ID: 247337
Sample Name: zeus 1_1.2.1.5.vir
Cookbook: default.jbs
Time: 03:25:24
Date: 20/07/2020
Version: 29.0.0 Ocean Jasper

Table of Contents

Copyright null 2020

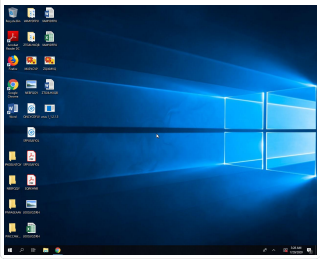
Analysis Report zeus 1_1.2.1.5.vir

Overview

General Information

Sample Name:	zeus 1_1.2.1.5.vir (renamed file extension from vir to exe)
Analysis ID:	247337
MD5:	11b83ace772235..
SHA1:	4151d739f6a42ad.
SHA256:	84cd847f2f244fc…

Most interesting Screenshot:



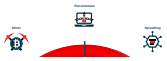
Detection

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_1.2.1.5.exe (PID: 5436 cmdline: 'C:\Users\user\Desktop\zeus 1_1.2.1.5.exe' MD5: 11B83ACE7722358A7172E55C8C896CD7)
  - winlogon.exe (PID: 548 cmdline: MD5: 3E56F9D58EBBB1B33E31B86267DBECFC)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

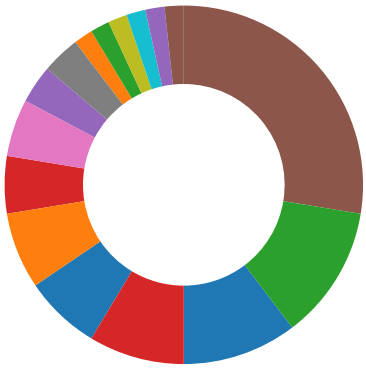
System Summary:

Sigma detected: Windows Processes Suspicious Parent Directory

Signature Overview

- AV Detection
- Cryptography
- Spreading

Copyright null 2020



- 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

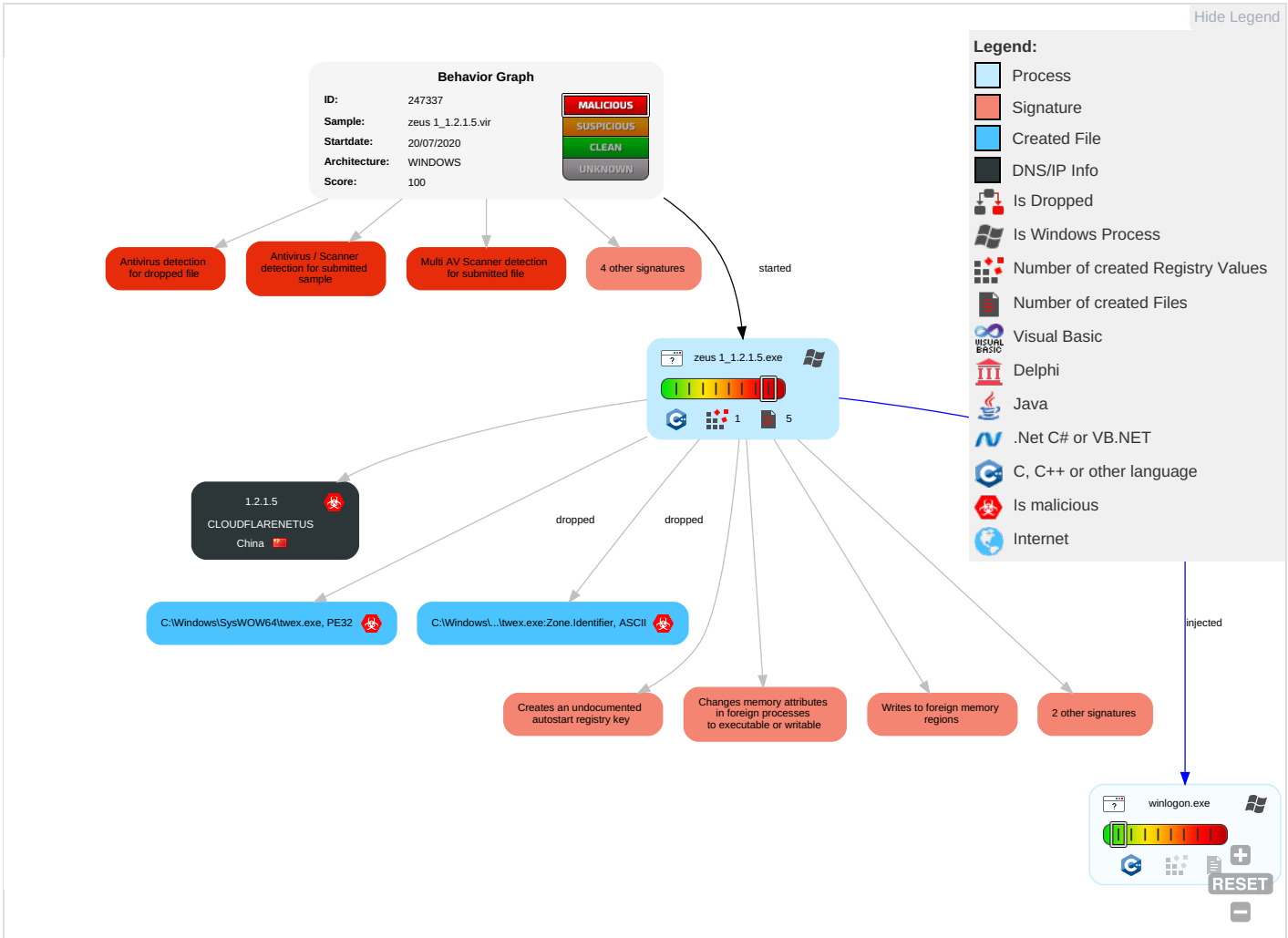
Mitre Att&ck Matrix

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 2	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 1	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 2	Windows Remote Management	Data from Network Shared Drive	Automated Exfiltration	Standard Cryptographic Protocol 2

Copyright null 2020

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

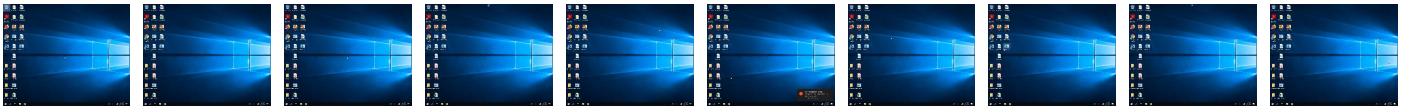
Behavior Graph



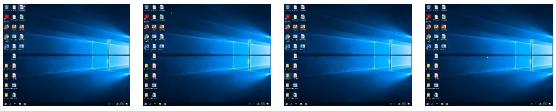
Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Copyright null 2020



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
zeus 1_1.2.1.5.exe	85%	Virustotal		Browse
zeus 1_1.2.1.5.exe	78%	Metadefender		Browse
zeus 1_1.2.1.5.exe	86%	ReversingLabs	Win32.Spyware.Zbot	
zeus 1_1.2.1.5.exe	100%	Avira	TR/Dropper.Gen	
zeus 1_1.2.1.5.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Windows\SysWOW64\twex.exe	100%	Avira	TR/Dropper.Gen	
C:\Windows\SysWOW64\twex.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

Copyright null 2020

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.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
0.0.zeus 1_1.2.1.5.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.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

Copyright null 2020

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

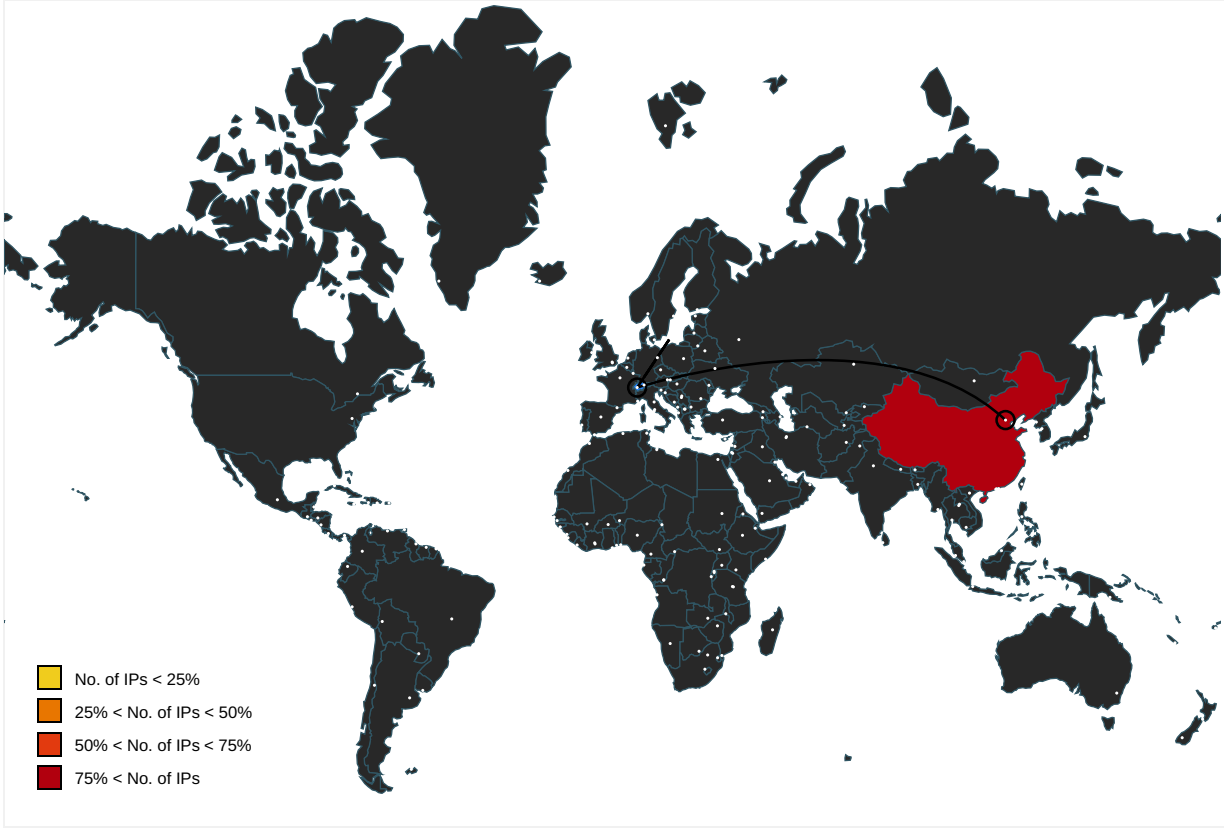
Contacted Domains

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_1.2.1.5.exe, 00000000.00000002.1211320945.0000000000A03000.00000004.00000040.sdmp	false		low

Contacted IPs



Public

IP	Country	Flag	ASN	ASN Name	Malicious
1.2.1.5	China		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	29.0.0 Ocean Jasper
Analysis ID:	247337
Start date:	20.07.2020
Start time:	03:25:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	zeus 1_1.2.1.5.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

Copyright null 2020

HDC Information:	• Successful, ratio: 98.4% (good quality ratio 93.3%) • Quality average: 84.5% • Quality standard deviation: 27%
HCA Information:	Failed
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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	http://comtechadsl.com/ehepsqm.exe	Get hash	malicious	Browse	• 104.20.74.28
	http://blueeyeswebsite.com/	Get hash	malicious	Browse	• 104.24.110.109
	ATT20893.HTML	Get hash	malicious	Browse	• 104.16.133.229
	ATT84128.HTML	Get hash	malicious	Browse	• 104.16.133.229
	http://https://bit.ly/30cSl6K	Get hash	malicious	Browse	• 104.16.124.96
	http://https://jhmetalinc-my.sharepoint.com/:o:/p/office/EiJ0PCnWDtJHiWQIXRi7bWgB6cFzFQtLhcLET3v8d3NRLA?rtime=ORiHa4Eq2Eg	Get hash	malicious	Browse	• 104.16.132.229
	ATT39268.HTM	Get hash	malicious	Browse	• 104.16.133.229
	payment730.xls	Get hash	malicious	Browse	• 104.27.180.83
	http://atcsagacity.com/wp-admin/MYWZIKG/eigyho/s9w0816332646203713g44z0n2u/	Get hash	malicious	Browse	• 172.67.186.191
	http://https://gogoanime1.net/.well-known/acme-challenge/bid/login.php	Get hash	malicious	Browse	• 104.16.132.229
	http://https://lroetrgpfxciziew.frb.io/?bbre=pdsi93reodfxci	Get hash	malicious	Browse	• 104.16.133.229
	http://mapfrecomercial.com/	Get hash	malicious	Browse	• 104.16.202.237
	http://https://event.on24.com/wcc/r/2462461/BB0A869CCD07459AE0E4C73F0AD810E3/1209023?partnerref=connect	Get hash	malicious	Browse	• 104.17.71.206
	http://https://u10500736.ct.sendgrid.net/ls/click?upn=GJ-2Fwg0v0GjXICnjOzCZwjhkRw9-2BbFlj0p-2BETjV5NQUzZanQeaYMDpzIDJ401Kach0E7l_YxCxpoge33FNHhRVcK23d3jJCq3cIHwc-2BD1XeO3y4vWhDSyEnUs6U-2FsQ3r28LvMmBf0-2FyPTfw7LkuX8KPrqtuiBKVLJGudFG5cgos-2FYMheOpZ3KzgDMXMKE-2BA6yiT-2Bi5BQtK80dm1zrijWZnCRa6hF0zjqp3QnkLp0NHHccLK9ZW3lYLn1ntwPI5yxeaqK-2FwMj6c4bzGzF8lmQMxhNRSLY2oartjGJW1716gR3wWT6FnAMuuMr-2BmVOWIDO3doJzx	Get hash	malicious	Browse	• 104.22.0.232

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://youbue.com	Get hash	malicious	Browse	• 104.20.21.239
	MuMuInstaller_1.1.0.4_a2ca17_yxmrfz_zh-Hans_1573441614.exe	Get hash	malicious	Browse	• 1.1.0.4
	Invoice2867.hTMl	Get hash	malicious	Browse	• 104.27.165.84
	http://https://www.seat26.com/wp-includes/js/tinymce/plugins/colorpicker/gastblogg/warenkorb.php?street=kqh1sdty120gb0c&face=guess&window=section	Get hash	malicious	Browse	• 104.16.132.229
	http://www.hobbyfarms.com/how-to-build-a-vermin-proof-chicken-feeder/	Get hash	malicious	Browse	• 104.18.99.60
	Scanned_from_Xerox_Multifunction.htm	Get hash	malicious	Browse	• 104.16.133.229

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Windows\SysWOW64\twex.exe

Process:	C:\Users\user\Desktop\zeus 1_1.2.1.5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Size (bytes):	925696
Entropy (8bit):	7.424007871258338
Encrypted:	false
MD5:	8787E4E8D58D7D70F1098FE979B8BB99
SHA1:	C7B017973A941C6A0F6539460EC5910F7CB3F2A1
SHA-256:	43678D199F5897899E981EAB2F4D54DD6C74F01F6E202F497ADE4C360D0CBD74
SHA-512:	D3B9FBF1EE869791B8398530B6AA27DB4A4EF903EFB750A57AAC31C8F1F79C2A88012E80AB660FFB19223E2962E1E0601E0B76715CCCC494B19F190EBF20B041
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....j*...KgE.KgE.KgE.NQErKgE.tLE^KgE.`\E%KgERich.KgE.....PE..L.....#H.....B.....@.....`.....d...d.....text... ....`.data....@.....@..... .....

C:\Windows\SysWOW64\twex.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\zeus 1_1.2.1.5.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

General

Entropy (8bit):	7.424180621515364
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_1.2.1.5.exe
File size:	465920
MD5:	11b83ace7722358a7172e55c8c896cd7
SHA1:	4151d739f6a42adbd4d3a138142e10690cc7413c
SHA256:	84cd847f2f244fc4f45d9ea1615018fd478f601e455236b6c662aeb94064004a
SHA512:	657ca377b5f80b5dfc6514b54a0cf34a6a50bed22cfe01a7b7bd08039fd5a651f1953168a81e2c9899e91b39f7b58ccc7d77fabd00bf81d8d5f1c2bcec7e3ac2
SSDEEP:	12288:e1IEwtNj3mmhRe02MvG+tpjrRRcXqitcbgjY6:LtproMvtb/Dca4vjR
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....j*...KgE.KgE.KgE.NQErKgE.tLE^KgE.`\E%KgERich.KgE.....PE..L.....#H.....B.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40b919
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x4823D499 [Fri May 9 04:35:37 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:	0b3bcc53f0d2e75a55e4b8dd85b7fc6b

Entrypoint Preview

Instruction
xor eax, eax
call 00007F7700A8FAC6h
ret
push esp
push 00000001h
push 001F0003h
call dword ptr [00401028h]
jl 00007F7700A8FAB2h
xor edi, edi
push 00000040h
push 00003000h
push 00010285h
push 00000000h
call dword ptr [00401014h]

Instruction
xor edi, edi
mov esi, dword ptr [esp]
add esi, 62h
mov edi, eax
mov ecx, 000001F5h
xor ebp, ebp
mov edx, 26AFE4B2h
mov bh, byte ptr [esi]
add bh, dl
add bh, bl
mov byte ptr [edi], bh
inc edi
inc esi
shr edx, 08h
inc ebp
cmp ebp, 04h
jne 00007F7700A8FAC9h
xor ebp, ebp
mov edx, 26AFE4B2h
sub ecx, 01h
cmp ecx, 00000000h
jne 00007F7700A8FAA0h
jmp eax
ret
fisubr word ptr [ecx-2BFE2896h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x10664	0x64	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
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	0x1000	0x104	.text
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	0xfc20	0xfe00	False	0.855484128937	data	6.76029815561	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x11000	0x40f3	0x200	False	0.177734375	data	1.12592999128	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.dll	GetFileSize, GetUserDefaultUILanguage, GetModuleFileNameW, GetTimeZoneInformation, VirtualProtect, VirtualAlloc, GetLastError, SystemTimeToFileTime, GetLocalTime, HeapReAlloc, OpenEventW, lstrcpyA, CreateThread, SetFileTime, GetModuleFileNameA, GetFileSizeEx
SHLWAPI.dll	PathMatchSpecW, PathCombineW, SHDeleteKeyA, StrCmpNIW, PathRemoveFileSpecW, wnsprintfW, StrStrW, wvnsprintfA, PathFindFileNameW, PathFileExistsW, StrCmpNIA
USER32.dll	DispatchMessageA, GetDlgItem, CharLowerBuffA, ToUnicode, LoadCursorA, GetKeyState, OpenDesktopA, GetForegroundWindow, PeekMessageA, GetIconInfo, GetDlgItemTextA, DrawIcon, OpenWindowStationA, CloseDesktop, MsgWaitForMultipleObjects, SetThreadDesktop, GetMessageA, GetClipboardData, FindWindowExA, EndDialog, SendMessageA

Copyright null 2020

DLL	Import
ADVAPI32.dll	CryptReleaseContext, DuplicateTokenEx, CryptCreateHash, CryptGetHashParam, CryptDestroyHash, RegCloseKey, CryptAcquireContextW, CryptHashData, RegSetValueExA, RegDeleteValueA, GetUserNameW, RegEnumKeyExA, RegQueryValueExA

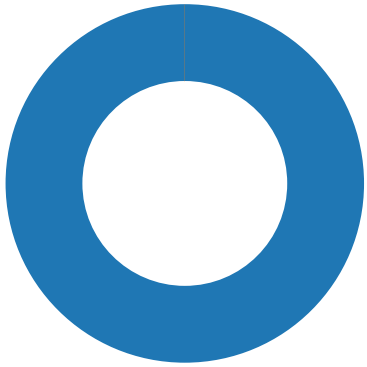
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: zeus 1_1.2.1.5.exe PID: 5436 Parent PID: 3828

General

Start time:	03:26:36
Start date:	20/07/2020
Path:	C:\Users\user\Desktop\zeus 1_1.2.1.5.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\zeus 1_1.2.1.5.exe'
Imagebase:	0x400000
File size:	465920 bytes
MD5 hash:	11B83ACE7722358A7172E55C8C896CD7
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

Copyright null 2020

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\twex.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	405783	CopyFileW
C:\Windows\SysWOW64\twex.exe:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	405783	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\twex.exe	0	131072	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 6a 2a 09 16 2e 4b 67 45 2e 4b 67 45 2e 4b 67 45 d2 4e 51 45 72 4b 67 45 19 74 4c 45 5e 4b 67 45 f1 60 5c 45 25 4b 67 45 52 69 63 68 2e 4b 67 45 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 02 00 99 d4 23 48 00 00 00 00 00 00 00 00 e0 00 03 01 0b 01 09 00 00 fe 00 00 00 42 00 00 00 00 00 00 19 b9 00 00 00 10 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......j*...KgE.KgE.KgE.NQ ErK gE.tLE^KgE.`\E%KgERich. KgE.... ....PE ..L.....#H.................... .B............	success or wait	4	405783	CopyFileW
C:\Windows\SysWOW64\twex.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	405783	CopyFileW

Copyright null 2020

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\twex.exe	unknown	459776	98 6f 09 11 5f 12 00 27 59 07 0d 51 47 00 59 49 01 32 ee 15 01 03 55 09 0d 0d 00 02 1e cb 35 04 14 31 16 35 74 6c d2 38 14 13 13 1a 12 00 10 08 05 66 75 09 09 11 09 65 59 46 0c 06 3d 2e 8c 94 e3 0c 2c 94 be 15 35 3a a9 31 3f 94 63 09 23 0a 08 15 0d 0d 19 01 66 5b 4c 06 1d 53 05 2d 86 07 24 07 7e 2c 0f c0 05 05 04 bb 01 59 90 35 01 12 5e 0e 07 31 59 16 b5 77 99 8c 01 01 32 58 06 1c a8 00 b8 d7 00 06 0a 8a 0b 42 1f 01 52 02 38 18 11 09 64 3a 5e 17 01 1f 37 13 18 1c 49 10 84 25 26 49 3b 09 30 2d 3c 06 01 92 09 08 61 22 6f 07 61 08 2f 26 47 1a 3c 11 16 87 3b 0e 29 0c 03 00 6d 14 96 0b 18 08 19 18 1b 01 6e 09 5f 1e d8 38 03 68 25 1a 0c 1c 1a 6a 02 06 0a 18 9c 05 a5 1f 31 3c 00 08 0e 75 5e 3d 25 7a 31 a7 3a 07 aa 08 07 09 04 33 75 3a 11 68 10 42 01 01 45 0f 03	.o.._..'Y..QG.YI.2....U..... 5..1.5tl.8.....fu....eYF.. =.....,..5:.1?.c.#.....f[L..S.- ..$.~,.....Y.5..^..1Y..w ....2X.....B..R.8...d:^. ..7...I..%&I;.0-<.....a"o.a./& G.<...;.)...m.....n._..8.h %....j.....1<...u^=%z1.:... ...3u:.h.B..E..	success or wait	1	405823	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\twex.exe,	success or wait	1	40995F	RegSetValueExW

Analysis Process: winlogon.exe PID: 548 Parent PID: 5436

General

Start time:	03:26:37
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