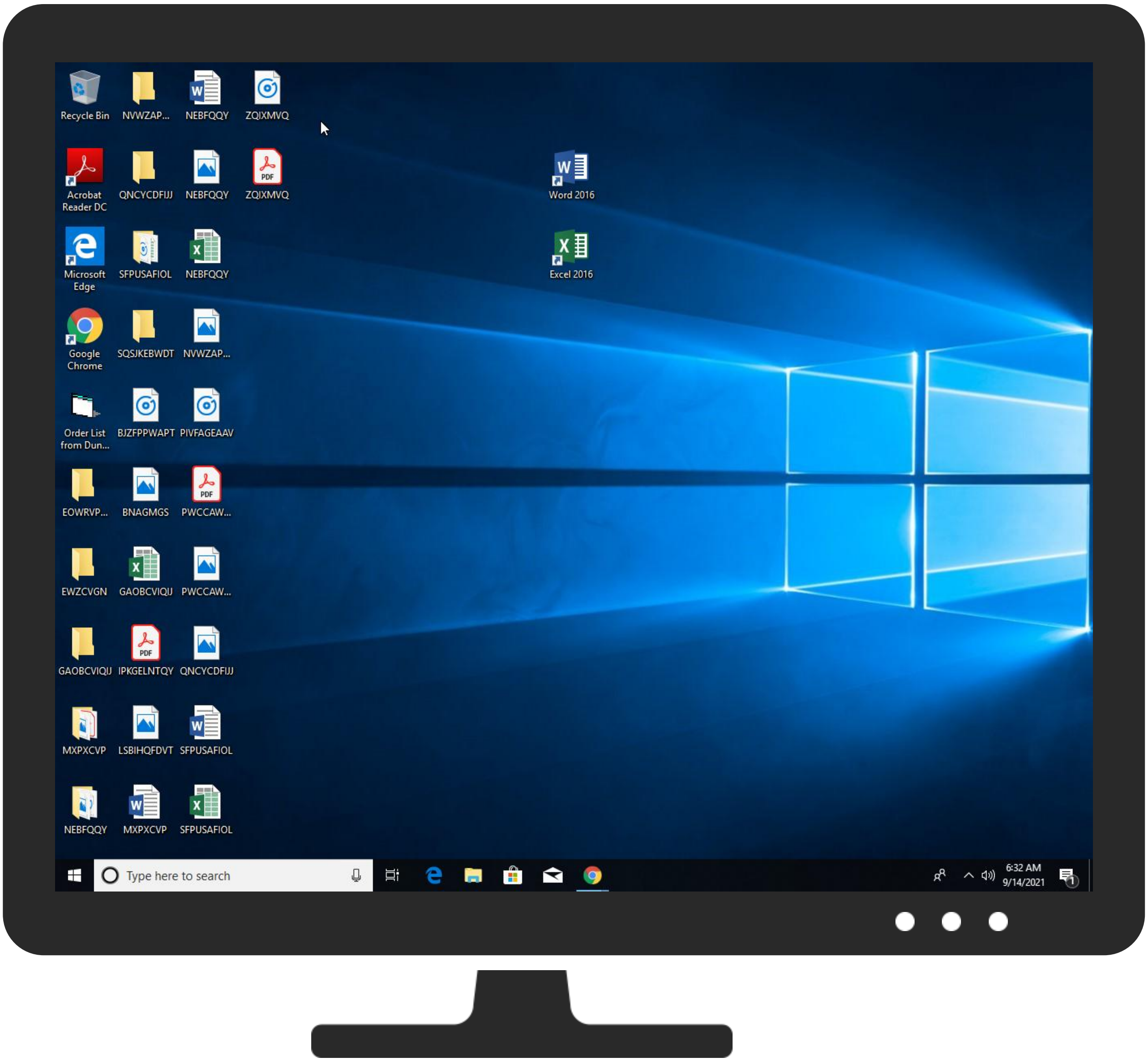


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Order List from Dunen Enterprise Corporation.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.mx-online-service.xyz/hhse/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
onedrive.live.com	unknown	unknown	false		high
irbzka.bl.files.1drv.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.mx-online-service.xyz/hhse/	true	• Avira URL Cloud: safe	low
http://https://onedrive.live.com/download?cid=3B15BFABEF8C3B9%()	false		high

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	482788
Start date:	14.09.2021
Start time:	06:27:44
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Order List from Dunen Enterprise Corporation.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.rans.troj.spyw.evad.winEXE@4/0@2/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 52.5% (good quality ratio 42.6%) • Quality average: 65.3% • Quality standard deviation: 37%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

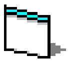
No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.852738656529827
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Order List from Dunen Enterprise Corporation.exe
File size:	131072
MD5:	744d832006910318b2826e4cc8db4b11
SHA1:	b58f485d5153dc4cb1a608091e1174d6fc966a4a
SHA256:	e015835dd69bbd384cb9b347984b648562281ba9e532ca 110b6962bce9262251
SHA512:	2ef7a81389e03fe8cdaa42e39e9df842d811b87b97d50e9 15e01d8fa35e3eaa49f7aaa03aa5a534e3413a636d3bf01 1ff9774a4b5b2553fbecef24aa8425deb4
SSDEEP:	3072:CwbDzFr9RfmrBv2ubFB2NNq1KvyFwZddImz:Cw bDzFrnfmrUWD2/6wpIm
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.......O........... ....D.......=.......Rich............PE..L...f7.Y..................... P......t.............@................

File Icon



Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401574
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x59B03766 [Wed Sep 6 17:59:02 2017 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	44cde914d1969d7de2a52adae7c22460

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1ad44	0x1b000	False	0.581353081597	data	7.10915094479	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1c000	0x1910	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1e000	0x296b	0x3000	False	0.702962239583	data	6.62180270851	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 14, 2021 06:32:19.164278030 CEST	192.168.2.7	8.8.8.8	0xf90e	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Sep 14, 2021 06:32:20.294226885 CEST	192.168.2.7	8.8.8.8	0x1ed8	Standard query (0)	irbzka.bl.files.1drv.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 14, 2021 06:32:19.222822905 CEST	8.8.8.8	192.168.2.7	0xf90e	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Sep 14, 2021 06:32:20.403966904 CEST	8.8.8.8	192.168.2.7	0x1ed8	No error (0)	irbzka.bl.files.1drv.com	bl-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Sep 14, 2021 06:32:20.403966904 CEST	8.8.8.8	192.168.2.7	0x1ed8	No error (0)	bl-files.fe.1drv.com	odc-bl-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Order List from Dunen Enterprise Corporation.exe PID: 2968 Parent PID: 5428

General

Start time:	06:28:36
Start date:	14/09/2021
Path:	C:\Users\user\Desktop\Order List from Dunen Enterprise Corporation.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Order List from Dunen Enterprise Corporation.exe'
Imagebase:	0x400000
File size:	131072 bytes
MD5 hash:	744D832006910318B2826E4CC8DB4B11
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.473954904.0000000002880000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: Order List from Dunen Enterprise Corporation.exe PID: 5796 Parent PID: 2968

General

Start time:	06:30:28
Start date:	14/09/2021
Path:	C:\Users\user\Desktop\Order List from Dunen Enterprise Corporation.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Order List from Dunen Enterprise Corporation.exe'
Imagebase:	0x400000
File size:	131072 bytes
MD5 hash:	744D832006910318B2826E4CC8DB4B11
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000016.00000002.768114646.000000001E3D0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000016.00000002.768114646.000000001E3D0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000016.00000002.768114646.000000001E3D0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: explorer.exe PID: 3292 Parent PID: 5796

General

Start time:	06:32:22
Start date:	14/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff662bf0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001A.00000000.748909950.0000000006D25000.00000040.00020000.sdmp, Author: Joe Security - Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001A.00000000.748909950.0000000006D25000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com - Rule: Formbook, Description: detect Formbook in memory, Source: 0000001A.00000000.748909950.0000000006D25000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group - Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000001A.00000000.735368674.0000000006D25000.00000040.00020000.sdmp, Author: Joe Security - Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000001A.00000000.735368674.0000000006D25000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com - Rule: Formbook, Description: detect Formbook in memory, Source: 0000001A.00000000.735368674.0000000006D25000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: msdt.exe PID: 4780 Parent PID: 3292

General

Start time:	06:32:42
Start date:	14/09/2021
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	
File size:	1508352 bytes
MD5 hash:	7F0C51DBA69B9DE5DDF6AA04CE3A69F4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

Code Analysis