ID: 337854
Sample Name: Scan_order.scr
Cookbook: default.jbs
Time: 08:08:12
Date: 11/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report Scan_order.scr 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Sigma Overview 5
System Summary: 5
Signature Overview 5
Networking: 5
System Summary: 5
Data Obfuscation: 5
Malware Analysis System Evasion: 5
Anti Debugging: 5
HIPS / PFW / Operating System Protection Evasion: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 8
Contacted Domains 9
Contacted IPs 9
Public 9
General Information 9
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 12
ASN 12
JA3 Fingerprints 13
Dropped Files 14
Created / dropped Files 14
Static File Info 14
General 14
File Icon 15
Static PE Info 15
General 15
Entrypoint Preview 15
Data Directories 16
Sections 16
Resources 16
Imports 16
Version Infos 16
Possible Origin 16

Network Behavior 17
Network Port Distribution 17
TCP Packets 17
UDP Packets 19
DNS Queries 20
DNS Answers 20
HTTPS Packets 20
Code Manipulations 21
Statistics 21
Behavior 21
System Behavior 21
Analysis Process: Scan_order.exe PID: 5260 Parent PID: 5568 21
General 21
File Activities 22
Analysis Process: ieinstal.exe PID: 5468 Parent PID: 5260 22
General 22
Analysis Process: ieinstal.exe PID: 6128 Parent PID: 5260 22
General 22
File Activities 22
File Created 22
File Deleted 23
File Written 23
Registry Activities 24
Key Created 24
Key Value Created 24
Analysis Process: wscript.exe PID: 5776 Parent PID: 6128 24
General 24
File Activities 25
File Deleted 25
Disassembly 25
Code Analysis 25

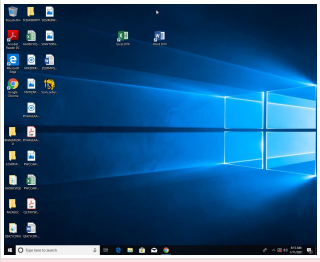
Analysis Report Scan_order.scr

Overview

General Information

Sample Name:	Scan_order.scr (renamed file extension from scr to exe)
Analysis ID:	337854
MD5:	04be7ed51e345a..
SHA1:	44f5fdf6902d114…
SHA256:	ab77af2c0fe4a39..
Tags:	GuLoader RemcosRAT sc

Most interesting Screenshot:



Errors

⚠ Sigma syntax error: Has an empty selector, Rule: Abusing Azure Browser SSO

Detection

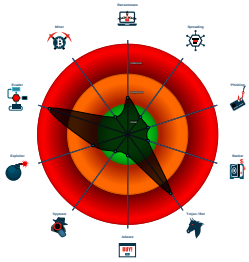
Remcos GuLoader

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

Signatures

- Malicious sample detected (through …
- Sigma detected: Remcos
- Yara detected GuLoader
- Connects to many ports of the same…
- Contains functionality to detect hard…
- Contains functionality to hide a threa…
- Detected RDTSC dummy instruction…
- Hides threads from debuggers
- Initial sample is a PE file and has a …
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Writes to foreign memory regions
- Yara detected VB6 Downloader Gen…
- Abnormal high CPU Usage
- Checks if the current process is bein…

Classification



Startup

- **System is w10x64**
- Scan_order.exe (PID: 5260 cmdline: 'C:\Users\user\Desktop\Scan_order.exe' MD5: 04BE7ED51E345A56403DF4657B376990)
  - ieinstal.exe (PID: 5468 cmdline: 'C:\Users\user\Desktop\Scan_order.exe' MD5: DAD17AB737E680C47C8A44CBB95EE67E)
  - ieinstal.exe (PID: 6128 cmdline: 'C:\Users\user\Desktop\Scan_order.exe' MD5: DAD17AB737E680C47C8A44CBB95EE67E)
    - wscript.exe (PID: 5776 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\uninstall.vbs' MD5: 7075DD7B9BE8807FCA93ACD86F724884)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.204159990.000000000040A000.00000020.00020000.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth	• 0xf40:$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB
00000019.00000002.689367509.00000000032D1000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
00000000.00000002.595879092.000000000040A000.00000020.00020000.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth	• 0xf40:$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB
Process Memory Space: ieinstal.exe PID: 6128	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

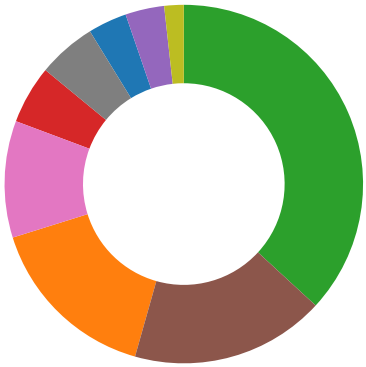
Source	Rule	Description	Author	Strings
Process Memory Space: Scan_order.exe PID: 5260	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Remcos

Signature Overview



- Compliance
- Networking
- 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

Networking:

Connects to many ports of the same IP (likely port scanning)

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Contains functionality to hide a thread from the debugger

Hides threads from debuggers

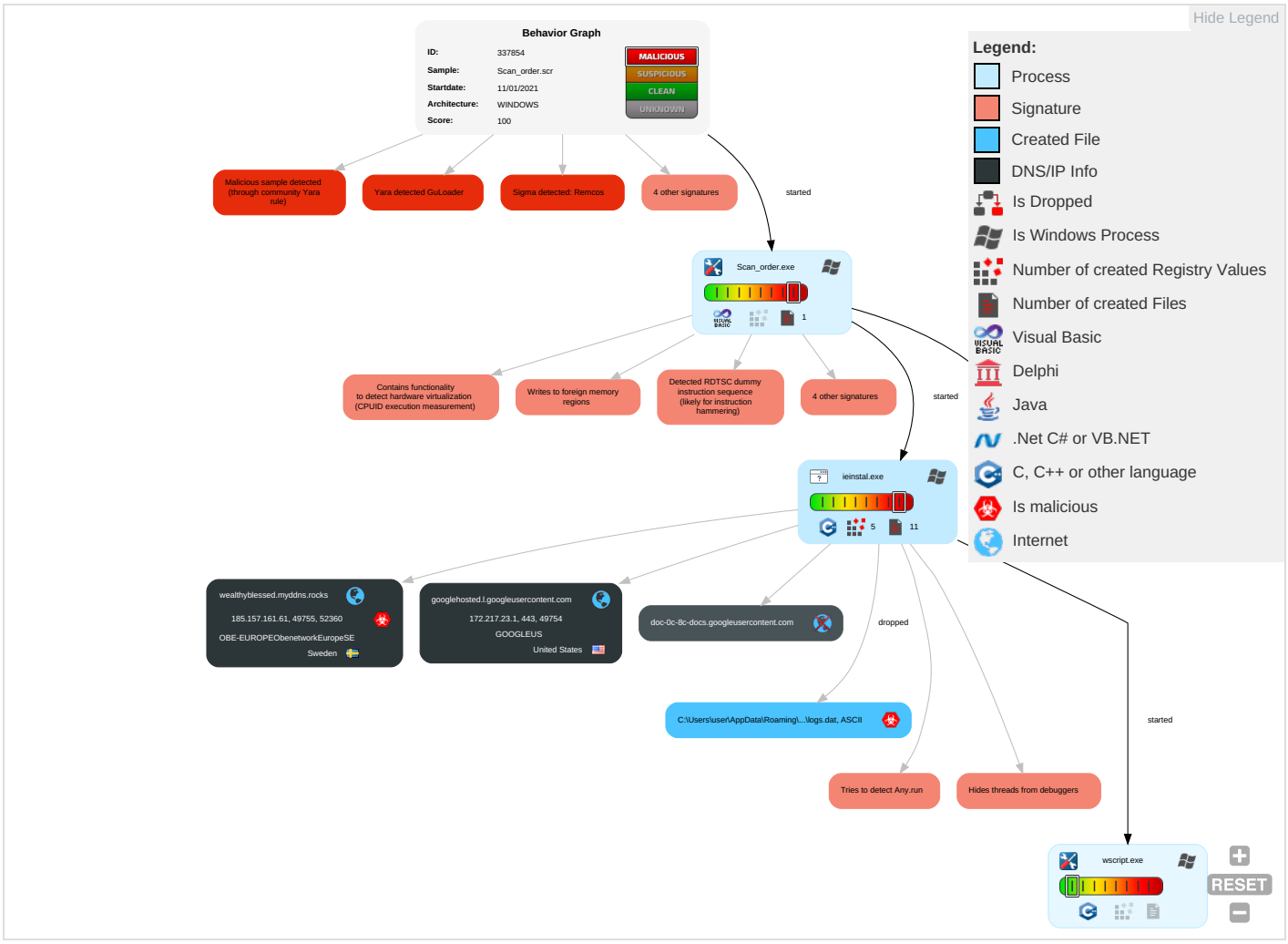
HIPS / PFW / Operating System Protection Evasion:

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	Network Effects
Valid Accounts	Scripting 1 1	Path Interception	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop Insecure Network Communic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2 3	LSASS Memory	Security Software Discovery 7 3 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS Redirect P Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 2	Security Account Manager	Virtualization/Sandbox Evasion 2 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Scripting 1 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 3 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi Access Po

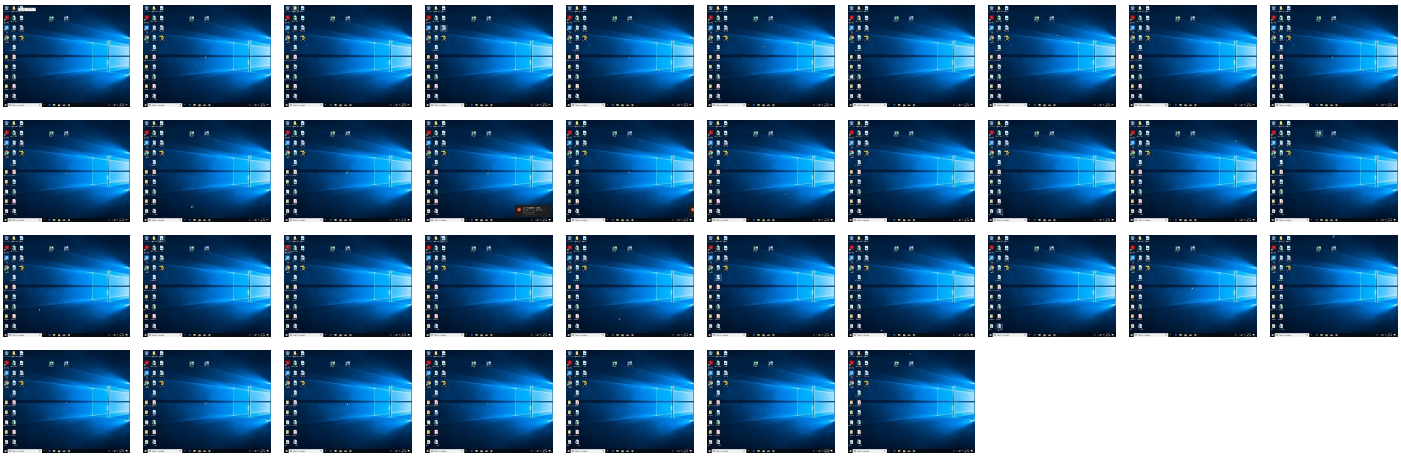
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

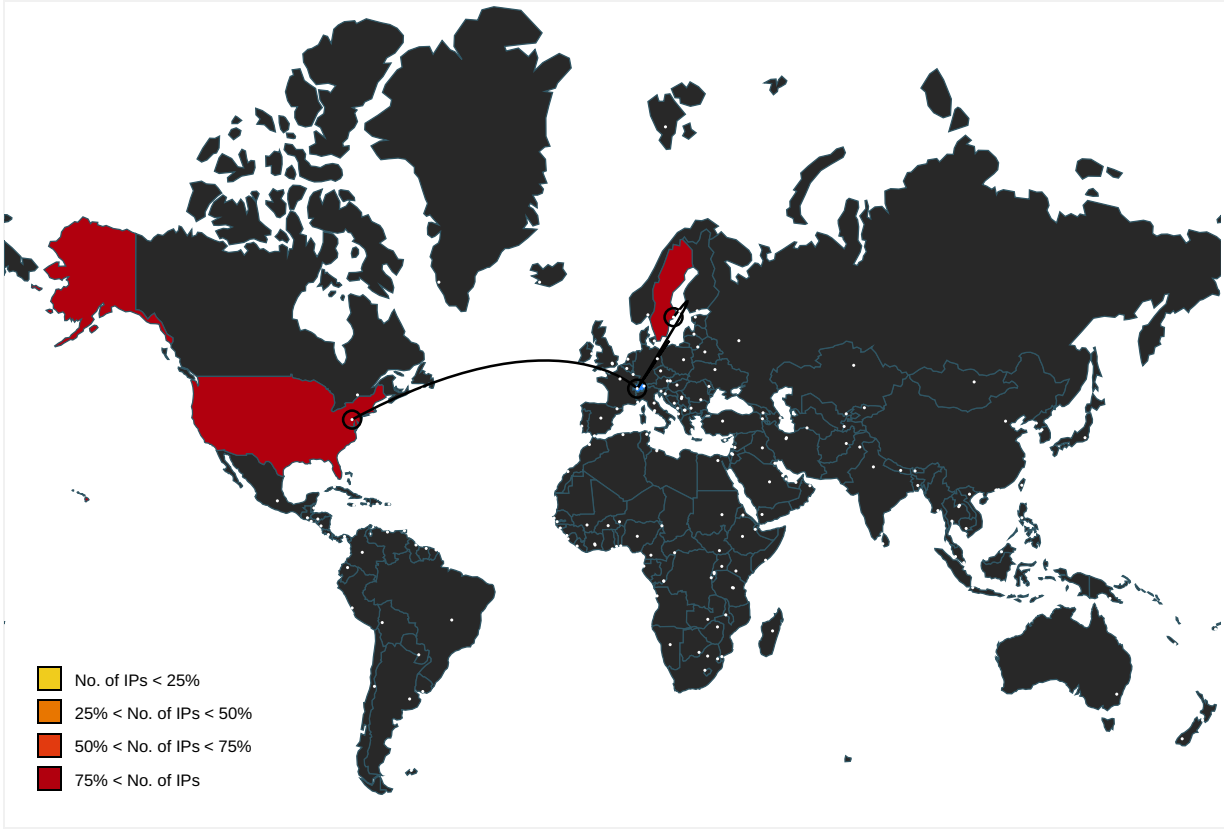
No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
wealthyblessed.myddns.rocks	185.157.161.61	true	true		unknown
googlehosted.l.googleusercontent.com	172.217.23.1	true	false		high
doc-0c-8c-docs.googleusercontent.com	unknown	unknown	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.23.1	unknown	United States		15169	GOOGLEUS	false
185.157.161.61	unknown	Sweden		197595	OBE-EUROPEObenetworkEuropeSE	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	337854
Start date:	11.01.2021
Start time:	08:08:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Scan_order.scr (renamed file extension from scr 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:	39
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:	MAL
Classification:	mal100.troj.evad.winEXE@7/2@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.5% (good quality ratio 1.4%) • Quality average: 45.8% • Quality standard deviation: 11.2%
HCA Information:	• Successful, ratio: 78% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.139.144, 13.64.90.137, 104.79.90.110, 20.190.129.2, 40.126.1.145, 20.190.129.160, 20.190.129.133, 40.126.1.128, 20.190.129.130, 40.126.1.130, 40.126.1.142, 51.104.139.180, 92.122.213.247, 92.122.213.194, 20.54.26.129, 51.11.168.160, 52.155.217.156, 172.217.23.14, 20.190.129.17, 20.190.129.24, 40.126.1.166, 20.190.129.19, 51.11.168.232, 2.20.142.209, 2.20.142.210 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, login.live.com, audownload.windowsupdate.nsatc.net, drive.google.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, settings-win.data.microsoft.com, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, login.msa.msidentity.com, settingsfd-geo.trafficmanager.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, dub2.next.a.prd.aadg.trafficmanager.net, www.tm.lg.prod.aadmsa.trafficmanager.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/337854/sample/Scan_order.exe
Errors:	• Sigma syntax error: Has an empty selector, Rule: Abusing Azure Browser SSO

Simulations

Behavior and APIs

Time	Type	Description
08:12:00	API Interceptor	408x Sleep call for process: ieinstal.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.217.23.1	Images for New materials H12Etxknwemhib9.exe	Get hash	malicious	Browse	
	undefined.html	Get hash	malicious	Browse	
	http://www.dropbox.com/l/AAA5d-90vlipt6OAJjh2DZ1FLO-gN1n6Y0k	Get hash	malicious	Browse	
	Order List.exe	Get hash	malicious	Browse	
	http://https://docs.google.com/document/d/e/2PACX-1vQ2WKVd3JleNdWlUHfoPHiI9meS5tPYCvu_arjbyKKIg7TwWXSlOD1XSnaOARjo0G7h2c08To_2PmFI/pub	Get hash	malicious	Browse	
	http://https://www.evernote.com/shard/s392/sh/fa9d8bce-6c75-8e4b-f292-c8e5922b6f12/2c2e75787ef91022dc2eb256a739682c	Get hash	malicious	Browse	
	http://freeaccountnow.com	Get hash	malicious	Browse	
	http://https://docs.google.com/document/d/e/2PACX-1vRFLfuWRihaQHjGEPs8-Dm7Y3VxEFRpiUJuJmD9Vm6y3xVSSG9Vc3XxRnbyHQzIoWQ_5REbdDbkOq0s/pub	Get hash	malicious	Browse	
	Request For quotation-00900.exe	Get hash	malicious	Browse	
	http://www.146146.cynemas.site./RGFybmVsbC5NYXRoZXdAY29nZWNvcGVlcjEuY29t#aHR0cHM6Ly9zaXRlcy5nb29nbGUuY29tL3ZpZXcvZWVyZTM0Mi8lRDglQTclRDklODQlRDglQjUlRDklODElRDglQUQlRDglQTktJUQ4JUE3JUQ5JTg0JUQ4JUIxJUQ4JUE2JUQ5JThBJUQ4JUIzJUQ5JThBJUQ4JUE5	Get hash	malicious	Browse	
	http://https://docs.google.com/document/d/e/2PACX-1vSXSFqM3FyfkgqlaUuBs15kxzZ2ytYMtEH-lt-VAyaJGjbE3AvRzWL0WZQ7F1gIxKGQpEkm2Ri_snvl/pub	Get hash	malicious	Browse	
	PR-0012575 (P 999).exe	Get hash	malicious	Browse	
	http://https://tuak.cmail19.com/t/t-i-xykuka-l-r/	Get hash	malicious	Browse	
	http://www.154154.bd.ntipak.com/aXJlbmVfY2hhbkBzdXRkLmVkdS5zZw==#aHR0cHM6Ly9zaXRlcy5nb29nbGUuY29tL3ZpZXcvbW1uYi8lRDglQTclRDklODQlRDglQjUlRDklODElRDglQUQlRDglQTktJUQ4JUE3JUQ5JTg0JUQ4JUIxJUQ4JUE2JUQ5JThBJUQ4JUIzJUQ5JThBJUQ4JUE5	Get hash	malicious	Browse	
	http://www.154154.bd.ntipak.com/aXJlbmVfY2hhbkBzdXRkLmVkdS5zZw==#aHR0cHM6Ly9zaXRlcy5nb29nbGUuY29tL3ZpZXcvbW1uYi8lRDglQTclRDklODQlRDglQjUlRDklODElRDglQUQlRDglQTktJUQ4JUE3JUQ5JTg0JUQ4JUIxJUQ4JUE2JUQ5JThBJUQ4JUIzJUQ5JThBJUQ4JUE5	Get hash	malicious	Browse	
	http://https://docs.google.com/document/d/e/2PACX-1vSddy8cuFSrePEDADFWqOFMq31iEt3VTknn8s0o66ouwgLfYqTCG7MSJvch7KcyR03mvmYMJg1Kh7lk/pub	Get hash	malicious	Browse	
	http://https://docs.google.com/document/d/e/2PACX-1vQl8xkPTC5qcRYddleeD1wWjcL_--hdx0xmAEkwmmMnX6FXnPPI-eTnY7H4kljKVOeNuw_n16-YWE8v/pub	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://u2109837.ct.sendgrid.net/ls/click?upn=ZZ6GL0ia6ZQqkHdNqmcfnzjKMlvomZCQgE3kAyJdsXh7HvgQ2sCYDvk7NVAOuyTHb4xXVycnbXvYmGLTwLvXqlr-2FBH7O-2F0sVebcrSi3wRAMnqysyGCkq3KDTz4rGE56KJbrbg5mYb0pZbdZr2hfCwkjkHfsLEQHJq26n9MbwBgSPBCfBmTAw89TNFmIXOWNgEnCv_TmoPLIbax9Jh83rXf3CKCVf12BRNQLs5vTp0XFzzHhSTjJ689hADNCj94vLJ0pVWCcnqGZbEr5n33c4fDosWEocENGB3Oz4505qLzziVwjY-2FU2OHI-2BUytdgZg08iOUQHYVA2mg-2F765B7tOcBDzWCeXXJvpMpTRZrtem0FeuQJ9Lt-2BKa-2BPLFmOTTbRy6Mp3SEhYQHWiVe4JER4ZKmX41wsxK3Nbbdn0r-2FMyMZS2hyINI-3D	Get hash	malicious	Browse	
	http://https://l.facebook.com/l.php?u=https%3A%2F%2Ftinyurl.com%2Fy3da9xbq%3Ffbclid%3DIwAR11jNtpFJqmHsfB6MuN4oB-gl7-RlVZqSgYIbmZW4ycJwtQ-tC85PzgLO4&h=AT1i9PU8X_itDVqe5yg4Afn5zFPp0KVwni5sQg-Oc5Yor7a-8EWrOl11b-y21X_Oi92_H_jMhPiEjm3aKUnMEib9p96Fuptgd9vraABiOS8AO8X86OxcPZyET7VlHYnKBg&__tn__=H-R&c[0]=AT26jLdBW-b9efDmUD2-IVQDmvnfjC8zMcJVpGrmXtfU07ZmaRqvjC3hcq86tiO8rGqmY2DrakboCaPRMLQtsl2m1yZfExawqplv_zZwazNNYlc2wsoaV6LvzXDEPrWYoMbJFnx7l8Qm7vznPPnkddWEuQ	Get hash	malicious	Browse	
	http://https://u8044497.ct.sendgrid.net/ls/click?upn=2kG68ZigzTjarF-2BMq-2BkFKRCI85rLMeWLq4nFd21f8aWMar1nyH1bpDl6QTriB-2BCg9ZRVuS5KNgyqJvrwEERxoCN-2FuJNCLk-2FKWpotJvzpXzhK5ZrQRQIuKE2scLJ6pxOJGqxvH-2FdFgC9ylH2T9F-2F-2F87QanD-2B78vn33Psi-2FpSvawsFv5nBPk3yW8zOfIG-2F8LMbQKnY_E0HJ-2FOm5MWj9o-2F074sR7ar3EENZ9HXqrwFihx-2BlxgKrKtNrT8HHD9UvVOlQfmJqHouKdBiD0cPuRxKhdbr-2BdBDCJw-2FpPJ6Rhg8Rcuykg2re83cPJOlx1ck9OfAJuT20-2Bg-2FHKW3ZtFIgFXmtA3eRHIhUPakM-2F1wd24fcVrApKwPA4Zq7KEN7k9VTA7qQX29revWsMXFb-2FufLF7Xz8-2FlzYJA-3D-3D	Get hash	malicious	Browse	
185.157.161.61	SecuriteInfo.com.generic.ml.exe	Get hash	malicious	Browse	
	New PO.doc	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
wealthyblessed.myddns.rocks	SecuriteInfo.com.generic.ml.exe	Get hash	malicious	Browse	• 185.157.161.61
	New PO.doc	Get hash	malicious	Browse	• 185.157.161.61
googlehosted.l.googleusercontent.com	SecuriteInfo.com.generic.ml.exe	Get hash	malicious	Browse	• 142.250.180.97
	New PO.doc	Get hash	malicious	Browse	• 142.250.180.97
	http://down10d.zol.com.cn/zoldownload/fangsong_GB2312@81_432727.exe	Get hash	malicious	Browse	• 142.250.180.97
	http://https://r0qp15r0b1rq05rrpbqbrpq5.s3-eu-west-1.amazonaws.com/Ap3dX.html#joetorre@gmail.com	Get hash	malicious	Browse	• 142.250.180.97
	http://kubecloud.com	Get hash	malicious	Browse	• 142.250.180.97
	http://https://blog.dericoin.com/wp-includes/shell/ivd/office/office/voicemail/index.php	Get hash	malicious	Browse	• 142.250.180.97
	http://www.secured-mailsharepoint.online/	Get hash	malicious	Browse	• 142.250.180.97
	jfuoevj.exe	Get hash	malicious	Browse	• 142.250.180.97
	http://subreqxserver1132.azurewebsites.net	Get hash	malicious	Browse	• 142.250.180.97
	http://46.101.152.151/?email=michael.little@austalusa.com	Get hash	malicious	Browse	• 142.250.180.97
	http://https://wfuwdbjwquoiynfb-dot-tundasma.el.r.appspot.com/#test@test.com	Get hash	malicious	Browse	• 142.250.180.97
	r0u.exe	Get hash	malicious	Browse	• 142.250.180.97
	r0u.exe	Get hash	malicious	Browse	• 142.250.180.97
	http://bit.ly/3nlGvk0	Get hash	malicious	Browse	• 216.58.206.33
	http://fokpsrhpqilmgun.65kjh455kh566gf.camdvr.org	Get hash	malicious	Browse	• 216.58.206.33
	http://https://pdfsharedmessage.xtensio.com/7wtcdlta	Get hash	malicious	Browse	• 216.58.206.33
	#Ud83d#Udcde_8360.htm	Get hash	malicious	Browse	• 216.58.215.225
	Westernsouthernlife8PG5-YSGL2K-TVU4.htm	Get hash	malicious	Browse	• 216.58.215.225
	http://https://alijafari6.wixsite.com/owa-projection-aspx	Get hash	malicious	Browse	• 216.58.215.225
	zsmcirs.exe	Get hash	malicious	Browse	• 216.58.215.225

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OBE-EUROPEObenetworkEuropeSE	inrfzFzDHR.exe	Get hash	malicious	Browse	• 45.148.16.42

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SecuriteInfo.com.generic.ml.exe	Get hash	malicious	Browse	• 185.157.161.61
	New PO.doc	Get hash	malicious	Browse	• 185.157.161.61
	89GsVCJAXv.exe	Get hash	malicious	Browse	• 185.157.162.81
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 185.157.162.81
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.160.233
	dpR3o92MH1.exe	Get hash	malicious	Browse	• 185.157.162.81
	0qNSJXB8nG.exe	Get hash	malicious	Browse	• 185.157.162.81
	Order_1101201918_AUTECH.exe	Get hash	malicious	Browse	• 185.157.161.86
	7w7LwD8bqe.exe	Get hash	malicious	Browse	• 185.157.162.81
	ZZB5zuv1X0.exe	Get hash	malicious	Browse	• 185.157.162.81
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 185.157.162.81
	ptoovvKZ80.exe	Get hash	malicious	Browse	• 185.157.162.81
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 185.157.162.81
	EnJsj6nuD4.exe	Get hash	malicious	Browse	• 185.157.162.81
	AdviceSlip.xls	Get hash	malicious	Browse	• 217.64.149.169
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.160.233
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.160.233
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.160.233
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.160.233
GOOGLEUS	correos-1.apk	Get hash	malicious	Browse	• 216.58.198.42
	correos-1.apk	Get hash	malicious	Browse	• 216.58.198.10
	parler.apk	Get hash	malicious	Browse	• 216.58.198.10
	parler.apk	Get hash	malicious	Browse	• 142.250.180.131
	Riskware.apk	Get hash	malicious	Browse	• 216.58.198.10
	transcach.exe	Get hash	malicious	Browse	• 172.253.120.109
	PCS.exe	Get hash	malicious	Browse	• 172.253.120.109
	transcach.exe	Get hash	malicious	Browse	• 172.253.120.109
	freezer-arm32-0.6.8.apk	Get hash	malicious	Browse	• 216.239.35.12
	freezer-arm32-0.6.8.apk	Get hash	malicious	Browse	• 216.239.35.0
	mobdro.apk	Get hash	malicious	Browse	• 142.250.180.174
	mobdro.apk	Get hash	malicious	Browse	• 142.250.180.174
	ddkMUJ9VLH.exe	Get hash	malicious	Browse	• 8.8.8.8
	AptoideTV-5.1.2.apk	Get hash	malicious	Browse	• 142.250.180.142
	com.parler.parler-2.6.6-free-www.apksum.com.apk	Get hash	malicious	Browse	• 142.250.180.74
	Pending PURCHASE ORDER - 47001516.pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	SecuriteInfo.com.generic.ml.exe	Get hash	malicious	Browse	• 142.250.180.97
	FTH2004-005.exe	Get hash	malicious	Browse	• 34.102.136.180
	Curriculo Laura.xlsm	Get hash	malicious	Browse	• 35.241.57.45
	Confirm!!!..exe	Get hash	malicious	Browse	• 34.102.136.180

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	_00AC0000.exe	Get hash	malicious	Browse	• 172.217.23.1
	SecuriteInfo.com.BehavesLike.Win32.Trojan.jc.exe	Get hash	malicious	Browse	• 172.217.23.1
	SecuriteInfo.com.BehavesLike.Win32.Trojan.jc.exe	Get hash	malicious	Browse	• 172.217.23.1
	SecuriteInfo.com.BehavesLike.Win32.Trojan.jc.exe	Get hash	malicious	Browse	• 172.217.23.1
	SecuriteInfo.com.Trojan.GenericKD.44525883.8642.exe	Get hash	malicious	Browse	• 172.217.23.1
	11998704458248.exe	Get hash	malicious	Browse	• 172.217.23.1
	KeyMaker.exe	Get hash	malicious	Browse	• 172.217.23.1
	SecuriteInfo.com.generic.ml.exe	Get hash	malicious	Browse	• 172.217.23.1
	home.css.ps1	Get hash	malicious	Browse	• 172.217.23.1
	Curriculo Laura.xlsm	Get hash	malicious	Browse	• 172.217.23.1
	36.exe	Get hash	malicious	Browse	• 172.217.23.1
	Buran.exe	Get hash	malicious	Browse	• 172.217.23.1

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://r0qp15r0b1rq05rrpbqbrpq5.s3-eu-west-1.amazonaws.com/Ap3dX.html#joetorre@gmail.com	Get hash	malicious	Browse	• 172.217.23.1
	http://https://survey.alchemer.com/s3/6130663/Check-11-Payment	Get hash	malicious	Browse	• 172.217.23.1
	http://https://smlfinance.com/wp-content/uploads/2021/DHL2021/MARKET/	Get hash	malicious	Browse	• 172.217.23.1
	atikmdag-patcher 1.4.8.exe	Get hash	malicious	Browse	• 172.217.23.1
	http://https://atacadaodocompensado.com.br/office356.com-RD163	Get hash	malicious	Browse	• 172.217.23.1
	http://www.secured-mailsharepoint.online/	Get hash	malicious	Browse	• 172.217.23.1
	jfuoevj.exe	Get hash	malicious	Browse	• 172.217.23.1
	http://https://blog.dericoin.com/wp-includes/shell/ivd/Office/office/voicemail/index.php	Get hash	malicious	Browse	• 172.217.23.1

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\uninstall.vbs	
Process:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
File Type:	data
Category:	dropped
Size (bytes):	366
Entropy (8bit):	3.376225730361457
Encrypted:	false
SSDEEP:	6:xPW+YR4lA2QOm3OOZgypjRQIQMlziKJRBgUubdlrYM3LkMl4YLMYRdn9YKJRB4y8:xQ4lA2++ugypjBQMB3DubdpYGkMJH9Zk
MD5:	0FE2423601D3291B0B6326E6518286A0
SHA1:	09746EB739147F191068ABA1552CD616EABD5E1D
SHA-256:	1A899121E3969C2BB894E08765A57E8A65CB9154D71C3825BAA6B4F2DA61D8F3
SHA-512:	9632ACAA96BF0D7BC5F3754D15117079888FCC23591007FC7F4D5DABFDB1E9300CF96FF3EE9266FE2D29EA118623651773D1002D5A3F91270471841D5012CEC
Malicious:	false
Reputation:	low
Preview:	O.n. .E.r.r.o.r. .R.e.s.u.m.e. .N.e.x.t...S.e.t. .f.s.o. .=. .C.r.e.a.t.e.O.b.j.e.c.t.(.".S.c.r.i.p.t.i.n.g...F.i.l.e.S.y.s.t.e.m.O.b.j.e.c.t.".)...f.s.o...D.e.l.e.t.e.F.i.l.e. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.i.n.t.e.r.n.e.t. .e.x.p.l.o.r.e.r.\.i.e.i.n.s.t.a.l...e.x.e."...f.s.o...D.e.l.e.t.e.F.i.l.e.(.W.s.c.r.i.p.t...S.c.r.i.p.t.F.u.l.l.N.a.m.e.).

C:\Users\user\AppData\Roaming\remcos\logs.dat	
Process:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	125
Entropy (8bit):	4.639773731024033
Encrypted:	false
SSDEEP:	3:ttUAdUPVWJKrA4RXMRPHv31ae1voVEAv5EJMLrA4RXMRPHvn:tmSgO4XqdHv3l92NM/XqdHvn
MD5:	5B63CB81C36495441D67E06B293B0320
SHA1:	14246085597E9585F67E58065DE13C096926F008
SHA-256:	787158C4FCB177C4861EC3BC08D21AEA5D0807EE46725D35EFB392530E079834
SHA-512:	A077CF0DF572B374B411E2AFED6C749E4D54F8FFDB4AF9538AF7443C92BB7B59B76A28DB00BB5C6734594F88956C9B89B3DA510046A8853DAD3D791EECAC888
Malicious:	**true**
Reputation:	low
Preview:	..[2021/01/11 08:12:00 Offline Keylogger Started]....[Program Manager]....[2021/01/11 09:16:06 Offline Keylogger Started]..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.746554652121395

General

TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • 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:	Scan_order.exe
File size:	77824
MD5:	04be7ed51e345a56403df4657b376990
SHA1:	44f5fdf6902d114524afc110cd927f95f72903fa
SHA256:	ab77af2c0fe4a39b3e2ec7b7450ef36999baf7c66316f4b3934d5a60e124d50c
SHA512:	0b71a26ad38bbc0c1fb37854f636125012cfa6177afa1de4291756e5bdbe3bc07df157a1eb4ba7c3ee82055ece44ec21157ff14a6d66df14b0a720ad410afd21
SSDEEP:	1536:Klk8B6BXvSJtdFpIqRD0rKMIU/EmmwMOKEKkLQJDy2:crYVvOtdFp9gK88zOKEKkLQJd
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~...0.....0...Rich1.....PE..L...5>.O.....\.....@.....

File Icon

Icon Hash:	1adaf8c2cacada48

Static PE Info

General

Entrypoint:	0x40145c
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:	0x4F063E35 [Fri Jan 6 00:20:05 2012 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:	064d9ba8d40942674328edc4d8e0fd2c

Entrypoint Preview

Instruction
push 0040AB44h
call 00007F03F4CDB823h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
cmp byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xchg eax, ebp
test byte ptr [eax-1Dh], al

Instruction
push esp
dec ebp
or cl, byte ptr [ebx-5Fh]
popfd
adc byte ptr [esi-62h], ah

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x10904	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x12000	0xfd0	.rsrc
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	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x120	.text
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	0xfe00	0x10000	False	0.402313232422	data	5.25950000678	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x11000	0xa18	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x12000	0xfd0	0x1000	False	0.179443359375	data	2.23330666999	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x12328	0xca8	data		
RT_GROUP_ICON	0x12314	0x14	data		
RT_VERSION	0x120f0	0x224	data	Chinese	Taiwan

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaStrCat, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaLateMemSt, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, _CIsin, __vbaErase, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, __vbaVarTstEq, __vbaObjVar, _adj_fpatan, __vbaLateIdCallLd, __vbaRedim, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarAdd, __vbaVarDup, __vbaStrComp, __vbaVarLateMemCallLd, __vbaFpI4, __vbaLateMemCallLd, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

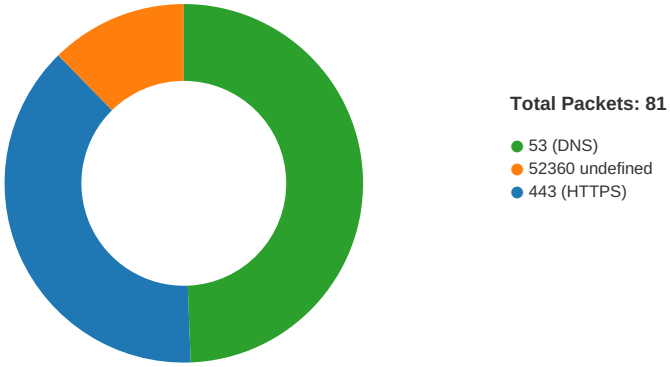
Description	Data
Translation	0x0404 0x04b0
InternalName	UNFUGI
FileVersion	1.00
CompanyName	Double Fine Productions
ProductName	COPR
ProductVersion	1.00
OriginalFilename	UNFUGI.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Chinese	Taiwan	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 08:12:01.061997890 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.104787111 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.104908943 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.105503082 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.148252010 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.161623001 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.161823034 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.161878109 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.161914110 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.162003040 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.162054062 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.179040909 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.222057104 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.222176075 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.224553108 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.271717072 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.500399113 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.500454903 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.500499010 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.500540972 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.500581980 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.500664949 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.500698090 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.503282070 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.503338099 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.504602909 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.506263018 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.506310940 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.506398916 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.509248972 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.509289980 CET	443	49754	172.217.23.1	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 08:12:01.509393930 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.509413958 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.512204885 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.512252092 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.513495922 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.514645100 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.514693975 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.514758110 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.543378115 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.543421984 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.543456078 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.543481112 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.544977903 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.545031071 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.545147896 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.547833920 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.547884941 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.548156977 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.550843954 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.550885916 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.550925016 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.550945997 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.553823948 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.553863049 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.555123091 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.556824923 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.556863070 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.556948900 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.557034016 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.559856892 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.559895992 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.562644005 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.562880993 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.562927008 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.565923929 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.565979958 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.566020966 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.566052914 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.568497896 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.568547964 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.568651915 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.571171999 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.571213007 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.571341038 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.573820114 CET	443	49754	172.217.23.1	192.168.2.3
Jan 11, 2021 08:12:01.574940920 CET	49754	443	192.168.2.3	172.217.23.1
Jan 11, 2021 08:12:01.864685059 CET	49755	52360	192.168.2.3	185.157.161.61
Jan 11, 2021 08:12:02.080409050 CET	52360	49755	185.157.161.61	192.168.2.3
Jan 11, 2021 08:12:02.082844019 CET	49755	52360	192.168.2.3	185.157.161.61
Jan 11, 2021 08:12:02.085031033 CET	49755	52360	192.168.2.3	185.157.161.61
Jan 11, 2021 08:12:02.341301918 CET	52360	49755	185.157.161.61	192.168.2.3
Jan 11, 2021 08:12:02.460266113 CET	52360	49755	185.157.161.61	192.168.2.3
Jan 11, 2021 08:12:02.467345953 CET	49755	52360	192.168.2.3	185.157.161.61
Jan 11, 2021 08:12:02.730282068 CET	52360	49755	185.157.161.61	192.168.2.3
Jan 11, 2021 08:12:07.461051941 CET	52360	49755	185.157.161.61	192.168.2.3
Jan 11, 2021 08:12:07.464006901 CET	49755	52360	192.168.2.3	185.157.161.61
Jan 11, 2021 08:12:07.720292091 CET	52360	49755	185.157.161.61	192.168.2.3
Jan 11, 2021 08:12:12.470863104 CET	52360	49755	185.157.161.61	192.168.2.3
Jan 11, 2021 08:12:12.516609907 CET	49755	52360	192.168.2.3	185.157.161.61
Jan 11, 2021 08:12:12.615115881 CET	49755	52360	192.168.2.3	185.157.161.61
Jan 11, 2021 08:12:12.880552053 CET	52360	49755	185.157.161.61	192.168.2.3
Jan 11, 2021 08:12:17.470907927 CET	52360	49755	185.157.161.61	192.168.2.3
Jan 11, 2021 08:12:17.473575115 CET	49755	52360	192.168.2.3	185.157.161.61
Jan 11, 2021 08:12:17.751055956 CET	52360	49755	185.157.161.61	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 08:12:22.480979919 CET	52360	49755	185.157.161.61	192.168.2.3
Jan 11, 2021 08:12:22.485896111 CET	49755	52360	192.168.2.3	185.157.161.61
Jan 11, 2021 08:12:22.750473022 CET	52360	49755	185.157.161.61	192.168.2.3
Jan 11, 2021 08:12:27.470366955 CET	52360	49755	185.157.161.61	192.168.2.3
Jan 11, 2021 08:12:27.473355055 CET	49755	52360	192.168.2.3	185.157.161.61

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 08:08:56.034691095 CET	63492	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:08:56.085526943 CET	53	63492	8.8.8.8	192.168.2.3
Jan 11, 2021 08:08:57.539195061 CET	60831	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:08:57.590198040 CET	53	60831	8.8.8.8	192.168.2.3
Jan 11, 2021 08:08:58.997844934 CET	60100	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:08:59.059166908 CET	53	60100	8.8.8.8	192.168.2.3
Jan 11, 2021 08:08:59.992403030 CET	53195	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:09:00.040544033 CET	53	53195	8.8.8.8	192.168.2.3
Jan 11, 2021 08:09:01.331974983 CET	50141	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:09:01.382942915 CET	53	50141	8.8.8.8	192.168.2.3
Jan 11, 2021 08:09:02.373349905 CET	53023	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:09:02.421516895 CET	53	53023	8.8.8.8	192.168.2.3
Jan 11, 2021 08:09:03.819200993 CET	49563	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:09:03.867108107 CET	53	49563	8.8.8.8	192.168.2.3
Jan 11, 2021 08:09:04.752156973 CET	51352	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:09:04.800386906 CET	53	51352	8.8.8.8	192.168.2.3
Jan 11, 2021 08:09:06.000201941 CET	59349	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:09:06.048269987 CET	53	59349	8.8.8.8	192.168.2.3
Jan 11, 2021 08:09:07.186904907 CET	57084	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:09:07.235117912 CET	53	57084	8.8.8.8	192.168.2.3
Jan 11, 2021 08:09:08.298183918 CET	58823	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:09:08.346400976 CET	53	58823	8.8.8.8	192.168.2.3
Jan 11, 2021 08:09:09.535099983 CET	57568	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:09:09.583108902 CET	53	57568	8.8.8.8	192.168.2.3
Jan 11, 2021 08:09:28.973202944 CET	50540	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:09:29.032784939 CET	53	50540	8.8.8.8	192.168.2.3
Jan 11, 2021 08:09:37.395679951 CET	54366	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:09:37.443648100 CET	53	54366	8.8.8.8	192.168.2.3
Jan 11, 2021 08:09:38.408901930 CET	53034	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:09:38.456998110 CET	53	53034	8.8.8.8	192.168.2.3
Jan 11, 2021 08:09:50.190967083 CET	57762	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:09:50.250932932 CET	53	57762	8.8.8.8	192.168.2.3
Jan 11, 2021 08:09:59.925106049 CET	55435	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:09:59.989722013 CET	53	55435	8.8.8.8	192.168.2.3
Jan 11, 2021 08:10:14.570008039 CET	50713	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:10:14.620887995 CET	53	50713	8.8.8.8	192.168.2.3
Jan 11, 2021 08:10:19.093394995 CET	56132	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:10:19.153832912 CET	53	56132	8.8.8.8	192.168.2.3
Jan 11, 2021 08:10:50.901370049 CET	58987	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:10:50.949441910 CET	53	58987	8.8.8.8	192.168.2.3
Jan 11, 2021 08:10:56.035588026 CET	56579	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:10:56.083764076 CET	53	56579	8.8.8.8	192.168.2.3
Jan 11, 2021 08:11:46.976233006 CET	60633	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:11:47.098877907 CET	53	60633	8.8.8.8	192.168.2.3
Jan 11, 2021 08:11:49.292625904 CET	61292	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:11:49.349224091 CET	53	61292	8.8.8.8	192.168.2.3
Jan 11, 2021 08:11:50.505830050 CET	63619	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:11:50.562891006 CET	53	63619	8.8.8.8	192.168.2.3
Jan 11, 2021 08:11:51.038547039 CET	64938	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:11:51.095021009 CET	53	64938	8.8.8.8	192.168.2.3
Jan 11, 2021 08:11:51.672871113 CET	61946	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:11:51.734428883 CET	53	61946	8.8.8.8	192.168.2.3
Jan 11, 2021 08:11:52.378628016 CET	64910	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:11:52.437542915 CET	53	64910	8.8.8.8	192.168.2.3
Jan 11, 2021 08:11:53.229226112 CET	52123	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 08:11:53.341048002 CET	53	52123	8.8.8.8	192.168.2.3
Jan 11, 2021 08:11:56.489923954 CET	56130	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:11:56.549196959 CET	53	56130	8.8.8.8	192.168.2.3
Jan 11, 2021 08:11:58.056026936 CET	56338	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:11:58.112437010 CET	53	56338	8.8.8.8	192.168.2.3
Jan 11, 2021 08:11:58.734754086 CET	59420	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:11:58.791250944 CET	53	59420	8.8.8.8	192.168.2.3
Jan 11, 2021 08:12:00.079550982 CET	58784	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:12:00.144229889 CET	53	58784	8.8.8.8	192.168.2.3
Jan 11, 2021 08:12:00.972094059 CET	63978	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:12:01.049339056 CET	53	63978	8.8.8.8	192.168.2.3
Jan 11, 2021 08:12:01.649941921 CET	62938	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:12:01.862879038 CET	53	62938	8.8.8.8	192.168.2.3
Jan 11, 2021 08:13:44.708283901 CET	55708	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:13:44.765296936 CET	53	55708	8.8.8.8	192.168.2.3
Jan 11, 2021 08:13:45.210810900 CET	56803	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:13:45.267163992 CET	53	56803	8.8.8.8	192.168.2.3
Jan 11, 2021 08:13:49.075913906 CET	57145	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:13:49.124016047 CET	53	57145	8.8.8.8	192.168.2.3
Jan 11, 2021 08:13:53.082916021 CET	55359	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:13:53.133667946 CET	53	55359	8.8.8.8	192.168.2.3
Jan 11, 2021 08:13:53.463779926 CET	58306	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:13:53.520102978 CET	53	58306	8.8.8.8	192.168.2.3
Jan 11, 2021 08:14:53.789446115 CET	64124	53	192.168.2.3	8.8.8.8
Jan 11, 2021 08:14:53.845844984 CET	53	64124	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 11, 2021 08:12:00.972094059 CET	192.168.2.3	8.8.8.8	0x8b1c	Standard query (0)	doc-0c-8c-docs.googleusercontent.com	A (IP address)	IN (0x0001)
Jan 11, 2021 08:12:01.649941921 CET	192.168.2.3	8.8.8.8	0x93ca	Standard query (0)	wealthyblessed.myddns.rocks	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 11, 2021 08:09:37.443648100 CET	8.8.8.8	192.168.2.3	0x3c5e	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jan 11, 2021 08:12:01.049339056 CET	8.8.8.8	192.168.2.3	0x8b1c	No error (0)	doc-0c-8c-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Jan 11, 2021 08:12:01.049339056 CET	8.8.8.8	192.168.2.3	0x8b1c	No error (0)	googlehosted.l.googleusercontent.com		172.217.23.1	A (IP address)	IN (0x0001)
Jan 11, 2021 08:12:01.862879038 CET	8.8.8.8	192.168.2.3	0x93ca	No error (0)	wealthyblessed.myddns.rocks		185.157.161.61	A (IP address)	IN (0x0001)
Jan 11, 2021 08:13:44.765296936 CET	8.8.8.8	192.168.2.3	0xa7c0	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

HTTPS Packets

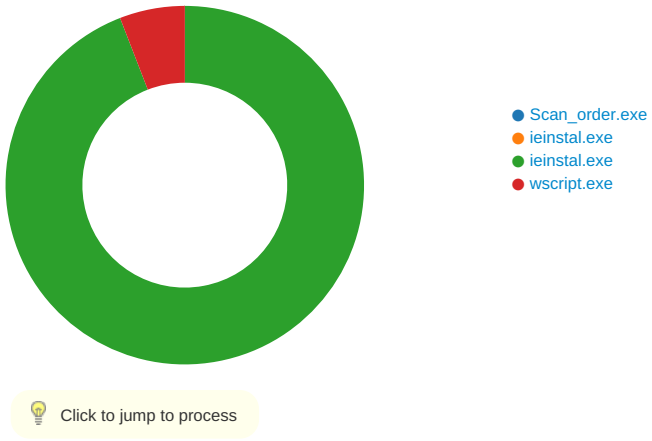
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 11, 2021 08:12:01.161914110 CET	172.217.23.1	443	192.168.2.3	49754	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Dec 15 15:47:09 CET 2020 Thu Jun 15 02:00:42 CEST 2017	Tue Mar 09 15:47:08 CET 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Scan_order.exe PID: 5260 Parent PID: 5568

General

Start time:	08:09:00
Start date:	11/01/2021
Path:	C:\Users\user\Desktop\Scan_order.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Scan_order.exe'
Imagebase:	0x400000
File size:	77824 bytes
MD5 hash:	04BE7ED51E345A56403DF4657B376990
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000000.00000000.204159990.000000000040A000.00000020.00020000.sdmp, Author: Florian Roth • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000000.00000002.595879092.000000000040A000.00000020.00020000.sdmp, Author: Florian Roth
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ieinstal.exe PID: 5468 Parent PID: 5260

General

Start time:	08:11:36
Start date:	11/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\Scan_order.exe'
Imagebase:	0x1250000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: 6128 Parent PID: 5260

General

Start time:	08:11:36
Start date:	11/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Scan_order.exe'
Imagebase:	0x1250000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000019.00000002.689367509.00000000032D1000.00000040.00000001.sdmp, Author: Joe Security
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 | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	32D3091	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	32D3091	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	32D3091	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	32D3091	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	32D3091	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	32D3091	InternetOpenUrlA
C:\Users\user\AppData\Roaming\remcos	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40564C	CreateDirectoryW
C:\Users\user\AppData\Roaming\remcos\logs.dat	append data or add subdirectory or create pipe instance | read attributes | synchronize	device | sparse file	synchronous io non alert | non directory file	success or wait	3	412D99	CreateFileW
C:\Users\user\AppData\Roaming\remcos	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	40564C	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\uninstall.vbs	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	412D99	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\remcos\logs.dat	success or wait	1	406D13	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\remcos\logs.dat	unknown	51	0d 0a 5b 32 30 32 31 2f 30 31 2f 31 31 20 30 38 3a 31 32 3a 30 30 20 4f 66 66 6c 69 6e 65 20 4b 65 79 6c 6f 67 67 65 72 20 53 74 61 72 74 65 64 5d 0d 0a	..[2021/01/11 08:12:00 Offline Keylogger Started]..	success or wait	3	412DCC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\uninstall.vbs	unknown	366	4f 00 6e 00 20 00 45 00 72 00 72 00 6f 00 72 00 20 00 52 00 65 00 73 00 75 00 6d 00 65 00 20 00 4e 00 65 00 78 00 74 00 0a 00 53 00 65 00 74 00 20 00 66 00 73 00 6f 00 20 00 3d 00 20 00 43 00 72 00 65 00 61 00 74 00 65 00 4f 00 62 00 6a 00 65 00 63 00 74 00 28 00 22 00 53 00 63 00 72 00 69 00 70 00 74 00 69 00 6e 00 67 00 2e 00 46 00 69 00 6c 00 65 00 53 00 79 00 73 00 74 00 65 00 6d 00 4f 00 62 00 6a 00 65 00 63 00 74 00 22 00 29 00 0a 00 66 00 73 00 6f 00 2e 00 44 00 65 00 6c 00 65 00 74 00 65 00 46 00 69 00 6c 00 65 00 20 00 22 00 43 00 3a 00 5c 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 46 00 69 00 6c 00 65 00 73 00 20 00 28 00 78 00 38 00 36 00 29 00 5c 00 69 00 6e 00 74 00 65 00 72 00 6e 00 65 00 74 00 20 00 65 00 78 00 70 00 6c 00 6f 00 72	O.n. .E.r.r.o.r. .R.e.s.u.m.e. .N.e.x.t...S.e.t. .f.s.o. .=. .C.r.e.a.t.e.O.b.j.e.c.t.(.". S.c.r.i.p.t.i.n.g...F.i.l.e.S. y.s.t.e.m.O.b.j.e.c.t.".)...f. s.o...D.e.l.e.t.e.F.i.l.e. .". C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s. .(.x.8.6.).\.i.n.t.e.r.n.e.t. .e.x.p.l.o.r	success or wait	1	412DCC	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Remcos-DPTVOE\	success or wait	1	40B71B	RegCreateKeyA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Remcos-DPTVOE	exepath	binary	A0 52 98 BB BE 5D 96 1A 66 5B 05 E1 86 87 86 1B 4D 4A 3F 0C 2C 7E 31 CF 4D 77 66 9A 1F E3 5C E5 22 C2 37 A4 62 3F 17 D0 32 DD F4 58 AA 08 5F 96 2D 2E 69 A5 F9 89 7F D5 9F 2C 69 B7 D2 6B C2 35 E5 10 14 B1 97 AF 32 53 F8 DE 66 7E EF BD 1F 66 87 A0 9D 36 6E 86 05 38 95 E4 DF 58 BB AA DC 7A 1D 62 9B C6 36 E8 20 22 7A A1 EE 89	success or wait	1	40B747	RegSetValueExA
HKEY_CURRENT_USER\Software\Remcos-DPTVOE	licence	unicode	1EEC0DFF4EC642D83246EB0D24CD72F5	success or wait	1	40B747	RegSetValueExA

Analysis Process: wscript.exe PID: 5776 Parent PID: 6128

General

Start time:	08:12:45
Start date:	11/01/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\uninstall.vbs'

Imagebase:	0xea0000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\uninstall.vbs	success or wait	1	7368A8A4	DeleteFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis