ID: 680524
Sample Name: Packing list.exe
Cookbook: default.jbs
Time: 18:32:06
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

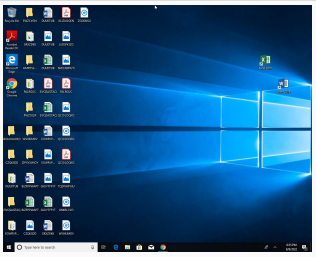
Windows Analysis Report

Packing list.exe

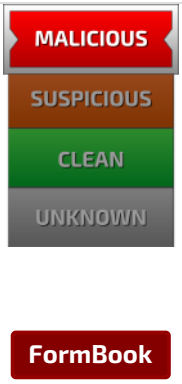
Overview

General Information

Sample Name:	Packing list.exe
Analysis ID:	680524
MD5:	c7a4e2993e53b7..
SHA1:	c5cc5b995685cf…
SHA256:	2698f26bc94c6e…
Tags:	exe Formbook
Infos:	



Detection



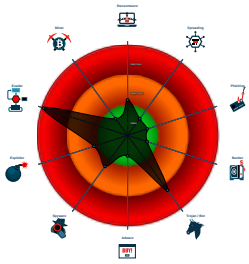
FormBook

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Yara detected AntiVM3
- System process connects to networ…
- Antivirus detection for URL or domain
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- Injects a PE file into a foreign proce…
- .NET source code contains method …

Classification



Process Tree

- **System is w10x64**
- Packing list.exe (PID: 6064 cmdline: "C:\Users\user\Desktop\Packing list.exe" MD5: C7A4E2993E53B71353110DEBF193F711)
  - schtasks.exe (PID: 6020 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\jcWxLdFqdoHatB" /XML "C:\Users\user\AppData\Local\Temp\tmp7D6D.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5788 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Packing list.exe (PID: 1320 cmdline: {path} MD5: C7A4E2993E53B71353110DEBF193F711)
    - explorer.exe (PID: 684 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - raserver.exe (PID: 3856 cmdline: C:\Windows\SysWOW64\raserver.exe MD5: 2AADF65E395BFBD0D9B71D7279C8B5EC)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.pahunt.org/umhl/"
  ],
  "decoy": [
    "mB8gvYWKNnd+6kcRK8M=",
    "7zn0DtefQVZc3UcRK8M=",
    "qj9AgFfem/K5",
    "7W+k2buMQnZxzkqW8v2wDA==",
    "BXmNsJSLLt9UZYuO3C2l",
    "PHnylup3Ec5YTj8qPV+8",
    "5wuv0g7RYfoLhg==",
    "qy3Wf2Qv9yamjg==",
    "EWjULZ91La2UEjQ=",
    "aN2KCV/tiOP2gyVROJbK2Fg=",
    "a9tVEduGJF1q4GcHnr2dBg==",
    "111flmRlGlRY0vPmzRR63KW1wyqR6Q==",
    "f7+r8NeWp+WZYf6D8v2wDA==",
    "LGG2X0VJ1rSPHL0Yd/60",
    "A21qVr1P5aZSS/pCOZbK2Fg=",
    "W7uNpIBT4NZ+WoHtRGa+",
    "YpWyeGx/Qx22izPhZenb5O65",
    "xPm54b/IeWRI4IYqPV+8",
    "gtxoMfmYZ0HgmQ==",
    "LMlLAuXndyCmnEXPMpdwBwxB0g==",
    "siWU81PxsC+0oEWT8v2wDA==",
    "ks2JuqR+Kkb324cqPV+8",
    "7CHy2pNs9fzthn43",
    "uTnZelYp9yamjg==",
    "FYR8ZtIuEACu",
    "QV+IJwsM0kTK+2oVgQ==",
    "I60qeTRmGDxa4UcRK8M=",
    "bI7FSA8iSlsh0IMkgw==",
    "fPDj0E0bvTlUwOLGFVq2",
    "oOS6vYWSNl3Gn4c1",
    "MMijCmIt6ShS2/7z4Dvb5O65",
    "hMS597ZZ/MZLKR7nZ54/kNuz",
    "K2nSnIFmKWqgHFcyv/imbncPSqo=",
    "4Xb7v/PEdz7Y+2oVgQ==",
    "Vt2QCbF0aJ4=",
    "m9VmkEwbxnIa/p3YBFc98Gux",
    "Q7lAGwwBhTLthn43",
    "DlGQCZkaysdZJh8yWdKN6m+x",
    "CF0uM/wT2M7JHzQqPV+8",
    "1wevt3hI3tPaR2ozyQe1it7fHPg/eczb",
    "qxcRVQuWHw1MKdA4",
    "dMADqcZ+K4I=",
    "H3ZFO+VrJQ6lnpmPa5bK2Fg=",
    "I2NcqXM1zEPK+2oVgQ==",
    "XoQXQA0PxDRI+2oVgQ==",
    "9VDJi2RwODvp3Hz5d+nb5O65",
    "H4PEOo8dwjlj9KRE8v2wDA==",
    "fq1yc81rHThNtiRPOJbK2Fg=",
    "90u1gKqiSJc=",
    "HnInjdeMNq2UEjQ=",
    "3O7PDrhF5tWQl8Iwiw==",
    "AXuXhUUotKqgEHuvpP/GHaUbXbTp8o5Lpg==",
    "edtWHfXmei7thn43",
    "1vdgIc5iAGSI60cRK8M=",
    "sj5/NqAuEACu",
    "dpQOonl8Rr7LGTZGYZX9RTsVSrM=",
    "rt0X7dDlpHsQFcJC8v2wDA==",
    "+nf/2b/GeGL/AHBFB0erBoHNITKM4Q==",
    "MLMz38fRYBvGpEWX8v2wDA==",
    "I186c0wbqBqOlnEPXsSi6j64nGru",
    "CipT7MK3Xrk2U7YQJHvxBA==",
    "2k/ZrIpV38eJR3Au",
    "83OJo30uEACu",
    "yva3tQ7Zsm36/6Qbgtk8EOkFF2SA6Q=="
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000013.00000002.682502518.0000000002FD0000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000013.00000002.682502518.0000000002FD0000.00000040.10000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x65f1:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1e1b0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xa90f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x17307:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000013.00000002.682502518.0000000002FD0000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x17105:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x16bb1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x17207:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1737f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa4da:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x15dcc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb222:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ce07:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1df1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000013.00000002.682502518.0000000002FD0000.00000040.10000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x19829:$sqlite3step: 68 34 1C 7B E1 • 0x1995c:$sqlite3step: 68 34 1C 7B E1 • 0x1986b:$sqlite3text: 68 38 2A 90 C5 • 0x199b3:$sqlite3text: 68 38 2A 90 C5 • 0x19882:$sqlite3blob: 68 53 D8 7F 8C • 0x199d5:$sqlite3blob: 68 53 D8 7F 8C
00000013.00000002.679680318.0000000000600000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 27 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.0.Packing list.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
8.0.Packing list.exe.400000.0.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x57f1:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1d3b0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x9b0f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x16507:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
8.0.Packing list.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x16305:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15db1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x16407:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1657f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x96da:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x14fcc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa422:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1c007:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1d11a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
8.0.Packing list.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18a29:$sqlite3step: 68 34 1C 7B E1 • 0x18b5c:$sqlite3step: 68 34 1C 7B E1 • 0x18a6b:$sqlite3text: 68 38 2A 90 C5 • 0x18bb3:$sqlite3text: 68 38 2A 90 C5 • 0x18a82:$sqlite3blob: 68 53 D8 7F 8C • 0x18bd5:$sqlite3blob: 68 53 D8 7F 8C

Source	Rule	Description	Author	Strings
0.2.Packing list.exe.33f638c.1.raw.unpack	INDICATOR_SUSPICIOUS_DisableWinDefender	Detects executables containing artifcats associated with disabling Widnows Defender	ditekSHen	• 0xcdec:$reg1: SOFTWARE\Microsoft\Windows Defender\Features • 0xce30:$reg2: SOFTWARE\Policies\Microsoft\Windows Defender • 0xce78:$reg2: SOFTWARE\Policies\Microsoft\Windows Defender • 0xd104:$s1: Set-MpPreference -SignatureDisableUpdateOnStartupWithoutEngine $true • 0xd168:$s2: Set-MpPreference -DisableArchiveScanning $true • 0xd1c0:$s3: Set-MpPreference -DisableIntrusionPreventionSystem $true • 0xd218:$s4: Set-MpPreference -DisableScriptScanning $true • 0xd264:$s5: Set-MpPreference -SubmitSamplesConsent 2 • 0xd2a4:$s6: Set-MpPreference -MAPSReporting 0 • 0xd2f0:$s7: Set-MpPreference -HighThreatDefaultAction 6 • 0xd348:$s8: Set-MpPreference -ModerateThreatDefaultAction 6 • 0xd398:$s9: Set-MpPreference -LowThreatDefaultAction 6 • 0xd3e8:$s10: Set-MpPreference -SevereThreatDefaultAction 6

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

Data Obfuscation

.NET source code contains method to dynamically call methods (often used by packers)

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection

Deletes itself after installation

Malware Analysis System Evasion

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information

Yara detected FormBook

Remote Access Functionality

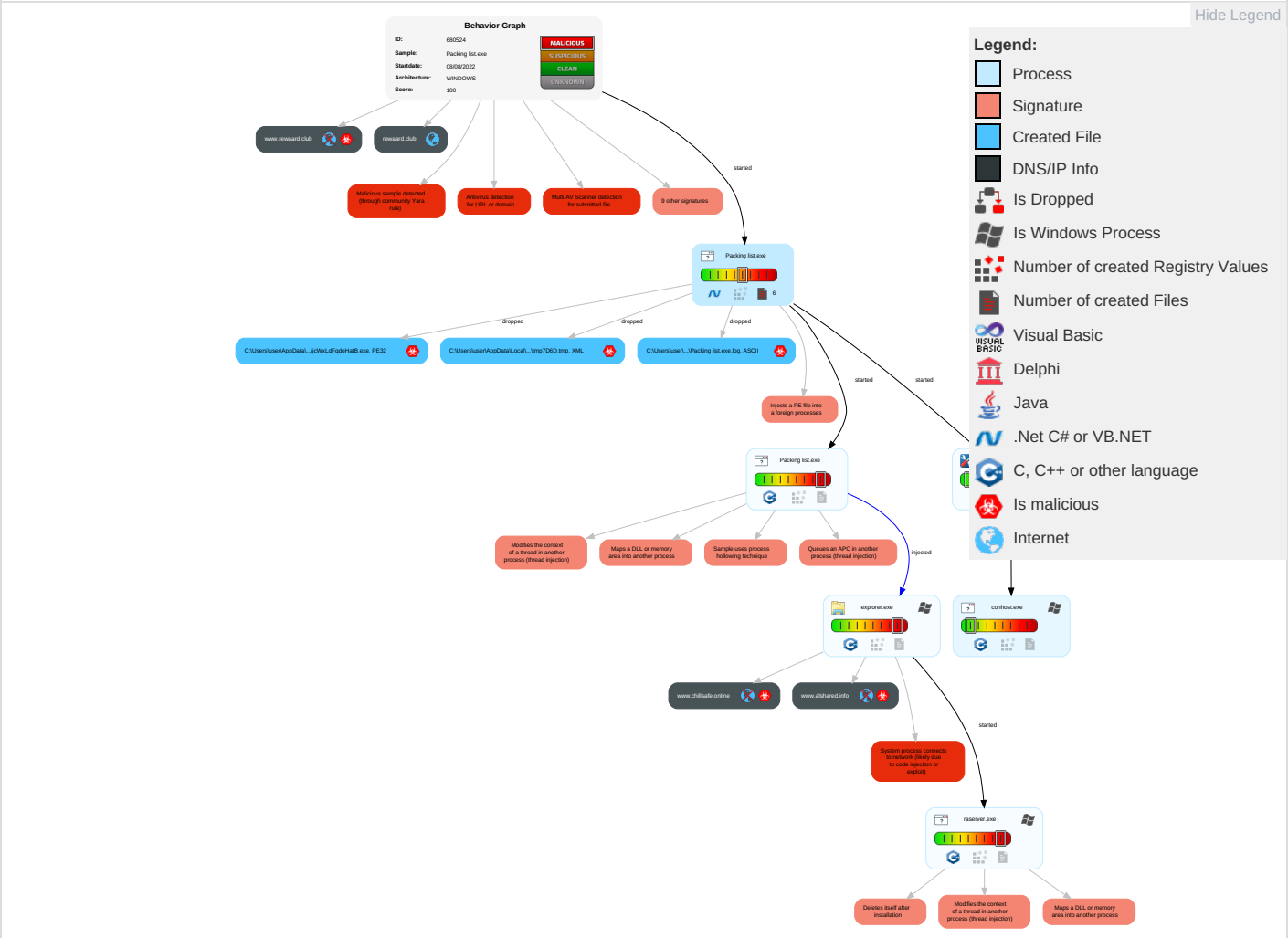
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Command and Scripting Interpreter	1 Scheduled Task/Job	6 1 2 Process Injection	1 Masquerading	1 Input Capture	1 2 1 Security Software Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Shared Modules	Logon Script (Windows)	Logon Script (Windows)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	6 1 2 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	4 Obfuscated Files or Information	Cached Domain Credentials	1 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 File Deletion	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

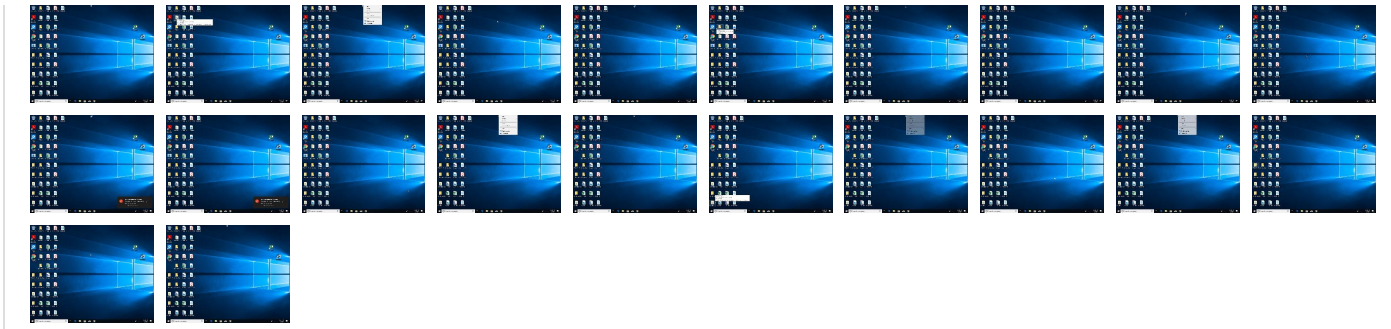
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Packing list.exe	44%	Virustotal		Browse
Packing list.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\jcWxLdFqdoHatB.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.0.Packing list.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnx	0%	Avira URL Cloud	safe	
http://www.carterandcone.comRes	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.comlic	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.carterandcone.coma-dY	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn$	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.comC	0%	Avira URL Cloud	safe	
www.pahunt.org/umhl/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
rewaard.club	185.192.114.83	true	false		unknown
www.chillsafe.online	unknown	unknown	true		unknown
www.rewaard.club	unknown	unknown	true		unknown
www.alshared.info	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.pahunt.org/umhl/	true	• Avira URL Cloud: malware	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	Packing list.exe, 00000000.00000003.4174 39081.0000000006106000.00000004.00000800 .00020000.00000000.sdmp, Packing list.exe, 0000000 0.00000002.471132417.00000000073F2000.00 000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Packing list.exe, 00000000.00000002.4711 32417.00000000073F2000.00000004.00000800 .00020000.00000000.sdmp, Packing list.exe, 0000000 0.00000003.456872900.0000000006100000.00 000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	Packing list.exe, 00000000.00000002.4711 32417.00000000073F2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/	Packing list.exe, 00000000.00000003.4242 93456.0000000006102000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	Packing list.exe, 00000000.00000002.4711 32417.00000000073F2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Packing list.exe, 00000000.00000002.4711 32417.00000000073F2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Packing list.exe, 00000000.00000002.4711 32417.00000000073F2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.zhongyicts.com.cnx	Packing list.exe, 00000000.00000003.4174 39081.0000000006106000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comRes	Packing list.exe, 00000000.00000003.4176 13150.0000000006106000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	Packing list.exe, 00000000.00000002.4711 32417.00000000073F2000.00000004.00000800 .00020000.00000000.sdmp, Packing list.exe, 0000000 0.00000003.417883204.0000000006103000.00 000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comlic	Packing list.exe, 00000000.00000003.4178 83204.0000000006103000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Packing list.exe, 00000000.00000002.4711 32417.00000000073F2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	Packing list.exe, 00000000.00000002.4711 32417.00000000073F2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	Packing list.exe, 00000000.00000003.4176 13150.0000000006106000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	Packing list.exe, 00000000.00000002.4711 32417.00000000073F2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	Packing list.exe, 00000000.00000002.4711 32417.00000000073F2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coma-dY	Packing list.exe, 00000000.00000003.4176 13150.0000000006106000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/	Packing list.exe, 00000000.00000003.4170 47585.0000000006105000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	Packing list.exe, 00000000.00000002.4711 32417.00000000073F2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Packing list.exe, 00000000.00000002.4711 32417.00000000073F2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Packing list.exe, 00000000.00000002.4711 32417.00000000073F2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Packing list.exe, 00000000.00000002.4711 32417.00000000073F2000.00000004.00000800 .00020000.00000000.sdmp, Packing list.exe, 0000000 0.00000003.424293456.0000000006102000.00 000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Packing list.exe, 00000000.00000002.4711 32417.00000000073F2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	Packing list.exe, 00000000.00000002.4711 32417.00000000073F2000.00000004.00000800 .00020000.00000000.sdmp, Packing list.exe, 0000000 0.00000003.417011575.000000000610B000.00 000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Packing list.exe, 00000000.00000002.4711 32417.00000000073F2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.zhongyicts.com.cn$	Packing list.exe, 00000000.00000003.4174 39081.0000000006106000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/	Packing list.exe, 00000000.00000002.4711 32417.00000000073F2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.como	Packing list.exe, 00000000.00000003.4568 72900.0000000006100000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Packing list.exe, 00000000.00000002.4711 32417.00000000073F2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cno.	Packing list.exe, 00000000.00000003.4174 39081.0000000006106000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Packing list.exe, 00000000.00000002.4711 32417.00000000073F2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.fonts.com	Packing list.exe, 00000000.00000002.4711 32417.00000000073F2000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Packing list.exe, 00000000.00000002.4711 32417.00000000073F2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Packing list.exe, 00000000.00000002.4711 32417.00000000073F2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Packing list.exe, 00000000.00000003.4174 39081.0000000006106000.00000004.00000800 .00020000.00000000.sdmp, Packing list.exe, 0000000 0.00000002.471132417.00000000073F2000.00 000004.00000800.00020000.00000000.sdmp, Packing list.exe, 00000000.00000003.4176 13150.0000000006106000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Packing list.exe, 00000000.00000002.4590 45143.00000000033B1000.00000004.00000800 .00020000.00000000.sdmp	false		high
http://www.sakkal.com	Packing list.exe, 00000000.00000002.4711 32417.00000000073F2000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comC	Packing list.exe, 00000000.00000003.4568 72900.0000000006100000.00000004.00000800 .00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

⊘ **No contacted IP infos**

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680524
Start date and time: 08/08/202218:32:06	2022-08-08 18:32:06 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Packing list.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:	24
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@7/3@3/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 59.4% (good quality ratio 51.7%) • Quality average: 71.6% • Quality standard deviation: 33.4%
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, client.wns.windows.com, licensing.mp.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:33:20	API Interceptor	1x Sleep call for process: Packing list.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\Packing list.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp7D6D.tmp

Process:	C:\Users\user\Desktop\Packing list.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1651
Entropy (8bit):	5.17949713007774
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKButn:cbhC7ZlNQF/rydbz9l3YODOLNdq3W
MD5:	6527089BACCDC5417F25E75F643B1384
SHA1:	5DC2EEC38E431AAD51106626913E4AD0D74D241F
SHA-256:	661A8DEBE0FB8BCB91202D6806C30BE748E69709EC0C57FDC4D992CB855687D4
SHA-512:	4D238245D556825E9CAE02EE2712C82CEB9819EC4F062C437CB1BB8349AF1AF895D921E73D91CBDDEC66047852DA4C87B83F06C0418EFA77FC28D6354758C89
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

C:\Users\user\AppData\Roaming\jcWxLdFqdoHatB.exe

Process:	C:\Users\user\Desktop\Packing list.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	866816
Entropy (8bit):	7.774266041426872
Encrypted:	false
SSDEEP:	12288:Py5/O6uz02iN2SeIo4D6KftU7+ZbWLlbjskXIdpcum3FO9m/8UgxBzifEBJw87o:PIWE18SeWOKft2lJbPQcnM68UmXo
MD5:	C7A4E2993E53B71353110DEBF193F711

SHA1:	C5CC5B995685CF3474D0998DC8F8BE0080635F2C
SHA-256:	2698F26BC94C6EE64DD216F13C805F6A2EE512C47F1A23F026DD606ADC42FCB9
SHA-512:	B657DCF76D2BBEFB933738E61948886DBA367AAF8DF226175114C8261580C2AA6D821E93F1F9FF56740825B683403A5726681202B535E7D010A240972A361819
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....P..0.....N... ...`....@.. ..@.....hN..O...`..... ....H.....text..... ...0..... ..`.rsrc.....`.....2.....@..@.rel oc.....8.....@..B.....N.....H.....8~..XH.....(...*&..(!...*.s".....s#.....s$.....s%.....s&.....*...0.....~....o'....+.. *.0.....~....o(....+..*.0.....~....o)....+..*.0.....~....o*....+..*.0.....~....o+....+..*.0..<.....~.....(,.....!r...p.....(-...o....s/.....~.....+..*.0.....~.....+..*"".....*.0..&..... (....r5..p~....o0...(1.....t$....+..*...0..&.....(....rC..p~....o0...(1.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.774266041426872
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Packing list.exe
File size:	866816
MD5:	c7a4e2993e53b71353110debf193f711
SHA1:	c5cc5b995685cf3474d0998dc8f8be0080635f2c
SHA256:	2698f26bc94c6ee64dd216f13c805f6a2ee512c47f1a23f026dd606adc42fcb9
SHA512:	b657dcf76d2bbefb933738e61948886dba367aaf8df226175114c8261580c2aa6d821e93f1f9ff56740825b683403a5726681202b535e7d010a240972a361819
SSDEEP:	12288:Py5/O6uz02iN2SeIo4D6KftU7+ZbWLlbjskXldpcum3FO9m/8UgxBzifEBJw87o:PIWE18SeWOKft2lJbPQcnM68UmXo
TLSH:	0C05F1F09AF9B658F035637636D0A03C6BF3EA1BC908E1399D67934D9316EC145E1A23
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....P..0.....N... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d4eba
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62F118C3 [Mon Aug 8 14:08:03 2022 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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd4e68	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd6000	0x5b4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd8000	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	0xd2ec0	0xd3000	False	0.8657967083827014	data	7.781035493181961	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xd6000	0x5b4	0x600	False	0.427734375	data	4.099660684112187	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd8000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xd6090	0x324	data		
RT_MANIFEST	0xd63c4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 18:34:59.524580002 CEST	58748	53	192.168.2.5	8.8.8.8
Aug 8, 2022 18:34:59.548988104 CEST	53	58748	8.8.8.8	192.168.2.5
Aug 8, 2022 18:35:09.584357977 CEST	62972	53	192.168.2.5	8.8.8.8
Aug 8, 2022 18:35:09.629686117 CEST	53	62972	8.8.8.8	192.168.2.5
Aug 8, 2022 18:35:19.659698009 CEST	64559	53	192.168.2.5	8.8.8.8
Aug 8, 2022 18:35:19.717200041 CEST	53	64559	8.8.8.8	192.168.2.5

DNS Queries

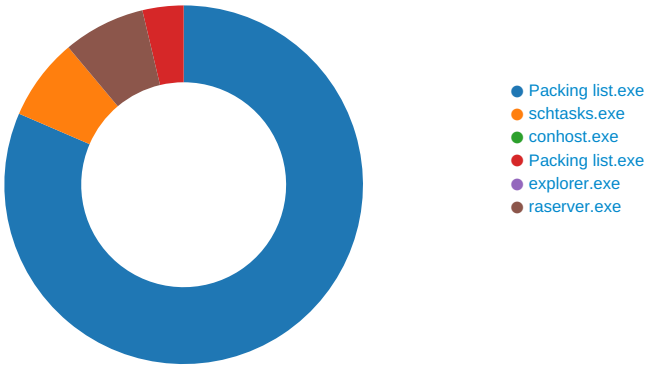
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 18:34:59.524580002 CEST	192.168.2.5	8.8.8.8	0x5c60	Standard query (0)	www.chillsafe.online	A (IP address)	IN (0x0001)
Aug 8, 2022 18:35:09.584357977 CEST	192.168.2.5	8.8.8.8	0xb990	Standard query (0)	www.alshared.info	A (IP address)	IN (0x0001)
Aug 8, 2022 18:35:19.659698009 CEST	192.168.2.5	8.8.8.8	0x88e0	Standard query (0)	www.rewaard.club	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 18:34:59.548988104 CEST	8.8.8.8	192.168.2.5	0x5c60	No error (0)	www.chillsafe.online	tropical-basin-s8sbx7dp132gwikfbpmorir6.herokudns.com		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 18:35:09.629686117 CEST	8.8.8.8	192.168.2.5	0xb990	Name error (3)	www.alshared.info	none	none	A (IP address)	IN (0x0001)
Aug 8, 2022 18:35:19.717200041 CEST	8.8.8.8	192.168.2.5	0x88e0	No error (0)	www.rewaard.club	rewaard.club		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 18:35:19.717200041 CEST	8.8.8.8	192.168.2.5	0x88e0	No error (0)	rewaard.club		185.192.114.83	A (IP address)	IN (0x0001)

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Packing list.exe PID: **6064**, Parent PID: **5596**

General

Target ID:	0
Start time:	18:33:09
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\Packing list.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Packing list.exe"
Imagebase:	0xe70000
File size:	866816 bytes
MD5 hash:	C7A4E2993E53B71353110DEBF193F711
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: 00000000.00000002.464998989.00000000043B9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.464998989.00000000043B9000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.464998989.00000000043B9000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.464998989.00000000043B9000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Analysis Process: schtasks.exe PID: **6020**, Parent PID: **6064**

General

Target ID:	6
Start time:	18:33:28
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\jcWxLdFqdoHatB" /XML "C:\Users\user\AppData\Local\Temp\tmp7D6D.tmp
Imagebase:	0x1250000

File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
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

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7D6D.tmp	unknown	2	success or wait	1	125AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7D6D.tmp	unknown	1652	success or wait	1	125ABD9	ReadFile

Analysis Process: conhost.exe PID: **5788**, Parent PID: **6020**

General

Target ID:	7
Start time:	18:33:28
Start date:	08/08/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff77f440000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Packing list.exe PID: **1320**, Parent PID: **6064**

General

Target ID:	8
Start time:	18:33:29
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\Packing list.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xff0000
File size:	866816 bytes
MD5 hash:	C7A4E2993E53B71353110DEBF193F711
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: 00000008.00000000.455277708.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000008.00000000.455277708.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.455277708.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.455277708.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41B867	NtReadFile

Analysis Process: explorer.exe PID: **684**, Parent PID: **1320**

General

Target ID:	10
Start time:	18:33:33
Start date:	08/08/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff74fc70000
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: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.542334317.000000000ACD4000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000A.00000000.542334317.000000000ACD4000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.542334317.000000000ACD4000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.542334317.000000000ACD4000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.521600311.000000000ACD4000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000A.00000000.521600311.000000000ACD4000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.521600311.000000000ACD4000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.521600311.000000000ACD4000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: raserver.exe PID: **3856**, Parent PID: **684**

General

Target ID:	19
Start time:	18:34:15
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\raserver.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\raserver.exe
Imagebase:	0x350000
File size:	108544 bytes
MD5 hash:	2AADF65E395BFBD0D9B71D7279C8B5EC
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: 00000013.00000002.682502518.0000000002FD0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000013.00000002.682502518.0000000002FD0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.682502518.0000000002FD0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.682502518.0000000002FD0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.679680318.0000000000600000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000013.00000002.679680318.0000000000600000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.679680318.0000000000600000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.679680318.0000000000600000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000013.00000002.682654257.00000000032D0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000013.00000002.682654257.00000000032D0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000002.682654257.00000000032D0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000002.682654257.00000000032D0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Packing list.exe	success or wait	1	32EB897	NtDeleteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	32EB867	NtReadFile

Disassembly

No disassembly