ID: 338985
Sample Name: Po-covid19 2372#w2..exe
Cookbook: default.jbs
Time: 08:49:19
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

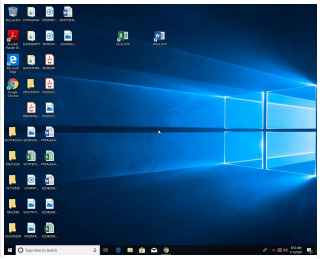
Analysis Report Po-covid19 2372#w2..exe

Overview

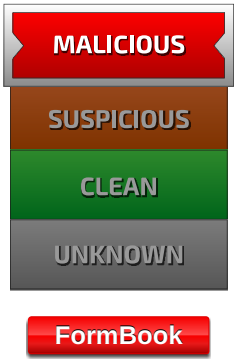
General Information

Sample Name:	Po-covid19 2372#w2..exe
Analysis ID:	338985
MD5:	bf53c9dc0d0f032..
SHA1:	eeba1ef352c0997.
SHA256:	a1558391914f423.
Tags:	COVID19 exe Formbook

Most interesting Screenshot:



Detection

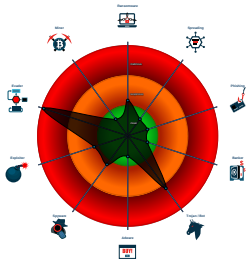


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e…
- System process connects to networ…
- Yara detected AntiVM_3
- Yara detected FormBook
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…

Classification



Startup

- **System is w10x64**
- Po-covid19 2372#w2..exe (PID: 5532 cmdline: 'C:\Users\user\Desktop\Po-covid19 2372#w2..exe' MD5: BF53C9DC0D0F032033C318ACEEF906C6)
  - Po-covid19 2372#w2..exe (PID: 4308 cmdline: {path} MD5: BF53C9DC0D0F032033C318ACEEF906C6)
  - Po-covid19 2372#w2..exe (PID: 5404 cmdline: {path} MD5: BF53C9DC0D0F032033C318ACEEF906C6)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msiexec.exe (PID: 6748 cmdline: C:\Windows\SysWOW64\msiexec.exe MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
        - cmd.exe (PID: 7092 cmdline: /c del 'C:\Users\user\Desktop\Po-covid19 2372#w2..exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 7100 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x8bc3",
    "KEY1_OFFSET 0x1d7db",
    "CONFIG SIZE : 0xd9",
    "CONFIG OFFSET 0x1d8dd",
    "URL SIZE : 28",
    "searching string pattern",
    "strings_offset 0x1c383",
    "searching hashes pattern",
    "-------------------------------------------------",
    "Decrypted Function Hashes",
    "-------------------------------------------------",
    "0xfd2db44c",
    "0xf43668a6",
    "0x980476e5",
    "0x35a6d50c",
    "0xf89290dc",
    "0x94261f57",
    "0x7d54c891",
    "0x47cb721",
    "0xf72d70b3",
    "0x9f715022",
    "0xbf0a5e41",
    "0x2902d074",
    "0xf653b199",
```

```
"0xc8c42cc6",
"0x2e1b7599",
"0x210d4d07",
"0x6d2a7921",
"0x8ea85a2f",
"0x207c50ff",
"0xb967410a",
"0x1eb17415",
"0xb46802f8",
"0x11da8518",
"0xf42ed5c",
"0x2885a3d3",
"0x445675fa",
"0x5c289b4c",
"0x40ede5aa",
"0xf24946a2",
"0x8559c3e2",
"0xb9d34d23",
"0xa14d0a19",
"0x2d07bbe2",
"0xbbd1d68c",
"0xb28c29d4",
"0x3911edeb",
"0xefad046d",
"0xa0605497",
"0xf5529cbf",
"0x5507576a",
"0xfa2467c8",
"0x5b6423bf",
"0xe22409b9",
"0xde1eba2",
"0xae847e2",
"0xa8cfcc9",
"0x26fc2c69",
"0x5d8a75ac",
"0x22eb3474",
"0x2b37c918",
"0x79402007",
"0x7544791c",
"0x641b2c94",
"0x1db04ecf",
"0xf5d02cd8",
"0xad0121d2",
"0x6206e716",
"0x5e4b9b9a",
"0xe4e2f5f4",
"0x54c93159",
"0x25ea79b",
"0x5bf29119",
"0xd6507db",
"0x32ffc9f8",
"0xe4cfab72",
"0x98db5380",
"0xce4cc542",
"0x3092a0a2",
"0x66053660",
"0x2607a133",
"0xfcd01541",
"0x80b41d4",
"0x4102ad8d",
"0x857bf6a6",
"0xd3ec6064",
"0x23145fc4",
"0xc026698f",
"0x8f5385d8",
"0x2430512b",
"0x3ebe9086",
"0x4c6fddb5",
"0x276db13e",
"0xe00f0a8e",
"0x85cf9404",
"0xb2248784",
"0xcdc7e023",
"0x11f5f50",
"0x1dd4bc1c",
"0x8235fce2",
"0x21b17672",
"0xbba64d93",
"0x2f0ee0d8",
"0x9cb95240",
"0x28c21e3f",
"0x9347ac57",
"0x9d9522dc",
"0x911bc70e",
"0x74443db9",
"0xf04c1aa9",
"0x6484bcb5",
"0x11fc2f72",
"0x2b44324f",
"0x9d70beea",
"0x59adf952",
```

```
"0x172ac7b4",
"0x5d4b4e66",
"0xed297eae",
"0xa88492a6",
"0xb21b057c",
"0x70f35767",
"0xb6f4d5a8",
"0x67cea859",
"0xc1626bff",
"0xb4e1ae2",
"0x24a48dcf",
"0xe11da208",
"0x1c920818",
"0x65f4449c",
"0xc30bc050",
"0x3e86e1fb",
"0x9e01fc32",
"0x216500c2",
"0x48e207c9",
"0x2decf13e",
"0x19996921",
"0xb7da3dd7",
"0x47f39d2b",
"0x6777e2de",
"0xd980e37f",
"0x963fea3b",
"0xacddb7ea",
"0x110aec35",
"0x647331f3",
"0x2e381da4",
"0x50f66474",
"0xec16e0c0",
"0xf9d81a42",
"0xd6c6f9db",
"0xef3df91",
"0x60e0e203",
"0x7c81caaf",
"0x71c2ec76",
"0x25e431cc",
"0x106f568f",
"0x6a60c8a9",
"0xb758aab3",
"0x3b34de90",
"0x700420f5",
"0xee359a7e",
"0xd1d808a",
"0x47ba47a5",
"0xff959c4c",
"0x5d30a87d",
"0xaa95a900",
"0x80b19064",
"0x9c5a481a",
"0x1dd252d",
"0xdb3055fc",
"0xe0cf8bf1",
"0x3a48eabc",
"0xf0472f97",
"0x4a6323de",
"0x4260edca",
"0x53f7fb4f",
"0x3d2e9c99",
"0xf6879235",
"0xe6723cac",
"0xe184dfaa",
"0xe99ffaa0",
"0xf6aebe25",
"0xefadf9a5",
"0x215de938",
"0x757906aa",
"0x84f8d766",
"0xb6494f65",
"0x13a75318",
"0x5bde5587",
"0xe9eba2a4",
"0x6b8a0df3",
"0x9c02f250",
"0xe52a2a2e",
"0xdb96173c",
"0x3c0f2fc",
"0xd45e157c",
"0x4edd1210",
"0x2b127ce0",
"0xadc887b6",
"0xf45a1c52",
"0xc84869d7",
"0x36dc1f04",
"0x50c2a508",
"0x3e88e8bf",
"0x4b6374a6",
"0x72a93198",
"0x85426977",
```

```
    "0xea193e11",
    "0xea653007",
    "0xe297c9c",
    "0x65399e87",
    "0x23609e75",
    "0xb92e8a5a",
    "0xabc89476",
    "0xd989572f",
    "0x4536ab86",
    "0x3476afc1",
    "0xaf24a63b",
    "0x393b9ac8",
    "0x414a3c70",
    "0x487e77f4",
    "0xbee1bdf6",
    "0xc30c49a6",
    "0xcb591d7f",
    "0x5c4ee455",
    "0x7c81c71d",
    "0x11c6f95e",
    "----------------------------------------------",
    "Decrypted Strings",
    "----------------------------------------------",
    "USERNAME",
    "LOCALAPPDATA",
    "USERPROFILE",
    "APPDATA",
    "TEMP",
    "ProgramFiles",
    "CommonProgramFiles",
    "ALLUSERSPROFILE",
    "/c copy \"",
    "/c del \"",
    "\\Run",
    "\\Policies",
    "\\Explorer",
    "\\Registry\\User",
    "\\Registry\\Machine",
    "\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion",
    "Office\\15.0\\Outlook\\Profiles\\Outlook\\",
    " NT\\CurrentVersion\\Windows Messaging Subsystem\\Profiles\\Outlook\\",
    "\\SOFTWARE\\Mozilla\\Mozilla ",
    "\\Mozilla",
    "Username: ",
    "Password: ",
    "formSubmitURL",
    "usernameField",
    "encryptedUsername",
    "encryptedPassword",
    "\\logins.json",
    "\\signons.sqlite",
    "\\Microsoft\\Vault\\",
    "SELECT encryptedUsername, encryptedPassword, formSubmitURL FROM moz_logins",
    "\\Google\\Chrome\\User Data\\Default\\Login Data",
    "SELECT origin_url, username_value, password_value FROM logins",
    ".exe",
    ".com",
    ".scr",
    ".pif",
    ".cmd",
    ".bat",
    "ms",
    "win",
    "gdi",
    "mfc",
    "vga",
    "igfx",
    "user",
    "help",
    "config",
    "update",
    "regsvc",
    "chkdsk",
    "systray",
    "audiodg",
    "certmgr",
    "autochk",
    "taskhost",
    "colorcpl",
    "services",
    "IconCache",
    "ThumbCache",
    "Cookies",
    "SeDebugPrivilege",
    "SeShutdownPrivilege",
    "\\BaseNamedObjects",
    "config.php",
    "POST ",
    " HTTP/1.1",
    "",
    "Host: ",
```

```
"",
"Connection: close",
"",
"Content-Length: ",
"",
"Cache-Control: no-cache",
"",
"Origin: http://",
"",
"User-Agent: Mozilla Firefox/4.0",
"",
"Content-Type: application/x-www-form-urlencoded",
"",
"Accept: */*",
"",
"Referer: http://",
"",
"Accept-Language: en-US",
"",
"Accept-Encoding: gzip, deflate",
"",
"dat=",
"f-start",
"kimberlyrutledge.com",
"auctus.agency",
"johnemotions.com",
"guilt-brilliant.com",
"wxshangdian.com",
"theolivetreeonline.com",
"stellarfranchisebrands.com",
"every1no1.com",
"hoangthanhgroup.com",
"psm-gen.com",
"kingdomwow.com",
"digitalksr.com",
"karynpolitoforlg.com",
"youthdaycalgary.com",
"libertyhandymanservicesllc.com",
"breatheohio.com",
"allenleather.com",
"transformafter50.info",
"hnhsylsb.com",
"hmtradebd.com",
"besrhodislandhomes.com",
"zuwozo.com",
"southernhighlandsnails.com",
"kaaxg.com",
"bauer-cobolt.com",
"steelyourselfshop.net",
"linksoflondoncharmscheap.com",
"groundwork-pt.com",
"beautifulangelicskin.com",
"aduhelmfinancialsupport.com",
"xn--carpinteratarifa-hsb.com",
"thekingink.net",
"ocotegrill.com",
"gilbertdodge.com",
"insuranceinquirer.com",
"withagentcy.com",
"deeparchivesvpn.com",
"blamekd.com",
"acsdealta.xyz",
"dsxcj.com",
"kimonoshihan.com",
"bosquefamily.com",
"5587sk.com",
"integrative.life",
"unitedjournal.info",
"lynxdeck.com",
"onlyfanyou.com",
"aminomedicalscience.com",
"rachenstern-technik.com",
"thejewelrybox.net",
"stopcolleges.com",
"thesaltlifestyle.com",
"tappesupportservices.com",
"andrewgreenhomes.com",
"meidiansc.com",
"gobalexporter.com",
"rvpji571m.xyz",
"alwekalaaladabeya.com",
"scientificimaginetics.com",
"skaizenpharma.com",
"balloonpost.club",
"thefunnythingabout.com",
"premium-vitality.com",
"businesscalmcoaching.com",
"f-end",
"-------------------------------------------------",
"Decrypted CnC URL",
"-------------------------------------------------",
```

```
    "www.styrelseforum.com/p95n/\u0000"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.616475940.0000000000B40000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000E.00000002.616475940.0000000000B40000.00000040.00000001.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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b507:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c50a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000E.00000002.616475940.0000000000B40000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18429:$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:$sqlite3blob: 68 53 D8 7F 8C
00000003.00000002.297322370.0000000000FB0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000002.297322370.0000000000FB0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$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 • 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

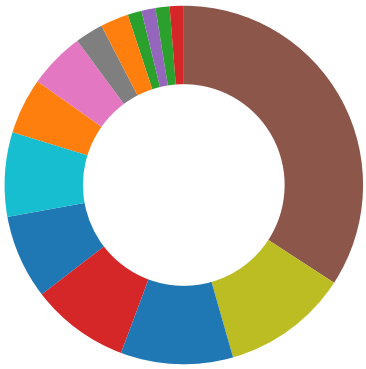
Source	Rule	Description	Author	Strings
3.2.Po-covid19 2372#w2..exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.Po-covid19 2372#w2..exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a707:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b70a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.Po-covid19 2372#w2..exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17629:$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
3.2.Po-covid19 2372#w2..exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
3.2.Po-covid19 2372#w2..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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b507:$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 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- 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

AV Detection:

Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Compliance:

Detected unpacking (overwrites its own PE header)

Networking:

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

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

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 AntiVM_3

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)

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:

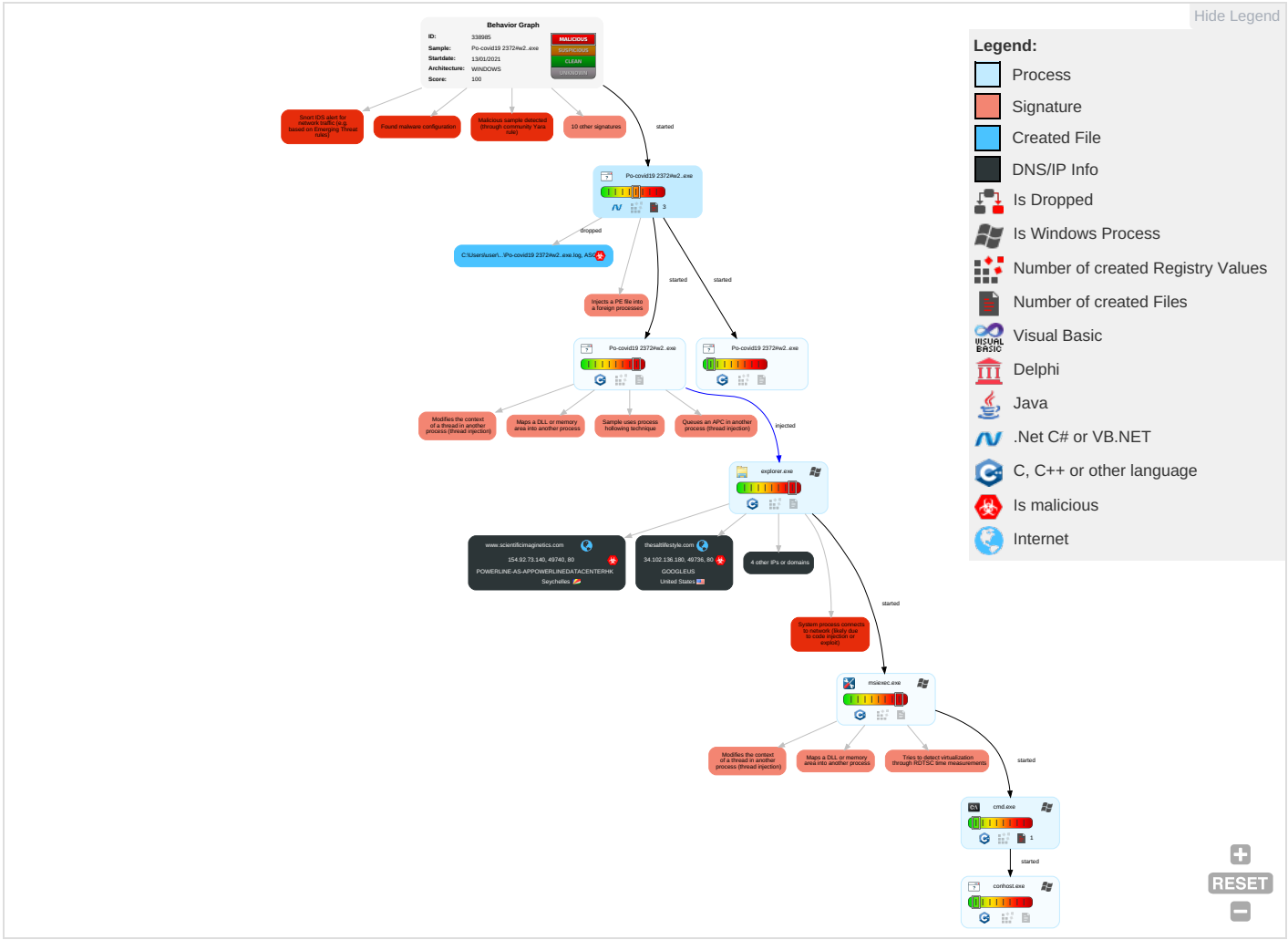
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	DLL Side-Loading 1	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop (Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Masquerading 1	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Disable or Modify Tools 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poir
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2 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)	DLL Side-Loading 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 Cellu Base Statio

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
Po-covid19 2372#w2..exe	27%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
Po-covid19 2372#w2..exe	100%	Avira	HEUR/AGEN.1120329	
Po-covid19 2372#w2..exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.Po-covid19 2372#w2..exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.0.Po-covid19 2372#w2..exe.9b0000.0.unpack	100%	Avira	HEUR/AGEN.1120329		Download File
0.0.Po-covid19 2372#w2..exe.70000.0.unpack	100%	Avira	HEUR/AGEN.1120329		Download File
0.2.Po-covid19 2372#w2..exe.70000.0.unpack	100%	Avira	HEUR/AGEN.1134873		Download File
3.2.Po-covid19 2372#w2..exe.9b0000.1.unpack	100%	Avira	HEUR/AGEN.1120329		Download File
2.2.Po-covid19 2372#w2..exe.130000.0.unpack	100%	Avira	HEUR/AGEN.1120329		Download File
2.0.Po-covid19 2372#w2..exe.130000.0.unpack	100%	Avira	HEUR/AGEN.1120329		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/jp/?	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/H	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htmpu	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://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.founder.com.cn/cn=	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://www.fontbureau.comnc./S	0%	Avira URL Cloud	safe	
http://www.thesaltlifestyle.com/p95n/?u6ihA=cjlpdRL8ZtfDvB1&oH5h=BBaWJPlPEO+nvtMqhmqrcRgDtKq1LKrnuc6I0tDI+4mn5icveD46W7DXUUudv5GhOCct	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalsF	0%	URL Reputation	safe	
http://www.fontbureau.comalsF	0%	URL Reputation	safe	
http://www.fontbureau.comalsF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-cz	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/ghtsl	0%	Avira URL Cloud	safe	
http://https://www.johnemotions.com/p95n/?oH5h=OkCbzDuuF1pG8/	0%	Avira URL Cloud	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.jiyu-kobo.co.jp/Y0e	0%	Avira URL Cloud	safe	
http://www.urwpp.de.	0%	Avira URL Cloud	safe	
http://www.fontbureau.com-	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/.	0%	Avira URL Cloud	safe	
http://www.fontbureau.com0	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdic	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
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://crl.;	0%	Avira URL Cloud	safe	
http://www.fontbureau.comessedZ	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF&	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://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	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://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/Z	0%	Avira URL Cloud	safe	
http://www.fontbureau.com=	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/~	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Z	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/S	0%	Avira URL Cloud	safe	
http://www.fontbureau.comgritoe	0%	Avira URL Cloud	safe	
http://www.fontbureau.comaA	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/H	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/H	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/H	0%	URL Reputation	safe	
http://www.fontbureau.comzana	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/A	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/?	0%	Avira URL Cloud	safe	
http://www.urwpp.de3z	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdl	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.fontbureau.comeH	0%	Avira URL Cloud	safe	
http://www.urwpp.deXz	0%	Avira URL Cloud	safe	
http://www.monotype.7	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/w	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.scientificimaginetics.com	154.92.73.140	true	true		unknown
thesaltlifestyle.com	34.102.136.180	true	true		unknown
www.aduhelmfinancialsupport.com	165.160.13.20	true	false		high
www.johnemotions.com	104.24.109.70	true	true	• 0%, Virustotal, Browse	unknown
www.steelyourselfshop.net	unknown	unknown	true		unknown
www.thesaltlifestyle.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.aduhelmfinancialsupport.com/p95n/?oH5h=yIt3vHGcFY19i9LszRbGqv8br4EBNSz7kQseU3pL44UQdgKo/VZu2mbLhFyK51ONzUns&u6ihA=cjlpdRL8ZtfDvB1	false		high
http://www.thesaltlifestyle.com/p95n/?u6ihA=cjlpdRL8ZtfDvB1&oH5h=BBaWJPlPEO+nvtMqhmqrcRgDtKq1LKrnuc6I0tDI+4mn5icveD46W7DXUUudv5GhOCct	true	• Avira URL Cloud: safe	unknown
http://www.johnemotions.com/p95n/?oH5h=OkCbzDuuF1pG8/+FjCqUEbhCI/Ef9I/I5jzkOiKX/zkELnGsjuBbK/8sh3SawKW3Kze/&u6ihA=cjlpdRL8ZtfDvB1	true	• Avira URL Cloud: safe	unknown
http://www.scientificimaginetics.com/p95n/?u6ihA=cjlpdRL8ZtfDvB1&oH5h=gRhj5HMuZvR/Ec7o8oi+HxLziNFcY38IPUSKESyExHr5bx7zEB/jrV73UqEK091YdqI8	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/?	Po-covid19 2372#w2..exe, 00000000.00000003.223340232.000000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	Po-covid19 2372#w2..exe, 00000000.00000002.262331435.000000008B22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.277115115.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	Po-covid19 2372#w2..exe, 00000000.00000002.262331435.000000008B22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.277115115.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Po-covid19 2372#w2..exe, 00000000.00000002.262331435.000000008B22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.277115115.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Po-covid19 2372#w2..exe, 00000000.00000002.262331435.000000008B22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.277115115.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/H	Po-covid19 2372#w2..exe, 00000000.00000003.223340232.000000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htmpu	Po-covid19 2372#w2..exe, 00000000.00000003.229096001.000000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	explorer.exe, 00000004.00000000.277115115.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000004.00000000.277115115.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comessed	Po-covid19 2372#w2..exe, 00000000.00000003.226385689.000000000791B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn=	Po-covid19 2372#w2..exe, 00000000.00000003.221689950.000000007923000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	Po-covid19 2372#w2..exe, 00000000.00000002.262331435.000000008B22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.277115115.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

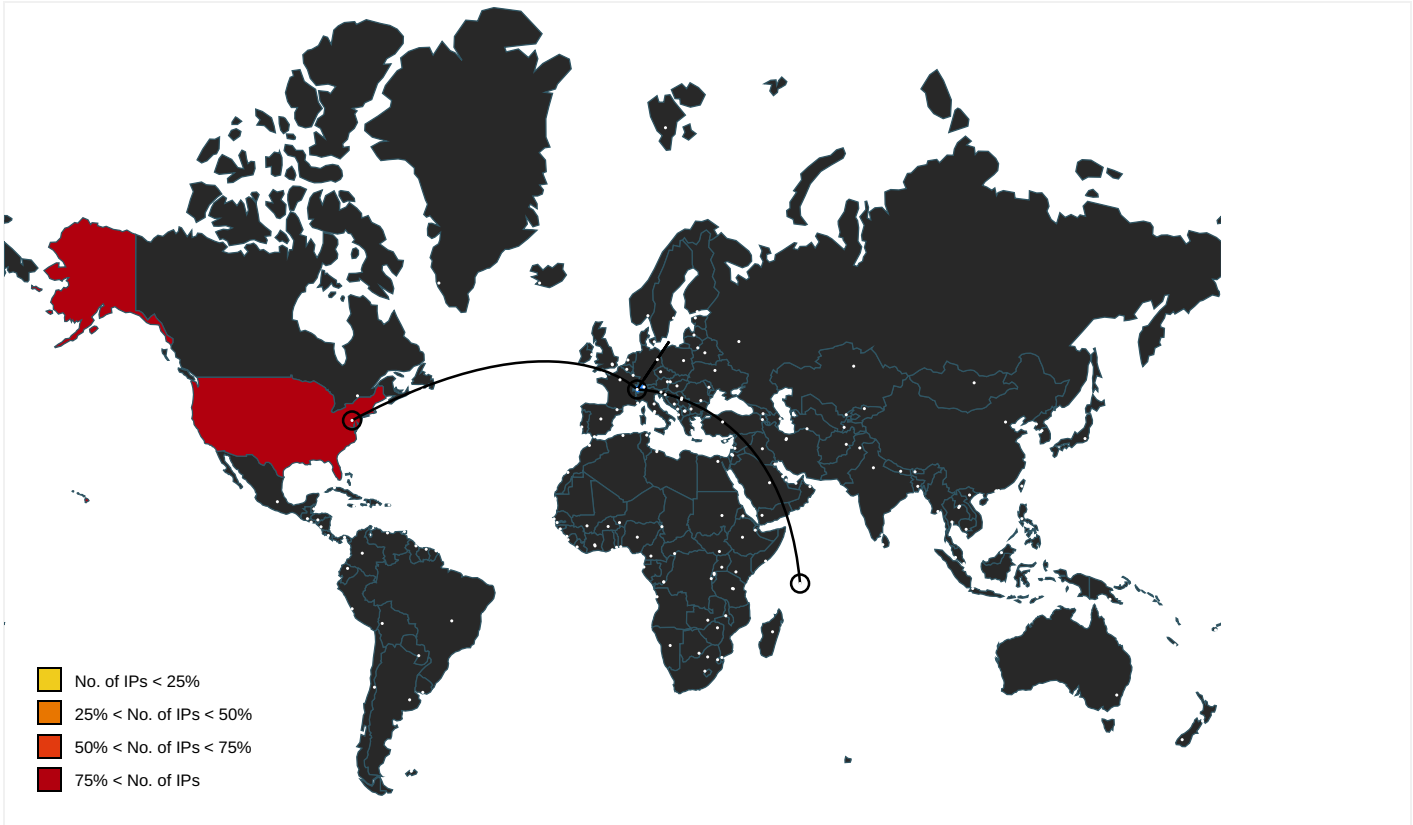
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comnc./S	Po-covid19 2372#w2..exe, 00000000.00000003.225055826.00000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comalsF	Po-covid19 2372#w2..exe, 00000000.00000003.227873217.00000000791B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/-cz	Po-covid19 2372#w2..exe, 00000000.00000003.223056311.00000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/ghtsl	Po-covid19 2372#w2..exe, 00000000.00000003.222591223.00000000007916000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.johnemotions.com/p95n/?oH5h=OkCbzDuuF1pG8/	msiexec.exe, 0000000E.00000002.622832165.000000000501F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	Po-covid19 2372#w2..exe, 00000000.00000002.262331435.0000000008B22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.277115115.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Po-covid19 2372#w2..exe, 00000000.00000002.262331435.0000000008B22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.277115115.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Po-covid19 2372#w2..exe, 00000000.00000002.262331435.0000000008B22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.277115115.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Po-covid19 2372#w2..exe, 00000000.00000002.262331435.0000000008B22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.277115115.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Po-covid19 2372#w2..exe, 00000000.00000002.262331435.0000000008B22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.277115115.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0e	Po-covid19 2372#w2..exe, 00000000.00000003.222591223.00000000007916000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.de.	Po-covid19 2372#w2..exe, 00000000.00000003.227697228.00000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com-	Po-covid19 2372#w2..exe, 00000000.00000003.226795444.00000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/.	Po-covid19 2372#w2..exe, 00000000.00000003.222363668.00000000007913000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com0	Po-covid19 2372#w2..exe, 00000000.00000003.227873217.00000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comdic	Po-covid19 2372#w2..exe, 00000000.00000003.226140808.00000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/	Po-covid19 2372#w2..exe, 00000000.00000003.225390108.00000000791B000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	Po-covid19 2372#w2..exe, 00000000.00000002.262331435.0000000008B22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.277115115.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.;	explorer.exe, 00000004.00000000.281618251.000000000F5C4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.comessedZ	Po-covid19 2372#w2..exe, 00000000.00000003.225516592.00000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comF&	Po-covid19 2372#w2..exe, 00000000.00000003.226385689.00000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	Po-covid19 2372#w2..exe, 00000000.00000002.262331435.0000000008B22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.277115115.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	Po-covid19 2372#w2..exe, 00000000.00000002.262331435.0000000008B22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.277115115.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Po-covid19 2372#w2..exe, 00000000.00000002.262331435.0000000008B22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.277115115.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.de	Po-covid19 2372#w2..exe, 00000000.00000003.225055826.0000000000791B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Po-covid19 2372#w2..exe, 00000000.00000002.262331435.0000000008B22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.277115115.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	Po-covid19 2372#w2..exe, 00000000.00000003.223340232.0000000000791B000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.277115115.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com.TTF	Po-covid19 2372#w2..exe, 00000000.00000003.227104715.0000000000791B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/Z	Po-covid19 2372#w2..exe, 00000000.00000003.223056311.0000000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com=	Po-covid19 2372#w2..exe, 00000000.00000003.226385689.0000000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/jp/~	Po-covid19 2372#w2..exe, 00000000.00000003.222591223.0000000007916000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Z	Po-covid19 2372#w2..exe, 00000000.00000003.222591223.0000000007916000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Po-covid19 2372#w2..exe, 00000000.00000002.262331435.0000000008B22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.277115115.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	Po-covid19 2372#w2..exe, 00000000.00000003.225055826.0000000000791B000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.277115115.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.galapagosdesign.com/	Po-covid19 2372#w2..exe, 00000000.00000003.229096001.0000000000791B000.00000004.00000001.sdmp, Po-covid19 2372#w2..exe, 00000000.00000003.228852233.000000000791B000.00000004.00000001.sdmp, Po-covid19 2372#w2..exe, 00000000.00000003.228815722.0000000007942000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/S	Po-covid19 2372#w2..exe, 00000000.00000003.223056311.0000000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comgritoe	Po-covid19 2372#w2..exe, 00000000.00000003.225158941.0000000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comaA	Po-covid19 2372#w2..exe, 00000000.00000003.225516592.0000000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/H	Po-covid19 2372#w2..exe, 00000000.00000003.222719848.0000000000791A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comzana	Po-covid19 2372#w2..exe, 00000000.00000003.226385689.00000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/A	Po-covid19 2372#w2..exe, 00000000.00000003.223056311.00000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	Po-covid19 2372#w2..exe, 00000000.00000003.222591223.00000000007916000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comd	Po-covid19 2372#w2..exe, 00000000.00000003.226385689.00000000791B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/?	Po-covid19 2372#w2..exe, 00000000.00000003.222591223.00000000007916000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.de3z	Po-covid19 2372#w2..exe, 00000000.00000003.224891432.00000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comdl	Po-covid19 2372#w2..exe, 00000000.00000003.227873217.00000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	Po-covid19 2372#w2..exe, 00000000.00000002.262331435.0000000008B22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.277115115.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comeH	Po-covid19 2372#w2..exe, 00000000.00000003.227873217.00000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deXz	Po-covid19 2372#w2..exe, 00000000.00000003.225055826.00000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.monotype.7	Po-covid19 2372#w2..exe, 00000000.00000003.225451084.00000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designers/cabarga.htmlN	Po-covid19 2372#w2..exe, 00000000.00000002.262331435.0000000008B22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.277115115.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/w	Po-covid19 2372#w2..exe, 00000000.00000003.223056311.00000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	Po-covid19 2372#w2..exe, 00000000.00000002.262331435.0000000008B22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.277115115.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Po-covid19 2372#w2..exe, 00000000.00000003.226091255.00000000791B000.00000004.00000001.sdmp, Po-covid19 2372#w2..exe, 00000000.00000002.262331435.0000000008B22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.277115115.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comoitu	Po-covid19 2372#w2..exe, 00000000.00000003.227873217.00000000791B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	Po-covid19 2372#w2..exe, 00000000.00000003.226977608.00000000007942000.00000004.00000001.sdmp, Po-covid19 2372#w2..exe, 00000000.00000003.226763972.00000000007942000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comlic0	Po-covid19 2372#w2..exe, 00000000.00000003.226795444.00000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deo	Po-covid19 2372#w2..exe, 00000000.00000003.225055826.00000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comdZ	Po-covid19 2372#w2..exe, 00000000.00000003.226385689.00000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	Po-covid19 2372#w2..exe, 00000000.00000003.225055826.00000000791B000.00000004.00000001.sdmp, Po-covid19 2372#w2..exe, 00000000.00000003.222591223.0000000007916000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.277115115.0000000008B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/-	Po-covid19 2372#w2..exe, 00000000.00000003.223340232.00000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	Po-covid19 2372#w2..exe, 00000000.00000002.262331435.0000000008B22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.277115115.0000000008B40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/	Po-covid19 2372#w2..exe, 00000000.00000003.225055826.00000000791B000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comow	Po-covid19 2372#w2..exe, 00000000.00000003.226385689.00000000791B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn$	Po-covid19 2372#w2..exe, 00000000.00000003.221689950.0000000007923000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
154.92.73.140	unknown	Seychelles		132839	POWERLINE-AS-APPOWERLINEDATACENTERHK	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
165.160.13.20	unknown	United States		19574	CSCUS	false
104.24.109.70	unknown	United States		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	338985
Start date:	13.01.2021
Start time:	08:49:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Po-covid19 2372#w2..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:	36
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@9/1@6/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 17.4% (good quality ratio 14.6%) • Quality average: 67.6% • Quality standard deviation: 35.6%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 104.43.193.48, 52.255.188.83, 92.122.144.200, 51.11.168.160, 40.88.32.150, 92.122.213.194, 92.122.213.247, 8.248.131.254, 8.253.207.120, 67.26.83.254, 8.253.95.120, 8.248.137.254, 20.54.26.129, 168.61.161.212, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:50:23	API Interceptor	1x Sleep call for process: Po-covid19 2372#w2..exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
34.102.136.180	FtLroeD5Kmr6rNC.exe	Get hash	malicious	Browse	• www.abilitiesin.com/umSa/?8p=z9MTiPW3cvjSA5QkES0lRL7QE5QWzpSIb/5mf6QApKD6hYKwb/M4i12nx+gX2coGSm9PIjo5qw==&o2=jL30vpcXe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	6blnUJRr4yKrjCS.exe	Get hash	malicious	Browse	• www.vettedwealthmanagement.com/umSa/?ET8T=brJeVU7eljMQcn5t6nrZLyoDpHpFr+iqwzUSRB88e+cRILPvJ2TiW12sA30gV7y33iXX&URfl=00DdGJE8CBEXFLip
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• www.basalmeals.com/h3qo/?CR=nh/gKqoyV5HeFjYxMy0eFbMJOpM49Sz3DGf/FH2Dw3liEqigPonoEfAZFGiauGMw1oau&RX=dnC44rW8qdHLY2q
	5DY3NrVgpI.exe	Get hash	malicious	Browse	• www.schustermananinterests.com/de92/?FdC4E2D=otFI+gArfm9oxno+NIFHPe8CZ87dio0DjOpD7CEQ1ohXI6jwcMVL1BNDFt16zf60LSstTEfOYg==&AjR=9r4L1
	xrxSVsbRli.exe	Get hash	malicious	Browse	• www.luxpropertyandassociates.com/nki/?yrsdQvAx=9rwO08mLgykW/+F5WoH4KAy1ieMCsMl+05AKyLP7HaXoaQuR30wAwJPKQnvqcJUpdIyD&D8h8=kHux
	3S1VPrT4IK.exe	Get hash	malicious	Browse	• www.qiemfsolutions.com/xle/?D8bDL=df7alruH/sVOZEWxdb4cimNlzghqgII+JQbYN3M53vXLFmJTlVjRvjRu86vT99I8VeyiFG/dAw==&nbph=uzu87Xq
	AOA4sx8Z7l.exe	Get hash	malicious	Browse	• www.eventsdonevirtually.com/c8so/?Wx=JxEHfAEgu9b4xQJDcyjTWSaEjlpoxhWg+fCl4c24OKbRsAQRgKKiPuXHFwp0UmB835cw&vB=lhr0E

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	g2fUeYQ7Rh.exe	Get hash	malicious	Browse	• www.multipleofferonline.com/nki/?-Z1l=5yWKC4X4OOjUlUftTYCRYdpq8Xl+R2ST+EfenRWsFQpL7Lmr0RV0+cHmGR5gosgcZWiS+YlJJw==&5ju=UlSpo
	pHUWiFd56t.exe	Get hash	malicious	Browse	• www.brainandbodystrengthcoach.com/csv8/?Rxl=4rzgp1jZc7l8Whg0IztLQnvubqNqMY/2oz5HEUeZ+SGIDqCjyjtIs6qqwzFhp9I+dVCC&LJB=GbtlyLR0j
	invoice.xlsx	Get hash	malicious	Browse	• www.cleverwares.com/c8so/?AFNDR=7n20cVCpbL7dqxQ&BBW=P253+QYRdhKTDdzjq4pa7Wp7svBpTNddHFol+cUWSKGzAXl94gLhBIvIcI/Xp4fU197IMA==
	BSL 01321 PYT.xlsx	Get hash	malicious	Browse	• www.e-butchery.com/de92/?GBHXf2VP=SyfQvNxnxGuBvZveE7q+Mx8oTZDk0vYyrvtp8jcHqguCzq9Wh/Rqj3ZWA4DRZ6ODcHDiqw==&bB=oN64w0
	payment advice.xlsx	Get hash	malicious	Browse	• www.fatboidonuts.com/wgn/?QDKx=ismPDkb1kDsJJlmQEj1IWX8WHEdOBI7aPWpMJ4Az70/HitJ3Qnb/ojRR8i7WZLNLjqtDug==&MDHl9T=mps01jexw
	Arrival notice.xlsx	Get hash	malicious	Browse	• www.george-beauty.com/oean/?pJEtdJ=YYiBnx+uTbiyOiWOsIleXMl+TWVBeMM+hRG2hzgR9H7uS/Z2u5QgYOS3OsKMSH1P3GhSdw==&pL08=Grxte8Fh1bipd8g

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ.xlsx	Get hash	malicious	Browse	• www.experiencemoretogether.com/aky/?L2Jx=PJExAl&ObUhgbrX=TwjU4bk/hK/Rz/irfwftDMSiQA9z9Xtr+ITmJXkGe82JMHXMiJ/i+qjd6uOQ0U6KfPvIfw==
	13012021.exe	Get hash	malicious	Browse	• www.whatilikeabouttoday.com/rbg/?Ezr0p8=arITf878KNHP92&rZvXUD=A6nTsYtjbxvih6vkmaX1Jrl6YwOaLYk0AAMk9b3gNlyy1aX90h7Cg1+rLkFaTXBkKYm6
	LOI.exe	Get hash	malicious	Browse	• www.burgersandbarley.com/nhk9/?9r4P2=izkbuIM4pS07nj/jSOe9cHFSdHik4vqQ2XAojvhb7pCHWVIPZ7goRwN7tqCoHPvvvKwVcKFBmg==&0rT=g0DpkZJPuF6Hb
	Listings.exe	Get hash	malicious	Browse	• www.uqabi.net/kta/
	quotation.exe	Get hash	malicious	Browse	• www.ugcfashion.com/x2ee/?iBZLH8e=gj00CanoOA/MIDSuzzd4wA+9Xgu8XrjDu3Jyqr0DAD/cDq+vlAKlZeTP8PFKHz8QASJL27BTBA==&_RA89r=ZL3D3PvXurq
	Doc_74657456348374.xlsx.exe	Get hash	malicious	Browse	• www.aaliyahchhabra.com/hpg3/?b8=omXuB1JLE2RxeysDSMNUzZRSUIahHxHrLG/5bHt0ZFUEfFlaWVdzHHrASVFC83QB2ak+xsl1fQ==&C0D=_DK4YF6
	Revise Order.exe	Get hash	malicious	Browse	• www.endpedophiles.com/ehxh/?Lh0l=ZTdpL2D0k&nVjxUJ=zzMqP3gr9AvtiM4KAG8kTXsRbsDP8AWJ/7zGMGcvxlaU9iwirqdQaCWQ+gUupaaEafR3
165.160.13.20	61Order 0516.exe	Get hash	malicious	Browse	• www.ostrum-am.com//ti/
	index[1].htm	Get hash	malicious	Browse	• www.replicarolexllc.com/favicon.ico

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	1(RFQ) - 14000102697.exe	Get hash	malicious	Browse	• www.allianzpartnershop.com/ma/?BtIL=TV7UHZzggVvSZQDAWvGTdcqQjAICBJyilGxCRJLxTLSDLGEYUsm0jkgD8/qj9CQ5FOV8&_jL0dX=6lR0Brc8LNMdo8GP

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CSCUS	microsoft.exe	Get hash	malicious	Browse	• 165.160.15.20
POWERLINE-AS-APPOWERLINEDATACENTERHK	5DY3NrVgpI.exe	Get hash	malicious	Browse	• 154.215.48.175
	3S1VPrT4IK.exe	Get hash	malicious	Browse	• 154.92.73.145
	6OUYcd3GIs.exe	Get hash	malicious	Browse	• 154.216.110.70
	Swift transferi pdf.exe	Get hash	malicious	Browse	• 156.242.159.206
	yaQjVEGNEb.exe	Get hash	malicious	Browse	• 154.93.103.186
	zz4osC4FRa.exe	Get hash	malicious	Browse	• 154.216.110.171
	btVnDhh5K7.exe	Get hash	malicious	Browse	• 154.201.243.172
	c6Rg7xug26.exe	Get hash	malicious	Browse	• 154.218.55.251
	PURCHASE ORDER-34002174.doc	Get hash	malicious	Browse	• 156.252.104.205
	PO 24000109490.xlsx	Get hash	malicious	Browse	• 154.216.110.70
	Pending PURCHASE ORDER - 47001516.pdf.exe	Get hash	malicious	Browse	• 154.213.237.41
	order FTH2004-005 .exe	Get hash	malicious	Browse	• 154.213.159.8
	http://https://bit.ly/3hDDoTm	Get hash	malicious	Browse	• 160.124.53.36
	Order (2021.01.06).exe	Get hash	malicious	Browse	• 107.151.72.246
	order FTH2004-005.exe	Get hash	malicious	Browse	• 154.213.159.8
	990109.exe	Get hash	malicious	Browse	• 154.218.215.218
	IRS Notice Letter.exe	Get hash	malicious	Browse	• 154.216.102.213
	scan_118637_pdf.exe	Get hash	malicious	Browse	• 154.209.36.118
	SecuriteInfo.com.Heur.16160.xls	Get hash	malicious	Browse	• 154.209.36.118
	TqWufCUvxV.exe	Get hash	malicious	Browse	• 154.218.55.251
GOOGLEUS	FtLroeD5Kmr6rNC.exe	Get hash	malicious	Browse	• 35.204.150.5
	6blnUJRr4yKrjCS.exe	Get hash	malicious	Browse	• 34.102.136.180
	Consignment Document PL&BL Draft.exe	Get hash	malicious	Browse	• 34.102.136.180
	5DY3NrVgpI.exe	Get hash	malicious	Browse	• 34.102.136.180
	xrxSVsbRli.exe	Get hash	malicious	Browse	• 34.102.136.180
	3S1VPrT4IK.exe	Get hash	malicious	Browse	• 34.102.136.180
	AOA4sx8Z7l.exe	Get hash	malicious	Browse	• 34.102.136.180
	81msxxUisn.exe	Get hash	malicious	Browse	• 216.239.36.21
	g2fUeYQ7Rh.exe	Get hash	malicious	Browse	• 34.102.136.180
	pHUWiFd56t.exe	Get hash	malicious	Browse	• 35.184.90.176
	invoice.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	BSL 01321 PYT.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	payment advice.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	Arrival notice.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	RFQ.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	5Q8WDPTQu3.jar	Get hash	malicious	Browse	• 108.177.119.139
	13012021.exe	Get hash	malicious	Browse	• 34.102.136.180
	1gEpBw4A95.exe	Get hash	malicious	Browse	• 216.239.32.21
	Covid19-Min-Saude-Comuinicado-STIBY-11-01-21-224.vbs	Get hash	malicious	Browse	• 108.177.119.128
	LOI.exe	Get hash	malicious	Browse	• 34.102.136.180

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	FtLroeD5Kmr6rNC.exe	Get hash	malicious	Browse	• 23.227.38.74
	6blnUJRr4yKrjCS.exe	Get hash	malicious	Browse	• 104.24.111.173
	3S1VPrT4IK.exe	Get hash	malicious	Browse	• 104.19.152.30
	cGLVytu1ps.exe	Get hash	malicious	Browse	• 23.227.38.74
	onYLLDPXswyCVZu.exe	Get hash	malicious	Browse	• 104.28.4.151
	AOA4sx8Z7l.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO-75013.exe	Get hash	malicious	Browse	• 104.28.4.151
	BSL 01321 PYT.xlsx	Get hash	malicious	Browse	• 66.235.200.145
	mssecsvc.exe	Get hash	malicious	Browse	• 104.17.244.81
	ZwFwevQtlv.exe	Get hash	malicious	Browse	• 172.67.188.154
	ssDV3d9O9o.exe	Get hash	malicious	Browse	• 172.67.188.154
	wjSwL3KItA.exe	Get hash	malicious	Browse	• 104.28.4.151
	Invoice-ID43739424297.vbs	Get hash	malicious	Browse	• 104.28.30.67
	Company Docs.exe	Get hash	malicious	Browse	• 104.23.98.190
	SecuriteInfo.com.Generic.mg.5a4b41327cabca49.exe	Get hash	malicious	Browse	• 104.28.5.151
	#U266b Audio_47720.wavv - - Copy.htm	Get hash	malicious	Browse	• 104.18.54.96
	PortionPac Chemical Corp..html	Get hash	malicious	Browse	• 104.16.19.94
	TD-10057.exe	Get hash	malicious	Browse	• 172.67.188.154
	NKP210102-NIT-SC2.exe	Get hash	malicious	Browse	• 172.67.188.154
	Listings.exe	Get hash	malicious	Browse	• 162.159.13 4.233

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Po-covid19 2372#w2..exe.log

Process:	C:\Users\user\Desktop\Po-covid19 2372#w2..exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
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..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.200648874318885
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Po-covid19 2372#w2..exe
File size:	1304576
MD5:	bf53c9dc0d0f032033c318aceef906c6
SHA1:	eeba1ef352c09979dfdfb4afdcdc5f41fe2a0119
SHA256:	a1558391914f4235dfdcdddcdf0de915a800541a4271feb4aff34af82b83a935
SHA512:	7db00f26f4c0e6e6865ff4561ace1d6af4c8804e8534b29d6b1977f48c1863b7fbbd766a360e9d400aad4070568d33247e832b07da69a482004f14eab7c61383
SSDEEP:	24576:SlSjKBb8prhPsxedJuxzPiGqi4y5GLLnr:SlS+BQhEAJuxjlqhnr
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...?^_.....0..b..... .....@.. .....`.....@.....

File Icon

Icon Hash:	d4d6d2d2d2ccc4d4

Static PE Info

General

Entrypoint:	0x5080fe
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:	0x5FFE5E3F [Wed Jan 13 02:43:11 2021 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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1080a4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x10a000	0x381a0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x144000	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	0x106104	0x106200	False	0.756649193789	data	7.44459929766	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x10a000	0x381a0	0x38200	False	0.308106556236	data	5.20096741512	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x144000	0xc	0x200	False	0.041015625	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x10a460	0x668	data		
RT_ICON	0x10aac8	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 2290649224, next used block 7403519		
RT_ICON	0x10adb0	0x1e8	data		
RT_ICON	0x10af98	0x128	GLS_BINARY_LSB_FIRST		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x10b0c0	0x6739	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x1117fc	0xea8	data		
RT_ICON	0x1126a4	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x112f4c	0x6c8	data		
RT_ICON	0x113614	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x113b7c	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x1243a4	0x94a8	data		
RT_ICON	0x12d84c	0x67e8	data		
RT_ICON	0x134034	0x5488	data		
RT_ICON	0x1394bc	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 254, next used block 2130706432		
RT_ICON	0x13d6e4	0x25a8	data		
RT_ICON	0x13fc8c	0x10a8	data		
RT_ICON	0x140d34	0x988	data		
RT_ICON	0x1416bc	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x141b24	0x102	data		
RT_VERSION	0x141c28	0x388	data		
RT_MANIFEST	0x141fb0	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

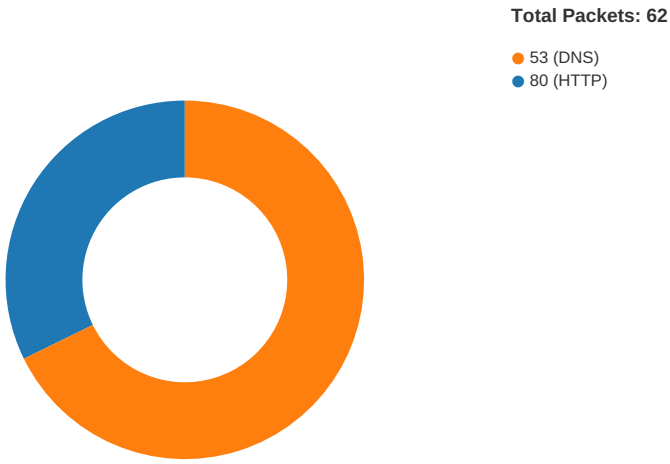
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Overwolf 2011 - 2020
Assembly Version	2.159.0.0
InternalName	fC.exe
FileVersion	2.159.0.0
CompanyName	Overwolf Ltd.
LegalTrademarks	
Comments	Overwolf Launcher
ProductName	OverwolfLauncher
ProductVersion	2.159.0.0
FileDescription	OverwolfLauncher
OriginalFilename	fC.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/21-08:51:26.238514	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49736	34.102.136.180	192.168.2.3
01/13/21-08:51:47.060177	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.3	165.160.13.20
01/13/21-08:51:47.060177	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.3	165.160.13.20
01/13/21-08:51:47.060177	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.3	165.160.13.20

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 08:51:26.058993101 CET	49736	80	192.168.2.3	34.102.136.180
Jan 13, 2021 08:51:26.099194050 CET	80	49736	34.102.136.180	192.168.2.3
Jan 13, 2021 08:51:26.099675894 CET	49736	80	192.168.2.3	34.102.136.180
Jan 13, 2021 08:51:26.099952936 CET	49736	80	192.168.2.3	34.102.136.180
Jan 13, 2021 08:51:26.140018940 CET	80	49736	34.102.136.180	192.168.2.3
Jan 13, 2021 08:51:26.238513947 CET	80	49736	34.102.136.180	192.168.2.3
Jan 13, 2021 08:51:26.238548994 CET	80	49736	34.102.136.180	192.168.2.3
Jan 13, 2021 08:51:26.238703012 CET	49736	80	192.168.2.3	34.102.136.180
Jan 13, 2021 08:51:26.238806009 CET	49736	80	192.168.2.3	34.102.136.180
Jan 13, 2021 08:51:26.278973103 CET	80	49736	34.102.136.180	192.168.2.3
Jan 13, 2021 08:51:46.925688982 CET	49737	80	192.168.2.3	165.160.13.20
Jan 13, 2021 08:51:47.059837103 CET	80	49737	165.160.13.20	192.168.2.3
Jan 13, 2021 08:51:47.060144901 CET	49737	80	192.168.2.3	165.160.13.20
Jan 13, 2021 08:51:47.060177088 CET	49737	80	192.168.2.3	165.160.13.20
Jan 13, 2021 08:51:47.194394112 CET	80	49737	165.160.13.20	192.168.2.3
Jan 13, 2021 08:51:47.204091072 CET	80	49737	165.160.13.20	192.168.2.3
Jan 13, 2021 08:51:47.204368114 CET	80	49737	165.160.13.20	192.168.2.3
Jan 13, 2021 08:51:47.204384089 CET	49737	80	192.168.2.3	165.160.13.20
Jan 13, 2021 08:51:47.204555988 CET	49737	80	192.168.2.3	165.160.13.20
Jan 13, 2021 08:51:47.338469982 CET	80	49737	165.160.13.20	192.168.2.3
Jan 13, 2021 08:52:09.772108078 CET	49740	80	192.168.2.3	154.92.73.140
Jan 13, 2021 08:52:10.069128990 CET	80	49740	154.92.73.140	192.168.2.3
Jan 13, 2021 08:52:10.069379091 CET	49740	80	192.168.2.3	154.92.73.140
Jan 13, 2021 08:52:10.069588900 CET	49740	80	192.168.2.3	154.92.73.140
Jan 13, 2021 08:52:10.366414070 CET	80	49740	154.92.73.140	192.168.2.3
Jan 13, 2021 08:52:10.370596886 CET	80	49740	154.92.73.140	192.168.2.3
Jan 13, 2021 08:52:10.370621920 CET	80	49740	154.92.73.140	192.168.2.3
Jan 13, 2021 08:52:10.371207952 CET	49740	80	192.168.2.3	154.92.73.140
Jan 13, 2021 08:52:10.371253967 CET	49740	80	192.168.2.3	154.92.73.140
Jan 13, 2021 08:52:10.668201923 CET	80	49740	154.92.73.140	192.168.2.3
Jan 13, 2021 08:52:29.575284004 CET	49741	80	192.168.2.3	104.24.109.70
Jan 13, 2021 08:52:29.626151085 CET	80	49741	104.24.109.70	192.168.2.3
Jan 13, 2021 08:52:29.626616001 CET	49741	80	192.168.2.3	104.24.109.70
Jan 13, 2021 08:52:29.626843929 CET	49741	80	192.168.2.3	104.24.109.70
Jan 13, 2021 08:52:29.677926064 CET	80	49741	104.24.109.70	192.168.2.3
Jan 13, 2021 08:52:29.685899973 CET	80	49741	104.24.109.70	192.168.2.3
Jan 13, 2021 08:52:29.686090946 CET	80	49741	104.24.109.70	192.168.2.3
Jan 13, 2021 08:52:29.686255932 CET	49741	80	192.168.2.3	104.24.109.70
Jan 13, 2021 08:52:29.686317921 CET	49741	80	192.168.2.3	104.24.109.70
Jan 13, 2021 08:52:29.736743927 CET	80	49741	104.24.109.70	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 08:50:11.885349989 CET	57544	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 08:50:11.933260918 CET	53	57544	8.8.8.8	192.168.2.3
Jan 13, 2021 08:50:16.002233028 CET	55984	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:50:16.053175926 CET	53	55984	8.8.8.8	192.168.2.3
Jan 13, 2021 08:50:17.099298000 CET	64185	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:50:18.100469112 CET	64185	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:50:18.937895060 CET	53	64185	8.8.8.8	192.168.2.3
Jan 13, 2021 08:50:19.940901995 CET	65110	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:50:19.988956928 CET	53	65110	8.8.8.8	192.168.2.3
Jan 13, 2021 08:50:20.795383930 CET	58361	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:50:20.843681097 CET	53	58361	8.8.8.8	192.168.2.3
Jan 13, 2021 08:50:21.789251089 CET	63492	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:50:21.840061903 CET	53	63492	8.8.8.8	192.168.2.3
Jan 13, 2021 08:50:36.541491985 CET	60831	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:50:36.604506969 CET	53	60831	8.8.8.8	192.168.2.3
Jan 13, 2021 08:50:38.455226898 CET	60100	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:50:38.506031990 CET	53	60100	8.8.8.8	192.168.2.3
Jan 13, 2021 08:50:41.168618917 CET	53195	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:50:41.216862917 CET	53	53195	8.8.8.8	192.168.2.3
Jan 13, 2021 08:50:51.317357063 CET	50141	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:50:51.368170023 CET	53	50141	8.8.8.8	192.168.2.3
Jan 13, 2021 08:50:51.476964951 CET	53023	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:50:51.534848928 CET	53	53023	8.8.8.8	192.168.2.3
Jan 13, 2021 08:50:52.558315039 CET	49563	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:50:52.606209040 CET	53	49563	8.8.8.8	192.168.2.3
Jan 13, 2021 08:50:53.523490906 CET	51352	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:50:53.571402073 CET	53	51352	8.8.8.8	192.168.2.3
Jan 13, 2021 08:50:54.668806076 CET	59349	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:50:54.725231886 CET	53	59349	8.8.8.8	192.168.2.3
Jan 13, 2021 08:50:55.702863932 CET	57084	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:50:55.750634909 CET	53	57084	8.8.8.8	192.168.2.3
Jan 13, 2021 08:50:56.748745918 CET	58823	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:50:56.796597004 CET	53	58823	8.8.8.8	192.168.2.3
Jan 13, 2021 08:50:57.905464888 CET	57568	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:50:57.953366041 CET	53	57568	8.8.8.8	192.168.2.3
Jan 13, 2021 08:50:57.972630978 CET	50540	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:50:58.024038076 CET	53	50540	8.8.8.8	192.168.2.3
Jan 13, 2021 08:51:12.496237993 CET	54366	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:51:12.568166018 CET	53	54366	8.8.8.8	192.168.2.3
Jan 13, 2021 08:51:16.039330959 CET	53034	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:51:16.087538004 CET	53	53034	8.8.8.8	192.168.2.3
Jan 13, 2021 08:51:16.768254995 CET	57762	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:51:16.825938940 CET	53	57762	8.8.8.8	192.168.2.3
Jan 13, 2021 08:51:16.839108944 CET	55435	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:51:16.886858940 CET	53	55435	8.8.8.8	192.168.2.3
Jan 13, 2021 08:51:17.842907906 CET	50713	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:51:17.893759966 CET	53	50713	8.8.8.8	192.168.2.3
Jan 13, 2021 08:51:25.981870890 CET	56132	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:51:26.053591967 CET	53	56132	8.8.8.8	192.168.2.3
Jan 13, 2021 08:51:46.852432966 CET	58987	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:51:46.924470901 CET	53	58987	8.8.8.8	192.168.2.3
Jan 13, 2021 08:51:48.151747942 CET	56579	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:51:48.199973106 CET	53	56579	8.8.8.8	192.168.2.3
Jan 13, 2021 08:51:50.372817993 CET	60633	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:51:50.428982973 CET	53	60633	8.8.8.8	192.168.2.3
Jan 13, 2021 08:52:09.404354095 CET	61292	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:52:09.769263029 CET	53	61292	8.8.8.8	192.168.2.3
Jan 13, 2021 08:52:29.502216101 CET	63619	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:52:29.573985100 CET	53	63619	8.8.8.8	192.168.2.3
Jan 13, 2021 08:52:57.307991028 CET	64938	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:52:57.364401102 CET	53	64938	8.8.8.8	192.168.2.3
Jan 13, 2021 08:52:58.448940039 CET	61946	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:52:58.508014917 CET	53	61946	8.8.8.8	192.168.2.3
Jan 13, 2021 08:52:59.604159117 CET	64910	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:52:59.660727978 CET	53	64910	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 08:53:00.640948057 CET	52123	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:53:00.691749096 CET	53	52123	8.8.8.8	192.168.2.3
Jan 13, 2021 08:53:01.215671062 CET	56130	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:53:01.274918079 CET	53	56130	8.8.8.8	192.168.2.3
Jan 13, 2021 08:53:02.101735115 CET	56338	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:53:02.157994032 CET	53	56338	8.8.8.8	192.168.2.3
Jan 13, 2021 08:53:03.029258966 CET	59420	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:53:03.077163935 CET	53	59420	8.8.8.8	192.168.2.3
Jan 13, 2021 08:53:04.407246113 CET	58784	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:53:04.463922977 CET	53	58784	8.8.8.8	192.168.2.3
Jan 13, 2021 08:53:05.615227938 CET	63978	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:53:05.663167000 CET	53	63978	8.8.8.8	192.168.2.3
Jan 13, 2021 08:53:06.348125935 CET	62938	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:53:06.446002960 CET	53	62938	8.8.8.8	192.168.2.3
Jan 13, 2021 08:53:12.572185993 CET	55708	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:53:13.559467077 CET	55708	53	192.168.2.3	8.8.8.8
Jan 13, 2021 08:53:13.636240959 CET	53	55708	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 08:51:25.981870890 CET	192.168.2.3	8.8.8.8	0x3fec	Standard query (0)	www.thesaltlifestyle.com	A (IP address)	IN (0x0001)
Jan 13, 2021 08:51:46.852432966 CET	192.168.2.3	8.8.8.8	0x5aad	Standard query (0)	www.aduhelmfinancialsupport.com	A (IP address)	IN (0x0001)
Jan 13, 2021 08:52:09.404354095 CET	192.168.2.3	8.8.8.8	0x70c8	Standard query (0)	www.scientificimaginetics.com	A (IP address)	IN (0x0001)
Jan 13, 2021 08:52:29.502216101 CET	192.168.2.3	8.8.8.8	0x249c	Standard query (0)	www.johnemotions.com	A (IP address)	IN (0x0001)
Jan 13, 2021 08:53:12.572185993 CET	192.168.2.3	8.8.8.8	0x53bf	Standard query (0)	www.steelyourselfshop.net	A (IP address)	IN (0x0001)
Jan 13, 2021 08:53:13.559467077 CET	192.168.2.3	8.8.8.8	0x53bf	Standard query (0)	www.steelyourselfshop.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 08:51:26.053591967 CET	8.8.8.8	192.168.2.3	0x3fec	No error (0)	www.thesaltlifestyle.com	thesaltlifestyle.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 08:51:26.053591967 CET	8.8.8.8	192.168.2.3	0x3fec	No error (0)	thesaltlifestyle.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 13, 2021 08:51:46.924470901 CET	8.8.8.8	192.168.2.3	0x5aad	No error (0)	www.aduhelmfinancialsupport.com		165.160.13.20	A (IP address)	IN (0x0001)
Jan 13, 2021 08:51:46.924470901 CET	8.8.8.8	192.168.2.3	0x5aad	No error (0)	www.aduhelmfinancialsupport.com		165.160.15.20	A (IP address)	IN (0x0001)
Jan 13, 2021 08:52:09.769263029 CET	8.8.8.8	192.168.2.3	0x70c8	No error (0)	www.scientificimaginetics.com		154.92.73.140	A (IP address)	IN (0x0001)
Jan 13, 2021 08:52:29.573985100 CET	8.8.8.8	192.168.2.3	0x249c	No error (0)	www.johnemotions.com		104.24.109.70	A (IP address)	IN (0x0001)
Jan 13, 2021 08:52:29.573985100 CET	8.8.8.8	192.168.2.3	0x249c	No error (0)	www.johnemotions.com		104.24.108.70	A (IP address)	IN (0x0001)
Jan 13, 2021 08:52:29.573985100 CET	8.8.8.8	192.168.2.3	0x249c	No error (0)	www.johnemotions.com		172.67.142.17	A (IP address)	IN (0x0001)
Jan 13, 2021 08:53:13.636240959 CET	8.8.8.8	192.168.2.3	0x53bf	Name error (3)	www.steelyourselfshop.net	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.thesaltlifestyle.com
- www.aduhelmfinancialsupport.com
- www.scientificimaginetics.com
- www.johnemotions.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49736	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 08:51:26.099952936 CET	4471	OUT	GET /p95n/?u6ihA=cjlpdRL8ZtfDvB1&oH5h=BBaWJPlPEO+nvtMqhmqrcRgDtKq1LKrnuc6I0tDI+4mn5icveD46W7DXUUudv5GhOCct HTTP/1.1 Host: www.thesaltlifestyle.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 08:51:26.238513947 CET	4471	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 13 Jan 2021 07:51:26 GMT Content-Type: text/html Content-Length: 275 ETag: "5ffc83a1-113" 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>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49737	165.160.13.20	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 08:51:47.060177088 CET	4473	OUT	GET /p95n/?oH5h=yIt3vHGcFY19i9LszRbGqv8br4EBNSz7kQseU3pL44UQdgKo/VZu2mbLhFyK51ONzUns&u6ihA=cjlpdRL8ZtfDvB1 HTTP/1.1 Host: www.aduhelmfinancialsupport.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 08:51:47.204091072 CET	4473	IN	HTTP/1.1 200 OK Connection: close Date: Wed, 13 Jan 2021 07:51:47 GMT Content-Length: 94 X-ORACLE-DMS-ECID: ea9850e1-3635-4b18-92ae-e9076c77ad59-6e5b326b X-ORACLE-DMS-RID: 0 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 3c 2f 74 69 74 6c 65 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 76 69 73 65 64 22 20 63 6f 6e 74 65 6e 74 3d 22 31 2e 31 2e 37 22 20 2f 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <html><head><title></title><meta name="revised" content="1.1.7" /></head><body></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49740	154.92.73.140	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 08:52:10.069588900 CET	4493	OUT	GET /p95n/?u6ihA=cjlpdRL8ZtfDvB1&oH5h=gRhj5HMuZvR/Ec7o8oi+HxLziNFcY38IPUSKESyExHr5bx7zEB/jrV73UqEK091Ydql8 HTTP/1.1 Host: www.scientificimaginetics.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 08:52:10.370596886 CET	4493	IN	HTTP/1.1 200 OK Server: nginx Date: Wed, 13 Jan 2021 07:52:10 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 31 0d 0a 2e 0d 0a 30 0d 0a 0d 0a Data Ascii: 1.0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49741	104.24.109.70	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 08:52:29.626843929 CET	4494	OUT	GET /p95n/?oH5h=OkCbzDuuF1pG8/+FjCqUEbhCI/Ef9I/I5jzkOiKX/zkELnGsjuBbK/8sh3SawKW3Kze/&u6ihA=cjlpdRL8ZtfDvB1 HTTP/1.1 Host: www.johnemotions.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 08:52:29.685899973 CET	4495	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 13 Jan 2021 07:52:29 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Wed, 13 Jan 2021 08:52:29 GMT Location: https://www.johnemotions.com/p95n/?oH5h=OkCbzDuuF1pG8/+FjCqUEbhCI/Ef9I/I5jzkOiKX/zkELnGsjuBbK/8sh3SawKW3Kze/&u6ihA=cjlpdRL8ZtfDvB1 cf-request-id: 079c546cdf000041322a3d0000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=w99moivZwEdAiIc2yCtyAR0%2FANulYBqCpqCigrLpA%2FwtpANEJ0cKyvXA4kjcxYCQ9OtB5r2vufT9lf7t3ldGfJSk%2FfyPl3EDh5LIQKte1lnEAUpIaQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 610d89c169fc4132-PRG Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

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

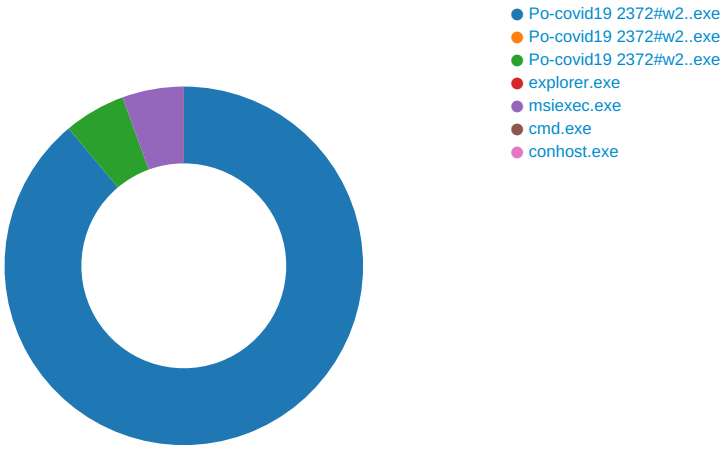
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x85 0x5E 0xEA
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x8D 0xDE 0xEA
GetMessageW	INLINE	0x48 0x8B 0xB8 0x8D 0xDE 0xEA
GetMessageA	INLINE	0x48 0x8B 0xB8 0x85 0x5E 0xEA

Statistics

Behavior



System Behavior

Analysis Process: Po-covid19 2372#w2..exe PID: 5532 Parent PID: 5604

General

Start time:	08:50:13
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\Po-covid19 2372#w2..exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Po-covid19 2372#w2..exe'
Imagebase:	0x70000
File size:	1304576 bytes
MD5 hash:	BF53C9DC0D0F032033C318ACEEF906C6
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: 00000000.00000002.253062095.0000000002708000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.256080598.000000000406F000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.256080598.000000000406F000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.256080598.000000000406F000.00000004.00000001.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	6E07CF06	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	6E07CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Po-covid19 2372#w2..exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E38C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Po-covid19 2372#w2..exe.log	unknown	1216	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	6E38C907	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	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E055705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E05CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E055705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEC1B4F	ReadFile

Analysis Process: Po-covid19 2372#w2..exe PID: 4308 Parent PID: 5532

General

Start time:	08:50:26
Start date:	13/01/2021

Path:	C:\Users\user\Desktop\Po-covid19 2372#w2..exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x130000
File size:	1304576 bytes
MD5 hash:	BF53C9DC0D0F032033C318ACEEF906C6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Po-covid19 2372#w2..exe PID: 5404 Parent PID: 5532

General

Start time:	08:50:27
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\Po-covid19 2372#w2..exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x9b0000
File size:	1304576 bytes
MD5 hash:	BF53C9DC0D0F032033C318ACEEF906C6
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: 00000003.00000002.297322370.0000000000FB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.297322370.0000000000FB0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.297322370.0000000000FB0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.296624622.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.296624622.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.296624622.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.298199420.00000000013B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.298199420.00000000013B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.298199420.00000000013B0000.00000040.00000001.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	41A037	NtReadFile

Analysis Process: explorer.exe PID: 3388 Parent PID: 5404

General

Start time:	08:50:31
Start date:	13/01/2021
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: msiexec.exe PID: 6748 Parent PID: 3388

General

Start time:	08:50:47
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msiexec.exe
Imagebase:	0xbf0000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
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: 0000000E.00000002.616475940.0000000000B40000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.616475940.0000000000B40000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.616475940.0000000000B40000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.614725408.0000000000680000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.614725408.0000000000680000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.614725408.0000000000680000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.616862762.0000000000B70000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.616862762.0000000000B70000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.616862762.0000000000B70000.00000004.00000001.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	69A037	NtReadFile

Analysis Process: cmd.exe PID: 7092 Parent PID: 6748

General

Start time:	08:50:52
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\Po-covid19 2372#w2..exe'
Imagebase:	0xbf0000
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: 7100 Parent PID: 7092

General

Start time:	08:50:53
Start date:	13/01/2021
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