ID: 510295
Sample Name: T-T Swift Copy.exe
Cookbook: default.jbs
Time: 17:20:15
Date: 27/10/2021
Version: 33.0.0 White Diamond

Table of Contents

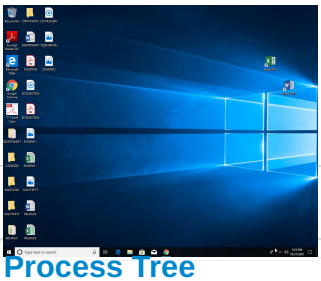
Windows Analysis Report T-T Swift Copy.exe

Overview

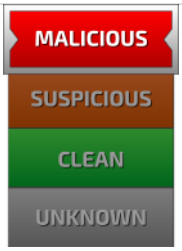
General Information

Sample Name:	T-T Swift Copy.exe
Analysis ID:	510295
MD5:	a3127d76c37d53..
SHA1:	fe6529ff5551463…
SHA256:	d9ca56d191efaa8.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



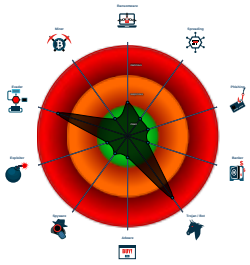
DBatLoader
FormBook

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

Signatures

- Found malware configuration
- Yara detected DBatLoader
- Yara detected FormBook
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Sigma detected: Execution from Sus…
- Maps a DLL or memory area into an…
- Writes to foreign memory regions
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Creates a thread in another existing …
- Allocates memory in foreign process…

Classification



Process Tree

- **System is w10x64**
- T-T Swift Copy.exe (PID: 5760 cmdline: 'C:\Users\user\Desktop\T-T Swift Copy.exe' MD5: A3127D76C37D53A8ECAAB821CE5D99A6)
  - mobsync.exe (PID: 5600 cmdline: C:\Windows\System32\mobsync.exe MD5: 44C19378FA529DD88674BAF647EBDC3C)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - Bukgwo.exe (PID: 5708 cmdline: 'C:\Users\Public\Libraries\Bukgwo\Bukgwo.exe' MD5: A3127D76C37D53A8ECAAB821CE5D99A6)
      - Bukgwo.exe (PID: 5060 cmdline: 'C:\Users\Public\Libraries\Bukgwo\Bukgwo.exe' MD5: A3127D76C37D53A8ECAAB821CE5D99A6)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.ehawkstech.com/s4mt/"
  ],
  "decoy": [
    "deviousrofwft.xyz",
    "iphone13.photos",
    "cameraderie.info",
    "flogotwheelz.com",
    "lunasconstructionllc.com",
    "unameofficial.com",
    "digitalboat.cloud",
    "hifi-cans.com",
    "breskizci.com",
    "kyleandconner.com",
    "punnyaseva.com",
    "elitephotoedit.com",
    "pizzatallrikar.one",
    "espacio40.com",
    "bvgsf.xyz",
    "splootingcorgi.com",
    "metaverse360.biz",
    "xnegbuy.com",
    "buysubarus.com",
    "optophonia.com",
    "jingcai16.com",
    "verdantpor.xyz",
    "mandyfarricker.com",
    "affiliategang.com",
    "chemissimo.com",
    "myspecialgift4you.com",
    "21cfintech.com",
    "parsvivid.com",
    "ufabetkhmer.net",
    "litunity.com",
    "bcwis.com",
    "ekokosiarki.com",
    "expocanna.net",
    "shanichara.com",
    "brightstarlogisticss.com",
    "intaom.net",
    "petshop.zone",
    "habxgg.com",
    "taiqen.com",
    "vehiculosvivienda.com",
    "igsc-eg.com",
    "jfhy88.com",
    "circuspolitician.com",
    "etxperiodontics.com",
    "wsxkd.com",
    "abosasaio.com",
    "magnacursos.online",
    "indigenousjobs.net",
    "digital904.com",
    "pp-jm.com",
    "hkqlxc.com",
    "mygutimautpribuinrop.com",
    "cosplayharem.com",
    "jsxybq.com",
    "fieldstationlodges.com",
    "ggrow-hairsalon.com",
    "aureliemorgane.com",
    "yian-ho.com",
    "woruke.club",
    "meet-hamburg.com",
    "leadergaterealty.com",
    "choitokki.com",
    "cfweb.tools",
    "loveyopu.com"
  ]
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\Public\Libraries\owgkuB.url	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x14:$file: URL= • 0x0:$url_explicit: [InternetShortcut]

Memory Dumps

Source	Rule	Description	Author	Strings
00000012.00000000.522824405.000000000DDB9000.00000004.00000001.sdmp	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x1d44:$file: URL= • 0x1d30:$url_explicit: [InternetShortcut]
00000015.00000002.520675116.00000000021A0000.00000004.00000001.sdmp	JoeSecurity_DBatLoader	Yara detected DBatLoader	Joe Security	
00000012.00000000.476572869.0000000006D0E000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000012.00000000.476572869.0000000006D0E000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x46a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x4191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x47a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000012.00000000.476572869.0000000006D0E000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x6ac9:$sqlite3step: 68 34 1C 7B E1 • 0x6bdc:$sqlite3step: 68 34 1C 7B E1 • 0x6af8:$sqlite3text: 68 38 2A 90 C5 • 0x6c1d:$sqlite3text: 68 38 2A 90 C5 • 0x6b0b:$sqlite3blob: 68 53 D8 7F 8C • 0x6c33:$sqlite3blob: 68 53 D8 7F 8C
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
17.0.mobsync.exe.72480000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
17.0.mobsync.exe.72480000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18d97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
17.0.mobsync.exe.72480000.1.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15cc9:$sqlite3step: 68 34 1C 7B E1 • 0x15ddc:$sqlite3step: 68 34 1C 7B E1 • 0x15cf8:$sqlite3text: 68 38 2A 90 C5 • 0x15e1d:$sqlite3text: 68 38 2A 90 C5 • 0x15d0b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e33:$sqlite3blob: 68 53 D8 7F 8C
17.0.mobsync.exe.72480000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
17.0.mobsync.exe.72480000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b97:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Sigma Overview

System Summary:

Sigma detected: Execution from Suspicious Folder

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected FormBook

Multi AV Scanner detection for dropped file

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Yara detected DBatLoader

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Writes to foreign memory regions

Creates a thread in another existing process (thread injection)

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

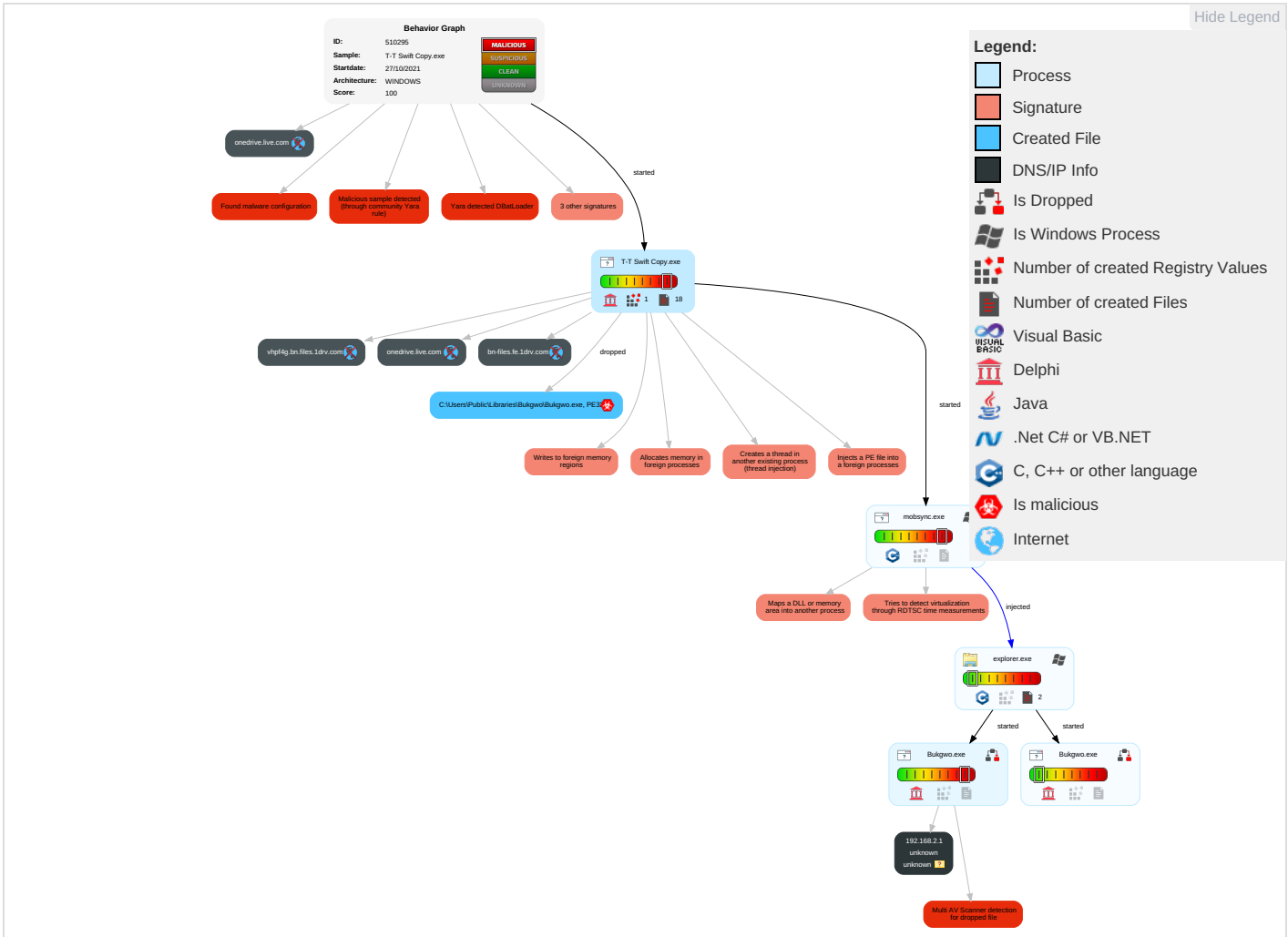
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Registry Run Keys / Startup Folder 1	Process Injection 5 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 1	Eavesdrop Insecure Network Communi
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Virtualization/Sandbox Evasion 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1 1	Exploit SS Redirect F Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 5 1 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	System Information Discovery 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communi
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service

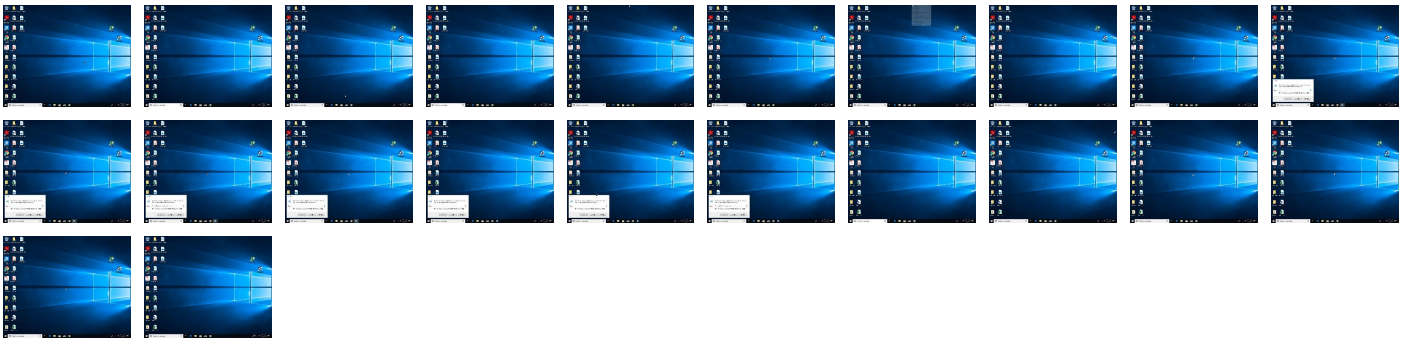
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\Libraries\Bukgwo\Bukgwo.exe	39%	ReversingLabs	Win32.Backdoor.Remcos	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
21.3.Bukgwo.exe.21fcb70.1557.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234e668.3796.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234cb70.2290.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.3.Bukgwo.exe.270c48c.187.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234e89c.3939.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234ef08.4348.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21f9a40.836.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234cb70.1731.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234cb70.2886.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21fcb70.2092.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234993c.706.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234cb70.3308.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21fcb70.435.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234cb70.2510.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234cb70.1025.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234ecb0.4200.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21fcb70.1813.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.3.Bukgwo.exe.270cb70.877.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21f9bec.1049.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21fd9d0.333.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234cb70.2924.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234cb70.2871.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21f9740.451.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234cb70.1001.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234d76c.129.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21f97ec.538.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21fcb70.1018.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21f9720.436.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234cb70.3022.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234cb70.1818.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21fcb70.486.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234cb70.2481.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21fcb70.507.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.23496fc.417.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234cb70.3430.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21f9830.572.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234e998.4002.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234cb70.3051.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21fcb70.2113.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234cb70.2939.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.3.Bukgwo.exe.270cb70.1666.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.3.Bukgwo.exe.27097f8.543.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21fcb70.1307.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234cb70.669.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21fcb70.1149.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21fcb70.2068.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21fcb70.1491.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234cb70.2749.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234b144.3782.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21fd9e8.341.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.3.Bukgwo.exe.2709984.741.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.3.Bukgwo.exe.270991c.690.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234cb70.2088.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234cb70.1477.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21fcb70.1993.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21fa274.1885.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234cb70.3470.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21fcb70.2192.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21fcb70.2088.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21fa390.2027.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.3.Bukgwo.exe.2709c5c.1105.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21f8574.43.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.3.Bukgwo.exe.270cb70.1360.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234a170.1756.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
21.3.Bukgwo.exe.21fcb70.2295.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234cb70.2011.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.2349e60.1364.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21f98b4.637.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234cb70.2442.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234cb70.2169.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21f955c.268.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21fcb70.2293.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234ad9c.234.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234e5a8.3748.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21f9e74.1374.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.3.Bukgwo.exe.2709e68.1368.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234e5b4.3753.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234cb70.2250.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21f9798.495.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.3.Bukgwo.exe.270cb70.1647.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.2349b40.963.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.2349e30.1340.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234c6cc.250.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.2349934.701.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234cb70.492.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.3.Bukgwo.exe.2709f44.1478.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.3.Bukgwo.exe.270cb70.1594.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21f96fc.418.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21f9fdc.1553.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234d8bc.241.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.2349880.611.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234e5e4.3765.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234a168.1752.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21fcb70.1093.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21f9898.623.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.23497c4.518.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.3.Bukgwo.exe.21fcb70.2079.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.234ef68.4374.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.T-T Swift Copy.exe.2349c00.1060.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.3.Bukgwo.exe.270a0ec.1689.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.ehawkstech.com/s4mt/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
onedrive.live.com	unknown	unknown	false		high
vhpf4g.bn.files.1drv.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.ehawkstech.com/s4mt/	true	• Avira URL Cloud: safe	low

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	510295
Start date:	27.10.2021
Start time:	17:20:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 19m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	T-T Swift Copy.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:	25
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@6/3@4/1
EGA Information:	Failed
HDC Information:	Failed
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

Simulations

Behavior and APIs

Time	Type	Description
17:22:23	API Interceptor	1x Sleep call for process: T-T Swift Copy.exe modified
17:22:29	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Bukgwo C:\Users\Public\Libraries\\owgkuB.url
17:22:37	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Bukgwo C:\Users\Public\Libraries\\owgkuB.url

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\Public\Libraries\Bukgwo\Bukgwo.exe	
Process:	C:\Users\user\Desktop\T-T Swift Copy.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1052672
Entropy (8bit):	7.030914360244136
Encrypted:	false
SSDEEP:	24576:6BMjoRADI2bZ77GjLkEg/0EZcN+fBPLtUqU9PPj2hqp8Zs7SZxD95UCcoyRcRCdS:6BMjVRGZg/0EZcN+fBPLtUqU9PPj2Apg
MD5:	A3127D76C37D53A8ECAAB821CE5D99A6
SHA1:	FE6529FF55514634D6CDE730E4C4C5B664B02CCF
SHA-256:	D9CA56D191EFAA8AC5BEEE52F508082D6E8EFB29045BB61C23851537982FA6BF
SHA-512:	503FB1825DEC1A108B4C307E561FB4DF829079BF53DEC6167B28A0C79D3DA81D188439EBD5590CA2AD24A528D1C63E4DBEAEECD516BE5665866BDC1F07D3ED0
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 39%
Reputation:	unknown
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....@.....@.....$%.....0..... ....CODE..... ..`DATA....,.....@...BSS.....i.....idata..$%.....&.....@....tls....@.....rdata..... .....@..P.reloc.....0.....@..P.rsrc.....f.....@..P.....@..P..... .....

C:\Users\Public\Libraries\owgkuB.url	
Process:	C:\Users\user\Desktop\T-T Swift Copy.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<file:"C:\\Users\\Public\\Libraries\\\\Bukgwo\\Bukgwo.exe">), ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	96
Entropy (8bit):	4.851591375784615
Encrypted:	false
SSDEEP:	3:HRAbABGQYmTWAX+rSF55i0XMLQtSiL3bsGKd4ovn:HRYFVmTWDyzSQgiL3bsblvn
MD5:	FDC2ECE626A79B30C114488195904125
SHA1:	0E282FA6243F23E1388E1711A43D3F4033EDFD9F
SHA-256:	23976F3C585AEF6EAEE80D2FF579B4114B06766A101F1A0788CD0E129FEBF84E
SHA-512:	6E549209E2D5B7BC6089E8EEDD11C482E62A5D12C08A60A5B075FB3E8EC8449DD86C406D6892FDC19265B557A6C42DC52F07EDAC3D2804DCBF97777940D22F9
Malicious:	false
Yara Hits:	• Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\Public\Libraries\owgkuB.url, Author: @itsreallynick (Nick Carr)
Reputation:	unknown

C:\Users\Public\Libraries\owgkuB.url	
Preview:	[InternetShortcut]..URL=file:"C:\\Users\\Public\\Libraries\\\\Bukgwo\\Bukgwo.exe"..IconIndex=0..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PEJLKQA8\Bukgwonqgngtrpkjastfgihmnxlmffz[2]	
Process:	C:\Users\user\Desktop\T-T Swift Copy.exe
File Type:	data
Category:	dropped
Size (bytes):	275456
Entropy (8bit):	**7.995996090484397**
Encrypted:	**true**
SSDEEP:	6144:eLRxllE7ow8bOFy5f0iAlZZ1CJWS5vg0GNwcNsoS58ErglehivLUHEJH:6zM0w8bl5siAlBCJWS5vWNwCxGg4ivLJ
MD5:	00BF4E71F9A6ECAD41587045D5591BE4
SHA1:	DAC3E45F849E280ABDEECB0010F71DB7FB92F68C
SHA-256:	D8C8989468B6EE8526A595B49DE36162DB5C6DE86DA9236529763AE16D0AE7C6
SHA-512:	E129420478F27FD888AC6821848C64BC332446B284021B1725702846F134202AB4C6197C1BBFEB20520FC1923169D933CE4652027FF7E20D4E9C5ACE967AB52B
Malicious:	false
Reputation:	unknown
Preview:	..@5...q.P.Yf..MD0....QJ.-..!...o....y9.{-..!...G.^..>..J..'.E.d.IQ@.....A..3....T.. `.V....o}X...X...).....v....E..E.Q}83..j...d.$m.FR.?....L.....af...:6;.&m&l.h.o.O!.....T..&.~.,.@("Yr.#..~.*v..u...J.Kid.L.....af...:6;.&m&l.h.o.O!.....T..&.~.,.@(]....0....%.....>.z'..7I...xP..;lM..... .T.4....a..b%{.N.l....*.I].#..h...9._Ua..s.`.[V...."..........F]..,'J.u..J...V.B3...j.=..g..=..[w..c.....f..#.4G.)..1.sL.....Cc.P....?{.6..&.K.d8.....(.S.+.W.....5J...,.w.m..`!5...M..zq..rB.Y.....m.....)D.~y.;pK.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.030914360244136
TrID:	• Win32 Executable (generic) a (10002005/4) 99.24% • InstallShield setup (43055/19) 0.43% • Win32 Executable Delphi generic (14689/80) 0.15% • Windows Screen Saver (13104/52) 0.13% • Win16/32 Executable Delphi generic (2074/23) 0.02%
File name:	T-T Swift Copy.exe
File size:	1052672
MD5:	a3127d76c37d53a8ecaab821ce5d99a6
SHA1:	fe6529ff55514634d6cde730e4c4c5b664b02ccf
SHA256:	d9ca56d191efaa8ac5beee52f508082d6e8efb29045bb61c23851537982fa6bf
SHA512:	503fb1825dec1a108b4c307e561fb4df829079bf53dec6167b28a0c79d3da81d188439ebd5590ca2ad24a528d1c63e4dbeaeecd516be5665866bdc1f07d3e2d0
SSDEEP:	24576:6BMjoRADI2bZ77GjLkEg/0EZcN+fBPLtUqU9PPj2hqp8Zs7SZxD95UCcoyRcRCdS:6BMjVRGZg/0EZcN+fBPLtUqU9PPj2Apg
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... ....

File Icon

Icon Hash:	252506584c9731c0

Static PE Info

General

Entrypoint:	0x490218
Entrypoint Section:	CODE
Digitally signed:	false
Imagebase:	0x400000

General

Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	c615e590ab9a424646aba34bad72f321

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
CODE	0x1000	0x8f29c	0x8f400	False	0.519360820244	data	6.57636511075	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
DATA	0x91000	0x5a82c	0x5aa00	False	0.421761853448	data	6.88948982392	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
BSS	0xec000	0x1269	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0xee000	0x2524	0x2600	False	0.362356085526	data	4.99675959328	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0xf1000	0x40	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0xf2000	0x18	0x200	False	0.05078125	data	0.199107517787	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0xf3000	0x9ba8	0x9c00	False	0.571890024038	data	6.65385066773	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0xfd000	0xaa00	0xaa00	False	0.274057904412	data	4.57303719616	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Network Port Distribution

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 27, 2021 17:22:23.840656042 CEST	192.168.2.5	8.8.8.8	0xc540	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Oct 27, 2021 17:22:24.971437931 CEST	192.168.2.5	8.8.8.8	0xd0ee	Standard query (0)	vhpf4g.bn.files.1drv.com	A (IP address)	IN (0x0001)
Oct 27, 2021 17:23:29.635649920 CEST	192.168.2.5	8.8.8.8	0x1701	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Oct 27, 2021 17:23:29.640189886 CEST	192.168.2.5	8.8.8.8	0x501	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 27, 2021 17:22:23.881091118 CEST	8.8.8.8	192.168.2.5	0xc540	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Oct 27, 2021 17:22:25.050039053 CEST	8.8.8.8	192.168.2.5	0xd0ee	No error (0)	vhpf4g.bn.files.1drv.com	bn-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Oct 27, 2021 17:22:25.050039053 CEST	8.8.8.8	192.168.2.5	0xd0ee	No error (0)	bn-files.fe.1drv.com	odc-bn-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Oct 27, 2021 17:23:29.654856920 CEST	8.8.8.8	192.168.2.5	0x1701	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Oct 27, 2021 17:23:29.695108891 CEST	8.8.8.8	192.168.2.5	0x501	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: T-T Swift Copy.exe PID: 5760 Parent PID: 2212

General

Start time:	17:21:10
Start date:	27/10/2021
Path:	C:\Users\user\Desktop\T-T Swift Copy.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\T-T Swift Copy.exe'
Imagebase:	0x400000
File size:	1052672 bytes
MD5 hash:	A3127D76C37D53A8ECAAB821CE5D99A6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: mobsync.exe PID: 5600 Parent PID: 5760

General

Start time:	17:22:28
Start date:	27/10/2021
Path:	C:\Windows\SysWOW64\mobsync.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\mobsync.exe
Imagebase:	0x1080000
File size:	93184 bytes
MD5 hash:	44C19378FA529DD88674BAF647EBDC3C
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: 00000011.00000000.406123178.0000000072480000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000000.406123178.0000000072480000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000000.406123178.0000000072480000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000000.407026308.0000000072480000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000000.407026308.0000000072480000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000000.407026308.0000000072480000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000000.406606133.0000000072480000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000000.406606133.0000000072480000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000000.406606133.0000000072480000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000000.405354552.0000000072480000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000000.405354552.0000000072480000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000000.405354552.0000000072480000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3472 Parent PID: 5600

General

Start time:	17:22:31
Start date:	27/10/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: 00000012.00000000.522824405.000000000DDB9000.00000004.00000001.sdmp, Author: @itsreallynick (Nick Carr) • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000012.00000000.476572869.0000000006D0E000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000012.00000000.476572869.0000000006D0E000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000012.00000000.476572869.0000000006D0E000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: Bukgwo.exe PID: 5708 Parent PID: 3472

General

Start time:	17:22:37
Start date:	27/10/2021
Path:	C:\Users\Public\Libraries\Bukgwo\Bukgwo.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\Libraries\Bukgwo\Bukgwo.exe'
Imagebase:	0x400000
File size:	1052672 bytes
MD5 hash:	A3127D76C37D53A8ECAAB821CE5D99A6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000015.00000002.520675116.00000000021A0000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 39%, ReversingLabs
Reputation:	low

Analysis Process: Bukgwo.exe PID: 5060 Parent PID: 3472

General

Start time:	17:22:46
Start date:	27/10/2021
Path:	C:\Users\Public\Libraries\Bukgwo\Bukgwo.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\Libraries\Bukgwo\Bukgwo.exe'
Imagebase:	0x7ff7e2800000
File size:	1052672 bytes
MD5 hash:	A3127D76C37D53A8ECAAB821CE5D99A6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000018.00000002.521099997.00000000026B0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis