ID: 384980
Sample Name: zeD11Fztx8
Cookbook: default.jbs
Time: 18:47:04
Date: 10/04/2021
Version: 31.0.0 Emerald

Table of Contents

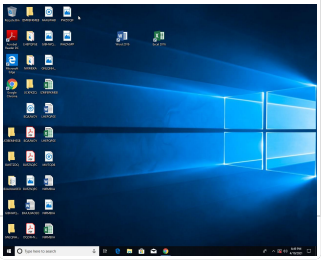
Analysis Report zeD11Fztx8

Overview

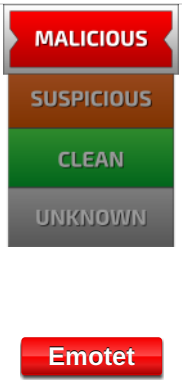
General Information

Sample Name:	zeD11Fztx8 (renamed file extension from none to exe)
Analysis ID:	384980
MD5:	ecbc4b40dcfec4e..
SHA1:	e08eb07c69d8fc8..
SHA256:	878d5137e0c9a0..
Infos:	

Most interesting Screenshot:



Detection

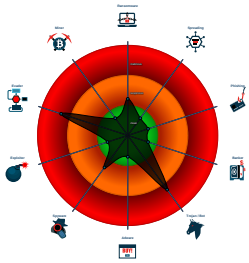


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Yara detected Emotet
- Drops executables to the windows d…
- Found evasive API chain (may stop…
- Hides that the sample has been dow…
- Machine Learning detection for samp…
- Contains capabilities to detect virtua…
- Contains functionality to dynamically…
- Contains functionality to read the PEB

Classification



Startup

- **System is w10x64**
- zeD11Fztx8.exe (PID: 6720 cmdline: 'C:\Users\user\Desktop\zeD11Fztx8.exe' MD5: ECBC4B40DCFEC4ED1B2647B217DA0441)
  - zeD11Fztx8.exe (PID: 6728 cmdline: C:\Users\user\Desktop\zeD11Fztx8.exe MD5: ECBC4B40DCFEC4ED1B2647B217DA0441)
- storageservice.exe (PID: 6812 cmdline: C:\Windows\SysWOW64\storageservice.exe MD5: ECBC4B40DCFEC4ED1B2647B217DA0441)
  - storageservice.exe (PID: 6828 cmdline: C:\Windows\SysWOW64\storageservice.exe MD5: ECBC4B40DCFEC4ED1B2647B217DA0441)
- svchost.exe (PID: 4800 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5688 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6352 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
zeD11Fztx8.exe	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
zeD11Fztx8.exe	Emotet	Emotet Payload	kevoreilly	• 0x16f0:$snippet1: FF 15 F8 C1 40 00 83 C4 0C 68 40 00 00 F0 6A 18 • 0x1732:$snippet2: 6A 13 68 01 00 01 00 FF 15 C4 C0 40 00 85 C0

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.640361081.0000000001381000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000000.00000002.633596595.0000000001381000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000000.638984509.0000000001381000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000001.00000000.633157257.0000000001381000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000003.00000000.639793428.0000000001381000.00000020.00020000.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 3 entries				

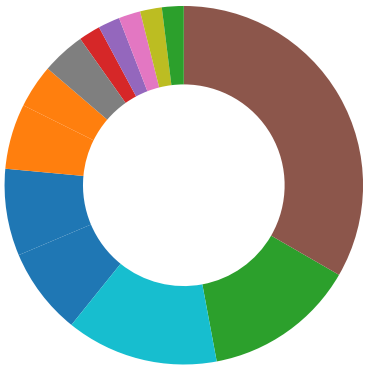
Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.storageservice.exe.1380000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
3.2.storageservice.exe.1380000.0.unpack	Emotet	Emotet Payload	kevoreilly	• 0x16f0:$snippet1: FF 15 F8 C1 38 01 83 C4 0C 68 40 00 00 F0 6A 18 • 0x1732:$snippet2: 6A 13 68 01 00 01 00 FF 15 C4 C0 38 01 85 C0
1.2.zeD11Fztx8.exe.1380000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
1.2.zeD11Fztx8.exe.1380000.0.unpack	Emotet	Emotet Payload	kevoreilly	• 0x16f0:$snippet1: FF 15 F8 C1 38 01 83 C4 0C 68 40 00 00 F0 6A 18 • 0x1732:$snippet2: 6A 13 68 01 00 01 00 FF 15 C4 C0 38 01 85 C0
3.0.storageservice.exe.1380000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 11 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- Language, Device and Operating System Detection
- Stealing of Sensitive Information

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

E-Banking Fraud:

Yara detected Emotet

System Summary:

Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior:

Drops executables to the windows directory (C:\Windows) and starts them

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Found evasive API chain (may stop execution after checking mutex)

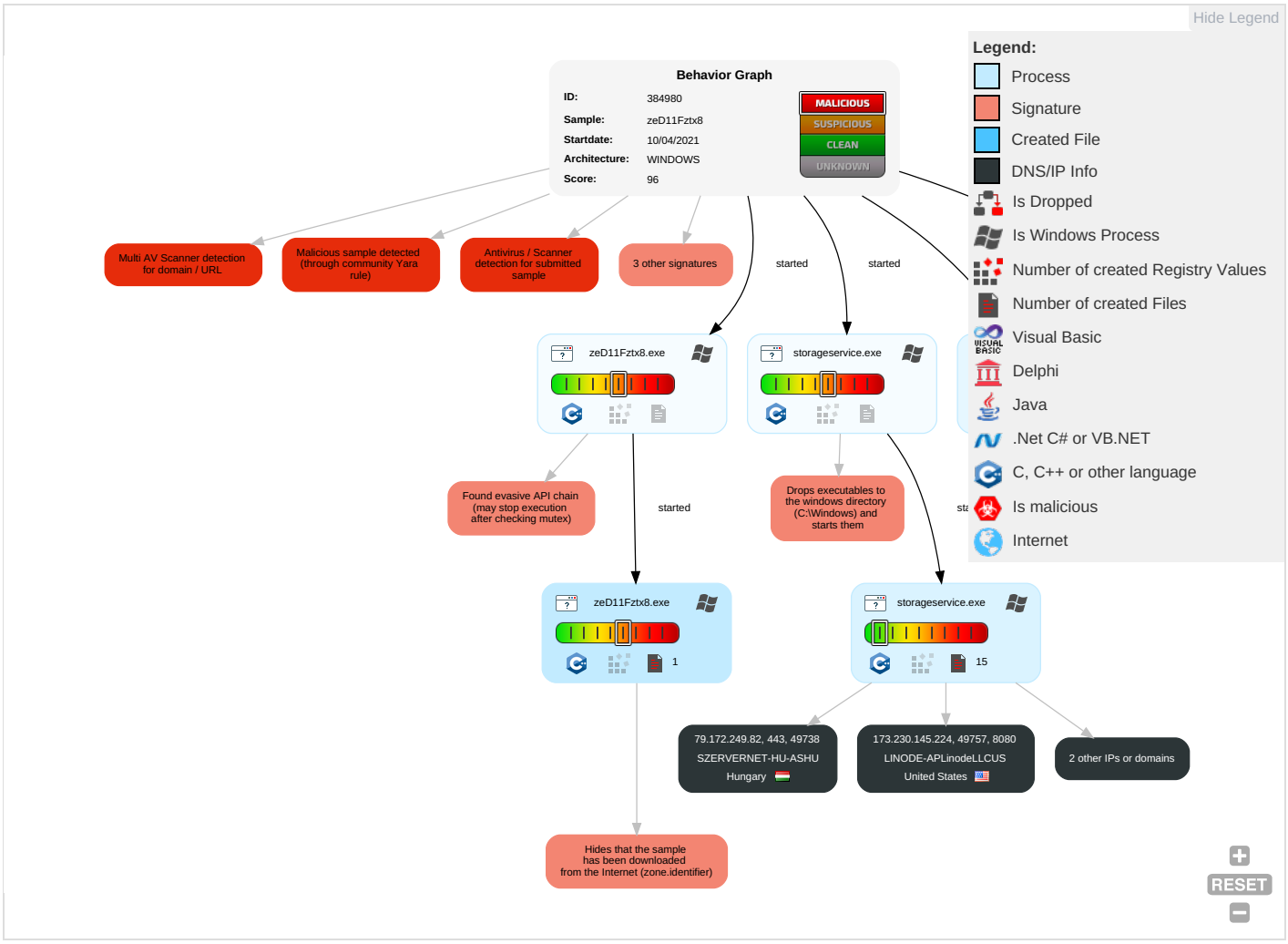
Stealing of Sensitive Information:

Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Native API 1 1	Path Interception	Process Injection 1	Masquerading 1 2	Input Capture 1	Security Software Discovery 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop on Insecure Network Communication	Remote Track D Without Authoriz
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 to Redirect Phone Calls/SMS	Remote Wipe Da Without Authoriz
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backup
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Hidden Files and Directories 1	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	File Deletion 1	LSA Secrets	System Information Discovery 1 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

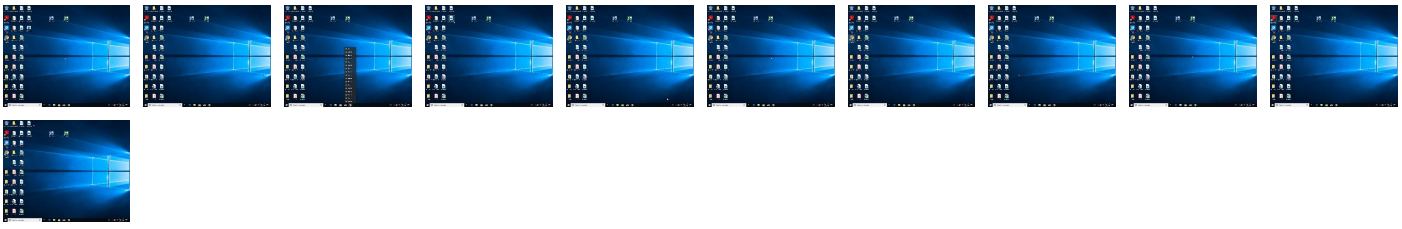
Behavior Graph



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
zeD11Fztx8.exe	83%	Virustotal		Browse
zeD11Fztx8.exe	97%	ReversingLabs	Win32.Trojan.Emotet	
zeD11Fztx8.exe	100%	Avira	TR/Crypt.XPACK.Gen	
zeD11Fztx8.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.storageservice.exe.1380000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.storageservice.exe.1380000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.zeD11Fztx8.exe.1380000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.zeD11Fztx8.exe.1380000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.storageservice.exe.1380000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.zeD11Fztx8.exe.1380000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.storageservice.exe.1380000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.zeD11Fztx8.exe.1380000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://173.230.145.224:8080/	6%	Virustotal		Browse
http://173.230.145.224:8080/	0%	Avira URL Cloud	safe	
http://173.230.145.224:8080/gP	0%	Avira URL Cloud	safe	
http://80.86.91.232:7080/	6%	Virustotal		Browse
http://80.86.91.232:7080/	0%	Avira URL Cloud	safe	
http://80.86.91.232:7080/h	0%	Avira URL Cloud	safe	
http://80.86.91.232:7080/G	0%	Avira URL Cloud	safe	
http://https://79.172.249.82:443/	0%	Avira URL Cloud	safe	
http://193.169.54.12:8080/	0%	Avira URL Cloud	safe	
http://79.172.249.82:443/$	0%	Avira URL Cloud	safe	
http://80.86.91.232:7080/24	0%	Avira URL Cloud	safe	
http://80.86.91.232:7080/ed	0%	Avira URL Cloud	safe	
http://80.86.91.232:7080/7	0%	Avira URL Cloud	safe	
http://79.172.249.82:443/	0%	Avira URL Cloud	safe	
http://80.86.91.232:7080/9.54.12:8080/;	0%	Avira URL Cloud	safe	
http://173.230.145.224:8080/m	0%	Avira URL Cloud	safe	
http://193.169.54.12:8080//	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

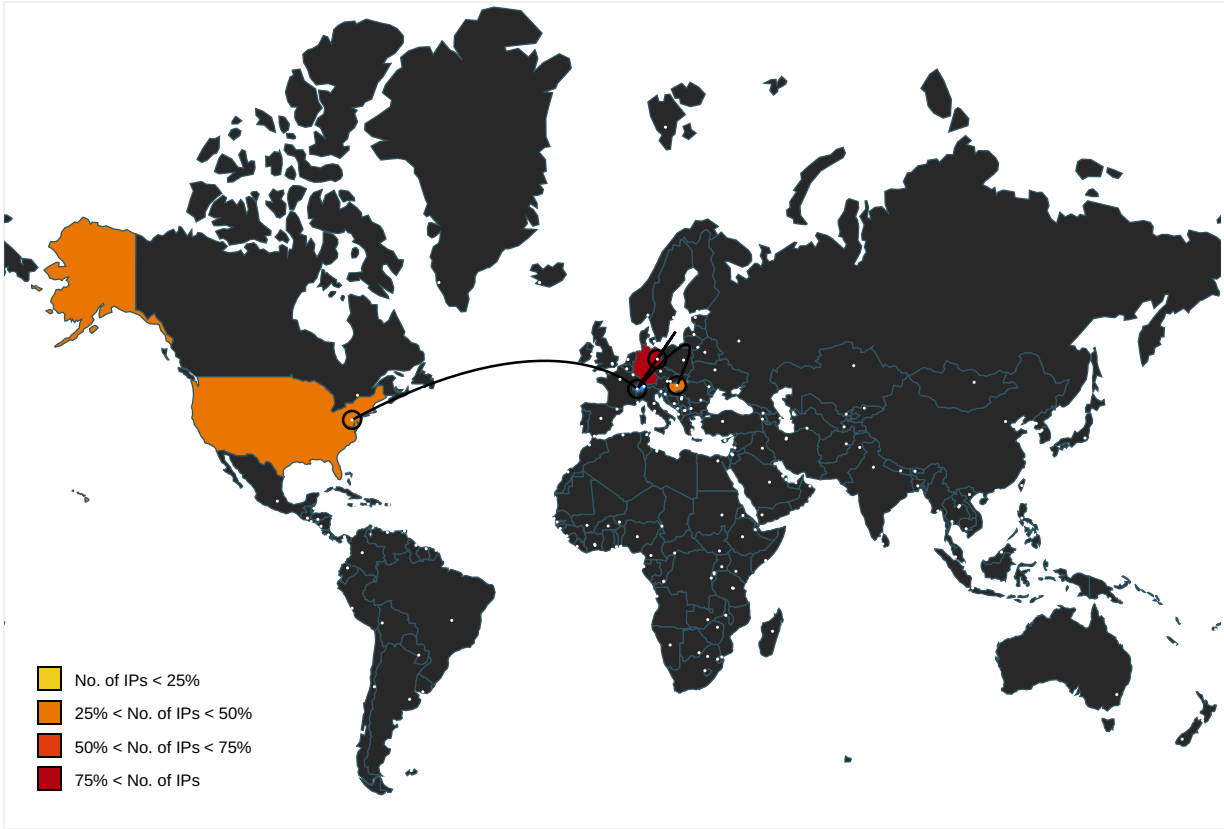
Name	Malicious	Antivirus Detection	Reputation
http://https://79.172.249.82:443/	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://173.230.145.224:8080/	storageservice.exe, 00000003.00000002.898823671.000000000105A000.00000004.00000020.sdmp	true	• 6%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://173.230.145.224:8080/gP	storageservice.exe, 00000003.00000002.898823671.000000000105A000.00000004.00000020.sdmp	true	• Avira URL Cloud: safe	unknown
http://80.86.91.232:7080/	storageservice.exe, 00000003.00000002.898823671.000000000105A000.00000004.00000020.sdmp	false	• 6%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://80.86.91.232:7080/h	storageservice.exe, 00000003.00000002.898823671.000000000105A000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://80.86.91.232:7080/G	storageservice.exe, 00000003.00000002.898823671.000000000105A000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://193.169.54.12:8080/	storageservice.exe, 00000003.00000002.898823671.000000000105A000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://79.172.249.82:443/$	storageservice.exe, 00000003.00000002.898800934.0000000001048000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://80.86.91.232:7080/24	storageservice.exe, 00000003.00000002.898823671.000000000105A000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://80.86.91.232:7080/ed	storageservice.exe, 00000003.00000002.898823671.000000000105A000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://80.86.91.232:7080/7	storageservice.exe, 00000003.00000002.898823671.000000000105A000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://79.172.249.82:443/	storageservice.exe, 00000003.00000002.898800934.0000000001048000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://80.86.91.232:7080/9.54.12:8080/;	storageservice.exe, 00000003.00000002.898823671.000000000105A000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://173.230.145.224:8080/m	storageservice.exe, 00000003.00000002.898823671.000000000105A000.00000004.00000020.sdmp	true	• Avira URL Cloud: safe	unknown
http://193.169.54.12:8080//	storageservice.exe, 00000003.00000002.898823671.000000000105A000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.169.54.12	unknown	Germany		49464	ICFSYSTEMSDE	false
80.86.91.232	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	false
173.230.145.224	unknown	United States		63949	LINODE-APLinodeLLCUS	false
79.172.249.82	unknown	Hungary		43711	SZERVERNET-HU-ASHU	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	384980
Start date:	10.04.2021
Start time:	18:47:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 46s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	zeD11Fztx8 (renamed file extension from none to 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:	22
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:	mal96.troj.evad.winEXE@9/0@0/4
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 42.7% (good quality ratio 39%) • Quality average: 79% • Quality standard deviation: 30.4%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
193.169.54.12	_01_.doc	Get hash	malicious	Browse	• 193.169.54.12:8080/
	hEHN0WzBF.exe	Get hash	malicious	Browse	• 193.169.54.12:8080/
	Outstanding Invoices.doc	Get hash	malicious	Browse	• 193.169.54.12:8080/
	Outstanding Invoices.doc	Get hash	malicious	Browse	• 193.169.54.12:8080/
	http://baseballpontedipiave.com/Sales-Invoice/	Get hash	malicious	Browse	• 193.169.54.12:8080/
	emotet2.doc	Get hash	malicious	Browse	• 193.169.54.12:8080/
	20180212-20_46_01_.doc	Get hash	malicious	Browse	• 193.169.54.12:8080/
	http://www.yourhabitchangecoach.co.uk/wp-content/Overdue-payment/	Get hash	malicious	Browse	• 193.169.54.12:8080/
	SalesInvoice.doc	Get hash	malicious	Browse	• 193.169.54.12:8080/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SalesInvoice.doc	Get hash	malicious	Browse	• 193.169.54.12:8080/
	mj03dyvx_2076767.exe	Get hash	malicious	Browse	• 193.169.54.12:8080/
	Scan1782384.doc	Get hash	malicious	Browse	• 193.169.54.12:8080/
	Scan1782384.doc	Get hash	malicious	Browse	• 193.169.54.12:8080/
	RDuYHvb2jQ.exe	Get hash	malicious	Browse	• 193.169.54.12:8080/
	Outstanding Invoices.doc	Get hash	malicious	Browse	• 193.169.54.12:8080/
	Outstanding Invoices.doc	Get hash	malicious	Browse	• 193.169.54.12:8080/
	http://okomekai.symphonic-net.com/Invoice-69070770/	Get hash	malicious	Browse	• 193.169.54.12:8080/
	Outstanding invoice.doc	Get hash	malicious	Browse	• 193.169.54.12:8080/
	Outstanding invoice.doc	Get hash	malicious	Browse	• 193.169.54.12:8080/
	mail.rodolfogvalencia.com/Invoice/	Get hash	malicious	Browse	• 193.169.54.12:8080/
80.86.91.232	Invoice.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Overdue payment.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Emotet.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Outstanding Invoices.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Outstanding Invoices.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Emote.exe	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Question.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	emotet.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Paypal.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Paypal.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	emotet.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	emotet.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	960-27-621120-257 & 960-27-621120-969.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Rechnung.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	Open invoices.doc	Get hash	malicious	Browse	• 80.86.91.232:4143/
	20180212-20_46_01_.doc	Get hash	malicious	Browse	• 80.86.91.232:7080/
	SalesInvoice.doc	Get hash	malicious	Browse	• 80.86.91.232:7080/
	SalesInvoice.doc	Get hash	malicious	Browse	• 80.86.91.232:7080/
	mj03dyvx_2076767.exe	Get hash	malicious	Browse	• 80.86.91.232:7080/
	Scan1782384.doc	Get hash	malicious	Browse	• 80.86.91.232:7080/

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GD-EMEA-DC-SXB1DE	TRS-11-0221-020.exe	Get hash	malicious	Browse	• 85.25.177.199
	Payment Advice.exe	Get hash	malicious	Browse	• 85.25.177.199

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	VMtEguRH.exe	Get hash	malicious	Browse	• 85.25.177.199
	Reports-018315.xlsm	Get hash	malicious	Browse	• 185.21.102.197
	Reports-018315.xlsm	Get hash	malicious	Browse	• 185.21.102.197
	D12547698.VBS	Get hash	malicious	Browse	• 85.25.93.141
	sample.exe.exe	Get hash	malicious	Browse	• 80.86.91.232
	5zc9vbGBo3.exe	Get hash	malicious	Browse	• 217.172.179.54
	InnAcjnAmG.exe	Get hash	malicious	Browse	• 217.172.179.54
	yxghUyIGb4.exe	Get hash	malicious	Browse	• 80.86.91.232
	TaTYytHaBk.exe	Get hash	malicious	Browse	• 85.25.43.31
	8X93Tzvd7V.exe	Get hash	malicious	Browse	• 217.172.179.54
	u8A8Qy5S7O.exe	Get hash	malicious	Browse	• 217.172.179.54
	SecuriteInfo.com.Mal.GandCrypt-A.24654.exe	Get hash	malicious	Browse	• 217.172.179.54
	SecuriteInfo.com.Mal.GandCrypt-A.5674.exe	Get hash	malicious	Browse	• 217.172.179.54
	csrss.bin.exe	Get hash	malicious	Browse	• 188.138.33.233
	yx8DBT3r5r.exe	Get hash	malicious	Browse	• 92.51.129.66
	E00636067E.exe	Get hash	malicious	Browse	• 85.25.177.199
	http___contributeindustry.com_js_engine-rawbin.exe	Get hash	malicious	Browse	• 85.25.177.199
	z2xQEFs54b.exe	Get hash	malicious	Browse	• 87.230.93.218
ICFSYSTEMSDE	9fdUNaHzLv.exe	Get hash	malicious	Browse	• 193.169.54.12
	sample.exe.exe	Get hash	malicious	Browse	• 193.169.54.12
	yxghUyIGb4.exe	Get hash	malicious	Browse	• 193.169.54.12
	0HvIGwMmBV.exe	Get hash	malicious	Browse	• 193.169.54.12
	pitEBNziGR.exe	Get hash	malicious	Browse	• 193.169.54.12
	_01_.doc	Get hash	malicious	Browse	• 193.169.54.12
	hEHN0WzBF.exe	Get hash	malicious	Browse	• 193.169.54.12
	Outstanding Invoices.doc	Get hash	malicious	Browse	• 193.169.54.12
	Outstanding Invoices.doc	Get hash	malicious	Browse	• 193.169.54.12
	http://baseballpontedipiave.com/Sales-Invoice/	Get hash	malicious	Browse	• 193.169.54.12
	emotet2.doc	Get hash	malicious	Browse	• 193.169.54.12
	20180212-20_46_01_.doc	Get hash	malicious	Browse	• 193.169.54.12
	http://www.yourhabitchangecoach.co.uk/wp-content/Overdue-payment/	Get hash	malicious	Browse	• 193.169.54.12
	SalesInvoice.doc	Get hash	malicious	Browse	• 193.169.54.12
	SalesInvoice.doc	Get hash	malicious	Browse	• 193.169.54.12
	mj03dyvx_2076767.exe	Get hash	malicious	Browse	• 193.169.54.12
	Scan1782384.doc	Get hash	malicious	Browse	• 193.169.54.12
	Scan1782384.doc	Get hash	malicious	Browse	• 193.169.54.12
	RDuYHvb2jQ.exe	Get hash	malicious	Browse	• 193.169.54.12
	Outstanding Invoices.doc	Get hash	malicious	Browse	• 193.169.54.12
LINODE-APLinodeLLCUS	CNTR-NO-GLDU7267089.xlsx	Get hash	malicious	Browse	• 45.56.127.45
	gunzipped.exe	Get hash	malicious	Browse	• 45.56.119.148
	frox0cheats.exe	Get hash	malicious	Browse	• 176.58.123.25
	nDHV6wKWHF.exe	Get hash	malicious	Browse	• 172.104.164.58
	OfficeConsultPlugin.exe	Get hash	malicious	Browse	• 109.237.24.104
	RFQ#798606.exe	Get hash	malicious	Browse	• 45.56.119.148
	Private doc.docm	Get hash	malicious	Browse	• 109.237.24.104
	lK8vF3n2e7.exe	Get hash	malicious	Browse	• 172.104.233.225
	newordermx.exe	Get hash	malicious	Browse	• 45.33.2.79
	sample.exe	Get hash	malicious	Browse	• 66.228.32.51
	BnJvVt951o.exe	Get hash	malicious	Browse	• 45.33.54.74
	BnJvVt951o.exe	Get hash	malicious	Browse	• 45.33.54.74
	SMtbg7yHyR.exe	Get hash	malicious	Browse	• 45.33.54.74
	9fdUNaHzLv.exe	Get hash	malicious	Browse	• 173.230.145.224
	Private doc.docm	Get hash	malicious	Browse	• 212.71.251.238
	invoice_document.docm	Get hash	malicious	Browse	• 212.71.251.238
	sample.exe.exe	Get hash	malicious	Browse	• 173.230.145.224
	Document_Opener.exe.14.exe	Get hash	malicious	Browse	• 88.80.186.210
	Audio playback (7656) for joew Camrosa.htm	Get hash	malicious	Browse	• 192.81.132.201
	Paymonth invoice.exe	Get hash	malicious	Browse	• 45.79.19.196

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.436116781781946
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	zeD11Fztx8.exe
File size:	45568
MD5:	ecbc4b40dcfec4ed1b2647b217da0441
SHA1:	e08eb07c69d8fc8e75927597767288a21d6ed7f6
SHA256:	878d5137e0c9a072c83c596b4e80f2aa52a8580ef214e5b a0d59daa5036a92f8
SHA512:	3ec4de3f35e10c874916a6402004e3b9fc60b5a026d2010 0ede992b592fe396db2bee0b225ab5f2fb85561f687a8abf 0c9e7c8b3cf0344c384c80297278be7b5
SSDEEP:	768:uhBY2Tumxi0mv/LWT3uBoGMUslwORSSrUBqvW zNQRC1s:ABxT6jW7uBgyOvWS
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....R..h...h...h.....h...i...h.....h.....h.Rich..h.....PE..L...7.]Z.....@

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x409ee0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5A5DA737 [Tue Jan 16 07:18:15 2018 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	4cfe8bbfb0ca5b84bbad08b043ea0c87

General

Entrypoint Preview

Instruction
push esi
push 0040C1F0h
push 3966646Ch
push 00000009h
mov ecx, D22E2014h
call 00007F2560F1290Eh
mov edx, 004011F0h
mov ecx, eax
call 00007F2560F12832h
add esp, 0Ch
mov ecx, 8F7EE672h
push 0040C0D0h
push 6677A1D2h
push 00000048h
call 00007F2560F128E9h
mov edx, 004010D0h
mov ecx, eax
call 00007F2560F1280Dh
add esp, 0Ch
push 08000000h
push 00000000h
call dword ptr [0040C1A8h]
push eax
call dword ptr [0040C10Ch]
mov esi, eax
test esi, esi
je 00007F2560F1AC48h
push 08000000h
push 00000000h
push esi
call dword ptr [0040C1F8h]
add esp, 0Ch
push esi
push 00000000h
call dword ptr [0040C1A8h]
push eax
call dword ptr [0040C1E8h]
call 00007F2560F1226Ah
push 00000000h
call dword ptr [0040C1ACh]
pop esi
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
sub esp, 0Ch
push ebx
push esi
push edi

Instruction
mov edi, edx
mov dword ptr [ebp-0Ch], ecx
mov esi, 00000001h
mov dword ptr [ebp-08h], esi
mov eax, dword ptr [edi]
cmp eax, 7Fh
jbe 00007F2560F1AC31h
lea ecx, dword ptr [ecx+00h]
shr eax, 07h
inc esi
cmp eax, 7Fh

Rich Headers

Programming Language:	• [LNK] VS2013 UPD4 build 31101 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbad0	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd000	0x5cc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0xb000	0x8	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

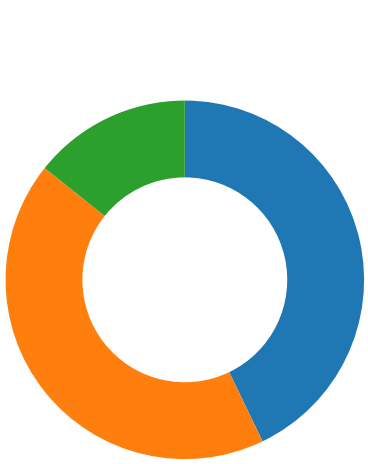
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x9883	0x9a00	False	0.503297483766	data	6.45508103349	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xb000	0xb2e	0xc00	False	0.160807291667	data	4.23495809712	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xc000	0xbd8	0x200	False	0.123046875	data	0.91267432928	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.reloc	0xd000	0x5cc	0x600	False	0.8671875	data	6.49434732961	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.dll	WTSGetActiveConsoleSessionId

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 10, 2021 18:47:54.465001106 CEST	49738	443	192.168.2.4	79.172.249.82
Apr 10, 2021 18:47:54.500535011 CEST	443	49738	79.172.249.82	192.168.2.4
Apr 10, 2021 18:47:54.500761032 CEST	49738	443	192.168.2.4	79.172.249.82
Apr 10, 2021 18:47:54.501919985 CEST	49738	443	192.168.2.4	79.172.249.82
Apr 10, 2021 18:47:54.537208080 CEST	443	49738	79.172.249.82	192.168.2.4
Apr 10, 2021 18:47:54.537532091 CEST	443	49738	79.172.249.82	192.168.2.4
Apr 10, 2021 18:47:54.537558079 CEST	443	49738	79.172.249.82	192.168.2.4
Apr 10, 2021 18:47:54.537693977 CEST	49738	443	192.168.2.4	79.172.249.82
Apr 10, 2021 18:47:54.537740946 CEST	49738	443	192.168.2.4	79.172.249.82
Apr 10, 2021 18:47:54.537854910 CEST	49738	443	192.168.2.4	79.172.249.82
Apr 10, 2021 18:47:54.573343992 CEST	443	49738	79.172.249.82	192.168.2.4
Apr 10, 2021 18:48:24.935547113 CEST	49746	8080	192.168.2.4	193.169.54.12
Apr 10, 2021 18:48:27.960725069 CEST	49746	8080	192.168.2.4	193.169.54.12
Apr 10, 2021 18:48:33.976751089 CEST	49746	8080	192.168.2.4	193.169.54.12
Apr 10, 2021 18:49:17.192873955 CEST	49757	8080	192.168.2.4	173.230.145.224
Apr 10, 2021 18:49:17.364305019 CEST	8080	49757	173.230.145.224	192.168.2.4
Apr 10, 2021 18:49:17.870801926 CEST	49757	8080	192.168.2.4	173.230.145.224
Apr 10, 2021 18:49:18.042294979 CEST	8080	49757	173.230.145.224	192.168.2.4
Apr 10, 2021 18:49:18.542711973 CEST	49757	8080	192.168.2.4	173.230.145.224
Apr 10, 2021 18:49:18.714617968 CEST	8080	49757	173.230.145.224	192.168.2.4
Apr 10, 2021 18:49:48.950465918 CEST	49763	7080	192.168.2.4	80.86.91.232
Apr 10, 2021 18:49:51.951813936 CEST	49763	7080	192.168.2.4	80.86.91.232

HTTP Request Dependency Graph

- 79.172.249.82:443

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49738	79.172.249.82	443	C:\Windows\SysWOW64\storageservice.exe

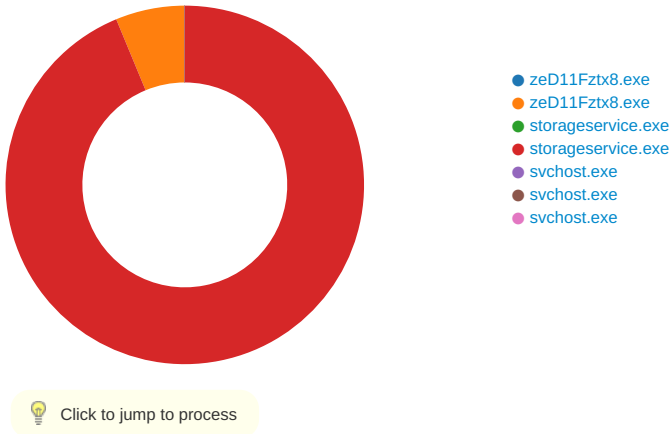
Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 10, 2021 18:47:54.501919985 CEST	284	OUT	POST / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: 79.172.249.82:443 Content-Length: 468 Connection: Keep-Alive Cache-Control: no-cache Data Raw: 77 ee 51 67 a8 c2 dc 38 20 bc 12 53 17 05 a1 e7 44 fa 23 2e b7 b8 71 13 ca 5f 34 cb 7d 0c be 09 5f d9 5a 5d 85 11 56 95 de d3 de 12 62 eb a8 08 e0 25 70 14 f1 93 c1 00 4a d5 23 a5 0e 77 2e d9 75 a6 89 1b 16 5a c1 dd 31 ce 32 df 13 a0 62 81 87 92 a5 75 31 ed 00 f4 09 08 7f ae 0e 3e f8 65 d0 b5 42 c2 d2 95 50 fe 33 48 54 55 da 3f 44 b3 df eb cb 47 92 31 e0 5c 2c 4d 46 89 f3 f7 e8 28 63 c8 8b 2d 43 6c f6 74 39 33 7f 21 86 82 16 e9 af 01 09 96 57 45 d8 63 20 47 a2 c1 62 3c 2d 74 bb 9d 73 46 51 ff 00 e2 16 99 bd 8a 96 75 c0 cc 9b 6b c8 76 2f 7d 1f 55 df 13 a3 4e 79 3d 0a 7d c1 09 f3 25 b0 1a 81 32 06 db 60 eb aa f9 77 7f 4f d5 65 00 d6 0f 40 ae d6 80 7d 6d d3 ee 85 09 f6 22 03 2f 33 e5 8b 34 8b db c6 73 67 06 01 9b 17 0a 4e 5b 3c f2 f3 aa 73 a9 cd 5f 3c 34 db da c3 54 41 f5 ea 56 26 df 67 5a 61 72 63 60 16 79 a7 db e1 af f6 2f 66 31 e2 88 4f 2d b7 94 7e cd ce 96 27 93 d4 79 59 88 98 23 46 23 99 b4 91 75 8e c1 dc 3b dd db f3 c3 0e 36 95 96 a2 94 42 6d b3 f7 b1 24 01 e7 71 a7 5e 9b 36 26 b2 96 3c 92 d8 90 7f db 79 c4 c3 fa 4e 68 ad ba 03 e9 19 9e d0 8a 2c 33 fb bd b2 75 f0 06 1f 2a 3f 5d 5b 6a 5d b5 14 d0 23 dd 58 78 93 f6 34 14 5e 10 ba 25 6e 54 d1 9d e9 4b b7 80 6f 7e 87 f1 04 26 22 80 65 b6 e1 bb f9 5c a2 ed 76 32 ff 84 0b d3 07 45 59 19 31 0c fe 79 50 52 83 bd d4 f3 e6 d7 cc e7 56 eb b7 23 59 81 8c 16 9c 72 74 e3 4a 61 67 88 c4 db bf 46 0d 23 37 4c 63 74 58 1e 57 77 32 e6 ef 17 cd 09 Data Ascii: wQg8 SD#.q_4}_Z]Vb%pJ#w.uZ12bu1>eBP3HTU?DG1\,MF(c-Clt93!WEc Gb<-tsFQukv/}UNy=}%2`wOe@}m" /34sgN[<s_<4TAV&gZarc`y/f1O-~`yY#F#u;6Bm$q^6&<yNh,3u*?][j]#Xx4^%nTKo~&"e\v2EY1yPRV#YrtJagF#7LctXWw2
Apr 10, 2021 18:47:54.537532091 CEST	284	IN	HTTP/1.1 400 Bad Request Date: Sat, 10 Apr 2021 16:47:54 GMT Server: Apache/2.4.25 (Debian) Content-Length: 362 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 42 61 64 20 52 65 71 75 65 73 74 3c 2f 68 31 3e 0a 3c 70 3e 59 6f 75 72 20 62 72 6f 77 73 65 72 20 73 65 6e 74 20 61 20 72 65 71 75 65 73 74 20 74 68 61 74 20 74 68 69 73 20 73 65 72 76 65 72 20 63 6f 75 6c 64 20 6e 6f 74 20 75 6e 64 65 72 73 74 61 6e 64 2e 3c 62 72 20 2f 3e 0a 52 65 61 73 6f 6e 3a 20 59 6f 75 27 72 65 20 73 70 65 61 6b 69 6e 67 20 70 6c 61 69 6e 20 48 54 54 50 20 74 6f 20 61 6e 20 53 53 4c 2d 65 6e 61 62 6c 65 64 20 73 65 72 76 65 72 20 70 6f 72 74 2e 3c 62 72 20 2f 3e 0a 20 49 6e 73 74 65 61 64 20 75 73 65 20 74 68 65 20 48 54 54 50 53 20 73 63 68 65 6d 65 20 74 6f 20 61 63 63 65 73 73 20 74 68 69 73 20 55 52 4c 2c 20 70 6c 65 61 73 65 2e 3c 62 72 20 2f 3e 0a 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>400 Bad Request</title> </head><body> Bad Request Your browser sent a request that this server could not understand. Reason: You're speaking plain HTTP to an SSL-enabled server port. Instead use the HTTPS scheme to access this URL, please. </body></html>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: zeD11Fztx8.exe PID: 6720 Parent PID: 5256

General

Start time:	18:47:45
Start date:	10/04/2021
Path:	C:\Users\user\Desktop\zeD11Fztx8.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\zeD11Fztx8.exe'
Imagebase:	0x1380000
File size:	45568 bytes
MD5 hash:	ECBC4B40DCFEC4ED1B2647B217DA0441
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000002.633596595.0000000001381000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000000.00000000.632271273.0000000001381000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: zeD11Fztx8.exe PID: 6728 Parent PID: 6720

General

Start time:	18:47:45
Start date:	10/04/2021
Path:	C:\Users\user\Desktop\zeD11Fztx8.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\zeD11Fztx8.exe
Imagebase:	0x1380000
File size:	45568 bytes
MD5 hash:	ECBC4B40DCFEC4ED1B2647B217DA0441
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000002.640361081.0000000001381000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000001.00000000.633157257.0000000001381000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\storageservice.exe:Zone.Identifier	success or wait	1	13819CE	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: storageservice.exe PID: 6812 Parent PID: 568

General

Start time:	18:47:48
Start date:	10/04/2021
Path:	C:\Windows\SysWOW64\storageservice.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\storageservice.exe
Imagebase:	0x1380000
File size:	45568 bytes
MD5 hash:	ECBC4B40DCFEC4ED1B2647B217DA0441
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000000.638984509.0000000001381000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000002.640209506.0000000001381000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: storageservice.exe PID: 6828 Parent PID: 6812

General

Start time:	18:47:48
Start date:	10/04/2021
Path:	C:\Windows\SysWOW64\storageservice.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\storageservice.exe
Imagebase:	0x1380000
File size:	45568 bytes
MD5 hash:	ECBC4B40DCFEC4ED1B2647B217DA0441
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000000.639793428.0000000001381000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000003.00000002.898946523.0000000001381000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1381E04	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\config\systemprofile\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1381E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1381E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache\IE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1381E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCache\Content.IE5	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1381E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1381E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1381E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1381E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1381E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1381E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1381E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1381E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1381E04	HttpSendRequestW
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1381E04	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windows\History\History.IE5	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1381E04	HttpSendRequestW

Analysis Process: svchost.exe PID: 4800 Parent PID: 568

General

Start time:	18:49:17
Start date:	10/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 5688 Parent PID: 568

General

Start time:	18:49:35
Start date:	10/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6352 Parent PID: 568

General

Start time:	18:49:49
Start date:	10/04/2021
Path:	C:\Windows\System32\svchost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis