ID: 483794
Sample Name:
Quote#56432.exe
Cookbook: default.jbs
Time: 13:49:17
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report Quote#56432.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: FormBook 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 6
Sigma Overview 7
System Summary: 7
Jbx Signature Overview 7
AV Detection: 7
Networking: 7
E-Banking Fraud: 7
System Summary: 7
Data Obfuscation: 7
Boot Survival: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 8
Stealing of Sensitive Information: 8
Remote Access Functionality: 8
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 11
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 12
Contacted IPs 12
Public 12
General Information 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 13
IPs 13
Domains 16
ASN 16
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
Static File Info 18
General 18
File Icon 18
Static PE Info 18
General 18
Entrypoint Preview 19
Data Directories 19
Sections 19
Resources 19
Imports 19
Version Infos 19
Network Behavior 19
Network Port Distribution 19
TCP Packets 19
UDP Packets 19
DNS Queries 19
DNS Answers 19
HTTP Request Dependency Graph 19
HTTP Packets 19
Code Manipulations 20
User Modules 20

Hook Summary 20
Processes 20
Statistics 20
Behavior 20
System Behavior 20
Analysis Process: Quote#56432.exe PID: 6792 Parent PID: 5468 20
General 20
File Activities 21
File Created 21
File Deleted 21
File Written 21
File Read 21
Analysis Process: schtasks.exe PID: 7100 Parent PID: 6792 21
General 21
File Activities 21
Analysis Process: conhost.exe PID: 5908 Parent PID: 7100 21
General 21
Analysis Process: RegSvcs.exe PID: 5848 Parent PID: 6792 22
General 22
File Activities 22
File Read 22
Analysis Process: explorer.exe PID: 3424 Parent PID: 5848 22
General 22
File Activities 23
Analysis Process: systray.exe PID: 5944 Parent PID: 5848 23
General 23
File Activities 24
File Read 24
Analysis Process: cmd.exe PID: 6492 Parent PID: 5944 24
General 24
File Activities 24
Analysis Process: conhost.exe PID: 6472 Parent PID: 6492 24
General 24
Disassembly 25
Code Analysis 25

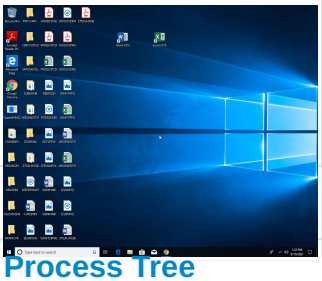
Windows Analysis Report Quote#56432.exe

Overview

General Information

Sample Name:	Quote#56432.exe
Analysis ID:	483794
MD5:	3812ebc395330b..
SHA1:	4dc9fd68e73e0b1.
SHA256:	97ea895e92f7619.
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

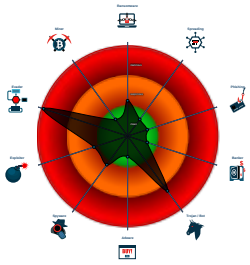
FormBook

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- System process connects to networ…
- Multi AV Scanner detection for dropp…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Sigma detected: Bad Opsec Default…
- Writes to foreign memory regions
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- Quote#56432.exe (PID: 6792 cmdline: 'C:\Users\user\Desktop\Quote#56432.exe' MD5: 3812EBC395330BEF949CC2C7264D1632)
  - schtasks.exe (PID: 7100 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ySWmXEgh' /XML 'C:\Users\user\AppData\Local\Temp\tmp994F.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5908 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 5848 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - systray.exe (PID: 5944 cmdline: C:\Windows\SysWOW64\systray.exe MD5: 1373D481BE4C8A6E5F5030D2FB0A0C68)
      - cmd.exe (PID: 6492 cmdline: /c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6472 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.constructioncleanup.pro/vd9n/"
  ],
  "decoy": [
    "theunwrappedcollective.com",
    "seckj-ic.com",
    "tyresandover.com",
    "thetrophyworld.com",
    "fonggrconstruction.com",
    "hopiproject.com",
    "sktitle.com",
    "charlotteobscurer.com",
    "qjuhe.com",
    "girlzglitter.com",
    "createmylawn.com",
    "hempcbgpill.com",
    "zzdfdzkj.com",
    "shreehariessential.com",
    "226sm.com",
    "getcupscall.com",
    "neuralviolin.com",
    "sanskaar.life",
    "xn--fhqrm54yyukopc.com",
    "togetherx4fantasy5star.today",
    "buyonlinesaree.com",
    "percyshandman.site",
    "hatchethangout.com",
    "rugpat.com",
    "zen-gizmo.com",
    "vipmomali.com",
    "lacerasavall.cat",
    "aqueouso.com",
    "mkolgems.com",
    "sevenhundredseventysix.fund",
    "fotografhannaneret.com",
    "mitravy.com",
    "bmtrans.net",
    "linterpreting.com",
    "izquay.com",
    "sawaturkey.com",
    "marche-maman.com",
    "eemygf.com",
    "animenovel.com",
    "travelssimply.com",
    "montecitobutterfly.com",
    "volebahis.com",
    "daniela.red",
    "ramseyedk12.com",
    "leyterealestate.info",
    "patriotstrong.net",
    "vkgcrew.com",
    "nadhiradeebaazkiya.online",
    "hotelcarre.com",
    "myfabulouscollection.com",
    "stellantis-luxury-rent.com",
    "hn2020.xyz",
    "emilyscopes.com",
    "lotosouq.com",
    "lovecord.date",
    "stconstant.online",
    "volkite-culverin.net",
    "allwaysautism.com",
    "sheisnatashasimone.com",
    "sepantaceram.com",
    "ishopgrady.com",
    "lifestorycard.com",
    "sexybbwavailable.website",
    "domainbaycapital.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.925308127.0000000000360000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000F.00000002.925308127.0000000000360000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000F.00000002.925308127.0000000000360000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.781503558.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.781503558.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 27 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.RegSvcs.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.2.RegSvcs.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
7.2.RegSvcs.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
7.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.2.RegSvcs.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 2 entries				

Sigma Overview

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Multi AV Scanner detection for dropped file

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 potential unpacker

Boot Survival:

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

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
- Writes to foreign memory regions
- Allocates memory in foreign processes
- 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

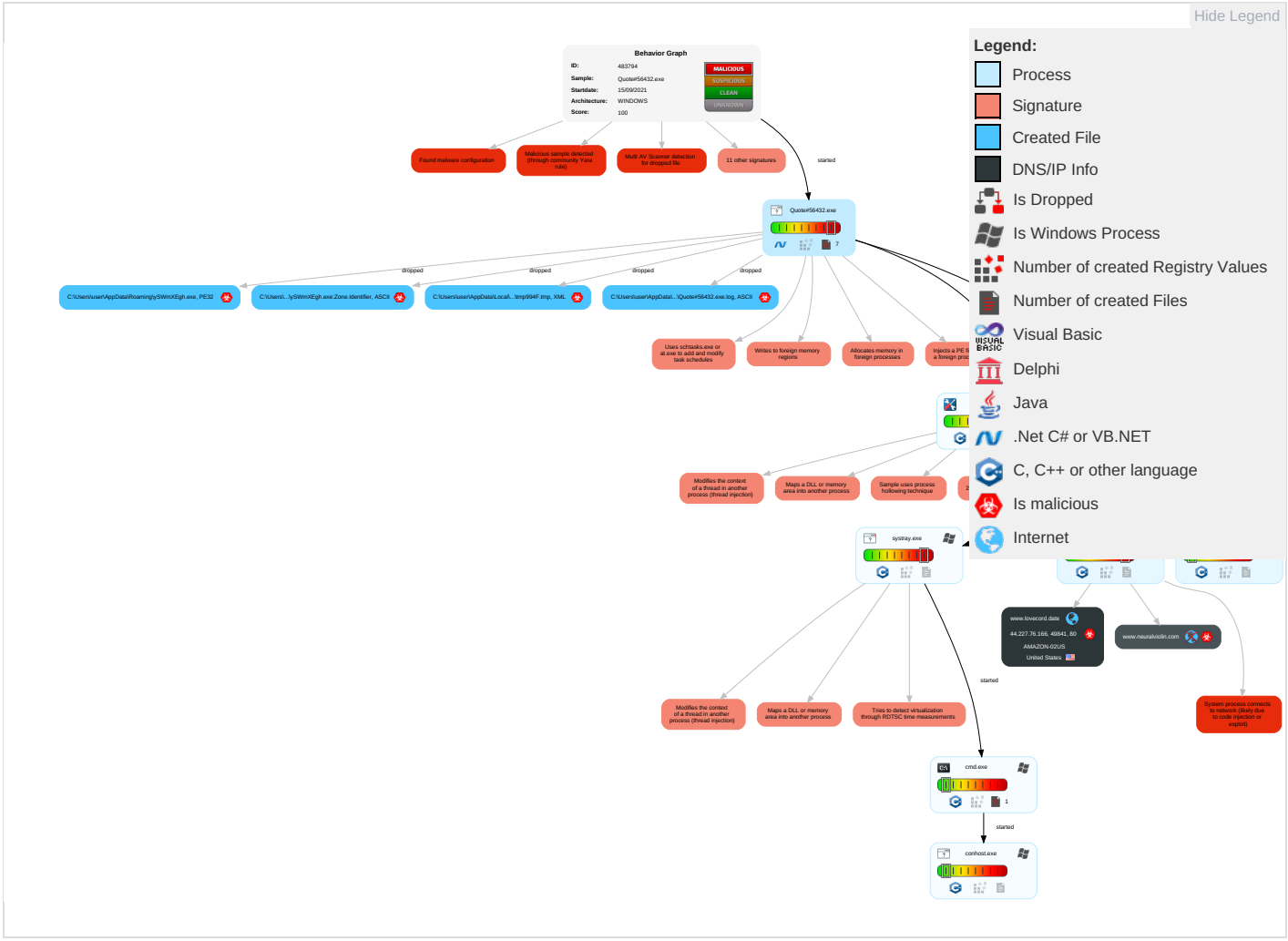
Remote Access Functionality:

- 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
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 8 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	Eavesdrop Insecure Network Communica
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Masquerading 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect Ph Calls/SMS
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	Exploit SS7 Track Devic Location
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	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 8 1 2	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1 1	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi
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	Downgrade Insecure Protocols

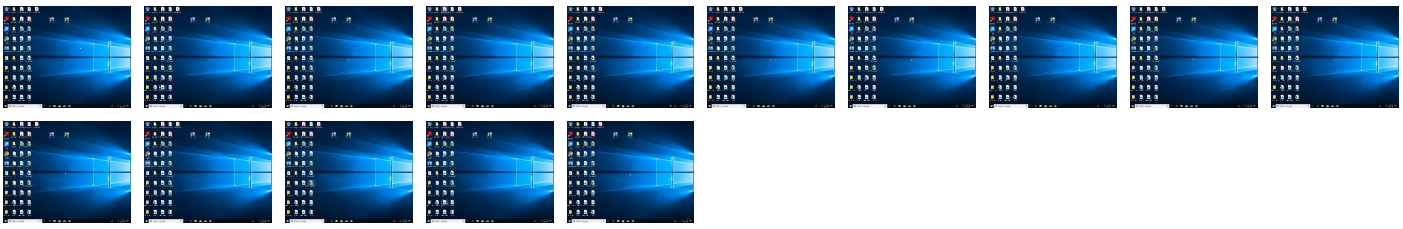
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Quote#56432.exe	30%	Virustotal		Browse
Quote#56432.exe	29%	Metadefender		Browse
Quote#56432.exe	79%	ReversingLabs	Win32.Trojan.SnakeKeylogger	
Quote#56432.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\ySWmXEgh.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\ySWmXEgh.exe	29%	Metadefender		Browse
C:\Users\user\AppData\Roaming\ySWmXEgh.exe	79%	ReversingLabs	Win32.Trojan.SnakeKeylogger	

Unpacked PE Files

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

Domains

Source	Detection	Scanner	Label	Link
www.neuralviolin.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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/cnk	0%	URL Reputation	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/4	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/n-us	0%	Avira URL Cloud	safe	
http://www.urwpp.de%Y	0%	Avira URL Cloud	safe	
http://www.urwpp.deoc	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.urwpp.deFT	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Norm	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
www.constructioncleanup.pro/vd9n/	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-t4	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.carterandcone.com.123	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://lovecord.date	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//z	0%	Avira URL Cloud	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0-d	0%	Avira URL Cloud	safe	
http://www.fontbureau.comiono	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/adnl	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/j	0%	URL Reputation	safe	
http://www.lovecord.date/vd9n/?NfB=6+C1z2NTXQU5TtDgYCNVveFhDHAhXY7UdOammGZxKywecd1Rk4eK0uo6Q7X2XlF/f8Go&o87p=d640H6WhXv9	0%	Avira URL Cloud	safe	
http://www.tiro.comic	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.lovecord.date	44.227.76.166	true	true		unknown
www.neuralviolin.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.constructioncleanup.pro/vd9n/	true	• Avira URL Cloud: safe	low
http://www.lovecord.date/vd9n/?NfB=6+C1z2NTXQU5TtDgYCNVveFhDHAhXY7UdOammGZxKywecd1Rk4eK0uo6Q7X2XlF/f8Go&o87p=d640H6WhXv9	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
44.227.76.166	www.lovecord.date	United States		16509	AMAZON-02US	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483794
Start date:	15.09.2021
Start time:	13:49:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Quote#56432.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	21
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@11/4@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 58.8% (good quality ratio 53.1%) • Quality average: 71.7% • Quality standard deviation: 32%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:50:18	API Interceptor	1x Sleep call for process: Quote#56432.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
44.227.76.166	PO-80722 .xlsx	Get hash	malicious	Browse	• www.thevone.net/utrf/?bXrD=-ZxLnH5X-fMHLB&_8Q=xTZ/dx9Pfi3OU30Zu6i00tru2qtEHUHZXqGrVY3sM47aXdpgIsf41O75Pz7bolMRtoM/3A==
	NOA_-_CMA_CGM_ARRIVAL_NOTICE .exe	Get hash	malicious	Browse	• www.priorpublic.com/kbl2/?X8sl8h70=mNAOX+y4WXabTwndEsz1KZpSG28Pw83WrUohbTsiXwD/y5SMj6F01NR7fqmkJVRgJocs&t48xlt=YTUh7PIXtPD8u2
	famz6.doc	Get hash	malicious	Browse	• www.thetechguruji.com/fzsg/?n0Gh7Vm=wf/sddlrHLxWr86DXNCm9QV1puGglNyoLAn8vaYV0LCioGC0TN4y00CVwxpFrjQTiRwfdg==&DL3=SvMLQz2XqF8DGd-P
	VINASHIP STAR.xlsx	Get hash	malicious	Browse	• www.vicdux.world/nthe/?U2=mv-t_rDPAPsD6l&xtxh=fxK+KfTKr6KIBuhveHuQUfG86Ez3Qoq+EupjvuH6WgTNxOFM1XFHU8sNgRKi0/CU5h4xKw==
	PAYMENT ADVICE.exe	Get hash	malicious	Browse	• www.mesinionisasi.com/bp39/?6lTp=4Y691hW0OvoMbZDSxgwq+J2aC3TtKFJ+npN7jojB5ipOYThD+1a8XyK2n4/ejz5uHklM&kd3=7nx4e8sXT

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ICM Stellar Presentation.xlsx	Get hash	malicious	Browse	• www.thisisatemporaryemail.com/sqwo/?yvFd9F8=gAKOWl9e4py7r9e21+qmV/gdCeDECP4mzyGv8UTw+U6fFj1uXcepbFj/x5Bbnj4wBe8X+Q==&Qp=kFNhNFH02
	Payment Copy.exe	Get hash	malicious	Browse	• www.marcosms.com/stvc/?6lMx=68TspAEfKzMUR4BPxynZES70/zX9zHvygiXQYFBrW0vyxz/NqBJQuAKB66V83/W4M617&vR-=SjQHeD
	Invoice BL Packing List.exe	Get hash	malicious	Browse	• www.injectionhub.com/bmg0/?YBZx=1b_TRVWpeFUP7&b0GLS69=D6f/MTSxB3eaujE6JnioweMJZfOBI5HjgQvuqdfcjvBFiHpIOxrA8TR699cvbxLWwjI1
	Niagara Sc Offer.xlsx	Get hash	malicious	Browse	• www.thisisatemporaryemail.com/sqwo/?yZKX=krU4JLwh4Lst3&fDK=gAKOWl9e4py7r9e21+qmV/gdCeDECP4mzyGv8UTw+U6fFj1uXcepbFj/x5Bbnj4wBe8X+Q==
	BALLANCE PAYMENT.doc	Get hash	malicious	Browse	• www.vayteudung360.com/n6ce/?JVdDiN60=NaS/yScp0tMhV2bQY4lu0z/cLtnzjeTafNc3PbEqgaRjB2tCAaVo0MIQ1Xzd3GKd5v62aA==&c8mH=8p54
	LBQYQx5glN.exe	Get hash	malicious	Browse	• www.thisisatemporaryemail.com/sqwo/?4hLpbf=gAKOWl9b4uy/rtS63+qmV/gdCeDECP4mzye/gXPx606eFSZoQMPlNBb9yfNdsSs7U4Ig&g2JLWb=jR-0iz5psD
	SOA.exe	Get hash	malicious	Browse	• www.promoteboost.com/bp39/?FL=aIfEOU17ssS9I9KNN0CRMP2+9kLyWdLqWCSTbg9WcvzDMJ03vmUXRFVPFPqLFna7q+Zc&3fkpkd=4hKTJV

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Swift Copy.xlsx	Get hash	malicious	Browse	• www.insideajazzyminute.net/uisg/?fpzH9PF=ZuNmzYaPDLkdl2OQeY25VE/FyEJjlFonRjJafNPrT7+ByqUytzr513aHzMqla/Ed/ODEBw==&3fol=bPAh_D2h7lHH
	VESSEL BOOKING DETAILS_pdf.exe	Get hash	malicious	Browse	• www.ketoforoodfight.club/b6a4/?TVnLHr=ICCxxlVw57lW6kbgt+4krLOhunydb8EaldPfbo2bDwvghjkJmYLoE8h2jqshGbu7U6UC&SlTd=2d9l4Zzx
	OoBepaLH3W.exe	Get hash	malicious	Browse	• www.hiddenwholesale.com/p2io/?brMXBhD=es7Y2j6d/8vbylETtmEK+cycNhd4T49F/A456A8m/a4HPEjAATL8KRpgCeYIIlfO3VWH&axl4i=0d9HO65X_T8H0F
	Transfer Payment For Invoice 321-1005703.exe	Get hash	malicious	Browse	• www.vicdux.life/um8e/?n0DTzP=_R7XpHxHj&w8nHuDNH=xbMoviQlEnjsHrEbTPTiLAbjABxJdIVdbR0FO8anDWX5sWiRIQHIKvYrn6XTqKSl/tf+
	Inv_7623980.exe	Get hash	malicious	Browse	• www.lagu45.com/m6b5/?hT4hjLd0=M8gjP7ya2LnHFoHlGDlt2eJ6DpCJ0XzT6n+66/k3ie3JdzdSn/c6UqnSsbXFVlilxba+&uX=8pr4D
	Tlz3P6ra10.exe	Get hash	malicious	Browse	• www.hiddenwholesale.com/p2io/?B6eTzpeH=es7Y2j6d/8vbylETtmEK+cycNhd4T49F/A456A8m/a4HPEjAATL8KRpgCd0fLkz10i3WOhn+bg==&xXk8kx=Bxltd27xbtZdOP20

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	bbZdhGxjJW.exe	Get hash	malicious	Browse	• www.hiddenwholesale.com/p2io/?M4=es7Y2j6d/8vbylETtmEK+cycNhd4T49F/A456A8m/a4HPEjAATL8KRpgCd0mUVT260rROhn5IQ==&3ff=ArcPHv
	CONTRACT 312000123 SSR ADVICE.xlsx	Get hash	malicious	Browse	• www.hiddenwholesale.com/p2io/?Z6E0vv=u0G47XCpG6&-ZYda82=es7Y2j6Y/7vfy1IfvmEK+cycNhd4T49F/AgpmDgn764GP1PGHDawcVRiB70ZTFr94UD3XQ==

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	kpbNbKpJfr.dll	Get hash	malicious	Browse	• 52.84.193.199
	mfQoul1M1Q.exe	Get hash	malicious	Browse	• 52.222.161.215
	k4fNN2WDpY.dll	Get hash	malicious	Browse	• 52.222.161.105
	(RFQ) No.109050.xlsx	Get hash	malicious	Browse	• 75.2.89.208
	Remittance_Advice_details001009142021.xlsx	Get hash	malicious	Browse	• 52.58.78.16
	fCW92GQu51.exe	Get hash	malicious	Browse	• 13.238.159.178
	TPJX2QwEdXs5sTV.exe	Get hash	malicious	Browse	• 54.194.41.141
	tgamf4XuLa.exe	Get hash	malicious	Browse	• 99.83.154.118
	SRMETALINDUSTRIES.exe	Get hash	malicious	Browse	• 44.227.65.245
	PI L032452021xxls.exe	Get hash	malicious	Browse	• 99.83.154.118
	Unpaid invoice.exe	Get hash	malicious	Browse	• 99.83.154.118
	FaxGUO65DE.391343-Faa.html	Get hash	malicious	Browse	• 3.139.50.24
	FaxGUO65DE.391343-Faa.html	Get hash	malicious	Browse	• 3.139.50.24
	Elon Musk Club - 024705 .htm	Get hash	malicious	Browse	• 13.226.156.103
	PGQBjDmDZ4	Get hash	malicious	Browse	• 34.249.145.219
	m5DozqUO2t	Get hash	malicious	Browse	• 54.70.167.99
	avxeC9Wssi	Get hash	malicious	Browse	• 13.52.148.225
	Wh3hrPWbBG	Get hash	malicious	Browse	• 34.249.145.219
	re2.x86	Get hash	malicious	Browse	• 184.77.232.100
	re2.arm7	Get hash	malicious	Browse	• 63.32.132.1

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Quote#56432.exe.log

Process:	C:\Users\user\Desktop\Quote#56432.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Quote#56432.exe.log	
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
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..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp994F.tmp	
Process:	C:\Users\user\Desktop\Quote#56432.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1641
Entropy (8bit):	5.1797729216492625
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGctn:cbhK79lNQR/rydbz9I3YODOLNdq3J
MD5:	A9A91EFB313644132CAF257F5A4DF482
SHA1:	09A7960E056F0B5094F35DBC9647B32F14EF9093
SHA-256:	93F74A2E739775D04BFC58579C1DE9B19D8B355A592161911DAA715F78574D6E
SHA-512:	76402E9405E917DC6DBD90507A0E9DFB8C4A6529C7DC311D9404C7F71E355AD57EB2DA91312342C27228B4E1C690B2E84F6F59F3C41AFA78DE00792889AFE15
Malicious:	**true**
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>true

C:\Users\user\AppData\Roaming\ySWmXEgh.exe	
Process:	C:\Users\user\Desktop\Quote#56432.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	549888
Entropy (8bit):	7.664798299556899
Encrypted:	false
SSDEEP:	12288:q6kJnWHCM2K4C5WA/w6eRH7/JE2m/u+GoqYcllpO8H:2F3C9m7RE2uuBZXL
MD5:	3812EBC395330BEF949CC2C7264D1632
SHA1:	4DC9FD68E73E0B14AB02670BB7C80372D0043BC4
SHA-256:	97EA895E92F76192010E02F12ACA8EC4FFA1B667E84C9958332D280CED624402
SHA-512:	6AB7E1DEC963D3229293E98146EA4A709D2D13413EC14BAF1711D693A6A2918D03E79DA9C6B27101682FE16ECF0021C334CB91006ECB69DDB17A306840E7510
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 29%, Browse • Antivirus: ReversingLabs, Detection: 79%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...J.@a.....0..Z.....x... .....@.. .....@.....w..O..... ....H.....text....X... ...Z..... ..`.rsrc.....\.....@..@.rel oc.....b.....@..B.....w.....H.....<[.. .....z...\...X.....0.....(.....+..~.....-.....~.....(....s.....s.....r...p(.....o.....r...p(.....o.....o. .....o ...t.....o!...o"...}.....d.S.....o#.....($.....o%...}.....($...r=..po&...o'...&.....rO..p(.....o(.....o(....r}..p(.....*.....0.....{.....+..*.0.....(.....+..r...p(.....~.....-.....~.....(....s.....s.....r...p(.....o.....r...p(.....o

C:\Users\user\AppData\Roaming\ySWmXEgh.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Quote#56432.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621

C:\Users\user\AppData\Roaming\ySWmXEgh.exe:Zone.Identifier	
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.664798299556899
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Quote#56432.exe
File size:	549888
MD5:	3812ebc395330bef949cc2c7264d1632
SHA1:	4dc9fd68e73e0b14ab02670bb7c80372d0043bc4
SHA256:	97ea895e92f76192010e02f12aca8ec4ffa1b667e84c9958332d280ced624402
SHA512:	6ab7e1dec963d3229293e98146ea4a709d2d13413ec14baf1711d693a6a2918d03e79da9c6b27101682fe16ecf0021c334cb91006ecb69ddb17a306840e7510c
SSDEEP:	12288:q6kJnWHCM2K4C5WA/w6eRH7/JE2m/u+GoqYcllpO8H:2F3C9m7RE2uuBZXL
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...J.@a.....0..Z.....x... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x487806
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6140D14A [Tue Sep 14 16:43:54 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0

General

Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x8580c	0x85a00	False	0.891785181829	data	7.67621668489	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x88000	0x5e4	0x600	False	0.429036458333	data	4.19079250393	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8a000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 13:51:49.930634975 CEST	192.168.2.4	8.8.8.8	0x4893	Standard query (0)	www.lovecord.date	A (IP address)	IN (0x0001)
Sep 15, 2021 13:52:10.904135942 CEST	192.168.2.4	8.8.8.8	0x7c6e	Standard query (0)	www.neuralviolin.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 13:51:50.126816988 CEST	8.8.8.8	192.168.2.4	0x4893	No error (0)	www.lovecord.date		44.227.76.166	A (IP address)	IN (0x0001)
Sep 15, 2021 13:51:50.126816988 CEST	8.8.8.8	192.168.2.4	0x4893	No error (0)	www.lovecord.date		44.227.65.245	A (IP address)	IN (0x0001)
Sep 15, 2021 13:52:10.950427055 CEST	8.8.8.8	192.168.2.4	0x7c6e	Name error (3)	www.neuralviolin.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.lovecord.date

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49841	44.227.76.166	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 13:51:50.497225046 CEST	5710	OUT	GET /vd9n/?NfB=6+C1z2NTXQU5TtDgYCNVveFhDHAhXY7UdOammGZxKywecd1Rk4eK0uo6Q7X2XlF/f8Go&o87p=d640H6WhXv9 HTTP/1.1 Host: www.lovecord.date Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 13:51:50.677776098 CEST	5715	IN	HTTP/1.1 307 Temporary Redirect Server: openresty Date: Wed, 15 Sep 2021 11:51:50 GMT Content-Type: text/html; charset=utf-8 Content-Length: 168 Connection: close Location: http://lovecord.date X-Frame-Options: sameorigin Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 37 20 54 65 6d 70 6f 72 61 72 79 20 52 65 64 69 72 65 63 74 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 37 20 54 65 6d 70 6f 72 61 72 79 20 52 65 64 69 72 65 63 74 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>307 Temporary Redirect</title></head><body> 307 Temporary Redirect <hr> openresty </body></html>

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: Quote#56432.exe PID: 6792 Parent PID: 5468

General

Start time:	13:50:10
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\Quote#56432.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Quote#56432.exe'
Imagebase:	0x680000

File size:	549888 bytes
MD5 hash:	3812EBC395330BEF949CC2C7264D1632
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: 00000000.00000002.690946204.0000000003C70000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.690946204.0000000003C70000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.690946204.0000000003C70000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.690221413.0000000002B51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.690791851.0000000003B59000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.690791851.0000000003B59000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.690791851.0000000003B59000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 7100 Parent PID: 6792

General

Start time:	13:50:24
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ySWmXEgh' /XML 'C:\Users\user\AppData\Local\Temp\tmp994F.tmp'
Imagebase:	0xdb0000
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

Show Windows behavior

Analysis Process: conhost.exe PID: 5908 Parent PID: 7100

General

Start time:	13:50:24

Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: RegSvcs.exe PID: 5848 Parent PID: 6792

General

Start time:	13:50:24
Start date:	15/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0xe90000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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: 00000007.00000002.781503558.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.781503558.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.781503558.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.782221543.0000000001490000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.782221543.0000000001490000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.782221543.0000000001490000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.782183245.0000000001460000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.782183245.0000000001460000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.782183245.0000000001460000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 5848

General

Start time:	13:50:26
Start date:	15/09/2021
Path:	C:\Windows\explorer.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
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: 00000008.00000000.738249263.000000000E47D000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.738249263.000000000E47D000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.738249263.000000000E47D000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000000.720837328.000000000E47D000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.720837328.000000000E47D000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.720837328.000000000E47D000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: systray.exe PID: 5944 Parent PID: 5848

General

Start time:	13:51:06
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\systray.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\systray.exe
Imagebase:	0xc70000
File size:	9728 bytes
MD5 hash:	1373D481BE4C8A6E5F5030D2FB0A0C68
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: 0000000F.00000002.925308127.0000000000360000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.925308127.0000000000360000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.925308127.0000000000360000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.925553519.0000000000B00000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.925553519.0000000000B00000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.925553519.0000000000B00000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000002.925610906.0000000000B30000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000002.925610906.0000000000B30000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000002.925610906.0000000000B30000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6492 Parent PID: 5944

General

Start time:	13:51:09
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6472 Parent PID: 6492

General

Start time:	13:51:10
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis