ID: 745000
Sample Name: En3ZIyuYdw.exe
Cookbook: default.jbs
Time: 16:53:04
Date: 13/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

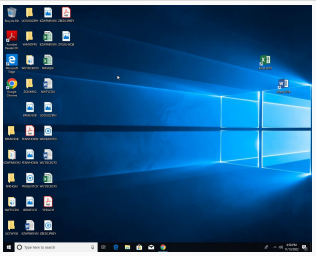
Windows Analysis Report

En3ZIyuYdw.exe

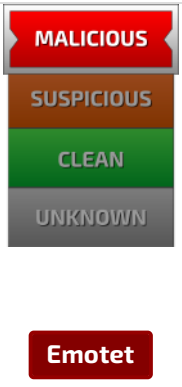
Overview

General Information

Sample Name:	En3ZIyuYdw.exe (renamed file extension from exe to dll)
Analysis ID:	745000
MD5:	633fd626fe5a132.
SHA1:	01d495949dd7e8.
SHA256:	23a872dfbba73a..
Tags:	dll exe
Infos:	



Detection



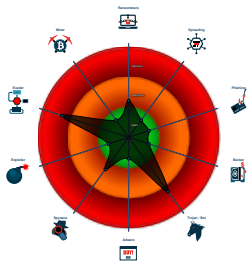
Emotet

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Emotet
- System process connects to networ…
- Snort IDS alert for network traffic
- Hides that the sample has been dow…
- Queries the volume information (nam…
- Contains functionality to check if a d…
- Deletes files inside the Windows fol…
- May sleep (evasive loops) to hinder…
- Uses code obfuscation techniques (…
- Creates files inside the system direc…
- PE file contains sections with non-s…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 4348 cmdline: loaddll64.exe "C:\Users\user\Desktop\En3ZIyuYdw.dll" MD5: C676FC0263EDD17D4CE7D644B8F3FCD6)
  - conhost.exe (PID: 860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 3752 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\En3ZIyuYdw.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 5860 cmdline: rundll32.exe "C:\Users\user\Desktop\En3ZIyuYdw.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
      - regsvr32.exe (PID: 4180 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\LkpZARPPMYxrpnAus\oSMG.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - regsvr32.exe (PID: 4992 cmdline: regsvr32.exe /s C:\Users\user\Desktop\En3ZIyuYdw.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - regsvr32.exe (PID: 6056 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\CVFdhpNOtsemq\TpsMttdDUpxciwO.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 5040 cmdline: rundll32.exe C:\Users\user\Desktop\En3ZIyuYdw.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
    - regsvr32.exe (PID: 6052 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\QkeveKELwVTlid\eYjpj.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - regsvr32.exe (PID: 64 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\Alnqcua\qiwFWDzKBdg.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
- regsvr32.exe (PID: 6112 cmdline: C:\Windows\system32\regsvr32.exe" "C:\Windows\system32\LkpZARPPMYxrpnAus\oSMG.dll MD5: D78B75FC68247E8A63ACBA846182740E)
  - regsvr32.exe (PID: 712 cmdline: C:\Windows\system32\regsvr32.exe "C:\Users\user\AppData\Local\RGgdaHRy\SOHUjYiDXi.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.462452546.0000000000640000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000000.00000002.318758650.000001E98A250000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000003.00000002.313082839.0000000001280000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.310936367.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000005.00000002.311118162.0000020D28BC0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 5 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.rundll32.exe.1e4c44e0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
14.2.regsvr32.exe.640000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0.2.loaddll64.exe.1e98a250000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
5.2.rundll32.exe.20d28bc0000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
3.2.regsvr32.exe.1280000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 5 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET CNC Feodo Tracker Reported CnC Server TCP group 3 - Source IP: 192.168.2.5 - Destination IP: 115.178.55.22 −

Timestamp:	192.168.2.5115.178.55.2249700802404304 11/13/22-16:54:45.127001
SID:	2404304
Source Port:	49700
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Networking

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

Snort IDS alert for network traffic

E-Banking Fraud

Yara detected Emotet

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion

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

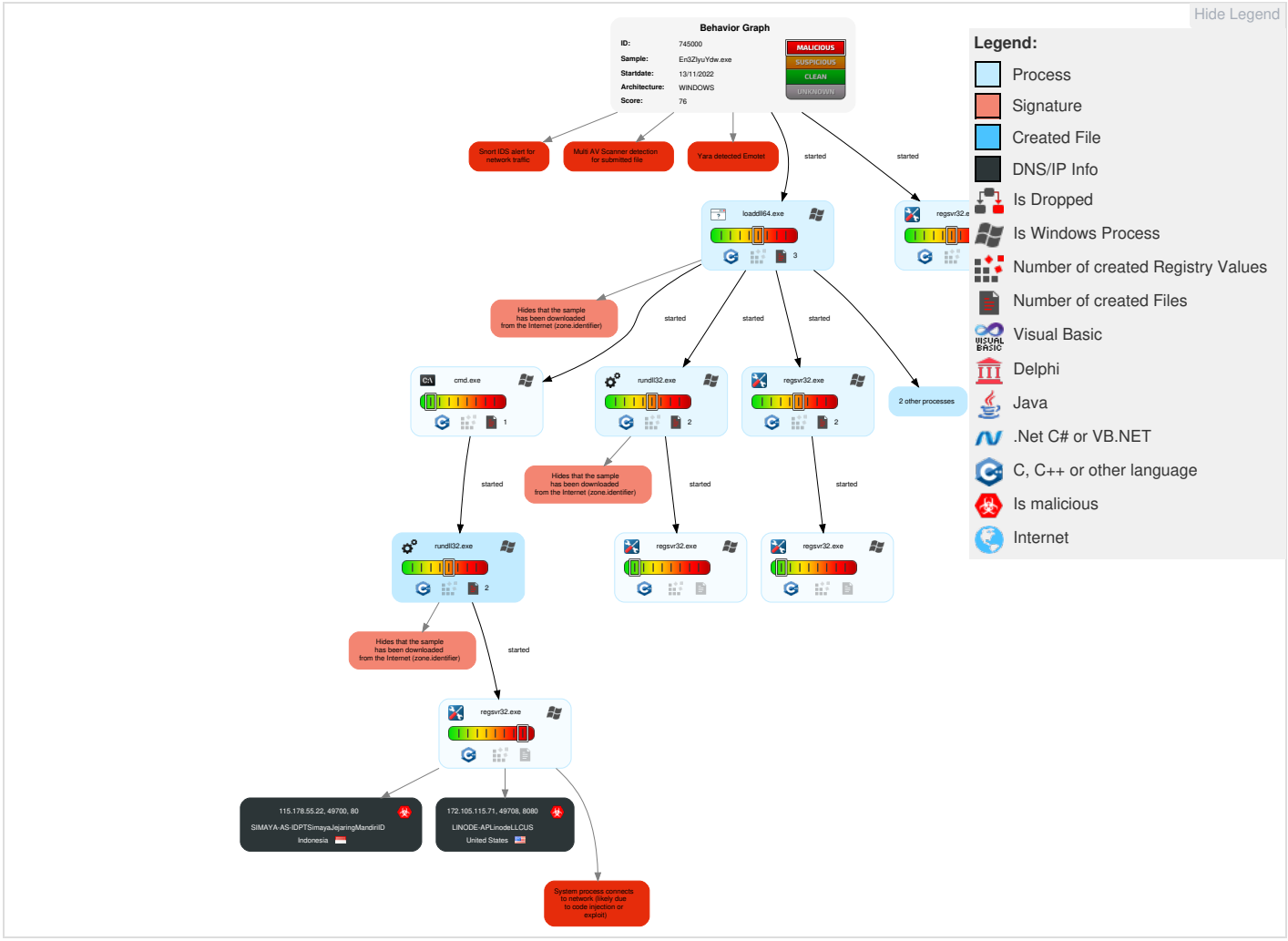
Stealing of Sensitive Information

Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	1 DLL Side-Loading	1 1 1 Process Injection	2 1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Virtualization/Sandbox Evasion	LSASS Memory	2 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 1 Process Injection	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Hidden Files and Directories	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Regsvr32	Cached Domain Credentials	2 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Rundll32	DCSync	2 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 DLL Side-Loading	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 File Deletion	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

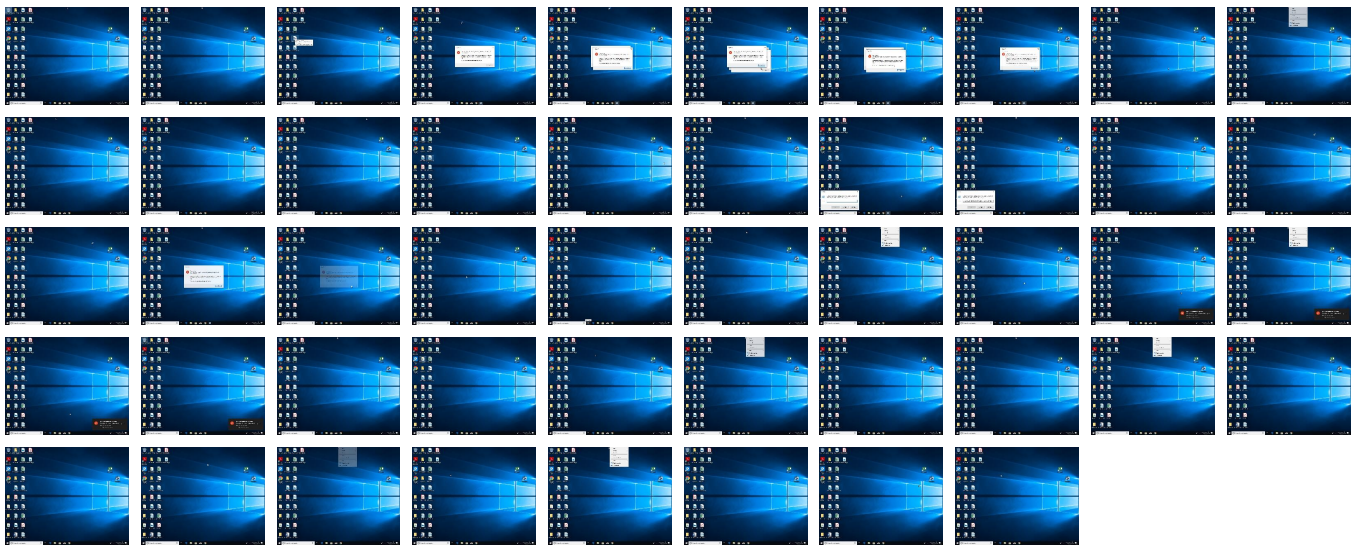
Behavior Graph



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
En3ZIyuYdw.dll	45%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.2.regsvr32.exe.640000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
0.2.loaddll64.exe.1e98a250000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
3.2.regsvr32.exe.1280000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.2.rundll32.exe.1e4c44e0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
5.2.rundll32.exe.20d28bc0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://172.105.115.71:8080/E	0%	Avira URL Cloud	safe	
http://https://172.105.115.71:8080/gumktuwcdwjgjgt/xmwkrcvtq/hnafdgsuhec/T	0%	Avira URL Cloud	safe	
http://https://172.105.115.71:8080/gumktuwcdwjgjgt/xmwkrcvtq/hnafdgsuhec/	0%	Avira URL Cloud	safe	

Domains and IPs

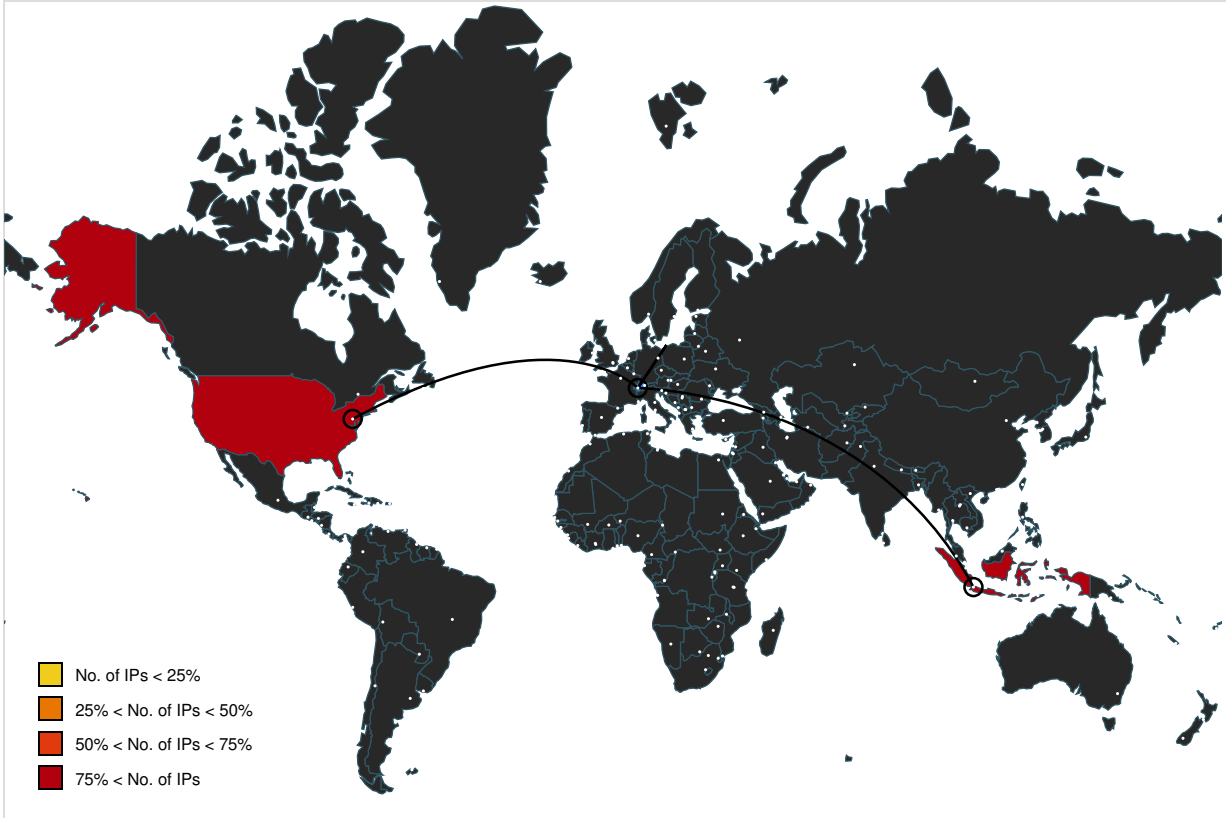
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://172.105.115.71:8080/E	regsvr32.exe, 00000006.00000003.55350441 1.00000000008E1000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.425341501.00000000008E0000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://172.105.115.71:8080/gumktuwcdwjgjgt/xmwkrc vtq/hnafdgsuhec/	regsvr32.exe, 00000006.00000003.55350441 1.00000000008E1000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.425341501.00000000008E0000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000006.00000003.425313 561.00000000008CF000.00000004.00000020.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://172.105.115.71:8080/gumktuwcdwjgjgt/xmwkrc vtq/hnafdgsuhec/T	regsvr32.exe, 00000006.00000003.55350441 1.00000000008E1000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 006.00000003.425341501.00000000008E0000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
115.178.55.22	unknown	Indonesia		38783	SIMAYA-AS-IDPTSimayaJejaringMandiriID	true
172.105.115.71	unknown	United States		63949	LINODE-APLinodeLLCUS	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	745000
Start date and time:	2022-11-13 16:53:04 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	En3ZIyuYdw.exe (renamed file extension from exe to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	17
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:	mal76.troj.evad.winDLL@21/2@0/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 58.8% (good quality ratio 53.4%) • Quality average: 60.9% • Quality standard deviation: 31.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, conhost.exe
- Excluded IPs from analysis (whitelisted): 209.197.3.8, 93.184.221.240, 40.126.31.72, 40.126.31.68, 20.190.159.1, 20.190.159.3, 40.126.31.64, 20.190.159.74, 20.190.159.5, 20.190.159.19, 20.73.194.208, 40.127.240.158
- Excluded domains from analysis (whitelisted): client.wns.windows.com, client-office365-tas.msedge.net, ocos-office365-s2s.msedge.net, wu.ec.azureedge.net, tile-service.weather.microsoft.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, cds.d2s7q6s2.hwcdn.net, wu-bg-shim.trafficmanager.net, wu.azureedge.net, login.msa.msidentity.com, www.tm.a.prd.aadg.trafficmanager.net, prda.aadg.msidentity.com, atm-settingsfe-prod-geo2.trafficmanager.net, login.live.com, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, settings-prod-weu-2.westeurope.cloudapp.azure.com, hlb.apr-52dd2-0.edgecastdns.net, settings-prod-neu-1.northeurope.cloudapp.azure.com, config.edge.skype.com, www.tm.lg.prod.aadmsa.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:54:46	API Interceptor	2x Sleep call for process: regsvr32.exe modified
16:55:00	Autostart	Run: HKLM64\Software\Microsoft\Windows\CurrentVersion\Run oSMG.dll C:\Windows\system32\regsvr32.exe "C:\Windows\system32\LkpZARPPMYxrpnAus\oSMG.dll"

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:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\regsvr32.exe
File Type:	Microsoft Cabinet archive data, Windows 2000/XP setup, 62919 bytes, 1 file, at 0x2c +A "authroot.stl", number 1, 6 datablocks, 0x1 compression
Category:	dropped
Size (bytes):	62919
Entropy (8bit):	**7.995280921994772**
Encrypted:	**true**
SSDEEP:	1536:d+OfVxHl7Wyf11IYom3xQcRVOtPHwQV4rP6Ji7:d+OxHxJlZcuPt4b6q
MD5:	3DCF580A93972319E82CAFBC047D34D5
SHA1:	8528D2A1363E5DE77DC3B1142850E51EAD0F4B6B
SHA-256:	40810E31F1B69075C727E6D557F9614D5880112895FF6F4DF1767E87AE5640D1
SHA-512:	98384BE7218340F95DAE88D1CB865F23A0B4E12855BEB6E74A3752274C9B4C601E493864DB777BCA677A370D0A9DBFFD68D94898A82014537F3A801CCE839C4
Malicious:	false
Preview:	MSCF.....,.....I.....Q.....GU.\ .authroot.stl..O..5..CK..<Tk...c_.d....A.K...+.d.-;%.BJII!.QIR..$t)Kd.-QQ*...g.....^..~|N=...y....{. .4{...W....b.i...j.I.....1:..b\.0.... .Ait.2t.....w.%.&.",tL_...4.8L[G..;.57....AT.k.....V..K.....(....mzS...G....r.".=H.?>.....x&...S%....X.M^.j...A..x.9`.9...A../.s..#.4#.....ld.w..B....s.8..(...dj....=L.)..s.d.]NxQX8 ....stV#.K.'7.tH..9u~.2..!..2./.....!..9C../...mP $..../y.....@p.6.}.`...5. 0r.w...@(.. .Q....)g.....m..z*.8rR..).].T9r<.L....0..`.....c.....;-.g..;.wk.).....i..c5....{v.u...AS..=.....&.:... .....+..P.N..9..EAQ.V.$s.....B.`.Mfe..8.....$...y-.q9J.....W...2.Q8...O.....i..@\^.=X..dG$.M..#=....m.h..{9.'...-.v..Z...!....z.....N....i..^.,.....d...%Xa~q.@D|0...Y.m..... ...&d.4..A..{t=...../.t.3._.....?-.....uroP?.d.Z..S..{...$.i....X..$.O..4..N.)....U.Z..P....X,.... ...Lg..35..W..s.!c...Ap.].P..8..M..W.....U.,...m.u..|=.m1..~..!..b...._.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	328
Entropy (8bit):	3.1108374798811247
Encrypted:	false
SSDEEP:	6:kKiN1HlNiN+SkQlPlEGYRMY9z+4KIDA3RUeKITAlWRyf1:W/kPlE99SNxAhUexYo1
MD5:	593B64510BE6E0F93F1D02E1287B59B8

SHA1:	4BB261DDE1E826957667276543C61EF316CED8A7
SHA-256:	99B77FB02312206AFEF0CFD2E6F0F64ED7BAE5AF005BFB91731A838C657DEF99
SHA-512:	01255EF7FEAF8552CEBFE56987B39E9EA8B328873EFDA6A5AC0AD3AD4E5ECCF30B379125F47B82A892A84709CE1F1624C4C29D5F586189CE930514EFDC2D009D
Malicious:	false
Preview:	p..... .....g.....(..... ....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.e.d.e.4.d.3.9.b.e.8.d.8.1.:.0."...

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	6.619217390480199
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:	En3ZlyuYdw.dll
File size:	528896
MD5:	633fd626fe5a1328fac74f20daf91f59
SHA1:	01d495949dd7e86ebdaf326da882d022d73c1d7f
SHA256:	23a872dfbba73a7f72bd24c68a0a3f5294bd0f60cab1ed0e5b2c80735fcb40ac
SHA512:	5c8e736c200d486fba5a6d12cc51f86bab4fee3c034e8fe01d71773eb3888ddb5243d7d1711aa820d65d43fa5de0a69910ada0d4387de1c2d66d7b7b1a65203b
SSDEEP:	6144:mW1239bnTe+0Qv7NSEBj43USaI6Y/jOpxHRikSYI+QALgIJ1divndEXFn:mW1e9PeexPBjvKSpuvYI+TLgs1dcEXF
TLSH:	34B4F829A59E76F0C951A1F5A0420B1595F33C88FEF68EAF03502F296F6F24425F768C
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....$...s...$.....$.....$.....`.....`.....e.h.....`.....Rich.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1800044e0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DLL
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x636D6724 [Thu Nov 10 21:03:32 2022 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:	81146e0614ccc4eb7174ad2ad695dedb

Entrypoint Preview

Instruction
dec eax
mov dword ptr [esp+08h], ebx

Instruction
dec eax
mov dword ptr [esp+10h], esi
push edi
dec eax
sub esp, 20h
dec ecx
mov edi, eax
mov ebx, edx
dec eax
mov esi, ecx
cmp edx, 01h
jne 00007F3674D4BB17h
call 00007F3674D4C0A8h
dec esp
mov eax, edi
mov edx, ebx
dec eax
mov ecx, esi
dec eax
mov ebx, dword ptr [esp+30h]
dec eax
mov esi, dword ptr [esp+38h]
dec eax
add esp, 20h
pop edi
jmp 00007F3674D4B98Ch
int3
int3
int3
inc eax
push ebx
dec eax
sub esp, 20h
dec eax
mov ebx, ecx
dec eax
mov eax, edx
dec eax
lea ecx, dword ptr [00033F0Dh]
dec eax
mov dword ptr [ebx], ecx
dec eax
lea edx, dword ptr [ebx+08h]
xor ecx, ecx
dec eax
mov dword ptr [edx], ecx
dec eax
mov dword ptr [edx+08h], ecx
dec eax
lea ecx, dword ptr [eax+08h]
call 00007F3674D4E311h
dec eax
lea eax, dword ptr [00033F1Dh]
dec eax
mov dword ptr [ebx], eax
dec eax
mov eax, ebx
dec eax
add esp, 20h

Instruction
pop ebx
ret
int3
xor eax, eax
dec eax
mov dword ptr [ecx+10h], eax
dec eax
lea eax, dword ptr [00033F13h]
dec eax
mov dword ptr [ecx+08h], eax
dec eax
lea eax, dword ptr [00033EF8h]
dec eax
mov dword ptr [ecx], eax
dec eax
mov eax, ecx
ret
int3
inc eax
push ebx
dec eax
sub esp, 20h
dec eax
mov ebx, ecx
dec eax
mov eax, edx
dec eax
lea ecx, dword ptr [00033EADh]
dec eax
mov dword ptr [ebx], ecx
dec eax
lea edx, dword ptr [ebx+08h]
xor ecx, ecx
dec eax
mov dword ptr [edx], ecx
dec eax
mov dword ptr [edx+08h], ecx
dec eax
lea ecx, dword ptr [eax+08h]

Rich Headers

Programming Language:	• [EXP] VS2015 UPD3.1 build 24215 • [RES] VS2015 UPD3 build 24213 • [LNK] VS2015 UPD3.1 build 24215

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x7cda0	0x58	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7cdf8	0x78	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x87000	0x1e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x82000	0x192c	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x88000	0x66c	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x7a410	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x7a430	0x94	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IAT	0x38000	0x370	.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	0x36fd5	0x37000	False	0.38967507102272725	data	5.930785005703424	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x38000	0x4597a	0x45a00	False	0.670532007405745	data	6.275607964984237	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x7e000	0x3394	0xc00	False	0.18294270833333334	DOS executable (block device driver \337-\231+])	2.573523630872546	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.pdata	0x82000	0x192c	0x1a00	False	0.4794170673076923	data	5.1711441720039435	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gfids	0x84000	0xdc	0x200	False	0.244140625	Spectrum .TAP data "6 " - BASIC program	1.1531659578770692	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gxfg	0x85000	0x1000	0x1000	False	0.44091796875	data	5.088628746947821	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gehcont	0x86000	0xc	0x200	False	0.0390625	data	0.06116285224115448	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x87000	0x1e0	0x200	False	0.52734375	data	4.724728911998389	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x88000	0x66c	0x800	False	0.537109375	data	4.9054360857170005	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x87060	0x17d	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	GetConsoleMode, GetConsoleOutputCP, WriteFile, FlushFileBuffers, SetStdHandle, HeapReAlloc, HeapSize, SetFilePointerEx, ExitProcess, GetStdHandle, GetProcessHeap, CreateFileW, CloseHandle, GetStringTypeW, LCMapStringW, GetFileType, VirtualAlloc, RtlCaptureContext, RtlLookupFunctionEntry, RtlVirtualUnwind, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetCurrentProcess, TerminateProcess, IsProcessorFeaturePresent, IsDebuggerPresent, GetStartupInfoW, GetModuleHandleW, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, RtlPcToFileHeader, EncodePointer, RaiseException, RtlUnwindEx, InterlockedFlushSList, GetLastError, SetLastError, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, GetProcAddress, LoadLibraryExW, GetModuleHandleExW, GetModuleFileNameW, HeapFree, HeapAlloc, FindClose, FindFirstFileExW, FindNextFileW, IsValidCodePage, GetACP, GetOEMCP, GetCPInfo, GetCommandLineA, GetCommandLineW, MultiByteToWideChar, WideCharToMultiByte, GetEnvironmentStringsW, FreeEnvironmentStringsW, FlsAlloc, FlsGetValue, FlsSetValue, FlsFree, WriteConsoleW
USER32.dll	EndPaint, BeginPaint, InvalidateRect, GetMessageW, DefWindowProcW, CloseTouchInputHandle, GetTouchInputInfo, DestroyWindow, MessageBoxW, CreateWindowExW, RegisterClassExW, LoadStringW, ShowWindow, DispatchMessageW, RegisterTouchWindow, MessageBoxA, UnregisterTouchWindow, TranslateAcceleratorW, TranslateMessage, LoadCursorW, PostQuitMessage, UpdateWindow
GDI32.dll	Polyline, LineTo, CreatePen, MoveToEx, DeleteObject, SelectObject
ole32.dll	CoUninitialize, CoCreateInstance, CoInitialize
CRYPT32.dll	CryptStringToBinaryA

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x180013f70

Possible Origin

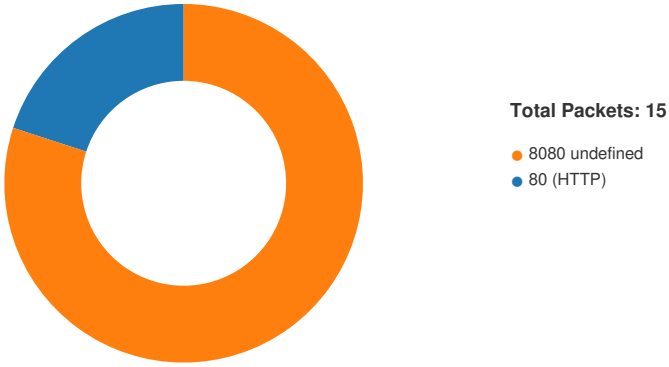
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5115.178.55.22 49700802404304 11/13/22-16:54:45.127001	TCP	2404304	ET CNC Feodo Tracker Reported CnC Server TCP group 3	49700	80	192.168.2.5	115.178.55.22

Network Port Distribution



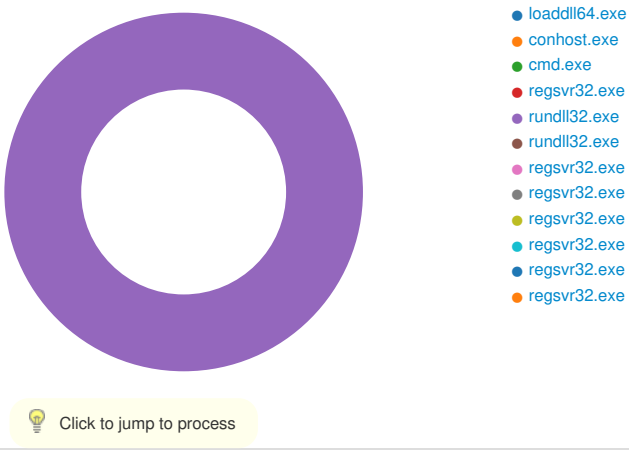
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 13, 2022 16:54:45.127001047 CET	49700	80	192.168.2.5	115.178.55.22
Nov 13, 2022 16:54:45.421077967 CET	80	49700	115.178.55.22	192.168.2.5
Nov 13, 2022 16:54:45.925299883 CET	49700	80	192.168.2.5	115.178.55.22
Nov 13, 2022 16:54:46.218974113 CET	80	49700	115.178.55.22	192.168.2.5
Nov 13, 2022 16:54:46.722256899 CET	49700	80	192.168.2.5	115.178.55.22
Nov 13, 2022 16:54:47.016133070 CET	80	49700	115.178.55.22	192.168.2.5
Nov 13, 2022 16:54:52.532732964 CET	49708	8080	192.168.2.5	172.105.115.71
Nov 13, 2022 16:54:52.705895901 CET	8080	49708	172.105.115.71	192.168.2.5
Nov 13, 2022 16:54:52.706121922 CET	49708	8080	192.168.2.5	172.105.115.71
Nov 13, 2022 16:54:52.750550032 CET	49708	8080	192.168.2.5	172.105.115.71
Nov 13, 2022 16:54:52.923871994 CET	8080	49708	172.105.115.71	192.168.2.5
Nov 13, 2022 16:54:52.941482067 CET	8080	49708	172.105.115.71	192.168.2.5
Nov 13, 2022 16:54:52.941518068 CET	8080	49708	172.105.115.71	192.168.2.5
Nov 13, 2022 16:54:52.941677094 CET	49708	8080	192.168.2.5	172.105.115.71
Nov 13, 2022 16:54:53.351596117 CET	49708	8080	192.168.2.5	172.105.115.71
Nov 13, 2022 16:54:53.525042057 CET	8080	49708	172.105.115.71	192.168.2.5
Nov 13, 2022 16:54:53.525784016 CET	8080	49708	172.105.115.71	192.168.2.5
Nov 13, 2022 16:54:53.566596985 CET	49708	8080	192.168.2.5	172.105.115.71
Nov 13, 2022 16:54:58.280989885 CET	49708	8080	192.168.2.5	172.105.115.71
Nov 13, 2022 16:54:58.281066895 CET	49708	8080	192.168.2.5	172.105.115.71

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 13, 2022 16:54:58.454478025 CET	8080	49708	172.105.115.71	192.168.2.5
Nov 13, 2022 16:54:58.454504967 CET	8080	49708	172.105.115.71	192.168.2.5
Nov 13, 2022 16:54:59.080671072 CET	8080	49708	172.105.115.71	192.168.2.5
Nov 13, 2022 16:54:59.161001921 CET	49708	8080	192.168.2.5	172.105.115.71
Nov 13, 2022 16:55:02.089238882 CET	8080	49708	172.105.115.71	192.168.2.5
Nov 13, 2022 16:55:02.089268923 CET	8080	49708	172.105.115.71	192.168.2.5
Nov 13, 2022 16:55:02.089543104 CET	49708	8080	192.168.2.5	172.105.115.71
Nov 13, 2022 16:55:02.089946985 CET	49708	8080	192.168.2.5	172.105.115.71
Nov 13, 2022 16:55:02.090179920 CET	49708	8080	192.168.2.5	172.105.115.71
Nov 13, 2022 16:55:02.264749050 CET	8080	49708	172.105.115.71	192.168.2.5
Nov 13, 2022 16:55:02.264775038 CET	8080	49708	172.105.115.71	192.168.2.5

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: 4348, Parent PID: 3324

General

Target ID:	0
Start time:	16:53:58
Start date:	13/11/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\En3ZIyuYdw.dll"
Imagebase:	0x7ff62f8a0000
File size:	139776 bytes
MD5 hash:	C676FC0263EDD17D4CE7D644B8F3FCD6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.318758650.000001E98A250000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.318571770.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **860**, Parent PID: **4348**

General

Target ID:	1
Start time:	16:53:58
Start date:	13/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **3752**, Parent PID: **4348**

General

Target ID:	2
Start time:	16:53:59
Start date:	13/11/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\En3ZIyuYdw.dll",#1
Imagebase:	0x7ff627730000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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: **4992**, Parent PID: **4348**

General

Target ID:	3
Start time:	16:53:59
Start date:	13/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\En3ZIyuYdw.dll
Imagebase:	0x7ff7f13b0000

File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.313082839.0000000001280000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.313769828.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **5860**, Parent PID: **3752**

General

Target ID:	4
Start time:	16:53:59
Start date:	13/11/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\En3ZlyuYdw.dll",#1
Imagebase:	0x7ff6e65e0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.311727072.000001E4C44E0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.310244277.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\System32\LkpZARPPMYxrpnAus\oSMG.dll:Zone.Identifier	success or wait	1	180020786	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **5040**, Parent PID: **4348**

General

Target ID:	5
Start time:	16:53:59
Start date:	13/11/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false

Commandline:	rundll32.exe C:\Users\user\Desktop\En3ZIyuYdw.dll,DllRegisterServer
Imagebase:	0x7ff6e65e0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.310936367.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.311118162.0000020D28BC0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **4180**, Parent PID: **5860**

General

Target ID:	6
Start time:	16:54:04
Start date:	13/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\LkpZARPPMYxrpnAus\oSMG.dll"
Imagebase:	0x7ff7f13b0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **6052**, Parent PID: **5040**

General

Target ID:	7
Start time:	16:54:04
Start date:	13/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\QkeveKELwVTlid\eYjpj.dll"
Imagebase:	0x7ff7f13b0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: regsvr32.exe PID: 6056, Parent PID: 4992

General

Target ID:	8
Start time:	16:54:04
Start date:	13/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\CVFdhpNOtsemq\TpsMttdDUpxciwO.dll"
Imagebase:	0x7ff7f13b0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: regsvr32.exe PID: 64, Parent PID: 4348

General

Target ID:	9
Start time:	16:54:08
Start date:	13/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\Alnqcua\qiwFWDzKBdg.dll"
Imagebase:	0x7ff7f13b0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

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: regsvr32.exe PID: 6112, Parent PID: 3324

General

Target ID:	14
Start time:	16:55:08
Start date:	13/11/2022

Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe" "C:\Windows\system32\LkpZARPPMYxrpnAus\oSMG.dll
Imagebase:	0x7ff7f13b0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.462452546.0000000000640000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000E.00000002.463594839.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **712**, Parent PID: **6112**

General

Target ID:	15
Start time:	16:55:15
Start date:	13/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Users\user\AppData\Local\RGgdaHRy\SOHUjYiDXi.dll"
Imagebase:	0x7ff7f13b0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly