ID: 1434212
Sample Name: RtlUpd.dll.dll
Cookbook: default.jbs
Time: 17:51:10
Date: 30/04/2024
Version: 40.0.0 Tourmaline

Table of Contents

Table of Contents 2
Windows Analysis Report RtlUpd.dll.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Signatures 4
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
Networking 5
Persistence and Installation Behavior 5
Malware Analysis System Evasion 5
HIPS / PFW / Operating System Protection Evasion 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 7
Domains and IPs 8
Contacted Domains 8
Contacted URLs 8
URLs from Memory and Binaries 8
World Map of Contacted IPs 8
Public IPs 9
General Information 9
Warnings 10
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASNs 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
C:\ProgramData\RtlUpd\RtlUpd.dll 10
C:\ProgramData\RtlUpd\RtlUpd.dll:Zone.Identifier 11
C:\Users\user\AppData\Roaming\RtlUpd\RtlUpd.dll 11
C:\Users\user\AppData\Roaming\RtlUpd\RtlUpd.dll:Zone.Identifier 11
C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache\IE\IQI4U9TB.htm 12
C:\Windows\Tasks\RtlUpd.job 12
Static File Info 12
General 12
File Icon 12
Static PE Info 13
General 13
Entrypoint Preview 13
Data Directories 14
Sections 14
Imports 18
Exports 18
Network Behavior 19
TCP Packets 19
HTTP Request Dependency Graph 20
Statistics 20
Behavior 20
System Behavior 21
Analysis Process: loaddll64.exePID: 6968, Parent PID: 2580 21
General 21
File Activities 21
Analysis Process: conhost.exePID: 6992, Parent PID: 6968 21
General 21
File Activities 22

Analysis Process: cmd.exePID: 1228, Parent PID: 6968 22
General 22
File Activities 22
Analysis Process: regsvr32.exePID: 7140, Parent PID: 6968 22
General 22
Analysis Process: rundll32.exePID: 7132, Parent PID: 1228 22
General 22
File Activities 23
File Created 23
File Written 23
Analysis Process: rundll32.exePID: 2496, Parent PID: 6968 23
General 23
Analysis Process: rundll32.exePID: 2140, Parent PID: 6968 24
General 24
File Activities 24
File Created 24
File Deleted 24
File Written 24
Analysis Process: rundll32.exePID: 7084, Parent PID: 1044 25
General 25
File Activities 25
File Written 25
Analysis Process: rundll32.exePID: 7052, Parent PID: 6968 26
General 26
File Activities 26
File Created 26
File Deleted 26
File Written 26
Analysis Process: rundll32.exePID: 180, Parent PID: 1044 27
General 27
Disassembly 27

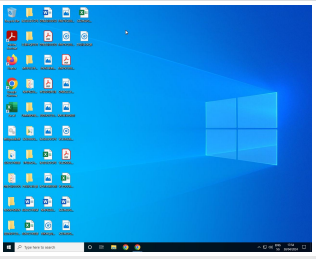
Windows Analysis Report

RtlUpd.dll.dll

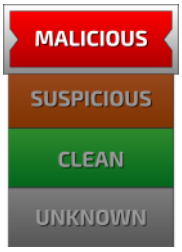
Overview

General Information

Sample name:	RtlUpd.dll.dllrenamed because original name is a hash value
Original sample name:	RtlUpd.dll.exe
Analysis ID:	1434212
MD5:	c16bdc61bbc8…
SHA1:	c2f98475c7be3..
SHA256:	6a195e6111c9…
Tags:	exe
Infos:	



Detection

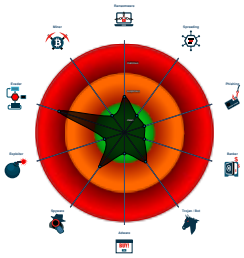


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- System process connects to networ…
- Creates files in the system32 config…
- Drops HTML or HTM files to system…
- Found stalling execution ending in A…
- Contains functionality to dynamicall…
- Contains functionality to record scre…
- Creates a process in suspended mo…
- Creates files inside the system direc…
- Creates job files (autostart)
- Deletes files inside the Windows fol…
- Detected potential crypto function
- Drops PE files

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 6968 cmdline: loaddll64.exe "C:\Users\user\Desktop\RtlUpd.dll.dll" MD5: 763455F9DCB24DFEECC2B9D9F8D46D52)
  - conhost.exe (PID: 6992 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - cmd.exe (PID: 1228 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\RtlUpd.dll.dll",#1 MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
    - rundll32.exe (PID: 7132 cmdline: rundll32.exe "C:\Users\user\Desktop\RtlUpd.dll.dll",#1 MD5: EF3179D498793BF4234F708D3BE28633)
  - regsvr32.exe (PID: 7140 cmdline: regsvr32.exe /s C:\Users\user\Desktop\RtlUpd.dll.dll MD5: B0C2FA35D14A9FAD919E99D9D75E1B9E)
  - rundll32.exe (PID: 2496 cmdline: rundll32.exe C:\Users\user\Desktop\RtlUpd.dll.dll,DllGetClassObject MD5: EF3179D498793BF4234F708D3BE28633)
  - rundll32.exe (PID: 2140 cmdline: rundll32.exe C:\Users\user\Desktop\RtlUpd.dll.dll,DllRegisterServer MD5: EF3179D498793BF4234F708D3BE28633)
  - rundll32.exe (PID: 7052 cmdline: rundll32.exe C:\Users\user\Desktop\RtlUpd.dll.dll,DllRegisterServerEx MD5: EF3179D498793BF4234F708D3BE28633)
- rundll32.exe (PID: 7084 cmdline: C:\Windows\system32\rundll32.exe "C:\ProgramData\RtlUpd\RtlUpd.dll",Start /p MD5: EF3179D498793BF4234F708D3BE28633)
- rundll32.exe (PID: 180 cmdline: C:\Windows\system32\rundll32.exe "C:\Users\user\AppData\Roaming\RtlUpd\RtlUpd.dll",Start /p MD5: EF3179D498793BF4234F708D3BE28633)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Networking

System process connects to network (likely due to code injection or exploit)

Persistence and Installation Behavior

Creates files in the system32 config directory

Drops HTML or HTM files to system directories

Malware Analysis System Evasion

Found stalling execution ending in API Sleep call

HIPS / PFW / Operating System Protection Evasion

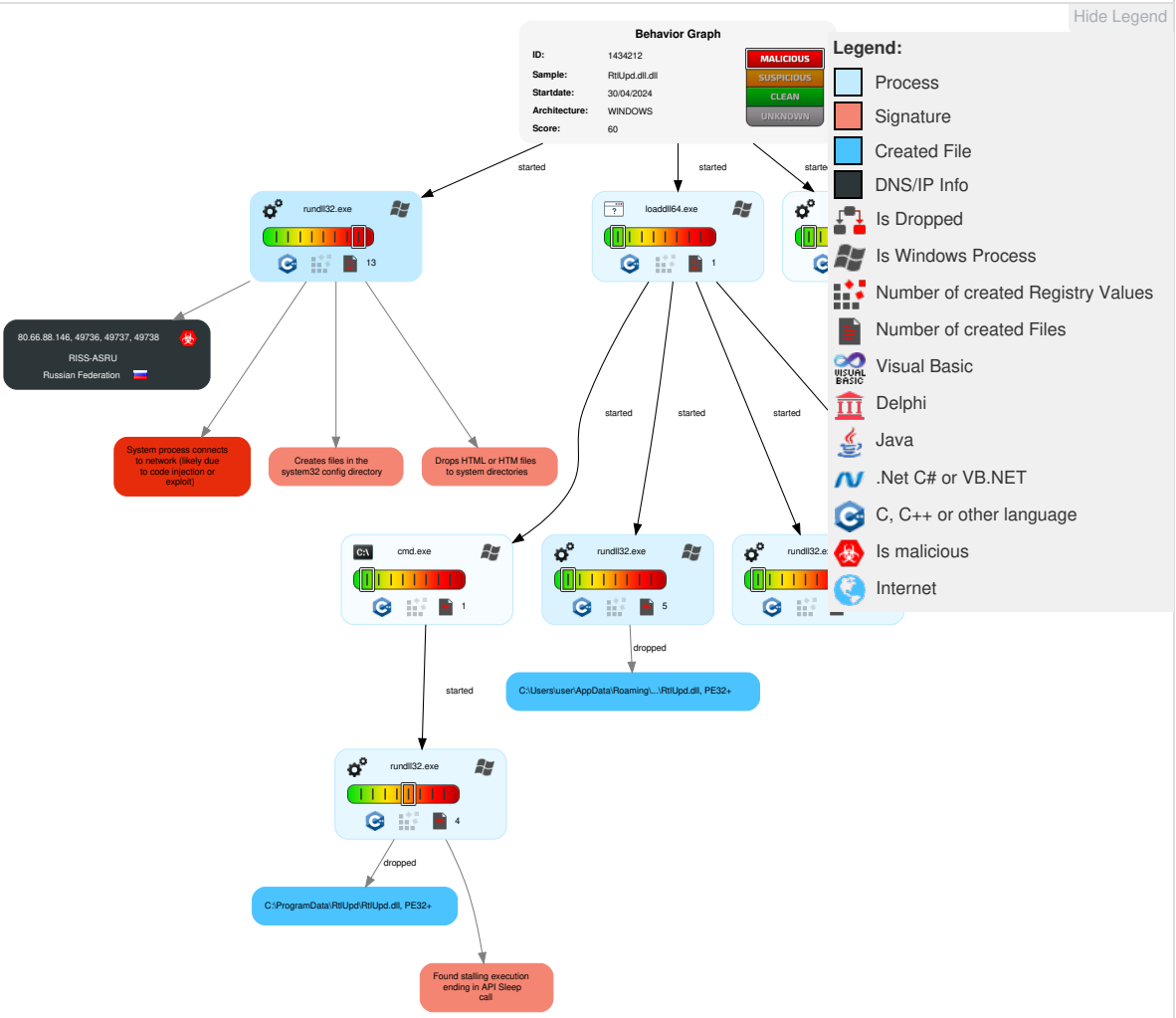
System process connects to network (likely due to code injection or exploit)

Mitre Att&ck Matrix

Reconnai...	Resource Developm...	Initial Access	Execution	Persisten...	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	Valid Accounts	1 Scheduled Task/Job	1 Scheduled Task/Job	1 1 1 Process Injection	1 1 1 Masquerading	OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Screen Capture	1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	1 Native API	1 DLL Side-Loading	1 Scheduled Task/Job	1 1 Virtualization/Sandbox Evasion	LSASS Memory	1 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Archive Collected Data	2 Ingress Tool Transfer	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	1 DLL Side-Loading	1 1 1 Process Injection	Security Account Manager	1 Application Window Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	2 Non-Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	1 Regsvr32	NTDS	1 Account Discovery	Distributed Component Object Model	Input Capture	1 2 Application Layer Protocol	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	1 Rundll32	LSA Secrets	1 System Owner/User Discovery	SSH	Keylogging	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	1 DLL Side-Loading	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	1 File Deletion	DCSync	2 3 System Information Discovery	Windows Remote Management	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery

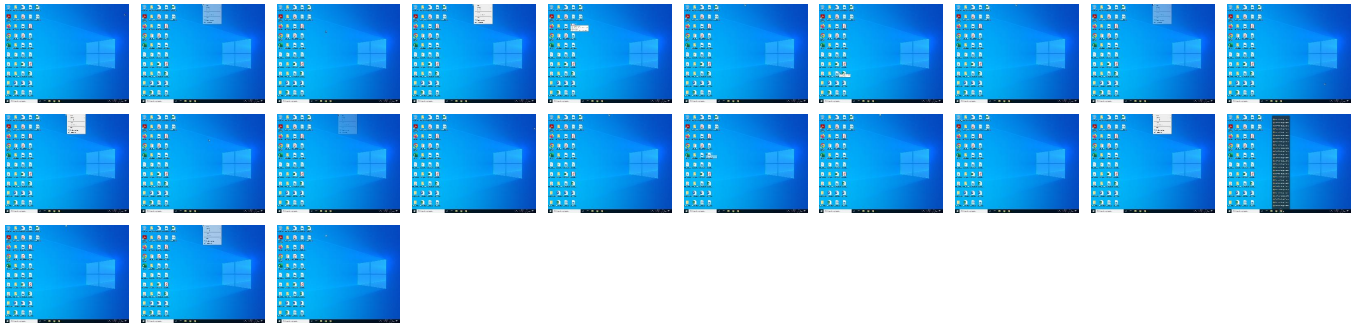
Behavior Graph



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
RtlUpd.dll.dll	8%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ProgramData\RtlUpd\RtlUpd.dll	8%	ReversingLabs		
C:\Users\user\AppData\Roaming\RtlUpd\RtlUpd.dll	8%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://80.66.88.146/$	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://80.66.88.146/ingsU	0%	Avira URL Cloud	safe	
http://80.66.88.146	0%	Avira URL Cloud	safe	
http://80.66.88.146/I	0%	Avira URL Cloud	safe	
http://80.66.88.146/LMEM	0%	Avira URL Cloud	safe	
http://80.66.88.146/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

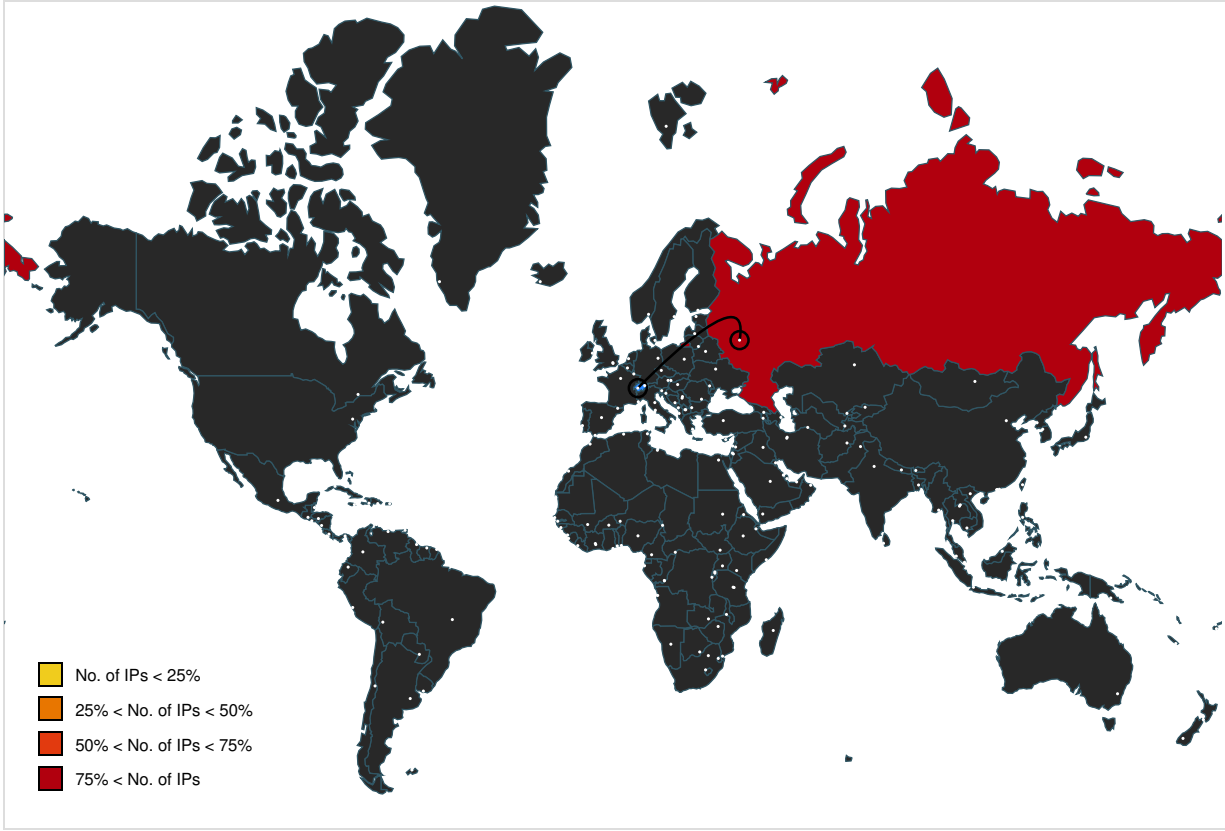
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://80.66.88.146/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://80.66.88.146	rundll32.exe, 00000007.00000002.34706654 14.000001EB5B20B000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://80.66.88.146/ingsU	rundll32.exe, 00000007.00000002.34706654 14.000001EB5B241000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://80.66.88.146/ingsu	rundll32.exe, 00000007.00000002.34706654 14.000001EB5B241000.00000004.00000020.00 020000.00000000.sdmp	false		unknown
http://80.66.88.146/I	rundll32.exe, 00000007.00000002.34706654 14.000001EB5B241000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://80.66.88.146/$	rundll32.exe, 00000007.00000002.34706654 14.000001EB5B241000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://80.66.88.146/LMEM	rundll32.exe, 00000007.00000002.34706654 14.000001EB5B241000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
80.66.88.146	unknown	Russian Federation		20803	RISS-ASRU	true

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1434212
Start date and time:	2024-04-30 17:51:10 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 5m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Run name:	Run with higher sleep bypass
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample name:	RtlUpd.dll.dllrenamed because original name is a hash value
Original Sample Name:	RtlUpd.dll.exe
Detection:	MAL
Classification:	mal60.evad.winDLL@16/6@0/1
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Found application associated with file extension: .dll • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SIHClient.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ocsp.digicert.com, slscr.update.microsoft.com, ctldl.windowsupdate.com, fe3cr.delivery.mp.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: RtlUpd.dll.dll

Simulations

Behavior and APIs

Time	Type	Description
17:52:36	API Interceptor	6941265x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\RtlUpd\RtlUpd.dll

Process:	C:\Windows\System32\rundll32.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	64000
Entropy (8bit):	5.9815146397872825
Encrypted:	false
SSDEEP:	1536:yyMGpJvykUU0mVWUBmJyB1NjKOaSHGfuUF8u7J8NG3:nrpPUUXWXK1NoLfuQ8u7J8Nw
MD5:	C16BDC61BBC82E9668F8CEE9CC5C94C5
SHA1:	C2F98475C7BE3064E0B294EF546F57D3C3A1E267
SHA-256:	6A195E6111C9A4B8C874D51937B53CD5B4B78EFC32F7BB255012D05087586D8F
SHA-512:	9337275916970BD88FB1DE18959BF587E29147CF6198E3A242679B198CCA26D7DDEEDA2E893145058444E494048768AC33CE36E75A44FB84B4A0C50A3814FAAE
Malicious:	false

Antivirus:	• Antivirus: ReversingLabs, Detection: 8%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....\.....".."...$.....P.....v1.. ..`... .....0.....@.....p..d..... ...(.....C.....text...x.....`.P`.data...@.....@. `..rdata..p.....@.`@.pdata.....@.0@.xdata.....@.0@.bss..... .....`..edata.....0.....@.0@.idata.....@.... .....@.0..CRT....X....P.....@.@..tls.....`.....@.@..reloc..d....p.....@.0B..... .....

C:\ProgramData\RtlUpd\RtlUpd.dll:Zone.Identifier

Process:	C:\Windows\System32\rundll32.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	false
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\RtlUpd\RtlUpd.dll

Process:	C:\Windows\System32\rundll32.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	64000
Entropy (8bit):	5.9815146397872825
Encrypted:	false
SSDEEP:	1536:yyMGpJvykUU0mVWUBmJyB1NjKOaSHGfuUF8u7J8NG3:nrpPUUXWXK1NoLfuQ8u7J8Nw
MD5:	C16BDC61BBC82E9668F8CEE9CC5C94C5
SHA1:	C2F98475C7BE3064E0B294EF546F57D3C3A1E267
SHA-256:	6A195E6111C9A4B8C874D51937B53CD5B4B78EFC32F7BB255012D05087586D8F
SHA-512:	9337275916970BD88FB1DE18959BF587E29147CF6198E3A242679B198CCA26D7DDEEDA2E893145058444E494048768AC33CE36E75A44FB84B4A0C50A3814FAAB
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 8%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....\.....".."...$.....P.....v1.. ..`... .....0.....@.....p..d..... ...(.....C.....text...x.....`.P`.data...@.....@. `..rdata..p.....@.`@.pdata.....@.0@.xdata.....@.0@.bss..... .....`..edata.....0.....@.0@.idata.....@.... .....@.0..CRT....X....P.....@.@..tls.....`.....@.@..reloc..d....p.....@.0B..... .....

C:\Users\user\AppData\Roaming\RtlUpd\RtlUpd.dll:Zone.Identifier

Process:	C:\Windows\System32\rundll32.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache\IE\IQI4U9TB.htm

Process:	C:\Windows\System32\rundll32.exe
File Type:	data
Category:	dropped
Size (bytes):	32
Entropy (8bit):	4.8125
Encrypted:	false
SSDEEP:	3:7l1uJEu:+Jd
MD5:	328235BEF59599CA93504FB142C7E9B2
SHA1:	5A29393A1853E8690B35003C4CD7BE48D36EB05D
SHA-256:	D214355692C767260D3D5D61F9377DA1B8F134CE11141EF6FFC17C8998E7B0F3
SHA-512:	F38918D2E7F328BAF0DAC0C76C65FD51702F7F99798C8D7F9C85121F52FC7F155337E19AFABC2C6AFB513434E6E3E52B82896D0D72621E71E45C8E1E59C1FA5
Malicious:	false
Preview:	G=..%.b.....y....z.?.!..,!b...

C:\Windows\Tasks\RtlUpd.job

Process:	C:\Windows\System32\rundll32.exe
File Type:	data
Category:	modified
Size (bytes):	358
Entropy (8bit):	3.5811470449240352
Encrypted:	false
SSDEEP:	6:odY3LsU/82On+SkSJkJAWhAlAtnRKUEZglJPZiY5DiliyjgsW2YRZuy0lGC1:oWnhO+fTWl4RKMJFuYyjzvYRQVGG
MD5:	8F1FEF7C9F3C52A700D463FAB6499AAD
SHA1:	1607BB266F1D03EBB1C63DB7E9C732ACD08B1548
SHA-256:	9CA148BAC0231789AC581B6FFEC71A9A84584D64309A59C636ED14E55C2BD049
SHA-512:	EE37315E05F25012B3C24F392F70BF9C991A1780A58DF9C3C60F6C8BFF7CDDF9335E5FCE9378A64C2C9DC28FDAF24AD69E3C1310824365B88ABC29AA58B70C9
Malicious:	false
Preview:	......F7.a.M.....F.4.....<... .....\..... .....!.C.:.\.W.i.n.d.o.w.s.\.s.y.s.t.e.m.3.2.\.r.u.n.d.l.l.3.2...e.x.e...<.".C.:.\.U.s.e.r.s.\.j.o.n.e.s.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.R.t.l.U.p.d.\.R.t.l.U.p.d...d.l.l.".,.S.t.a.r.t. ./.p.....J.O.N.E.S.-.P.C.\.j.o.n.e.s.....0.....5.....

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64 (stripped to external PDB), for MS Windows
Entropy (8bit):	5.9815146397872825
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 86.43% • Win64 Executable (generic) (12005/4) 10.17% • Generic Win/DOS Executable (2004/3) 1.70% • DOS Executable Generic (2002/1) 1.70% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	RtlUpd.dll.dll
File size:	64'000 bytes
MD5:	c16bdc61bbc82e9668f8cee9cc5c94c5
SHA1:	c2f98475c7be3064e0b294ef546f57d3c3a1e267
SHA256:	6a195e6111c9a4b8c874d51937b53cd5b4b78efc32f7bb255012d05087586d8f
SHA512:	9337275916970bd88fb1de18959bf587e29147cf6198e3a242679b198cca26d7ddeeda2e893145058444e494048768ac33ce36e75a44fb84b4a0c50a3814faae
SSDEEP:	1536:yyMGpJvykUU0mVWUBmJyB1NjKOaSHGfuUF8u7J8NG3:nrpPUUXWXK1NoLfuQ8u7J8Nw
TLSH:	C553175EE29361FCC92AD1704ABB6673E972F81244355F7F53A8DB352E20E601E1DB02
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....\....."...$.....P.....v1....`....

File Icon

Icon Hash:	7ae282899bbab082

Static PE Info

General

Entrypoint:	0x2eda31350
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x2eda30000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, LARGE_ADDRESS_AWARE, DEBUG_STRIPPED, DLL
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5CAA13F4 [Sun Apr 7 15:15:00 2019 UTC]
TLS Callbacks:	0xeda36690, 0x2, 0xeda36660, 0x2
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:	9e89b06661c393195797fb70ceba29aa

Entrypoint Preview

Instruction
dec eax
mov eax, dword ptr [0000DED9h]
mov dword ptr [eax], 00000000h
jmp 00007FF481332E23h
nop word ptr [eax+eax+00000000h]
nop dword ptr [eax]
dec eax
mov edx, ecx
dec eax
lea ecx, dword ptr [00010C86h]
jmp 00007FF48133E096h
nop
dec eax
lea ecx, dword ptr [00000009h]
jmp 00007FF481332F69h
nop dword ptr [eax+00h]
ret
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
dec eax
sub esp, 28h
call 00007FF48133384Ch
xor eax, eax
mov dword ptr [00010C6Bh], 00000001h

Instruction
dec eax
add esp, 28h
ret
nop word ptr [eax+eax+00h]
dec eax
sub esp, 48h
cmp edx, 01h
je 00007FF481332F91h
mov eax, 00000001h
dec eax
add esp, 48h
ret
nop dword ptr [eax+eax+00h]
dec eax
lea eax, dword ptr [esp+3Ch]
dec ecx
mov ecx, ecx
xor edx, edx
xor ecx, ecx
dec eax
mov dword ptr [esp+28h], eax
dec esp
lea eax, dword ptr [FFFFFFB0h]
mov dword ptr [esp+20h], 00000000h
call dword ptr [00012FE2h]
dec eax
mov ecx, eax
dec eax
test eax, eax
je 00007FF481332F45h
call dword ptr [00012FA4h]
mov eax, 00000001h
dec eax
add esp, 48h
ret
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x13000	0xb8	.edata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x14000	0xddc	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x10000	0x6a8	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x17000	0x64	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xec20	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x14380	0x308	.idata
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	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xb678	0xb800	a05bb3976a8535f5d7d2c9b263a8c0f4	False	0.5412703804347826	data	6.132863794462644	IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0xd000	0x240	0x400	39812a0080ea5a8e3b29986c7fac2ff7	False	0.3603515625	data	3.0854466330397283	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0xe000	0x1270	0x1400	e8010488f823135d4c017d13f665cb22	False	0.5732421875	data	5.999000118325584	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.pdata	0x10000	0x6a8	0x800	19ad9bed048378e8f4dc5b0745837971	False	0.4462890625	data	4.053471163001168	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ
.xdata	0x11000	0x6cc	0x800	253635c5a92f3bd2cf12f8af479d8999	False	0.30419921875	data	4.092124688054801	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ
.bss	0x12000	0xcb0	0x0	d41d8cd98f00b204e9800998ecf8427e	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.edata	0x13000	0xb8	0x200	8a46b896e2553bfa4a112a8c56d99f36	False	0.271484375	data	2.1155951975884175	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ
.idata	0x14000	0xddc	0xe00	46529325549e38d35928a2f85d917bd9	False	0.34486607142857145	data	4.457656157934565	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.CRT	0x15000	0x58	0x200	988a45858ec4e1a6fecf191e359a7478	False	0.05859375	data	0.25323120180391656	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.tls	0x16000	0x10	0x200	bf619eac0cdf3f68d496ea9344137e8b	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.reloc	0x17000	0x64	0x200	3ca19c693469494ae8d8d505a9ecf7a2	False	0.203125	data	1.0585418969030347	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
ADVAPI32.dll	GetUserNameW, RegCloseKey, RegEnumKeyExW, RegOpenKeyExW, RegQueryValueExW
KERNEL32.dll	CloseHandle, CopyFileW, CreateFileW, CreateMutexW, CreatePipe, CreateProcessW, CreateThread, DeleteCriticalSection, DeleteFileW, EnterCriticalSection, ExpandEnvironmentStringsW, FindClose, FindFirstFileW, FindNextFileW, GetCommandLineW, GetComputerNameExW, GetComputerNameW, GetCurrentDirectoryW, GetLastError, GetModuleFileNameW, GetModuleHandleW, GetProcAddress, GetProcessHeap, GetSystemInfo, GetTempPathW, GetTickCount, GetVolumeInformationW, GlobalMemoryStatusEx, HeapAlloc, HeapFree, HeapReAlloc, InitializeCriticalSection, IsDBCSLeadByteEx, LeaveCriticalSection, LoadLibraryW, MultiByteToWideChar, PeekNamedPipe, ReadFile, SetCurrentDirectoryW, SetFilePointer, SetHandleInformation, SetLastError, Sleep, TerminateProcess, TlsGetValue, VirtualProtect, VirtualQuery, WaitForSingleObject, WideCharToMultiByte, WriteFile
msvcrt.dll	___lc_codepage_func, ___mb_cur_max_func, __iob_func, _amsg_exit, _errno, _initterm, _lock, _unlock, _wcsnicmp, abort, calloc, fputwc, free, fwprintf, fwrite, localeconv, malloc, memcpy, memset, realloc, strcat, strcpy, strerror, strlen, strncmp, vfprintf, wcscat, wcscmp, wcscpy, wcslen
SHELL32.dll	CommandLineToArgvW, SHGetFolderPathW
WS2_32.dll	WSACleanup, WSAStartup, gethostbyname, gethostname, inet_ntoa

Exports

Name	Ordinal	Address
DllGetClassObject	1	0x2eda314a0
DllRegisterServer	2	0x2eda31420
DllRegisterServerEx	3	0x2eda31460
DllUnregisterServer	4	0x2eda314e0
Start	5	0x2eda31520

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 30, 2024 17:52:18.830410004 CEST	49736	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:19.054094076 CEST	80	49736	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:19.054316998 CEST	49736	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:19.054620981 CEST	49736	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:19.277686119 CEST	80	49736	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:19.279403925 CEST	80	49736	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:19.279604912 CEST	49736	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:19.305907011 CEST	49736	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:19.530771971 CEST	80	49736	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:19.530791044 CEST	80	49736	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:19.530843019 CEST	49736	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:19.530888081 CEST	49736	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:19.531183004 CEST	49736	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:19.550616980 CEST	49737	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:19.754061937 CEST	80	49736	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:19.766048908 CEST	80	49737	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:19.766141891 CEST	49737	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:19.766374111 CEST	49737	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:19.766396999 CEST	49737	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:19.981156111 CEST	80	49737	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:19.981172085 CEST	80	49737	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:19.981504917 CEST	80	49737	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:19.981585026 CEST	49737	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:19.981618881 CEST	80	49737	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:19.981662035 CEST	49737	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:19.981674910 CEST	49737	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:19.981674910 CEST	49737	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:20.196383953 CEST	80	49737	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:26.857930899 CEST	49738	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:27.072691917 CEST	80	49738	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:27.072913885 CEST	49738	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:27.073122025 CEST	49738	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:27.287964106 CEST	80	49738	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:27.290714979 CEST	80	49738	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:27.290775061 CEST	49738	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:27.290853024 CEST	80	49738	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:27.290882111 CEST	49738	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:27.290893078 CEST	49738	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:27.505444050 CEST	80	49738	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:32.327569008 CEST	49739	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:32.548178911 CEST	80	49739	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:32.548386097 CEST	49739	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:32.548837900 CEST	49739	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:32.769150019 CEST	80	49739	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:32.771917105 CEST	80	49739	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:32.771934986 CEST	80	49739	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:32.772038937 CEST	49739	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:32.772207022 CEST	49739	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:32.772207022 CEST	49739	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:32.993151903 CEST	80	49739	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:39.198965073 CEST	49740	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:39.417150021 CEST	80	49740	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:39.417325974 CEST	49740	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:39.417474031 CEST	49740	80	192.168.2.4	80.66.88.146

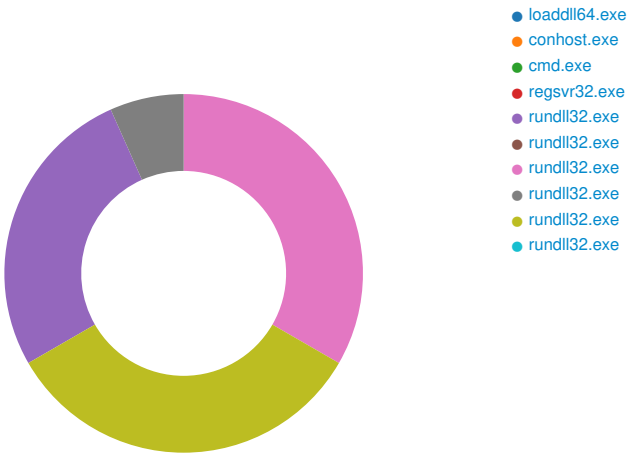
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 30, 2024 17:52:39.635485888 CEST	80	49740	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:39.637701035 CEST	80	49740	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:39.637715101 CEST	80	49740	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:39.637753010 CEST	49740	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:39.637780905 CEST	49740	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:39.637811899 CEST	49740	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:39.855859041 CEST	80	49740	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:45.031493902 CEST	49741	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:45.256762981 CEST	80	49741	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:45.256902933 CEST	49741	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:45.257078886 CEST	49741	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:45.481359959 CEST	80	49741	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:45.486555099 CEST	80	49741	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:45.486568928 CEST	80	49741	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:45.486658096 CEST	49741	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:45.486831903 CEST	49741	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:45.710442066 CEST	80	49741	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:49.855294943 CEST	49742	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:50.072323084 CEST	80	49742	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:50.072443962 CEST	49742	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:50.072643995 CEST	49742	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:50.287134886 CEST	80	49742	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:50.289186954 CEST	80	49742	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:50.289207935 CEST	80	49742	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:50.289271116 CEST	49742	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:50.289305925 CEST	49742	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:50.289387941 CEST	49742	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:50.503932953 CEST	80	49742	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:53.871150970 CEST	49744	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:54.098102093 CEST	80	49744	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:54.098189116 CEST	49744	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:54.098445892 CEST	49744	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:54.325212002 CEST	80	49744	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:54.327941895 CEST	80	49744	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:54.327960014 CEST	80	49744	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:54.327996016 CEST	49744	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:54.328028917 CEST	49744	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:54.328110933 CEST	49744	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:54.554904938 CEST	80	49744	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:58.392121077 CEST	49745	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:58.614100933 CEST	80	49745	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:58.614171982 CEST	49745	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:58.614346027 CEST	49745	80	192.168.2.4	80.66.88.146
Apr 30, 2024 17:52:58.836218119 CEST	80	49745	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:58.839211941 CEST	80	49745	80.66.88.146	192.168.2.4
Apr 30, 2024 17:52:58.839246988 CEST	80	49745	80.66.88.146	192.168.2.4

HTTP Request Dependency Graph

- 80.66.88.146

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: 6968, Parent PID: 2580

General

Target ID:	0
Start time:	17:51:55
Start date:	30/04/2024
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\RtlUpd.dll.dll"
Imagebase:	0x7ff6a0360000
File size:	165'888 bytes
MD5 hash:	763455F9DCB24DFEECC2B9D9F8D46D52
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6992, Parent PID: 6968

General

Target ID:	1
Start time:	17:51:55
Start date:	30/04/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 1228, Parent PID: 6968

General

Target ID:	2
Start time:	17:51:55
Start date:	30/04/2024
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\RtlUpd.dll.dll",#1
Imagebase:	0x7ff723f00000
File size:	289'792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 7140, Parent PID: 6968

General

Target ID:	3
Start time:	17:51:55
Start date:	30/04/2024
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\RtlUpd.dll.dll
Imagebase:	0x7ff7e1000000
File size:	25'088 bytes
MD5 hash:	B0C2FA35D14A9FAD919E99D9D75E1B9E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: rundll32.exe PID: 7132, Parent PID: 1228

General

Target ID:	4
Start time:	17:51:55
Start date:	30/04/2024

Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\RtlUpd.dll.dll",#1
Imagebase:	0x7ff7ee790000
File size:	71'680 bytes
MD5 hash:	EF3179D498793BF4234F708D3BE28633
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\RtlUpd\RtlUpd.dll	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	7FFE148D4C80	CopyFileW
C:\ProgramData\RtlUpd\RtlUpd.dll\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	7FFE148D4C80	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\RtlUpd\RtlUpd.dll	0	64000	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 0b 00 fd 13 fd 5c 00 00 00 00 00 00 00 00 fd 00 2e 22 0b 02 02 24 00 fd 00 00 00 fd 00 00 00 0e 00 00 50 13 00 00 00 10 00 00 00 00 fd fd 02 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 fd 01 00 00 04 00 00 76 31 01 00 02 00 60 01 00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEd\."$Pv1`	success or wait	1	7FFE148D4C80	CopyFileW
C:\ProgramData\RtlUpd\RtlUpd.dll:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	7FFE148D4C80	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **2496**, Parent PID: **6968**

General

Target ID:	5

Start time:	17:51:55
Start date:	30/04/2024
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\RtlUpd.dll.dll,DllGetClassObject
Imagebase:	0x7ff7ee790000
File size:	71'680 bytes
MD5 hash:	EF3179D498793BF4234F708D3BE28633
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: rundll32.exe PID: **2140**, Parent PID: **6968**

General

Target ID:	6
Start time:	17:51:58
Start date:	30/04/2024
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\RtlUpd.dll.dll,DllRegisterServer
Imagebase:	0x7ff7ee790000
File size:	71'680 bytes
MD5 hash:	EF3179D498793BF4234F708D3BE28633
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\RtlUpd\RtlUpd.dll	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	7FFE148D4C80	CopyFileW
C:\ProgramData\RtlUpd\RtlUpd.dll\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	7FFE148D4C80	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\RtlUpd\RtlUpd.dll	success or wait	1	7FFE148D4C71	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\RtlUpd\RtlUpd.dll	0	64000	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 0b 00 fd 13 fd 5c 00 00 00 00 00 00 00 00 fd 00 2e 22 0b 02 02 24 00 fd 00 00 00 fd 00 00 00 0e 00 00 50 13 00 00 00 10 00 00 00 00 fd fd 02 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 fd 01 00 00 04 00 00 76 31 01 00 02 00 60 01 00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEd\."$Pv1`	success or wait	1	7FFE148D4C80	CopyFileW
C:\ProgramData\RtlUpd\RtlUpd.dll:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	7FFE148D4C80	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe

PID: **7084**, Parent PID: **1044**

General

Target ID:	7
Start time:	17:52:00
Start date:	30/04/2024
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\rundll32.exe "C:\ProgramData\RtlUpd\RtlUpd.dll",Start /p
Imagebase:	0x7ff7ee790000
File size:	71'680 bytes
MD5 hash:	EF3179D498793BF4234F708D3BE28633
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	false

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache\IE\IQI4U9TB.htm	0	32	47 3d fd fd 25 fd 62 fd 12 fd 2e fd fd 79 12 81 fd fd 7a fd 3f fd 21 fd fd 2c 21 62 00 0f fd	G=%b.yz?!,!b	success or wait	1	7FFE148B2442	InternetReadFile

Analysis Process: rundll32.exe PID: 7052, Parent PID: 6968

General

Target ID:	8
Start time:	17:52:01
Start date:	30/04/2024
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\RtlUpd.dll.dll,DllRegisterServerEx
Imagebase:	0x800000
File size:	71'680 bytes
MD5 hash:	EF3179D498793BF4234F708D3BE28633
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\RtlUpd\RtlUpd.dll	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	7FFE148D4C80	CopyFileW
C:\Users\user\AppData\Roaming\RtlUpd\RtlUpd.dll\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	7FFE148D4C80	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\RtlUpd\RtlUpd.dll	cannot delete	1	7FFE148D4C71	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\RtlUpd\RtlUpd.dll	0	64000	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 fd 0b 00 fd 13 fd 5c 00 00 00 00 00 00 00 00 fd 00 2e 22 0b 02 02 24 00 fd 00 00 00 fd 00 00 00 0e 00 00 50 13 00 00 00 10 00 00 00 00 fd fd 02 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 fd 01 00 00 04 00 00 76 31 01 00 02 00 60 01 00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEd\."$Pv1`	success or wait	1	7FFE148D4C80	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\RtlUpd\RtlUpd.dll:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	7FFE148D4C80	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **180**, Parent PID: **1044**

General

Target ID:	12
Start time:	17:53:00
Start date:	30/04/2024
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\rundll32.exe "C:\Users\user\AppData\Roaming\RtlUpd\RtlUpd.dll",Start /p
Imagebase:	0x7ff7ee790000
File size:	71'680 bytes
MD5 hash:	EF3179D498793BF4234F708D3BE28633
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Disassembly

No disassembly