ID: 412322
Sample Name: New-Order 04758485.exe
Cookbook: default.jbs
Time: 15:58:35
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

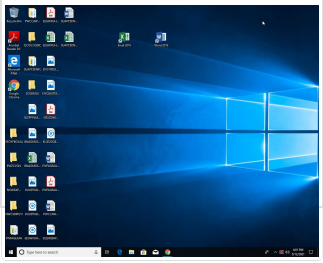
Analysis Report New-Order 04758485.exe

Overview

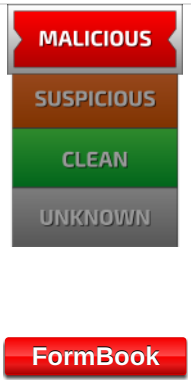
General Information

Sample Name:	New-Order 04758485.exe
Analysis ID:	412322
MD5:	ed4361a7909fc65.
SHA1:	b49fef47c793f39…
SHA256:	914c79c23d30b4..
Infos:	

Most interesting Screenshot:



Detection



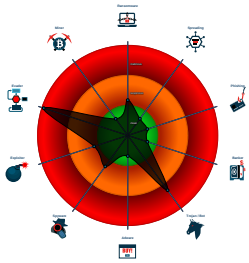
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…

Classification



Startup

- **System is w10x64**
- New-Order 04758485.exe (PID: 5632 cmdline: 'C:\Users\user\Desktop\New-Order 04758485.exe' MD5: ED4361A7909FC65A189B4ADAAC292991)
  - New-Order 04758485.exe (PID: 5884 cmdline: C:\Users\user\Desktop\New-Order 04758485.exe MD5: ED4361A7909FC65A189B4ADAAC292991)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmmon32.exe (PID: 2540 cmdline: C:\Windows\SysWOW64\cmmon32.exe MD5: 2879B30A164B9F7671B5E6B2E9F8DFDA)
        - cmd.exe (PID: 4936 cmdline: /c del 'C:\Users\user\Desktop\New-Order 04758485.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5400 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.bendhighswimming.com/crdi/"
  ],
  "decoy": [
    "propertyjumpstartwebinar.com",
    "boc-vip.club",
    "polestarnyc.com",
    "travelonlinebiz.com",
    "bukovynaent.com",
    "bestfashoin.com",
    "miniindiastore.com",
    "wehatebillgates.com",
    "holmescountyjusticecourt.com",
    "colectivorenovemosjuntos.com",
    "houstowarehouse.com",
    "aocsw.com",
    "sml-uniform.com",
    "bandanasaint.com",
    "petposhdeluxe.com",
    "ezcscpawq.com",
    "ladiesoption.club",
    "refixu.com",
    "selfwrrrth.com",
    "rovietry.com",
    "enaoc.com",
    "karyolaw.com",
    "diversitymarketingtx.net",
    "browsersentenderbanco.net",
    "samtheshepherd.com",
    "nash-arbitrazh.com",
    "gampang-kerja.tech",
    "ereplacementparrts.com",
    "eventmidasbuy14.com",
    "sia-rikvel.com",
    "top2016.net",
    "686638.com",
    "ton.blue",
    "desktower.net",
    "dbykq020.com",
    "stack30.com",
    "tiendasfotoprix.com",
    "kylesmaier.com",
    "ekmantsang.com",
    "jumlasx.xyz",
    "qingqingyuyin.com",
    "cdnsubs.xyz",
    "maxamoose.com",
    "huelling.com",
    "xn--bjrnnstet-z2a8q.online",
    "betale-posten.com",
    "lalatendu.info",
    "nochipmanicure.net",
    "bichat.website",
    "washington32reds.com",
    "centrodesaludcrecer.com",
    "phihoteldeimedaglioni.com",
    "kilmalliefarms.com",
    "icecreamsocialwp.com",
    "mac-makeup.club",
    "elzooz.com",
    "iqomw.com",
    "bestattorneycle.com",
    "startonsocial.com",
    "purensoessentials.com",
    "therealyolandafay.com",
    "feildwolf.com",
    "nativesupps.com",
    "nbatimeout.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.342372255.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000A.00000002.342372255.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000A.00000002.342372255.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18419:$sqlite3step: 68 34 1C 7B E1 • 0x1852c:$sqlite3step: 68 34 1C 7B E1 • 0x18448:$sqlite3text: 68 38 2A 90 C5 • 0x1856d:$sqlite3text: 68 38 2A 90 C5 • 0x1845b:$sqlite3blob: 68 53 D8 7F 8C • 0x18583:$sqlite3blob: 68 53 D8 7F 8C
0000000C.00000002.474310455.0000000004920000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000C.00000002.474310455.0000000004920000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 22 entries				

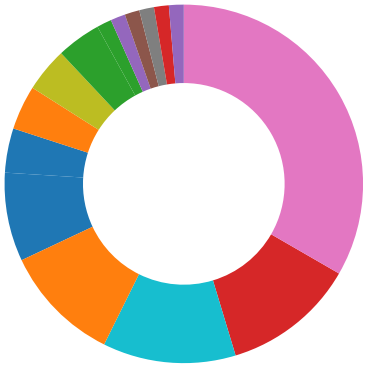
Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.New-Order 04758485.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
10.2.New-Order 04758485.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 • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a6f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b6fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
10.2.New-Order 04758485.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17619:$sqlite3step: 68 34 1C 7B E1 • 0x1772c:$sqlite3step: 68 34 1C 7B E1 • 0x17648:$sqlite3text: 68 38 2A 90 C5 • 0x1776d:$sqlite3text: 68 38 2A 90 C5 • 0x1765b:$sqlite3blob: 68 53 D8 7F 8C • 0x17783:$sqlite3blob: 68 53 D8 7F 8C
10.2.New-Order 04758485.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
10.2.New-Order 04758485.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b4f7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c4fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- 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:

Found malware configuration

Yara detected FormBook

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)

Initial sample is a PE file and has a suspicious name

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

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

Malware Analysis System Evasion:

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)

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

Modifies the context of a thread in another process (thread injection)

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

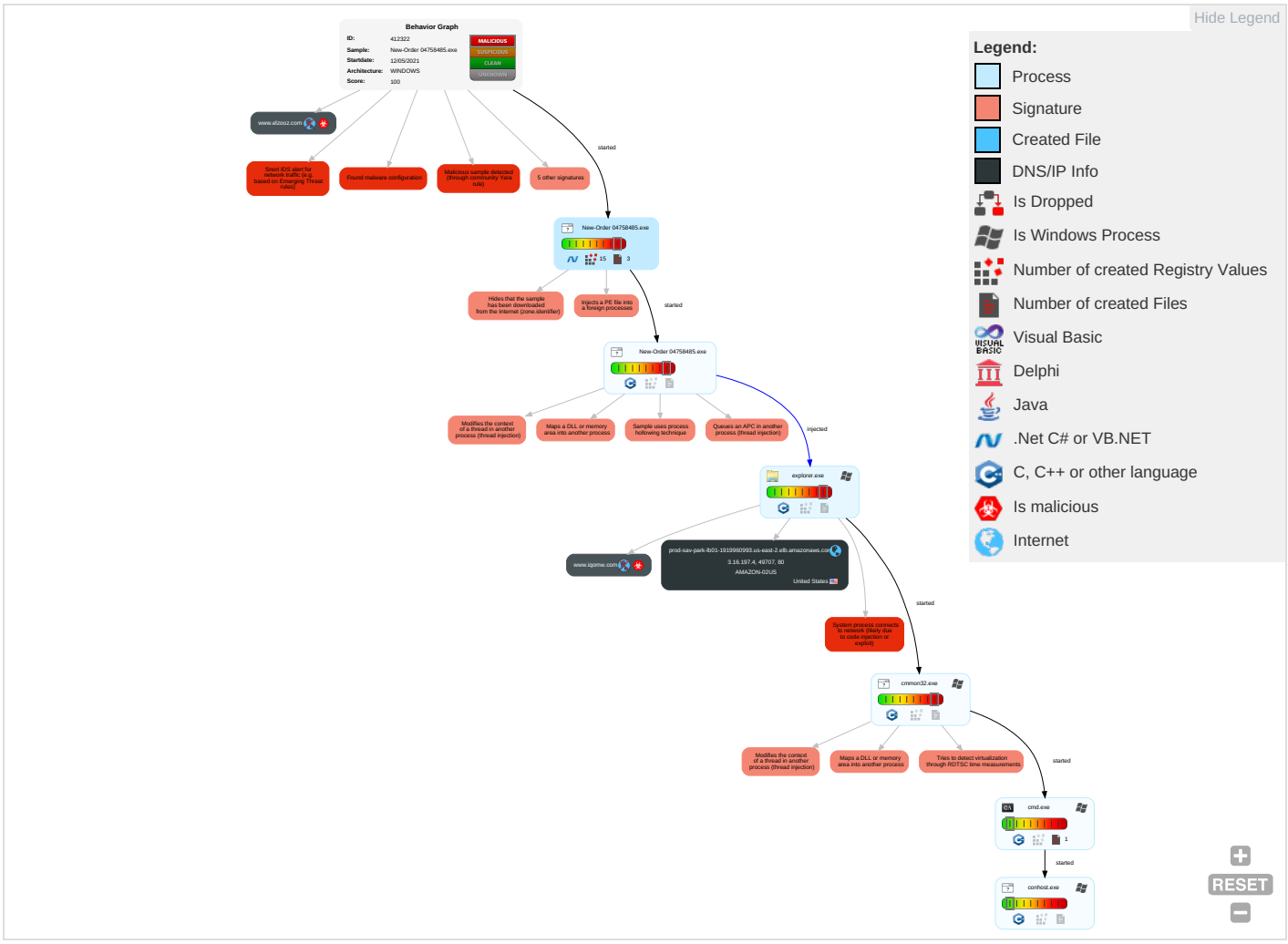
Remote Access Functionality:

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
Valid Accounts 1	Shared Modules 1	Valid Accounts 1	Valid Accounts 1	Rootkit 1	Credential API Hooking 1	Security Software Discovery 1 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Masquerading 1	Input Capture 1	Process Discovery 2	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 4
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 6 1 2	Valid Accounts 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Archive Collected Data 1	Automated Exfiltration	Non-Application Layer Protocol 3
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Disable or Modify Tools 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 3 1	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 6 1 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Deobfuscate/Decode Files or Information 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protoco
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Obfuscated Files or Information 3	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Software Packing 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols

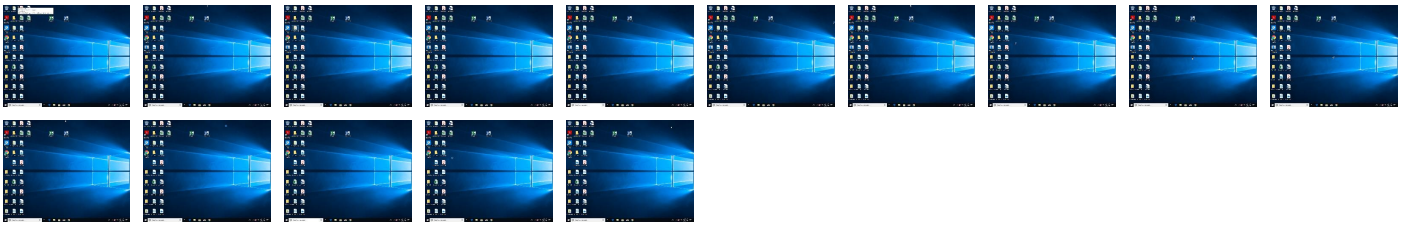
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.New-Order 04758485.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.iqomw.com	0%	Virustotal		Browse
www.elzooz.com	0%	Virustotal		Browse

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.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.co	0%	Virustotal		Browse
http://ns.adobe.co	0%	Avira URL Cloud	safe	
http://ns.adobe.c/gO	0%	Avira URL Cloud	safe	
http://purl.r	0%	Avira URL Cloud	safe	
http://www.iqomw.com/crdi/?qZ_l=s5ZBPuXj17fhOA1bx0aCq9ENe7PeNxUER8tsGnybxkKx7jlbiox1QoAzGi7ZgPeOdZ4f&y0Dluf=g480w6JH	0%	Avira URL Cloud	safe	
http://ns.adobe	0%	Avira URL Cloud	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://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://ns.adobe.cK	0%	Avira URL Cloud	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.cobjO	0%	Avira URL Cloud	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://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://ns.ado/1O	0%	Avira URL Cloud	safe	
http://ns.adob	0%	Avira URL Cloud	safe	
http://ns.adobe.cD	0%	Avira URL Cloud	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	
www.bendhighswimming.com/crdi/	0%	Avira URL Cloud	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	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.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	

Source	Detection	Scanner	Label	Link
http://ns.adb	0%	URL Reputation	safe	
http://ns.adb	0%	URL Reputation	safe	
http://ns.adb	0%	URL Reputation	safe	
http://logo.verisign	0%	Avira URL Cloud	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	
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://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	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	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	3.16.197.4	true	false		high
www.iqomw.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown
www.elzooz.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.iqomw.com/crdi/?qZ_l=s5ZBPuXj17fhOA1bx0aCq9ENe7PeNxUER8tsGnybxkKx7jlbiox1QoAzGi7ZgPeOdZ4f&y0Dluf=g480w6JH	true	• Avira URL Cloud: safe	unknown
www.bendhighswimming.com/crdi/	true	• Avira URL Cloud: safe	low

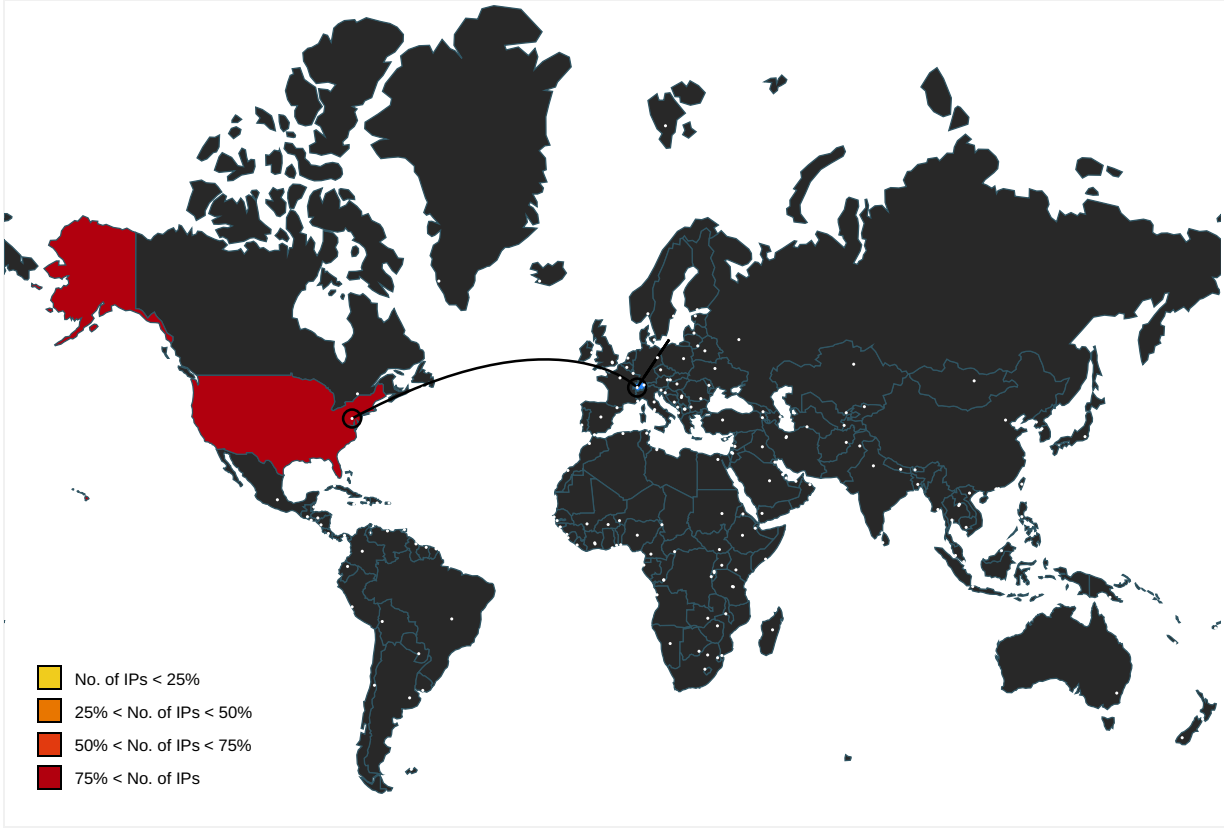
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 0000000B.00000000.328332626.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 0000000B.00000000.328332626.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 0000000B.00000000.328332626.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 0000000B.00000000.328332626.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 0000000B.00000000.328332626.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.cobj	New-Order 04758485.exe, 00000000.00000003.301805201.00000000006F4C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ns.adobe.co	New-Order 04758485.exe, 00000000.00000003.227583172.00000000 06F42000.00000004.00000001.sdmp, New-Order 04758485.exe, 00000000.00000003.301790150.00000000 06F42000.00000004.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 0000000B.00000000.328332626.0000000008B46000.00000002.00000001.sdmp	false		high
http://ns.adobe.c/gO	New-Order 04758485.exe, 00000000.00000003.227583172.00000000 06F42000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://purl.r	New-Order 04758485.exe, 00000000.00000003.227284672.00000000 06F42000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.adobe	New-Order 04758485.exe, 00000000.00000003.227583172.00000000 06F42000.00000004.00000001.sdmp, New-Order 04758485.exe, 00000000.00000003.227284672.00000000 06F42000.00000004.00000001.sdmp, New-Order 04758485.exe, 00000000.00000003.227189386.00000000 06F42000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	explorer.exe, 0000000B.00000000.328332626.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://pki.goog/gsr2/GTS1O1.crt0	New-Order 04758485.exe, 00000000.00000002.302607546.00000000 00F16000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.cK	New-Order 04758485.exe, 00000000.00000003.227490070.00000000 06F42000.00000004.00000001.sdmp, New-Order 04758485.exe, 00000000.00000003.227189386.00000000 06F42000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 0000000B.00000000.328332626.0000000008B46000.00000002.00000001.sdmp	false		high
http://ns.adobe.c/g	New-Order 04758485.exe, 00000000.00000003.301790150.00000000 06F42000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.cobjO	New-Order 04758485.exe, 00000000.00000003.227583172.00000000 06F42000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	explorer.exe, 0000000B.00000000.328332626.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pki.goog/repository/0	New-Order 04758485.exe, 00000000.00000002.302607546.00000000 00F16000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.ado/1O	New-Order 04758485.exe, 00000000.00000003.227583172.00000000 06F42000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.adob	New-Order 04758485.exe, 00000000.00000003.227284672.00000000 06F42000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.adobe.cD	New-Order 04758485.exe, 00000000.00000003.227189386.00000000 06F42000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	explorer.exe, 0000000B.00000000.328332626.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 0000000B.00000000.328332626.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 0000000B.00000000.328332626.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 0000000B.00000000.328332626.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 0000000B.00000000.328332626.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 0000000B.00000000.328332626.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	explorer.exe, 0000000B.0000000 0.328332626.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 0000000B.0000000 0.328332626.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 0000000B.0000000 0.328332626.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://crl.pki.goog/GTS1O1core.crl0	New-Order 04758485.exe, 000000 00.00000002.302607546.00000000 00F16000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	explorer.exe, 0000000B.0000000 0.328332626.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 0000000B.0000000 0.328332626.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adb	New-Order 04758485.exe, 000000 00.00000003.227583172.00000000 06F42000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 0000000B.0000000 0.328332626.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://logo.verisign	explorer.exe, 0000000B.0000000 0.331004335.000000000F640000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	explorer.exe, 0000000B.0000000 0.328332626.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 0000000B.0000000 0.328332626.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 0000000B.0000000 0.328332626.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.goog/gsr2/gsr2.crl0?	New-Order 04758485.exe, 000000 00.00000002.302607546.00000000 00F16000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 0000000B.0000000 0.328332626.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	New-Order 04758485.exe, 000000 00.00000002.302817037.00000000 02A21000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	explorer.exe, 0000000B.0000000 0.328332626.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.ado/1	New-Order 04758485.exe, 000000 00.00000003.301790150.00000000 06F42000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
3.16.197.4	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412322
Start date:	12.05.2021
Start time:	15:58:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	New-Order 04758485.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:	16
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@7/1@2/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 25.4% (good quality ratio 22.2%) • Quality average: 66.3% • Quality standard deviation: 35.1%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 104.43.193.48, 172.217.168.68, 131.253.33.200, 13.107.22.200, 184.30.24.56 • Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, a-0001.a-afdentry.net.trafficmanager.net, blobcollector.events.data.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, www.google.com, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:59:35	API Interceptor	216x Sleep call for process: New-Order 04758485.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3.16.197.4	4si5VtPNTe.exe	Get hash	malicious	Browse	• www.topsych.com/bucw/?APw8=pHmd48aeJBSPZZ4oXPqMUa9iB+zw7o9633Qm6JoN2J/ksYljdm2ak3+3AB9oAE45NnYEmo/gHQ==&b62T=5jlLiNy09
	BANK-ACCOUNT. NUMBER.PDF.exe	Get hash	malicious	Browse	• www.blockchainbiotech.com/bfos/?n6=RpHxKvXHpdiDbnbp&a2JT=nlGyaopHry7E6bdI+FTOLhsX82bxJb3FdwYLplkJtK7ddv9iNxe81y+/5BoFARz6j+UD

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PRF00202156KMT.exe	Get hash	malicious	Browse	• www.yellowways.com/epns/?BZ_PRR=g1HyJk+wG0QMozIZ4pSFaEKPb4YO3nGzZZ5CcX3yDfnOXFLur8M6WBwA2Tz5ODgZyyZKu9K6pg==&ctxXOb=9rSHdNip5
	Materialliste f#U00fcr Angebot.exe	Get hash	malicious	Browse	• www.gaixuexi.com/mbg/?d4tTFV0x=biSbQxXptFsFatGCwU6rH3jFlmn8/7PXCP5ApA8iXgWtFmg/kZZqbn1fxj5u3vE5BJvNMtq/NQ==&vP=9rQPzxEXvpg8-Jrp
	4LkSpeVqKR.exe	Get hash	malicious	Browse	• www.7chd.com/uoe8/?V2=LhqpTfJ8&rDHpw=pp2ekQWroypTFKaJa5Qkcd1bUyGAkfDbiqxtSX5G9L70Cmz7PeGJVxgmdicR3ONQ4/wh
	new order.xlsx	Get hash	malicious	Browse	• www.beachjunction.com/uoe8/?PbvtUz=UaWDVduFhUYoxBOntLFCG15pALMvw+tGTmrfHTf8nBW+JGuA66stVf5lwBUB/caHaGfK0Q==&-Z=zVeT
	2B0CsHzr8o.exe	Get hash	malicious	Browse	• www.herreramedical.com/bncm/?LXedv=rRFZcIV0o2WsZrj/H7Tic0eMA0JUK/5bHF3i9UX4kn8AQLz1xJTlllEaZDDEVH8ZeF4M&lhv4=O0DPaJ7hHb34yZ

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	PURCHASE ORDER REQUIREMENT.exe	Get hash	malicious	Browse	• 3.16.197.4
	4si5VtPNTe.exe	Get hash	malicious	Browse	• 3.16.197.4
	BANK-ACCOUNT. NUMBER.PDF.exe	Get hash	malicious	Browse	• 3.16.197.4
	PRF00202156KMT.exe	Get hash	malicious	Browse	• 3.16.197.4
	Materialliste f#U00fcr Angebot.exe	Get hash	malicious	Browse	• 3.16.197.4
	FY9Z5TR6rr.exe	Get hash	malicious	Browse	• 13.59.53.244
	KVYhrHPAgF.exe	Get hash	malicious	Browse	• 3.16.197.4
	4LkSpeVqKR.exe	Get hash	malicious	Browse	• 3.16.197.4
	new order.xlsx	Get hash	malicious	Browse	• 3.16.197.4
	Purchase Order-070POR044127.exe	Get hash	malicious	Browse	• 52.15.160.167
	New order list.exe	Get hash	malicious	Browse	• 13.59.53.244
	Request for Quotation.exe	Get hash	malicious	Browse	• 13.59.53.244
	2B0CsHzr8o.exe	Get hash	malicious	Browse	• 52.15.160.167
	tgix.exe	Get hash	malicious	Browse	• 13.59.53.244

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	8c2d96ab_by_Libranalysis.exe	Get hash	malicious	Browse	• 52.15.160.167
	DHL Receipt_AWB811470484778.exe	Get hash	malicious	Browse	• 52.15.160.167
	NEW ORDER.exe	Get hash	malicious	Browse	• 52.15.160.167
	Quotation_05052021.Pdf.exe	Get hash	malicious	Browse	• 52.15.160.167
	945AEE9E799851EB1A2215FE1A60E55E41EB6D69EF4CB.exe	Get hash	malicious	Browse	• 3.14.18.91
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 52.15.160.167

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	350969bc_by_Libranalysis.exe	Get hash	malicious	Browse	• 52.58.78.16
	7bYDInO.rtf	Get hash	malicious	Browse	• 52.210.171.182
	nT5pUwoJSS.dll	Get hash	malicious	Browse	• 54.247.61.18
	1c60a1e9_by_Libranalysis.rtf	Get hash	malicious	Browse	• 44.230.85.241
	Order 122001-220 guanzo.exe	Get hash	malicious	Browse	• 18.219.49.238
	main_setup_x86x64.exe	Get hash	malicious	Browse	• 104.192.141.1
	A6FAm1ae1j.exe	Get hash	malicious	Browse	• 3.138.180.119
	New_Order.exe	Get hash	malicious	Browse	• 75.2.115.196
	NAVTECO_R1_10_05_2021,pdf.exe	Get hash	malicious	Browse	• 13.58.50.133
	YDHhjjAEFbel88t.exe	Get hash	malicious	Browse	• 99.83.175.80
	yU7RItYEQ9kCkZE.exe	Get hash	malicious	Browse	• 99.83.175.80
	Shipment Document BL,INV and packing List.exe	Get hash	malicious	Browse	• 52.58.78.16
	4xPBZai06p.dll	Get hash	malicious	Browse	• 13.225.75.73
	0OyVQNXrTo.exe	Get hash	malicious	Browse	• 3.142.167.54
	rAd00Nae9w.dll	Get hash	malicious	Browse	• 13.225.75.73
	DOC24457188209927.exe	Get hash	malicious	Browse	• 13.224.193.2
	user-invoice-8488888.doc	Get hash	malicious	Browse	• 104.192.141.1
	user-invoice-8488888.doc	Get hash	malicious	Browse	• 104.192.141.1
	ProForma Invoice 20210510.exe	Get hash	malicious	Browse	• 13.113.228.117
	PO9448882.exe	Get hash	malicious	Browse	• 18.219.49.238

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New-Order 04758485.exe.log	
Process:	C:\Users\user\Desktop\New-Order 04758485.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1619
Entropy (8bit):	5.337900566095637
Encrypted:	false
SSDEEP:	48:MIHK5HKXE1qHxvbHK5AHKzvIHmYHKhQnoPtHoxH6HK1HD8mHj:Pq5qXEwRzq2qzAGYqhQnoPtIxH6q17D
MD5:	C0DC87FFFF01072EBCBB902D65319450
SHA1:	4A6842A765DFE94AF4CF92E0411AA10C75C0EB44
SHA-256:	E21F44D67E40BC67307C0DA25FD54CCA1EFD768B3E2479AC6555A6B1942EB697
SHA-512:	7555C34F9373ACF381BDA12BBC81A34CF20ABEEDD035B84340D5EACBB3991549B82D5BDAE1D4A73019F6CFDD9F68EBC5BA501C8EAC773BA1B00754589ED5E21D
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New-Order 04758485.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.Windows.Forms.DataVisualization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\ass

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.19960356247498
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:	New-Order 04758485.exe
File size:	1693696
MD5:	ed4361a7909fc65a189b4adaac292991
SHA1:	b49fef47c793f39be360ce9a1e2f8bee9e254706
SHA256:	914c79c23d30b4df795779800b6e14ac42bec2dc618d11d7c0b526960fc6283c
SHA512:	2ec1019b53db86e7c82f28cfea369203fdf2a0c82f6932f34785ef2a4d0e845b800a25df13d1a2e11abcb34cb750ecdd59e370f8bdfd99c906c866ad15e72eff
SSDEEP:	24576:fBVRWITiQ+diVXMrPyfGOkzrodjHl7NA68qQwV3Z1PGg:nBTiQ7pMPy7kzraDl7R8qQK3z
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....T.2..... .....@.. .....@.....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x59e5ee
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, HIGH_ENTROPY_VA
Time Stamp:	0x32AB54D5 [Sun Dec 8 23:52:53 1996 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
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x19e598	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1a0000	0xd2f	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x1a2000	0xc	.reloc
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	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
.text	0x2000	0x19c5f4	0x19c600	False	0.497171846582	data	6.20151324644	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x1a0000	0xd2f	0xe00	False	0.368303571429	data	4.68496519206	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x1a2000	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	0x1a00a0	0x3ec	data		
RT_MANIFEST	0x1a048c	0x8a3	XML 1.0 document, UTF-8 Unicode (with BOM) text		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

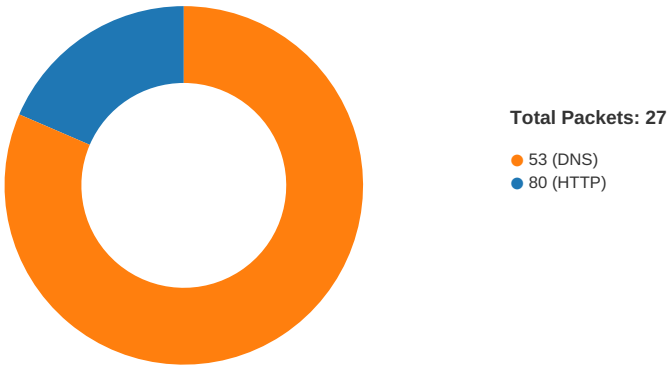
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright The Ecclesbourne School 2015
Assembly Version	1.0.0.0
InternalName	Year 11 Dynamic Grade data.exe
FileVersion	1.0.0.0
CompanyName	SCCM2K12
LegalTrademarks	
Comments	
ProductName	Year 11 Dynamic Grade data
ProductVersion	1.0.0.0
FileDescription	Year 11 Dynamic Grade data
OriginalFilename	Year 11 Dynamic Grade data.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-16:01:12.217029	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49707	80	192.168.2.3	3.16.197.4
05/12/21-16:01:12.217029	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49707	80	192.168.2.3	3.16.197.4
05/12/21-16:01:12.217029	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49707	80	192.168.2.3	3.16.197.4

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 16:01:12.073072910 CEST	49707	80	192.168.2.3	3.16.197.4
May 12, 2021 16:01:12.209650993 CEST	80	49707	3.16.197.4	192.168.2.3
May 12, 2021 16:01:12.209789038 CEST	49707	80	192.168.2.3	3.16.197.4
May 12, 2021 16:01:12.217029095 CEST	49707	80	192.168.2.3	3.16.197.4
May 12, 2021 16:01:12.353585005 CEST	80	49707	3.16.197.4	192.168.2.3
May 12, 2021 16:01:12.354059935 CEST	80	49707	3.16.197.4	192.168.2.3
May 12, 2021 16:01:12.354101896 CEST	80	49707	3.16.197.4	192.168.2.3
May 12, 2021 16:01:12.354343891 CEST	49707	80	192.168.2.3	3.16.197.4
May 12, 2021 16:01:12.354446888 CEST	49707	80	192.168.2.3	3.16.197.4
May 12, 2021 16:01:12.491090059 CEST	80	49707	3.16.197.4	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 15:59:17.559443951 CEST	59353	53	192.168.2.3	8.8.8.8
May 12, 2021 15:59:17.609463930 CEST	53	59353	8.8.8.8	192.168.2.3
May 12, 2021 15:59:18.608581066 CEST	52238	53	192.168.2.3	8.8.8.8
May 12, 2021 15:59:18.660043001 CEST	53	52238	8.8.8.8	192.168.2.3
May 12, 2021 15:59:19.578691959 CEST	49873	53	192.168.2.3	8.8.8.8
May 12, 2021 15:59:19.631653070 CEST	53	49873	8.8.8.8	192.168.2.3
May 12, 2021 15:59:20.499625921 CEST	53196	53	192.168.2.3	8.8.8.8
May 12, 2021 15:59:20.551640034 CEST	53	53196	8.8.8.8	192.168.2.3
May 12, 2021 15:59:21.498747110 CEST	56777	53	192.168.2.3	8.8.8.8
May 12, 2021 15:59:21.547563076 CEST	53	56777	8.8.8.8	192.168.2.3
May 12, 2021 15:59:22.409842968 CEST	58643	53	192.168.2.3	8.8.8.8
May 12, 2021 15:59:22.458745003 CEST	53	58643	8.8.8.8	192.168.2.3
May 12, 2021 15:59:23.316637039 CEST	60985	53	192.168.2.3	8.8.8.8
May 12, 2021 15:59:23.366002083 CEST	53	60985	8.8.8.8	192.168.2.3
May 12, 2021 15:59:24.231729031 CEST	50200	53	192.168.2.3	8.8.8.8
May 12, 2021 15:59:24.280591011 CEST	53	50200	8.8.8.8	192.168.2.3
May 12, 2021 15:59:25.494689941 CEST	51281	53	192.168.2.3	8.8.8.8
May 12, 2021 15:59:25.545285940 CEST	53	51281	8.8.8.8	192.168.2.3
May 12, 2021 15:59:26.535496950 CEST	49199	53	192.168.2.3	8.8.8.8
May 12, 2021 15:59:26.584317923 CEST	53	49199	8.8.8.8	192.168.2.3
May 12, 2021 15:59:27.252641916 CEST	50620	53	192.168.2.3	8.8.8.8
May 12, 2021 15:59:27.305210114 CEST	53	50620	8.8.8.8	192.168.2.3
May 12, 2021 15:59:27.571415901 CEST	64938	53	192.168.2.3	8.8.8.8
May 12, 2021 15:59:27.621311903 CEST	53	64938	8.8.8.8	192.168.2.3
May 12, 2021 15:59:27.779794931 CEST	60152	53	192.168.2.3	8.8.8.8
May 12, 2021 15:59:27.847409964 CEST	53	60152	8.8.8.8	192.168.2.3
May 12, 2021 15:59:27.858779907 CEST	57544	53	192.168.2.3	8.8.8.8
May 12, 2021 15:59:27.919125080 CEST	53	57544	8.8.8.8	192.168.2.3
May 12, 2021 15:59:28.483575106 CEST	55984	53	192.168.2.3	8.8.8.8
May 12, 2021 15:59:28.535130978 CEST	53	55984	8.8.8.8	192.168.2.3
May 12, 2021 15:59:29.406898975 CEST	64185	53	192.168.2.3	8.8.8.8
May 12, 2021 15:59:29.464296103 CEST	53	64185	8.8.8.8	192.168.2.3
May 12, 2021 15:59:30.667299032 CEST	65110	53	192.168.2.3	8.8.8.8
May 12, 2021 15:59:30.716304064 CEST	53	65110	8.8.8.8	192.168.2.3
May 12, 2021 15:59:31.618115902 CEST	58361	53	192.168.2.3	8.8.8.8
May 12, 2021 15:59:31.669806004 CEST	53	58361	8.8.8.8	192.168.2.3
May 12, 2021 15:59:33.399279118 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 15:59:33.448721886 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 15:59:52.801012039 CEST	60831	53	192.168.2.3	8.8.8.8
May 12, 2021 15:59:52.863289118 CEST	53	60831	8.8.8.8	192.168.2.3
May 12, 2021 16:01:11.902173042 CEST	60100	53	192.168.2.3	8.8.8.8
May 12, 2021 16:01:12.065808058 CEST	53	60100	8.8.8.8	192.168.2.3
May 12, 2021 16:01:32.535322905 CEST	53195	53	192.168.2.3	8.8.8.8
May 12, 2021 16:01:32.609401941 CEST	53	53195	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 16:01:11.902173042 CEST	192.168.2.3	8.8.8.8	0x5e50	Standard query (0)	www.iqomw.com	A (IP address)	IN (0x0001)
May 12, 2021 16:01:32.535322905 CEST	192.168.2.3	8.8.8.8	0xd4d5	Standard query (0)	www.elzooz.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 16:01:12.065808058 CEST	8.8.8.8	192.168.2.3	0x5e50	No error (0)	www.iqomw.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 16:01:12.065808058 CEST	8.8.8.8	192.168.2.3	0x5e50	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.16.197.4	A (IP address)	IN (0x0001)
May 12, 2021 16:01:12.065808058 CEST	8.8.8.8	192.168.2.3	0x5e50	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		13.59.53.244	A (IP address)	IN (0x0001)
May 12, 2021 16:01:12.065808058 CEST	8.8.8.8	192.168.2.3	0x5e50	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		52.15.160.167	A (IP address)	IN (0x0001)
May 12, 2021 16:01:32.609401941 CEST	8.8.8.8	192.168.2.3	0xd4d5	Name error (3)	www.elzooz.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.iqomw.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49707	3.16.197.4	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 16:01:12.217029095 CEST	530	OUT	GET /crdi/?qZ_l=s5ZBPuXj17fhOA1bx0aCq9ENe7PeNxUER8tsGnybxkKx7jlbiox1QoAzGi7ZgPeOdZ4f&y0Dluf=g480w6JH HTTP/1.1 Host: www.iqomw.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 16:01:12.354059935 CEST	530	IN	HTTP/1.1 404 Not Found Date: Wed, 12 May 2021 14:01:12 GMT Content-Type: text/html Content-Length: 153 Connection: close Server: nginx/1.16.1 Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 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 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 36 2e 31 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx/1.16.1 </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

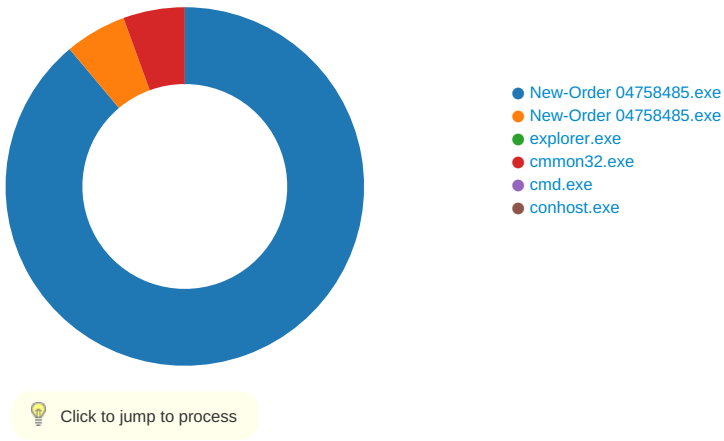
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xE8
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xE8
GetMessageW	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xE8
GetMessageA	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xE8

Statistics

Behavior



System Behavior

Analysis Process: New-Order 04758485.exe PID: 5632 Parent PID: 5576

General

Start time:	15:59:24
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\New-Order 04758485.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\New-Order 04758485.exe'
Imagebase:	0x540000
File size:	1693696 bytes
MD5 hash:	ED4361A7909FC65A189B4ADAAC292991
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.307323456.0000000003AFA000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.307323456.0000000003AFA000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.307323456.0000000003AFA000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.307802950.0000000003BDE000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.307802950.0000000003BDE000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.307802950.0000000003BDE000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.307176477.0000000003A97000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.307176477.0000000003A97000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.307176477.0000000003A97000.00000004.00000001.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	6DEDCF06	unknown
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	6DEDCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New-Order 04758485.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1EC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\New-Order 04758485.exe.log	unknown	1619	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 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 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 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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_v4.0.3	success or wait	1	6E1EC907	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	6DEB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEBCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD21B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD21B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: New-Order 04758485.exe PID: 5884 Parent PID: 5632

General

Start time:	16:00:06

Start date:	12/05/2021
Path:	C:\Users\user\Desktop\New-Order 04758485.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\New-Order 04758485.exe
Imagebase:	0xa70000
File size:	1693696 bytes
MD5 hash:	ED4361A7909FC65A189B4ADAAC292991
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: 0000000A.00000002.342372255.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.342372255.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.342372255.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.342960367.00000000011A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.342960367.00000000011A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.342960367.00000000011A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.342980918.00000000011D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.342980918.00000000011D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.342980918.00000000011D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41A027	NtReadFile

Analysis Process: explorer.exe PID: 3388 Parent PID: 5884

General

Start time:	16:00:11
Start date:	12/05/2021
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: 2540 Parent PID: 3388

General

Start time:	16:00:26
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\cmmon32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmmon32.exe
Imagebase:	0xe60000
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: 0000000C.00000002.474310455.0000000004920000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.474310455.0000000004920000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.474310455.0000000004920000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.474480183.0000000004950000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.474480183.0000000004950000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.474480183.0000000004950000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.472057276.0000000000C60000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.472057276.0000000000C60000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.472057276.0000000000C60000.00000040.00000001.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	C7A027	NtReadFile

Analysis Process: cmd.exe PID: 4936 Parent PID: 2540

General

Start time:	16:00:29
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\New-Order 04758485.exe'
Imagebase:	0xb90000
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: 5400 Parent PID: 4936

General

Start time:	16:00:30
Start date:	12/05/2021
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