



ID: 504577
Sample Name: DHL_AWB 51887788299___pdf.exe
Cookbook: default.jbs
Time: 12:17:25
Date: 18/10/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report DHL_AWB 51887788299___pdf.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Jbx Signature Overview 5
AV Detection: 5
Compliance: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
System Summary: 6
Data Obfuscation: 6
Boot Survival: 6
Malware Analysis System Evasion: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 10
Contacted IPs 10
General Information 10
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 13
General 13
File Icon 13
Static PE Info 14
General 14
Entrypoint Preview 14
Data Directories 14
Sections 14
Resources 14
Imports 14
Version Infos 14
Network Behavior 14
Code Manipulations 14
Statistics 14
Behavior 14
System Behavior 14
Analysis Process: DHL_AWB 51887788299___pdf.exe PID: 5288 Parent PID: 4904 15
General 15
File Activities 15
File Created 15
File Deleted 15
File Written 15
File Read 15
Analysis Process: schtasks.exe PID: 1380 Parent PID: 5288 15
General 15
File Activities 15
Analysis Process: conhost.exe PID: 5216 Parent PID: 1380 16

Copyright Joe Security LLC 2021

General 16
Analysis Process: DHL_AWB 51887788299___pdf.exe PID: 5336 Parent PID: 5288 16
General 16
Analysis Process: DHL_AWB 51887788299___pdf.exe PID: 1740 Parent PID: 5288 16
General 16
Analysis Process: DHL_AWB 51887788299___pdf.exe PID: 4720 Parent PID: 5288 16
General 16
Analysis Process: DHL_AWB 51887788299___pdf.exe PID: 5216 Parent PID: 5288 17
General 17
Analysis Process: DHL_AWB 51887788299___pdf.exe PID: 1480 Parent PID: 5288 17
General 17
File Activities 18
File Created 18
File Deleted 18
File Written 18
File Read 18
Analysis Process: vbc.exe PID: 3388 Parent PID: 1480 18
General 18
File Activities 19
File Created 19
File Deleted 19
File Written 19
File Read 19
Analysis Process: vbc.exe PID: 4960 Parent PID: 1480 19
General 19
Disassembly 19
Code Analysis 19

Copyright Joe Security LLC 2021

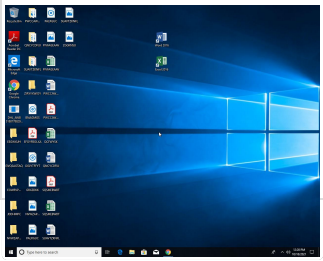
Windows Analysis Report DHL_AWB 51887788299___pd…

Overview

General Information

Sample Name:	DHL_AWB 51887788299___pdf.exe
Analysis ID:	504577
MD5:	c453335b8c0417..
SHA1:	57160596f02d067.
SHA256:	0a0e7c81912b02..
Tags:	DHL exe HawkEye
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

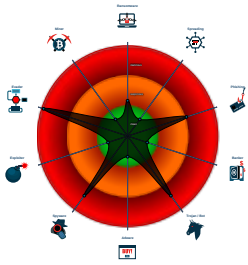
HawkEye
MailPassView

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

Signatures

- Yara detected MailPassView
- Multi AV Scanner detection for subm…
- Yara detected HawkEye Keylogger
- Malicious sample detected (through …
- Detected unpacking (overwrites its o…
- Yara detected AntiVM3
- Detected unpacking (changes PE se…
- Detected HawkEye Rat
- Multi AV Scanner detection for dropp…
- Sample uses process hollowing tech…
- Initial sample is a PE file and has a …
- Writes to foreign memory regions

Classification



Process Tree

- **System is w10x64**
- DHL_AWB 51887788299___pdf.exe (PID: 5288 cmdline: 'C:\Users\user\Desktop\DHL_AWB 51887788299___pdf.exe' MD5: C453335B8C0417BD1C7E7E84278BAC71)
  - schtasks.exe (PID: 1380 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\qyEytITFs' /XML 'C:\Users\user\AppData\Local\Temp\tmp395D.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5216 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - DHL_AWB 51887788299___pdf.exe (PID: 5336 cmdline: C:\Users\user\Desktop\DHL_AWB 51887788299___pdf.exe MD5: C453335B8C0417BD1C7E7E84278BAC71)
  - DHL_AWB 51887788299___pdf.exe (PID: 1740 cmdline: C:\Users\user\Desktop\DHL_AWB 51887788299___pdf.exe MD5: C453335B8C0417BD1C7E7E84278BAC71)
  - DHL_AWB 51887788299___pdf.exe (PID: 4720 cmdline: C:\Users\user\Desktop\DHL_AWB 51887788299___pdf.exe MD5: C453335B8C0417BD1C7E7E84278BAC71)
  - DHL_AWB 51887788299___pdf.exe (PID: 5216 cmdline: C:\Users\user\Desktop\DHL_AWB 51887788299___pdf.exe MD5: C453335B8C0417BD1C7E7E84278BAC71)
  - DHL_AWB 51887788299___pdf.exe (PID: 1480 cmdline: C:\Users\user\Desktop\DHL_AWB 51887788299___pdf.exe MD5: C453335B8C0417BD1C7E7E84278BAC71)
    - vbc.exe (PID: 3388 cmdline: 'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmpCFD5.tmp' MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 4960 cmdline: 'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmpC9A7.tmp' MD5: C63ED21D5706A527419C9FBD730FFB2E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000020.00000002.438579523.000000000400000.00000040.00000001.sdmp	APT_NK_BabyShark_KimJoingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	• 0x147b0:$a1: logins.json • 0x14710:$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encryptedUsername, encryptedPassword FROM moz_login • 0x14f34:$s4: \mozsqlite3.dll • 0x137a4:$s5: SMTP Password
00000020.00000002.438579523.000000000400000.00000040.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	

Source	Rule	Description	Author	Strings
00000013.00000002.527639915.0000000002A7F000.00000004.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
00000000.00000002.300702164.000000000466A000.00000004.00000001.sdmp	MAL_HawkEye_Keylogger_Gen_Dec18	Detects HawkEye Keylogger Reborn	Florian Roth	• 0x87e0e:$s1: HawkEye Keylogger • 0x87e77:$s1: HawkEye Keylogger • 0x81251:$s2: _ScreenshotLogger • 0x8121e:$s3: _PasswordStealer
00000000.00000002.300702164.000000000466A000.00000004.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
Click to see the 24 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
32.2.vbc.exe.400000.0.unpack	APT_NK_BabyShark_KimJoingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	• 0x131b0:$a1: logins.json • 0x13110:$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encryptedUsername, encryptedPassword FROM moz_login • 0x13934:$s4: \mozsqlite3.dll • 0x121a4:$s5: SMTP Password
32.2.vbc.exe.400000.0.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
19.3.DHL_AWB 51887788299___pdf.exe.422dbda.1.raw.unpack	APT_NK_BabyShark_KimJoingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	• 0x131b0:$a1: logins.json • 0x13110:$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encryptedUsername, encryptedPassword FROM moz_login • 0x13934:$s4: \mozsqlite3.dll • 0x121a4:$s5: SMTP Password
19.3.DHL_AWB 51887788299___pdf.exe.422dbda.1.raw.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
32.2.vbc.exe.400000.0.raw.unpack	APT_NK_BabyShark_KimJoingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	• 0x147b0:$a1: logins.json • 0x14710:$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encryptedUsername, encryptedPassword FROM moz_login • 0x14f34:$s4: \mozsqlite3.dll • 0x137a4:$s5: SMTP Password
Click to see the 46 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:



Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Compliance:



Detected unpacking (overwrites its own PE header)

Key, Mouse, Clipboard, Microphone and Screen Capturing:



Yara detected HawkEye Keylogger

Copyright Joe Security LLC 2021

System Summary:



- Malicious sample detected (through community Yara rule)
- Initial sample is a PE file and has a suspicious name

Data Obfuscation:



- Detected unpacking (overwrites its own PE header)
- Detected unpacking (changes PE section rights)

Boot Survival:



- Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion:



- Yara detected AntiVM3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:



- Sample uses process hollowing technique
- Writes to foreign memory regions
- .NET source code references suspicious native API functions
- Allocates memory in foreign processes
- Injects a PE file into a foreign processes

Stealing of Sensitive Information:



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

Remote Access Functionality:



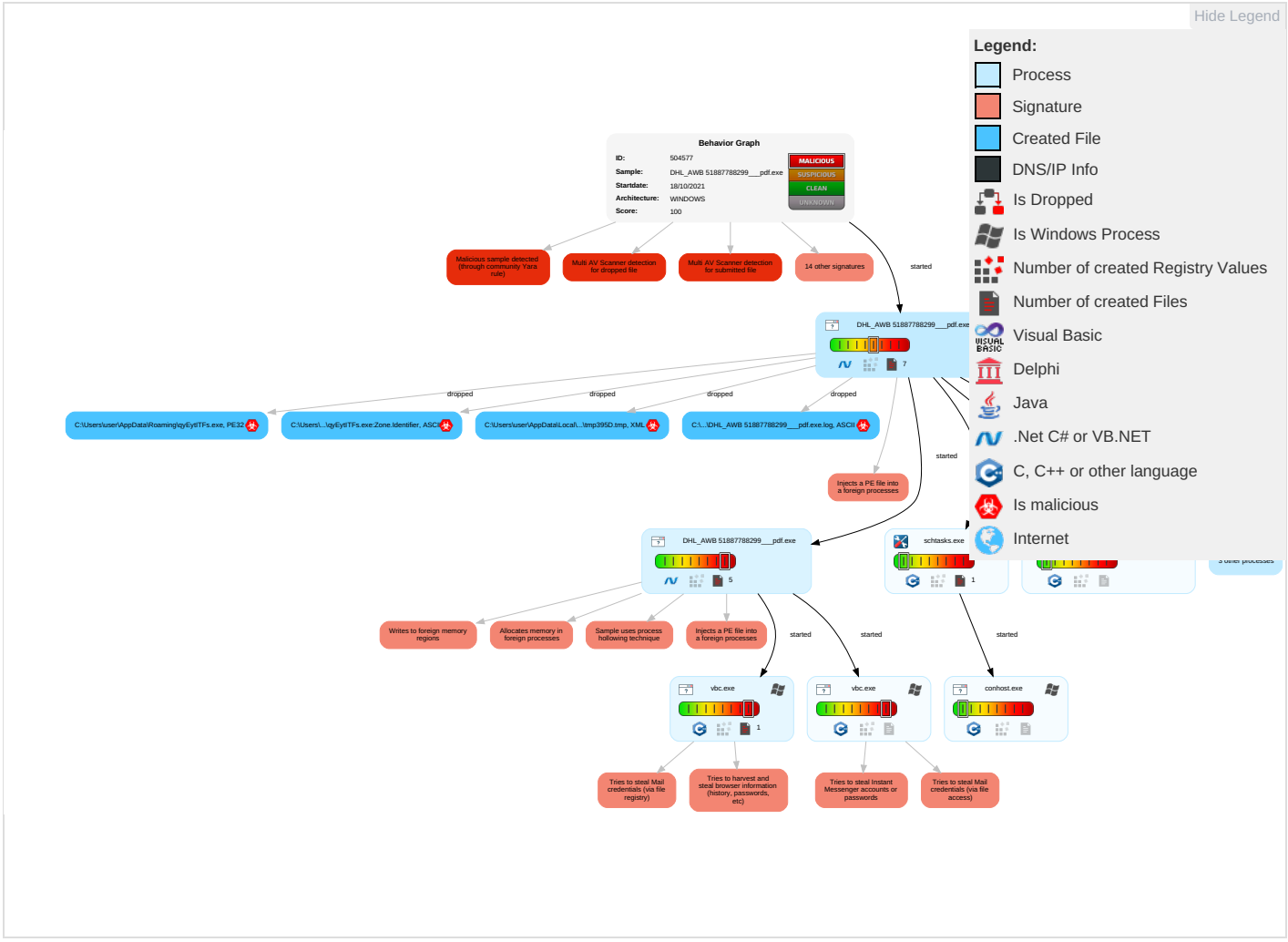
- Yara detected HawkEye Keylogger
- Detected HawkEye Rat

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 Shimming 1	Application Shimming 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Default Accounts	Native API 1 1	Scheduled Task/Job 1	Process Injection 4 1 2	Deobfuscate/Decode Files or Information 1 1	Credentials in Registry 2	Account Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Remote Acce Software 1
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 3	Credentials In Files 1	File and Directory Discovery 2	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Steganograp
Local Accounts	Scheduled Task/Job 1	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2 3	NTDS	System Information Discovery 1 9	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Protocol Impersonatio
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 3 3 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicati
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 4 1 2	DCSync	Process Discovery 4	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	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protoc

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
DHL_AWB 51887788299___pdf.exe	30%	Virustotal		Browse
DHL_AWB 51887788299___pdf.exe	20%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	
DHL_AWB 51887788299___pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\qyEytITFs.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\qyEytITFs.exe	20%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
19.2.DHL_AWB 51887788299___pdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
20.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
0.2.DHL_AWB 51887788299___pdf.exe.4f0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.goodfont.co.kr-d	0%	Avira URL Cloud	safe	
http://https://deff.nelreports.net/api/report?cat=msn	0%	URL Reputation	safe	
http://https://mem.gfx.ms/me/MeControl/10.19168.0/en-US/meCore.min.js	0%	URL Reputation	safe	
http://www.tiro.comBl	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.typography.netlic	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://mem.gfx.ms/meversion?partner=RetailStore2&market=en-us&uhf=1	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.comof	0%	URL Reputation	safe	
http://www.sandoll.co.krhy/	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com$	0%	Avira URL Cloud	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTSGIAG3.crt0)	0%	URL Reputation	safe	
http://www.carterandcone.comt-p	0%	Avira URL Cloud	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6IjAxMmRiZGQ2ZTMxY2I0MTYxNmZjOWNjNjExZDU3MzhiY2UwN	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://aefd.nelreports.net/api/report?cat=bingth	0%	URL Reputation	safe	
http://www.sandoll.co.krFZ	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.carterandcone.comXj	0%	Avira URL Cloud	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.fontbureau.comB.TTF	0%	URL Reputation	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6IjAxOGQyZTYxNTQ5NjE3M2VjYzlkYWMyMWExY2Q4ZDFlYTRmM	0%	Avira URL Cloud	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6IjJkYTFhZDAwNDEyNzQ2M2E3MGUyMWVkZmIxNmUyZjQ2MjBkM	0%	Avira URL Cloud	safe	
http://www.carterandcone.comV	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.carterandcone.comJ	0%	Avira URL Cloud	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6ImQ3OGFmNTY2YzEzMzI1ZTIwNzU3Y2FhOTg3NTNjNGRmMzYwZ	0%	Avira URL Cloud	safe	
http://pomf.cat/upload.php	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/Y	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/fo	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://www.founder.com.cn/cn	0%	URL Reputation	safe	

Copyright Joe Security LLC 2021

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	504577
Start date:	18.10.2021
Start time:	12:17:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL_AWB 51887788299___pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	34
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.evad.winEXE@18/7@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 8.4% (good quality ratio 6.8%) • Quality average: 64.4% • Quality standard deviation: 38.5%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
12:18:33	API Interceptor	2x Sleep call for process: DHL_AWB 51887788299___pdf.exe modified

Copyright Joe Security LLC 2021

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL_AWB 51887788299___pdf.exe.log	
Process:	C:\Users\user\Desktop\DHL_AWB 51887788299___pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\97695d7d-f686-3bef-0bdf-699df2eb7081	
Process:	C:\Users\user\Desktop\DHL_AWB 51887788299___pdf.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	88
Entropy (8bit):	5.361372635874905
Encrypted:	false
SSDEEP:	3:/o3Q2QffK1zJcNXCDYnOUEU8ARZEYY:/yjQfi1uN84Eko
MD5:	C0E51F45B53C7238AF5A1F4B1DCF1931
SHA1:	846FD39DE731D6C9D2829D586AD009F13FB25954
SHA-256:	F4A352FDA42C6B11EF30471C653020667966DBE93151CBC42BBC391388CD97E5
SHA-512:	6869CD38287B7F44CF3D1FABA93A20DC6BD5833E1EAAAAB4FC6C2D713646A9B5E0A3907D6D2E55B396AF3DA3E0ADDA4220F3E441B8FCE7BC392E47A6632E578A
Malicious:	false

C:\Users\user\AppData\Local\Temp\97695d7d-f686-3bef-0bdf-699df2eb7081	
Preview:	vMSR5XyDGaw1S/nFeKjG9z/ZXgLmXlt/JGB9hvSuvginM1+wNBRAb4BSxMm6GSOXqKY5eXHQMTtNvXr1HIdW1A==

C:\Users\user\AppData\Local\Temp\bhv360E.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x29982920, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	26738688
Entropy (8bit):	1.0616470367564328
Encrypted:	false
SSDEEP:	24576:g1qhtSFKmL3cCDPf6r0i1cREikolT3YEgI:bsL3c46r4
MD5:	5974D181790002AEA45D96C4BEC189AD
SHA1:	A9C28C81583ADCD9E3C017F41209F7D7BBD0C539
SHA-256:	A529DD54651A9DA03A4E826283726ED580B35392BB8035481419058634A1A162
SHA-512:	F0433D4849853CBD7776134EE3D21BB35DCA3E2B94D0DB021594210B945FB99205CF5FF94ABE296AB4A000BB35F333DC025118A5840272E023182D449A84B218
Malicious:	false
Preview:	).) ... .9.....p*.~.....w7.....x7.....yu.h.....z.....w....._.....B..... ....3....x..... ....i..O/....y+.....'....y..... .....

C:\Users\user\AppData\Local\Temp\tmp395D.tmp	
Process:	C:\Users\user\Desktop\DHL_AWB 51887788299___pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1658
Entropy (8bit):	5.172379903143974
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBtOtn:cbhH7MlNQ8/rydbz9I3YODOLNdq3Ho
MD5:	F01606DFFA93B906ADADAF9CCF0BCD82
SHA1:	B56CFDFB4D077FD658DE028E5452C3DFE8EA418D
SHA-256:	61B3653451D1203EF4DE3F895A820180ED1D20EE43CAD98CA3E690253350F5C8
SHA-512:	B2E71A1517F3683932EFA1E2F8FB429F75965B68E9E52F815E36D5839B2B80FFD14C4C03AF1906E2D62C00E860B6BA6D3CC6A5798F0CBEA1A22D601260C6A30
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAv

C:\Users\user\AppData\Local\Temp\tmpCFD5.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	modified
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\qyEytITFs.exe	
Process:	C:\Users\user\Desktop\DHL_AWB 51887788299___pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	852480
Entropy (8bit):	7.814230472508504
Encrypted:	false
SSDEEP:	12288:FwLm88jyKO+ihkMqxus73XBez9wPDWmiHe/bM+77TBl+67WsjYlu2DLrLXaU:FwLoVOS8YiwP63He/brTBlDzeu

C:\Users\user\AppData\Roaming\qyEytITFs.exe	
MD5:	C453335B8C0417BD1C7E7E84278BAC71
SHA1:	57160596F02D06791805A2324AAEC47A2CAB9B26
SHA-256:	0A0E7C81912B02E6EC1C7FBB338F4EF200E23D441D57C692CC88FEF616593F0D
SHA-512:	95C03192ECA1756435F2580F562A36F6EEAE42415EBD5932A2BDA60DD8107E3415DBFB7BF93D2AEE5120D1CF26A62BF36B3881250C2540654FD26B96FA95473C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 20%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....la.....0.....n.... ... .@.. .....`..... ..@.....W.... .....@..... ..... ..H.....text...t.... ..... ..`.rsrc..... .....@..@.rel oc.....@.....@..B.....P.....H.....|.....b.y..n}F2.}(.&zx...Q..2....L.....i..tn..p.e.l.....8...)..."g.....A..'....~.H.H..}6..B<..... 8N!._..@...Qr.f@c.<V.T..D...f%.,.>.ua..y..v.."p.W.[!&^....U..Vsl..L.....!.!..>....]i.<U.....i...S...>IaQ_Gos"....{...E.6.....*..."/8.T..Ji.O..y....>7.....c.W.x>.`.\N.:Z#,...A.G3.|. 0.,...@.....Y..KX.6.;l.\...m.Q..9f.....J....]s.W...'.....C!..-.. .$...[Ig.T..

C:\Users\user\AppData\Roaming\qyEytITFs.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\DHL_AWB 51887788299___pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.814230472508504
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	DHL_AWB 51887788299___pdf.exe
File size:	852480
MD5:	c453335b8c0417bd1c7e7e84278bac71
SHA1:	57160596f02d06791805a2324aaec47a2cab9b26
SHA256:	0a0e7c81912b02e6ec1c7fbb338f4ef200e23d441d57c692cc88fef616593f0d
SHA512:	95c03192eca1756435f2580f562a36f6eeae42415ebd5932a2bda60dd8107e3415dbfb7bf93d2aee5120d1cf26a62bf36b3881250c2540654fd26b96fa95473c
SSDEEP:	12288:FwLm88jyKO+ihkMqxus73XBez9wPDWmiHe/bM+77TBl+67WsjYlu2DLrLXaU:FwLoVOS8YiwP63He/brTBlDzeu
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....la.....0.....n.... ... .@.. .....`.....@.....

File Icon



Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d176e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x616CD4C5 [Mon Oct 18 01:58:29 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xcf774	0xcf800	False	0.870147778614	data	7.8197081023	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xd2000	0x5d8	0x600	False	0.420572916667	data	4.12172736374	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd4000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: DHL_AWB 51887788299___pdf.exe PID: 5288 Parent PID: 4904

General

Start time:	12:18:25
Start date:	18/10/2021
Path:	C:\Users\user\Desktop\DHL_AWB 51887788299___pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DHL_AWB 51887788299___pdf.exe'
Imagebase:	0x4f0000
File size:	852480 bytes
MD5 hash:	C453335B8C0417BD1C7E7E84278BAC71
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000000.00000002.300702164.000000000466A000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.300702164.000000000466A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.296408700.0000000002809000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000000.00000002.298050605.0000000004009000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.298050605.0000000004009000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 1380 Parent PID: 5288

General

Start time:	12:18:40
Start date:	18/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\qyEytITFs' /XML 'C:\Users\user\AppData\Local\Temp\tmp395D.tmp'
Imagebase:	0x870000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 5216 Parent PID: 1380

General

Start time:	12:18:41
Start date:	18/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: DHL_AWB 51887788299___pdf.exe PID: 5336 Parent PID: 5288

General

Start time:	12:18:41
Start date:	18/10/2021
Path:	C:\Users\user\Desktop\DHL_AWB 51887788299___pdf.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\DHL_AWB 51887788299___pdf.exe
Imagebase:	0x480000
File size:	852480 bytes
MD5 hash:	C453335B8C0417BD1C7E7E84278BAC71
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: DHL_AWB 51887788299___pdf.exe PID: 1740 Parent PID: 5288

General

Start time:	12:18:43
Start date:	18/10/2021
Path:	C:\Users\user\Desktop\DHL_AWB 51887788299___pdf.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\DHL_AWB 51887788299___pdf.exe
Imagebase:	0x340000
File size:	852480 bytes
MD5 hash:	C453335B8C0417BD1C7E7E84278BAC71
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: DHL_AWB 51887788299___pdf.exe PID: 4720 Parent PID: 5288

General

Start time:	12:18:43
Start date:	18/10/2021
Path:	C:\Users\user\Desktop\DHL_AWB 51887788299___pdf.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\DHL_AWB 51887788299___pdf.exe
Imagebase:	0x3e0000
File size:	852480 bytes
MD5 hash:	C453335B8C0417BD1C7E7E84278BAC71
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: DHL_AWB 51887788299___pdf.exe PID: 5216 Parent PID: 5288

General

Start time:	12:18:43
Start date:	18/10/2021
Path:	C:\Users\user\Desktop\DHL_AWB 51887788299___pdf.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\DHL_AWB 51887788299___pdf.exe
Imagebase:	0x340000
File size:	852480 bytes
MD5 hash:	C453335B8C0417BD1C7E7E84278BAC71
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: DHL_AWB 51887788299___pdf.exe PID: 1480 Parent PID: 5288

General

Start time:	12:18:44
Start date:	18/10/2021
Path:	C:\Users\user\Desktop\DHL_AWB 51887788299___pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHL_AWB 51887788299___pdf.exe
Imagebase:	0x4c0000
File size:	852480 bytes
MD5 hash:	C453335B8C0417BD1C7E7E84278BAC71
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2021

Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000013.00000002.527639915.0000000002A7F000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000013.00000002.526218473.0000000002971000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000013.00000002.526218473.0000000002971000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000013.00000002.526218473.0000000002971000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000013.00000002.521607657.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000013.00000002.521607657.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000013.00000003.294671201.00000000041D5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000013.00000003.294671201.00000000041D5000.00000004.00000001.sdmp, Author: Joe Security • Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 00000013.00000002.528751258.0000000007280000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000013.00000002.528751258.0000000007280000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000013.00000002.528751258.0000000007280000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000013.00000002.528093886.0000000003965000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000013.00000002.528093886.0000000003965000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 3388 Parent PID: 1480

General

Start time:	12:18:47
Start date:	18/10/2021
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\tmpCFD5.tmp'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000014.00000002.309474312.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 4960 Parent PID: 1480

General

Start time:	12:19:51
Start date:	18/10/2021
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\tmpC9A7.tmp'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 00000020.00000002.438579523.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000020.00000002.438579523.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021