ID: 326673
Sample Name: egregor.rar
Cookbook: default.jbs
Time: 20:40:13
Date: 03/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

Analysis Report egregor.rar

Overview

General Information

Sample Name:	egregor.rar
Analysis ID:	326673
MD5:	0df77a02ed7a9bf..
SHA1:	a3acc24e78bc20...
SHA256:	b2d1865bca4392..

Most interesting Screenshot:

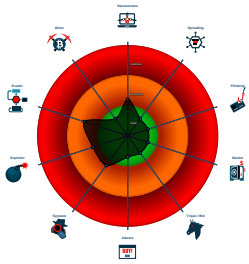
Detection

Score:	3
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Contains long sleeps (>= 3 min)
- Creates a DirectInput object (often fo...
- Creates a process in suspended mo...
- Detected potential crypto function
- Found inlined nop instructions (likely...
- May sleep (evasive loops) to hinder ...
- Uses code obfuscation techniques (...

Classification



Startup

- **System is w10x64**
- unarchiver.exe (PID: 4808 cmdline: 'C:\Windows\SysWOW64\unarchiver.exe' 'C:\Users\user\Desktop\egregor.rar' MD5: 8B435F8731563566F3F49203BA277865)
  - 7za.exe (PID: 2932 cmdline: 'C:\Windows\System32\7za.exe' x -pinfected -y -o'C:\Users\user\AppData\Local\Temp\x4hkmmij.rk2' 'C:\Users\user\Desktop\egregor.rar' MD5: 77E556CDFDC5C592F5C46DB4127C6F4C)
    - conhost.exe (PID: 4708 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

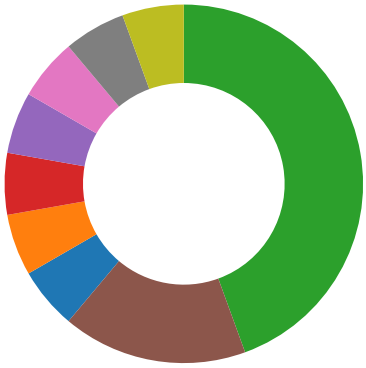
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



- Software Vulnerabilities
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- 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

Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

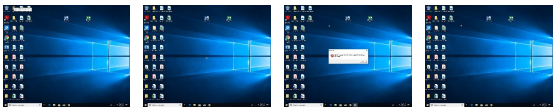
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Virtualization/Sandbox Evasion 2	Input Capture 1	Virtualization/Sandbox Evasion 2	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	System Information Discovery 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap

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
egregor.rar	2%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	326673
Start date:	03.12.2020
Start time:	20:40:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	egregor.rar
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:	3
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	CLEAN
Classification:	clean3.winRAR@4/2@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .rar • Stop behavior analysis, all processes terminated

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\Microsoft\CLR_v2.0_32\UsageLogs\unarchiver.exe.log	
Process:	C:\Windows\SysWOW64\unarchiver.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	388
Entropy (8bit):	5.2529463157768355
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk7v:MLF20NaL329hJ5g522r0
MD5:	FF3B761A021930205BEC9D7664AE9258
SHA1:	1039D595C6333358D5F7EE5619FE6794E6F5FDB1
SHA-256:	A3517BC4B1E6470905F9A38466318B302186496E8706F1976F1ED76F3E87AF0F
SHA-512:	1E77D09CF965575EF9800B1EE8947A02D98F88DBFA267300330860757A0C7350AF857A2CB7001C49AFF1F5BD1E0AE6E90F643B27054522CADC730DD14BC3DE1
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..

C:\Users\user\AppData\Local\Temp\leaicdiy.jqm\unarchiver.log	
Process:	C:\Windows\SysWOW64\unarchiver.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2190
Entropy (8bit):	5.121845844833368
Encrypted:	false
SSDEEP:	48:6TYGVGbVGVGpnGYGVGpsUpGTEGmG3CGGGaCGCGaGVGVGm3GVGoGVGmcj/d+g:6VWHf
MD5:	2DA915E4AD9A07C6E9742C9DC0DCFF17
SHA1:	F98153B6CFFF214CFFAE73CEC5C237B8E8EF87C8
SHA-256:	AF4FA7DA7B42ADB263FAF583D76C57283ECCFCF4E252C3F2DDECCBA911AB9D63
SHA-512:	55DF756272B6CBE13EA4D3E6099757A425D5CF6EF3BD9A822DD2C0287E5B0F1501AD30CB3C3216CD083B556586283D66BA54E648390D1DC214F3D4F33456800
Malicious:	false
Reputation:	low
Preview:	12/03/2020 8:41 PM: Unpack: C:\Users\user\Desktop\egregor.rar..12/03/2020 8:41 PM: Tmp dir: C:\Users\user\AppData\Local\Temp\x4hkmmij.rk2..12/03/2020 8:41 PM: Received from standard out: ..12/03/2020 8:41 PM: Received from standard out: 7-Zip 18.05 (x86) : Copyright (c) 1999-2018 Igor Pavlov : 2018-04-30..12/03/2020 8:41 PM: Received from standard out: ..12/03/2020 8:41 PM: Received from standard out: Scanning the drive for archives:..12/03/2020 8:41 PM: Received from standard out: 1 file, 380911 bytes (372 KiB)..12/03/2020 8:41 PM: Received from standard out: ..12/03/2020 8:41 PM: Received from standard out: Extracting archive: C:\Users\user\Desktop\egregor.rar..12/03/2020 8:41 PM: Received from standard error: ERROR: Wrong password : RECOVER-FILES.txt..12/03/2020 8:41 PM: Received from standard error: ERROR: Wrong password : fasm.dll..12/03/2020 8:41 PM: Received from standard out: Path = C:\Users\user\Desktop\egregor.rar..12/03/2020 8:41 PM: Received from standard er

Static File Info

General

File type:	RAR archive data, v5
Entropy (8bit):	7.999555082667929
TrID:	• RAR Archive (5005/1) 100.00%
File name:	egregor.rar
File size:	380911
MD5:	0df77a02ed7a9bf131fc409855c1b62c
SHA1:	a3acc24e78bc20e50a6566b1f161e96b4fdf1f42
SHA256:	b2d1865bca4392aaf2fc77b308ac9ebf59271d775252576d2d437155a8c33f4a
SHA512:	139ca359b145af2390ae3587a02119f6b94d111af92fe4a232d7eac070bff8305cd2e7c384d576d19d973679713573cf51d5d229ff2852278c60a725eaae2a8d
SSDEEP:	6144:8lAs+cS2BBdtmQ3T0imsAhgA2Mg4YbD+JL7V/OzrSdovGeyTj9M87w+A:sX+tSYyQimfhgA214YbD+JV/OAovGUAA
File Content Preview:	Rar!....~..2.....[..a..<.....@I..'....RECOVER-FILES.txt0....2 ..l...KK._..)7...)...h..bf..fq..'..u..[..c...../....aWtq..l...";...O.@[eqW^...x.#..S. .s..$.....6OdA.Z....X.....[L...h..7..hQ.h;p...rm4A....L...'.....3.. h..G...;^N.

File Icon

	
Icon Hash:	00828e8e8686b000

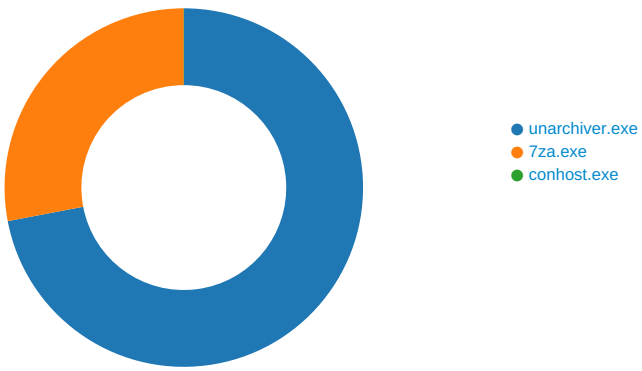
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: unarchiver.exe PID: 4808 Parent PID: 6064

General

Start time:	20:41:04
Start date:	03/12/2020
Path:	C:\Windows\SysWOW64\unarchiver.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\SysWOW64\unarchiver.exe' 'C:\Users\user\Desktop\egregor.rar'
Imagebase:	0xef0000
File size:	10240 bytes
MD5 hash:	8B435F8731563566F3F49203BA277865
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Local\Temp\leaicdiy.jqm	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	15EA4B1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\leaicdiy.jqm\unarchiver.log	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	15EA5AB	CreateFileW
C:\Users\user\AppData\Local\Temp\x4hkmmij.rk2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	15EA4B1	CreateDirectoryW

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\leaicdiy.jqm\unarchiver.log	unknown	67	31 32 2f 30 33 2f 32 30 32 30 20 38 3a 34 31 20 50 4d 3a 20 55 6e 70 61 63 6b 3a 20 43 3a 5c 55 73 65 72 73 5c 65 6e 67 69 6e 65 65 72 5c 44 65 73 6b 74 6f 70 5c 65 67 72 65 67 6f 72 2e 72 61 72 0d 0a	12/03/2020 8:41 PM: Unpack: C:\Users\user\Desktop\egregor.rar..	success or wait	1	15EA8EF	WriteFile
C:\Users\user\AppData\Local\Temp\leaicdiy.jqm\unarchiver.log	unknown	80	31 32 2f 30 33 2f 32 30 32 30 20 38 3a 34 31 20 50 4d 3a 20 54 6d 70 20 64 69 72 3a 20 43 3a 5c 55 73 65 72 73 5c 65 6e 67 69 6e 65 65 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 78 34 68 6b 6d 6d 69 6a 2e 72 6b 32 0d 0a	12/03/2020 8:41 PM: Tmp dir: C:\Users\user\AppData\Local\Temp\x4hkmmij.rk2..	success or wait	1	15EA8EF	WriteFile
C:\Users\user\AppData\Local\Temp\leaicdiy.jqm\unarchiver.log	unknown	50	31 32 2f 30 33 2f 32 30 32 30 20 38 3a 34 31 20 50 4d 3a 20 52 65 63 65 69 76 65 64 20 66 72 6f 6d 20 73 74 61 6e 64 61 72 64 20 6f 75 74 3a 20 0d 0a	12/03/2020 8:41 PM: Received from standard out: ..	success or wait	21	15EA8EF	WriteFile
C:\Users\user\AppData\Local\Temp\leaicdiy.jqm\unarchiver.log	unknown	93	31 32 2f 30 33 2f 32 30 32 30 20 38 3a 34 31 20 50 4d 3a 20 52 65 63 65 69 76 65 64 20 66 72 6f 6d 20 73 74 61 6e 64 61 72 64 20 65 72 72 6f 72 3a 20 45 52 52 4f 52 3a 20 57 72 6f 6e 67 20 70 61 73 73 77 6f 72 64 20 3a 20 52 45 43 4f 56 45 52 2d 46 49 4c 45 53 2e 74 78 74 0d 0a	12/03/2020 8:41 PM: Received from standard error: ERROR: Wrong password : RECOVER-FILES.txt..	success or wait	3	15EA8EF	WriteFile
C:\Users\user\AppData\Local\Temp\leaicdiy.jqm\unarchiver.log	unknown	31	31 32 2f 30 33 2f 32 30 32 30 20 38 3a 34 31 20 50 4d 3a 20 47 65 74 20 66 69 6c 65 73 0d 0a	12/03/2020 8:41 PM: Get files..	success or wait	1	15EA8EF	WriteFile
C:\Users\user\AppData\Local\Temp\leaicdiy.jqm\unarchiver.log	unknown	37	31 32 2f 30 33 2f 32 30 32 30 20 38 3a 34 31 20 50 4d 3a 20 4e 62 72 20 6f 66 20 66 69 6c 65 73 3a 20 34 0d 0a	12/03/2020 8:41 PM: Nbr of files: 4..	success or wait	1	15EA8EF	WriteFile
C:\Users\user\AppData\Local\Temp\leaicdiy.jqm\unarchiver.log	unknown	94	31 32 2f 30 33 2f 32 30 32 30 20 38 3a 34 31 20 50 4d 3a 20 46 69 6c 65 20 69 73 20 65 6d 70 74 79 3a 20 43 3a 5c 55 73 65 72 73 5c 65 6e 67 69 6e 65 65 72 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 78 34 68 6b 6d 6d 69 6a 2e 72 6b 32 5c 64 74 62 2e 64 61 74 0d 0a	12/03/2020 8:41 PM: File is empty: C:\Users\user\AppData\Local\Temp\x4hkmmij.rk2\dtb.dat..	success or wait	3	15EA8EF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\unarchiver.exe.log	unknown	388	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
unknown	unknown	1024	success or wait	2	15EA8EF	ReadFile
unknown	unknown	1024	pipe broken	2	15EA8EF	ReadFile

Analysis Process: 7za.exe PID: 2932 Parent PID: 4808

General

Start time:	20:41:05
Start date:	03/12/2020
Path:	C:\Windows\SysWOW64\7za.exe
Wow64 process (32bit):	true
Commandline:	'7za.exe' x -pinfected -y -o'C:\Users\user\AppData\Local\Temp\x4hkmmij.rk2' 'C:\Users\user\Desktop\egregor.rar'
Imagebase:	0x1040000
File size:	289792 bytes
MD5 hash:	77E556CDFDC5C592F5C46DB4127C6F4C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\x4hkmmij.rk2\RECOVER-FILES.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	10463B0	CreateFileW
C:\Users\user\AppData\Local\Temp\x4hkmmij.rk2\fasm.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	10463B0	CreateFileW
C:\Users\user\AppData\Local\Temp\x4hkmmij.rk2\run.bat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	10463B0	CreateFileW
C:\Users\user\AppData\Local\Temp\x4hkmmij.rk2\dtb.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	10463B0	CreateFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\egregor.rar	unknown	1024	success or wait	1	104686E	ReadFile
C:\Users\user\Desktop\egregor.rar	unknown	8	success or wait	1	104686E	ReadFile
C:\Users\user\Desktop\egregor.rar	unknown	7	success or wait	1	104686E	ReadFile

Analysis Process: conhost.exe PID: 4708 Parent PID: 2932

General

Start time:	20:41:05
Start date:	03/12/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis