ID: 344817
Sample Name: GRACE.exe
Cookbook: default.jbs
Time: 07:56:19
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

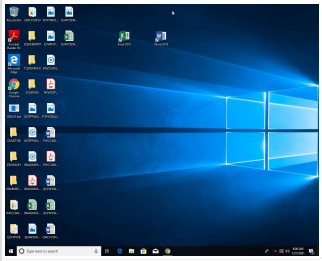
Analysis Report GRACE.exe

Overview

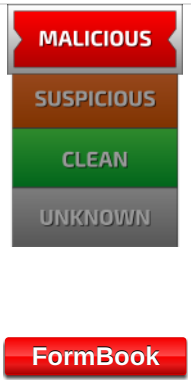
General Information

Sample Name:	GRACE.exe
Analysis ID:	344817
MD5:	9034acbb274228..
SHA1:	605948c4bcd7a0..
SHA256:	cd63e20a002279..
Tags:	COVID-19 Formbook

Most interesting Screenshot:



Detection



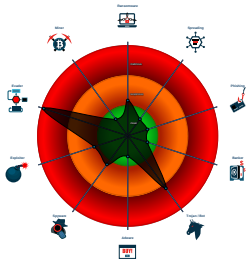
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected FormBook
- Allocates memory in foreign process…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- 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**
- GRACE.exe (PID: 6728 cmdline: 'C:\Users\user\Desktop\GRACE.exe' MD5: 9034ACBB2742281523525D715A4EE566)
  - AddInProcess32.exe (PID: 6508 cmdline: C:\Users\user\AppData\Local\Temp\AddInProcess32.exe MD5: F2A47587431C466535F3C3D3427724BE)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - netsh.exe (PID: 404 cmdline: C:\Windows\SysWOW64\netsh.exe MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
        - cmd.exe (PID: 2436 cmdline: /c del 'C:\Users\user\AppData\Local\Temp\AddInProcess32.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 7040 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook


```
{
  "Config: ": [
    "CONFIG_PATTERNS 0x8bc2",
    "KEY1_OFFSET 0x1d510",
    "CONFIG SIZE : 0xf7",
    "CONFIG OFFSET 0x1d615",
    "URL SIZE : 33",
    "searching string pattern",
    "strings_offset 0x1c1a3",
    "searching hashes pattern",
    "--------------------------------------------------",
    "Decrypted Function Hashes",
    "--------------------------------------------------",
    "0x1004744a",
    "0xf43668a6",
    "0x980476e5",
    "0x35a6d50c",
    "0xf89290dc",
    "0x94261f57",
    "0x7d54c891",
    "0x47cb721",
    "0xf72d70d3",
    "0x9f715026",
    "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",
"0xad012172",
"0x6206e716",
"0x5e4b9b9a",
"0xe4e2f5f4",
"0x54c93159",
"0x25ea79b",
"0x5bf29119",
"0xd6507db",
"0x32ffc9f8",
"0xe4cfab72",
"0x98db5380",
"0xce4cc542",
"0x3092a0a2",
"0x66053660",
"0x2607a133",
"0xfcd014c1",
"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",
"strahlenschutz.digital",
"soterppe.com",
"wlw-hnlt.com",
"topheadlinetowitness-today.info",
"droriginals.com",
"baculatechie.online",
"definity.finance",
"weddingmustgoon.com",
"ludisenofloral.com",
"kenniscourtureconsignments.com",
"dl888.net",
"singledynamics.com",
"internetmarkaching.com",
"solidconstruct.site",
"ip-freight.com",
"11sxsx.com",
"incomecontent.com",
"the343radio.com",
"kimberlygoedhart.net",
"dgdoughnuts.net",
"vivethk.com",
"st-reet.com",
"luxusgrotte.com",
"hareland.info",
"fitdramas.com",
"shakahats.com",
"cositasdepachecos.com",
"lhc965.com",
"5hnjy.com",
"zoommedicaremeetings.com",
"bebywye.site",
"ravenlewis.com",
"avia-sales.xyz",
"screwtaped.com",
"xaustock.com",
"hongreng.xyz",
"lokalised.com",
"neosolutionsllc.com",
"ecandkllc.com",
"sistertravelalliance.com",
"brotherhoodoffathers.com",
"mybestme.store",
"vigilantdis.com",
"sqatzx.com",
"kornteengoods.com",
"miamiwaterworld.com",
"mywillandmylife.com",
"novergi.com",
"eaglesnestpropheticministry.com",
"sterlworldshop.com",
"gabriellagullberg.com",
"toweroflifeinc.com",
"tiendazoom.com",
"dividupe.com",
"szyulics.com",
"theorangepearl.com",
"hotvidzhub.download",
"asacal.com",
"systemedalarmebe.com",
"margosbest.com",
"kathymusic.com",
"quintred.com",
"mad54.art",
"simplification.business",
"f-end",
"--------------------------------------------------",
"Decrypted CnC URL",
"--------------------------------------------------",
"www.registeredagentfirm.com/jqc/lv0000"
```

```
      www.registeredagentjfm.com/jqc/?u0000
    ]
  }
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000011.00000002.623489927.0000000000F30000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000011.00000002.623489927.0000000000F30000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000011.00000002.623489927.0000000000F30000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
0000000A.00000002.327464918.0000000000EB0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000A.00000002.327464918.0000000000EB0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$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 • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 19 entries

Unpacked PEs

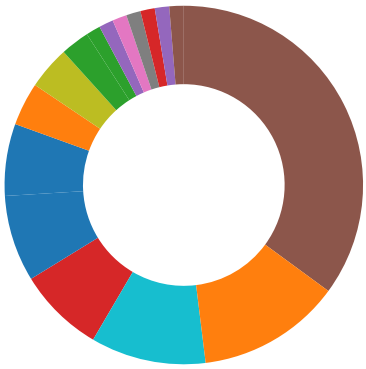
Source	Rule	Description	Author	Strings
10.2.AddInProcess32.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
10.2.AddInProcess32.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
10.2.AddInProcess32.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17609:$sqlite3step: 68 34 1C 7B E1 • 0x1771c:$sqlite3step: 68 34 1C 7B E1 • 0x17638:$sqlite3text: 68 38 2A 90 C5 • 0x1775d:$sqlite3text: 68 38 2A 90 C5 • 0x1764b:$sqlite3blob: 68 53 D8 7F 8C • 0x17773:$sqlite3blob: 68 53 D8 7F 8C
10.2.AddInProcess32.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
10.2.AddInProcess32.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:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$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
- Persistence and Installation Behavior
- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection:

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

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

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Allocates memory in foreign processes

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

Writes to foreign memory regions

Lowering of HIPS / PFW / Operating System Security Settings:

Uses netsh to modify the Windows network and firewall settings

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

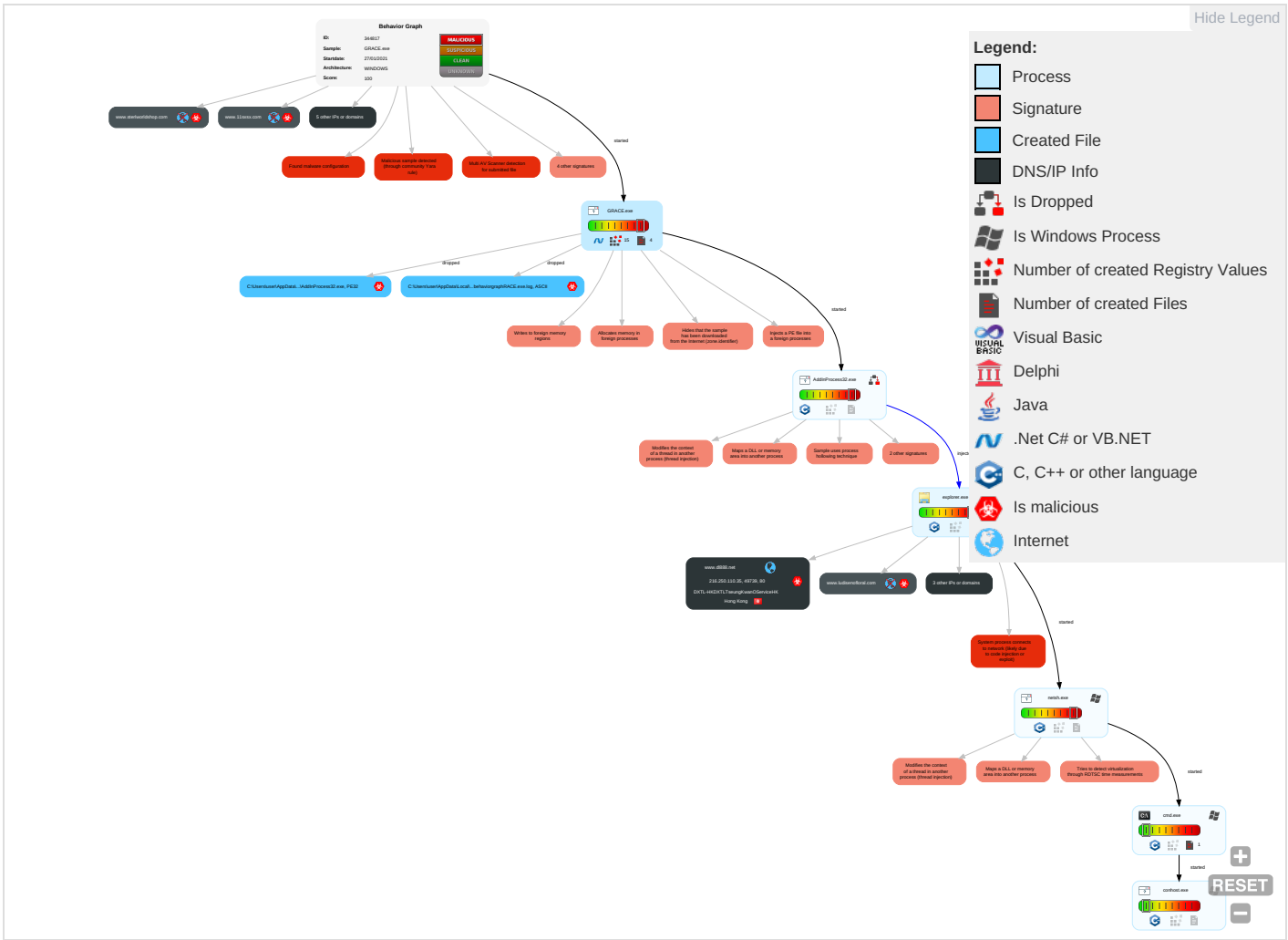
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts 1	Shared Modules 1	Valid Accounts 1	Valid Accounts 1	Rootkit 1	Credential API Hooking 1	Security Software Discovery 1 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Masquerading 1	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 8 1 2	Valid Accounts 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Virtualization/Sandbox Evasion 3	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Disable or Modify Tools 1 1	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 8 1 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Deobfuscate/Decode Files or Information 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protoco
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Obfuscated Files or Information 3	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Software Packing 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols

Behavior Graph

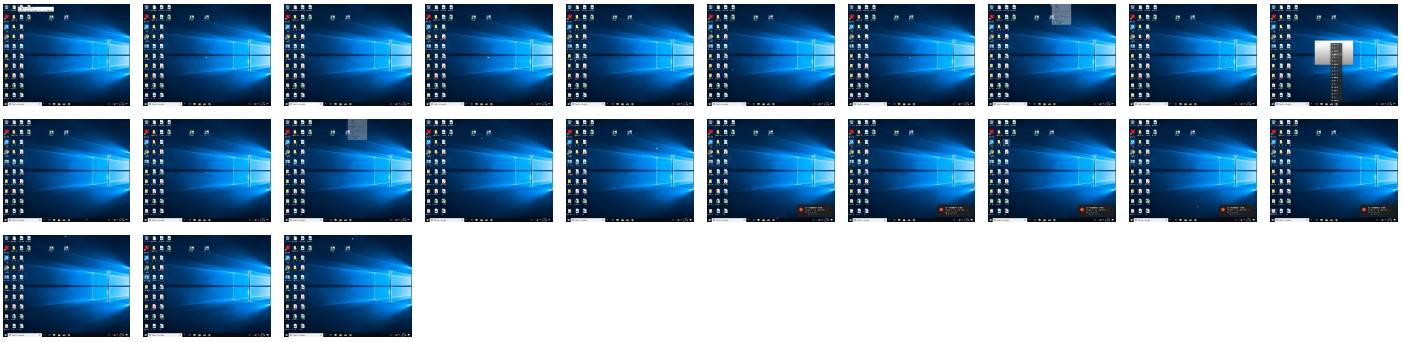


Screenshots

Thumbnails

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

Copyright null 2021



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
GRACE.exe	62%	Virustotal		Browse
GRACE.exe	16%	Metadefender		Browse
GRACE.exe	43%	ReversingLabs	ByteCode-MSIL.Trojan.Wacatac	
GRACE.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.AddInProcess32.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.luxusgrotte.com	0%	Virustotal		Browse
www.dl888.net	4%	Virustotal		Browse
shops.myshopify.com	0%	Virustotal		Browse
www.internetmarkaching.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.quintred.com/jqc/www.kimberlygoedhart.net	0%	Avira URL Cloud	safe	
http://www.dl888.net/jqc/www.hongreng.xyz	0%	Avira URL Cloud	safe	
http://www.kornteengoods.com/jqc/	0%	Avira URL Cloud	safe	
http://www.11sxsx.com/jqc/	0%	Avira URL Cloud	safe	
http://www.ludisenofloral.com/jqc/www.11sxsx.com	0%	Avira URL Cloud	safe	
http://www.quintred.comReferer:	0%	Avira URL Cloud	safe	
http://www.kimberlygoedhart.net/jqc/	0%	Avira URL Cloud	safe	
http://www.hongreng.xyz/jqc/www.hotvidzhub.download	0%	Avira URL Cloud	safe	
http://www.sterlworldshop.comReferer:	0%	Avira URL Cloud	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://www.novergi.com	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.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.szyulics.com/jqc/	0%	Avira URL Cloud	safe	
http://www.internetmarkaching.comReferer:	0%	Avira URL Cloud	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://www.hongreng.xyz/jqc/	0%	Avira URL Cloud	safe	
http://www.luxusgrotte.com	0%	Avira URL Cloud	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://www.ludisenofloral.com	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://ns.adb	0%	Avira URL Cloud	safe	
http://www.kimberlygoedhart.netReferer:	0%	Avira URL Cloud	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.11sxsx.comReferer:	0%	Avira URL Cloud	safe	
http://www.kornteengoods.com/jqc/www.ludisenofloral.com	0%	Avira URL Cloud	safe	
http://www.hongreng.xyz	0%	Avira URL Cloud	safe	
http://www.kimberlygoedhart.net/jqc/www.fitdramas.com	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.hotvidzhub.downloadReferer:	0%	Avira URL Cloud	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://www.sterlworldshop.com/jqc/	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://www.dl888.net/jqc/	0%	Avira URL Cloud	safe	
http://www.hotvidzhub.download/jqc/www.kornteengoods.com	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.sterlworldshop.com	0%	Avira URL Cloud	safe	
http://www.registeredagentfirm.com/jqc/	0%	Avira URL Cloud	safe	
http://www.wlw-hnlt.com/jqc/	0%	Avira URL Cloud	safe	
http://www.11sxsx.com	0%	Avira URL Cloud	safe	
http://www.luxusgrotte.com/jqc/	0%	Avira URL Cloud	safe	
http://www.internetmarkaching.com	0%	Avira URL Cloud	safe	
http://www.fitdramas.com	0%	Avira URL Cloud	safe	
http://www.11sxsx.com/jqc/www.luxusgrotte.com	0%	Avira URL Cloud	safe	
http://www.novergi.com/jqc/	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.registeredagentfirm.com/jqc/www.wlw-hnlt.com	0%	Avira URL Cloud	safe	
http://www.wlw-hnlt.com	0%	Avira URL Cloud	safe	
http://www.wlw-hnlt.com/jqc/www.novergi.com	0%	Avira URL Cloud	safe	
http://www.szyulics.comReferer:	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.ludisenofloral.comReferer:	0%	Avira URL Cloud	safe	
http://www.registeredagentfirm.comReferer:	0%	Avira URL Cloud	safe	
http://www.internetmarkaching.com/jqc/	0%	Avira URL Cloud	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.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.novergi.com/jqc/www.quintred.com	0%	Avira URL Cloud	safe	
http://www.kimberlygoedhart.net	0%	Avira URL Cloud	safe	
http://www.novergi.comReferer:	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.fitdramas.comReferer:	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.luxusgrotte.com	217.160.0.171	true	false	• 0%, Virustotal, Browse	unknown
gfw.cloud301.net	141.164.47.167	true	false		unknown
www.dl888.net	216.250.110.35	true	true	• 4%, Virustotal, Browse	unknown
shops.myshopify.com	23.227.38.74	true	false	• 0%, Virustotal, Browse	unknown
www.internetmarkaching.com	104.21.69.246	true	false	• 1%, Virustotal, Browse	unknown
www.hongreng.xyz	unknown	unknown	true		unknown
www.ludisenofloral.com	unknown	unknown	true		unknown
www.11sxsx.com	unknown	unknown	true		unknown
www.sterlworldshop.com	unknown	unknown	true		unknown
www.kornteengoods.com	unknown	unknown	true		unknown
www.hotvidzhub.download	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.dl888.net/jqc/?njq0dR=RzuPnv&JfE=fDutAcwv9Lxx6pK+U/h8/Jmgh7jy3dQeKhNoyB3Bjj0bKWR6mwge2sLPOJXFU1/1riqc	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.quintred.com/jqc/www.kimberlygoedhart.net	explorer.exe, 00000010.00000002.638723848.000000000569F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.dl888.net/jqc/www.hongreng.xyz	explorer.exe, 00000010.00000002.638723848.000000000569F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kornteengoods.com/jqc/	explorer.exe, 00000010.00000002.638723848.000000000569F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.11sxsx.com/jqc/	explorer.exe, 00000010.00000002.638723848.000000000569F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ludisenofloral.com/jqc/www.11sxsx.com	explorer.exe, 00000010.00000002.638723848.000000000569F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.quintred.comReferer:	explorer.exe, 00000010.00000002.638723848.000000000569F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kimberlygoedhart.net/jqc/	explorer.exe, 00000010.00000002.638723848.000000000569F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hongreng.xyz/jqc/www.hotvidzhub.download	explorer.exe, 00000010.00000002.638723848.000000000569F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sterlworldshop.comReferer:	explorer.exe, 00000010.00000002.638723848.000000000569F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000010.00000000.312521457.0000000008B46000.00000002.00000001.sdmp	false		high
http://ns.adobe.c/g	GRACE.exe, 00000000.00000003.291474996.0000000008610000.00000004.00000001.sdmp, GRACE.exe, 00000000.00000003.215101178.000000008601000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.novergi.com	explorer.exe, 00000010.00000002.638723848.000000000569F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000010.00000000.312521457.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000010.00000000.312521457.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.szyulics.com/jqc/	explorer.exe, 00000010.00000002.638723848.000000000569F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.internetmarkaching.comReferer:	explorer.exe, 00000010.00000002.638723848.000000000569F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

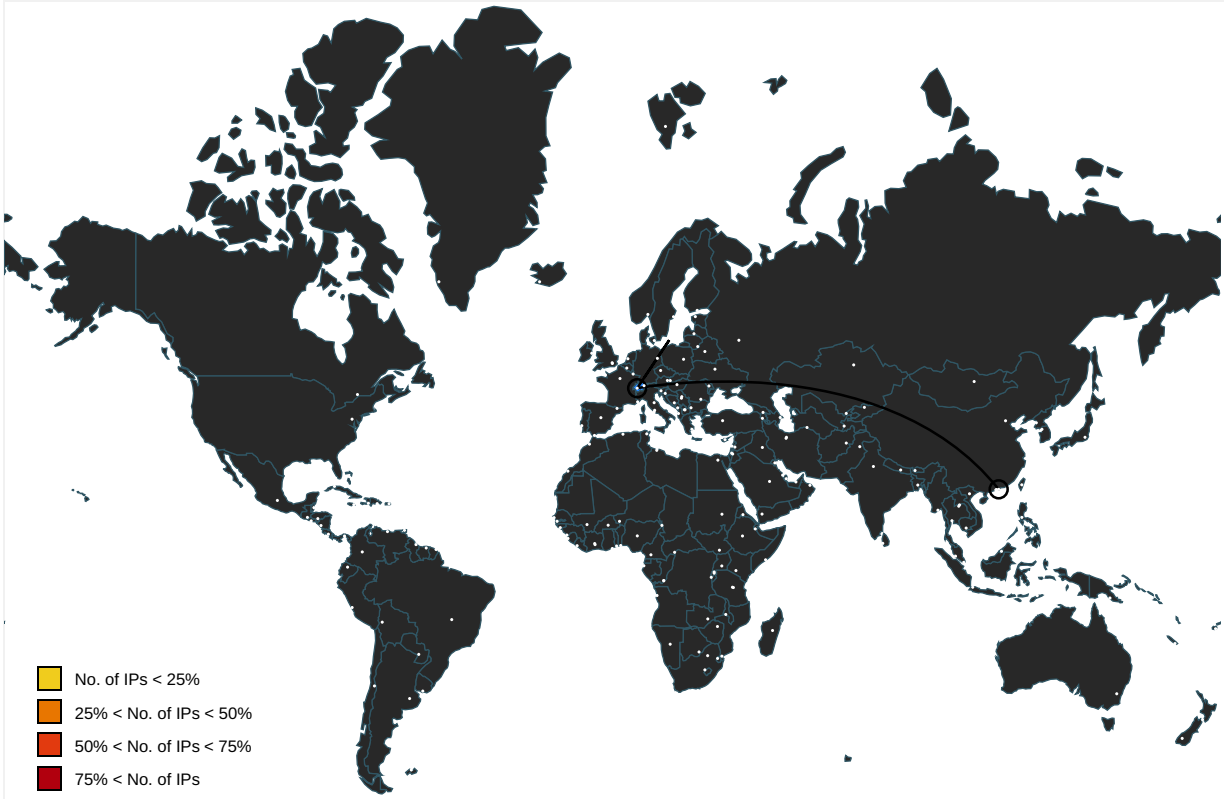
Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.pki.goog/gts1o1core0	GRACE.exe, 00000000.00000002.2 93213064.000000000286F000.0000 0004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hongreng.xyz/jqc/	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.luxusgrotte.com	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pki.goog/GTS1O1core.crl0	GRACE.exe, 00000000.00000002.2 93213064.000000000286F000.0000 0004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ludisenofloral.com	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000010.0000000 0.312521457.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adb	GRACE.exe, 00000000.00000003.2 91474996.0000000008610000.0000 0004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kimberlygoedhart.netReferer:	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000010.0000000 0.312521457.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000010.0000000 0.312521457.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.11sxsx.comReferer:	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	GRACE.exe, 00000000.00000002.2 93079053.0000000002841000.0000 0004.00000001.sdmp	false		high
http://www.kornteengoods.com/jqc/www.ludisenofloral.com	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hongreng.xyz	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kimberlygoedhart.net/jqc/www.fitdramas.com	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hotvidzhub.downloadReferer:	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.adobe.cobj	GRACE.exe, 00000000.00000003.2 91474996.0000000008610000.0000 0004.00000001.sdmp, GRACE.exe, 00000000.00000003.215101178.0 000000008601000.00000004.00000 001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sterlworldshop.com/jqc/	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pki.goog/gsr2/GTS1O1.crt0	GRACE.exe, 00000000.00000002.2 93213064.000000000286F000.0000 0004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.dl888.net/jqc/	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hotvidzhub.download/jqc/www.kornteengoods.com	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000010.0000000 0.312521457.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sterlworldshop.com	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.registeredagentfirm.com/jqc/	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.wlw-hnlt.com/jqc/	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.11sxsx.com	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000010.0000000 0.312521457.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.luxusgrotte.com/jqc/	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.internetmarkaching.com	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fitdramas.com	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.11sxsx.com/jqc/www.luxusgrotte.com	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.novergi.com/jqc/	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	explorer.exe, 00000010.0000000 0.312521457.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000010.0000000 0.312521457.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000010.0000000 0.312521457.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.registeredagentfirm.com/jqc/www.wlw-hnlt.com	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000010.0000000 0.312521457.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.wlw-hnlt.com	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.wlw-hnlt.com/jqc/www.novergi.com	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.szyulics.comReferer:	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	explorer.exe, 00000010.0000000 0.312521457.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.goodfont.co.kr	explorer.exe, 00000010.0000000 0.312521457.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ludisenofloral.comReferer:	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schema.org/WebPage	GRACE.exe, 00000000.00000002.2 93213064.000000000286F000.0000 0004.00000001.sdmp	false		high
http://www.registeredagentfirm.comReferer:	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.internetmarkaching.com/jqc/	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	explorer.exe, 00000010.0000000 0.312521457.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000010.0000000 0.312521457.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000010.0000000 0.312521457.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.novergi.com/jqc/www.quintred.com	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kimberlygoedhart.net	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.novergi.comReferer:	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	explorer.exe, 00000010.0000000 0.312521457.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000010.0000000 0.312521457.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fitdramas.comReferer:	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	explorer.exe, 00000010.0000000 0.312521457.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.luxusgrotte.com/jqc/www.sterlworldshop.com	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000010.0000000 0.312521457.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000010.0000000 0.312521457.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.szyulics.com/jqc/M	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hotvidzhub.download	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.dl888.netReferer:	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.wlw-hnlt.comReferer:	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.dl888.net	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sterlworldshop.com/jqc/www.internetmarkaching.com	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.registeredagentfirm.com	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kornteengoods.com	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.quintred.com	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hongreng.xyzReferer:	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000010.0000000 0.312521457.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.szyulics.com	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000010.0000000 0.312521457.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fitdramas.com/jqc/	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000010.0000000 0.312521457.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.internetmarkaching.com/jqc/www.registeredagentfirm.com	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.luxusgrotte.comReferer:	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fitdramas.com/jqc/www.szyulics.com	explorer.exe, 00000010.0000000 2.638723848.000000000569F000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers8	explorer.exe, 00000010.00000000.312521457.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.ludisenofloral.com/jqc/	explorer.exe, 00000010.00000002.638723848.000000000569F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.quintred.com/jqc/	explorer.exe, 00000010.00000002.638723848.000000000569F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.hotvidzhub.download/jqc/	explorer.exe, 00000010.00000002.638723848.000000000569F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.kornteengoods.comReferer:	explorer.exe, 00000010.00000002.638723848.000000000569F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.ado/1	GRACE.exe, 00000000.00000003.291474996.0000000008610000.00000004.00000001.sdmp, GRACE.exe, 00000000.00000003.215101178.0000000008601000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.250.110.35	unknown	Hong Kong		134548	DXTL-HKDXTLTseungKwanOServiceHK	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344817
Start date:	27.01.2021
Start time:	07:56:19
Joe Sandbox Product:	CloudBasic

Copyright null 2021

Overall analysis duration:	0h 12m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	GRACE.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:	33
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@7/2@12/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 13.2% (good quality ratio 12.1%) • Quality average: 74.7% • Quality standard deviation: 30.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 52.147.198.201, 172.217.23.36, 51.104.139.180, 92.122.144.200, 95.101.22.216, 95.101.22.224, 20.54.26.129, 67.27.158.126, 8.241.9.254, 8.248.139.254, 8.248.121.254, 8.241.122.126, 52.155.217.156 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, fs.microsoft.com, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, www.google.com, 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 • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:57:14	API Interceptor	216x Sleep call for process: GRACE.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.luxusgrotte.com	ordine.exe	Get hash	malicious	Browse	• 217.160.0.171
shops.myshopify.com	v07PSzmSp9.exe	Get hash	malicious	Browse	• 23.227.38.74
	win32.exe	Get hash	malicious	Browse	• 23.227.38.74
	documents_0084568546754.exe	Get hash	malicious	Browse	• 23.227.38.74
	Payment _Arabian Parts Co BSC#U00a9.exe	Get hash	malicious	Browse	• 23.227.38.74
	MPbBCArHPF.exe	Get hash	malicious	Browse	• 23.227.38.74
	G0ESHzsrvg.exe	Get hash	malicious	Browse	• 23.227.38.74
	SecuriteInfo.com.Trojan.PackedNET.507.23078.exe	Get hash	malicious	Browse	• 23.227.38.74
	SecuriteInfo.com.Trojan.PackedNET.507.15470.exe	Get hash	malicious	Browse	• 23.227.38.74
	CQAOPIhHJZ.exe	Get hash	malicious	Browse	• 23.227.38.74
	SAMSUNG C&T UPCOMING PROJECTS19-027-MP-010203 _ 19-028-MP-010203.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO20210120.exe	Get hash	malicious	Browse	• 23.227.38.74
	0iEsxw3D7A.exe	Get hash	malicious	Browse	• 23.227.38.74
	z1k1U9Vnnw.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO_610.20-21.A2424.UP_PDF.exe	Get hash	malicious	Browse	• 23.227.38.74
	RE.exe	Get hash	malicious	Browse	• 23.227.38.74
	Shipping Docs_pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	r.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO81053.exe	Get hash	malicious	Browse	• 23.227.38.74
	January RFQ..exe	Get hash	malicious	Browse	• 23.227.38.74
	KuPBIsrqbO.exe	Get hash	malicious	Browse	• 23.227.38.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DXTL-HKDXTLTseungKwanOServiceHK	WUHU95Apq3	Get hash	malicious	Browse	• 156.235.189.154
	New Year Inquiry List.xlsx	Get hash	malicious	Browse	• 156.237.162.40
	gPGTcEMoM1.exe	Get hash	malicious	Browse	• 154.80.226.18
	CiL08gVVjl.exe	Get hash	malicious	Browse	• 154.83.105.183
	MPbBCArHPF.exe	Get hash	malicious	Browse	• 156.237.170.187
	G0ESHzsrvg.exe	Get hash	malicious	Browse	• 45.199.38.93
	NEW AGREEMENT 2021.xlsx	Get hash	malicious	Browse	• 154.80.226.18
	SecuriteInfo.com.Trojan.PackedNET.507.23078.exe	Get hash	malicious	Browse	• 154.95.152.81
	SecuriteInfo.com.Trojan.PackedNET.507.15470.exe	Get hash	malicious	Browse	• 154.80.196.189
	PO20210120.exe	Get hash	malicious	Browse	• 154.219.198.4
	PO210119.exe.exe	Get hash	malicious	Browse	• 45.196.239.235
	synBIAIJ7b.exe	Get hash	malicious	Browse	• 154.95.134.253
	1tqW2LLr74.exe	Get hash	malicious	Browse	• 154.83.105.183
	ETD101210182 HBL.xlsx	Get hash	malicious	Browse	• 156.232.190.92
	NEW AGREEMENT 19 01 2021.xlsx	Get hash	malicious	Browse	• 154.80.226.18
	Calendario dei pagamenti.exe	Get hash	malicious	Browse	• 156.245.175.204
	SKM_C221200706052800n.exe	Get hash	malicious	Browse	• 154.215.134.40
	payment advise.exe	Get hash	malicious	Browse	• 154.86.237.210

Copyright null 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Shipping Document PL&BL Draft.exe	Get hash	malicious	Browse	• 154.218.85.183
	SWIFT Payment DOOEL EUR 74,246.41 20210101950848.exe	Get hash	malicious	Browse	• 154.95.162.109

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	SecuriteInfo.com.Trojan.Packed2.42783.32.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Packed2.42783.14936.exe	Get hash	malicious	Browse	
	SlaZL2LqI2.exe	Get hash	malicious	Browse	
	4NoiNHCNoU.exe	Get hash	malicious	Browse	
	SoPwZKv1Mf.exe	Get hash	malicious	Browse	
	bXFjrxjRlb.exe	Get hash	malicious	Browse	
	Generator.cont.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	560911_P.EXE	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	IMG_61779.pdf.exe	Get hash	malicious	Browse	
	IMG_5391.EXE	Get hash	malicious	Browse	
	czZ769nM6r.exe	Get hash	malicious	Browse	
	IMG_1107.EXE	Get hash	malicious	Browse	
	r3q6Bv8naR.exe	Get hash	malicious	Browse	
	sy1RnlHl8Y.exe	Get hash	malicious	Browse	
	qyMITIBawC.exe	Get hash	malicious	Browse	
	Qn2AQrgfqJ.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.509.28611.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.509.17348.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\GRACE.exe.log

Process:	C:\Users\user\Desktop\GRACE.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1873
Entropy (8bit):	5.355036985457214
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjovitHoxHhAHKzvr1qHj:iqXeqm00YqhQnouRqjoKtlxHeqzTwD
MD5:	CDA95282F22F47DA2FDDC9E912B67FEF
SHA1:	67A40582A092B5DF40C3EB61A361A2D336FC69E0
SHA-256:	179E50F31095D0CFA13DCBB9CED6DEE424DFE8CEF8E05BDE1F840273F45E5F49
SHA-512:	1D151D92AE982D2149C2255826C2FFB89A475A1EB9B9FE93DC3706F3016CD6B309743B36A4D7F6D68F48CE25391FDA7A2BAE42061535EEA7862460424A3A2036
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",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,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

C:\Users\user\AppData\Local\Temp\AddInProcess32.exe

Process:	C:\Users\user\Desktop\GRACE.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	42080
Entropy (8bit):	6.2125074198825105
Encrypted:	false

C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	
SSDEEP:	384:gc3JOvwWj8Gpw0A67dOpRIMKJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+QsPZw:g4JU8g17dl6Iq88MoBd7mFViqM5sL2
MD5:	F2A47587431C466535F3C3D3427724BE
SHA1:	90DF719241CE04828F0DD4D31D683F84790515FF
SHA-256:	23F4A2CCDCE499C524CF43793FDA8E773D809514B5471C02FA5E68F0CDA7A10B
SHA-512:	E9D0819478DDDA47763C7F5F617CD258D0FACBBBFFE0C7A965EDE9D0D884A6D7BB445820A3FD498B243BBD8BECBA146687B61421745E32B86272232C6F9E90D8
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: SecuriteInfo.com.Trojan.Packed2.42783.32.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.Packed2.42783.14936.exe, Detection: malicious, Browse • Filename: SlaZL2LqI2.exe, Detection: malicious, Browse • Filename: 4NoiNHCNoU.exe, Detection: malicious, Browse • Filename: SoPwZKv1Mf.exe, Detection: malicious, Browse • Filename: bXFjrxjRlb.exe, Detection: malicious, Browse • Filename: Generator.cont.exe, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: 560911_P.EXE, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: IMG_61779.pdf.exe, Detection: malicious, Browse • Filename: IMG_5391.EXE, Detection: malicious, Browse • Filename: czZ769nM6r.exe, Detection: malicious, Browse • Filename: IMG_1107.EXE, Detection: malicious, Browse • Filename: r3q6Bv8naR.exe, Detection: malicious, Browse • Filename: sy1RnlHl8Y.exe, Detection: malicious, Browse • Filename: qyMlTIBawC.exe, Detection: malicious, Browse • Filename: Qn2AQrgfqJ.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.PackedNET.509.28611.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.PackedNET.509.17348.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....0..X.....w... .....@.. ..... .`.....Hw..O..... .....f..`>.....v..... ....H.....text....W... ...X..... ..`.rsrc... .....Z.....@..@.relo c.....d.....@..B.....\|w.....H.....#...Q.....u.....0..K.....-..*..i....*...r...p.o....,...r...p.o....-..*.....o.....o.....$...*.....o....(....(.....:...(....o.....r...p.o.....4.....o..... .....o.....s .....o!...s".....s#.....r]..prg..po$.....r...p.o$.....r...pr...po$.....s.....(%.....tB...r...p(&...&..r...p.('...s(.....o)...&..o*....(+...o,.....&...(- ....*.....3..@.....R...s.....s....(....*:.(/.....}P...*J.{P....o0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.634685476400275
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:	GRACE.exe
File size:	3215360
MD5:	9034acbb2742281523525d715a4ee566
SHA1:	605948c4bcd7a0290e46a37d841a09ab43fbec86
SHA256:	cd63e20a002279934bc2ed4887d77605686a79f28f8114f9c01b678754a1e10a
SHA512:	cc2b848101ea9d63fa02a442171fd250f4be76cc9c8d5f6b4c32062436b48931e9b931102c5c392217740cc06661205729f1b2afa7b0dda147c113df3ce454d9
SSDEEP:	49152:YTrD4RqOGxx0KVuy+Z28fUANfo8L81ucdopCpC9aXCmczjF10:gD4R5GxxHs8dSQoSucOCpC8Izj/0
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...}#.....1.....N#1.. .....@.. .....1.....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x71234e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0xF9F237D [Sat Apr 22 10:05:49 1978 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3122fc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x314000	0x636	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x316000	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	0x310354	0x310400	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x314000	0x636	0x800	False	0.35546875	data	3.70922095564	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x316000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x3140a0	0x3ac	data		
RT_MANIFEST	0x31444c	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 2018 >8<2D6?3IB:F?3DB7A>JA9B5
Assembly Version	1.0.0.0
InternalName	GRACE.exe
FileVersion	9.14.19.23
CompanyName	>8<2D6?3IB:F?3DB7A>JA9B5
Comments	27J@CII8C76?EJ;
ProductName	<>I5?FEA3JEHG6CBH:C44DED
ProductVersion	9.14.19.23
FileDescription	<>I5?FEA3JEHG6CBH:C44DED
OriginalFilename	GRACE.exe

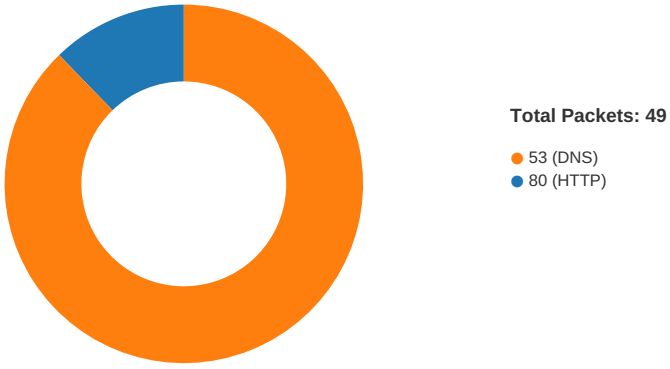
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/27/21-07:59:06.758330	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
01/27/21-08:00:11.194982	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/27/21-08:01:12.518069	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49754	23.227.38.74	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 07:58:44.645333052 CET	49739	80	192.168.2.3	216.250.110.35
Jan 27, 2021 07:58:44.928340912 CET	80	49739	216.250.110.35	192.168.2.3
Jan 27, 2021 07:58:44.928457975 CET	49739	80	192.168.2.3	216.250.110.35
Jan 27, 2021 07:58:44.928558111 CET	49739	80	192.168.2.3	216.250.110.35
Jan 27, 2021 07:58:45.210340023 CET	80	49739	216.250.110.35	192.168.2.3
Jan 27, 2021 07:58:45.210391998 CET	80	49739	216.250.110.35	192.168.2.3
Jan 27, 2021 07:58:45.210418940 CET	80	49739	216.250.110.35	192.168.2.3
Jan 27, 2021 07:58:45.210614920 CET	49739	80	192.168.2.3	216.250.110.35
Jan 27, 2021 07:58:45.210660934 CET	49739	80	192.168.2.3	216.250.110.35
Jan 27, 2021 07:58:45.210788965 CET	49739	80	192.168.2.3	216.250.110.35
Jan 27, 2021 07:58:45.492578983 CET	80	49739	216.250.110.35	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 07:57:03.687182903 CET	58361	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:57:03.736371994 CET	53	58361	8.8.8.8	192.168.2.3
Jan 27, 2021 07:57:04.684554100 CET	63492	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:57:04.735389948 CET	53	63492	8.8.8.8	192.168.2.3
Jan 27, 2021 07:57:05.631925106 CET	60831	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:57:05.682622910 CET	53	60831	8.8.8.8	192.168.2.3
Jan 27, 2021 07:57:06.526653051 CET	60100	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:57:06.577647924 CET	53	60100	8.8.8.8	192.168.2.3
Jan 27, 2021 07:57:07.402307987 CET	53195	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:57:07.450220108 CET	53	53195	8.8.8.8	192.168.2.3
Jan 27, 2021 07:57:08.477905035 CET	50141	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:57:08.528554916 CET	53	50141	8.8.8.8	192.168.2.3
Jan 27, 2021 07:57:09.424428940 CET	53023	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:57:09.473896027 CET	53	53023	8.8.8.8	192.168.2.3
Jan 27, 2021 07:57:10.614949942 CET	49563	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:57:10.673142910 CET	53	49563	8.8.8.8	192.168.2.3
Jan 27, 2021 07:57:11.587152004 CET	51352	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:57:11.635020018 CET	53	51352	8.8.8.8	192.168.2.3
Jan 27, 2021 07:57:11.710526943 CET	59349	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:57:11.771256924 CET	53	59349	8.8.8.8	192.168.2.3
Jan 27, 2021 07:57:12.465265036 CET	57084	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:57:12.514309883 CET	53	57084	8.8.8.8	192.168.2.3
Jan 27, 2021 07:57:13.268241882 CET	58823	53	192.168.2.3	8.8.8.8

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 07:57:13.317176104 CET	53	58823	8.8.8.8	192.168.2.3
Jan 27, 2021 07:57:31.523591042 CET	57568	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:57:31.573447943 CET	53	57568	8.8.8.8	192.168.2.3
Jan 27, 2021 07:57:35.922370911 CET	50540	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:57:35.983253956 CET	53	50540	8.8.8.8	192.168.2.3
Jan 27, 2021 07:57:39.079822063 CET	54366	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:57:39.137626886 CET	53	54366	8.8.8.8	192.168.2.3
Jan 27, 2021 07:57:48.028091908 CET	53034	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:57:48.094542027 CET	53	53034	8.8.8.8	192.168.2.3
Jan 27, 2021 07:57:53.722011089 CET	57762	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:57:53.771976948 CET	53	57762	8.8.8.8	192.168.2.3
Jan 27, 2021 07:58:09.577709913 CET	55435	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:58:09.628099918 CET	53	55435	8.8.8.8	192.168.2.3
Jan 27, 2021 07:58:15.467978954 CET	50713	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:58:15.529508114 CET	53	50713	8.8.8.8	192.168.2.3
Jan 27, 2021 07:58:44.575615883 CET	56132	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:58:44.639400959 CET	53	56132	8.8.8.8	192.168.2.3
Jan 27, 2021 07:58:46.025794983 CET	58987	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:58:46.073719978 CET	53	58987	8.8.8.8	192.168.2.3
Jan 27, 2021 07:58:47.430965900 CET	56579	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:58:47.502331972 CET	53	56579	8.8.8.8	192.168.2.3
Jan 27, 2021 07:59:05.447269917 CET	60633	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:59:06.435502052 CET	60633	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:59:06.739923954 CET	53	60633	8.8.8.8	192.168.2.3
Jan 27, 2021 07:59:06.758213997 CET	53	60633	8.8.8.8	192.168.2.3
Jan 27, 2021 07:59:25.173145056 CET	61292	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:59:25.235316992 CET	53	61292	8.8.8.8	192.168.2.3
Jan 27, 2021 07:59:47.537916899 CET	63619	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:59:47.611829996 CET	53	63619	8.8.8.8	192.168.2.3
Jan 27, 2021 07:59:53.490791082 CET	64938	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:59:53.547228098 CET	53	64938	8.8.8.8	192.168.2.3
Jan 27, 2021 07:59:54.199328899 CET	61946	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:59:54.261035919 CET	53	61946	8.8.8.8	192.168.2.3
Jan 27, 2021 07:59:55.497503042 CET	64910	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:59:55.554064989 CET	53	64910	8.8.8.8	192.168.2.3
Jan 27, 2021 07:59:56.105572939 CET	52123	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:59:56.167295933 CET	53	52123	8.8.8.8	192.168.2.3
Jan 27, 2021 07:59:56.889492035 CET	56130	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:59:56.950434923 CET	53	56130	8.8.8.8	192.168.2.3
Jan 27, 2021 07:59:57.763669014 CET	56338	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:59:57.819977999 CET	53	56338	8.8.8.8	192.168.2.3
Jan 27, 2021 07:59:58.676543951 CET	59420	53	192.168.2.3	8.8.8.8
Jan 27, 2021 07:59:58.735301018 CET	53	59420	8.8.8.8	192.168.2.3
Jan 27, 2021 07:59:59.986825943 CET	58784	53	192.168.2.3	8.8.8.8
Jan 27, 2021 08:00:00.045607090 CET	53	58784	8.8.8.8	192.168.2.3
Jan 27, 2021 08:00:01.559737921 CET	63978	53	192.168.2.3	8.8.8.8
Jan 27, 2021 08:00:01.616200924 CET	53	63978	8.8.8.8	192.168.2.3
Jan 27, 2021 08:00:02.453038931 CET	62938	53	192.168.2.3	8.8.8.8
Jan 27, 2021 08:00:02.514525890 CET	53	62938	8.8.8.8	192.168.2.3
Jan 27, 2021 08:00:08.715852022 CET	55708	53	192.168.2.3	8.8.8.8
Jan 27, 2021 08:00:09.726617098 CET	55708	53	192.168.2.3	8.8.8.8
Jan 27, 2021 08:00:10.742414951 CET	55708	53	192.168.2.3	8.8.8.8
Jan 27, 2021 08:00:10.826936007 CET	53	55708	8.8.8.8	192.168.2.3
Jan 27, 2021 08:00:11.194005013 CET	53	55708	8.8.8.8	192.168.2.3
Jan 27, 2021 08:00:30.982753992 CET	56803	53	192.168.2.3	8.8.8.8
Jan 27, 2021 08:00:31.529903889 CET	53	56803	8.8.8.8	192.168.2.3
Jan 27, 2021 08:00:51.924572945 CET	57145	53	192.168.2.3	8.8.8.8
Jan 27, 2021 08:00:51.993443966 CET	53	57145	8.8.8.8	192.168.2.3
Jan 27, 2021 08:01:12.236183882 CET	55359	53	192.168.2.3	8.8.8.8
Jan 27, 2021 08:01:12.307245016 CET	53	55359	8.8.8.8	192.168.2.3
Jan 27, 2021 08:01:32.660002947 CET	58306	53	192.168.2.3	8.8.8.8
Jan 27, 2021 08:01:32.728943110 CET	53	58306	8.8.8.8	192.168.2.3

ICMP Packets

Copyright null 2021

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Jan 27, 2021 07:59:06.758330107 CET	192.168.2.3	8.8.8.8	d067	(Port unreachable)	Destination Unreachable
Jan 27, 2021 08:00:11.194982052 CET	192.168.2.3	8.8.8.8	cff9	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 07:58:44.575615883 CET	192.168.2.3	8.8.8.8	0x4d08	Standard query (0)	www.dl888.net	A (IP address)	IN (0x0001)
Jan 27, 2021 07:59:05.447269917 CET	192.168.2.3	8.8.8.8	0x775a	Standard query (0)	www.hongreng.xyz	A (IP address)	IN (0x0001)
Jan 27, 2021 07:59:06.435502052 CET	192.168.2.3	8.8.8.8	0x775a	Standard query (0)	www.hongreng.xyz	A (IP address)	IN (0x0001)
Jan 27, 2021 07:59:25.173145056 CET	192.168.2.3	8.8.8.8	0xfea7	Standard query (0)	www.hotvidzhub.download	A (IP address)	IN (0x0001)
Jan 27, 2021 07:59:47.537916899 CET	192.168.2.3	8.8.8.8	0x6d9	Standard query (0)	www.kornteengoods.com	A (IP address)	IN (0x0001)
Jan 27, 2021 08:00:08.715852022 CET	192.168.2.3	8.8.8.8	0xe3ba	Standard query (0)	www.ludisenofloral.com	A (IP address)	IN (0x0001)
Jan 27, 2021 08:00:09.726617098 CET	192.168.2.3	8.8.8.8	0xe3ba	Standard query (0)	www.ludisenofloral.com	A (IP address)	IN (0x0001)
Jan 27, 2021 08:00:10.742414951 CET	192.168.2.3	8.8.8.8	0xe3ba	Standard query (0)	www.ludisenofloral.com	A (IP address)	IN (0x0001)
Jan 27, 2021 08:00:30.982753992 CET	192.168.2.3	8.8.8.8	0xeb0d	Standard query (0)	www.11sxsx.com	A (IP address)	IN (0x0001)
Jan 27, 2021 08:00:51.924572945 CET	192.168.2.3	8.8.8.8	0x50a	Standard query (0)	www.luxusgrotte.com	A (IP address)	IN (0x0001)
Jan 27, 2021 08:01:12.236183882 CET	192.168.2.3	8.8.8.8	0xd988	Standard query (0)	www.sterlworldshop.com	A (IP address)	IN (0x0001)
Jan 27, 2021 08:01:32.660002947 CET	192.168.2.3	8.8.8.8	0x7eb8	Standard query (0)	www.internetmarkaching.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 07:58:44.639400959 CET	8.8.8.8	192.168.2.3	0x4d08	No error (0)	www.dl888.net		216.250.110.35	A (IP address)	IN (0x0001)
Jan 27, 2021 07:59:06.739923954 CET	8.8.8.8	192.168.2.3	0x775a	Name error (3)	www.hongreng.xyz	none	none	A (IP address)	IN (0x0001)
Jan 27, 2021 07:59:06.758213997 CET	8.8.8.8	192.168.2.3	0x775a	Name error (3)	www.hongreng.xyz	none	none	A (IP address)	IN (0x0001)
Jan 27, 2021 07:59:25.235316992 CET	8.8.8.8	192.168.2.3	0xfea7	Name error (3)	www.hotvidzhub.download	none	none	A (IP address)	IN (0x0001)
Jan 27, 2021 07:59:47.611829996 CET	8.8.8.8	192.168.2.3	0x6d9	Name error (3)	www.kornteengoods.com	none	none	A (IP address)	IN (0x0001)
Jan 27, 2021 08:00:10.826936007 CET	8.8.8.8	192.168.2.3	0xe3ba	Server failure (2)	www.ludisenofloral.com	none	none	A (IP address)	IN (0x0001)
Jan 27, 2021 08:00:11.194005013 CET	8.8.8.8	192.168.2.3	0xe3ba	Server failure (2)	www.ludisenofloral.com	none	none	A (IP address)	IN (0x0001)
Jan 27, 2021 08:00:31.529903889 CET	8.8.8.8	192.168.2.3	0xeb0d	No error (0)	www.11sxsx.com	vps.temai.org		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 08:00:31.529903889 CET	8.8.8.8	192.168.2.3	0xeb0d	No error (0)	vps.temai.org	gfw.cloud301.net		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 08:00:31.529903889 CET	8.8.8.8	192.168.2.3	0xeb0d	No error (0)	gfw.cloud301.net		141.164.47.167	A (IP address)	IN (0x0001)
Jan 27, 2021 08:00:31.529903889 CET	8.8.8.8	192.168.2.3	0xeb0d	No error (0)	gfw.cloud301.net		158.247.206.75	A (IP address)	IN (0x0001)
Jan 27, 2021 08:00:31.529903889 CET	8.8.8.8	192.168.2.3	0xeb0d	No error (0)	gfw.cloud301.net		45.32.19.21	A (IP address)	IN (0x0001)
Jan 27, 2021 08:00:31.529903889 CET	8.8.8.8	192.168.2.3	0xeb0d	No error (0)	gfw.cloud301.net		45.32.11.11	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 08:00:31.529903889 CET	8.8.8.8	192.168.2.3	0xeb0d	No error (0)	gfw.cloud301.net		158.247.204.226	A (IP address)	IN (0x0001)
Jan 27, 2021 08:00:51.993443966 CET	8.8.8.8	192.168.2.3	0x50a	No error (0)	www.luxusgrotte.com		217.160.0.171	A (IP address)	IN (0x0001)
Jan 27, 2021 08:01:12.307245016 CET	8.8.8.8	192.168.2.3	0xd988	No error (0)	www.sterlworldshop.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 08:01:12.307245016 CET	8.8.8.8	192.168.2.3	0xd988	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Jan 27, 2021 08:01:32.728943110 CET	8.8.8.8	192.168.2.3	0x7eb8	No error (0)	www.internetmarkaching.com		104.21.69.246	A (IP address)	IN (0x0001)
Jan 27, 2021 08:01:32.728943110 CET	8.8.8.8	192.168.2.3	0x7eb8	No error (0)	www.internetmarkaching.com		172.67.216.18	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.dl888.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49739	216.250.110.35	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 07:58:44.928558111 CET	3995	OUT	GET /jqc/?njq0dR=RzuPnv&JfE=fDutAcwv9Lxx6pK+U/h8/Jmgh7jy3dQeKhNoyB3Bjj0bKWR6mwge2sLPOJXFU1/1riqc HTTP/1.1 Host: www.dl888.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 07:58:45.210340023 CET	3996	IN	HTTP/1.1 404 Not Found Content-Length: 1308 Content-Type: text/html Server: Microsoft-IIS/6.0 X-Powered-By: ASP.NET Date: Wed, 27 Jan 2021 06:58:37 GMT Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 54 49 54 4c 45 3e ce de b7 a8 d5 d2 b5 bd b8 c3 d2 b3 3c 2f 54 49 54 4c 45 3e 0d 0a 3c 4d 45 54 41 20 48 54 54 50 2d 45 51 55 49 56 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 43 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 47 42 32 33 31 32 22 3e 0d 0a 3c 53 54 59 4c 45 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 20 20 42 4f 44 59 20 7b 20 66 6f 6e 74 3a 20 39 70 74 2f 31 32 70 74 20 cb ce cc e5 20 7d 0d 0a 20 20 48 31 20 7b 20 66 6f 6e 74 3a 20 31 32 70 74 2f 31 35 70 74 20 cb ce cc e5 20 7d 0d 0a 20 20 48 32 20 7b 20 66 6f 6e 74 3a 20 39 70 74 2f 31 32 70 74 20 cb ce cc e5 20 7d 0d 0a 20 20 41 3a 6c 69 6e 6b 20 7b 20 63 6f 6c 6f 72 3a 20 72 65 64 20 7d 0d 0a 20 20 41 3a 76 69 73 69 74 65 64 20 7b 20 63 6f 6c 6f 72 3a 20 6d 61 72 6f 6f 6e 20 7d 0d 0a 3c 2f 53 54 59 4c 45 3e 0d 0a 3c 2f 48 45 41 44 3e 3c 42 4f 44 59 3e 3c 54 41 42 4c 45 20 77 69 64 74 68 3d 35 30 30 20 62 6f 72 64 65 72 3d 30 20 63 65 6c 6c 73 70 61 63 69 6e 67 3d 31 30 3e 3c 54 52 3e 3c 54 44 3e 0d 0a 0d 0a 3c 68 31 3e ce de b7 a8 d5 d2 b5 bd b8 c3 d2 b3 3c 2f 68 31 3e 0d 0a c4 fa d5 fd d4 da cb d1 cb f7 b5 c4 d2 b3 c3 e6 bf c9 c4 dc d2 d1 be ad c9 be b3 fd a1 a2 b8 fc c3 fb bb f2 d4 dd ca b1 b2 bb bf c9 d3 c3 a1 a3 0d 0a 3c 68 72 3e 0d 0a 3c 70 3e c7 eb b3 a2 ca d4 d2 d4 cf c2 b2 d9 d7 f7 a3 ba 3c 2f 70 3e 0d 0a 3c 75 6c 3e 0d 0a 3c 6c 69 3e c8 b7 b1 a3 e4 af c0 c0 c6 f7 b5 c4 b5 d8 d6 b7 c0 b8 d6 d0 cf d4 ca be b5 c4 cd f8 d5 be b5 d8 d6 b7 b5 c4 c6 b4 d0 b4 ba cd b8 f1 ca bd d5 fd c8 b7 ce de ce f3 a1 a3 3c 2f 6c 69 3e 0d 0a 3c 6c 69 3e c8 e7 b9 fb cd a8 b9 fd b5 a5 bb f7 c1 b4 bd d3 b6 f8 b5 bd b4 ef c1 cb b8 c3 cd f8 d2 b3 a3 ac c7 eb d3 eb cd f8 d5 be b9 dc c0 ed d4 b1 c1 aa cf b5 a3 ac cd a8 d6 aa cb fb c3 c7 b8 c3 c1 b4 bd d3 b5 c4 b8 f1 ca bd b2 bb d5 fd c8 b7 a1 a3 0d 0a 3c 2f 6c 69 3e 0d 0a 3c 6c 69 3e b5 a5 bb f7 3c 61 20 68 72 65 66 3d 22 6a 61 76 61 73 63 72 69 70 74 3a 68 69 73 74 6f 72 79 2e 62 61 63 6b 28 31 29 22 3e ba f3 cd cb 3c 2f 61 3e b0 b4 c5 a5 b3 a2 ca d4 c1 ed d2 bb b8 f6 c1 b4 bd d3 a1 a3 3c 2f 6c 69 3e 0d 0a 3c 2f 75 6c 3e 0d 0a 3c 68 32 3e 48 54 54 50 20 b4 ed ce f3 20 34 30 34 20 2d 20 ce c4 bc fe bb f2 c4 bf c2 bc ce b4 d5 d2 b5 bd a1 a3 3c 62 72 3e 49 6e 74 65 72 6e 65 74 20 d0 c5 cf a2 b7 fe ce f1 20 28 49 49 53 29 3c 2f 68 32 3e 0d 0a 3c 68 72 3e 0d 0a 3c 70 3e bc bc ca f5 d0 c5 cf a2 a3 a8 ce aa bc bc ca f5 d6 a7 b3 d6 c8 cb d4 b1 cc e1 b9 a9 a3 a9 3c 2f 70 3e 0d 0a 3c 75 6c 3e 0d 0a 3c 6c 69 3e d7 aa b5 bd 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 67 6f 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 66 77 6c 69 6e 6b 2f 3f 6c 69 6e 6b 69 64 3d 38 31 38 30 22 3e 4d 69 63 72 6f 73 6f 66 74 20 b2 fa c6 b7 d6 a7 b3 d6 b7 fe ce f1 3c 2f 61 3e b2 a2 cb d1 cb f7 b0 fc c0 a8 26 6c 64 71 75 6f 3b 48 54 54 50 26 72 64 71 75 6f 3b ba cd 26 6c 64 71 75 6f 3b 34 30 34 26 72 64 71 75 6f 3b b5 c4 b1 ea cc e2 a1 a3 3c 2f 6c 69 3e 0d 0a 3c 6c 69 3e b4 f2 bf aa 26 6c 64 71 75 6f 3b 49 49 53 20 b0 ef d6 fa 26 72 64 71 75 6f 3b a3 a8 bf c9 d4 da 20 49 49 53 20 b9 dc c0 ed c6 f7 20 28 69 6e 65 74 6d 67 72 29 20 d6 d0 b7 c3 ce ca a3 a9 a3 ac c8 bb ba f3 cb d1 cb Data Ascii: <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><HTML><HEAD><TITLE></TITLE><META HTTP-EQUIV="Content-Type" Content="text/html; charset=GB2312"><STYLE type="text/css"> BODY { font: 9pt/12pt } H1 { font: 12pt/15pt } H2 { font: 9pt/12pt } A:link { color: red } A:visited { color: maroon }</STYLE></HEAD><BODY><TABLE width=500 border=0 cellspacing=10><TR><TD> <hr> HTTP 404 - Internet (IIS) <hr> Microsoft “HTTP”“404” “IIS ” IIS (inetmgr)

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

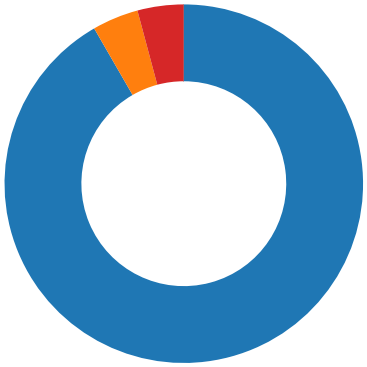
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE3
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE3
GetMessageW	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE3
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE3

Statistics

Behavior



System Behavior

Analysis Process: GRACE.exe PID: 6728 Parent PID: 5664

General

Start time:	07:57:09
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\GRACE.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\GRACE.exe'
Imagebase:	0x1e0000
File size:	3215360 bytes
MD5 hash:	9034ACBB2742281523525D715A4EE566
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.295510880.0000000004197000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.295510880.0000000004197000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.295510880.0000000004197000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.295698106.0000000004302000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.295698106.0000000004302000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.295698106.0000000004302000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6DE9CF06	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	6DE9CF06	unknown
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CEE2AB	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\GRACE.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1AC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	0	42080	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 1d 5a 8e 5a 00 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 58 00 00 00 0c 00 00 00 00 00 00 9a 77 00 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 c0 00 00 00 02 00 00 dc 8d 01 00 03 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....Z.Z.......... ....0..X...........w... ....@.. ....`................	success or wait	1	6CEE2AB	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\GRACE.exe.log	unknown	1873	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 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 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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..3,"PresentationCore, Version=	success or wait	1	6E1AC907	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	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCE1B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Copyright null 2021

Analysis Process: AddInProcess32.exe PID: 6508 Parent PID: 6728

General

Start time:	07:57:44
Start date:	27/01/2021
Path:	C:\Users\user\AppData\Local\Temp\AddInProcess32.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\AddInProcess32.exe
Imagebase:	0x8e0000
File size:	42080 bytes
MD5 hash:	F2A47587431C466535F3C3D3427724BE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.327464918.0000000000EB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.327464918.0000000000EB0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.327464918.0000000000EB0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.327302486.0000000000D80000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.327302486.0000000000D80000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.327302486.0000000000D80000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.327086258.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.327086258.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.327086258.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	419E57	NtReadFile

Analysis Process: explorer.exe PID: 3388 Parent PID: 6508

General

Start time:	07:57:49
Start date:	27/01/2021
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: netsh.exe PID: 404 Parent PID: 3388

General

Start time:	07:58:01
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\netsh.exe
Imagebase:	0x16b0000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
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: 00000011.00000002.623489927.0000000000F30000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.623489927.0000000000F30000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.623489927.0000000000F30000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000002.621878003.0000000000D00000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.621878003.0000000000D00000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.621878003.0000000000D00000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000002.623260769.0000000000E70000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.623260769.0000000000E70000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.623260769.0000000000E70000.00000040.00000001.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	D19E57	NtReadFile

Analysis Process: cmd.exe PID: 2436 Parent PID: 404

General

Start time:	07:58:07

Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Local\Temp\AddInProcess32.exe'
Imagebase:	0x1220000
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: 7040 Parent PID: 2436

General

Start time:	07:58:07
Start date:	27/01/2021
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