

JOeSandbox Cloud BASIC



ID: 330287

Sample Name: SWIFT.doc

Cookbook:

defaultwindowsofficecookbook.jbs

Time: 17:48:39

Date: 14/12/2020

Version: 31.0.0 Red Diamond

Table of Contents

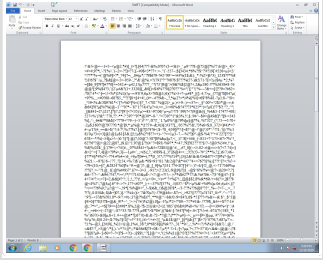
Table of Contents	2
Analysis Report SWIFT.doc	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Threatname: HawkEye	4
Yara Overview	4
Memory Dumps	4
Unpacked PEs	5
Sigma Overview	5
System Summary:	5
Signature Overview	5
AV Detection:	6
Exploits:	6
Key, Mouse, Clipboard, Microphone and Screen Capturing:	6
System Summary:	6
Data Obfuscation:	6
Persistence and Installation Behavior:	6
Malware Analysis System Evasion:	6
HIPS / PFW / Operating System Protection Evasion:	6
Stealing of Sensitive Information:	6
Remote Access Functionality:	7
Mitre Att&ck Matrix	7
Behavior Graph	7
Screenshots	8
Thumbnails	8
Antivirus, Machine Learning and Genetic Malware Detection	9
Initial Sample	9
Dropped Files	9
Unpacked PE Files	9
Domains	9
URLs	10
Domains and IPs	10
Contacted Domains	10
Contacted URLs	10
URLs from Memory and Binaries	10
Contacted IPs	11
Public	11
General Information	12
Simulations	12
Behavior and APIs	12
Joe Sandbox View / Context	13
IPs	13
Domains	13
ASN	13
JA3 Fingerprints	13
Dropped Files	13
Created / dropped Files	13
Static File Info	16
General	16
File Icon	16
Static RTF Info	16

Objects	16
Network Behavior	17
Network Port Distribution	17
TCP Packets	17
UDP Packets	18
DNS Queries	19
DNS Answers	19
HTTP Request Dependency Graph	19
HTTP Packets	19
Code Manipulations	20
Statistics	20
Behavior	20
System Behavior	20
Analysis Process: WINWORD.EXE PID: 2312 Parent PID: 584	20
General	20
File Activities	20
File Created	20
File Deleted	20
File Moved	21
Registry Activities	21
Key Created	21
Key Value Created	21
Key Value Modified	24
Analysis Process: EQNEDT32.EXE PID: 2488 Parent PID: 584	29
General	29
File Activities	29
Registry Activities	29
Key Created	29
Analysis Process: izux978537.scr PID: 2668 Parent PID: 2488	30
General	30
File Activities	30
File Read	30
Analysis Process: EQNEDT32.EXE PID: 2976 Parent PID: 584	30
General	30
File Activities	31
Registry Activities	31
Analysis Process: izux978537.scr PID: 2308 Parent PID: 2668	31
General	31
Analysis Process: izux978537.scr PID: 3016 Parent PID: 2668	31
General	31
File Activities	32
File Created	32
File Written	32
File Read	32
Analysis Process: vbc.exe PID: 1492 Parent PID: 3016	33
General	33
File Activities	33
File Read	33
Analysis Process: vbc.exe PID: 948 Parent PID: 3016	33
General	33
File Activities	34
File Read	34
Disassembly	34
Code Analysis	34

Analysis Report SWIFT.doc

Overview

General Information

Sample Name:	SWIFT.doc
Analysis ID:	330287
MD5:	516028d299e8b6..
SHA1:	fa9c3d41dcd61c1..
SHA256:	6de5a6a9169168..
Tags:	doc
Most interesting Screenshot:	
	

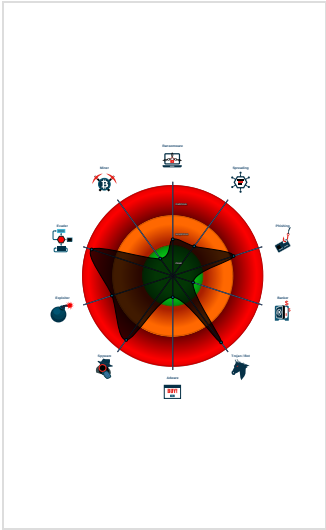
Detection

<div><div>MALICIOUS</div><div>SUSPICIOUS</div><div>CLEAN</div><div>UNKNOWN</div></div> <div>HawkEye M00nD3v Logger MailPassView</div> <div>Score: 100</div> <div>Range: 0 - 100</div> <div>Whitelisted: false</div> <div>Confidence: 100%</div>	
---	--









Signatures

Antivirus detection for URL or domain
Detected HawkEye Rat
Found malware configuration
Malicious sample detected (through ...
Multi AV Scanner detection for subm...
Sigma detected: Droppers Exploiting...
Sigma detected: EQNEDT32.EXE c...
Yara detected AntiVM_3
Yara detected HawkEye Keylogger
Yara detected M00nD3v Logger
Yara detected MailPassView
.NET source code contains potentia...
.NET source code references suspic...

Classification



Startup

■ System is w7x64
•  WINWORD.EXE (PID: 2312 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
•  EQNEDT32.EXE (PID: 2488 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
•  izux978537.scr (PID: 2668 cmdline: C:\Users\user\AppData\Roaming\izux978537.scr MD5: 7DA4F5E17791A774131C3C97538A2495)
•  izux978537.scr (PID: 2308 cmdline: C:\Users\user\AppData\Roaming\izux978537.scr MD5: 7DA4F5E17791A774131C3C97538A2495)
•  izux978537.scr (PID: 3016 cmdline: C:\Users\user\AppData\Roaming\izux978537.scr MD5: 7DA4F5E17791A774131C3C97538A2495)
•  vbc.exe (PID: 1492 cmdline: 'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp2915.tmp' MD5: 1672D0478049ABDAF0197BE64A7F867F)
•  vbc.exe (PID: 948 cmdline: 'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp2916.tmp' MD5: 1672D0478049ABDAF0197BE64A7F867F)
•  EQNEDT32.EXE (PID: 2976 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
■ cleanup

Malware Configuration

Threatname: HawkEye

<pre>{ "Modules": ["mailpv"], "Version": "" }</pre>

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.2378186428.0000000002D 68000.00000004.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	


Source	Rule	Description	Author	Strings
00000009.00000003.2226541368.0000000004335000.00000004.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
00000009.00000002.2376684630.0000000002C3A000.00000004.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
00000009.00000002.2371163613.00000000002C0000.00000004.00000001.sdmp	APT_NK_BabyShark_KimJ oingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	<ul style="list-style-type: none">0x134d2:\$a1: logins.json0x13432:\$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encryptedUsername, encryptedPassword FROM moz_login0x13c56:\$s4: \mozsqlite3.dll0x124c6:\$s5: SMTP Password
00000009.00000002.2371163613.00000000002C0000.00000004.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.vbc.exe.400000.0.raw.unpack	APT_NK_BabyShark_KimJ oingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	<ul style="list-style-type: none">0x147b0:\$a1: logins.json0x14710:\$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encryptedUsername, encryptedPassword FROM moz_login0x14f34:\$s4: \mozsqlite3.dll0x137a4:\$s5: SMTP Password
11.2.vbc.exe.400000.0.raw.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
10.2.vbc.exe.400000.0.raw.unpack	APT_NK_BabyShark_KimJ oingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	<ul style="list-style-type: none">0x147b0:\$a1: logins.json0x14710:\$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encryptedUsername, encryptedPassword FROM moz_login0x14f34:\$s4: \mozsqlite3.dll0x137a4:\$s5: SMTP Password
10.2.vbc.exe.400000.0.raw.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
9.2.izux978537.scr.2c0000.0.unpack	APT_NK_BabyShark_KimJ oingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	<ul style="list-style-type: none">0x116d2:\$a1: logins.json0x11632:\$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encryptedUsername, encryptedPassword FROM moz_login0x11e56:\$s4: \mozsqlite3.dll0x106c6:\$s5: SMTP Password
Click to see the 10 entries				

Sigma Overview

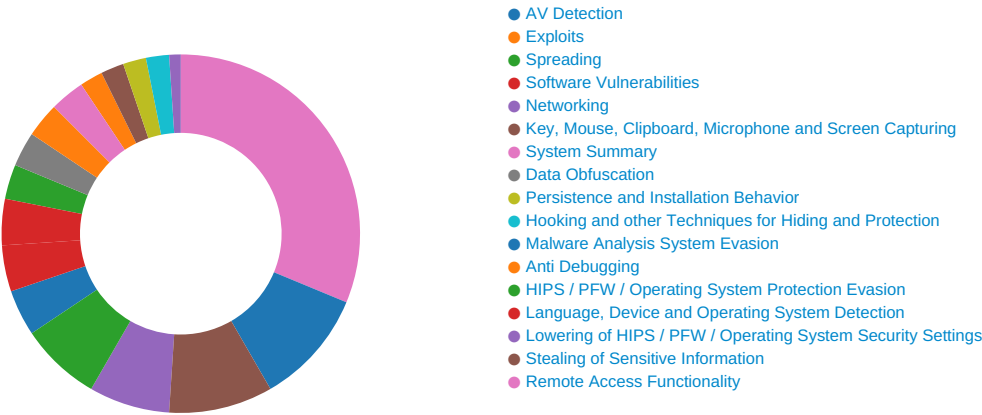
System Summary:



Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

Signature Overview



AV Detection:



Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for submitted file

Exploits:



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

Key, Mouse, Clipboard, Microphone and Screen Capturing:



Yara detected HawkEye Keylogger

System Summary:



Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Data Obfuscation:



.NET source code contains potential unpacker

Persistence and Installation Behavior:



Drops PE files with a suspicious file extension

Malware Analysis System Evasion:



Yara detected AntiVM_3

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

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

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 M00nD3v Logger

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)

Remote Access Functionality:



Detected HawkEye Rat

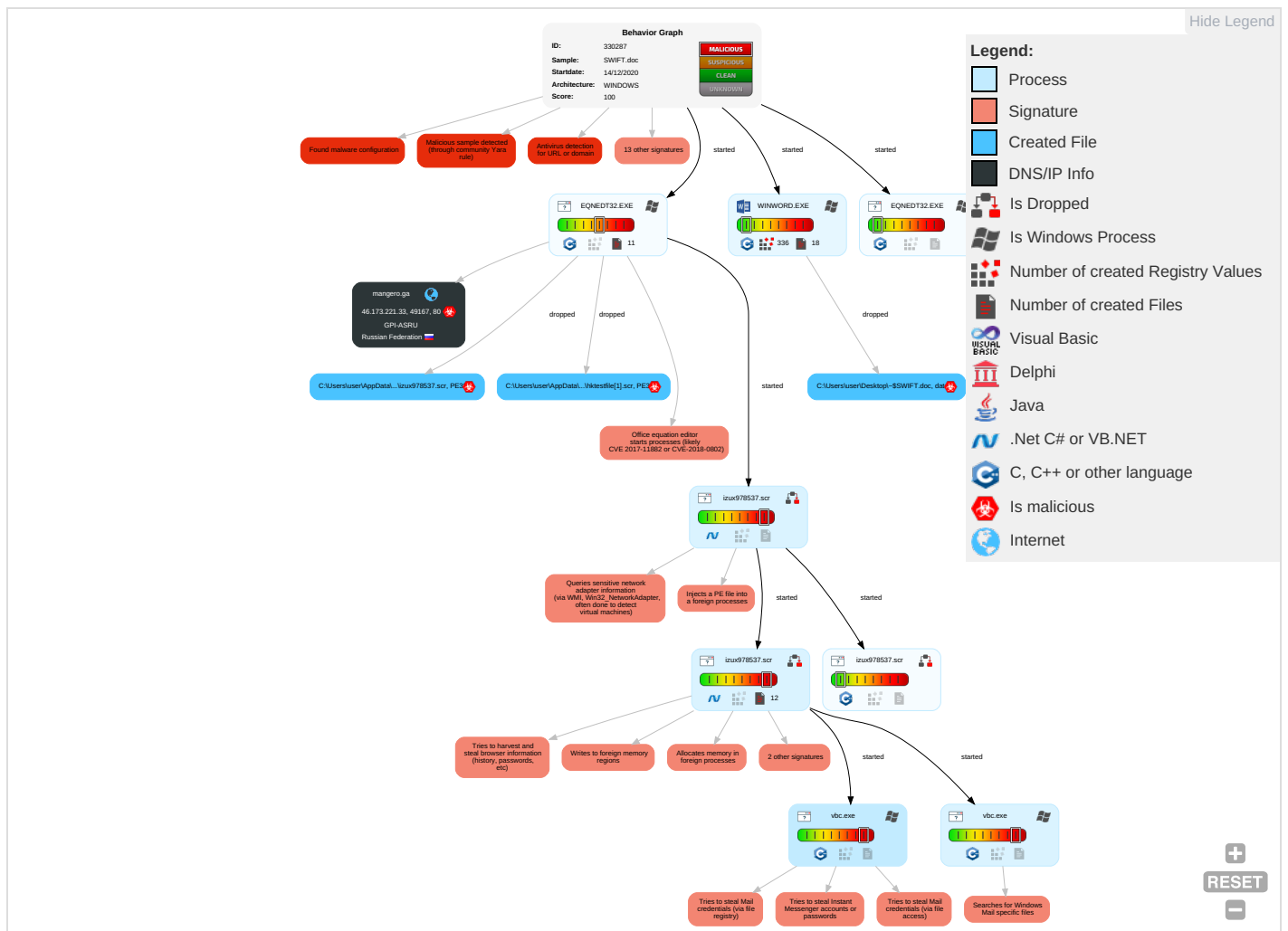
Yara detected HawkEye Keylogger

Yara detected M00nD3v Logger

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 1 1 1	Application Shimmming 1	Application Shimmming 1	Disable or Modify Tools 1	OS Credential Dumping 1	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 1
Default Accounts	Native API 1 1	Boot or Logon Initialization Scripts	Process Injection 4 1 2	Deobfuscate/Decode Files or Information 1 1	Credentials in Registry 2	File and Directory Discovery 1 3	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	Credentials In Files 1	System Information Discovery 1 5	SMB/Windows Admin Shares	Email Collection 2	Automated Exfiltration	Remote Access Software 1
Local Accounts	Exploitation for Client Execution 1 3	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 1	NTDS	Security Software Discovery 2 2	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Non-Application Layer Protocol 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1	LSA Secrets	Virtualization/Sandbox Evasion 1 3	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 4 1 2	DCSync	System Owner/User Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

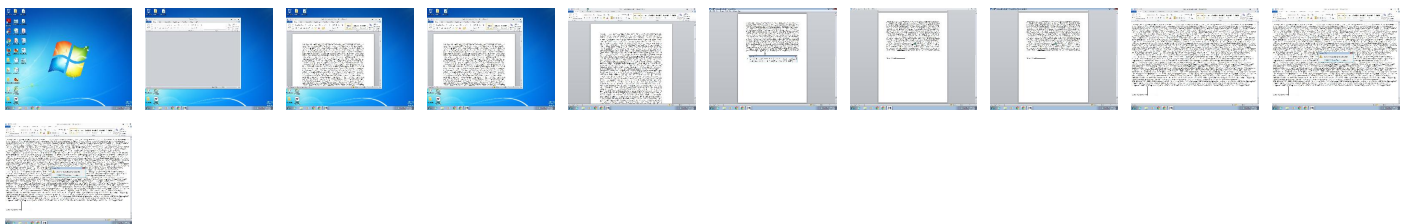
Behavior Graph

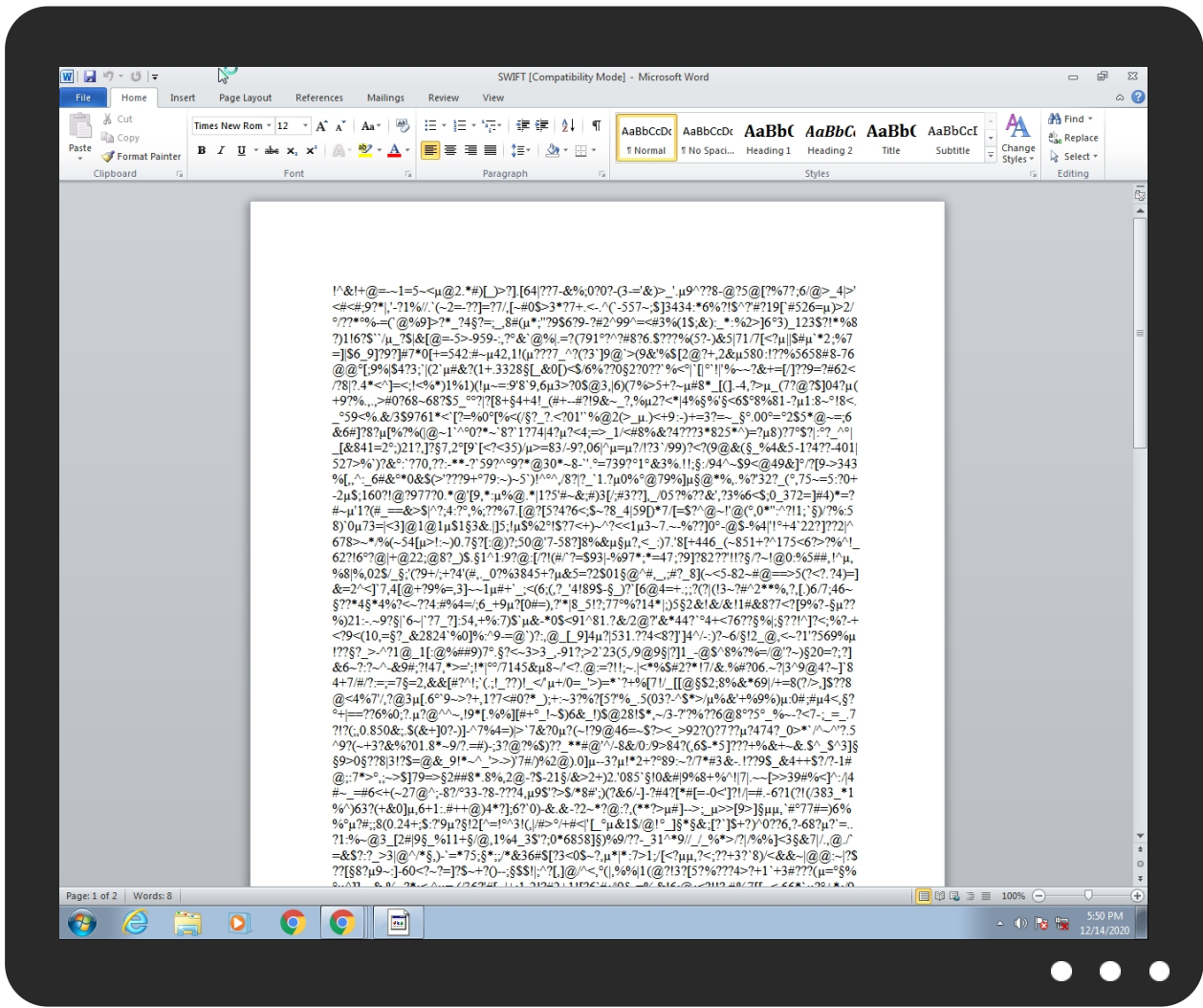


Screenshots

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
SWIFT.doc	44%	Virusotal		Browse
SWIFT.doc	48%	ReversingLabs	Document-RTF.Exploit.CVE-2017-11882	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.0.izux978537.scr.bc0000.0.unpack	100%	Avira	HEUR/AGEN.1100765		Download File
6.2.izux978537.scr.bc0000.0.unpack	100%	Avira	HEUR/AGEN.1100765		Download File
9.2.izux978537.scr.bc0000.2.unpack	100%	Avira	HEUR/AGEN.1100765		Download File
4.0.izux978537.scr.bc0000.0.unpack	100%	Avira	HEUR/AGEN.1100765		Download File
9.2.izux978537.scr.400000.1.unpack	100%	Avira	TR/Dropper.Gen		Download File
6.0.izux978537.scr.bc0000.0.unpack	100%	Avira	HEUR/AGEN.1100765		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://mangero.ga/izux/hktestfile.scr	100%	Avira URL Cloud	malware	
http://https://a.pomf.cat/	0%	Avira URL Cloud	safe	
http://pomf.cat/upload.php&https://a.pomf.cat/	0%	Avira URL Cloud	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://pomf.cat/upload.php	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://https://m00nd3v.com/M00nD3v/HawkEyeDecrypt/BouncyCastle.Crypto.dll	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://computername/printers/printrname/.printer	0%	Avira URL Cloud	safe	
http://tresearch.net	0%	URL Reputation	safe	
http://tresearch.net	0%	URL Reputation	safe	
http://tresearch.net	0%	URL Reputation	safe	
http://https://m00nd3v.com/M00nD3v/HawkEyeDecrypt/BouncyCastle.Crypto.dll;HawkEye	0%	Avira URL Cloud	safe	
http://pomf.cat/upload.phpContent-Disposition:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mangero.ga	46.173.221.33	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://mangero.ga/izux/hktestfile.scr	true	<ul style="list-style-type: none"> Avira URL Cloud: malware 	unknown

URLs from Memory and Binaries


Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	hktestfile[1].scr.2.dr	false	<ul style="list-style-type: none"> URL Reputation: safe URL Reputation: safe URL Reputation: safe 	unknown
http://https://a.pomf.cat/	izux978537.scr, 00000009.0000002.2375979476.0000000002B5B000.00000004.00000001.sdmp	false	<ul style="list-style-type: none"> Avira URL Cloud: safe 	unknown
http://pomf.cat/upload.php&https://a.pomf.cat/	izux978537.scr, 00000009.0000002.2371242328.000000000402000.00000040.00000001.sdmp	false	<ul style="list-style-type: none"> Avira URL Cloud: safe 	unknown
http://wellformedweb.org/CommentAPI/	izux978537.scr, 00000009.0000002.2379604509.000000000A600000.00000002.00000001.sdmp	false	<ul style="list-style-type: none"> URL Reputation: safe URL Reputation: safe URL Reputation: safe 	unknown
http://dyn.com/dns/	izux978537.scr, 00000009.0000002.2375979476.0000000002B5B000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://pomf.cat/upload.php	izux978537.scr, 00000009.00000002.2375979476.0000000002B5B000.00000004.00000001.sdmp	false	<ul style="list-style-type: none"> Avira URL Cloud: safe 	unknown
http://ocsp.sectigo.com0	hktestfile[1].scr.2.dr	false	<ul style="list-style-type: none"> URL Reputation: safe URL Reputation: safe URL Reputation: safe 	unknown
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	hktestfile[1].scr.2.dr	false	<ul style="list-style-type: none"> URL Reputation: safe URL Reputation: safe URL Reputation: safe 	unknown
http://www.iis.fhg.de/audioPA	izux978537.scr, 00000009.00000002.2379604509.000000000A600000.00000002.00000001.sdmp	false	<ul style="list-style-type: none"> URL Reputation: safe URL Reputation: safe URL Reputation: safe 	unknown
http://https://m00nd3v.com/M00nD3v/HawkEyeDecrypt/BouncyCastle.Crypto.dll	izux978537.scr, 00000009.00000002.2375869139.0000000002B31000.00000004.00000001.sdmp, izux978537.scr, 00000009.00000002.2375979476.0000000002B5B000.00000004.00000001.sdmp	false	<ul style="list-style-type: none"> Avira URL Cloud: safe 	unknown
http://https://sectigo.com/CPS0D	hktestfile[1].scr.2.dr	false	<ul style="list-style-type: none"> URL Reputation: safe URL Reputation: safe URL Reputation: safe 	unknown
http://computername/printers/printername/.printer	izux978537.scr, 00000009.00000002.2379604509.000000000A600000.00000002.00000001.sdmp	false	<ul style="list-style-type: none"> Avira URL Cloud: safe 	low
http://www.nirsoft.net/	vbc.exe, 0000000B.00000002.2242831512.0000000000400000.00000040.00000001.sdmp	false		high
http://treyresearch.net	izux978537.scr, 00000009.00000002.2379604509.000000000A600000.00000002.00000001.sdmp	false	<ul style="list-style-type: none"> URL Reputation: safe URL Reputation: safe URL Reputation: safe 	unknown
http://bot.whatismyipaddress.com/	izux978537.scr, 00000009.00000002.2375979476.0000000002B5B000.00000004.00000001.sdmp	false		high
http://https://m00nd3v.com/M00nD3v/HawkEyeDecrypt/BouncyCastle.Crypto.dll;HawkEye	izux978537.scr, 00000009.00000002.2375979476.0000000002B5B000.00000004.00000001.sdmp	false	<ul style="list-style-type: none"> Avira URL Cloud: safe 	unknown
http://pomf.cat/upload.phpContent-Disposition:	izux978537.scr, 00000009.00000002.2375979476.0000000002B5B000.00000004.00000001.sdmp	false	<ul style="list-style-type: none"> Avira URL Cloud: safe 	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
46.173.221.33	unknown	Russian Federation		56364	GPI-ASRU	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	330287
Start date:	14.12.2020
Start time:	17:48:39
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SWIFT.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:	12
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:	<ul style="list-style-type: none"> • 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@13/9@1/1
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none"> • Successful, ratio: 97.1% (good quality ratio 94.3%) • Quality average: 85.8% • Quality standard deviation: 23%
HCA Information:	<ul style="list-style-type: none"> • Successful, ratio: 90% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	<ul style="list-style-type: none"> • 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 • Active ActiveX Object • Scroll down • Close Viewer
Warnings:	<p>Show All</p> <ul style="list-style-type: none"> • Exclude process from analysis (whitelisted): dillhost.exe, WerFault.exe, svchost.exe • TCP Packets have been reduced to 100 • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryDirectoryFile calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:49:41	API Interceptor	298x Sleep call for process: EQNEDT32.EXE modified
17:49:47	API Interceptor	501x Sleep call for process: izux978537.scr modified
17:50:51	API Interceptor	15x Sleep call for process: vbc.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
46.173.221.33	purchase request sheet.doc	Get hash	malicious	Browse	<ul style="list-style-type: none">mangero.ga/cax/cax.exe
	order list.doc	Get hash	malicious	Browse	<ul style="list-style-type: none">mangero.ga/fortyseven/fortyseven.scr
	PMA1911003.doc	Get hash	malicious	Browse	<ul style="list-style-type: none">mangero.ga/kingtroupx/kingtroupx.scr

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mangero.ga	purchase request sheet.doc	Get hash	malicious	Browse	<ul style="list-style-type: none">46.173.221.33
	order list.doc	Get hash	malicious	Browse	<ul style="list-style-type: none">46.173.221.33
	PMA1911003.doc	Get hash	malicious	Browse	<ul style="list-style-type: none">46.173.221.33

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GPI-ASRU	purchase request sheet.doc	Get hash	malicious	Browse	<ul style="list-style-type: none">46.173.221.33
	order list.doc	Get hash	malicious	Browse	<ul style="list-style-type: none">46.173.221.33
	PMA1911003.doc	Get hash	malicious	Browse	<ul style="list-style-type: none">46.173.221.33
	290453721.xls	Get hash	malicious	Browse	<ul style="list-style-type: none">46.173.210.8
	290453721.xls	Get hash	malicious	Browse	<ul style="list-style-type: none">46.173.210.8

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\luser\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\hktestfile[1].scr	
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):	7447752
Entropy (8bit):	5.138250665474018
Encrypted:	false
SSDEEP:	98304:eUYsXqrhgjzKQYaqTvH6nn0GRj27SchULsKSNiT3i0jibPQMpG:FqrwaPQj2hawI
MD5:	7DA4F5E17791A774131C3C97538A2495
SHA1:	552B4A357B259935A35B06D040D7F2E3205C8E42
SHA-256:	AC8EF770D70DA42EA56D5B15FB5DB0BE89AE9250AC78B2BFD493843A50399A19
SHA-512:	4C0460E29457F9910F5EBB4090FBAF1E29D28E4D2ABB5F63DBE83061CDB306E0C545DB97662F6A380E438D615AD3B9F43EEC8D7B1F9B57EECFF63EF45557CE7B

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\hktestfile[1].scr	
Malicious:	true
Reputation:	low
IE Cache URL:	http://mangero.ga/izux/hktestfile.scr
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$......PE..L.....q.....q..q...@..q.....ur.. ..@.....q.W.....q.....q.....H.....text....q..q.....`..reloc.....q.....q.....@..B.....q.....H.....q.....**90...(.....9.....r.Z.p....(.....*(.....*(.....*J....._*J.....*J....._*J.....@..._@.....*J....._*(.....(%...S-.....(.....*(.....(&...S-.....(.....*(.....*V(#...9...(.....**0..wnp..... ...%M.%Z.%% ..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{1A2D0E25-5575-4F65-9737-3BA52E43A74D}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0DB60AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28B A4
Malicious:	false
Reputation:	high, very likely benign file
Preview:

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{3A3DB071-4F03-4D2B-8CA3-F1ADB9722678}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	11988
Entropy (8bit):	3.522915830051191
Encrypted:	false
SSDEEP:	192:MGZWnRflurDlp0ALuylPWAepVVYrz9Q+gyf2Sj7g+u4OzM1kj:wrHuep0ryl0YPBP7HOzM1kj
MD5:	ED4C38D3EA4025C9BBA22A2C89D7245E
SHA1:	8500C4BB1AAB0B521D3854C9556F9714FCA54318
SHA-256:	63512F967A20556F2D9FF59393F676A3FE6E1FA0724FB63A794F7AF7D650F276
SHA-512:	71AD1150886AF517F39C05358A4E8701074E4C0B45D1C02993341498FFE9904FEBB12D3D5168A33C12A4C8F1D7C4F3E7816CE7357293BF90C4C9B0CE717AF658
Malicious:	false
Reputation:	low
Preview:	!^&!+,@.=.-~.1.=5.~<...@.2...*#).[_]>?].[6.4. ??7.-&%.;0.?0.?-(3.-='&).>_'.....9^??.8.-@.?.5.@.[?%.7.?;6./.@.>_4. >.'<#.<#.;9.?*. ,.'-?1. %/./...`.(~2.=~??.?]=.?7./...[~#0.\$>.3.*?7.+...<~...^('.-5.5.7.-;\$.].3.4.3.4.:*.6.%.?!.\$^?'.#.?1.9.[?#.5.2.6.=...)>2./.../?.??...%.-=(.`@.%9.]>?.*_?4...?.=;_.. ,8.#(...*;'!?.9.\$6.?9.-?#2^9.9^=<#.3.%(1.\$;.&);...*_..%2.>].6...3)._1.2.3.\$?.!.*%8.?).1!6.?.\$`./..._?.\$.&.[@.=~5.>~9.5.9.-;...?...&`.@.% ...=? (.7.9.1...?^?#8.?6...\$?.??.?%(.5.?.-) &5. 7.1./7.[<?... .].\$#...`*2;.%7.= .].\$6._9.]?9.?.].#7*0.[+=5.4.2;.#~4.2;1.!(...??.?7._^?.(?3.`].9.@.`>.(9&'.%\$[2.@.?+...2&...5.8.0;!1.??.?%.5.6.5.8.#8.-7.6.@.@...[.;9.% .\$.4.7.3;`. (2.`...#&?.(1.+...3.3.2.8...[_&0.]<\$./6.%??0...2.?0.??`%<... .].[...`! .! %~.-.?&.+=[./].??.9.=.?#6.2.<./.

C:\Users\user\AppData\Local\Temp\73f52833-e0b3-84b4-f8d3-07db0b3195f9	
Process:	C:\Users\user\AppData\Roaming\izux978537.scr
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	64
Entropy (8bit):	5.140319531114784
Encrypted:	false
SSDEEP:	3:91sdUBmRhys8m0uR1rn:9eW4ys30m1
MD5:	AB986688BB63AF782CAD2D87A92C93E3
SHA1:	BDBF286D59A4B7898A17C52D17DBF2172163F35B
SHA-256:	A2B606F440BD3248A432F75747507B5A59AD1C9D5327A1A6ED6131BB9CC409AC
SHA-512:	C0DE1198EB7E0674E97E1A0770E0E394CCCC19A16B9E01B1C104AB762D78016DB5C87A478C33B87616C7D3F5D095535833497E66A2A1E84BCF12B2FED25B474
Malicious:	false
Reputation:	low
Preview:	6y8lxPKPPBIW+1duQx+1udgc8YpqENDI4Dt1IzqCDU/R9S7AL35y919NiQAPRZsN

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\SWIFT.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 Dec 15 00:49:39 2020, length=1258700, window=hide
Category:	dropped
Size (bytes):	1970
Entropy (8bit):	4.547116102220396
Encrypted:	false
SSDEEP:	48:80H/XT0jFHGRacojuQh20H/XT0jFHGRacojuQ/:8C/XojFmRhojuQh2C/XojFmRhojuQ/
MD5:	7457FB8646A6423F665D4F8C08B7849B
SHA1:	386D33E660A47241A3FA2F8263191D39EE2E0095
SHA-256:	EF16F973ED95215D10FBADA35945668E8D2B7DB488E62939AF84D1492BBB086C
SHA-512:	B5D18028524682730B15FA397CFE6B43A5713F458E891C2094E30358D39754B50467BE859A71709968072F6C8A4EE7859F37B050D008E4B2E4E4B3FBF8CA3BD5
Malicious:	false
Reputation:	low
Preview:	L.....F....[v..{..[v..{..~'.....4.....P.O. :i.....+00.../C:\.....t1....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.....X.2..4...Q4. .SWIFT.doc.@.....Q.y.Q.y*...8.....S.W.I.F.T...d.o.c.....S.....*...8...[.....?J.....C:\Users\..#.....\549163\Users.user\De sktop\SWIFT.doc.\.....\.....\D.e.s.k.t.o.p.\S.W.I.F.T...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.....549163.....D_...3N...W...9F.C.....[D_...3N...W...9F.C.....[...L.....

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):	53
Entropy (8bit):	4.114278124890147
Encrypted:	false
SSDEEP:	3:M1GZFSurNFSmX1GZFSv:MQ7Lvo7c
MD5:	9731EEE3C0A02AE27F1EE87C1F8D6715
SHA1:	4D5D69FD84A1DE2FB2865C456E57F5C27CEDA3CE
SHA-256:	90AE3C9111B4FB7EBD7F273088FB110C401DA00E07382D2B1D7BD181F436E49B
SHA-512:	5F603970D5A7310A737F6A9E8FF7DA8445C0533F87716EC65B9557268D23ACF7001F112E4F809C1957FEEA1D6D482997BB55C7D5ABD13E5E4B68C925662922FD
Malicious:	false
Reputation:	low
Preview:	[doc]..SWIFT.LNK=0..SWIFT.LNK=0..[doc]..SWIFT.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):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkwtVy3KGcils6w7Adtl:n:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....P.....Z.....X...

C:\Users\user\AppData\Roaming\lux978537.scr	
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):	7447752
Entropy (8bit):	5.138250665474018
Encrypted:	false
SSDEEP:	98304:eUYsXqrhgjzKQYaqTvH6nn0GRj27SchULsKSNiT3i0jibPQMpG:FqrwaPQj2hawI
MD5:	7DA4F5E17791A774131C3C97538A2495
SHA1:	552B4A357B259935A35B06D040D7F2E3205C8E42
SHA-256:	AC8EF770D70DA42EA56D5B15FB5DB0BE89AE9250AC78B2BFD493843A50399A19

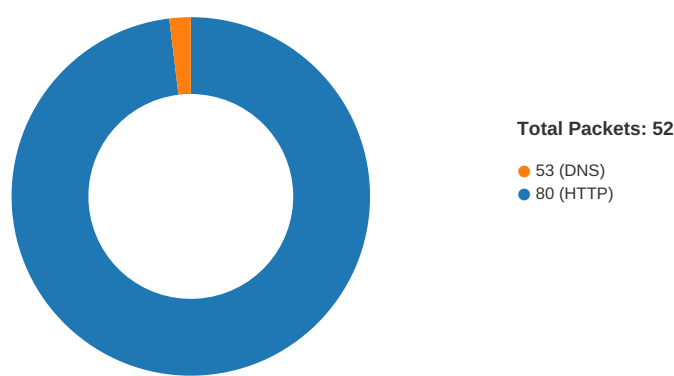
C:\Users\user\Desktop~\$SWIFT.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVy3KGcils6w7Adtl:n:vdsCkWthGciWfQl
MD5:	4A5DFFE330E8BBBF59615CB0C71B87BE
SHA1:	7B896C17F93ECFC9B69E84FC1EADEDD9DA550C4B
SHA-256:	D28616DC54FDEF1FF5C5BA05A77F178B7E3304493BAF3F4407409F2C84F4F215
SHA-512:	3AA160CB89F4D8393BCBF9FF4357FFE7AE00663F21F436D341FA4F5AD4AEDC737092985EB4A94A694A02780597C6375D1615908906A6CEC6D7AB616791B6285C
Malicious:	true
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

File type:	Rich Text Format data, version 1, unknown character set
Entropy (8bit):	4.036745127605034
TrID:	<ul style="list-style-type: none">Rich Text Format (5005/1) 55.56%Rich Text Format (4004/1) 44.44%
File name:	SWIFT.doc
File size:	1258700
MD5:	516028d299e8b6b9f947fdb4541a5d7e
SHA1:	fa9c3d41dcd61c1dcade0ba7943882cf640a71cd
SHA256:	6de5a6a916916823583495dae424fa8ce2f54c33f2a67da83337b6f2579e816c
SHA512:	63d59833ee33c2d743a5b7d95eebd6b1bc28b814253ce4f6cd53441eb0e5e3ecf1053cdf13a421a2eb5d0b1463f5b1a9c188f8ff6470ced7741c9362ac433022
SSDEEP:	24576:Np4EYWj0t4t9F97XxYJBfzroFtjC+o4hZkRkIMTqHr0ke:s
File Content Preview:	{\rtf1\o1\^&!+@=-~1=5~<.@2.*#)[_]>?].[64 ???-&%;0?0?-(3=*&)>_'.9^??8-@?5@[?%?7?;6/@>_.4 >'<#<#;9?* .'-?1%//\.'(-2=-??)=?7/[,-#0\$>3*?7+<.-^(-557~;,\$j3434:*6%? ;\$^?#?19[#526=.)>2/./??*.%-=('@%9]>?*_?4.?=-;8#(*;''9\$679-?#2^99^=<#3%(1\$&);_.*%2> 6.3)_123\$?

ID	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	TempPath	Exploit
0	00001568h	2	embedded	EqUat!On.3	626454				no

Network Behavior

Network Port Distribution



TCP Packets

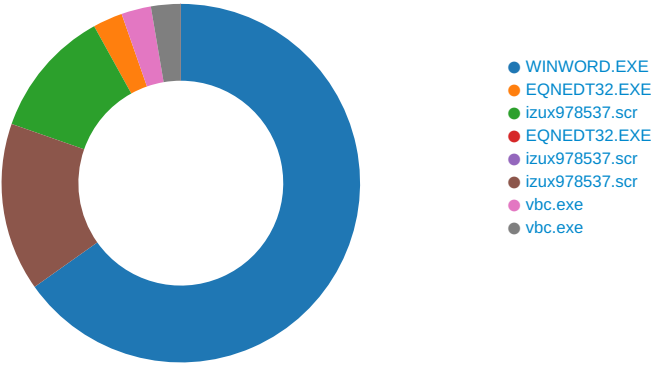
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 14, 2020 17:49:33.579776049 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.630593061 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.630748987 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.631094933 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.681514025 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.682003975 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.682048082 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.682086945 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.682126045 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.682163000 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.682202101 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.682212114 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.682255030 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.682260990 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.682265997 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.682271004 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.682462931 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.682504892 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.682543039 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.682543993 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.682580948 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.682586908 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.682620049 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.682658911 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.687187910 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.732657909 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.732722044 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.732760906 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.732808113 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.732810020 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.732834101 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.732839108 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.732853889 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.732856989 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.732902050 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.732904911 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.732954979 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.733072042 CET	80	49167	46.173.221.33	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 14, 2020 17:49:33.733114958 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.733122110 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.733160973 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.733184099 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.733222961 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.733232975 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.733261108 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.733270884 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.733306885 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.733309031 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.733361959 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.733555079 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.733572960 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.733596087 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.733603954 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.733640909 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.733644962 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.733690023 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.733694077 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.733740091 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.733882904 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.733932018 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.733983040 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.734025002 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.734029055 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.734062910 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.734067917 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.734107971 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.734731913 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.782946110 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.783004045 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.783129930 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.783188105 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.783471107 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.783514977 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.783551931 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.783555984 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.783567905 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.783595085 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.783627033 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.783633947 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.783647060 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.783674002 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.783698082 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.783721924 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.784116983 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.784158945 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.784189939 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.784190893 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.784209967 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.784229994 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.784251928 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.784292936 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.784425020 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.784487963 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.784501076 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.784562111 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.784575939 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.784615993 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.784637928 CET	49167	80	192.168.2.22	46.173.221.33
Dec 14, 2020 17:49:33.784663916 CET	80	49167	46.173.221.33	192.168.2.22
Dec 14, 2020 17:49:33.784665108 CET	49167	80	192.168.2.22	46.173.221.33

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2312 Parent PID: 584

General

Start time:	17:49:39
Start date:	14/12/2020
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:	0x13fb50000
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

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\VE	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	7FEE95226B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~\$SWIFT.doc	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\themedata.thm~	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\colorscchememapping.xml~	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml~	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Temp\~WRL0000.tmp	success or wait	1	7FEE9449AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Templ\mgs_files\themedata.thmx	C:\Users\user\AppData\Local\Templ\mgs_files\themedata.thm~	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Templ\mgs_files\colorscchemmapping.xml	C:\Users\user\AppData\Local\Templ\mgs_files\colorscchemmapping.xm~	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Templ\mgs_files\filelist.xml	C:\Users\user\AppData\Local\Templ\mgs_files\filelist.xm~m~	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Templ\mgs_files\themedata.thm_	C:\Users\user\AppData\Local\Templ\mgs_files\themedata.thmx..	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Templ\mgs_files\colorscchemmapping.xm_	C:\Users\user\AppData\Local\Templ\mgs_files\colorscchemmapping.xml	success or wait	1	7FEE9449AC0	unknown
C:\Users\user\AppData\Local\Templ\mgs_files\filelist.xm_	C:\Users\user\AppData\Local\Templ\mgs_files\filelist.xmlmx	success or wait	1	7FEE9449AC0	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE945E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\FD51A	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\Recent Locations\SharePoint	success or wait	1	7FEE9449AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft Office\14.0\WordResiliency\DocumentRecovery\FD51A	FD51A	binary	04 00 00 00 08 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 6B 5E 1E B4 84 D2 D6 01 1A D5 0F 00 1A D5 0F 00 00 00 00 00 DB 04 00 00 02 00 FF FF FF FF 00	success or wait	1	7FEE9449AC0	unknown

Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 2	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9713424497.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 3	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\0887538035.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 4	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\8416751812.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 5	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3580751004.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 6	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\5367203117.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 7	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3764832265.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 8	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3013890265.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 9	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\0615447233.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 10	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\4144085054.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 11	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\2109793820.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 12	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1417002460.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 13	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1387277564.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 14	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9281004682.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 15	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\1169381505.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 16	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9801086636.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 17	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\7838756049.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 18	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\8416181845.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 19	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\2874006916.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 20	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9369051781.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Place MRU	Max Display	dword	25	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Max Display	dword	25	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 1	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\6516896632.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 2	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\9713424497.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 3	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\0887538035.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 4	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\8416751812.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 5	unicode	[F0000000][T01D1BB6D4B429860] [O0000000]*C:\Users\user\Desktop\3580751004.docx	success or wait	1	7FEE9449AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 6	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desk top\5367203117.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 7	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desk top\3764832265.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 8	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desk top\3013890265.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 9	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desk top\0615447233.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 10	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desk top\4144085054.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 11	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desk top\2109793820.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 12	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desk top\1417002460.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 13	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desk top\1387277564.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 14	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desk top\9281004682.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 15	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desk top\1169381505.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 16	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desk top\9801086636.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 17	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desk top\7838756049.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 18	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desk top\8416181845.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 19	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desk top\2874006916.docx	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\file mru	Item 20	unicode	[F0000000][T01D1BB6D4B429860][O0000000]*C:\Users\user\Desk top\9369051781.docx	success or wait	1	7FEE9449AC0	unknown

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D300000001000000F01FEC\Usage	ProductFiles	dword	1368260654	1368260655	success or wait	1	7FEE9449AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D300000001000000F01FEC\Usage	ProductFiles	dword	1368260655	1368260656	success or wait	1	7FEE9449AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\FD51A	FD51A	binary	04 00 00 00 08 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 6B 5E 1E B4 84 D2 D6 01 1A D5 0F 00 1A D5 0F 00 00 00 00 00 DB 04 00 00 02 00	04 00 00 00 08 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1A D5 0F 00 1A D5 0F 00 00 00 00 00 DB 04 00 00 02 00 FF FF	success or wait	1	7FEE9449AC0	unknown

[illegible]

Analysis Process: EQNEDT32.EXE PID: 2488 Parent PID: 584

General

Start time:	17:49:40
Start date:	14/12/2020
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path				Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--	--	--	--------	------------	---------	------------	-------	----------------	--------

File Path			Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--	--	--------	--------	-------	-------	------------	-------	----------------	--------

File Path					Offset	Length	Completion	Count	Source Address	Symbol
-----------	--	--	--	--	--------	--------	------------	-------	----------------	--------

Registry Activities

Key Created

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

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

Analysis Process: izux978537.scr PID: 2668 Parent PID: 2488

General

Start time:	17:49:46
Start date:	14/12/2020
Path:	C:\Users\user\AppData\Roaming\izux978537.scr
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\izux978537.scr
Imagebase:	0xbc0000
File size:	7447752 bytes
MD5 hash:	7DA4F5E17791A774131C3C97538A2495
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E1D7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E1D7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0EDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E1DA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E0EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E0EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E0EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0EDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D1DB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D1DB2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E0EDE2C	ReadFile

Analysis Process: EQNEDT32.EXE PID: 2976 Parent PID: 584

General

Start time:	17:50:06
Start date:	14/12/2020
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding

Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol
-----------	--------	--------	------------	-------	----------------	--------

Registry Activities

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

Analysis Process: izux978537.scr PID: 2308 Parent PID: 2668

General

Start time:	17:50:37
Start date:	14/12/2020
Path:	C:\Users\user\AppData\Roaming\izux978537.scr
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\izux978537.scr
Imagebase:	0xbc0000
File size:	7447752 bytes
MD5 hash:	7DA4F5E17791A774131C3C97538A2495
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: izux978537.scr PID: 3016 Parent PID: 2668

General

Start time:	17:50:40
Start date:	14/12/2020
Path:	C:\Users\user\AppData\Roaming\izux978537.scr
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\izux978537.scr
Imagebase:	0xbc0000
File size:	7447752 bytes
MD5 hash:	7DA4F5E17791A774131C3C97538A2495
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	<ul style="list-style-type: none">• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000009.00000002.2378186428.0000000002D68000.00000004.00000001.sdmp, Author: Joe Security• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000009.00000003.2226541368.0000000004335000.00000004.00000001.sdmp, Author: Joe Security• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000009.00000002.2376684630.0000000002C3A000.00000004.00000001.sdmp, Author: Joe Security• Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 00000009.00000002.2371163613.00000000002C0000.00000004.00000001.sdmp, Author: Florian Roth• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000009.00000002.2371163613.00000000002C0000.00000004.00000001.sdmp, Author: Joe Security• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000009.00000002.2376638694.0000000002C1E000.00000004.00000001.sdmp, Author: Joe Security• Rule: JoeSecurity_M00nD3vLogger, Description: Yara detected M00nD3v Logger, Source: 00000009.00000002.2375979476.0000000002B5B000.00000004.00000001.sdmp, Author: Joe Security• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000009.00000002.2378260409.0000000003B31000.00000004.00000001.sdmp, Author: Joe Security• Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000009.00000002.2376075790.0000000002B90000.00000004.00000001.sdmp, Author: Florian Roth• Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000009.00000002.2376075790.0000000002B90000.00000004.00000001.sdmp, Author: Joe Security• Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000009.00000002.2371242328.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth• Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000009.00000002.2371242328.0000000000402000.00000040.00000001.sdmp, Author: Joe Security• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000009.00000002.2378154261.0000000002D45000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\73f52833-e0b3-84b4-f8d3-07db0b3195f9	read attributes synchronize generic write	device sparse file	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6D1DF4A8	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp2915.tmp	read attributes synchronize generic read	device sparse file	synchronous io non alert non directory file	success or wait	1	6D1D7C90	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp2916.tmp	read attributes synchronize generic read	device sparse file	synchronous io non alert non directory file	success or wait	1	6D1D7C90	GetTempFileNameW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\73f52833-e0b3-84b4-f8d3-07db0b3195f9	unknown	64	36 79 38 6c 78 50 4b 50 50 42 49 57 2b 31 64 75 51 78 2b 31 75 64 67 63 38 59 70 71 45 4e 44 49 34 44 74 31 49 7a 71 43 44 55 2f 52 39 53 37 41 4c 33 35 79 39 31 39 4e 69 51 41 50 52 5a 73 4e	6y8lxPKPBIW+1duQx+1udgc8YpqENDI4Dt1lzqCDU/R9S7AL35y919NiQAPRZsN	success or wait	1	6D1DB2B3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E1D7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E1D7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0EDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E1DA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E0EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E0EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core.leb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E0EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E0EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing.l1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E0EDE2C	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default>Login Data	unknown	40960	success or wait	1	6D1DB2B3	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2915.tmp	unknown	4096	end of file	59	6D1DB2B3	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2916.tmp	unknown	4096	end of file	59	6D1DB2B3	ReadFile

Analysis Process: vbc.exe PID: 1492 Parent PID: 3016

General

Start time:	17:50:49
Start date:	14/12/2020
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\tmp2915.tmp'
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:	<ul style="list-style-type: none">Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 0000000A.00000002.2248711261.0000000000400000.00000040.00000001.sdmp, Author: Florian RothRule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000A.00000002.2248711261.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows Mail\account{1A8FD30D-54EE-4EEB-8215-CD6025565AFB}.oeaccount	unknown	1506	success or wait	1	406742	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows Mail\account{33B756C3-F7A3-41C2-A60C-F1D01A06DF77}.oeaccount	unknown	1734	success or wait	1	406742	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows Mail\account{FA09A89F-FF90-4081-AEC2-49D0E839C9B5}.oeaccount	unknown	670	success or wait	1	406742	ReadFile

Analysis Process: vbc.exe PID: 948 Parent PID: 3016

General

Start time:	17:50:49
Start date:	14/12/2020
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\tmp2916.tmp'
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:	<ul style="list-style-type: none">• Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 0000000B.00000002.2242831512.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000B.00000002.2242831512.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows Mail\account{1A8FD30D-54EE-4EEB-8215-CD6025565AFB}.oeaccount	unknown	1506	success or wait	1	406742	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows Mail\account{33B756C3-F7A3-41C2-A60C-F1D01A06DF77}.oeaccount	unknown	1734	success or wait	1	406742	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows Mail\account{FA09A89F-FF90-4081-AEC2-49D0E839C9B5}.oeaccount	unknown	670	success or wait	1	406742	ReadFile

Disassembly

Code Analysis