ID: 756118
Sample Name: SecuriteInfo.com.Exploit.CVE-2018-0798.4.11301.24836.rtf
Cookbook: defaultwindowsofficecookbook.jbs
Time: 16:49:20
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Copyright Joe Security LLC 2022

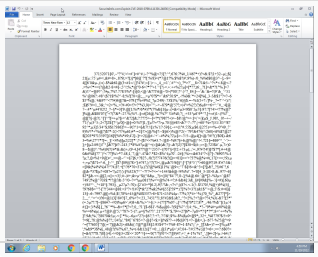
Windows Analysis Report

SecuriteInfo.com.Exploit.CVE-2018-0798.4.11301.24836.rtf

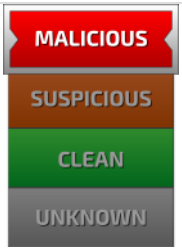
Overview

General Information

Sample Name:	SecuriteInfo.com.Exploit.CVE-2018-0798.4.11301.24836.rtf
Analysis ID:	756118
MD5:	f2de9aa2a7a3c9..
SHA1:	404dabf3e31da0..
SHA256:	d04bf8b1677e02..
Tags:	rtf
Infos:	



Detection



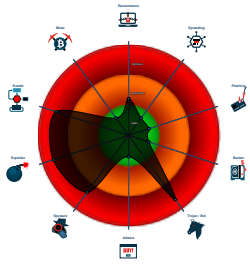
Snake Keylogger

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

Signatures

- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Yara detected Snake Keylogger
- Malicious sample detected (through…
- Yara detected Telegram RAT
- Yara detected AntiVM3
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal ftp login c…
- .NET source code references suspic…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 3024 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 1236 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - rinzearec84736.exe (PID: 296 cmdline: C:\Users\user\AppData\Roaming\rinzearec84736.exe MD5: D248194D56895A1FAE8914E81CD9B36A)
    - rinzearec84736.exe (PID: 648 cmdline: C:\Users\user\AppData\Roaming\rinzearec84736.exe MD5: D248194D56895A1FAE8914E81CD9B36A)
- EQNEDT32.EXE (PID: 2648 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
- **cleanup**

Malware Configuration

Threatname: Snake Keylogger


```
{
  "Exfil Mode": "SMTP",
  "Username": "arinzelog@saonline.xyz",
  "Password": "7213575aceACE@#$",
  "Host": "cp5ua.hyperhost.ua",
  "Port": "587"
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
SecuriteInfo.com.Exploit.CVE-2018-0798.4.11301.24836.rtf	SUSP_INDICATOR_RTF_MalVer_Objects	Detects RTF documents with non-standard version and embedding one of the object mostly observed in exploit (e.g. CVE-2017-11882) documents.	ditekSHen	• 0x1d14:$obj2: \objdata • 0x1edb:$obj3: \objupdate • 0x1cf0:$obj4: \objemb
SecuriteInfo.com.Exploit.CVE-2018-0798.4.11301.24836.rtf	INDICATOR_RTF_MalVer_Objects	Detects RTF documents with non-standard version and embeding one of the object mostly observed in exploit documents.	ditekSHen	• 0x1d14:$obj2: \objdata • 0x1edb:$obj3: \objupdate • 0x1cf0:$obj4: \objemb

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000000.919229211.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
00000006.00000000.919229211.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
00000006.00000000.919229211.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000006.00000000.919229211.0000000000402000.00000040.00000400.00020000.00000000.sdmp	MALWARE_Win_SnakeKeylogger	Detects Snake Keylogger	ditekSHen	• 0x176cc:$x1: $%SMTPDV$ • 0x176e2:$x2: $#TheHashHere%& • 0x18be3:$x3: %FTPDV$ • 0x18ca7:$x4: $%TelegramDv$ • 0x14f65:$x5: KeyLoggerEventArgs • 0x152fb:$x5: KeyLoggerEventArgs • 0x18c07:$m2: Clipboard Logs ID • 0x18e0d:$m2: Screenshot Logs ID • 0x18f1d:$m2: keystroke Logs ID • 0x19101:$m3: SnakePW • 0x18de5:$m4: \SnakeKeylogger\
00000006.00000000.919229211.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_SnakeKeylogger_af3faa65	unknown	unknown	• 0x13d90:$a1: get_encryptedPassword • 0x1407c:$a2: get_encryptedUsername • 0x13b9c:$a3: get_timePasswordChanged • 0x13c97:$a4: get_passwordField • 0x13da6:$a5: set_encryptedPassword • 0x15398:$a7: get_logins • 0x152fb:$a10: KeyLoggerEventArgs • 0x14f65:$a11: KeyLoggerEventArgsEventHandler
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.3.EQNEDT32.EXE.5c2588.0.raw.unpack	APT_NK_Methodology_Artificial_UserAgent_IE_Win7	Detects hard-coded User-Agent string that has been present in several APT37 malware families.	Steve Miller aka @stvemillertime	• 0x23f8:$a1: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko • 0x23f8:$a2: 4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28 57 69 6E 64 6F 77 73 20 4E 54 20 36 2E 31 3B 20 57 4F 57 36 34 3B 20 54 72 69 64 65 6E 74 2F 37 2E 30 3B 20 72 76 3A 31 31 2E 30 29 20 6C 69 6B 65 20 47 ...
2.3.EQNEDT32.EXE.5c2588.0.unpack	APT_NK_Methodology_Artificial_UserAgent_IE_Win7	Detects hard-coded User-Agent string that has been present in several APT37 malware families.	Steve Miller aka @stvemillertime	• 0x5f8:$a1: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko • 0x5f8:$a2: 4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28 57 69 6E 64 6F 77 73 20 4E 54 20 36 2E 31 3B 20 57 4F 57 36 34 3B 20 54 72 69 64 65 6E 74 2F 37 2E 30 3B 20 72 76 3A 31 31 2E 30 29 20 6C 69 6B 65 20 47 ...
2.2.EQNEDT32.EXE.5c2588.0.unpack	APT_NK_Methodology_Artificial_UserAgent_IE_Win7	Detects hard-coded User-Agent string that has been present in several APT37 malware families.	Steve Miller aka @stvemillertime	• 0x5f8:$a1: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko • 0x5f8:$a2: 4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28 57 69 6E 64 6F 77 73 20 4E 54 20 36 2E 31 3B 20 57 4F 57 36 34 3B 20 54 72 69 64 65 6E 74 2F 37 2E 30 3B 20 72 76 3A 31 31 2E 30 29 20 6C 69 6B 65 20 47 ...
2.2.EQNEDT32.EXE.5c2588.0.raw.unpack	APT_NK_Methodology_Artificial_UserAgent_IE_Win7	Detects hard-coded User-Agent string that has been present in several APT37 malware families.	Steve Miller aka @stvemillertime	• 0x23f8:$a1: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko • 0x23f8:$a2: 4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28 57 69 6E 64 6F 77 73 20 4E 54 20 36 2E 31 3B 20 57 4F 57 36 34 3B 20 54 72 69 64 65 6E 74 2F 37 2E 30 3B 20 72 76 3A 31 31 2E 30 29 20 6C 69 6B 65 20 47 ...

Source	Rule	Description	Author	Strings
5.2.rinzearec84736.exe.33d8c18.9.unpack	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x198d3:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x18b05:$a3: \Google\Chrome\User Data\Default\Login Data • 0x18f38:$a4: \Orbitum\User Data\Default\Login Data • 0x1a05f:$a5: \Kometa\User Data\Default\Login Data
Click to see the 46 entries				

Sigma Signatures

Exploits

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Exploits

Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

Office equation editor establishes network connection

Networking

May check the online IP address of the machine

Yara detected Generic Downloader

System Summary

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Malware Analysis System Evasion

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion

HIPS / PFW / Operating System Protection Evasion

.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Snake Keylogger

Yara detected Telegram RAT

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal ftp login credentials

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

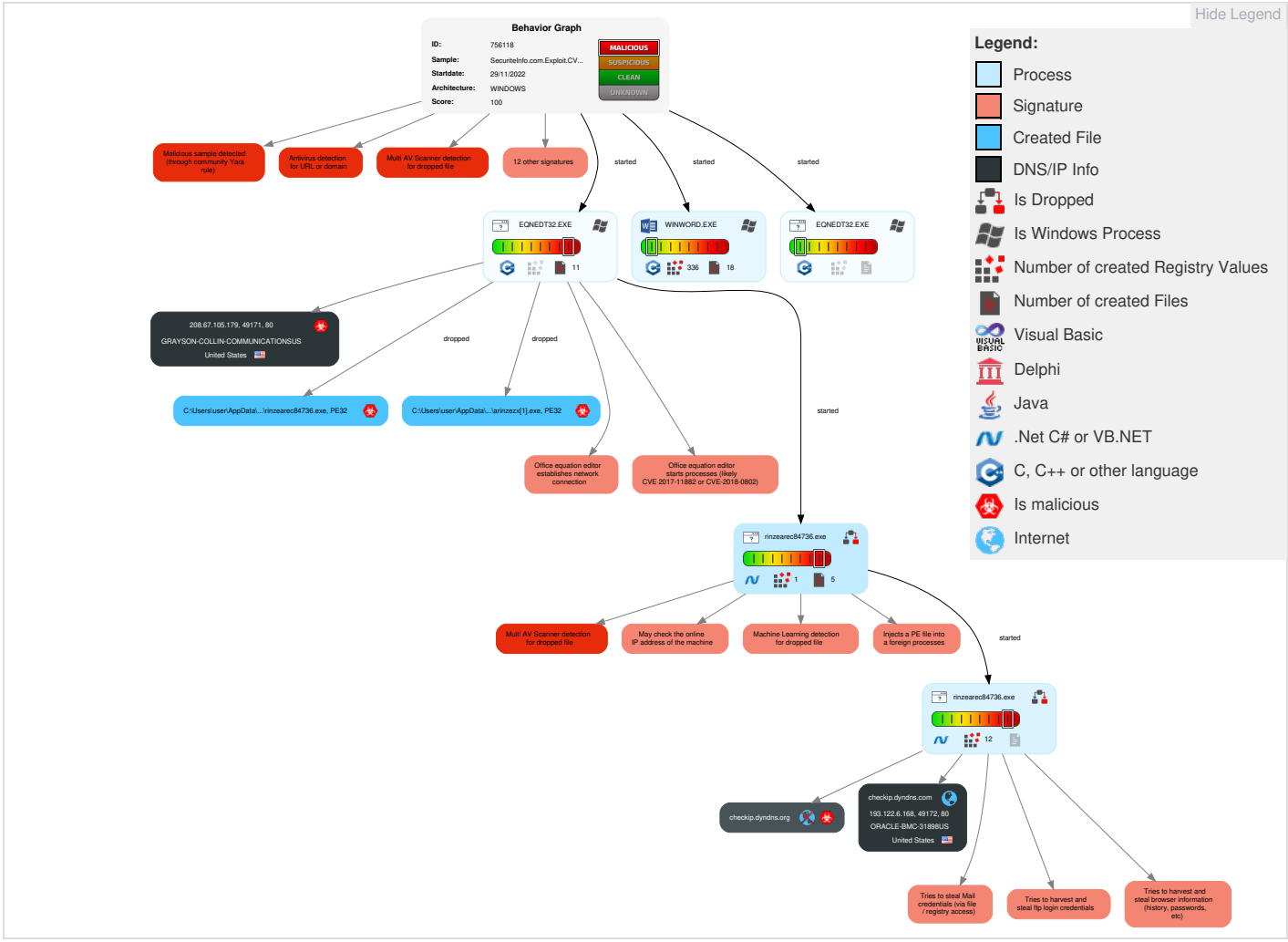
Yara detected Snake Keylogger

Yara detected Telegram RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	Path Interception	1 1 1 Process Injection	1 Masquerading	2 OS Credential Dumping	2 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 3 Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 2 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 System Network Configuration Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 Obfuscated Files or Information	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 Software Packing	DCSync	1 3 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

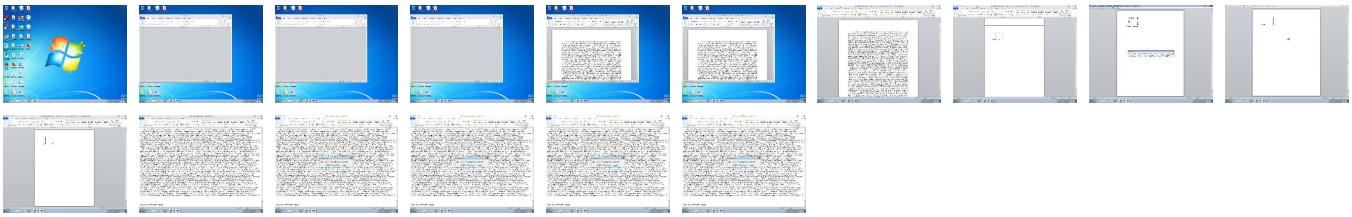
Behavior Graph

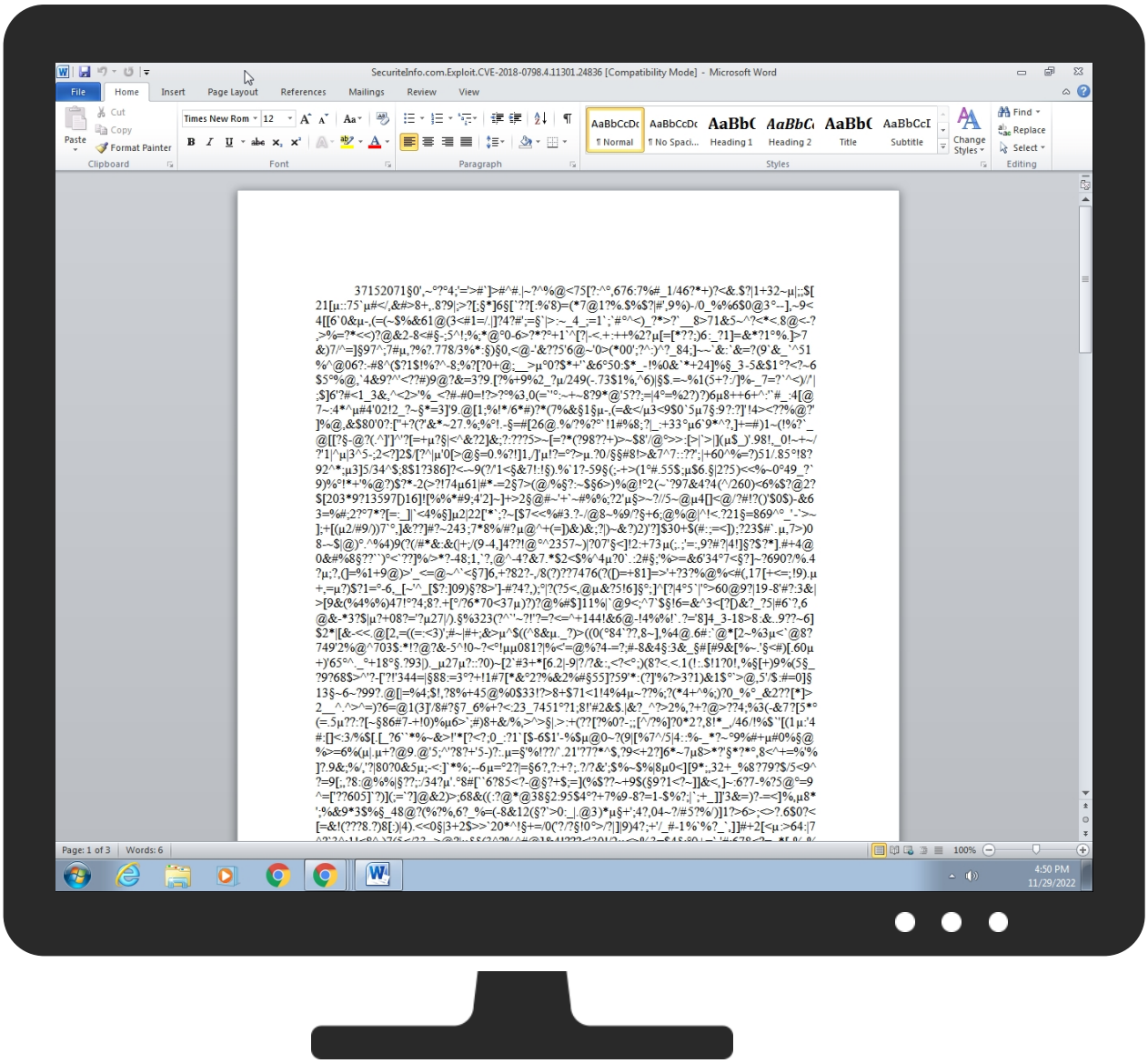


Screenshots

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
SecuriteInfo.com.Exploit.CVE-2018-0798.4.11301.24836.rtf	20%	ReversingLabs	Document-RTF.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\rinzearec84736.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\arinzezx[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\arinzezx[1].exe	40%	ReversingLabs	ByteCode-MSIL.Trojan.Mamut	
C:\Users\user\AppData\Roaming\rinzearec84736.exe	40%	ReversingLabs	ByteCode-MSIL.Trojan.Mamut	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.rinzearec84736.exe.400000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://checkip.dyndns.org	0%	URL Reputation	safe	
http://checkip.dyndns.orgP	0%	URL Reputation	safe	
http://checkip.dyndns.org/	0%	URL Reputation	safe	
http://checkip.dyndns.com	0%	URL Reputation	safe	
http://checkip.dyndns.org/q	0%	URL Reputation	safe	
http://208.67.105.179/arinzezx.exej	100%	Avira URL Cloud	malware	
http://208.67.105.179/arinzezx.exe	100%	Avira URL Cloud	malware	
http://208.67.105.179/arinzezx.exemmC:	100%	Avira URL Cloud	malware	
http://208.67.105.179/arinzezx.exeC:	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
checkip.dyndns.com	193.122.6.168	true	false		unknown
checkip.dyndns.org	unknown	unknown	true		unknown

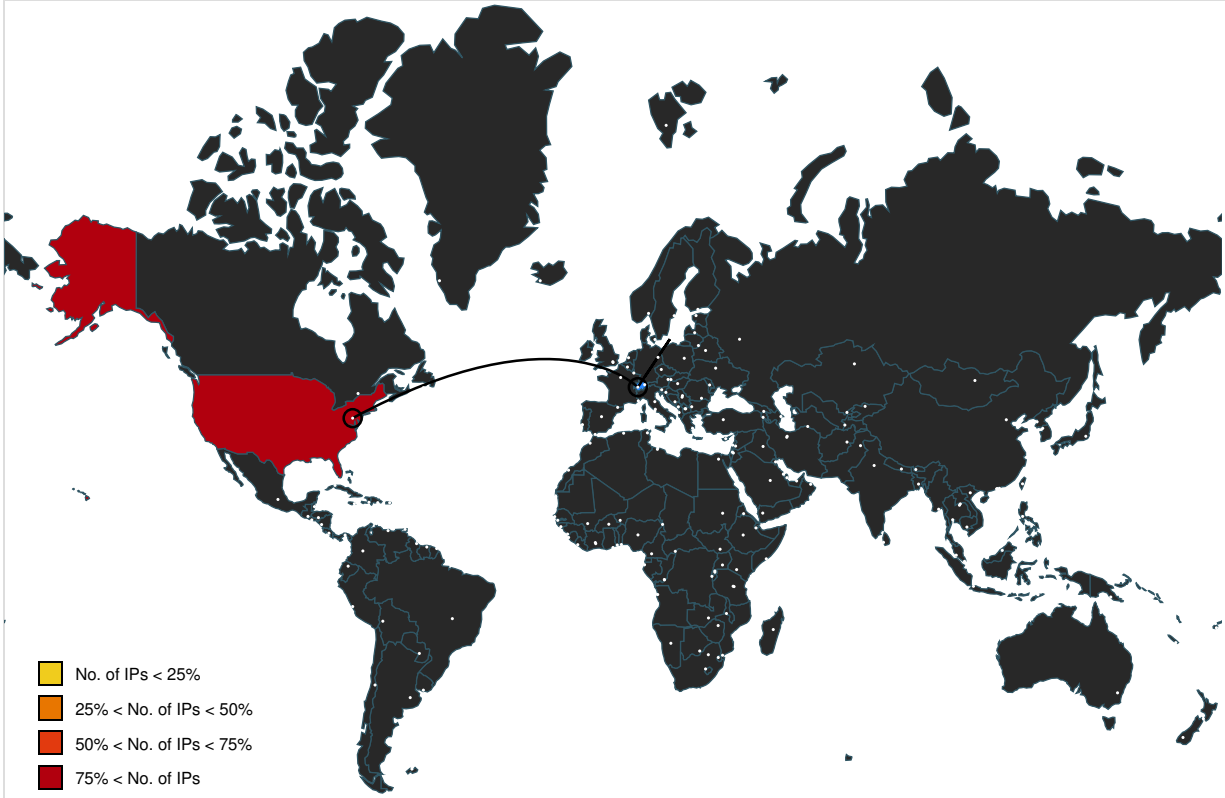
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://208.67.105.179/arinzezx.exe	true	• Avira URL Cloud: malware	unknown
http://checkip.dyndns.org/	false	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://208.67.105.179/arinzezx.exemmC:	EQNEDT32.EXE, 00000002.00000002.90827048 4.000000000058F000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://208.67.105.179/arinzezx.exej	EQNEDT32.EXE, 00000002.00000002.90827048 4.000000000058F000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://checkip.dyndns.org	rinzearec84736.exe, 00000006.00000002.11 73839391.00000000023B9000.00000004.00000 800.00020000.00000000.sdmp, rinzearec84736.exe, 00000006.00000002.1173667930.0000000002361 000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://checkip.dyndns.orgP	rinzearec84736.exe, 00000006.00000002.11 73667930.0000000002361000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://checkip.dyndns.com	rinzearec84736.exe, 00000006.00000002.11 73839391.00000000023B9000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org/bot	rinzearec84736.exe, 00000005.00000002.92 4373144.0000000003374000.00000004.000008 00.00020000.00000000.sdmp, rinzearec84736.exe, 00000006.00000000.919229211.000000000402000.00000040.00000400.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	rinzearec84736.exe, 00000006.00000002.11 73667930.0000000002361000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://208.67.105.179/arinzezx.exeC:	EQNEDT32.EXE, 00000002.00000003.90798913 0.0000000000602000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://checkip.dyndns.org/q	rinzearec84736.exe, 00000005.00000002.92 4373144.0000000003374000.00000004.000008 00.00020000.00000000.sdmp, rinzearec84736.exe, 00000006.00000000.919229211.000000000402000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.122.6.168	checkip.dyndns.com	United States		31898	ORACLE-BMC-31898US	false
208.67.105.179	unknown	United States		20042	GRAYSON-COLLIN-COMMUNICATIONSUS	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756118
Start date and time:	2022-11-29 16:49:20 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Exploit.CVE-2018-0798.4.11301.24836.rtf
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	10
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.spyw.expl.evad.winRTF@7/6@2/2

Copyright Joe Security LLC 2022

EGA Information:	• Successful, ratio: 66.7%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 93% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .rtf • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Active ActiveX Object • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WerFault.exe, svchost.exe
- TCP Packets have been reduced to 100
- Execution Graph export aborted for target EQNEDT32.EXE, PID 1236 because there are no executed function
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtEnumerateValueKey calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: SecuriteInfo.com.Exploit.CVE-2018-0798.4.11301.24836.rtf

Simulations

Behavior and APIs

Time	Type	Description
16:50:16	API Interceptor	250x Sleep call for process: EQNEDT32.EXE modified
16:50:21	API Interceptor	254x Sleep call for process: rinzearec84736.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\arinzezx[1].exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

Category:	dropped
Size (bytes):	842240
Entropy (8bit):	7.591937795879761
Encrypted:	false
SSDEEP:	24576:62w3IksIWwMIA7ujjbdDerIY/HGDdEPf:XRksIWwMfQDef/HPP
MD5:	D248194D56895A1FAE8914E81CD9B36A
SHA1:	3F70834B9D80A8CAFB2FFBEE029D577660C90DCD
SHA-256:	61008831508DC534A4D55097106589C5761A011C6DC710977217DE7ED884B996
SHA-512:	D6B5B3F13C908BB1EB953091FC83FA65F3F4B650191E82D72CFAB17B5A7DDB452452C0F5E3B85A8A4FF624223657EC8FA5BA57D80DC84109244D64A1AE86A25D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 40%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...-..c.....0..... .....@.. .....@..... ..@.....O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....<.....l...8u..X{.....^..}.....(.....(.....*.0.....s.....o.....(.....*...0.....s.....o.....(.....*...0.....s.....o..... (.....*...0.....s.....o.....(.....*...0..+.....,..{.....+...,..{....o.....(.....*..0..r.....(....s.....s....}.....s....}.....s....}.....s....}.....(.....{....(....o.....{.....o.....{.....o .....{....r...p "..@A...s!...o".....{....(#...o$.....{.... .... ..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\SecuriteInfo.com.Exploit.CVE-2018-0798.4.11301.24836.LNK

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue Mar 8 15:45:56 2022, mtime=Tue Mar 8 15:45:56 2022, atime=Tue Nov 29 23:50:14 2022, length=14484, window=hide
Category:	dropped
Size (bytes):	1224
Entropy (8bit):	4.561234909144671
Encrypted:	false
SSDEEP:	24:8ZN/XT9SU+MZTHCdH6eChrHHCdHDDv3qvu7D:8ZN/XTQr2THCF6hzHCFqv0D
MD5:	64F2897E2EE75D5959D062DD2925BB94
SHA1:	55400D4BDA7A405A3A17F1DC3CE4E349B22978E8
SHA-256:	490550A0B7F27F22660AF912CE716CA2792BE0D245A49B9712962A3AFBB65D5F
SHA-512:	4D3387646A5D3614A072614EB6AB464085E8A4EC36689EF1297D0B862663138904E9E9DB64A29E8D26E9DB83A1846ADD5A71145F10CFE90D7287667F2013B53E
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...w.p..3..w.p..3....h.U....8.....#....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l. ,.-.2.1.8.1.3.....L.1.....hT....user.8.....QK.XhT..*...&=....U.....A.l.b.u.s.....z.1.....hT....Desktop.d.....QK.XhT..*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2 .1.7.6.9.....2..8..~UH. .SECURI~1.RTF.....hT..hT..*...r....'.....S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...E.x.p.l.o.i.t...C.V.E.-.2.0.1.8.-.0.7.9.8...4...1.1.3.0.1...2.4.8.3.6...r.t.f..... .....-...8...[.....?J.....C:\Users\..#.....\\642294\Users.user\Desktop\SecuriteInfo.com.Exploit.CVE-2018-0798.4.11301.24836.rtf.O.....\.....\.....\.....\... .\.D.e.s.k.t.o.p.\.S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...E.x.p.l.o.i.t...C.V.E.-.2.0.1.8.-.0.7.9.8...4...1.1.3.0.1...2.4.8.3.6...r.t.f.....:..,.LB.)...Ag.....1SPS.XF.L8C.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Generic INItialization configuration [misc]
Category:	dropped
Size (bytes):	156
Entropy (8bit):	5.092884717261391
Encrypted:	false
SSDEEP:	3:bDuMJluscbcK+KUmjAomxW9rbcK+KUmjAov:bCVwKhRAOrwKhRAy
MD5:	2794692EF70251257065A2A957CC1EAC
SHA1:	CB3DA2288CFB2A84DAEFEC9D6BB5B82CA6F62378
SHA-256:	95BC66B886BF0A8C136DBE53867C0683976E80D24B5740DF5799507C941E2ACF
SHA-512:	C7842286162E773DE700B4DDB9BA43F94B8C175A517C4DF5886A1319398F3DB6EAF51DAD5E4C7F1193857A5FD4D1194D909068D296E56AA2CBA53E7B144BD68
Malicious:	false
Reputation:	low
Preview:	[folders]..Templates.LNK=0..SecuriteInfo.com.Exploit.CVE-2018-0798.4.11301.24836.LNK=0..[misc]..SecuriteInfo.com.Exploit.CVE-2018-0798.4.11301.24836.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped

Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHH/cgQfmW+eMdln:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F05265 5
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....15.....25.....@35.....35.....z.....p45.....x...

C:\Users\user\AppData\Roaming\rinzearec84736.exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	842240
Entropy (8bit):	7.591937795879761
Encrypted:	false
SSDEEP:	24576:62w3lksIWwMIA7ujjbdDerIY/HGDdEPf:XRksIWwMfQDef/HPP
MD5:	D248194D56895A1FAE8914E81CD9B36A
SHA1:	3F70834B9D80A8CAFB2FFBEE029D577660C90DCD
SHA-256:	61008831508DC534A4D55097106589C5761A011C6DC710977217DE7ED884B996
SHA-512:	D6B5B3F13C908BB1EB953091FC83FA65F3F4B650191E82D72CFAB17B5A7DDB452452C0F5E3B85A8A4FF624223657EC8FA5BA57D80DC84109244D64A1AE86A25 D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 40%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...-..c.....0..... .....@.. .....@..... ..@.....O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....<.....l...8u..X{.....^..}.....(.....(.....*.0.....s.....o.....(.....*...0.....s.....o.....(.....*...0.....s.....o..... (.....*...0.....s.....o.....(.....*...0..+.....,..{.....+.....,..{....o.....(.....*..0..r.....(....s.....s....}.....s....}.....s....}.....s....}.....(.....{....(....o.....{.....o.....{.....o .....{....r...p "..@A...s!...o".....{....(#...o$.....{.... .... ..

C:\Users\user\Desktop\~$curiteInfo.com.Exploit.CVE-2018-0798.4.11301.24836.rtf

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHH/cgQfmW+eMdln:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F05265 5
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....15.....25.....@35.....35.....z.....p45.....x...

Static File Info

General

File type:	Rich Text Format data, version 1
Entropy (8bit):	5.4057733010793765
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	SecuriteInfo.com.Exploit.CVE-2018-0798.4.11301.24836.rtf

File size:	14484
MD5:	f2de9aa2a7a3c9890d2f799adc95c35b
SHA1:	404dabf3e31da0bbf666df6397f803983961794f
SHA256:	d04bf8b1677e02ada795c9a0e84abfca0ba2c1565736e9f34115783af32be764
SHA512:	46dde73a4611e2f99f6ddb8676442f1b6c93c659e61d43cf4bdc4cae331ff57396b363f2116297224b551c88743ae55261acc3e25d03d240fd1950944579 54f8
SSDEEP:	384:JR3ll9FfS6+D+uk/LQn9ze6faYZ0pzTOv2ZgLo:LIlfIyuBe4iTOeZgLo
TLSH:	4A526D7CE7445A9FDB9DB2F9121B722C069CBD2573D191EA0AB87333F42982E6707094
File Content Preview:	{\rtf1.....{\mmodso257517810 \#}.{\6371520 71.0',~.?.4;'=>#`]>#^#.|~?^%@<75[?:^.,676:7%#_1/46?*+)?<&.$?\|1+32~.\|;;$[21[.::75`.#</,&#>8+,.8?9|;>?[;.*]6.[`?? [:%'8)=(*7@1?%.$%$?|#',9%)-/0_%%6$0@3.--],~9<4[[6`0&.-,(=(~$%&61@(3<#1=/.|]?4?#';=.`|>:~_4_

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

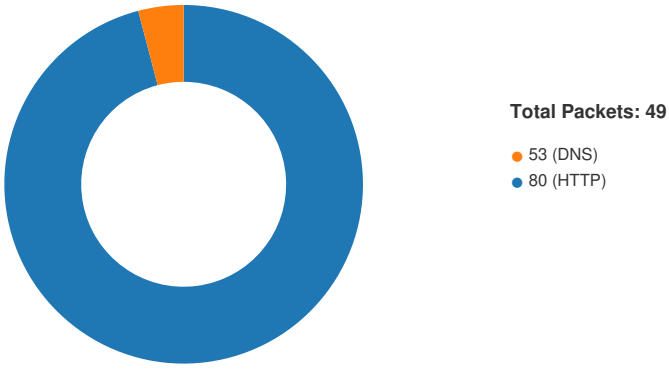
Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	00001D1Eh								no

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:50:19.295629025 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.324132919 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.324248075 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.325438976 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.353758097 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.357974052 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.358020067 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.358045101 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.358069897 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.358093977 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.358114004 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.358134031 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.358160019 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.358185053 CET	80	49171	208.67.105.179	192.168.2.22

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:50:19.358211040 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.358222008 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.358247042 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.358272076 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.358283043 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.358308077 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.358340979 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.371212959 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.386260033 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.386347055 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.386384964 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.386415005 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.386415005 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.386436939 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.386460066 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.386497021 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.386508942 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.386543036 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.386555910 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.386609077 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.386640072 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.386661053 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.386674881 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.386712074 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.386733055 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.386754990 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.386765957 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.386809111 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.386826038 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.386845112 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.386858940 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.386900902 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.386921883 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.386962891 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.386984110 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.387001038 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.387020111 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.387054920 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.387073994 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.387110949 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.387125969 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.387161970 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.387176991 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.387214899 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.387236118 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.387275934 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.387286901 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.387327909 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.404854059 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.415020943 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.415066957 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.415092945 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.415112019 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.415131092 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.415157080 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.415157080 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.415194035 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.427968979 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.428016901 CET	80	49171	208.67.105.179	192.168.2.22

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:50:19.428041935 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.428066015 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.428091049 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.428124905 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.428138018 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.428138018 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.428167105 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.428193092 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.428220987 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.428232908 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.428258896 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.428273916 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.428289890 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.428307056 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.428337097 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.428349972 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.428371906 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.428390026 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.428416014 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.428426981 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.428447962 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.428459883 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.428484917 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.428497076 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.428510904 CET	49171	80	192.168.2.22	208.67.105.179
Nov 29, 2022 16:50:19.428529024 CET	80	49171	208.67.105.179	192.168.2.22
Nov 29, 2022 16:50:19.428538084 CET	49171	80	192.168.2.22	208.67.105.179

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 16:50:27.643722057 CET	55868	53	192.168.2.22	8.8.8.8
Nov 29, 2022 16:50:27.662585974 CET	53	55868	8.8.8.8	192.168.2.22
Nov 29, 2022 16:50:27.702518940 CET	49688	53	192.168.2.22	8.8.8.8
Nov 29, 2022 16:50:27.721494913 CET	53	49688	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 16:50:27.643722057 CET	192.168.2.22	8.8.8.8	0xb186	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:50:27.702518940 CET	192.168.2.22	8.8.8.8	0x63a8	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 16:50:27.662585974 CET	8.8.8.8	192.168.2.22	0xb186	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:50:27.662585974 CET	8.8.8.8	192.168.2.22	0xb186	No error (0)	checkip.dyndns.com		193.122.6.168	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:50:27.662585974 CET	8.8.8.8	192.168.2.22	0xb186	No error (0)	checkip.dyndns.com		132.226.8.169	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:50:27.662585974 CET	8.8.8.8	192.168.2.22	0xb186	No error (0)	checkip.dyndns.com		158.101.44.242	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:50:27.662585974 CET	8.8.8.8	192.168.2.22	0xb186	No error (0)	checkip.dyndns.com		132.226.247.73	A (IP address)	IN (0x0001)	false

Copyright Joe Security LLC 2022

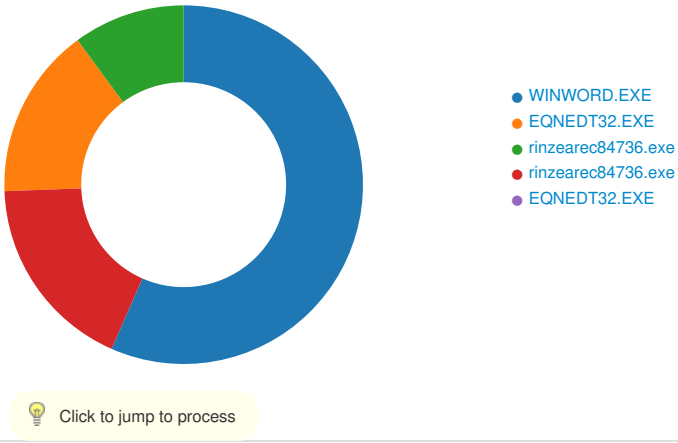
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 16:50:27.662585974 CET	8.8.8.8	192.168.2.22	0xb186	No error (0)	checkip.dyndns.com		193.122.130.0	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:50:27.721494913 CET	8.8.8.8	192.168.2.22	0x63a8	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 16:50:27.721494913 CET	8.8.8.8	192.168.2.22	0x63a8	No error (0)	checkip.dyndns.com		193.122.130.0	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:50:27.721494913 CET	8.8.8.8	192.168.2.22	0x63a8	No error (0)	checkip.dyndns.com		132.226.8.169	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:50:27.721494913 CET	8.8.8.8	192.168.2.22	0x63a8	No error (0)	checkip.dyndns.com		132.226.247.73	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:50:27.721494913 CET	8.8.8.8	192.168.2.22	0x63a8	No error (0)	checkip.dyndns.com		158.101.44.242	A (IP address)	IN (0x0001)	false
Nov 29, 2022 16:50:27.721494913 CET	8.8.8.8	192.168.2.22	0x63a8	No error (0)	checkip.dyndns.com		193.122.6.168	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- 208.67.105.179
- checkip.dyndns.org

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: **3024**, Parent PID: **576**

General

Target ID:	0
Start time:	16:50:15
Start date:	29/11/2022

Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x13fe90000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Registry Activities

Analysis Process: EQNEDT32.EXE PID: **1236**, Parent PID: **576**

General

Target ID:	2
Start time:	16:50:16
Start date:	29/11/2022
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
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	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	5B6F2C	URLDownloadToFileW
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	5B6F2C	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	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	5B6F2C	URLDownloadToFileW
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	5B6F2C	URLDownloadToFileW
C:\Users\user\AppData\Roaming	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	5B6F2C	URLDownloadToFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	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	5B6F2C	URLDownloadToFileW
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	5B6F2C	URLDownloadToFileW
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	5B6F2C	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\History	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	5B6F2C	URLDownloadToFileW
C:\Users\user\AppData\Roaming\rinzearec84736.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	5B6F2C	URLDownloadToFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\arinzezx[1].exe	0	735	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 50 45 00 00 4c 01 03 00 2d fd fd 63 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 0c 00 00 06 00 00 00 00 00 00 fd fd 0c 00 00 20 00 00 00 00 0d 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 0d 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL-c0 @ @@	success or wait	1	5B6F2C	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\arinzezx[1].exe	735	8192	11 00 73 1a 00 00 06 0a 06 6f 15 00 00 0a 00 02 28 16 00 00 0a 00 2a 00 00 13 30 02 00 2b 00 00 00 05 00 00 11 00 03 2c 0b 02 7b 01 00 00 04 14 fd 03 2b 01 16 0a 06 2c 0e 00 02 7b 01 00 00 04 6f 17 00 00 0a 00 00 02 03 28 18 00 00 0a 00 2a 00 13 30 06 00 72 04 00 00 06 00 00 11 00 fd 02 00 00 02 28 19 00 00 0a 73 1a 00 00 0a 0a 02 73 1b 00 00 0a 7d 02 00 00 04 02 73 1b 00 00 0a 7d 03 00 00 04 02 73 1b 00 00 0a 7d 04 00 00 04 02 73 1b 00 00 0a 7d 05 00 00 04 02 28 1c 00 00 0a 00 02 7b 02 00 00 04 28 1d 00 00 0a 6f 1e 00 00 0a 00 02 7b 02 00 00 04 19 6f 1f 00 00 0a 00 02 7b 02 00 00 04 16 6f 20 00 00 0a 00 02 7b 02 00 00 04 72 01 00 00 70 22 00 00 40 41 17 19 16 73 21 00 00 0a 6f 22 00 00 0a 00 02 7b 02 00 00 04 28 23 00 00 0a 6f 24 00 00 0a 00 02 7b 02 00	so(*0+,{+,{o(*0r(ss}s}s}s}({{o{o{o {rp"@As!o"{(#o${	success or wait	1	5B6F2C	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\arinzezx[1].exe	8927	1072	09 00 70 6f 27 00 00 0a 00 02 7b 27 00 00 04 1f 2a 6f 67 00 00 0a 00 02 7b 27 00 00 04 20 fd 00 00 00 1f 20 73 28 00 00 0a 6f 29 00 00 0a 00 02 7b 27 00 00 04 1f 26 6f 2a 00 00 0a 00 02 7b 27 00 00 04 17 6f 68 00 00 0a 00 02 7b 28 00 00 04 17 6f 49 00 00 0a 00 02 7b 28 00 00 04 28 4a 00 00 0a 6f 1e 00 00 0a 00 02 7b 28 00 00 04 72 01 00 00 70 22 00 00 40 41 17 19 16 73 21 00 00 0a 6f 22 00 00 0a 00 02 7b 28 00 00 04 28 23 00 00 0a 6f 24 00 00 0a 00 02 7b 28 00 00 04 1f 61 20 14 01 00 00 73 25 00 00 0a 6f 26 00 00 0a 00 02 7b 28 00 00 04 72 fd 09 00 70 6f 27 00 00 0a 00 02 7b 28 00 00 04 1f 50 1f 18 73 28 00 00 0a 6f 29 00 00 0a 00 02 7b 28 00 00 04 1f 25 6f 2a 00 00 0a 00 02 7b 28 00 00 04 72 fd 09 00 70 6f 2b 00 00 0a 00 02 7b 29 00 00 04 17 6f 49 00 00	po'{'*og{' s(o){'&o* {'oh{(ol{((Jo{(rp"@As!o" {((#o${(a s%o&{ (rpo'{(Ps(o){(%o*{(rpo+ {}ol	success or wait	1	5B6F2C	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\rinzearec84736.exe	0	9999	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 50 45 00 00 4c 01 03 00 2d fd fd 63 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 0c 00 00 06 00 00 00 00 00 00 fd fd 0c 00 00 20 00 00 00 00 0d 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 0d 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL-c0 @ @@	success or wait	1	5B6F2C	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\arinzezx[1].exe	13471	8192	7d 39 00 00 04 02 02 7b 39 00 00 04 6f 60 00 00 0a 7d 3a 00 00 04 2b 21 02 7b 3e 00 00 04 6f 51 00 00 0a 02 7b 3a 00 00 04 72 51 0e 00 70 6f 61 00 00 0a 6f 52 00 00 0a 26 02 7b 3a 00 00 04 6f 63 00 00 0a 0a 06 2d fd 02 7b 3a 00 00 04 6f 6c 00 00 0a 00 02 7b 38 00 00 04 6f 45 00 00 0a 00 2a 13 30 02 00 2b 00 00 00 05 00 00 11 00 03 2c 0b 02 7b 3b 00 00 04 14 fd 03 2b 01 16 0a 06 2c 0e 00 02 7b 3b 00 00 04 6f 17 00 00 0a 00 00 02 03 28 18 00 00 0a 00 2a 00 13 30 06 00 fd 04 00 00 06 00 00 11 00 fd 07 00 00 02 28 19 00 00 0a 73 1a 00 00 0a 0a 02 73 47 00 00 0a 7d 3c 00 00 04 02 73 57 00 00 0a 7d 3d 00 00 04 02 73 57 00 00 0a 7d 3e 00 00 04 02 73 1b 00 00 0a 7d 3f 00 00 04 02 73 1b 00 00 0a 7d 40 00 00 04 02 28 1c 00 00 0a 00 02 7b 3c 00 00 04 17 6f 49 00 00	}9{9o`}:+! {>oQ{:rQpoaoR&{:oc-{ :ol{8oE*0+,{;+,{;o(*0(ssG}<sW}=sW}>s}?s}@({<ol	success or wait	109	5B6F2C	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\rinzearec84736.exe	9999	28292	04 17 6f 58 00 00 0a 00 02 7b 2e 00 00 04 6f 51 00 00 0a 19 fd 13 00 00 01 25 16 72 fd 0a 00 70 fd 25 17 72 fd 0a 00 70 fd 25 18 72 fd 0a 00 70 fd 6f 69 00 00 0a 00 02 7b 2e 00 00 04 20 2f 01 00 00 20 40 01 00 00 73 25 00 00 0a 6f 26 00 00 0a 00 02 7b 2e 00 00 04 72 fd 0a 00 70 6f 27 00 00 0a 00 02 7b 2e 00 00 04 20 fd 00 00 00 1f 20 73 28 00 00 0a 6f 29 00 00 0a 00 02 7b 2e 00 00 04 1f 2b 6f 2a 00 00 0a 00 02 7b 2f 00 00 04 17 6f 65 00 00 0a 00 02 7b 2f 00 00 04 72 01 00 00 70 22 00 00 40 41 16 19 16 73 21 00 00 0a 6f 22 00 00 0a 00 02 7b 2f 00 00 04 20 2f 01 00 00 20 fd 00 00 00 73 25 00 00 0a 6f 26 00 00 0a 00 02 7b 2f 00 00 04 19 18 19 18 73 4d 00 00 0a 6f 5e 00 00 0a 00 02 7b 2f 00 00 04 72 03 0b 00 70 6f 27 00 00 0a 00 02 7b 2f 00 00 04 1f 2a 6f 67	oX{.oQ%rp%rp%rpoi{. / @s%o&{.rpo'{. s(o){.+o* {/oe{/rp"@As!o"{/ / s%o& {/sMo^{/rpo'{/*og	success or wait	23	5B6F2C	URLDownloadToFileW
C:\Users\user\AppData\Roaming\rinzearec84736.exe	800889	41351	39 fd fd fd fd fd 1e fd fd 52 6f fd 33 4a fd fd 00 58 fd c3 07 fd fd 79 27 2c 77 b0 42 fd 1e fd fd fd 7e 14 fd 55 71 32 76 5d fd 12 fd 28 fd fd fd fd fd fd 05 fd 08 1e fd 26 35 fd 7f fd fd 4a 34 fd 1e fd fd 1c fd 30 fd 57 02 00 4c 7f 34 41 26 6d 4a fd fd fd fd 7c fd 14 fd 00 fd fd 35 fd 5b 19 01 60 69 02 59 09 00 4a 5e fd fd 00 24 5f fd 38 fd 34 fd 24 74 fd fd 2b 22 46 00 50 3f 4a 28 fd 08 58 fd fd 3a fd 3c fd 75 5e 73 20 63 fd fd 1e fd 5d fd fd fd 2f fd 6d fd 20 fd fd fd 05 20 0c fd fd 5e 10 7f fd 2b f1 7c fd 13 00 2b 02 2c 1f 7f fd 03 fd fd 33 fd fd fd 02 28 11 48 fd 07 d5 10 77 fd 2d fd fd 26 51 fd 14 fd fd 3a 72 fd 28 fd fd 1e 08 40 55 fd 74 7f 63 fd 54 fd fd 11 fd fd 10 fd 29 20 fd 74 60 fd 6b fd fd fd 4f fd fd 00 5c	9Ro3JXy'wB~Uq2v](&5J4WL4A&mJ|5[`iYJ^$_84$t+"FP?J(X:<us c]/m ^+|+,3(Hw-&Q:r(@UtcT) t`kO\	success or wait	1	5B6F2C	URLDownloadToFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: rinzearec84736.exe PID: **296**, Parent PID: **1236**

General

Target ID:	5
Start time:	16:50:20
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\rinzearec84736.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\rinzearec84736.exe
Imagebase:	0x9c0000
File size:	842240 bytes
MD5 hash:	D248194D56895A1FAE8914E81CD9B36A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000005.00000002.923783682.0000000002498000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000005.00000002.922046499.0000000002241000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000005.00000002.924373144.0000000003374000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000005.00000002.924373144.0000000003374000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.924373144.0000000003374000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000005.00000002.924373144.0000000003374000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_SnakeKeylogger_af3faa65, Description: unknown, Source: 00000005.00000002.924373144.0000000003374000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 40%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6BF091F6	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DED7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DED7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDEDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEDA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6DDEDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6DDEDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6DDEDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDEDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6DDEDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDEDE2C	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	success or wait	1	6BF091F6	unknown

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	FontCachePath	unicode	C:\Users\user\AppData\Local	success or wait	1	6BF091F6	unknown

Analysis Process: rinzearec84736.exe PID: **648**, Parent PID: **296**

General

Target ID:	6
Start time:	16:50:25
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\rinzearec84736.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\rinzearec84736.exe
Imagebase:	0x9c0000
File size:	842240 bytes
MD5 hash:	D248194D56895A1FAE8914E81CD9B36A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000006.00000000.919229211.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000006.00000000.919229211.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000000.919229211.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000006.00000000.919229211.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_SnakeKeylogger_af3faa65, Description: unknown, Source: 00000006.00000000.919229211.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DED7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DED7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDEDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEDA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6DDEDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6DDEDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6DDEDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6DDEDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDEDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDEDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDEDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEDB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEDB2B3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CEDB2B3	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Web.28b9ef5a#\97cbf6eb6477005cffa6992126db856c\System.Web.Extensions.ni.dll.aux	unknown	3712	success or wait	1	6DDEDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Web\9e5950923286f171d1649a05bdc62830\System.Web.ni.dll.aux	unknown	3972	success or wait	1	6DDEDE2C	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Tracing\rinzearec84736_RASAPI32	success or wait	1	6C26AD76	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rinzearec84736_RASAPI32	EnableFileTracing	dword	0	success or wait	1	6C26AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rinzearec84736_RASAPI32	EnableConsoleTracing	dword	0	success or wait	1	6C26AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rinzearec84736_RASAPI32	FileTracingMask	dword	-65536	success or wait	1	6C26AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rinzearec84736_RASAPI32	ConsoleTracingMask	dword	-65536	success or wait	1	6C26AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rinzearec84736_RASAPI32	MaxFileSize	dword	1048576	success or wait	1	6C26AD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\rinzearec84736_RASAPI32	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	6C26AD76	unknown

Analysis Process: EQNEDT32.EXE PID: **2648**, Parent PID: **576**

General

Target ID:	7
Start time:	16:50:40
Start date:	29/11/2022
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Copyright Joe Security LLC 2022

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly