ID: 409287
Sample Name: P8jE8nmN7G
Cookbook: default.jbs
Time: 20:35:16
Date: 09/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

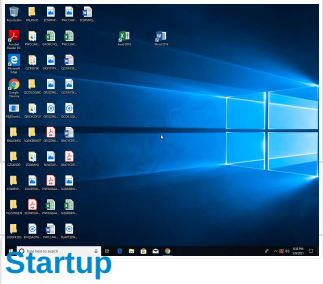
Analysis Report P8jE8nmN7G

Overview

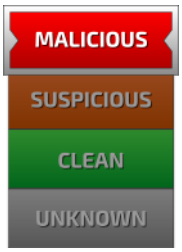
General Information

Sample Name:	P8jE8nmN7G (renamed file extension from none to exe)
Analysis ID:	409287
MD5:	ac514dce9416eb..
SHA1:	b0e1d96605cdc3..
SHA256:	67334c1b7f629c0..
Tags:	zeus1
Infos:	

Most interesting Screenshot:



Detection

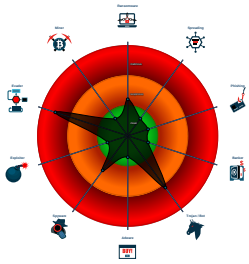


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 VNC / remote desktop func…
- 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

Classification



Startup

- **System is w10x64**
- P8jE8nmN7G.exe (PID: 4860 cmdline: 'C:\Users\user\Desktop\P8jE8nmN7G.exe' MD5: AC514DCE9416EB9E4148431016629174)
  - winlogon.exe (PID: 560 cmdline: MD5: F9017F2DC455AD373DF036F5817A8870)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

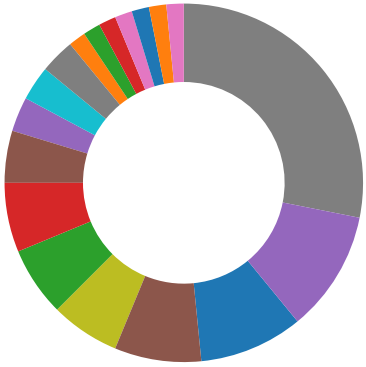
Sigma Overview

System Summary:

Sigma detected: Windows Processes Suspicious Parent Directory

Signature Overview

- AV Detection
- Cryptography
- Compliance
- Spreading



- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- Protection of GUI
- 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

Remote Access Functionality:

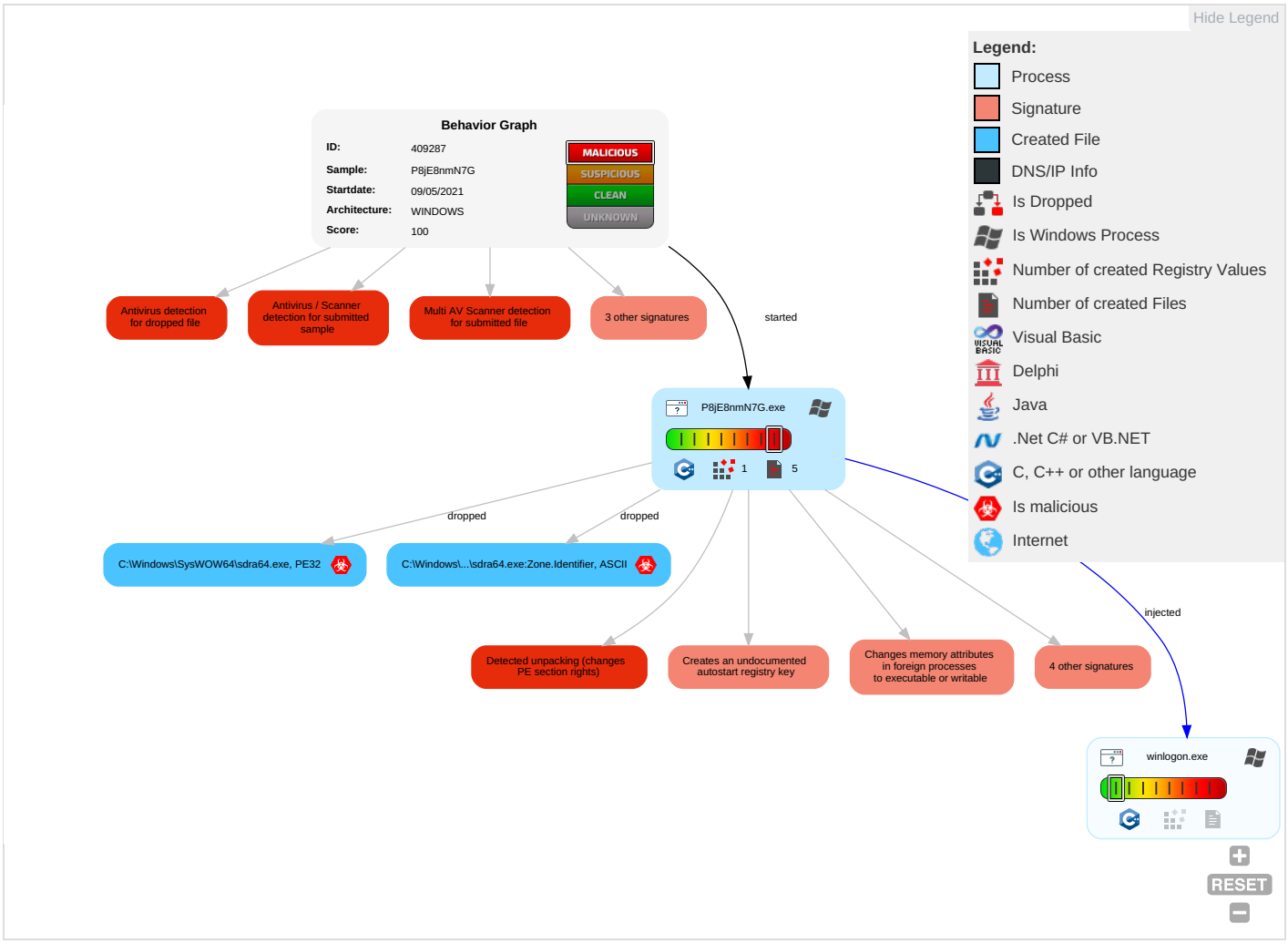
Contains VNC / remote desktop functionality (version string found)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts 1	Native API 1	DLL Side-Loading 1	DLL Side-Loading 1	Obfuscated Files or Information 2	Input Capture 2 1	System Time Discovery 2	Remote Desktop Protocol 1	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eave Insec Netw Comi

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Default Accounts	Scheduled Task/Job	Application Shimming 1	Application Shimming 1	Install Root Certificate 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Encrypted Channel 2	Explo Redir Calls
Domain Accounts	At (Linux)	Create Account 1	Valid Accounts 1	Software Packing 1 3	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Remote Access Software 1	Explo Track Local
Local Accounts	At (Windows)	Valid Accounts 1	Access Token Manipulation 1 1	DLL Side-Loading 1	NTDS	System Information Discovery 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM (Swap
Cloud Accounts	Cron	Registry Run Keys / Startup Folder 1	Process Injection 4 2	Masquerading 2	LSA Secrets	Security Software Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mani Devic Comm
Replication Through Removable Media	Launchd	Rc.common	Registry Run Keys / Startup Folder 1	Valid Accounts 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamr Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1	DCSync	Process Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1 1	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Proto
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 4 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogu Base

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
P8jE8nmN7G.exe	80%	Virustotal		Browse
P8jE8nmN7G.exe	96%	ReversingLabs	Win32.Trojan.Zeus	
P8jE8nmN7G.exe	100%	Avira	TR/Dropper.Gen	
P8jE8nmN7G.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
2.2.winlogon.exe.d6a0000.108.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.d1a0000.68.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.1.P8jE8nmN7G.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
2.2.winlogon.exe.d8a0000.124.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.P8jE8nmN7G.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.fa60000.394.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.10760000.498.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
2.2.winlogon.exe.d740000.113.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.f440000.345.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.d1c0000.69.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.10800000.503.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.eaa0000.268.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.e060000.186.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.fae0000.398.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.100c0000.445.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.dfa0000.180.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.f260000.330.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.e5e0000.230.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.e480000.219.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.fa40000.393.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.dfe0000.182.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.fa80000.395.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.106c0000.493.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.e660000.234.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.e7c0000.245.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.ed20000.288.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.f920000.384.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.fd20000.416.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.ebe0000.278.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.d5a0000.100.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.fb80000.403.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.efa0000.308.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.d2e0000.78.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.f420000.344.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.f540000.353.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.f580000.355.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.e7e0000.246.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.c960000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.e360000.210.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.d960000.130.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.10160000.450.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.e6e0000.238.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.f9e0000.390.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.f9a0000.388.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.db00000.143.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.eac0000.269.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.cfe0000.54.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.ce40000.41.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.10620000.488.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.d040000.57.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.e9a0000.260.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.10960000.514.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.ca00000.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.102c0000.461.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.d880000.123.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.cbc0000.21.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.10720000.496.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.d7a0000.116.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.df20000.176.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.efe0000.310.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.10680000.491.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.f1a0000.324.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.f960000.386.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.103e0000.470.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.ea40000.265.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.cc80000.27.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.f720000.368.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.dc40000.153.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.cf60000.50.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.10280000.459.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
2.2.winlogon.exe.ec40000.281.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.cea0000.44.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.f2e0000.334.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.e880000.251.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.e3a0000.212.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.ca60000.10.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.10300000.463.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.fbe0000.406.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.f940000.385.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.f240000.329.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.108e0000.510.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.f400000.343.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.e0e0000.190.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.d140000.65.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.cba0000.20.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.100e0000.446.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.f5e0000.358.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.10460000.474.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.e720000.240.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.e940000.257.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.e620000.232.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.fec0000.429.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.fd00000.415.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.d9a0000.132.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.eb20000.272.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.cb80000.19.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.d940000.129.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.f460000.346.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.de00000.167.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://onlineeast#.bankofamerica.com/cgi-bin/ias/	0%	Avira URL Cloud	safe	

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/	P8jE8nmN7G.exe, 00000000.00000002.464936104.0000000002563000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs

No contacted IP infos

General Information

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	409287
Start date:	09.05.2021
Start time:	20:35:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	P8jE8nmN7G (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	23
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.troj.evad.winEXE@1/2@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 87.2% (good quality ratio 82.8%) • Quality average: 83.4% • Quality standard deviation: 27.7%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Windows\SysWOW64\sdra64.exe	
Process:	C:\Users\user\Desktop\P8jE8nmN7G.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	960512
Entropy (8bit):	7.4471687140914185
Encrypted:	false
SSDEEP:	24576:+Vy+qcRpdmAA4xiaUG5al4+0JgF8VDn50JTJtFW1a7wt:V+tTmIzD4O+4gF+5Qjka7+
MD5:	8834EA3D0BD0092967199887FAA44929
SHA1:	411441B2883B67FECDC085B6E5F7E7F51D68AA90
SHA-256:	2C3A335C1B7760346149BEC5BE904E9DD6289E18C81A5264E5C8C073D58DDE03
SHA-512:	42E28B003961CC94D9F26AE5C347AD972A45283B4213123F818BC4F76829E54BC33C22ACD92BEBA3EE4A22E5FFC82163F9FBB4E82BA9DB6E68C051DB840D6CDE
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....$.....".R.C...C...C..Zg2..C..4...C..N.F..C...)0..C..\|...GC..Rich.C..... .....PE..L....G0G..... ...v.....Tt.....0....@.....5..x..... .....0.....text..... ....`.rdata..@#...0...$...$.....@..@.data...}P...`.....H.....@..... ....

C:\Windows\SysWOW64\sdra64.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\P8jE8nmN7G.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
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):	7.463091044475583

General

TrID:	• Win32 Executable (generic) a (10002005/4) 99.83% • Windows Screen Saver (13104/52) 0.13% • 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:	P8jE8nmN7G.exe
File size:	602112
MD5:	ac514dce9416eb9e4148431016629174
SHA1:	b0e1d96605cdc3da995a667a1fdc7189b67bfdcd
SHA256:	67334c1b7f629c04efefbfb466e5996a425af4a43c07a5ce51d4f142222b0de7
SHA512:	8c485630cae11e23c5eb790aa061681fe161ea390e07731ea7742a9f029806f43eb432eb08af280b301e889a6b4932ae6c6b436b8d78afb333e5cf0ba8e8907a
SSDEEP:	12288:+VZuL+Kd3LSbFPFX3PL2w5+9naFA4xixYUSl5alHY+0JgKsOaRC:+Vy+qcRpdmAA4xiaUG5al4+0JgFU
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....".R.C...C...C..Zg2..C..4....C..N.F..C...)0..C..|...GC..Rich.C.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x407454
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:	0x4730479C [Tue Nov 6 10:53:16 2007 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:	fbbf51b163121df5cf4fc9419aafa3af

Entrypoint Preview

Instruction
call 00007FE68087D0EBh
xor edi, edi
pop esi
retn 0028h
xor esi, esi
push 0000000Eh
push 00681494h
push 00FFFE7Ch
push 00000001h
push 00AAC0FBh
push 00000000h
call dword ptr [004130FCh]
mov edx, eax
or edx, 000000BEh

Instruction
add esi, edx
push edx
push 00000000h
call dword ptr [00413100h]
pop ebx
cmp esi, 08407BE0h
jnl 00007FE68087D0E4h
jmp 00007FE68087D0A9h
mov eax, 0001362Fh
add eax, 5Bh
mov ecx, edx
sub esp, 04h
mov dword ptr [esp], ecx
sub esp, 04h
mov dword ptr [esp], 00000040h
sub esp, 04h
mov dword ptr [esp], 00003000h
push eax
sub esp, 04h
mov dword ptr [esp], 00000000h
call dword ptr [004130F8h]
pop ecx
mov ecx, esi
mov esi, dword ptr [esp]
mov edi, eax
add esi, 000000F3h
push eax
mov ecx, 000001E6h
mov edx, 137D02D9h
mov ebp, 00000000h
mov bh, dl
add bh, byte ptr [esi]
add esi, 01h
mov byte ptr [edi], bh
add byte ptr [edi], bl
add edi, 01h
sub esp, 04h
mov dword ptr [esp], edx
sub esp, 04h
mov dword ptr [esp], ecx
push 0000001Dh
push 0000001Eh
push 00FFFC60h
push 00000005h
push 006D2D0Ch
push 00000000h
call dword ptr [000000FCh]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x135c8	0x78	.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	0x13000	0x4e0	.rdata

Name	Virtual Address	Virtual Size	Is in Section
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	0x11f89	0x12000	False	0.879055447049	data	7.22037238545	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x13000	0x2340	0x2400	False	0.452256944444	data	5.58339650142	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x16000	0x507d	0x200	False	0.13671875	data	0.819758377798	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.dll	FatalAppExitW, WriteTapemark, CreatePipe, FindClose, GetWindowsDirectoryA, FatalAppExitA, TerminateProcess, ReadConsoleW, MoveFileExW, GetPrivateProfileSectionW, CreateProcessA, DebugBreak, VerLanguageNameA, WaitForSingleObject, ReleaseMutex, OpenWaitableTimerW, GetQueuedCompletionStatus, LocalSize, lstrcpyn, GetProcAddress, GetLogicalDriveStringsA, FlushViewOfFile, GetCurrentProcess, BackupSeek, SystemTimeToTzSpecificLocalTime, SetConsoleCP, InitAtomTable, HeapCompact, WriteProfileStringA, FindNextFileW, GetDateFormatA, GetNumberFormatA, CommConfigDialogA, RemoveDirectoryA, ReadConsoleOutputCharacterA, IsBadCodePtr, GetFileAttributesA, GetProcessPriorityBoost, WriteFileEx, ConvertDefaultLocale, IsBadReadPtr, CreateSemaphoreA, Toolhelp32ReadProcessMemory, SetThreadPriority, SuspendThread, GetProcessAffinityMask, CreateMailslotW, VirtualProtect, SetConsoleTitleA, GetCurrentThread, VirtualProtectEx, ReadConsoleOutputA, EnumCalendarInfoExA, FindFirstChangeNotificationA, lstrcpyW, GetFileInformationByHandle, DebugActiveProcess, DisableThreadLibraryCalls, SetLocaleInfoA, OpenEventW, FreeLibraryAndExitThread, EnumSystemCodePagesA, VirtualAlloc, MapViewOfFileEx, GetFileType
ole32.dll	GetHookInterface, CoRevertToSelf, OleDraw, OleBuildVersion, OleCreateFromFile, StgCreateDocfileOnILockBytes, OpenOrCreateStream, OleCreateFromData, CreateAntiMoniker, GetHGlobalFromStream, OleSetMenuDescriptor, ReleaseStgMedium, ReadStringStream, CoFileTimeToDosDateTime, OleCreateEmbeddingHelper, RegisterDragDrop, GetHGlobalFromILockBytes, OleConvertIStorageToOLESTREAM, DllDebugObjectRPCHook, UtGetDvtd16Info, OleMetafilePictFromIconAndLabel, CoRevokeClassObject, ReadOleStg, CoRegisterMessageFilter, CreateGenericComposite, CreateStreamOnHGlobal, IsEqualGUID, OleRegEnumFormatEtc, CoFreeLibrary, CoGetTreatAsClass, OleSave, StgOpenAsyncDocfileOnIFillLockBytes, CoCopyProxy, CoIsOle1Class, CoBuildVersion, CoGetCurrentLogicalThreadId, CoReleaseMarshalData, CoQueryAuthenticationServices, OleConvertOLESTREAMToIStorageEx, CreateClassMoniker, CoImpersonateClient, StgOpenStorageEx, CoRevokeMallocSpy, OleCreate, CoUnmarshalInterface, CoGetCurrentProcess, CreateDataCache, StringFromGUID2, CoTreatAsClass, StgOpenStorage, OleCreateLinkFromData, OleGetIconOfFile, OleTranslateAccelerator, CreateDataAdviseHolder, OleCreateLinkEx, CoGetCallerTID, CoTaskMemRealloc, UtConvertDvtd32toDvtd16
ADVAPI32.dll	CryptEnumProvidersW, CryptSetProviderA, QueryServiceObjectSecurity, LookupPrivilegeValueA, CryptEnumProviderTypesA, LookupSecurityDescriptorPartsW, GetLengthSid, CopySid, BuildSecurityDescriptorW, SetSecurityDescriptorDacl, RegQueryValueW, BuildTrusteeWithSidW, SetEntriesInAuditListA, BuildTrusteeWithNameW, CryptSetProvParam, RegReplaceKeyA, OpenBackupEventLogA, RegSaveKeyA, RegisterEventSourceW, UnlockServiceDatabase, LookupAccountNameA, CloseServiceHandle, GetSidSubAuthorityCount, CryptAcquireContextW, SetServiceStatus, OpenThreadToken, CryptGetDefaultProviderW, RegEnumKeyExW, AreAnyAccessesGranted, GetOldestEventLogRecord, CryptSetHashParam, CryptContextAddRef, StartServiceW, RegSetValueExA, ReadEventLogW, GetCurrentHwProfileW, GetSecurityDescriptorGroup, GetMultipleTrusteeOperationA, CryptGenRandom, ChangeServiceConfigA, SetNamedSecurityInfoExA, GetAccessPermissionsForObjectW, AddAuditAccessAce, GetOverlappedAccessResults, RegCreateKeyW, SetSecurityDescriptorSacl, LookupAccountSidA, ReportEventA, CryptSignHashW, RegQueryMultipleValuesW, DeregisterEventSource, CancelOverlappedAccess, RegQueryValueExW, OpenBackupEventLogW, BackupEventLogW, CryptDecrypt, AccessCheckAndAuditAlarmA, CreateProcessAsUserA, InitializeSecurityDescriptor, RegEnumKeyA, SetTokenInformation, AddAccessDeniedAce, RegCreateKeyExA, GetTokenInformation, IsValidAcl, RegCreateKeyExW, LookupPrivilegeNameW
SHLWAPI.dll	PathMakePrettyA, SHEnumKeyExW, PathCompactPathExA, SHDeleteKeyA, UrlEscapeA, SHCreateStreamOnFileW, PathIsUNCServerA, PathFindExtensionA, SHRegDeleteUSValueA, PathFindSuffixArrayW, PathIsUNCServerW, SHRegGetUSValueW, StrCmpNA, SHRegEnumUSValueA, StrStrIA, SHSetValueW, SHOpenRegStream2A, PathIsNetworkPathA, StrCpyNW, StrRChrIW, PathSkipRootA, UrlHashA, SHRegDeleteEmptyUSKeyW, PathGetArgsA, StrRetToBufA, SHRegOpenUSKeyA, StrCatBuffW, PathRemoveArgsA, ChrCmpIA, PathBuildRootA, SHRegDeleteUSValueW, PathCompactPathA, PathIsRootW, PathSearchAndQualifyW, wnsprintfW, StrToIntW, SHQueryInfoKeyA, PathAddBackslashW, StrCmpNW, UrlUnescapeA, StrCSpnIA, SHStrDupW, PathRemoveFileSpecW, StrFormatKBSizeA, SHSetThreadRef, StrCSpnA, SHRegDuplicateHKey, UrlCanonicalizeA, UrlIsOpaqueW, SHQueryValueExA, PathCommonPrefixA, StrChrW, SHRegSetUSValueW, PathRemoveExtensionA, wvnsprintfA, PathIsDirectoryA, SHEnumValueW, StrRetToStrA, UrlEscapeW, StrCSpnIW, UrlIsW, PathStripToRootA
USER32.dll	IsRectEmpty, GetSubMenu, DialogBoxParamW, ReleaseCapture, ExitWindowsEx, LoadCursorW, EndDialog, MessageBoxIndirectW, GetMenuState, TranslateMessage, SetLastErrorEx, CreateDialogParamA, GetTabbedTextExtentW, SetDlgItemTextA, GetMenuInfo, CharLowerBuffW, DdeConnect, EnumThreadWindows, UnregisterClassA, ChangeDisplaySettingsExW, TrackPopupMenuEx, SetCursorPos, GetMenuItemRect, GetCaretBlinkTime, IsMenu, GetThreadDesktop, SetPropA, GetClipboardOwner, EnumPropsExW, GetClipboardFormatNameA, DrawEdge, GetMenuCheckMarkDimensions, IsChild, DrawStateW, GetAncestor, FillRect, DlgDirListComboBoxW, WinHelpA, EnumClipboardFormats, SetPropW, EnumDisplayMonitors, GetWindowInfo, EnumDisplaySettingsA, CharUpperW, LookupIconIdFromDirectoryEx, GetQueueStatus, GetMessageTime, GetKeyboardState, DdeAddData, SendMessageTimeoutA, EnumDesktopsA, SetWindowPos, InvalidateRect, SetMessageExtraInfo, SetClipboardData

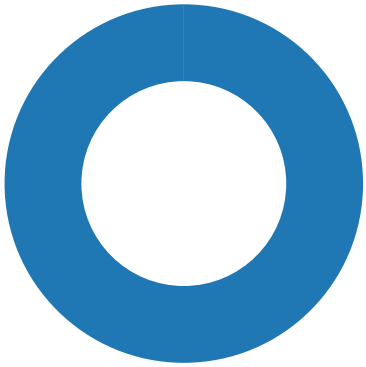
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



P8jE8nmN7G.exe
winlogon.exe

Click to jump to process

System Behavior

Analysis Process: P8jE8nmN7G.exe PID: 4860 Parent PID: 5760

General

Start time:	20:35:59
Start date:	09/05/2021
Path:	C:\Users\user\Desktop\P8jE8nmN7G.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\P8jE8nmN7G.exe'
Imagebase:	0x400000
File size:	602112 bytes
MD5 hash:	AC514DCE9416EB9E4148431016629174
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	406467	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	406467	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\sdra64.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 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 8b 22 e2 52 cf 43 8c 01 cf 43 8c 01 cf 43 8c 01 5a 67 32 01 d4 43 8c 01 34 c6 91 01 95 43 8c 01 4e d7 46 01 c7 43 8c 01 e2 29 30 01 9b 43 8c 01 7c b8 de 01 47 43 8c 01 52 69 63 68 cf 43 8c 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........".R.C...C...C..Zg2..C ..4....C..N.F..C...)0..C..|... GC..Rich.C....................	success or wait	3	406467	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	406467	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\sdra64.exe	unknown	358400	23 1d 21 59 04 d4 cb 0b 39 3b 34 2b 04 5a 0e 35 34 28 04 3f 03 48 40 6f 47 0a 38 63 23 10 39 17 44 4d 1c 47 08 2d 65 08 93 9f 63 13 47 22 1f 98 08 01 68 00 2e 57 27 10 10 17 0d 99 06 dc 0a 08 2d 3b 05 56 19 95 24 12 8d 3d 1f 06 1e 72 65 63 42 4f 0c 11 64 33 28 51 1b 08 74 7f 37 00 35 1c ba 96 01 01 56 05 21 01 98 48 07 25 29 02 a9 11 33 31 23 21 3e 36 83 10 10 71 44 03 45 0e 23 16 8f 3c 63 7e 72 5f 04 05 42 61 51 0d 12 3a 93 15 c1 08 54 ce 0a ee 85 96 12 4a 2e 5e 0d 10 2d 4a 16 c7 03 48 43 2e 2e 19 2d 4f 6f 46 3f 27 1b 02 76 2c 13 0a 04 08 0e af 14 00 08 36 04 22 4e 6d 1a 15 6e 01 00 3f 66 37 9c 3a 04 1b 05 05 2a 22 00 1d f8 88 26 0c ac 25 16 00 28 24 09 02 01 1a 01 5b 89 c6 53 20 35 0a 8b 5a 28 40 07 4e 1a 1a 17 0f 8c 36 36 31 b3 03 01 b4 02 49 21 21 05	#.!Y....9;4+.Z.54(.?.H@oG.8c#.9.DM.G.-e...c.G"....h..W'.....-;.V..$..=...recBO..d3(Q..t.7.5.....V.!..H.%)...31#!>6..qD.E.#..<c~r_..BaQ..:....T......J.^..-J...HC...-OoF?'..v,..6."Nm..n..?f7.:....*"..&..%..($.....[..S 5..Z(@.N...661.....I!!.	success or wait	1	406505	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	40BDAA	RegSetValueExW

Analysis Process: winlogon.exe PID: 560 Parent PID: 4860

General

Start time:	20:36:00
Start date:	09/05/2021
Path:	C:\Windows\System32\winlogon.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff739090000
File size:	677376 bytes
MD5 hash:	F9017F2DC455AD373DF036F5817A8870
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

Code Analysis