ID: 247311
Sample Name: zeus 1_1.2.7.16.vir
Cookbook: default.jbs
Time: 02:50:32
Date: 20/07/2020
Version: 29.0.0 Ocean Jasper

Table of Contents

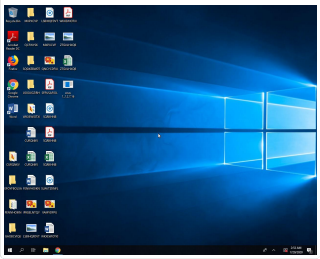
Analysis Report zeus 1_1.2.7.16.vir

Overview

General Information

Sample Name:	zeus 1_1.2.7.16.vir (renamed file extension from vir to exe)
Analysis ID:	247311
MD5:	110bb0c198f670b.
SHA1:	35415b49a99545..
SHA256:	c09598cf7797d78..

Most interesting Screenshot:



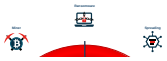
Detection

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Detected unpacking (changes PE se…
- Multi AV Scanner detection for subm…
- Allocates memory in foreign process…
- Changes memory attributes in foreig…
- Contains functionality to change the…
- Creates an undocumented autostart …
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Writes to foreign memory regions
- AV process strings found (often use…

Classification



Startup

- **System is w10x64**
- zeus 1_1.2.7.16.exe (PID: 2496 cmdline: 'C:\Users\user\Desktop\zeus 1_1.2.7.16.exe' MD5: 110BB0C198F670B5596D69DD555758B5)
  - winlogon.exe (PID: 548 cmdline: MD5: 3E56F9D58EBBB1B33E31B86267DBECFC)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

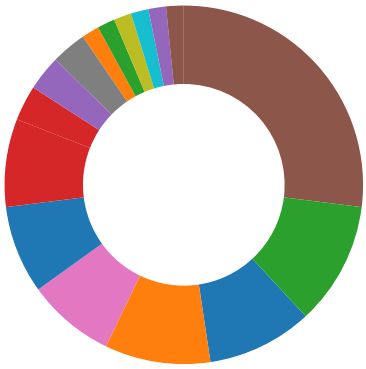
Sigma Overview

System Summary:

Sigma detected: Windows Processes Suspicious Parent Directory

Signature Overview

- AV Detection
- Cryptography
- Spreading



- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Data Obfuscation:

Detected unpacking (changes PE section rights)

Boot Survival:

Creates an undocumented autostart registry key

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Changes memory attributes in foreign processes to executable or writable

Contains functionality to change the desktop window for a process (likely to hide graphical interactions)

Injects a PE file into a foreign processes

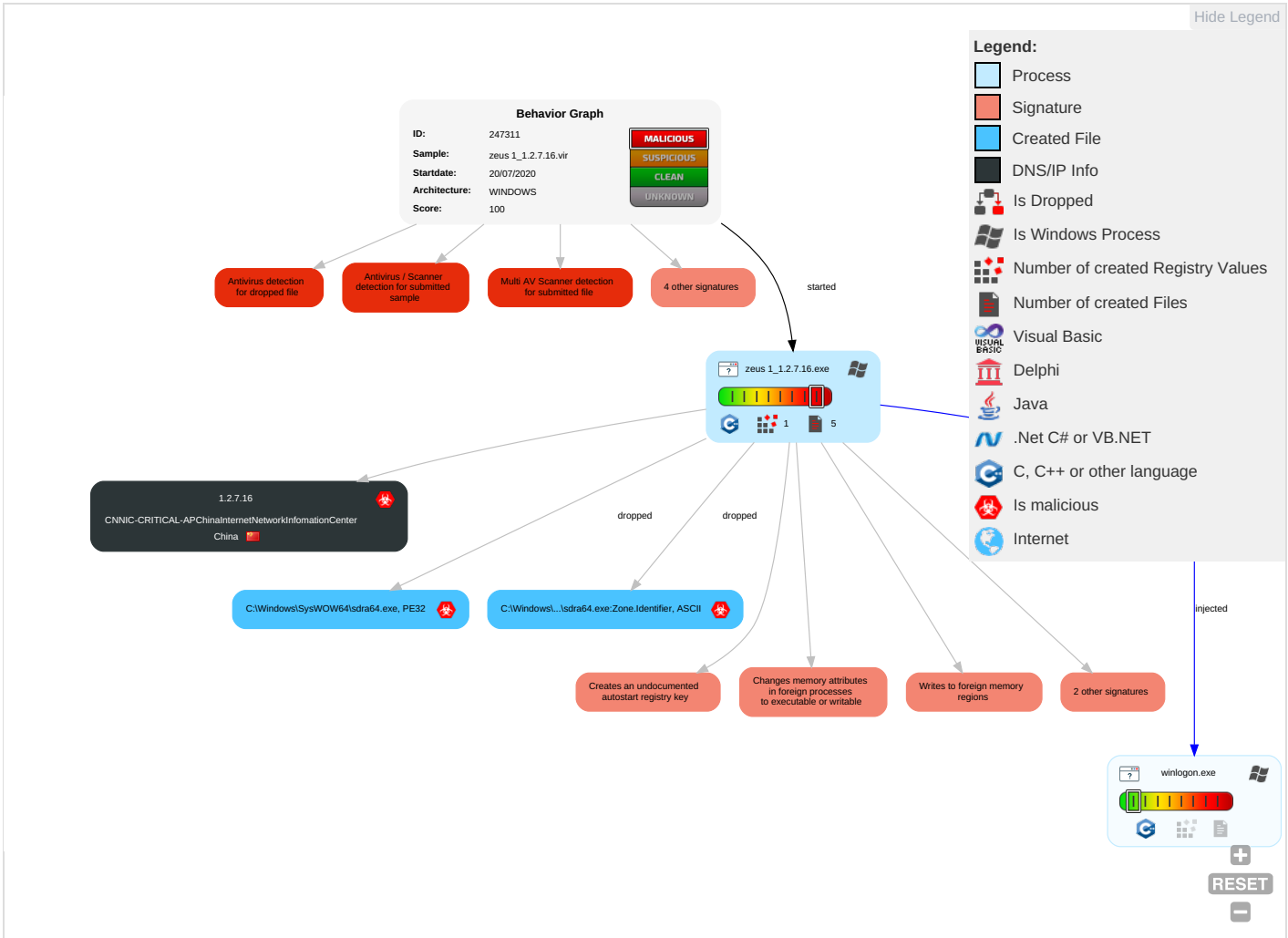
Writes to foreign memory regions

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts 1	Execution through API 1	Registry Run Keys / Startup Folder 1	Valid Accounts 1	Software Packing 1 3	Input Capture 1 1	System Time Discovery 2	Remote File Copy 1	Input Capture 1 1	Data Encrypted 1	Commonly Used Port 1
Replication Through Removable Media	Graphical User Interface 1	Valid Accounts 1	Access Token Manipulation 1 1	Obfuscated Files or Information 2	Network Sniffing	Account Discovery 1	Remote Services	Clipboard Data 1	Exfiltration Over Other Network Medium	Remote File Copy 1
External Remote Services	Windows Management Instrumentation	Application Shimming 1	Process Injection 4 2	Masquerading 2	Input Capture	Security Software Discovery 3	Windows Remote Management	Data from Network Shared Drive	Automated Exfiltration	Standard Cryptographic Protocol 2

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	Scheduled Task	System Firmware	Application Shimming 1	Valid Accounts 1	Credentials in Files	File and Directory Discovery 1	Logon Scripts	Input Capture	Data Encrypted	Multiband Communication
Exploit Public-Facing Application	Command-Line Interface	Shortcut Modification	File System Permissions Weakness	Virtualization/Sandbox Evasion 1	Account Manipulation	System Information Discovery 3	Shared Webroot	Data Staged	Scheduled Transfer	Standard Cryptographic Protocol
Spearphishing Link	Graphical User Interface	Modify Existing Service	New Service	Access Token Manipulation 1 1	Brute Force	Virtualization/Sandbox Evasion 1	Third-party Software	Screen Capture	Data Transfer Size Limits	Commonly Used Port
Spearphishing Attachment	Scripting	Path Interception	Scheduled Task	Process Injection 4 2	Two-Factor Authentication Interception	Process Discovery 3	Pass the Hash	Email Collection	Exfiltration Over Command and Control Channel	Uncommonly Used Port
Spearphishing via Service	Third-party Software	Logon Scripts	Process Injection	Install Root Certificate 1	Bash History	System Owner/User Discovery 1	Remote Desktop Protocol	Clipboard Data	Exfiltration Over Alternative Protocol	Standard Application Layer Protocol

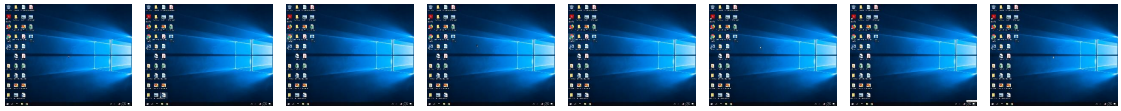
Behavior Graph



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
zeus 1_1.2.7.16.exe	85%	Virustotal		Browse
zeus 1_1.2.7.16.exe	79%	Metadefender		Browse
zeus 1_1.2.7.16.exe	92%	ReversingLabs	Win32.Trojan.Zbot	
zeus 1_1.2.7.16.exe	100%	Avira	TR/Dropper.Gen	
zeus 1_1.2.7.16.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\SysWOW64\sdra64.exe	100%	Avira	TR/Dropper.Gen	
C:\Windows\SysWOW64\sdra64.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.winlogon.exe.15e50000.480.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
1.2.winlogon.exe.14ed0000.356.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.15cd0000.468.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.15690000.418.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.146d0000.292.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.14670000.289.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13490000.146.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13e10000.222.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.15310000.390.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.14e10000.350.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13050000.112.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.12430000.15.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13390000.138.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.16150000.504.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.15230000.383.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.15550000.408.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13890000.178.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.15a30000.447.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.15050000.368.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.15ed0000.484.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.15210000.382.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.125f0000.29.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.14cd0000.340.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13150000.120.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.15b90000.458.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.14050000.240.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.15510000.406.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13ed0000.228.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.14770000.297.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.12c30000.79.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13ff0000.237.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.136f0000.165.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.12f90000.106.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.14bf0000.333.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.16110000.502.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13c10000.206.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.12ed0000.100.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.130b0000.115.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.14d30000.343.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.14330000.263.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.15d50000.472.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.14df0000.349.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.14b50000.328.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13990000.186.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13a70000.193.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13530000.151.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.12c50000.80.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.14d10000.342.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.15250000.384.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13570000.153.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13c90000.210.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.12930000.55.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13770000.169.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.14090000.242.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.12310000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.150f0000.373.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13730000.167.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.12810000.46.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.15f30000.487.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.15910000.438.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.16070000.497.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.12d30000.87.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.15a70000.449.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.123b0000.11.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.15df0000.477.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
1.2.winlogon.exe.12610000.30.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.14a70000.321.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13a10000.190.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.14ab0000.323.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.15130000.375.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.14850000.304.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13590000.154.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.138f0000.181.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.15710000.422.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.12650000.32.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.14710000.294.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.15bf0000.461.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.14790000.298.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13350000.136.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.15cf0000.469.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.156f0000.421.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.15d90000.474.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.14870000.305.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.12a70000.65.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.127d0000.44.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13c50000.208.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.144d0000.276.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.14e90000.354.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.14930000.311.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.15570000.409.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.12f70000.105.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.15d10000.470.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.14f10000.358.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.15010000.366.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.12d70000.89.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.15810000.430.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.12530000.23.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13670000.161.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13a30000.191.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13df0000.221.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

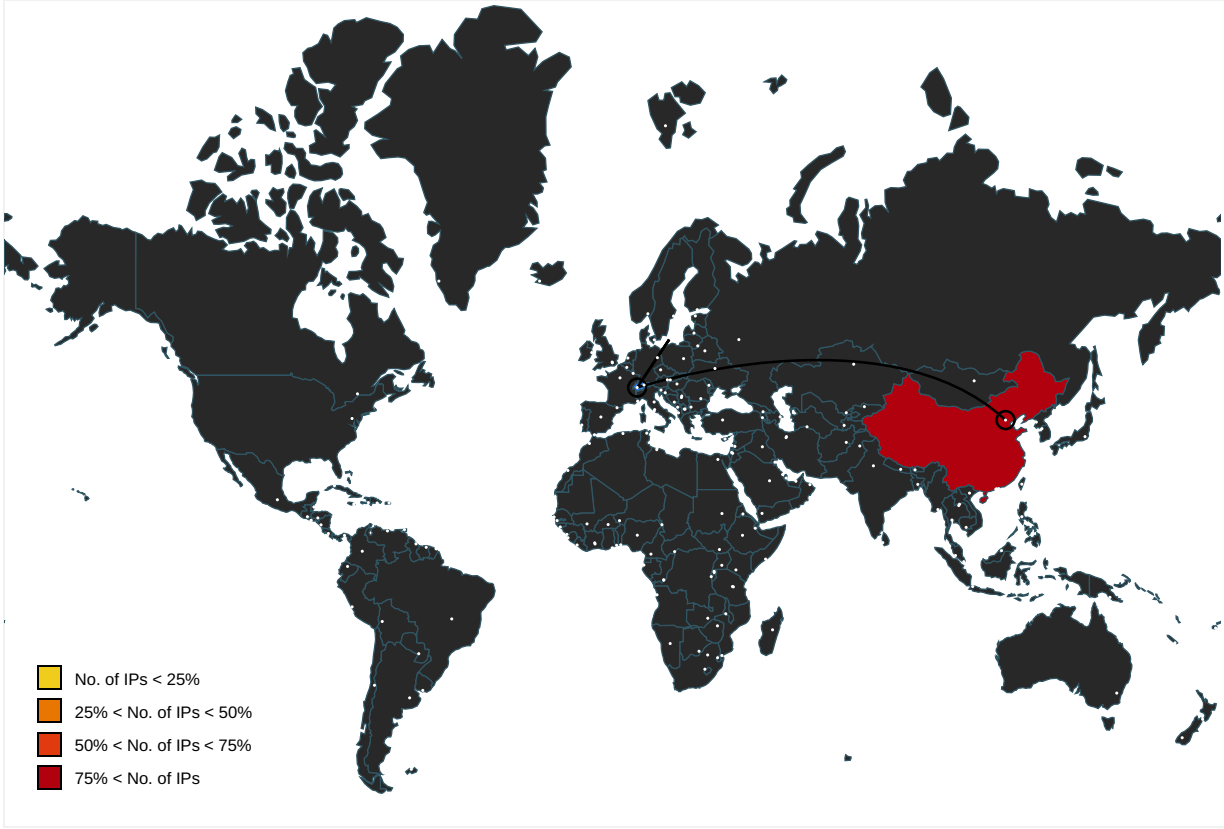
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://onlineeast#.bankofamerica.com/cgi-bin/ias/	zeus 1_1.2.7.16.exe, 00000000.00000002.1201500570.0000000002373000.00000004.00000040.sdmp	false		low

Contacted IPs



Public

IP	Country	Flag	ASN	ASN Name	Malicious
1.2.7.16	China		24409	CNNIC-CRITICAL-APChinaInternetNetworkInfomationCenter	true

General Information

Joe Sandbox Version:	29.0.0 Ocean Jasper
Analysis ID:	247311
Start date:	20.07.2020
Start time:	02:50:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	zeus 1_1.2.7.16.vir (renamed file extension from vir to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit (version 1803) with **Office 2016**, Adobe Reader DC 19, Chrome 70, Firefox 63, Java 8.171, Flash 30.0.0.113
Number of analysed new started processes analysed:	6
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.evad.winEXE@1/2@0/1

EGA Information:	Failed
HDC Information:	• Successful, ratio: 90.8% (good quality ratio 82.2%) • Quality average: 77.1% • Quality standard deviation: 32.2%
HCA Information:	• Successful, ratio: 51% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): WMIADAP.exe, MusNotifyIcon.exe, UsoClient.exe • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Windows\SysWOW64\sdra64.exe	
Process:	C:\Users\user\Desktop\zeus 1_1.2.7.16.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Size (bytes):	896512
Entropy (8bit):	7.490732749711434
Encrypted:	false
MD5:	F198AE2117AF7DAD0ED1537759F48866
SHA1:	632C4801759344DCD695D8D0234F9AD5A65EA4CF
SHA-256:	F8E7189DCA0AB88E3E146E3625E7AB5505975DB694219CBA44947499C6FEBD21
SHA-512:	ABA6CB5B5B219E70481865E9B31D66706DF467CE084BD05D82B2F1AD525171D46B7A3BFCBE233F3202F5CB844EF1509908259A85F14E56772DBABB3074D0144

C:\Windows\SysWOW64\sdra64.exe	
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....I..\I..\I..\I..\o..\d..\'..\!..\;..\1..\P..\...\...\A..\...\...\RichI..\.....PE..L...G.[I..... ....."....e.....@.....5.....p...P.....text....p.....&..... . .`.data.....*.....@..@.rdata... .....,.....@..@.rsrc.....H.....@..@.....

C:\Windows\SysWOW64\sdra64.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\zeus 1_1.2.7.16.exe
File Type:	ASCII text, with CRLF line terminators
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.515489627725481
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:	zeus 1_1.2.7.16.exe
File size:	673280
MD5:	110bb0c198f670b5596d69dd555758b5
SHA1:	35415b49a99545a7887432fb0acfbf52bbea2d24
SHA256:	c09598cf7797d78f3da54d780bb4180ce6518216ec25fe85063f7af4fbd486c5
SHA512:	6785005c8d7fc33cb6e8c1687c99ef2bb1f2df733bbe05057532665369b160e4ab2d356413c0ee2cf9b63ef95c8dee12f4c8ed9c5e9c19f2bee6cf05a7dafbfc
SSDEEP:	12288:SZ7rNePRuTgREnok8oc8YjfvNzWRksxNWI7ndnMnJIqEaKsKAh207ZdV8ZU4W2Os:I5TgREnok5Yjn9WRhzvkJVffZdVT2Okl
File Content Preview:	MZ.....@.....I..\I..\I..\I..\o..\d..\'..\!..\;..\1..\P..\...\...\A..\...\...\RichI..\.....PE..L...G.[I.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x411d65
Entrypoint Section:	.text
Digitally signed:	false

General

Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x495BD347 [Wed Dec 31 20:17:11 2008 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	5654571c1bcaea25702815802614af7f

Entrypoint Preview

Instruction
dec ecx
sub ah, ch
dec bl
sub edx, ecx
mov ebx, edx
xor dl, 00000051h
mov bh, 8Dh
add ch, bh
sbb ebx, eax
mov edx, 703C68F7h
xor al, bl
dec al
or bh, FFFFFF8Dh
jmp 00007F6C98784F23h
out dx, al
pop es
test byte ptr [ebp-0FF5BCB5h], bh
add bl, cl
xor dl, 00000026h
add dh, 0000003Ch
sub dl, al
adc bl, bh
inc ch
cmp eax, 0EAF013Fh
je 00007F6C987855C0h
sub dh, ch
and edx, edi
jmp 00007F6C98785220h
jns 00007F6C987853F9h
mov dword ptr [92E1802Eh], eax
and bl, dl
xor ch, bh
sub ebx, esi
or bh, 0000007Eh
mov bl, F3h
inc cl
jmp 00007F6C98784D7Eh
mov ebp, 3D93B740h
retf 1B49h
fiadd dword ptr [eax-373E7E39h]
add dword ptr [edi], ecx
add al, 00000000h
add byte ptr [eax], al
inc edi
or cl, 0000000Eh
jmp 00007F6C98784D82h

Instruction
or ah, byte ptr [ebx]
rcl byte ptr [eax-15h], 1
outsd
or bl, 00000065h
and bh, 0000002Eh
mov al, ECh
and esi, eax
inc ebx
ret
add esi, ecx
adc eax, edi
add edx, esi
mov edi, esi
xor al, ah
jmp 00007F6C98785209h
outsb
and eax, FB8ABBD8h
sub ecx, edx
sbb ch, cl
and bl, 00000030h
sbb edi, eax
and dl, ch
add ch, 0000006Ah
mov edx, eax
sub bl, 0000007Ch
sub edi, eax
or ch, ah
add edi, edx
je 00007F6C98785406h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x19470	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1b000	0xa080	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x0	0x0	
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	0x17000	0x12600	False	0.977691857993	data	7.93043162948	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x18000	0x1000	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rdata	0x19000	0x2000	0x1c00	False	0.315011160714	data	5.3503765786	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x1b000	0x1000	0x400	False	0.4443359375	data	3.05603843411	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x1b058	0x300	data	Russian	Russia

Imports

DLL	Import
KERNEL32.DLL	VirtualProtect, Sleep, VirtualAlloc, SetLastError, QueryPerformanceCounter, GetCurrentProcess, InterlockedDecrement, CreateFileW, GetLastError, UnhandledExceptionFilter, ReadFile, HeapFree, CloseHandle, GetSystemTimeAsFileTime, CreateThread, VirtualAlloc, GetSystemTimeAsFileTime, lstrcmpiW, GetProcessHeap, lstrcmpiW, EnterCriticalSection, HeapFree, DeleteCriticalSection, GetModuleHandleA, GetTickCount, InitializeCriticalSection, GetProcAddress, InterlockedDecrement, VirtualAlloc, lstrcmpiW, HeapAlloc, CreateEventW, GetCurrentProcessId, VirtualAlloc, GetTickCount, GetTickCount, CreateEventW, CreateFileW, GetModuleFileNameA, InterlockedDecrement, GetModuleHandleW, GetProcAddress, SetLastError, EnterCriticalSection, LocalAlloc, GetProcessHeap, FreeLibrary, InterlockedIncrement, CreateFileW, GetCurrentProcess, Sleep, lstrlenA, GetTickCount, EnterCriticalSection, EnterCriticalSection, HeapFree, CloseHandle, LocalFree, InterlockedDecrement, GetTickCount, InterlockedDecrement, HeapDestroy, GetModuleFileNameA, GetCurrentProcess, SetLastError, LocalFree, GetModuleFileNameW, GetProcessHeap, UnhandledExceptionFilter, GetModuleHandleA, GetModuleFileNameW, GetCurrentProcessId, GetModuleFileNameA, GetVersionExA, GetProcessHeap, GetModuleFileNameW, VirtualProtect, lstrlenA, LoadLibraryW, GetModuleHandleW, ReadFile, HeapFree, LocalAlloc, UnhandledExceptionFilter, VirtualProtect, GetLastError, CreateEventW, InterlockedIncrement, HeapDestroy, GetModuleHandleW, HeapFree, HeapFree, GetModuleFileNameW
GDI32.DLL	SetBkColor, MoveToEx, CreateCompatibleDC, SetWindowOrgEx, PatBlt, LineTo, PatBlt, SetBrushOrgEx, SelectObject, GetPixel, Rectangle, CreateBitmapIndirect, CreateBitmapIndirect, CreateRectRgn, GetBrushOrgEx, CombineRgn, Polygon, SetPixel, SetWindowOrgEx, CreateCompatibleDC, GetWindowOrgEx, BitBlt, SetWindowExtEx, GetBrushOrgEx, Rectangle, CreateSolidBrush, PatBlt, GetWindowOrgEx, GetWindowOrgEx, SetWindowExtEx, CreateCompatibleDC, BitBlt, SetBrushOrgEx, Ellipse, RoundRect, CreateDIBitmap, GetPixel, Polygon, CombineRgn, SetWindowExtEx, SetPixel, BitBlt, Polygon, GetBkColor, PatBlt, Rectangle, Rectangle, BitBlt, GetBkColor, GetBkMode, GetWindowOrgEx, StretchBlt, SetPixel, Polygon, RoundRect, CombineRgn, LineTo, CreatePen, BitBlt, CreateRectRgn, SetBkColor, GetBkMode, GetBkColor, CreateCompatibleDC, CreateSolidBrush, SetWindowExtEx, SetBrushOrgEx, BitBlt, CreateFontA, GetCurrentObject, CreateSolidBrush, SelectObject, SetPixel, CreateDIBitmap, GetBkColor, CombineRgn, RoundRect, CreateSolidBrush, CreateSolidBrush, CreateDIBitmap, Rectangle, CreateDIBSection, CreateFontA, SelectObject, GetBkColor, SetPixel, CreateCompatibleDC, SetTextColor, GetCurrentObject, SetBrushOrgEx, StretchBlt, BitBlt, GetBkColor
USER32.DLL	DefWindowProcW, BeginPaint, LoadIconW, SendDlgItemMessageW, ReleaseDC, EnableWindow, KillTimer, DefWindowProcW, SetDlgItemTextW, SendMessageW, LoadIconW, PeekMessageW, SendMessageW, GetWindowLongW, GetWindowLongW, wsprintfA, LoadStringW, GetDesktopWindow, SendDlgItemMessageW, GetWindowRect, PostQuitMessage, BeginPaint, DispatchMessageW, InvalidateRect, GetDesktopWindow, GetClientRect, CreateWindowExW, DefWindowProcW, DialogBoxParamW, MessageBoxW, BeginPaint, TranslateMessage, GetClientRect, EnableWindow, DispatchMessageW, SetWindowTextW, GetDC, SendMessageW, PostQuitMessage, LoadCursorW, DialogBoxParamW, CreateWindowExW, ReleaseDC, InvalidateRect, SendMessageW, SendDlgItemMessageW, LoadCursorW, wsprintfA, DialogBoxParamW, PostMessageW, GetWindowLongW, PostQuitMessage, EnableWindow, IsDlgButtonChecked, LoadCursorW, ShowWindow, SetWindowPos, LoadStringW, KillTimer, PostQuitMessage, SetWindowPos, DialogBoxParamW, PeekMessageW, GetWindowLongW, EndPaint, GetDlgItem, GetDlgItem, GetParent, IsWindow, SetFocus, IsDlgButtonChecked, GetDC, GetDC, KillTimer, SetFocus, MessageBoxW, GetDC, GetWindowRect, LoadCursorW, GetSysColor, DispatchMessageW, GetFocus, EnableWindow, LoadCursorW, LoadIconW, SetWindowLongW, GetParent, GetFocus, SetForegroundWindow, GetClientRect, CharNextW, SetCursor, MessageBoxW, BeginPaint

Version Infos

Description	Data
LegalCopyright	oFPnaVuvvAmEViAH
InternalName	Ioh7CXN8XmIJi
FileVersion	q2V54BNs7dmpNR
CompanyName	SOFTWIN TQoeE2bRkcG8B
ProductName	GGMCDheOY25gYWfFE
ProductVersion	WgJp2fEoGiiKDPn
FileDescription	Ehklr7jBf5jU
OriginalFilename	ITH1Vf56KGqg5ND
Translation	0x0800 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map
Russian	Russia	

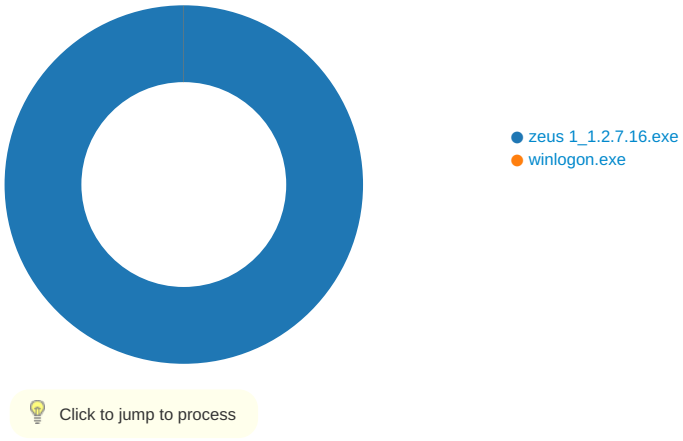
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: zeus 1_1.2.7.16.exe PID: 2496 Parent PID: 5400

General

Start time:	02:51:41
Start date:	20/07/2020
Path:	C:\Users\user\Desktop\zeus 1_1.2.7.16.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\zeus 1_1.2.7.16.exe'
Imagebase:	0x400000
File size:	673280 bytes
MD5 hash:	110BB0C198F670B5596D69DD555758B5
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\sdra64.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	405B38	CopyFileW
C:\Windows\SysWOW64\sdra64.exe:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	405B38	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\sdra64.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0d f7 e0 0f 49 96 8e 5c 49 96 8e 5c 49 96 8e 5c 49 96 8e 5c 49 96 8e 5c 6f 96 8e 5c 64 96 8e 5c 27 96 8e 5c 21 96 8e 5c 3b 96 8e 5c 31 96 8e 5c 50 96 8e 5c 01 96 8e 5c 08 96 8e 5c 41 96 8e 5c 15 96 8e 5c 03 96 8e 5c 52 69 63 68 49 96 8e 5c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 47 d3 5b 49 00 00 00 00 00 00 00 00 e0 00 0b 01 0b 01 05 0c 00 00 00	MZ......................@..... ....I..\I..\I..\I..\I. .\o..\d..\'..\!..\;..\1..\P..\ ...\...\A..\...\...\RichI..\.. ..............PE..L...G.[I....	success or wait	3	405B38	CopyFileW
C:\Windows\SysWOW64\sdra64.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	405B38	CopyFileW
C:\Windows\SysWOW64\sdra64.exe	unknown	223232	0c 06 1d 11 7c 62 04 a1 03 12 0f 03 1d 13 8f 7a 28 4c 21 0b 05 ce 18 06 8a c0 33 72 bb 3f 00 86 31 3b 14 36 0d 2c 76 3a 9c 6e 21 1d be 4a 74 19 7e 8f 8a 0e 23 2c 50 6b 1c 33 2a 2b 87 02 00 3d 43 8e 3c 7a 55 41 b0 44 18 3a 6f 1a 07 5f 77 08 10 13 23 82 45 4a 3e 06 20 5e 9b 00 42 1f 05 41 3e 0b 1f 3c 0c 1d b0 56 9b 8b 0f 79 4a 0d 01 21 3f b1 02 60 39 77 2d 18 03 69 15 bd 2a 91 33 90 01 02 79 d7 31 b8 3c 60 29 32 aa 28 0e 96 7b 20 0a 03 4a b1 22 3b 37 04 af 13 22 00 0b 12 06 08 6f 38 37 49 7d 88 1b be 85 0d 12 0a 0f 2d 04 1d 1d fb 19 69 5e 09 1d 40 3d 3a 12 04 01 47 0e 73 1a 57 1f 3f 8a 28 02 01 41 23 88 15 90 5c 3f 62 16 04 76 08 07 05 0c 48 03 08 40 12 be 09 72 0a 78 87 a2 4c 61 0a 25 21 45 22 04 2d a8 43 01 4c 29 ae 4f b6 35 3d 02 cf 3e 53 0b 05 47 30 0a	....|b.........z(L!.......3r.? ..1;.6.,v:.n!..Jt.~...#,Pk.3*+ ...=C. <zUA.D.:o.._w...#.EJ>. ^ ..B..A>..<...V...yJ..!?..`9w-. .i..*.3...y.1.<`)2.(..{ ..J."; 7...".....o87I}........-.....i ^..@=:...G.s.W.?.(..A#...\? b..v....H..@...r.x..La.%!E".- .C.L).O.5=..>S..G0.	success or wait	1	405BD6	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	userinit	unicode	C:\Windows\system32\sdra64.exe,	success or wait	1	409D97	RegSetValueExW

Analysis Process: winlogon.exe PID: 548 Parent PID: 2496

General

Start time:	02:51:46
Start date:	20/07/2020
Path:	C:\Windows\System32\winlogon.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff660a60000
File size:	677376 bytes
MD5 hash:	3E56F9D58EBBB1B33E31B86267DBECFC
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

Code Analysis