ID: 381781
Sample Name: Ue0N2amgcH
Cookbook: default.jbs
Time: 02:57:32
Date: 05/04/2021
Version: 31.0.0 Emerald

Table of Contents

Analysis Report Ue0N2amgcH

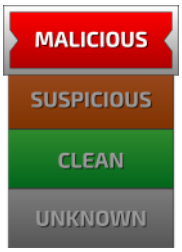
Overview

General Information

Sample Name:	Ue0N2amgcH (renamed file extension from none to exe)
Analysis ID:	381781
MD5:	ccb2db4a8a284f6..
SHA1:	b2bdb5ed1ff7431..
SHA256:	4fb04b099a37aea.
Tags:	zeus1
Infos:	

Most interesting Screenshot:

Detection

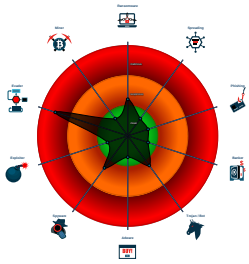


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 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**
- Ue0N2amgcH.exe (PID: 6080 cmdline: 'C:\Users\user\Desktop\Ue0N2amgcH.exe' MD5: CCB2DB4A8A284F62DB7002BE470AC542)
  - winlogon.exe (PID: 560 cmdline: MD5: F9017F2DC455AD373DF036F5817A8870)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

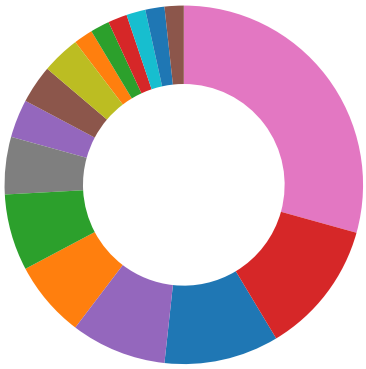
Sigma Overview

System Summary:

Sigma detected: Windows Processes Suspicious Parent Directory

Signature Overview

- AV Detection
- Cryptography
- Compliance



- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- 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

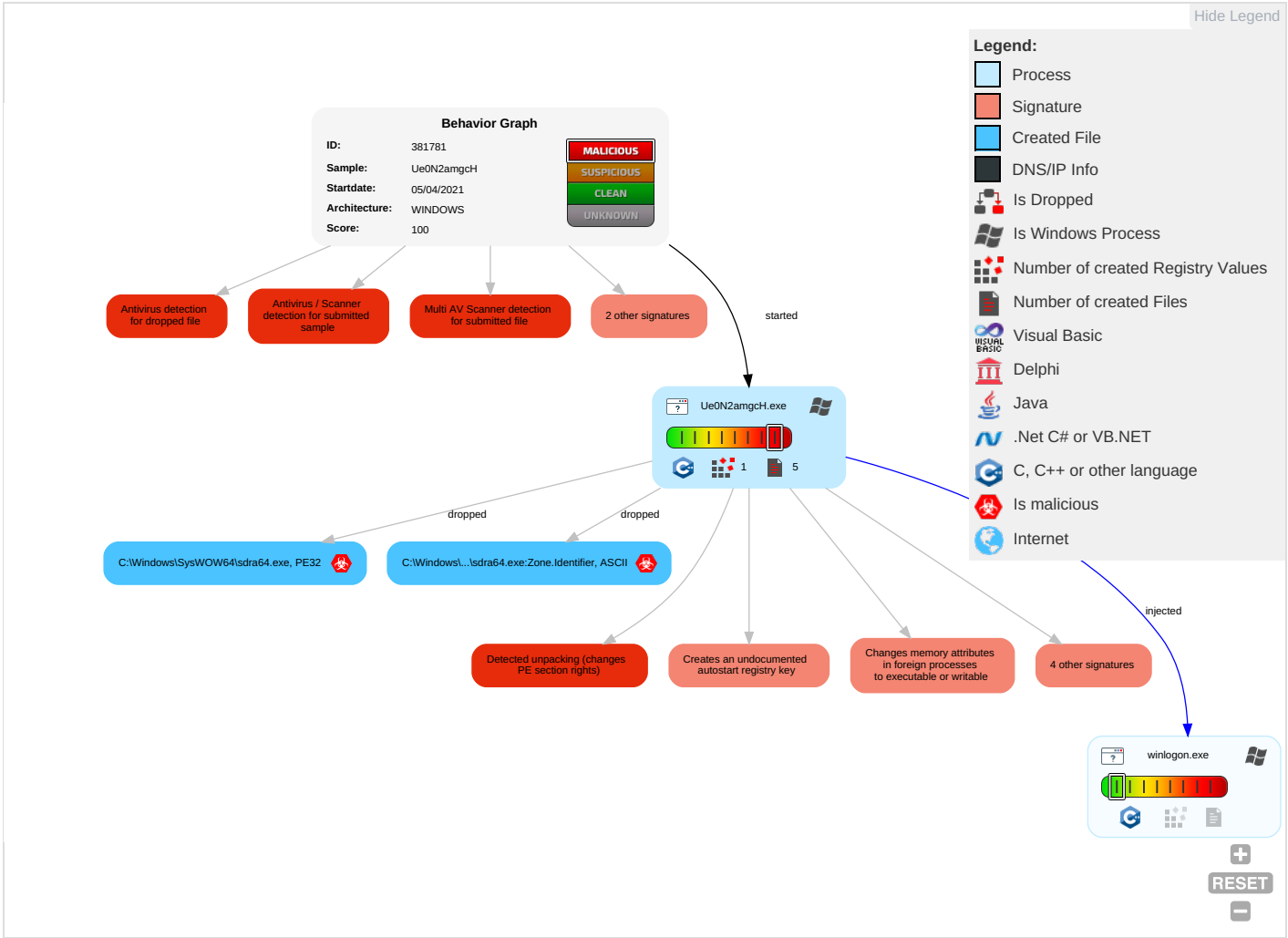
Writes to foreign memory regions

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts 1	Native API 1	Valid Accounts 1	Valid Accounts 1	Masquerading 2	Input Capture 1 1	System Time Discovery 2	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1 1	Valid Accounts 1	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Explo Redir Calls/
Domain Accounts	At (Linux)	Application Shimming 1	Process Injection 4 2	Virtualization/Sandbox Evasion 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Steganography	Explo Track Locati

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Local Accounts	At (Windows)	Logon Script (Mac)	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1 1	NTDS	Process Discovery 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Application Shimming 1	Process Injection 4 2	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comn
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Install Root Certificate 1	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	System Information Discovery 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insecu Protoc

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
Ue0N2amgcH.exe	90%	Virustotal		Browse
Ue0N2amgcH.exe	100%	ReversingLabs	Win32.Trojan.Zeus	
Ue0N2amgcH.exe	100%	Avira	TR/Crypt.ZPACK.Gen	
Ue0N2amgcH.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.111a0000.580.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.d6a0000.108.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
2.2.winlogon.exe.11e80000.683.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.d1a0000.68.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.10c20000.536.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.d8a0000.124.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.11360000.594.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.12600000.743.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.10760000.498.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.127c0000.757.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
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.12da0000.804.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.10fc0000.565.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.11780000.627.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.12d20000.800.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.124c0000.733.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.12ac0000.781.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.11ac0000.653.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.11180000.579.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.11060000.570.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.11ce0000.670.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.11220000.584.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.10de0000.550.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.11080000.571.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.11ea0000.684.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.12a00000.775.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.12700000.751.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.12b40000.785.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.122a0000.716.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.11f20000.688.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

Source	Detection	Scanner	Label	Link	Download
2.2.winlogon.exe.10da0000.548.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.11640000.617.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.10c00000.535.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.11920000.640.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.10f20000.560.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.10e60000.554.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.12360000.722.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.11c60000.666.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.10f60000.562.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.11140000.577.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.11b40000.657.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.128e0000.766.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.11d60000.674.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.114a0000.604.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.winlogon.exe.11ba0000.660.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/	Ue0N2amgcH.exe, 00000000.00000002.464238365.00000000023F3000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	381781
Start date:	05.04.2021
Start time:	02:57:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Ue0N2amgcH (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:	27
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@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 98.7% (good quality ratio 93.4%) • Quality average: 83.9% • Quality standard deviation: 27.7%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Windows\SysWOW64\sdra64.exe	
Process:	C:\Users\user\Desktop\Ue0N2amgcH.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	439808
Entropy (8bit):	7.486506470434463
Encrypted:	false
SSDEEP:	12288:tKLKS3ugwI5Z1BRzmWwP05WLNl6ZHkMR0xiDkAMf:tKLyg9vDRzmHP05Y6+iDkV
MD5:	66E599A0E60235530CE34127717CBD69
SHA1:	7E42442474AD8BAF2BD39EDBCD771728879194BF
SHA-256:	6DFB5E87C7226012F130032F4F8F9B9A3C1193843A11F0C1418CA3654AD78A83
SHA-512:	B7A0D723BD45E7037E1C53CC6E0FBC13906F3DDE598A9FCEAE8BA4057FD859B2416A4D37129568C306BE810E43D2FB5644EF66656BAC1C8202C06056CE55F2 5
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....$.....77uQsV..sV..sV..V.).LV...0M.\V..`8..DV..mQ.."V...a...V.....V..j....V.. RichsV.....PE..L...b..G.....X.....@.....p.....d..... .....text..... ..`.rdata.....@..@.data....P.....@..... ....

C:\Windows\SysWOW64\sdra64.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Ue0N2amgcH.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):	7.18265444554369
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:	Ue0N2amgcH.exe
File size:	60928
MD5:	ccb2db4a8a284f62db7002be470ac542
SHA1:	b2bdb5ed1ff743117cdf8500a498e247febbb6ec
SHA256:	4fb04b099a37aeae2f58685b8fb08bca298f8f68d5dfc45ceb9fa398e9f109ea
SHA512:	1472e175170bb13173963b479cd90e304b58554908b27caa0e813c47eaf8f85ac3783ce9240cab70a2d6349840ea5069cf44196695f64fdddf1a68ba1ce68f29
SSDEEP:	768:dtwaDQxDzRaaLoXfZ1yjpenwgb4uDAv5RhahPUCrjtrSfnnd8LCPCct8WL6pPlBa:puRuXzjh4k2gUgoPdNLYPba
File Content Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....77uQsV..sV..sV..V.).LV...0M.\V..`8..DV..mQ.."V...a...V.....V..j....V..RichsV.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4081b7
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:	0x47DCEE62 [Sun Mar 16 09:54:42 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:	41da589848b0ea7c32b44ddd22d7ade5

Entrypoint Preview

Instruction
call 00007FC730833680h
xor edi, edi
mov esi, dword ptr [esp]
add esp, 04h
retn 0024h
xor esi, esi
push 00000000h
push 00BC7A6Dh
push 00000004h
push 00000000h
push 00CCBE13h
push 00000007h

Instruction
push 00000000h
call dword ptr [00410084h]
and eax, 000000FDh
xor edx, edx
mov dl, al
add esi, edx
cmp esi, 3FFCD967h
jnl 00007FC730833674h
jmp 00007FC730833643h
mov bl, dl
xor eax, eax
mov eax, 0000F607h
add eax, 00088C23h
sub eax, 00088B52h
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
push 00000000h
call dword ptr [0041007Ch]
pop ecx
mov ecx, esi
mov esi, dword ptr [esp]
mov edi, eax
add esi, 00000103h
sub esp, 04h
mov dword ptr [esp], eax
mov ecx, 000001DBh
mov edx, CE0E523Dh
mov ebp, 00000000h
mov bh, byte ptr [esi]
add bh, dl
sub esi, 000B54D0h
add esi, 000B54D1h
add bh, bl
mov byte ptr [edi], bh
inc edi
sub esp, 04h
mov dword ptr [esp], edx
push ecx
push 00000000h
push 00000007h
push 00000005h
push 00000000h
push 00000000h
push 008AF758h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x100f0	0x64	.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	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x10000	0xa0	.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	0xe1f0	0xe200	False	0.886874308628	data	7.30372755134	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x10000	0x508	0x600	False	0.509765625	data	4.76117916035	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x11000	0x50cb	0x200	False	0.087890625	data	0.483984725135	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
ole32.dll	StgOpenStorageOnILockBytes, ReadClassStg, CoQueryProxyBlanket, OleLoad, PropVariantClear, WriteStringStream, StgCreateDocfileOnILockBytes, CoRegisterMessageFilter, CoGetCallerTID, StgOpenStorage
SHLWAPI.dll	UrlIsNoHistoryW, PathGetArgsW, PathMakePrettyW, wnsprintfW, SHRegSetUSValueA, PathRemoveArgsA, SHQueryInfoKeyA, StrToIntA, PathIsUNCA
KERNEL32.dll	WriteConsoleW, CopyFileExW, GetAtomNameA, SetConsoleCursorPosition, OpenSemaphoreW, EnumCalendarInfoExA, IsBadHugeWritePtr, SetConsoleActiveScreenBuffer, CreateDirectoryExA, SetNamedPipeHandleState, VirtualAlloc, VirtualProtect, CreateFileA
ADVAPI32.dll	BuildImpersonateExplicitAccessWithNameA, CryptGenRandom, CryptDestroyHash, SetEntriesInAuditListA

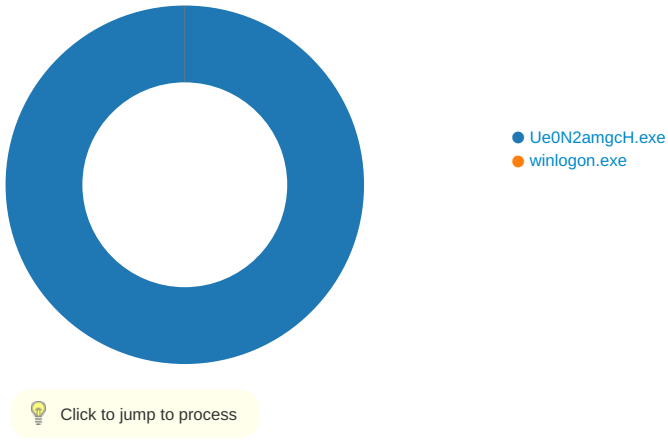
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Ue0N2amgcH.exe PID: 6080 Parent PID: 5532

General

Start time:	02:58:17
Start date:	05/04/2021
Path:	C:\Users\user\Desktop\Ue0N2amgcH.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Ue0N2amgcH.exe'
Imagebase:	0x400000
File size:	60928 bytes
MD5 hash:	CCB2DB4A8A284F62DB7002BE470AC542
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
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	405A70	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	405A70	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	60928	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 20 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 37 37 75 51 73 56 1b 02 73 56 1b 02 73 56 1b 02 56 09 29 02 4c 56 1b 02 be 30 4d 02 5c 56 1b 02 60 38 15 02 44 56 1b 02 6d 51 f6 02 22 56 1b 02 02 61 ad 02 c0 56 1b 02 94 19 bd 02 e4 56 1b 02 6a f6 1c 02 b9 56 1b 02 52 69 63 68 73 56 1b 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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.... $.......77uQsV..sV..sV..V.). LV ...0M.\V..`8..DV..mQ.."V...a ...V.......V..j....V..RichsV....	success or wait	1	405A70	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	405A70	CopyFileW
C:\Windows\SysWOW64\sdra64.exe	unknown	378880	03 2d 63 04 11 31 1a 31 15 03 89 3d ac 60 c4 6f 77 55 02 0a 47 73 59 5a 4e 12 06 37 02 19 1c 69 42 b7 2e 4f b2 04 0c 3b 85 32 73 11 38 37 7b 2b 10 04 13 0c 0e 32 19 68 1a c1 38 03 16 0a 21 4d 8d 15 60 0e 27 49 61 2a 0e 8b 86 04 10 80 03 03 25 0b b5 d8 79 0b 0f 2f 25 09 13 09 60 18 03 53 35 08 0e 1f 26 1f 37 5b 04 4f 14 3a 22 81 06 03 44 94 0c 65 72 1e 08 c7 6c 3e 1a 2a 09 b0 06 21 03 53 ba 3d 01 7d 10 a6 33 65 18 98 6d 21 51 28 5e 28 2d 93 58 14 b9 32 68 59 34 2e 00 34 00 7f 06 14 36 5f 12 29 ab 55 d2 75 b6 2a 52 36 11 65 17 1c 50 03 7d 2b 02 08 31 54 0d 1d 57 19 19 4d 1e 13 77 12 16 02 c5 3c a7 0d 16 9e 11 40 1d 02 69 00 03 06 07 61 1c 14 00 0c 01 4b a4 1f 6e b8 6d 37 21 5c 41 35 bd 11 9a 03 04 21 0d 55 04 55 17 b3 26 c7 06 3b 3e 49 17 87 7a dd 1a 4a 06	.- c..1.1...=.`.owU..GsYZN..7. ..iB..O...;.2s.87{+.....2.h..8. ..!M..`.'Ia*........%...y../%. ..`..S5...&.7[.O.:"...D..er... l>.*...!.S.=.}..3e..m!Q(^(-.X. .2hY4..4....6_.).U.u.*R6.e.. P.}+..1T..W..M..w.... <.....@..i. ...a.....K..n.m7!\A5.....!.U.U ..&..;>I..z..J.	success or wait	1	405B0E	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	409CB1	RegSetValueExW

Analysis Process: winlogon.exe PID: 560 Parent PID: 6080

General

Start time:	02:58:18
Start date:	05/04/2021
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