ID: 247166
Sample Name: zeus 1_1.2.4.10.vir
Cookbook: default.jbs
Time: 22:57:15
Date: 19/07/2020
Version: 29.0.0 Ocean Jasper

Table of Contents

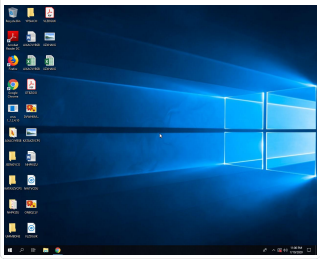
Analysis Report zeus 1_1.2.4.10.vir

Overview

General Information

Sample Name:	zeus 1_1.2.4.10.vir (renamed file extension from vir to exe)
Analysis ID:	247166
MD5:	b9c618bfccb4c70..
SHA1:	e548106618d375..
SHA256:	8df08ecd3c08c6e..

Most interesting Screenshot:



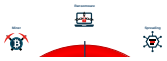
Detection

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 dropp…
- 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…
- PE file has nameless sections

Classification



Startup

- **System is w10x64**
- zeus 1_1.2.4.10.exe (PID: 4600 cmdline: 'C:\Users\user\Desktop\zeus 1_1.2.4.10.exe' MD5: B9C618BFCCB4C700F538415B4A475992)
  - tmp2.exe (PID: 4808 cmdline: C:\Users\user\AppData\Local\Temp\tmp2.exe MD5: A9B2054ADF150709FDB27DEF286008B1)
    - winlogon.exe (PID: 548 cmdline: MD5: 3E56F9D58EBBB1B33E31B86267DBECFC)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

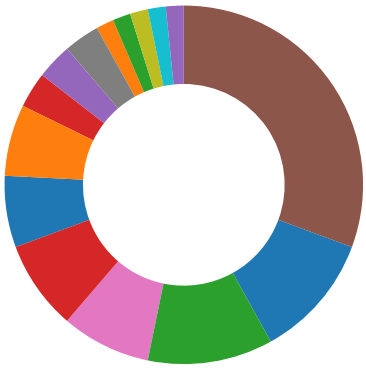
Sigma Overview

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 dropped file
- Multi AV Scanner detection for submitted file
- Machine Learning detection for dropped file
- Machine Learning detection for sample

System Summary:

- PE file has nameless sections

Data Obfuscation:

- Detected unpacking (changes PE section rights)

Boot Survival:

- Creates an undocumented autostart registry key

HIPS / PFW / Operating System Protection Evasion:

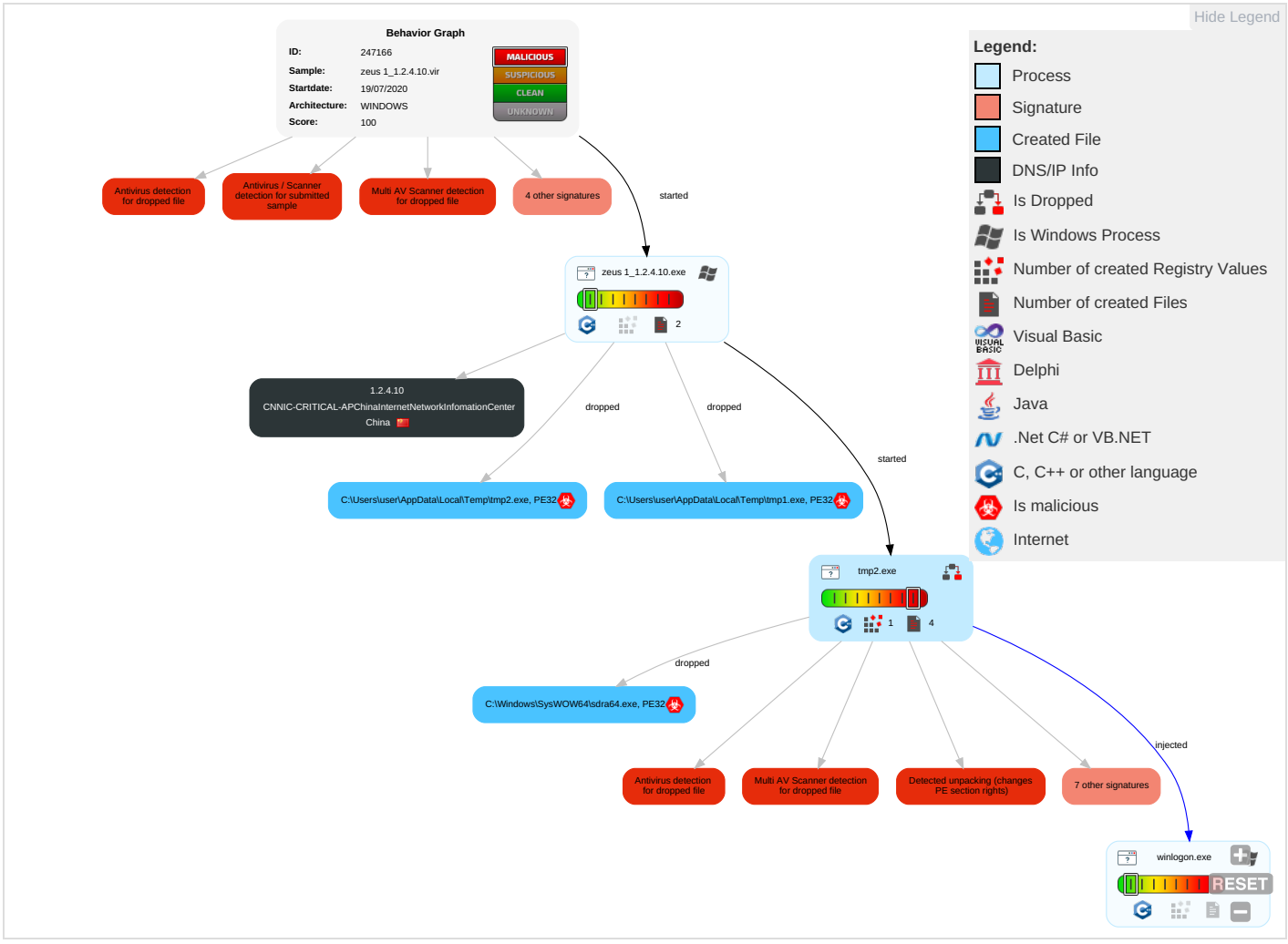
- Allocates memory in foreign processes
- Changes memory attributes in foreign processes to executable or writable
- Contains functionality to change the desktop window for a process (likely to hide graphical interactions)
- Injects a PE file into a foreign processes
- Writes to foreign memory regions

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
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 3	Masquerading 2	Input Capture	Security Software Discovery 1 1	Windows Remote Management	Data from Network Shared Drive	Automated Exfiltration	Standard Cryptographic Protocol 2
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 3	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

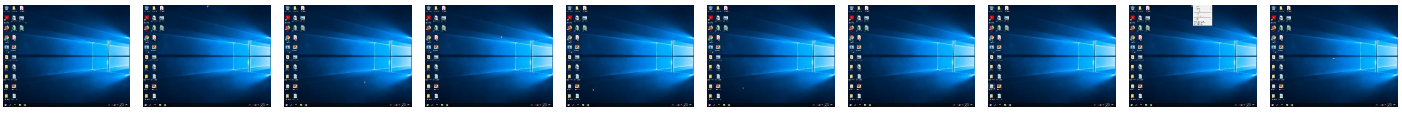
Behavior Graph



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_1.2.4.10.exe	89%	Virustotal		Browse
zeus 1_1.2.4.10.exe	76%	Metadefender		Browse
zeus 1_1.2.4.10.exe	93%	ReversingLabs	Win32.Downloader.Small	
zeus 1_1.2.4.10.exe	100%	Avira	TR/Dropper.Gen	
zeus 1_1.2.4.10.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\tmp2.exe	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Windows\SysWOW64\sdra64.exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Local\Temp\tmp2.exe	100%	Joe Sandbox ML		
C:\Windows\SysWOW64\sdra64.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\tmp1.exe	7%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\tmp1.exe	11%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\tmp1.exe	13%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\tmp2.exe	87%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\tmp2.exe	96%	ReversingLabs	Win32.Spyware.Zbot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.winlogon.exe.2d9c0000.455.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2c0e0000.256.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2d180000.389.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2f420000.666.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2f600000.681.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2c2a0000.270.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2a1e0000.8.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2d020000.378.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2c900000.321.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2c620000.298.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2a140000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2d2c0000.399.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2dac0000.463.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2bce0000.224.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.30be0000.856.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2e3e0000.536.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2a880000.61.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.30220000.778.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2bc20000.218.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.30420000.794.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2a900000.65.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2ce80000.365.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2aee0000.112.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2c8e0000.320.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2b6a0000.174.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2e0a0000.510.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2b180000.133.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2f8c0000.703.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2f020000.634.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2d660000.428.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2d000000.377.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2ccc0000.351.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2d6a0000.430.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2d8c0000.447.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2dd40000.483.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2b5e0000.168.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2df40000.499.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2a3e0000.24.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2b220000.138.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2df00000.497.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2a440000.27.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2e080000.509.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2b200000.137.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2c8a0000.318.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2e740000.563.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.30600000.809.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2abc0000.87.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2b920000.194.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2c880000.317.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2cc60000.348.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2b860000.188.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2b2e0000.144.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2e4e0000.544.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2bb40000.211.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
2.2.winlogon.exe.2a940000.67.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.30c80000.861.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2c260000.268.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2af00000.113.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2bec0000.239.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2aea0000.110.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.305e0000.808.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2a280000.13.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2be60000.236.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.30a80000.845.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2e8a0000.574.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.304e0000.800.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2e720000.562.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2ca20000.330.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.1.tmp2.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
2.2.winlogon.exe.30840000.827.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2dc00000.473.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2a4e0000.32.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.30100000.769.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2d640000.427.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2ec60000.604.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2ffc0000.759.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2b8c0000.191.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.30200000.777.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2dca0000.478.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2c3e0000.280.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2bba0000.214.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2c1a0000.262.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2cda0000.358.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2e6c0000.559.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2efe0000.632.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2b0a0000.126.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2a2a0000.14.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2a9a0000.70.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2fd40000.739.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2d960000.452.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2b060000.124.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2a7c0000.55.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2c280000.269.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.30cc0000.863.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2c060000.252.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.30ae0000.848.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2d6e0000.432.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2a6a0000.46.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.2f820000.698.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

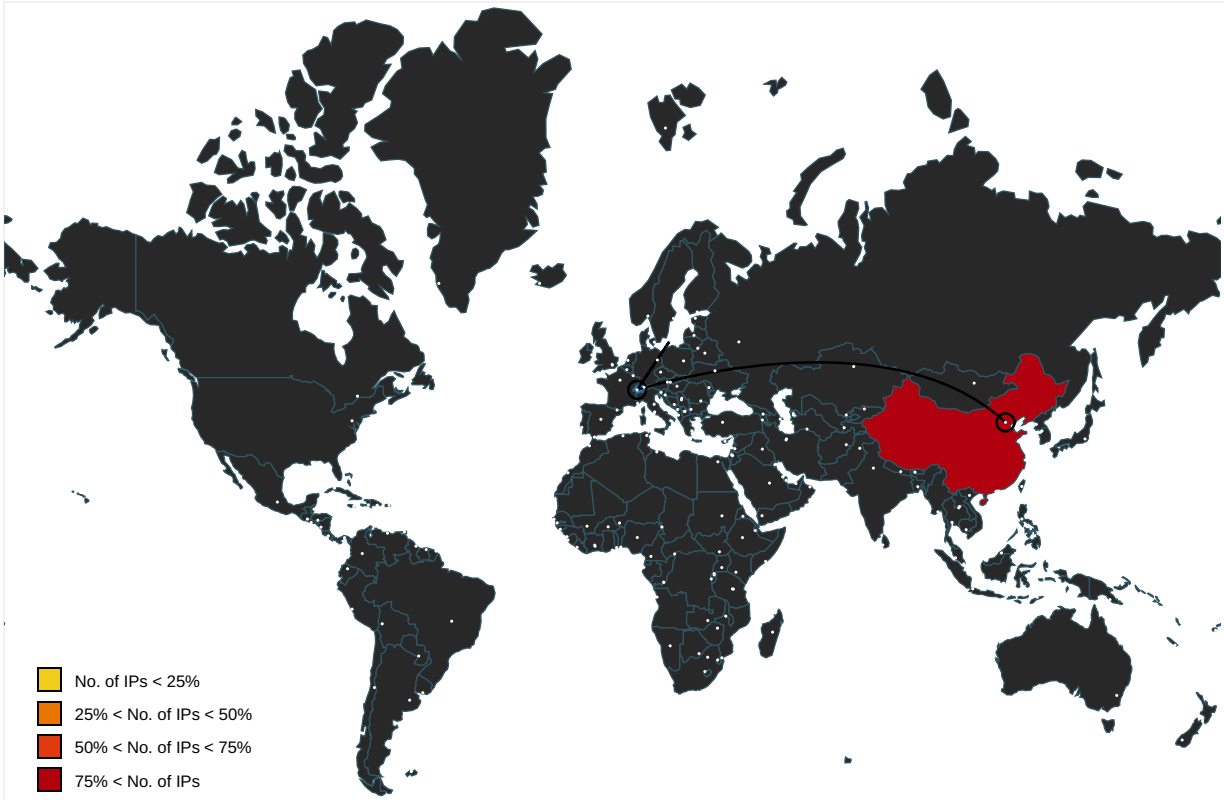
Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://onlineeast#.bankofamerica.com/cgi-bin/ias/	tmp2.exe, 00000001.00000002.866040303.00000000008E3000.00000004.00000040.sdmp	false		low

Contacted IPs



Public

IP	Country	Flag	ASN	ASN Name	Malicious
1.2.4.10	China		24409	CNNIC-CRITICAL-APChinaInternetNetworkInfomationCenter	false

General Information

Joe Sandbox Version:	29.0.0 Ocean Jasper
Analysis ID:	247166
Start date:	19.07.2020
Start time:	22:57:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	zeus 1_1.2.4.10.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:	7
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@4/3@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 81.6% (good quality ratio 65.5%) • Quality average: 53.3% • Quality standard deviation: 37.2%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.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:\Users\user\AppData\Local\Temp\tmp1.exe	
Process:	C:\Users\user\Desktop\zeus 1_1.2.4.10.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Size (bytes):	89760

C:\Users\user\AppData\Local\Temp\tmp1.exe

Entropy (8bit):	6.5522781426620185
Encrypted:	false
MD5:	663E518983B1FDA0BAF822D1EE94F928
SHA1:	520192D4A7ABD4C505C392A2921ED448D1CE0677
SHA-256:	25FC4BC872069973D5F8D758C932A0F81458EAC178E0F4F8380A5FEABF097252
SHA-512:	87E93449465B488C58B97582030AB29E4F1B79BEE5D609D3253004C2252B50D0FA743A0F3ABEA22F0843EF31CADA53DDB6DE89F6BA6CE541BEF2D124EB367D8 3
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 7%, Browse • Antivirus: Metadefender, Detection: 11%, Browse • Antivirus: ReversingLabs, Detection: 13%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....rT...:...:...:.0)...:...;...:.d.g...:.=0&...:...:...:..00...:..01...:. .<...:.Ric h..:.....PE..L.....?.....@...0.....P....@..... .....@...?.....P... .....text....8.....@..... ..`.rdata.....P.....P.....@..@.data..... ....@....data1..... .....@....CRT.....0.....@....rs rc....?...@...@.....@..@Intel(R) C++ Compiler for 32-bit applications, Version 6.0 Build 020321Z : C:\Flashfarm\depot\main\player\branches\FlashPlayer\Fla shPlayer7_DotReleases\core\kraster.cpp : -Qvc6 -Qlocation,link,C:\Program Files\Microsoft Visual Studio\VC98\Bin -nologo -MT -W3 -O2 -I ..\

C:\Users\user\AppData\Local\Temp\tmp2.exe

Process:	C:\Users\user\Desktop\zeus 1_1.2.4.10.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Size (bytes):	67584
Entropy (8bit):	7.125089118081598
Encrypted:	false
MD5:	A9B2054ADF150709FDB27DEF286008B1
SHA1:	5AA4C511122C00257255454CBCAD910AA47C89FE
SHA-256:	23B374A9C51F24DB2749C37E236C2CFE433633CEDD999423EEABC45D5E67B3FE
SHA-512:	37B28222AFAFADDF7B1EDA988C732C4F2386D42EB3F029809FA0B89AA9FB3AF86DAEC02BBE6CE919EFB007867634F66E8F8850EFFF9A7AB3B131119FD87A15 2E
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 87%, Browse • Antivirus: ReversingLabs, Detection: 96%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r.l...?...?...?.=.?y..?z.b?...?.>.?...?@.?n..?1.G?...?Rich...?..... .....PE..L.....G.....V.....[.....@.....p.....d..... .....text...B..... ..`.rdata.....@..@.data....@... .....@..... ....

C:\Windows\SysWOW64\sdra64.exe

Process:	C:\Users\user\AppData\Local\Temp\tmp2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Size (bytes):	363520
Entropy (8bit):	7.482360293904006
Encrypted:	false
MD5:	70D2C3C2191E926393FDF6825D19A934
SHA1:	D04337CE4F6D4C0F49814361EC4B69AA74A2D534
SHA-256:	046033C63D8CF7D86D262BF309A8524B45CBF8DF03F1915E3DCDA9CA9E086C44
SHA-512:	D8FE76EC3D33BE7C73F4EAD73579D01A6EA8D6DB2260F74630306DA0869E6F35D7B33AEB3F87D55F133DC53E08D58AB94067B45262156E4E937582D5CC1F09F
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....$.....r.l...?...?...?.=.?y..?z.b?...?.>.?...?@.?n..?1.G?...?Rich...?..... .....PE..L.....G.....V.....[.....@.....p.....d..... .....text...B..... ..`.rdata.....@..@.data....@... .....@..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.936811523553103
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_1.2.4.10.exe
File size:	160263
MD5:	b9c618bfccb4c700f538415b4a475992
SHA1:	e548106618d37564ec9271cd622f980837e98057
SHA256:	8df08ecd3c08c6e28a5d73869b6c3a980363856cce72dd9a1c2170c75332a451
SHA512:	a59497535a32eb78c25472b10208be8221a6318e465af328de3ecd1a4157673494784f97305f2c0b8a9607f9fd2f03fff380275123eb5bf91613389a3f0d3328
SSDEEP:	3072:wfG1WFOeI3vaxOqyg0Q7eqigDicQ9mZRiSIZGmzpPxYO0q7xEB:m3FGvaEaigeZMZRdlZvpPxYO0Gxw
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....f.TK"v:."v:."v:...i).-v:...V(.#v:.Rich"v:.....PE..L.....C..... ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x401000
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x43830CF1 [Tue Nov 22 12:20:01 2005 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:	ef33d20ab851f174cdd759e358c92fc3

Entrypoint Preview

Instruction
push 00403078h
push 000000FFh
call 00007F1C5C4D2D2Eh
push 00403078h
push dword ptr [0040301Ah]
push dword ptr [00403012h]
push 00403000h
call 00007F1C5C4D2C9Ah
jmp 00007F1C5C4D2C6Ah
mov byte ptr [eax+00403078h], 00000000h
inc eax
cmp byte ptr [eax+00403078h], 00000000h

Instruction
jne 00007F1C5C4D2C51h
push 00403078h
push dword ptr [0040301Eh]
push dword ptr [00403016h]
push 00403009h
call 00007F1C5C4D2C6Ch
push 00000000h
call 00007F1C5C4D2CD8h
push ebp
mov ebp, esp
push eax
push dword ptr [ebp+08h]
push dword ptr [ebp+14h]
call 00007F1C5C4D2CDBh
push 00000000h
push 00000000h
push 00000002h
push 00000000h
push 00000000h
push C0000000h
push dword ptr [ebp+14h]
call 00007F1C5C4D2CA6h
push eax
push dword ptr [ebp+10h]
push dword ptr [ebp+0Ch]
push eax
call 00007F1C5C4D2CB1h
pop eax
push eax
call 00007F1C5C4D2C8Ch
push 00403066h
push 00403022h
push 00000000h
push 00000000h
push 00000020h
push 00000000h
push 00000000h
push 00000000h
push 00403078h
push 00000000h
call 00007F1C5C4D2C76h
pop eax
leave
retn 0010h
jmp dword ptr [00402000h]
jmp dword ptr [00000000h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2020	0x28	.rdata
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	0x2000	0x20	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0xea	0x200	False	0.322265625	data	2.38780990407	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x2000	0xe4	0x200	False	0.294921875	data	2.17351444905	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3000	0x177	0x200	False	0.08203125	data	0.461273696222	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
	0x4000	0x16000	0x16000	False	0.569169477983	PE32 executable (GUI) Intel 80386, for MS Windows	6.53855060715	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
	0x1a000	0x11000	0x10800	False	0.828568892045	PE32 executable (GUI) Intel 80386, for MS Windows	7.12508911808	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
kernel32.dll	CloseHandle, CreateFileA, CreateProcessA, ExitProcess, GetTempPathA, _lwrite, lstrcatA

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

- zeus 1_1.2.4.10.exe
- tmp2.exe
- winlogon.exe

Click to jump to process

System Behavior

Analysis Process: zeus 1_1.2.4.10.exe PID: 4600 Parent PID: 4620

General

Start time:	22:58:43
Start date:	19/07/2020
Path:	C:\Users\user\Desktop\zeus 1_1.2.4.10.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\zeus 1_1.2.4.10.exe'
Imagebase:	0x400000
File size:	160263 bytes
MD5 hash:	B9C618BFCCB4C700F538415B4A475992
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:\Users\user\AppData\Local\Temp\tmp1.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	401085	CreateFileA
C:\Users\user\AppData\Local\Temp\tmp2.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	401085	CreateFileA

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:\Users\user\AppData\Local\Temp\tmp1.exe	unknown	89760	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 f0 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 a3 72 54 b7 e7 13 3a e4 e7 13 3a e4 e7 13 3a e4 be 30 29 e4 e3 13 3a e4 e7 13 3b e4 c6 12 3a e4 64 1b 67 e4 f4 13 3a e4 3d 30 26 e4 e6 13 3a e4 e7 13 3a e4 ee 13 3a e4 e1 30 30 e4 e6 13 3a e4 e1 30 31 e4 2e 13 3a e4 20 15 3c e4 e6 13 3a e4 52 69 63 68 e7 13 3a e4 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 06 00 16 f6 d4 3f 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........rT...:...:...:..0)... :...;...:.d.g...:.=0&...:...:. ..:..00...:..01...:. .<...:.Ri ch..:......................... PE..L......?...	success or wait	1	401092	_lwrite
C:\Users\user\AppData\Local\Temp\tmp2.exe	unknown	67584	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 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 f1 72 9c 6c b5 13 f2 3f b5 13 f2 3f b5 13 f2 3f e7 3d e1 3f 79 13 f2 3f 7a 10 62 3f f1 13 f2 3f 7f 3e ec 3f dd 13 f2 3f 40 e3 b4 3f 6e 13 f2 3f 31 00 47 3f 15 13 f2 3f 52 69 63 68 b5 13 f2 3f 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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........r.l...?...?...?.=.?y..? z.b?...?.>.?...?@..?n..? 1.G?...? Rich...?..................	success or wait	1	401092	_lwrite

Analysis Process: tmp2.exe PID: 4808 Parent PID: 4600

General

Start time:	22:58:43
Start date:	19/07/2020
Path:	C:\Users\user\AppData\Local\Temp\tmp2.exe
Wow64 process (32bit):	true

Commandline:	C:\Users\user\AppData\Local\Temp\tmp2.exe
Imagebase:	0x400000
File size:	67584 bytes
MD5 hash:	A9B2054ADF150709FDB27DEF286008B1
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 87%, Virustotal, Browse • Detection: 96%, ReversingLabs
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	405AB6	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\sdra64.exe	0	67584	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 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 f1 72 9c 6c b5 13 f2 3f b5 13 f2 3f b5 13 f2 3f e7 3d e1 3f 79 13 f2 3f 7a 10 62 3f f1 13 f2 3f 7f 3e ec 3f dd 13 f2 3f 40 e3 b4 3f 6e 13 f2 3f 31 00 47 3f 15 13 f2 3f 52 69 63 68 b5 13 f2 3f 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	MZ.....................@..... ....!..L.!This program cannot be run in DOS mode.... $........r.l...?...?...?.=.?y..? z.b?...?.>.?...?@..?n..? 1.G?...?Rich...?.................	success or wait	1	405AB6	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\sdra64.exe	unknown	295936	61 3c 06 16 c1 76 12 1c 18 1d 28 c7 00 69 59 c5 52 19 7c 35 2f 3c 84 d3 2b ef 66 64 0a 47 2e 05 48 3c 72 3d 26 38 ab 17 c5 4c 28 ca 35 47 19 08 37 44 2d 29 53 03 95 41 04 58 01 03 29 d0 6b 53 03 1d 71 2d 01 13 2d 52 00 0b 74 7a 32 66 11 17 02 30 30 03 30 af 82 01 9a 14 5f 24 56 16 41 1b 3e 7f 59 0b 1f 26 29 1e 1f 2c 6b 4f 00 00 af 09 35 68 43 0b 02 e0 97 34 07 d4 05 0f 59 51 14 3f 27 07 55 15 01 6c 78 6d 14 77 01 21 0b c9 1a 97 0b 3f 22 63 44 73 7b 6b 02 d1 5e 31 32 31 34 8e 08 32 3b a4 01 17 38 45 81 04 97 0d 42 3c 8e 98 44 56 bc 07 40 33 30 62 37 10 4e 5b 60 09 0f 27 14 34 46 31 19 66 60 69 0b e1 54 36 45 2d 3f 7b 63 27 44 1f 08 25 74 18 0c 28 91 1f 14 17 9f 4e 30 03 a4 44 0a 38 1e 24 09 11 35 9e 33 5c 0b 39 07 1f 32 4e 43 2e 0f a2 5a 5c 17 0c 15 0a 60	a<...v....(..iY.R.|5/<..+.fd.G ..H<r=&8...L(.5G..7D-)S..A.X..).kS..q-..- R..tz2f...00.0..... _$V.A.>.Y..&)..,kO....5hC... .4 ....YQ.?'.U..lxm.w.!.....?"cD s {k..^1214..2;...8E....B<..DV ..@30b7.N[`..'.4F1.f`i..T6E- ?{c'D..%t.. (.....N0..D.8.$..5.3\.9 ..2NC...Z\....`	success or wait	1	405B54	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	40A4AF	RegSetValueExW

Analysis Process: winlogon.exe PID: 548 Parent PID: 4808

General

Start time:	22:58:45
Start date:	19/07/2020
Path:	C:\Windows\System32\winlogon.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6893a0000
File size:	677376 bytes
MD5 hash:	3E56F9D58EBBB1B33E31B86267DBECFC
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

Code Analysis