JoeSandbox Cloud BASIC

ID: 410913
Sample Name: A5uTdwOwJ1.dll
Cookbook: default.jbs
Time: 12:56:38
Date: 11/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report A5uTdwOwJ1.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: Ursnif 4
Yara Overview 4
Memory Dumps 5
Sigma Overview 5
Signature Overview 5
AV Detection: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
E-Banking Fraud: 5
System Summary: 5
Hooking and other Techniques for Hiding and Protection: 5
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
Contacted IPs 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 12
General 12
File Icon 13
Static PE Info 13
General 13
Entrypoint Preview 13
Data Directories 15
Sections 15
Resources 15
Imports 16
Exports 16
Version Infos 16
Possible Origin 16

Copyright Joe Security LLC 2021

Network Behavior 16
UDP Packets 16
DNS Queries 17
DNS Answers 17
Code Manipulations 18
Statistics 19
Behavior 19
System Behavior 19
Analysis Process: loaddll32.exe PID: 7048 Parent PID: 5776 19
General 19
File Activities 19
Analysis Process: cmd.exe PID: 7056 Parent PID: 7048 19
General 19
File Activities 20
Analysis Process: rundll32.exe PID: 7064 Parent PID: 7048 20
General 20
File Activities 20
Analysis Process: rundll32.exe PID: 7076 Parent PID: 7056 20
General 20
File Activities 20
Analysis Process: rundll32.exe PID: 7132 Parent PID: 7048 20
General 21
File Activities 21
Analysis Process: rundll32.exe PID: 7148 Parent PID: 7048 21
General 21
File Activities 21
Analysis Process: iexplore.exe PID: 4640 Parent PID: 800 21
General 21
File Activities 21
Registry Activities 22
Analysis Process: iexplore.exe PID: 1668 Parent PID: 4640 22
General 22
File Activities 22
File Read 22
Disassembly 22
Code Analysis 22

Copyright Joe Security LLC 2021

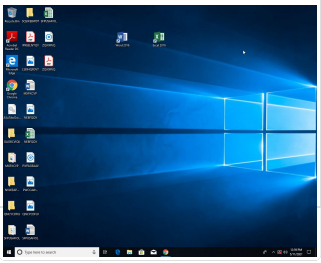
Analysis Report A5uTdwOwJ1.dll

Overview

General Information

Sample Name:	A5uTdwOwJ1.dll
Analysis ID:	410913
MD5:	1752fe2b8419be8.
SHA1:	eb7346a6d5a53d..
SHA256:	e81869620b9a18..
Tags:	dll Gozi ISFB Ursnif
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

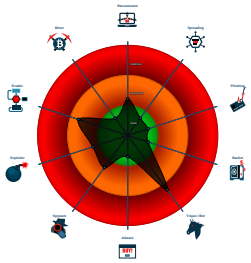
Ursnif

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Ursnif
- Writes registry values via WMI
- Allocates a big amount of memory (p…
- Contains functionality to call native f…
- Contains functionality to check if a d…
- Contains functionality to check if a d…
- Contains functionality to dynamically…
- Contains functionality to query CPU …
- Contains functionality to read the PEB
- Creates a DirectInput object (often fo…
- Creates a process in suspended mo…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 7048 cmdline: loaddll32.exe 'C:\Users\user\Desktop\A5uTdwOwJ1.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 7056 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\A5uTdwOwJ1.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 7076 cmdline: rundll32.exe 'C:\Users\user\Desktop\A5uTdwOwJ1.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7064 cmdline: rundll32.exe C:\Users\user\Desktop\A5uTdwOwJ1.dll,Hundredpopulate@@8 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7132 cmdline: rundll32.exe C:\Users\user\Desktop\A5uTdwOwJ1.dll,Mark@@12 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 7148 cmdline: rundll32.exe C:\Users\user\Desktop\A5uTdwOwJ1.dll,Seefit@@8 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 4640 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 1668 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4640 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key": "KujE77ctKyR8x3/dODwZbEsxGmck+FW9384s5u0Kacw8y1gCN+8m2bfjJPovkn+Uzufcdfss+a43eI6oHR1KgWQmvEAO6LK8tJv+Wl7iCBPJP7eef8xKeXht/Mhk1PSj7mHnJ9lcqKMtTteEdSecVvMRtb/WSKVTFfHDva9My7AJ/NbXqHdzCG7znACswLxD",
  "c2_domain": [
    "outlook.com/login",
    "gmail.com",
    "worunekulo.club",
    "horunekulo.website"
  ],
  "botnet": "8877",
  "server": "12",
  "serpent_key": "30218409ILPAJDUR",
  "sleep_time": "10",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0",
  "DGA_count": "10"
}
```


Yara Overview

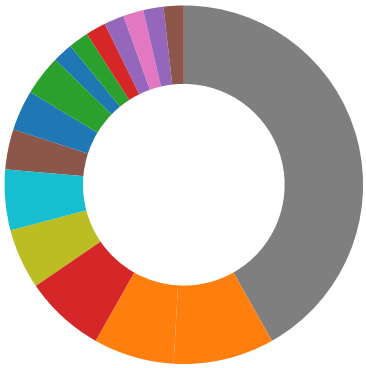
Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.933933475.00000000050E8000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Process Memory Space: rundll32.exe PID: 7076	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

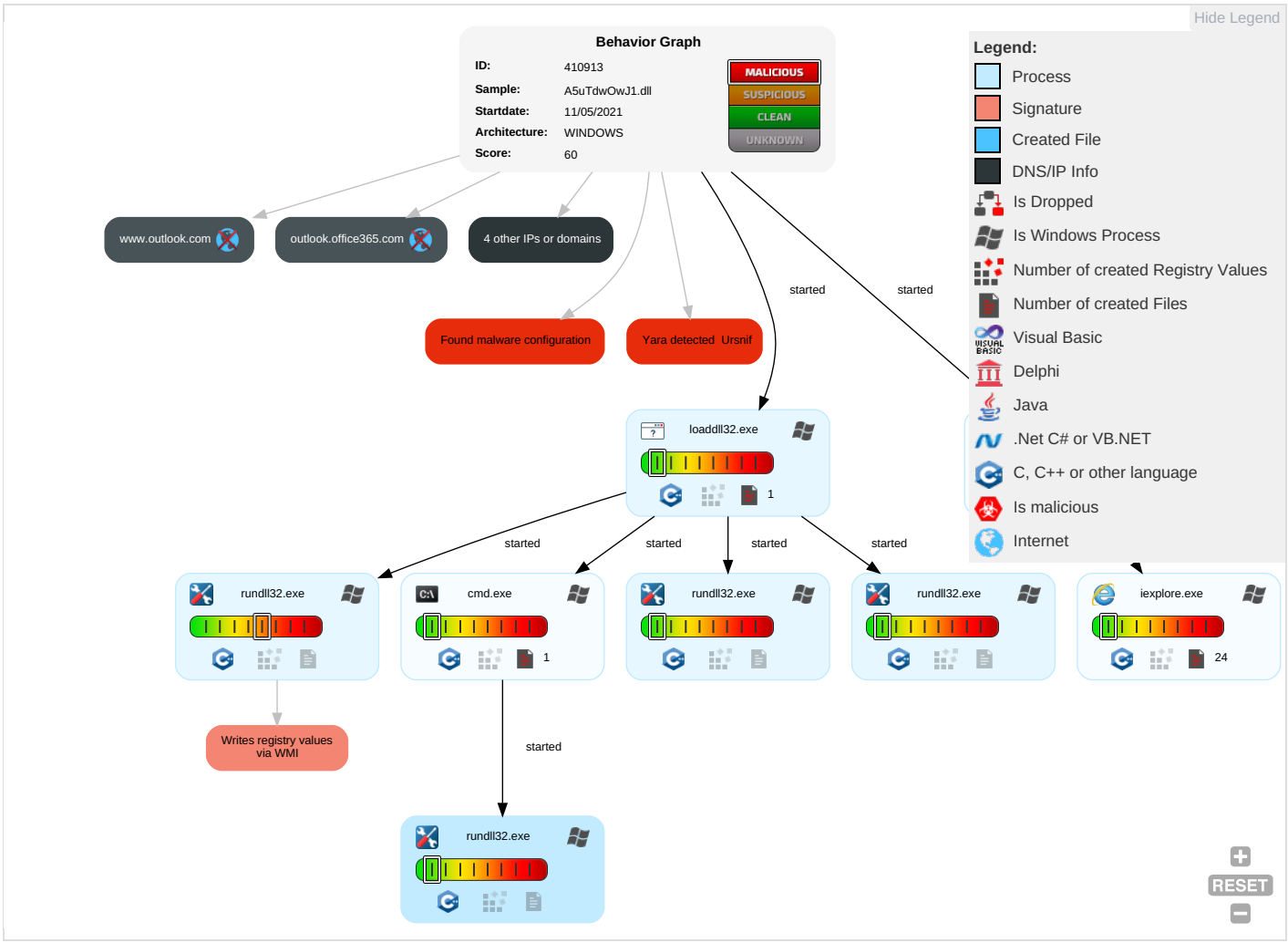
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Ren Serv Effe
Valid Accounts	Windows Management Instrumentation 1	Application Shimming 1	Process Injection 1 2	Masquerading 1	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Rem Trac With Auth
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Application Shimming 1	Process Injection 1 2	LSASS Memory	Security Software Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Rem Wip With Auth
Domain Accounts	At (Linux)	Logon Script (Windows)	Extra Window Memory Injection 1	Obfuscated 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	Exploit SS7 to Track Device Location	Obta Dev Clou Bac
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1	NTDS	Account Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Extra Window Memory Injection 1	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	

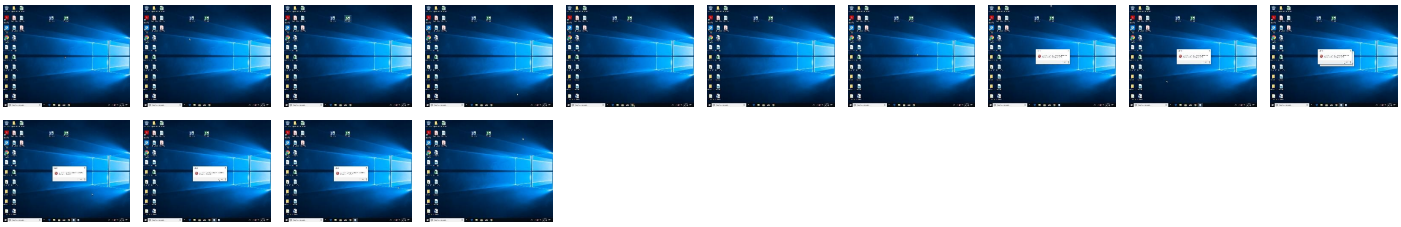
Behavior Graph



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

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.2b60000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
4.2.rundll32.exe.2d40000.1.unpack	100%	Avira	HEUR/AGEN.1108168		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
outlook.com	40.97.116.82	true	false		high
HHN-efz.ms-acdc.office.com	40.101.138.210	true	false		high
www.outlook.com	unknown	unknown	false		high
outlook.office365.com	unknown	unknown	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	410913
Start date:	11.05.2021
Start time:	12:56:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	A5uTdwOwJ1.dll
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:	14
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:	mal60.troj.winDLL@14/4@3/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 8.9% (good quality ratio 8.5%) • Quality average: 79.5% • Quality standard deviation: 28.6%
HCA Information:	• Successful, ratio: 69% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll

Copyright Joe Security LLC 2021

Warnings:	Show All • Excluded IPs from analysis (whitelisted): 13.107.3.254, 104.43.193.48, 13.107.246.254, 40.88.32.150, 13.64.90.137, 131.253.33.200, 13.107.22.200, 104.43.139.144, 20.190.160.133, 20.190.160.70, 20.190.160.9, 20.190.160.5, 20.190.160.72, 20.190.160.7, 20.190.160.74, 20.190.160.68, 20.50.102.62, 92.122.213.247, 92.122.213.194, 88.221.62.148 • Excluded domains from analysis (whitelisted): s-ring.msedge.net, www.tm.lg.prod.aadmsa.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, login.live.com, www-bing-com.dual-a-0001.a-msedge.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, www.bing.com, skypedataprdcolwus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, s-ring.s-9999.s-msedge.net, t-ring.msedge.net, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, t-9999.t-msedge.net, a-0001.a-afdentry.net.trafficmanager.net, s-9999.s-msedge.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, t-ring.t-9999.t-msedge.net • Report size getting too big, too many NtOpenKeyEx calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:59:18	API Interceptor	1x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HHN-efz.ms-acdc.office.com	FuiZSHt8Hx.dll	Get hash	malicious	Browse	• 52.98.151.242
	609a460e94791.tiff.dll	Get hash	malicious	Browse	• 52.97.201.34
	iJdlvBxhYu.dll	Get hash	malicious	Browse	• 52.97.150.2
	8OKQ6ogGRx.dll	Get hash	malicious	Browse	• 40.101.138.2
	609110f2d14a6.dll	Get hash	malicious	Browse	• 40.101.137.34
	New%20order%20contract.html	Get hash	malicious	Browse	• 52.98.175.2
outlook.com	file.msg.exe	Get hash	malicious	Browse	• 104.47.56.138
	Update-KB1484-x86.exe	Get hash	malicious	Browse	• 104.47.57.138
	n6osajjc938.exe	Get hash	malicious	Browse	• 104.47.54.36
	9b3d7f02.exe	Get hash	malicious	Browse	• 104.47.54.36
	5zc9vbGBo3.exe	Get hash	malicious	Browse	• 52.101.24.0
	InnAcjnAmG.exe	Get hash	malicious	Browse	• 104.47.53.36
	8X93Tzvd7V.exe	Get hash	malicious	Browse	• 52.101.24.0
	u8A8Qy5S7O.exe	Get hash	malicious	Browse	• 104.47.53.36
	SecuriteInfo.com.Mal.GandCrypt-A.24654.exe	Get hash	malicious	Browse	• 104.47.54.36

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.Mal.GandCrypt-A.5674.exe	Get hash	malicious	Browse	• 104.47.54.36
	SecuriteInfo.com.W32.AIDetect.malware2.29567.exe	Get hash	malicious	Browse	• 104.47.53.36
	lsass(1).exe	Get hash	malicious	Browse	• 104.47.59.138
	rtofwqxq.exe	Get hash	malicious	Browse	• 104.47.53.36
	VufxYArno1.exe	Get hash	malicious	Browse	• 104.47.53.36

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{FA9A4670-B247-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	21592
Entropy (8bit):	1.7538928547404984
Encrypted:	false
SSDEEP:	48:IwVGcpr8GwpL/G/ap8hGIpcWGvnZpvUoGokPqp9RGo4wqzpmpGWk5YTR:rLZ0Zn2jWztUxifiwqzMYCV
MD5:	B9765F08D46BFC88BBFDCCFC0D775FF6
SHA1:	8160BFAE549AB412C71C7AB0DD67FE046F8BE085
SHA-256:	0AA48A18F107E6EA8C938E35497041F02B8389C6F763AC2B43EF55C7C38EBCB2
SHA-512:	7C86AE85DC93DC7D0BEFBA30C6B7A9794145E35633E5722C9726AA755E58973FEAEBF07ECDD03744F9E88FF0E121F93DED4780C00C3E8437EB884C99CFC553 5
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r. y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{FA9A4672-B247-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5736827119957864
Encrypted:	false
SSDEEP:	48:Iwa7GcprHGwpaUG4pQoGrapbS7GQpBSGHHpcvTGUpG:rahZRQk62BS1jp25A
MD5:	5EAB8D7BB7320BB13DEB73905A1A53FB
SHA1:	4B28FC7F388C96242071D35AD7E75D928508C311
SHA-256:	901D4FD58A650A36B0F17605AF165FDA50C6B9F26C44DBA3C940C0BCE0C0689F
SHA-512:	19D5128ABD62B212D4E445405BA6257632CA2DCD0A794DD0D9733FBD108EA76D8BB657E4134E71178577FD1C38DA825378628D3FAA01573C82E6C58193DA53D
Malicious:	false
Reputation:	low
Preview:	.....R.o.o.t. .E.n.t.r. y.....

C:\Users\user\AppData\Local\Temp\~DF1B654EC27DD768D2.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Temp\~DF1B654EC27DD768D2.TMP	
Size (bytes):	25657
Entropy (8bit):	0.3144468490138463
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwSz9lwSz9l2S6:kBqoxKAuvScS+1bN
MD5:	82A8AF58D95219C47E4A30F27A7C206E
SHA1:	C20BBE085E1EDA657B8E68E513C2A10E3235BE54
SHA-256:	F1BAB6976EAEDB52338DE2D26B481D9C33EDA97219D5238FF5A3F3482F2AC385
SHA-512:	A729B550BBDA1DE7C946CE4AF0715D88E082E0AC287C95AD146D9D189E6EE33D5B6686741009FC35B856BCC7A6727420DE11BFFA23B5C81044907FA1801C6E 5
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....

C:\Users\user\AppData\Local\Temp\~DF7A757557FCA01EC0.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12917
Entropy (8bit):	0.39582328508219533
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9logi9logS9lWgfE:kBqoIC85
MD5:	857EE0C1FAE8C14013D145E688ECCCE8
SHA1:	E692896F7D7BFF731D73C947851F3C1C1E26FA08
SHA-256:	4DA381D3C5014EE7A29C1BF58AA4C4B5BF5225A3AE40A3021A2A2E6976380BD5
SHA-512:	FA43E3BE7959D040AB1EED343E350271892A5A8DAC4972143F1AAD092E77B1C6AD1B071E9AAE45AEC92DC4CD742A988F102646385C98273121C683F8BBA7198 5
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... .....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.388583358089739
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.40% • Win16/32 Executable Delphi generic (2074/23) 0.21% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	A5uTdwOwJ1.dll
File size:	841216
MD5:	1752fe2b8419be8241ecd08859a5800f
SHA1:	eb7346a6d5a53ddaf8fd073f266c64d642b40a7d
SHA256:	e81869620b9a18c3702c7be2fcf2e170cbc5c3de1ddbc84ae1fe190b57e917a0
SHA512:	0718e566bdec828d59890818a65af53f467d1bab92abbd 2ecfe3eca55be7ad3692793e4310ea41f2ab2a9f5e9fe6d 29e1873cacc1614c6f2cceaf6b320c8f15
SSDEEP:	12288:mzCoXRvNZrA8Res/TPUOjUUGcqcoWEx9kMGUS6vOV5y4gnuD5wtqqB7ol:udNZr5RLL1AZ/clUnHvk5hgU
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...L..`.....!.....0.....@.....{..x..

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1033080
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x1000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6092C34C [Wed May 5 16:09:48 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	dc55991f7b8a912c780d10d352635290

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007FDB40955B47h
call 00007FDB40956817h
mov eax, dword ptr [ebp+10h]
push eax
mov ecx, dword ptr [ebp+0Ch]
push ecx
mov edx, dword ptr [ebp+08h]
push edx
call 00007FDB40955926h
add esp, 0Ch
pop ebp
retn 000Ch
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
push ecx
mov dword ptr [ebp-04h], ecx
mov esp, ebp
pop ebp
ret
int3
int3
int3

Instruction
int3
int3
push ebp
mov ebp, esp
push ecx
mov eax, dword ptr [ebp+08h]
mov ecx, dword ptr [eax]
mov dword ptr [ebp-04h], ecx
mov eax, dword ptr [ebp-04h]
mov esp, ebp
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push eax
call 00007FDB40955B19h
add esp, 04h
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push eax
call 00007FDB40955BB9h
add esp, 04h
test eax, eax
je 00007FDB40955B43h
int3
pop ebp
ret
int3
int3
int3
int3
int3

Instruction
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push eax
call 00007FDB40955B99h
add esp, 04h
test eax, eax
je 00007FDB40955B49h
mov ecx, 00000041h
int 29h
pop ebp
ret
int3
int3
int3
int3
push ebp
mov ebp, esp
push ecx
mov eax, dword ptr [ebp+08h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0xc7bb0	0x78	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc7c28	0x64	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe8000	0x3a0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe9000	0x51e0	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xc5ecc	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xc5f20	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x9b000	0x1a4	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x997af	0x99800	False	0.488931761502	data	6.50078545852	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x9b000	0x2d5aa	0x2d600	False	0.326892863292	data	4.74980452387	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xc9000	0x1efdc	0xe00	False	0.209821428571	data	3.01039741419	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xe8000	0x3a0	0x400	False	0.404296875	data	3.03375733203	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe9000	0x51e0	0x5200	False	0.770293445122	data	6.74990882481	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xe8060	0x340	data	English	United States

Imports

DLL	Import
KERNEL32.dll	CreateFileW, GetWindowsDirectoryW, ReadFile, GetConsoleMode, OpenMutexW, CloseHandle, GetFileSize, DeleteCriticalSection, ReadConsoleW, VirtualProtectEx, GetConsoleCP, FlushFileBuffers, SetFilePointerEx, GetFileSizeEx, SetStdHandle, GetStringTypeW, EnterCriticalSection, LeaveCriticalSection, SetLastError, InitializeCriticalSectionAndSpinCount, CreateEventW, SwitchToThread, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, GetSystemTimeAsFileTime, GetTickCount, GetModuleHandleW, GetProcAddress, IsProcessorFeaturePresent, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, GetCurrentProcess, TerminateProcess, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, InitializeSListHead, RaiseException, RtlUnwind, InterlockedPushEntrySList, InterlockedFlushSList, GetLastError, EncodePointer, FreeLibrary, LoadLibraryExW, GetModuleFileNameW, GetModuleHandleExW, ExitProcess, HeapAlloc, HeapValidate, GetSystemInfo, GetCurrentThread, GetStdHandle, GetFileType, WriteFile, OutputDebugStringW, WriteConsoleW, SetConsoleCtrlHandler, GetDateFormatW, GetTimeFormatW, CompareStringW, LCMapStringW, GetLocaleInfoW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, FindClose, FindFirstFileExW, FindNextFileW, IsValidCodePage, GetACP, GetOEMCP, GetCPInfo, GetCommandLineA, GetCommandLineW, MultiByteToWideChar, WideCharToMultiByte, GetEnvironmentStringsW, FreeEnvironmentStringsW, SetEnvironmentVariableW, GetProcessHeap, HeapFree, HeapReAlloc, HeapSize, HeapQueryInformation, DecodePointer
UxTheme.dll	CloseThemeData
AVIFIL32.dll	AVIFileGetStream, AVIFileOpenW, AVIFileExit, AVIFileInit, AVIFileEndRecord
TAPI32.dll	lineRedirectW, lineInitialize, lineHold, lineShutdown, lineTranslateAddressW

Exports

Name	Ordinal	Address
Hundredpopulate@@8	1	0x1030208
Mark@@12	2	0x10303fe
Seefit@@8	3	0x103046c

Version Infos

Description	Data
LegalCopyright	Dad plan Corporation. All rights reserved
InternalName	Team Lonesell
FileVersion	7.2.6.201
CompanyName	Dad plan Corporation
These	95
ProductName	Dad plan Fair fell
ProductVersion	7.2.6.201
FileDescription	Dad plan Fair fell
OriginalFilename	fall.dll
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 12:57:28.205221891 CEST	53097	53	192.168.2.4	8.8.8.8
May 11, 2021 12:57:28.254018068 CEST	53	53097	8.8.8.8	192.168.2.4
May 11, 2021 12:57:28.258095980 CEST	49257	53	192.168.2.4	8.8.8.8
May 11, 2021 12:57:28.309806108 CEST	53	49257	8.8.8.8	192.168.2.4
May 11, 2021 12:57:28.481270075 CEST	62389	53	192.168.2.4	8.8.8.8
May 11, 2021 12:57:28.541296959 CEST	53	62389	8.8.8.8	192.168.2.4
May 11, 2021 12:57:30.231909990 CEST	49910	53	192.168.2.4	8.8.8.8
May 11, 2021 12:57:30.283821106 CEST	53	49910	8.8.8.8	192.168.2.4

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2021 12:57:31.195168018 CEST	55854	53	192.168.2.4	8.8.8.8
May 11, 2021 12:57:31.249306917 CEST	53	55854	8.8.8.8	192.168.2.4
May 11, 2021 12:57:31.965966940 CEST	64549	53	192.168.2.4	8.8.8.8
May 11, 2021 12:57:32.017632961 CEST	53	64549	8.8.8.8	192.168.2.4
May 11, 2021 12:57:33.175950050 CEST	63153	53	192.168.2.4	8.8.8.8
May 11, 2021 12:57:33.234396935 CEST	53	63153	8.8.8.8	192.168.2.4
May 11, 2021 12:57:34.227926016 CEST	52991	53	192.168.2.4	8.8.8.8
May 11, 2021 12:57:34.276879072 CEST	53	52991	8.8.8.8	192.168.2.4
May 11, 2021 12:57:35.045386076 CEST	53700	53	192.168.2.4	8.8.8.8
May 11, 2021 12:57:35.094764948 CEST	53	53700	8.8.8.8	192.168.2.4
May 11, 2021 12:58:05.709156036 CEST	51726	53	192.168.2.4	8.8.8.8
May 11, 2021 12:58:05.766822100 CEST	53	51726	8.8.8.8	192.168.2.4
May 11, 2021 12:59:10.954557896 CEST	56794	53	192.168.2.4	8.8.8.8
May 11, 2021 12:59:11.003338099 CEST	53	56794	8.8.8.8	192.168.2.4
May 11, 2021 12:59:13.758358955 CEST	56534	53	192.168.2.4	8.8.8.8
May 11, 2021 12:59:13.819736958 CEST	53	56534	8.8.8.8	192.168.2.4
May 11, 2021 12:59:13.830044985 CEST	56627	53	192.168.2.4	8.8.8.8
May 11, 2021 12:59:13.878669024 CEST	53	56627	8.8.8.8	192.168.2.4
May 11, 2021 12:59:14.270876884 CEST	56621	53	192.168.2.4	8.8.8.8
May 11, 2021 12:59:14.339066982 CEST	53	56621	8.8.8.8	192.168.2.4
May 11, 2021 12:59:14.962776899 CEST	63116	53	192.168.2.4	8.8.8.8
May 11, 2021 12:59:15.016153097 CEST	53	63116	8.8.8.8	192.168.2.4
May 11, 2021 12:59:15.930468082 CEST	64078	53	192.168.2.4	8.8.8.8
May 11, 2021 12:59:15.979353905 CEST	53	64078	8.8.8.8	192.168.2.4
May 11, 2021 12:59:16.595551014 CEST	64801	53	192.168.2.4	8.8.8.8
May 11, 2021 12:59:16.655761003 CEST	53	64801	8.8.8.8	192.168.2.4
May 11, 2021 12:59:16.871294975 CEST	61721	53	192.168.2.4	8.8.8.8
May 11, 2021 12:59:16.920097113 CEST	53	61721	8.8.8.8	192.168.2.4
May 11, 2021 12:59:17.917881966 CEST	51255	53	192.168.2.4	8.8.8.8
May 11, 2021 12:59:17.968229055 CEST	53	51255	8.8.8.8	192.168.2.4
May 11, 2021 12:59:18.826654911 CEST	61522	53	192.168.2.4	8.8.8.8
May 11, 2021 12:59:18.887479067 CEST	53	61522	8.8.8.8	192.168.2.4
May 11, 2021 12:59:19.947118998 CEST	52337	53	192.168.2.4	8.8.8.8
May 11, 2021 12:59:19.998945951 CEST	53	52337	8.8.8.8	192.168.2.4
May 11, 2021 12:59:21.046000957 CEST	55046	53	192.168.2.4	8.8.8.8
May 11, 2021 12:59:21.094729900 CEST	53	55046	8.8.8.8	192.168.2.4
May 11, 2021 12:59:22.124907017 CEST	49612	53	192.168.2.4	8.8.8.8
May 11, 2021 12:59:22.173950911 CEST	53	49612	8.8.8.8	192.168.2.4
May 11, 2021 12:59:23.050267935 CEST	49285	53	192.168.2.4	8.8.8.8
May 11, 2021 12:59:23.099495888 CEST	53	49285	8.8.8.8	192.168.2.4
May 11, 2021 12:59:23.971749067 CEST	50601	53	192.168.2.4	8.8.8.8
May 11, 2021 12:59:24.020672083 CEST	53	50601	8.8.8.8	192.168.2.4
May 11, 2021 12:59:39.877810955 CEST	60875	53	192.168.2.4	8.8.8.8
May 11, 2021 12:59:39.939281940 CEST	53	60875	8.8.8.8	192.168.2.4
May 11, 2021 12:59:41.132989883 CEST	56448	53	192.168.2.4	8.8.8.8
May 11, 2021 12:59:41.183327913 CEST	53	56448	8.8.8.8	192.168.2.4
May 11, 2021 12:59:42.164243937 CEST	59172	53	192.168.2.4	8.8.8.8
May 11, 2021 12:59:42.221401930 CEST	53	59172	8.8.8.8	192.168.2.4
May 11, 2021 12:59:42.400079012 CEST	62420	53	192.168.2.4	8.8.8.8
May 11, 2021 12:59:42.448762894 CEST	53	62420	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 11, 2021 12:59:41.132989883 CEST	192.168.2.4	8.8.8.8	0x8bf7	Standard query (0)	outlook.com	A (IP address)	IN (0x0001)
May 11, 2021 12:59:42.164243937 CEST	192.168.2.4	8.8.8.8	0xdcad	Standard query (0)	www.outlook.com	A (IP address)	IN (0x0001)
May 11, 2021 12:59:42.400079012 CEST	192.168.2.4	8.8.8.8	0xb7af	Standard query (0)	outlook.of fice365.com	A (IP address)	IN (0x0001)

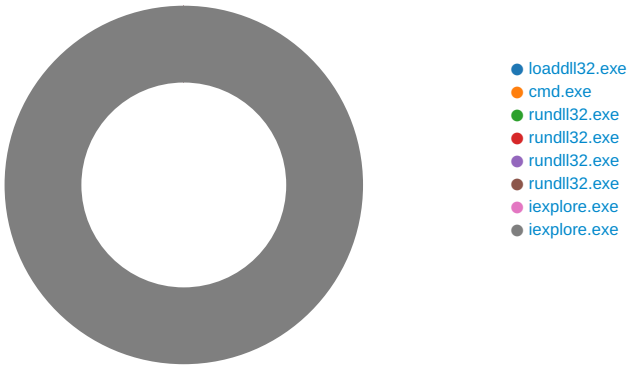
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 11, 2021 12:59:13.819736958 CEST	8.8.8.8	192.168.2.4	0xb976	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 12:59:41.183327913 CEST	8.8.8.8	192.168.2.4	0x8bf7	No error (0)	outlook.com		40.97.116.82	A (IP address)	IN (0x0001)
May 11, 2021 12:59:41.183327913 CEST	8.8.8.8	192.168.2.4	0x8bf7	No error (0)	outlook.com		40.97.160.2	A (IP address)	IN (0x0001)
May 11, 2021 12:59:41.183327913 CEST	8.8.8.8	192.168.2.4	0x8bf7	No error (0)	outlook.com		40.97.148.226	A (IP address)	IN (0x0001)
May 11, 2021 12:59:41.183327913 CEST	8.8.8.8	192.168.2.4	0x8bf7	No error (0)	outlook.com		40.97.164.146	A (IP address)	IN (0x0001)
May 11, 2021 12:59:41.183327913 CEST	8.8.8.8	192.168.2.4	0x8bf7	No error (0)	outlook.com		40.97.128.194	A (IP address)	IN (0x0001)
May 11, 2021 12:59:41.183327913 CEST	8.8.8.8	192.168.2.4	0x8bf7	No error (0)	outlook.com		40.97.156.114	A (IP address)	IN (0x0001)
May 11, 2021 12:59:41.183327913 CEST	8.8.8.8	192.168.2.4	0x8bf7	No error (0)	outlook.com		40.97.153.146	A (IP address)	IN (0x0001)
May 11, 2021 12:59:41.183327913 CEST	8.8.8.8	192.168.2.4	0x8bf7	No error (0)	outlook.com		40.97.161.50	A (IP address)	IN (0x0001)
May 11, 2021 12:59:42.221401930 CEST	8.8.8.8	192.168.2.4	0xdcad	No error (0)	www.outlook.com	outlook.office365.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 12:59:42.221401930 CEST	8.8.8.8	192.168.2.4	0xdcad	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 12:59:42.221401930 CEST	8.8.8.8	192.168.2.4	0xdcad	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 12:59:42.221401930 CEST	8.8.8.8	192.168.2.4	0xdcad	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 12:59:42.221401930 CEST	8.8.8.8	192.168.2.4	0xdcad	No error (0)	HHN-efz.ms-acdc.office.com		40.101.138.210	A (IP address)	IN (0x0001)
May 11, 2021 12:59:42.221401930 CEST	8.8.8.8	192.168.2.4	0xdcad	No error (0)	HHN-efz.ms-acdc.office.com		52.98.151.242	A (IP address)	IN (0x0001)
May 11, 2021 12:59:42.221401930 CEST	8.8.8.8	192.168.2.4	0xdcad	No error (0)	HHN-efz.ms-acdc.office.com		40.101.136.18	A (IP address)	IN (0x0001)
May 11, 2021 12:59:42.221401930 CEST	8.8.8.8	192.168.2.4	0xdcad	No error (0)	HHN-efz.ms-acdc.office.com		52.97.233.34	A (IP address)	IN (0x0001)
May 11, 2021 12:59:42.448762894 CEST	8.8.8.8	192.168.2.4	0xb7af	No error (0)	outlook.office365.com	outlook.ha.office365.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 12:59:42.448762894 CEST	8.8.8.8	192.168.2.4	0xb7af	No error (0)	outlook.ha.office365.com	outlook.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 12:59:42.448762894 CEST	8.8.8.8	192.168.2.4	0xb7af	No error (0)	outlook.ms-acdc.office.com	HHN-efz.ms-acdc.office.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2021 12:59:42.448762894 CEST	8.8.8.8	192.168.2.4	0xb7af	No error (0)	HHN-efz.ms-acdc.office.com		40.101.137.50	A (IP address)	IN (0x0001)
May 11, 2021 12:59:42.448762894 CEST	8.8.8.8	192.168.2.4	0xb7af	No error (0)	HHN-efz.ms-acdc.office.com		52.97.233.66	A (IP address)	IN (0x0001)
May 11, 2021 12:59:42.448762894 CEST	8.8.8.8	192.168.2.4	0xb7af	No error (0)	HHN-efz.ms-acdc.office.com		52.97.233.34	A (IP address)	IN (0x0001)
May 11, 2021 12:59:42.448762894 CEST	8.8.8.8	192.168.2.4	0xb7af	No error (0)	HHN-efz.ms-acdc.office.com		52.98.152.178	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 7048 Parent PID: 5776

General

Start time:	12:57:34
Start date:	11/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\A5uTdwOwJ1.dll'
Imagebase:	0x8a0000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 7056 Parent PID: 7048

General

Start time:	12:57:35
Start date:	11/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\A5uTdwOwJ1.dll',#1
Imagebase:	0x11d0000
File size:	232960 bytes

MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 7064 Parent PID: 7048

General

Start time:	12:57:35
Start date:	11/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\A5uTdwOwJ1.dll,Hundredpopulate@@8
Imagebase:	0x3c0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 7076 Parent PID: 7056

General

Start time:	12:57:35
Start date:	11/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\A5uTdwOwJ1.dll',#1
Imagebase:	0x3c0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000003.00000002.933933475.00000000050E8000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 7132 Parent PID: 7048

General

Start time:	12:57:39
Start date:	11/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\A5uTdwOwJ1.dll,Mark@@12
Imagebase:	0x3c0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 7148 Parent PID: 7048

General

Start time:	12:57:42
Start date:	11/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\A5uTdwOwJ1.dll,Seefit@@8
Imagebase:	0x3c0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 4640 Parent PID: 800

General

Start time:	12:59:38
Start date:	11/05/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff621d60000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: iexplore.exe PID: 1668 Parent PID: 4640

General

Start time:	12:59:39
Start date:	11/05/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:4640 CREDAT:17410 /prefetch:2
Imagebase:	0x850000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\drivers\etc\hosts	unknown	2	success or wait	1	6AC719DD	ReadFile
C:\Windows\System32\drivers\etc\hosts	unknown	998	success or wait	1	6AC80D27	ReadFile

Disassembly

Code Analysis