ID: 635260
Sample Name:
600000sqm_pdf.exe
Cookbook: default.jbs
Time: 18:01:45
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

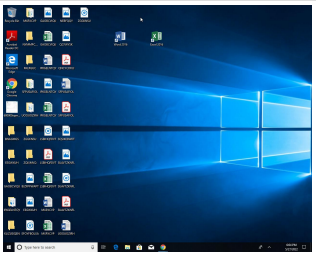
Windows Analysis Report

600000sqm_pdf.exe

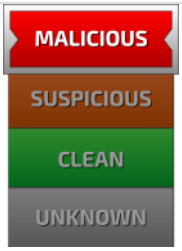
Overview

General Information

Sample Name:	600000sqm_pdf.exe
Analysis ID:	635260
MD5:	3e08fed24c7e27..
SHA1:	d00231c828b96f..
SHA256:	10c1f9eb418d31..
Infos:	



Detection



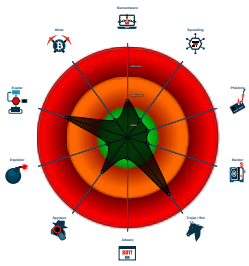
FormBook

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Antivirus detection for URL or domain
- Malicious sample detected (through…
- Multi AV Scanner detection for drop…
- Found evasive API chain (may stop…
- Initial sample is a PE file and has a…
- C2 URLs / IPs found in malware con…
- Creates a DirectInput object (often f…
- Uses 32bit PE files
- Yara signature match

Classification



Process Tree

- **System is w10x64**
- 600000sqm_pdf.exe (PID: 6444 cmdline: "C:\Users\user\Desktop\600000sqm_pdf.exe" MD5: 3E08FED24C7E27A75F6D9C52FC226376)
  - oampomo.exe (PID: 6532 cmdline: C:\Users\user\AppData\Local\Temp\oampomo.exe C:\Users\user\AppData\Local\Temp\buziwssym MD5: 420F226DE2598C3A2DE1C56C9607055F)
    - oampomo.exe (PID: 6636 cmdline: C:\Users\user\AppData\Local\Temp\oampomo.exe C:\Users\user\AppData\Local\Temp\buziwssym MD5: 420F226DE2598C3A2DE1C56C9607055F)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.theayushtrivedi.xyz/m1e8/"
  ],
  "decoy": [
    "balanceforpaws.com",
    "landseamed.com",
    "drayseavci.com",
    "tattydaddystattoos.com",
    "fzkj-qtq.com",
    "garagedoorrepairwestcovina.com",
    "mixmarkt.site",
    "mark-ebook2store.com",
    "vermeer-mi.com",
    "shopspliced.com",
    "alrafidane.net",
    "themaisonmargiela.com",
    "suncasacentral-vsip.net",
    "creatcard-mine.site",
    "studiopounce.com",
    "hao685.com",
    "ipanemashoesaustralia.com",
    "51898dy.com",
    "nfttoknow.com",
    "multiple-player.com",
    "npbtechteam.com",
    "cyptocred.com",
    "pradsley-portfolio.site",
    "stangerenterprises.com",
    "swz9.com",
    "m3mofficespace.com",
    "projectyoka.com",
    "magazini-kristi.com",
    "fortunekey-vt.com",
    "joshlortiz9.net",
    "joincfn.com",
    "amazttt.com",
    "jjewelryun.com",
    "basecampsolarkit.com",
    "klausstilling.com",
    "mendce.online",
    "projectextinguish.com",
    "voyagedecor.com",
    "caliaboriginal.com",
    "shelfdb.club",
    "asianshemalestube.com",
    "bestimonials.com",
    "narroyo.space",
    "zzbzjx.com",
    "ilamatrix.com",
    "reviewmymedication.com",
    "acurademo.com",
    "tllechateau.com",
    "nun.finance",
    "99onlinesports-18.xyz",
    "visitqrcode.com",
    "for-policy-ingame.xyz",
    "kurui800.com",
    "manugryson.net",
    "bottomboitatz.com",
    "creaactivos.com",
    "culionerosx.com",
    "satknight.com",
    "agpglassco.com",
    "freshmeneve.com",
    "realjoboptionalfreedoms.com",
    "mid-puzzle.com",
    "asop-shop.com",
    "3dnkf.com"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.265512226.0000000001360000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.265512226.0000000001360000.00000004.00001000.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000002.265512226.0000000001360000.00000004.00001000.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.oampomo.exe.1360000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.oampomo.exe.1360000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x143a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x979a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1361c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa493:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab27:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.oampomo.exe.1360000.1.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a49:$sqlite3step: 68 34 1C 7B E1 • 0x17b5c:$sqlite3step: 68 34 1C 7B E1 • 0x17a78:$sqlite3text: 68 38 2A 90 C5 • 0x17b9d:$sqlite3text: 68 38 2A 90 C5 • 0x17a8b:$sqlite3blob: 68 53 D8 7F 8C • 0x17bb3:$sqlite3blob: 68 53 D8 7F 8C
1.2.oampomo.exe.1360000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.oampomo.exe.1360000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 1 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Malware Analysis System Evasion

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

Stealing of Sensitive Information

Yara detected FormBook

Remote Access Functionality

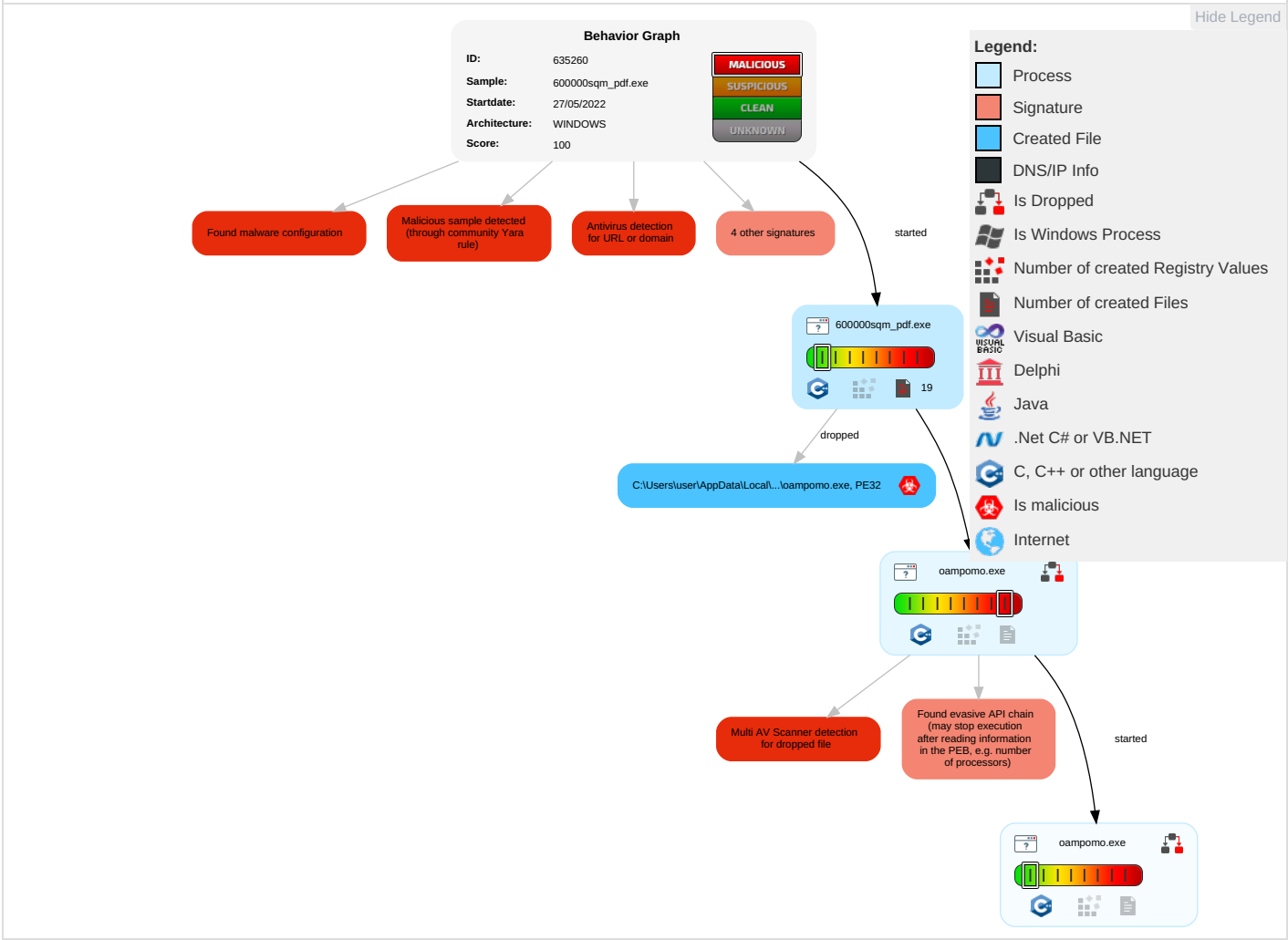
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 2 Native API	Path Interception	1 1 Process Injection	1 1 Process Injection	1 Input Capture	1 System Time Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Obfuscated Files or Information	LSASS Memory	1 3 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Software Packing	Security Account Manager	2 File and Directory Discovery	SMB/Windows Admin Shares	1 Clipboard Data	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	1 3 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

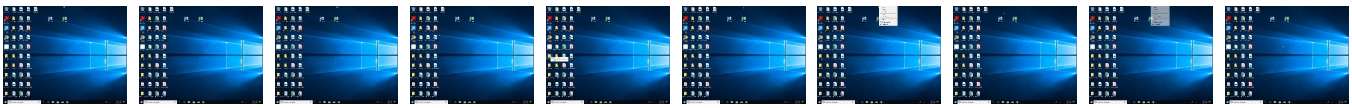
Behavior Graph

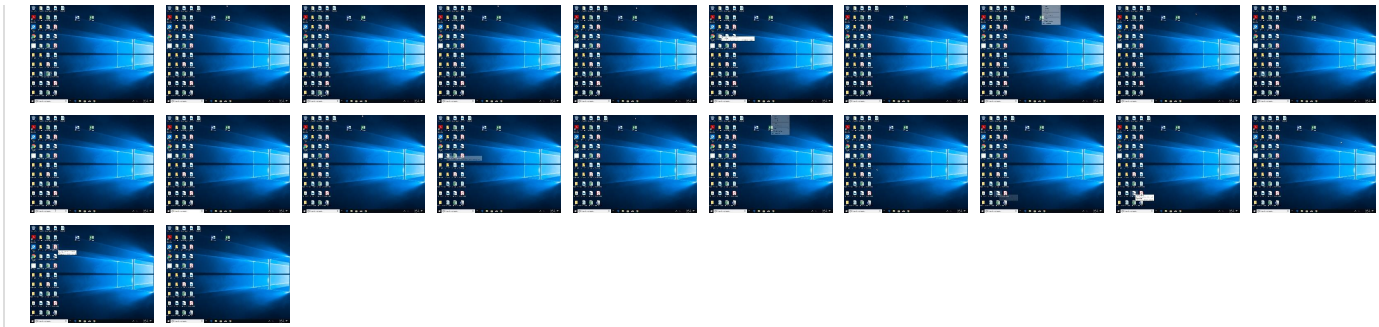


Screenshots

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
600000sqm_pdf.exe	24%	ReversingLabs	Win32.Trojan.Injexa	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\oampomo.exe	34%	ReversingLabs	Win32.Trojan.Jaik	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.oampomo.exe.1360000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.theayushtrivedi.xyz/m1e8/	1%	Virustotal		Browse
www.theayushtrivedi.xyz/m1e8/	100%	Avira URL Cloud	phishing	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.theayushtrivedi.xyz/m1e8/	true	• 1%, Virustotal, Browse • Avira URL Cloud: phishing	low

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635260
Start date and time: 27/05/202218:01:45	2022-05-27 18:01:45 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	600000sqm_pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	26
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.evad.winEXE@5/4@0/0
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 94.9% (good quality ratio 89%) • Quality average: 78.3% • Quality standard deviation: 28.9%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.223.24.244
- Excluded domains from analysis (whitelisted): fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, settings-win.data.microsoft.com, ctldl.windowsupdate.com, arc.msn.com, ris.api.iris.microsoft.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\buziwssym

Process:	C:\Users\user\Desktop\600000sqm_pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	4846
Entropy (8bit):	6.19128158947241
Encrypted:	false
SSDEEP:	96:2c4cTOkDU0x2rpbmSYIKxxVjGqRjkfDHy4vzvQRy8B3/dnD52+oG:2Ov8rpqTX5GqRjkrHVzvQg8dVnD52BG

MD5:	24F50F0F58C0C96C0CF910BA8ABF860E
SHA1:	D03E9B72D9ACA8220924C6FE42E53B2DC20521FE
SHA-256:	09D99B98DEAC1E6BF491CB455BADA50485D69719A1F5FCD6A8220D33FCB12943
SHA-512:	F766E4244246023A28A283C512E28D2B2CBDE238B9652530669F40CE422CC089D99A5F1C21F50C5ECB509FDD3600101282BAA2ED3BE4BEC4BA1D4DFF329563 6
Malicious:	false
Reputation:	low

Preview:

......T3|3....|Z/..?Y....?Y...|Z'.8.....|Z+.......R.'......v..v.#......R.'......v..v........R.'......v.7v........R.'......v.?v.;|B....U...?....Fv..v..T..|...6v..v.3T..T..R.>..U.(.T.....R.=v...vZ+|./U......|....
.Z...........7....?........z)..X.T.(X.v.+.|1../.....T....v./.Z......8.......|....TZ+..T./...6=...T3...?Y..'T..T.....T..T.T..T.>T.>.v.'v..T..T..T..v.T.'T..6=..W.%9@.....W...=..WY. @._.......=
..W.d@........=...T3|3..?Y...8.'....R..v..|B'...T..9..T..v..T.'.v.'4.....z?..T..FU...6.v...v..#R..FU..>..v...v..#U.U...?.R....WY. @...........v.+4.R.........v.+|B+...|Z/.4.8./....T./6=...T3|3..?
Y...8.'....R.?v..|B'...T..9..T..v..T.'.v.'4..F...z?.{u...T..FU...6.v..?v..;T..FU..>..v..?v..;T..FU....v..?v..;T...6U.....v..?v..;R..FU..>..v..?v..;U.U...?.R..?.W.%9@...........v.+|B....T
..T..v.4.....................v.+|B+...|Z/.4.8./....T./6=...T3|3.8.'....R..v..|B'...T..9..T..v..T.'.v.'4......z?..T..FU...6.v...v...T..FU..>..v...v...U.U...?.R...W.d@..........v.+4........h..

C:\Users\user\AppData\Local\Temp\nsm7EC9.tmp

Process:	C:\Users\user\Desktop\600000sqm_pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	333039
Entropy (8bit):	7.539849969909107
Encrypted:	false
SSDEEP:	6144:ZRocEP2nYwkIbzFxoypqHZWU26zgYcg5v3zZWxvBvipvncWdJsSGw:zsP2n7keXoypeXdDcg5v3zIvccWnsS
MD5:	56919D917C91AA748752CF88F254CB38
SHA1:	1AC3EF9E10CC8E3BFDAD099533915F4D43B47131
SHA-256:	7B4782A70EB6A35F1EA9F6F3ABAE92F947C322461C9BADBD9DF3426DE4F044B9
SHA-512:	DCB34FFC5381F062AF614C51595928D10F6B0132AF3FD57ECECC09BEFBFC00B1CB4F288696785D1CA43581390DBFAB5D8A6D75C9BCB40E349B533A7EE1FF2 34
Malicious:	false
Reputation:	low
Preview:	........,....................:...........,... ....B...................j.. ....

C:\Users\user\AppData\Local\Temp\oampomo.exe

Process:	C:\Users\user\Desktop\600000sqm_pdf.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	134144
Entropy (8bit):	6.412383509028528
Encrypted:	false
SSDEEP:	1536:NFTOG+x8+YaGDARvmJVBqNvnlajcCOO0LdXU8JiA1OynPl6zqjzswa+98qSIJnXR:efbnR6BqNvncvhwdYz2swteq4iG5sFv
MD5:	420F226DE2598C3A2DE1C56C9607055F
SHA1:	2328B1AFCBD3823CBD499A1508FD9506E85E3664
SHA-256:	85B26D2C71B2D64678749F5F1C338AC41D383F9CACE83471AA946D56ADD9ECA8
SHA-512:	C9CFBE723BDFB4933AD87F510304943D3979D1745153F8A26947C5A0A51FD442D513086C7CF76DD813343330E094C8123CFA172AD71AC2FBA861382C7A8315B
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 34%
Reputation:	low
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$..........(.}c{.}c{.}c{./.{.}c{./.{.}c{./.{.}c{(.bz.}c{.}b{.}c{y.gz.}c{y..{.}c{ y.az.}c{Rich.}c{........................PE..L...6..b...@..........................`............@..........................................@.......................P..........T.......................... ....@............................................text...5.......................... ..`.rdata..>N.......P..................@..@.data....1..........................@....rsrc........@......................@..@.reloc.......P........ ....@..B.. ....

C:\Users\user\AppData\Local\Temp\r8pmu65b4mp

Process:	C:\Users\user\Desktop\600000sqm_pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	189439
Entropy (8bit):	**7.990149083409857**
Encrypted:	**true**
SSDEEP:	3072:pHYBv4lcDMXPbKnH40O7YkIbhxoQujgFxo0vQU+3TzU+fnWU26RbhgYcgOyfH3zq:eocEP2nYwkIbzFxoypqHZWU26zgYcg5m
MD5:	883E8E6E1970481CD91AE93A1A43A47B

SHA1:	F051F3955C4C37205160406E71E8E2A5BFC3F076
SHA-256:	3B31B72CBBA1FE88740655612674F220EEEE903CD4640FDB6858CFF7C10BBA55
SHA-512:	CA6CB93CB058F44821696674697982D13837031BB46D325102489164F335CCFA770ED812F9919A44699AECB5461A137D8A87BAD852C1A1FA5513A624F8DC0C64
Malicious:	false
Reputation:	low
Preview:	v..;..v[p..pv.07.....o.....=.....t.9....1.U..u.q.@.G....y-Mw.t.....&.v...k2.K.AW..@(r..B...,T..?....mD"+..;",..[Qd.u....L.>O.....B.....K...}..og.^...."y....r.k.'...j.{...U#.+..z..T.....8 <b...._e.k^.^..".+.B8....36..7...H...U....M.6.a.k..v[..w....."....wp..l....=.....9....1.E..u.q.@.G....Z.M.6.0...._.w{....j_sW..f.....w.o...y..x.R..U.....[Qd.uS...M.=./)y#I....B8..*.... <K^&W.....ze..O./hv.GX.r.k.'...Z.....U.#.+..}.o.>....8<b..b..4...k..XV.".+.B8.0"T36..7...H...U.Q....6.a.k..v[p.6.....{."....wp.....=.....t.9....1.U..u.q.@.G....Z.M.6.0...._.w{....j_sW.. f.....w.o...y..x.R..U.....[Qd.uS...M.=./)y#I....B8..*....<K^&W.....ze..O./hv.GX.r.k.'...j.{...UT".+..}.o.....8<b..b..4...k^.X..".+.B8.0"T36..7...H...U.Q....6.a.k..v[p.6.....{."....wp.... ...=.....t.9....1.U..u.q.@.G....Z.M.6.0...._.w{....j_sW..f.....w.o...y..x.R..U.....[Qd.uS...M.=./)y#I....B8..*....<K^&W.....ze..O./hv.GX.r.k.'...j.{...UT".+..}.o.....8<b..b..4...k^.X..".+.B8.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.137966707966572
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	600000sqm_pdf.exe
File size:	407658
MD5:	3e08fed24c7e27a75f6d9c52fc226376
SHA1:	d00231c828b96ff0178ab59240e5ba53f7b0ce25
SHA256:	10c1f9eb418d31fb36efefe032ccd9a8a057728cd757dca4e47ed124e9e8d791
SHA512:	6dc8596a94585f2ee7b83975bf93c370188e145c4fd1d7d5194454455ef5b9c2afaa9c97d86e923e1cf87f61e5e3d7dbdabd13487930454ae8b6086efa97cbd4
SSDEEP:	6144:10YOG0SkOr1KCHtyOBumZ1JP0iMiBrOMSO0r28Wp+9mlTC39cm2HO7rI:a9+gOYU1Nr+VrfW4JH2L
TLSH:	CF84E0E6E78148A5ED5207B588378C3A6293BE7EBC70A60E575E78716F733D3006250B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qJ...$...$...$./. {...$...%.;.$.".y...$..3....$.f."...$.Rich..$.....PE..L.....iF.....Z.....

File Icon

Icon Hash:	f131617131042321

Static PE Info

General

Entrypoint:	0x4032fa
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4669CEB6 [Fri Jun 8 21:48:38 2007 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	55f3dfd13c0557d3e32bcbc604441dd3

Entrypoint Preview

Instruction
sub esp, 00000180h
push ebx
push ebp
push esi
xor ebx, ebx
push edi
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 00409170h
xor esi, esi
mov byte ptr [esp+14h], 00000020h
call dword ptr [00407030h]
push ebx
call dword ptr [00407278h]
mov dword ptr [00423FD4h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 00000160h
push eax
push ebx
push 0041F4E8h
call dword ptr [00407154h]
push 0040922Ch
push 00423720h
call 00007F7FF12DC318h
call dword ptr [004070B4h]
mov edi, 00429000h
push eax
push edi
call 00007F7FF12DC306h
push ebx
call dword ptr [00407108h]
cmp byte ptr [00429000h], 00000022h
mov dword ptr [00423F20h], eax
mov eax, edi
jne 00007F7FF12D9B7Ch
mov byte ptr [esp+14h], 00000022h
mov eax, 00429001h
push dword ptr [esp+14h]
push eax
call 00007F7FF12DBDF9h
push eax
call dword ptr [00407218h]
mov dword ptr [esp+1Ch], eax
jmp 00007F7FF12D9BD5h
cmp cl, 00000020h
jne 00007F7FF12D9B78h
inc eax
cmp byte ptr [eax], 00000020h
je 00007F7FF12D9B6Ch
cmp byte ptr [eax], 00000022h
mov byte ptr [esp+14h], 00000020h
jne 00007F7FF12D9B78h
inc eax
mov byte ptr [esp+14h], 00000022h
cmp byte ptr [eax], 0000002Fh
jne 00007F7FF12D9BA5h
inc eax
cmp byte ptr [eax], 00000053h
jne 00007F7FF12D9B80h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x73a0	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2c000	0x20118	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x288	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x59ac	0x5a00	False	0.668142361111	data	6.45807821776	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x117a	0x1200	False	0.4453125	data	5.17513527374	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1afd8	0x400	False	0.6015625	data	4.98110806401	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x20118	0x20200	False	0.325077517023	data	4.21955172329	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2c280	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x2c6e8	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4294967295, next used block 4294967295	English	United States
RT_ICON	0x2d790	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 4294901759, next used block 4294901503	English	United States
RT_ICON	0x2fd38	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 4294967295, next used block 4294113788	English	United States
RT_ICON	0x33f60	0x10828	data	English	United States
RT_ICON	0x44788	0x74be	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_DIALOG	0x4bc48	0x100	data	English	United States
RT_DIALOG	0x4bd48	0x11c	data	English	United States
RT_DIALOG	0x4be68	0x60	data	English	United States
RT_GROUP_ICON	0x4bec8	0x5a	data	English	United States
RT_MANIFEST	0x4bf28	0x1eb	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetFileTime, CompareFileTime, SearchPathA, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CreateDirectoryA, SetFileAttributesA, Sleep, CreateFileA, GetFileSize, GetModuleFileNameA, GetTickCount, GetCurrentProcess, CloseHandle, ExitProcess, GetWindowsDirectoryA, GetTempPathA, GetCommandLineA, LoadLibraryA, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, GetTempFileNameA, lstrlenA, lstrcatA, GetSystemDirectoryA, lstrcmpiA, lstrcmpA, ExpandEnvironmentStringsA, GlobalFree, GlobalAlloc, WaitForSingleObject, GetExitCodeProcess, SetErrorMode, GetModuleHandleA, LoadLibraryExA, GetProcAddress, FreeLibrary, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, WriteFile, ReadFile, MulDiv, SetFilePointer, FindClose, FindNextFileA, FindFirstFileA, DeleteFileA, CopyFileA
USER32.dll	EndDialog, ScreenToClient, GetWindowRect, EnableMenuItem, GetSystemMenu, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, SetClipboardData, EmptyClipboard, RegisterClassA, TrackPopupMenu, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, CreateDialogParamA, DestroyWindow, SetTimer, SetWindowTextA, PostQuitMessage, SetForegroundWindow, wsprintfA, SendMessageTimeoutA, FindWindowExA, SystemParametersInfoA, CreateWindowExA, GetClassInfoA, DialogBoxParamA, CharNextA, OpenClipboard, ExitWindowsEx, IsWindow, GetDlgItem, SetWindowLongA, LoadImageA, GetDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, EndPaint, ShowWindow
GDI32.dll	SetBkColor, GetDeviceCaps, DeleteObject, CreateBrushIndirect, CreateFontIndirectA, SetBkMode, SetTextColor, SelectObject
SHELL32.dll	SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA, SHGetSpecialFolderLocation
ADVAPI32.dll	RegQueryValueExA, RegSetValueExA, RegEnumKeyA, RegEnumValueA, RegOpenKeyExA, RegDeleteKeyA, RegDeleteValueA, RegCloseKey, RegCreateKeyExA
COMCTL32.dll	ImageList_AddMasked, ImageList_Destroy, ImageList_Create
ole32.dll	CoTaskMemFree, OleInitialize, OleUninitialize, CoCreateInstance
VERSION.dll	GetFileVersionInfoSizeA, GetFileVersionInfoA, VerQueryValueA

Possible Origin

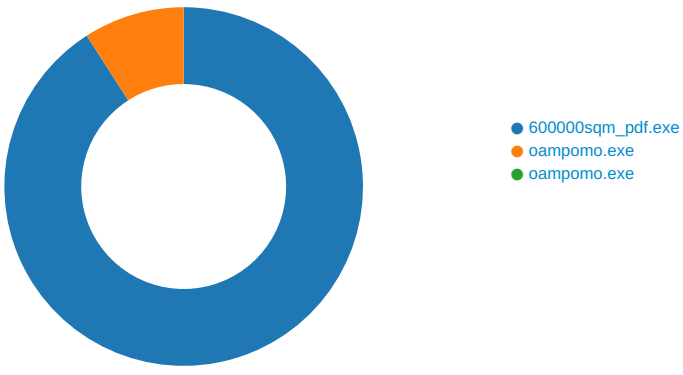
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: 600000sqm_pdf.exe PID: **6444**, Parent PID: **5160**

General

Target ID:	0
Start time:	18:02:55
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\600000sqm_pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\600000sqm_pdf.exe"
Imagebase:	0x400000
File size:	407658 bytes
MD5 hash:	3E08FED24C7E27A75F6D9C52FC226376
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4032ED	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsm7EC8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40582D	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsm7EC9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40582D	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nsh7EF9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40582D	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E9	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E9	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E9	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E9	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E9	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsh7EF9.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4015E9	CreateDirectoryA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E9	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E9	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E9	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E9	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	4015E9	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\r8pmu65b4mp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4057F7	CreateFileA
C:\Users\user\AppData\Local\Temp\buziwssym	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4057F7	CreateFileA
C:\Users\user\AppData\Local\Temp\oampomo.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4057F7	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsm7EC8.tmp	success or wait	1	40345C	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsh7EF9.tmp	success or wait	1	40544C	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\nsm7EC9.tmp</td><td>0</td><td>24993</td><td>fd 11 00 00 fd 00 00 00 2c 01 00 00 02 00 00 00 fd 01 00 00 01 00 00 00 fd 05 00 00 3a 00 00 00 1c 0c 00 00 00 00 00 00 2c 11 00 00 01 00 00 00 fd 11 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 fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 fd 00 00 fd 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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 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 00 00 00 00 00 00</td><td>,:,</td><td>success or wait</td><td>17</td><td>4031E9</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\r8pmu65b4mp</td><td>0</td><td>16384</td><td>76 fd fd 3b fd 0c 76 5b 70 fd fd 70 76 14 30 37 fd 7f 0e fd ea fd 6f fd 23 fd fd fd fd 14 fd 10 fd 3d fd fd 1c fd 19 74 fd 39 01 fd fd fd 31 fd 55 fd 1c 75 fd 71 fd 40 fd 47 18 fd fd fd 79 2d 4d 77 fd 74 fd fd fd fd 26 fd 76 fd 18 fd 6b 32 0b 4b fd 41 57 fd fd 40 28 72 fd fd 42 fd 14 11 2c 54 fd fd 3f fd fd fd fd 6d 44 22 2b fd fd 3b 22 2c fd 11 5b 51 64 17 75 fd 11 fd fd 4c fd 3e 4f fd fd 10 fd 0c fd fd fd 2e 42 fd fd fd fd 00 dc 1a 1c fd 4b fd fd fd 7d 02 fd 6f 67 fd 5e fd 15 06 fd 22 79 fd fd 00 fd 72 fd 6b fd 27 fd 2e fd 6a fd 7b 11 fd fd 55 23 dd 2b fd fd 7a 1b fd 54 fd 17 09 fd fd 38 3c 62 fd fd 52 fd 5f 65 fd 6b 5e fd 5e 0f fd 22 fd 2b fd 42 38 fd fd fd fd 33 36 fd 07 37 1b 02 fd 48 fd 0c fd 55 17 fd a0 fd 4d fd</td><td>v;v[ppv07o=t91Uuq@Gy-Mwt&vk2KAW@(rB,T?mD"+;",[QduL>O.BK}og^"yrk'.j{U#+zT8<b_ek^^"+B8367HUM</td><td>success or wait</td><td>12</td><td>40303D</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\buziwssym</td><td>0</td><td>4846</td><td>fd fd fd fd fd fd 54 33 7c 33 fd fd fd fd 7c 5a 2f fd 08 3f 59 fd 3a fd 08 3f 59 fd 3a fd 7c 5a 27 fd 38 fd d7 fd fd fd 7c 5a 2b fd fd fd fd fd fd fd 52 fd 27 fd fd fd fd fd fd 76 fd 07 76 fd 23 fd fd fd fd fd fd 52 fd 27 fd fd fd fd fd fd 76 fd 0f 76 fd 0b fd fd fd fd fd fd 52 fd 27 fd fd 0e fd fd fd 76 fd 37 76 fd 13 fd fd fd fd fd fd 52 fd 27 fd fd 03 fd fd fd 76 fd 3f 76 fd 3b 7c 42 fd fd fd fd 55 fd fd fd 3f fd fd fd fd 46 76 fd fd 76 fd fd 54 fd fd 7c fd fd fd 36 76 fd fd 76 fd 33 54 fd fd 54 fd fd 52 fd 3e fd 0d 55 c6 28 2e 54 fd fd fd fd fd 52 fd 3d 76 fd c8 fd 76 5a 2b 7c fd 2f 55 fd fd fd fd fd fd 7c fd fd fd 14 fd 5a fd fd fd 07 fd fd fd 0f fd fd fd 37 fd fd fd fd 3f fd fd fd fd e0 fd fd e1 7a 29 fd fd 58 fd 54 fd 28</td><td>T3|3|Z/?Y?Y|Z'8|Z+R'vv#R'vvR'v7vR'v?v;|BU?FvvT|6vv3TTR>U(.TR=vvZ+|/U|Z7?z)XT(</td><td>success or wait</td><td>1</td><td>40303D</td><td>WriteFile</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\oampomo.exe	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd 1c 0d 28 fd 7d 63 7b fd 7d 63 7b fd 7d 63 7b fd 2f fd 7b fd 7d 63 7b fd 2f fd 7b fd 7d 63 7b fd 2f fd 7b fd 7d 63 7b 28 0f 62 7a fd 7d 63 7b fd 7d 62 7b fd 7d 63 7b 79 04 67 7a fd 7d 63 7b 79 04 fd 7b fd 7d 63 7b 79 04 61 7a fd 7d 63 7b 52 69 63 68 fd 7d 63 7b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 36 fd fd 62 00 00 00	MZ@!L!This program cannot be run in DOS mode.$(}c{}c{}c{/{}c{/{}c{/{}c{(bz}c{}b{}c{ygz}c{y{}c{yaz}c{Rich}c{PEL6b	success or wait	9	40303D	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\600000sqm_pdf.exe	unknown	512	success or wait	316	40329A	ReadFile
C:\Users\user\Desktop\600000sqm_pdf.exe	unknown	16384	success or wait	16	40329A	ReadFile
C:\Users\user\AppData\Local\Temp\nsm7EC9.tmp	unknown	4	success or wait	1	402FC7	ReadFile
C:\Users\user\AppData\Local\Temp\nsm7EC9.tmp	unknown	4594	success or wait	1	40307D	ReadFile
C:\Users\user\AppData\Local\Temp\nsm7EC9.tmp	unknown	4	success or wait	3	402FC7	ReadFile
C:\Users\user\AppData\Local\Temp\nsm7EC9.tmp	unknown	16384	success or wait	22	403021	ReadFile

Analysis Process: oampomo.exe

PID: **6532**, Parent PID: **6444**

General

Target ID:	1
Start time:	18:02:58
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Local\Temp\oampomo.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\oampomo.exe C:\Users\user\AppData\Local\Temp\buziwssym
Imagebase:	0x210000
File size:	134144 bytes
MD5 hash:	420F226DE2598C3A2DE1C56C9607055F
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: 00000001.00000002.265512226.0000000001360000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.265512226.0000000001360000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.265512226.0000000001360000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 34%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\buziwssym	unknown	4096	success or wait	1	21F88C	ReadFile
C:\Users\user\AppData\Local\Temp\buziwssym	unknown	4096	success or wait	1	21F88C	ReadFile
C:\Users\user\AppData\Local\Temp\r8pmu65b4mp	unknown	189439	success or wait	1	DF09ED	ReadFile

Analysis Process: oampomo.exe PID: **6636**, Parent PID: **6532**

General

Target ID:	2
Start time:	18:03:00
Start date:	27/05/2022
Path:	C:\Users\user\AppData\Local\Temp\oampomo.exe
Wow64 process (32bit):	
Commandline:	C:\Users\user\AppData\Local\Temp\oampomo.exe C:\Users\user\AppData\Local\Temp\buziwssym
Imagebase:	
File size:	134144 bytes
MD5 hash:	420F226DE2598C3A2DE1C56C9607055F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

No disassembly