ID: 247445
Sample Name: zeus 1_1.2.3.1.vir
Cookbook: default.jbs
Time: 06:24:17
Date: 20/07/2020
Version: 29.0.0 Ocean Jasper

Table of Contents

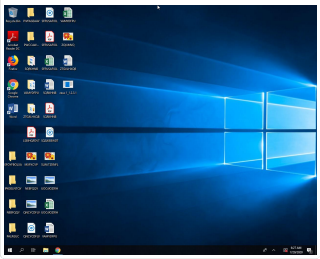
Analysis Report zeus 1_1.2.3.1.vir

Overview

General Information

Sample Name:	zeus 1_1.2.3.1.vir (renamed file extension from vir to exe)
Analysis ID:	247445
MD5:	0797dda9930e3b..
SHA1:	6c21660acf1c1af..
SHA256:	9c01cf666c922c1..

Most interesting Screenshot:



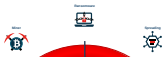
Detection

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
- Antivirus or Machine Learning detec

Classification



Startup

- **System is w10x64**
- zeus 1_1.2.3.1.exe (PID: 2916 cmdline: 'C:\Users\user\Desktop\zeus 1_1.2.3.1.exe' MD5: 0797DDA9930E3B0A7345984D4FBB9509)
  - winlogon.exe (PID: 548 cmdline: MD5: 3E56F9D58EBBB1B33E31B86267DBECFC)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

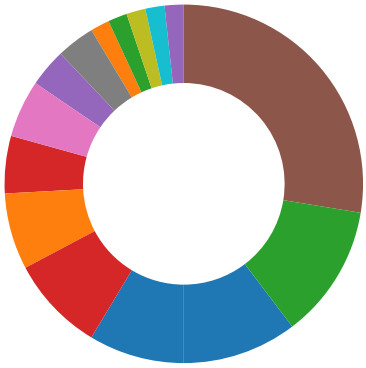
Sigma Overview

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
- 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

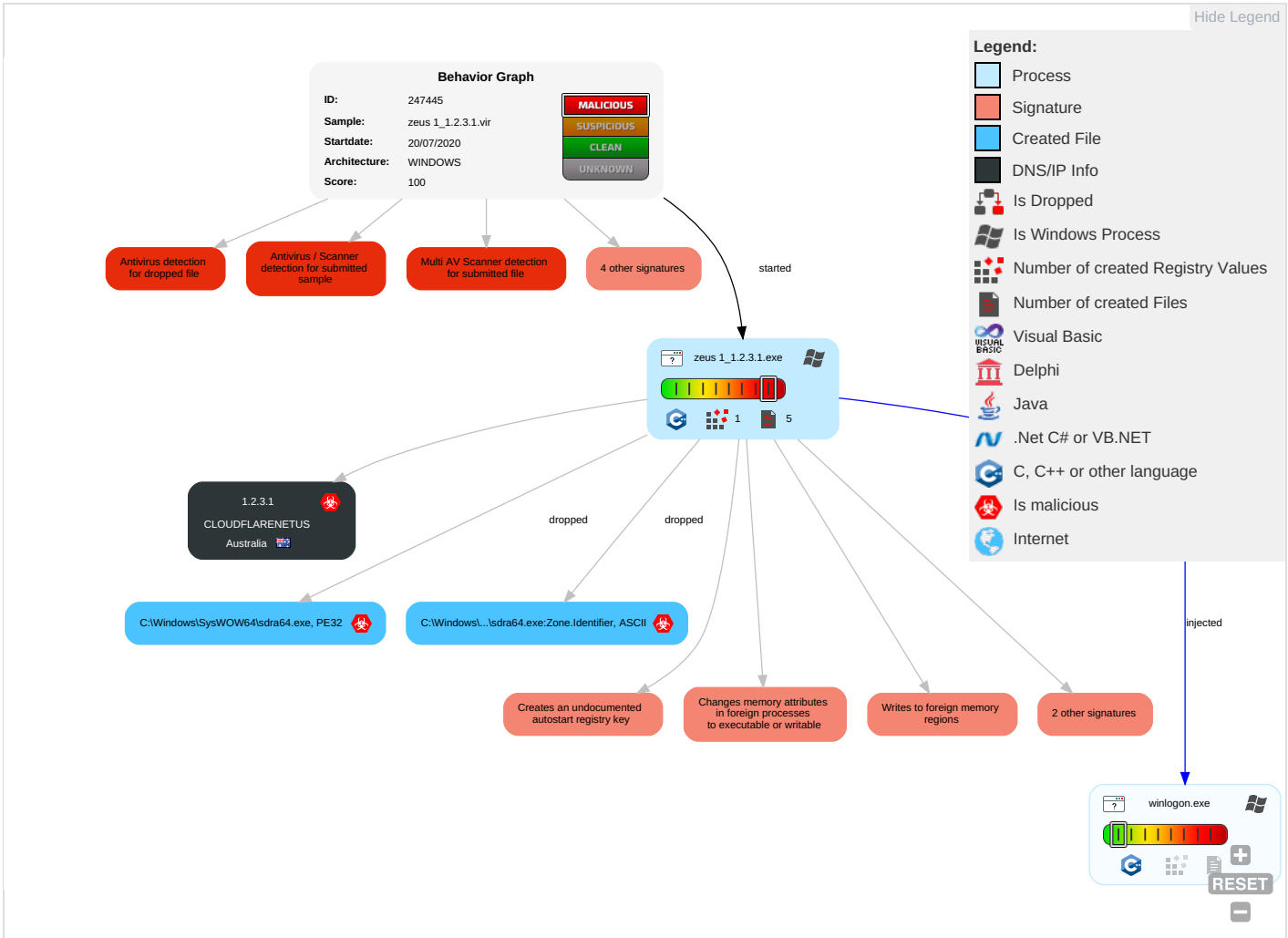
Writes to foreign memory regions

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 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 1	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

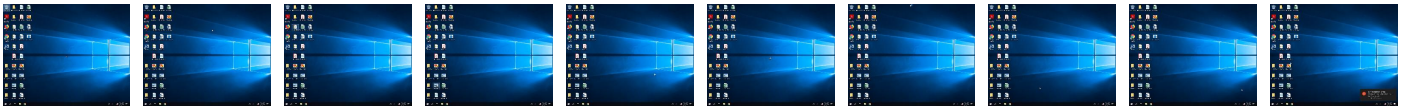
Behavior Graph

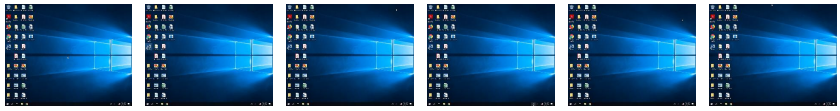


Screenshots

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_1.2.3.1.exe	88%	Virustotal		Browse
zeus 1_1.2.3.1.exe	90%	Metadefender		Browse
zeus 1_1.2.3.1.exe	100%	ReversingLabs	Win32.Spyware.Zbot	
zeus 1_1.2.3.1.exe	100%	Avira	TR/Dropper.Gen	
zeus 1_1.2.3.1.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.14ed0000.356.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
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.15050000.368.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.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.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.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
0.2.zeus 1_1.2.3.1.exe.400000.0.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.12d30000.87.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.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.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.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.14870000.305.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
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.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.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
1.2.winlogon.exe.132b0000.131.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13110000.118.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.12cf0000.85.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.124f0000.21.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.15450000.400.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.131b0000.123.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.14a50000.320.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13d90000.218.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.12eb0000.99.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.12ff0000.109.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13010000.110.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.14370000.265.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.142d0000.260.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.132f0000.133.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.148d0000.308.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13370000.137.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.133d0000.140.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13130000.119.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.13eb0000.227.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.winlogon.exe.14390000.266.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

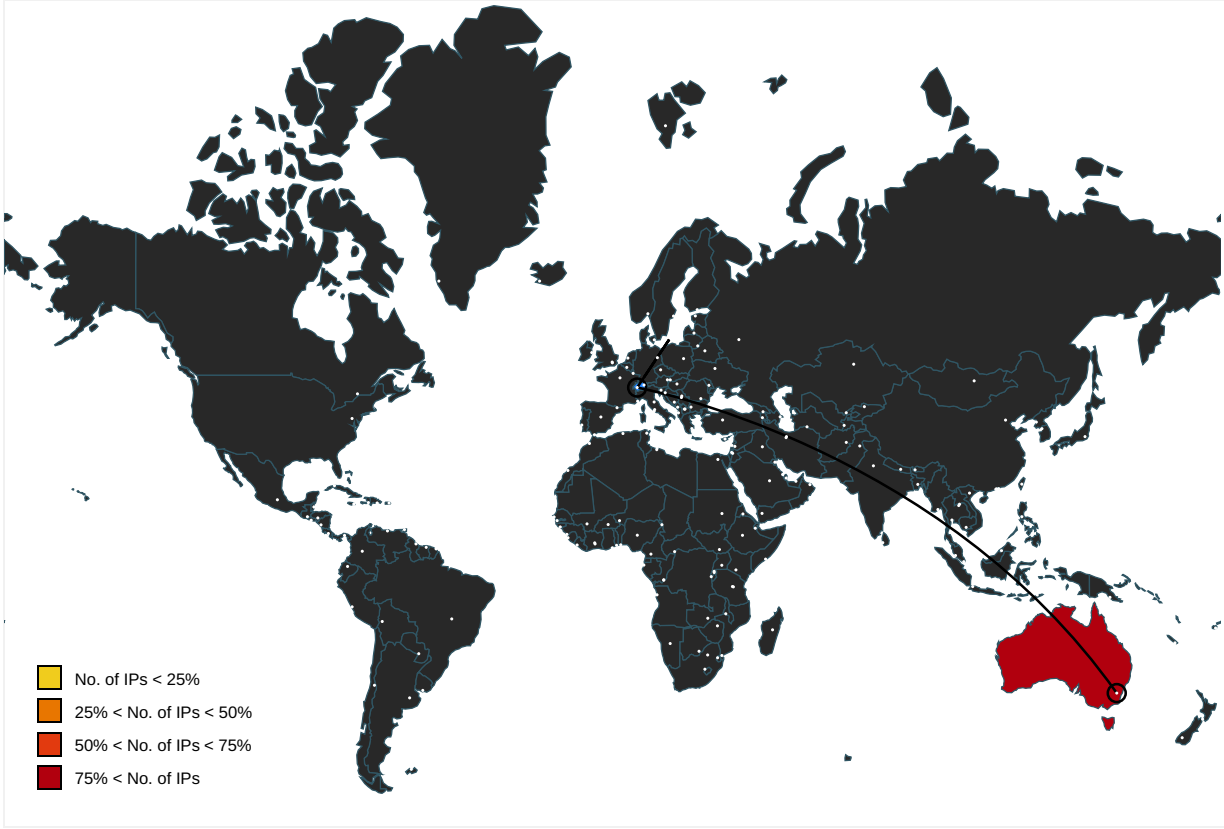
Contacted Domains

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_1.2.3.1.exe, 00000000.0 0000002.1214363661.00000000022 F3000.00000004.00000040.sdmp	false		low

Contacted IPs



Public

IP	Country	Flag	ASN	ASN Name	Malicious
1.2.3.1	Australia		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	29.0.0 Ocean Jasper
Analysis ID:	247445
Start date:	20.07.2020
Start time:	06:24:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	zeus 1_1.2.3.1.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: 97.9% (good quality ratio 92.5%) • Quality average: 83.8% • Quality standard deviation: 27.6%
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_157344 1614.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\sdra64.exe	
Process:	C:\Users\user\Desktop\zeus 1_1.2.3.1.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Size (bytes):	963584
Entropy (8bit):	7.445784291165281
Encrypted:	false
MD5:	8D6D0568C0C3CBB5E60A7CEAC246BB06
SHA1:	CD38C12ECBA493E90E4E0EE68E55DCEADCFD76AB
SHA-256:	990F37D5A6A9FA809BC039D272947DB8E4AFA2FD37B177E1191BC85F28F7A10E
SHA-512:	FED9F4636CC0266E03859952BA8F3772FB24AAD728DC90A8BDAEA47A266E10582143978094080396423DC63C60EA8991DA3EBD2207910C84184A93DB540016AA
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....$.....N....z..z..z.\...yz.....z.....z.....z.....z.....z.}1..z....5z.Rich.z..... .....PE..L....u.H.....Z.....^.....@.....p.....d..... .....text...D..... ..`.rdata.....@..@.data....P.....@..... ....

C:\Windows\SysWOW64\sdra64.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\zeus 1_1.2.3.1.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):	7.466032626413536

General

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_1.2.3.1.exe
File size:	544768
MD5:	0797dda9930e3b0a7345984d4fbb9509
SHA1:	6c21660acf1c1af1eae98aececa607bed5305fe0
SHA256:	9c01cf666c922c17867f4d2a85d090376c6f82e2c77b16de330d116f147fca59
SHA512:	b12cede9810d8176706ae9f089176d16bfaadad3e5b0107629cc3d1f3374a72b7bb12cae12cf909d5ea892eab41e16ed95d3351f07ed3acfde8de30318caada
SSDEEP:	12288:uox9UcsJqj3cW1bpWgSM9n+dPRZXO05us4:V9UfJQf1bIgfWpZX/cs4
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....N....z...z...z..\...yz.....z.....z.....z.....z..}1...z.....5z..Rich.z.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x405e92
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:	0x48E775A7 [Sat Oct 4 13:54:47 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:	7317869d03af58d1e61247d66faab71d

Entrypoint Preview

Instruction
call 00007FD79C68D4E6h
ret
xor esi, esi
push 00000000h
call dword ptr [00410080h]
mov eax, 00000000h
push eax
call dword ptr [00410080h]
xor ecx, ecx
push ecx
call dword ptr [00410080h]
test eax, eax
js 00007FD79C68D4EAh
push 00000000h
call dword ptr [00410080h]

Instruction
or eax, 000000E1h
mov edx, 00000000h
mov dl, al
add esi, edx
cmp esi, 3FEFABF0h
jl 00007FD79C68D4A3h
mov bl, dl
mov ecx, edx
push ecx
push 00000040h
push 00003000h
push 00010608h
push 00000000h
call dword ptr [00410090h]
xor ecx, ecx
pop ecx
mov esi, dword ptr [esp]
add esi, 000000B9h
mov edi, eax
push eax
mov ecx, 000001F5h
mov edx, CABFE433h
mov ebp, 00000000h
mov bh, byte ptr [esi]
inc esi
add bh, bl
add bh, dl
mov byte ptr [edi], bh
inc edi
push edx
push ecx
push 00000000h
call dword ptr [00410080h]
pop ecx
pop edx
and eax, 000000FFh
add eax, 04h
shr edx, 08h
inc ebp
cmp ebp, eax
jne 00007FD79C68D4EEh
mov ebp, CABFE433h
mov edx, ebp
mov ebp, 00000000h
sub ecx, 01h
cmp ecx, 00000000h
jne 00007FD79C68D4A8h
pop eax
mov edx, eax
jmp edx
ret
jl 00007FD79C68D4ADh
in eax, 75h
and bl, ah
inc ecx
add ah, al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x101a4	0x64	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0x10000	0x104	.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	0xea44	0xec00	False	0.870994438559	lif file	7.22640789062	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x10000	0x780	0x800	False	0.53369140625	data	5.37247936763	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x11000	0x50ea	0x200	False	0.111328125	data	0.666094913852	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
USER32.dll	GetWindowThreadProcessId, FindWindowExA, CloseDesktop, GetCursorPos, GetIconInfo, ToUnicode, ExitWindowsEx, GetDlgItemTextA, EndDialog, GetMessageA, SendMessageA, SetProcessWindowStation, OpenWindowStationA, MsgWaitForMultipleObjects, DrawIcon, GetKeyboardState, SetThreadDesktop
ADVAPI32.dll	RegSetValueExA, CryptGetHashParam, DuplicateTokenEx, GetUserNameW, RegDeleteValueA, RegQueryValueExA, CryptDestroyHash, CryptAcquireContextW
KERNEL32.dll	ExpandEnvironmentStringsW, lstrcmpiW, WaitForSingleObject, GetModuleFileNameA, GetCurrentThreadId, GetModuleHandleA, lstrcpynW, VirtualProtect, SetEvent, VirtualAlloc, EnterCriticalSection, ResetEvent, GetSystemTimeAsFileTime, SetFileTime, lstrcatW, GetUserDefaultUILanguage, GetLastError, GetProcAddress, GetAtomNameW, GetFileSizeEx, CreateMutexW, lstrcatA, HeapReAlloc, GetEnvironmentVariableW, MultiByteToWideChar
SHLWAPI.dll	SHDeleteKeyA, wvnsprintfW, PathMatchSpecW, wvnsprintfA, PathFileExistsW, StrCmpNIA, wnsprintfW, PathCombineW, StrStrW, StrCmpNIW, PathRemoveFileSpecW

Network Behavior

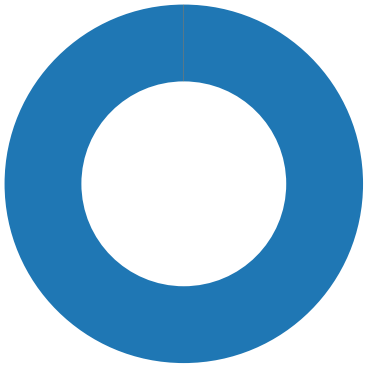
No network behavior found

Code Manipulations

Statistics

Behavior

● zeus 1_1.2.3.1.exe
● winlogon.exe



Click to jump to process

System Behavior

Analysis Process: zeus 1_1.2.3.1.exe PID: 2916 Parent PID: 4952

General

Start time:	06:25:31
Start date:	20/07/2020
Path:	C:\Users\user\Desktop\zeus 1_1.2.3.1.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\zeus 1_1.2.3.1.exe'
Imagebase:	0x400000
File size:	544768 bytes
MD5 hash:	0797DDA9930E3B0A7345984D4FBB9509
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	40599A	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	40599A	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

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 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 10 01 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 4e 1b a2 db 0a 7a cc 88 0a 7a cc 88 0a 7a cc 88 5c f8 a2 88 79 7a cc 88 bd cf af 88 16 7a cc 88 de 13 d8 88 cf 7a cc 88 c1 f9 98 88 bc 7a cc 88 95 bb d0 88 d3 7a cc 88 7d 31 f1 88 de 7a cc 88 f5 cf d1 88 35 7a cc 88 52 69 63 68 0a 7a cc 88 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ.....................@..... ....!..L.!This program cannot be run in DOS mode.... $.......N....z...z...z..\...yz ....z.......z.......z...... .z..}1...z......5z..Rich.z....	success or wait	3	40599A	CopyFileW
C:\Windows\SysWOW64\sdra64.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	40599A	CopyFileW
C:\Windows\SysWOW64\sdra64.exe	unknown	418816	79 a5 03 1a 0f 11 6d 5f 76 82 39 13 67 57 b8 2c 91 6c 4e 35 64 47 2a 38 14 69 21 90 3d 32 12 01 22 45 14 1b 83 15 4a 86 a0 85 07 bd 0a 01 3a 0e ca 36 37 38 00 67 08 0e 27 06 84 23 05 1a 97 5c 00 06 35 f6 16 6a 27 4f 55 10 27 03 02 01 3e 4f 19 4a 8d cb 07 66 09 1e 6a 09 1d 1e 51 21 b8 73 17 0b 00 1e 24 0c 2e 2e 21 4f 19 3e 47 9a 1a a8 01 a2 49 89 4b de 49 be 06 1b 0c 04 53 1a 36 6a 54 4d 5e 04 0a 06 55 1c 88 80 0f 25 73 2e 22 62 07 ac 47 71 36 42 06 7e 96 b4 4c 55 0d 0c 3d 36 12 00 37 09 a7 4d 31 06 13 08 65 4d 0b 0c 2e 08 00 3b d9 3b ed 99 c0 49 14 02 7a 05 40 08 15 2c 02 0b 10 a9 1b 59 42 a4 0c 33 13 48 2a 07 e7 d8 08 70 19 12 09 03 32 13 9d 08 69 05 02 4f 2b 33 34 36 06 a9 21 0e 38 03 6e 0a 39 a2 01 d5 00 7d 0a ac 49 0e 13 72 73 67 22 2e 41 63 07 75 05	y.....m_v.9.gW.,.lN5dG*8.i! .=2.."E.....J.......:..678.g..'..# ...\..5..j'OU.'...>O.J...f..j. ..Q!.s....$...!O.>G.....I.K.I. ....S.6jTM^...U....%s."b..Gq 6B .~..LU..=6..7..M1...eM.....;.; ...I..z.@..,.....YB..3.H*....p ....2...i..O+346..!.8.n.9....} ..I..rsg".Ac.u.	success or wait	1	405A3A	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	40A38A	RegSetValueExW

Analysis Process: winlogon.exe PID: 548 Parent PID: 2916

General

Start time:	06:25:33
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