ID: 756291
Sample Name: workalone.exe
Cookbook: default.jbs
Time: 00:06:06
Date: 30/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Copyright Joe Security LLC 2022

Copyright Joe Security LLC 2022

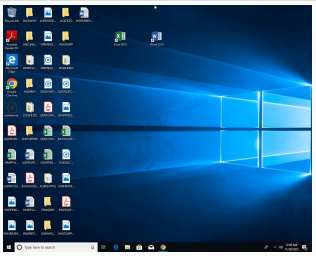
Windows Analysis Report

workalone.exe

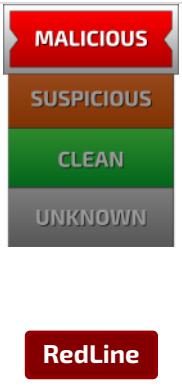
Overview

General Information

Sample Name:	workalone.exe
Analysis ID:	756291
MD5:	68f42f485ece933..
SHA1:	c63f1a56d12a0a..
SHA256:	5d526be000146c..
Tags:	exe RedLineStealer
Infos:	



Detection



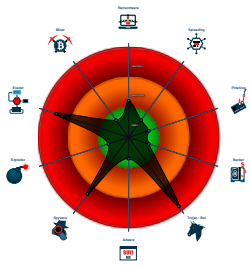
RedLine

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

Signatures

- Yara detected RedLine Stealer
- Malicious sample detected (through…
- Sigma detected: Schedule system p…
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Tries to steal Crypto Currency Walle…
- Connects to many ports of the same…
- Uses known network protocols on n…
- Machine Learning detection for sam…
- Injects a PE file into a foreign proce…
- Queries sensitive video device infor…
- Queries sensitive disk information (v…

Classification



Process Tree

- **System is w10x64**
- workalone.exe (PID: 5836 cmdline: C:\Users\user\Desktop\workalone.exe MD5: 68F42F485ECE93306BEF1E4084D3052E)
  - workalone.exe (PID: 5956 cmdline: C:\Users\user\Desktop\workalone.exe MD5: 68F42F485ECE93306BEF1E4084D3052E)
    - conhost.exe (PID: 5964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5972 cmdline: cmd" /c mkdir "C:\Users\user\AppData\Roaming\svchost MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6020 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 6040 cmdline: "cmd" /c schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\user\AppData\Roaming\svchost\svchost.exe'" /f MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6072 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6108 cmdline: schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\user\AppData\Roaming\svchost\svchost.exe'" /f MD5: 15FF7D8324231381BAD48A052F85DF04)
  - cmd.exe (PID: 6080 cmdline: cmd" /c copy "C:\Users\user\Desktop\workalone.exe" "C:\Users\user\AppData\Roaming\svchost\svchost.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6124 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: RedLine


```
{
  "C2 url": [
    "saleshor12.duckdns.org:46539"
  ],
  "Bot Id": "cheat"
}
```


Yara Signatures

Copyright Joe Security LLC 2022

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000000.262815044.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000001.00000000.262815044.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000000.262815044.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_f54632eb	unknown	unknown	• 0x133ca:$a4: get_ScannedWallets • 0x12228:$a5: get_ScanTelegram • 0x1304e:$a6: get_ScanGeckoBrowsersPaths • 0x10e6a:$a7: <Processes>k__BackingField • 0xed7c:$a8: <GetWindowsVersion>g__HKLM_GetString\|11_0 • 0x1079e:$a9: <ScanFTP>k__BackingField
00000001.00000002.406713080.000000000309F000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000000.00000002.270249352.00000000039F9000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Click to see the 8 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
1.0.workalone.exe.400000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
1.0.workalone.exe.400000.0.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
1.0.workalone.exe.400000.0.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1048a:$u7: RunPE • 0x13b41:$u8: DownloadAndEx • 0x9130:$pat14: , CommandLine: • 0x13079:$v2_1: ListOfProcesses • 0x1068b:$v2_2: get_ScanVPN • 0x1072e:$v2_2: get_ScanFTP • 0x1141e:$v2_2: get_ScanDiscord • 0x1240c:$v2_2: get_ScanSteam • 0x12428:$v2_2: get_ScanTelegram • 0x124ce:$v2_2: get_ScanScreen • 0x13216:$v2_2: get_ScanChromeBrowsersPaths • 0x1324e:$v2_2: get_ScanGeckoBrowsersPaths • 0x13509:$v2_2: get_ScanBrowsers • 0x135ca:$v2_2: get_ScannedWallets • 0x135f0:$v2_2: get_ScanWallets • 0x13610:$v2_3: GetArguments • 0x11cd9:$v2_4: VerifyUpdate • 0x165fe:$v2_4: VerifyUpdate • 0x139ca:$v2_5: VerifyScanRequest • 0x130c6:$v2_6: GetUpdates • 0x165df:$v2_6: GetUpdates
1.0.workalone.exe.400000.0.unpack	Windows_Trojan_RedLineStealer_f54632eb	unknown	unknown	• 0x135ca:$a4: get_ScannedWallets • 0x12428:$a5: get_ScanTelegram • 0x1324e:$a6: get_ScanGeckoBrowsersPaths • 0x1106a:$a7: <Processes>k__BackingField • 0xef7c:$a8: <GetWindowsVersion>g__HKLM_GetString\|11_0 • 0x1099e:$a9: <ScanFTP>k__BackingField
0.2.workalone.exe.3a29170.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Click to see the 15 entries

Sigma Signatures

Persistence and Installation Behavior

Sigma detected: Schedule system process

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Connects to many ports of the same IP (likely port scanning)

Uses known network protocols on non-standard ports

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

System Summary

Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior

Drops PE files with benign system names

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

Malware Analysis System Evasion

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected RedLine Stealer

Tries to steal Crypto Currency Wallets

Found many strings related to Crypto-Wallets (likely being stolen)

Copyright Joe Security LLC 2022

Tries to harvest and steal browser information (history, passwords, etc)

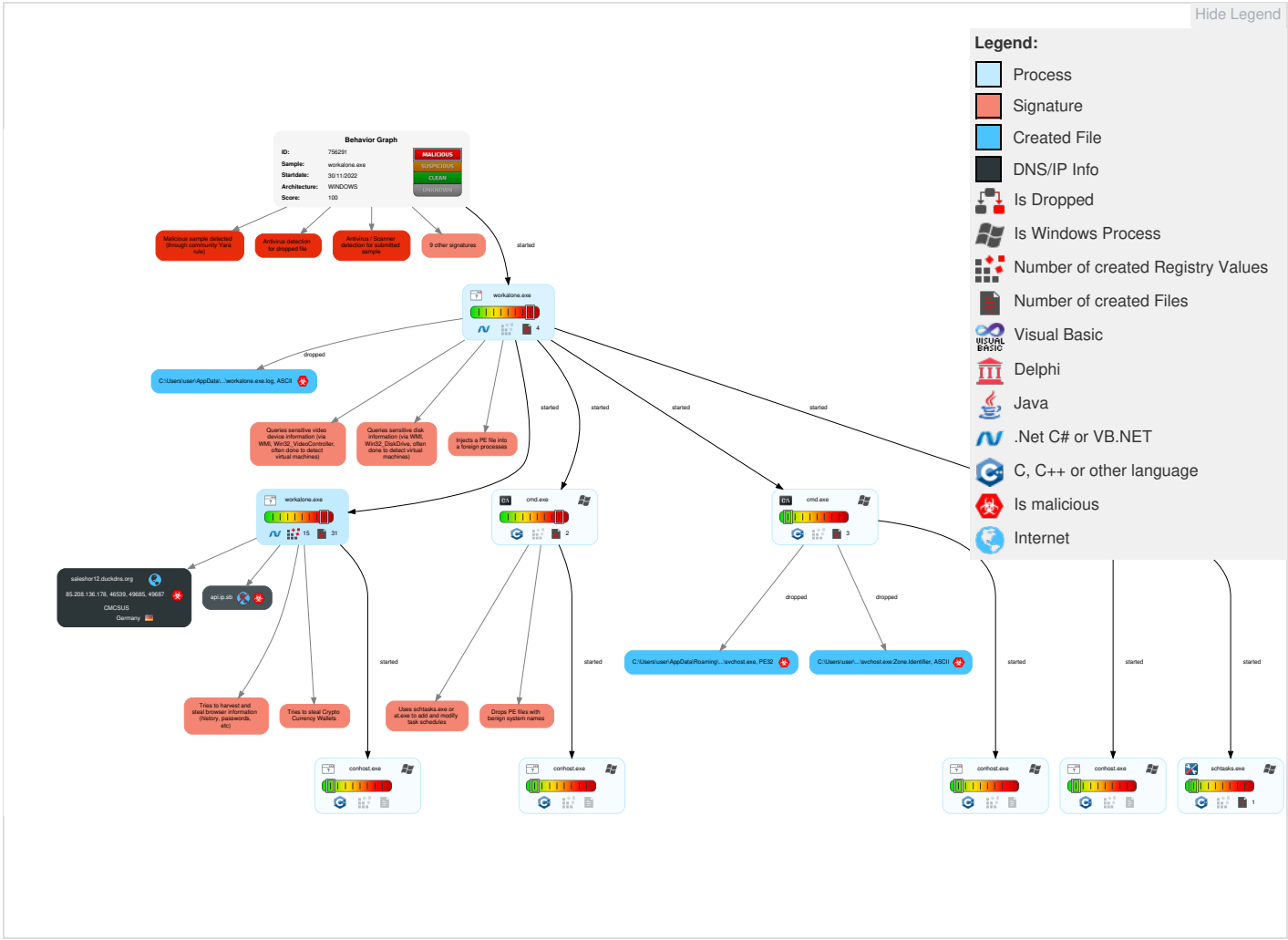
Remote Access Functionality

Yara detected RedLine Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Valid Accounts	2 2 1 Windows Management Instrumentation	1 Valid Accounts	1 Valid Accounts	1 1 Masquerading	1 OS Credential Dumping	2 3 1 Security Software Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	1 Scheduled Task/Job	1 Access Token Manipulation	1 Valid Accounts	LSASS Memory	1 1 Process Discovery	Remote Desktop Protocol	3 Data from Local System	Exfiltration Over Bluetooth	1 1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 1 1 Process Injection	1 Access Token Manipulation	Security Account Manager	2 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 Scheduled Task/Job	1 Disable or Modify Tools	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	2 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 3 1 Virtualization/Sandbox Evasion	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 1 Process Injection	Cached Domain Credentials	1 2 3 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Deobfuscate/Decode Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 Obfuscated Files or Information	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	2 Software Packing	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

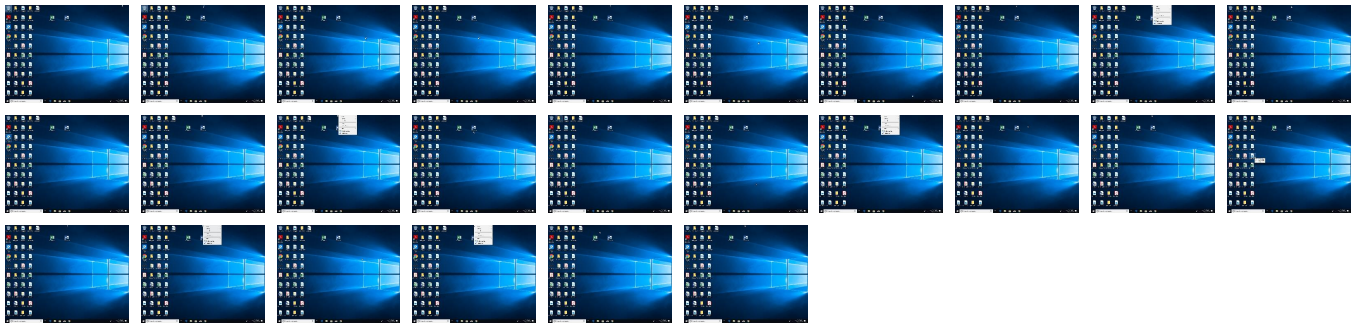
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
workalone.exe	100%	Avira	HEUR/AGEN.1235903	
workalone.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\svchost\svchost.exe	100%	Avira	HEUR/AGEN.1235903	
C:\Users\user\AppData\Roaming\svchost\svchost.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.workalone.exe.590000.0.unpack	100%	Avira	HEUR/AGEN.1235903		Download File
1.0.workalone.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1234943		Download File

Domains

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
api.ip.sb	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/CheckConnectResponse	0%	URL Reputation	safe	
http://schemas.datacontract.org/2004/07/	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/EnvironmentSettings	0%	URL Reputation	safe	
http://tempuri.org/t_	0%	URL Reputation	safe	
http://https://api.ip.sb/geoip%USERPEnvironmentROFILE%	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/CheckConnect	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/VerifyUpdateResponse	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/SetEnviron	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/SetEnvironment	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/SetEnvironmentResponse	0%	URL Reputation	safe	
http://saleshor12.duckdns.org:46539	0%	Avira URL Cloud	safe	
http://saleshor12.duckdns.org:46539/	0%	Avira URL Cloud	safe	
saleshor12.duckdns.org:46539	0%	Avira URL Cloud	safe	
http://tempuri.org/Endpoint/GetUpdates	0%	URL Reputation	safe	
http://saleshor12.duckdns.org	0%	Avira URL Cloud	safe	
http://https://api.ipify.orgcookies//settinString.Removeg	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/GetUpdatesResponse	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/EnvironmentSettingsResponse	0%	URL Reputation	safe	
http://tempuri.org/Endpoint/VerifyUpdate	0%	URL Reputation	safe	
http://tempuri.org/0	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://saleshor12.duckdns.org:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
saleshor12.duckdns.org	85.208.136.178	true	true		unknown
api.ip.sb	unknown	unknown	true	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://saleshor12.duckdns.org:46539/	true	• Avira URL Cloud: safe	unknown
saleshor12.duckdns.org:46539	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

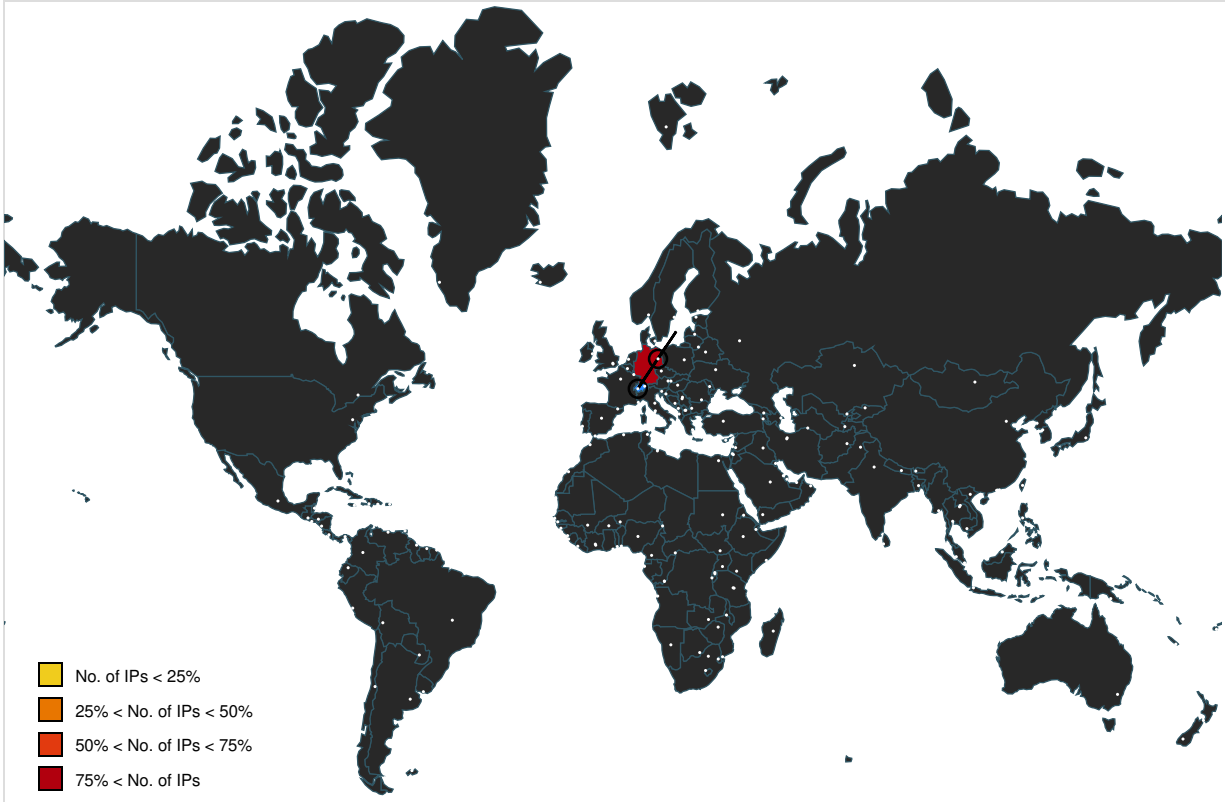
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ipinfo.io/ip%appdata%	workalone.exe, 00000000.00000002.2702493 52.00000000039F9000.00000004.00000800.00 020000.00000000.sdmp, workalone.exe, 000 00001.00000000.262815044.000000000040200 0.00000040.00000400.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/chrome_newtab	workalone.exe, 00000001.00000002.4128359 43.000000000432F000.00000004.00000800.00 020000.00000000.sdmp, workalone.exe, 000 00001.00000003.372893673.000000000695E00 0.00000004.00000800.00020000.00000000.sdmp, tmp10B8.tmp.1.dr, tmpE08F.tmp.1.dr, tmp4D74.tm p.1.dr, tmp10E8.tmp.1.dr, tmp6FE4.tmp.1.dr, tmp407 5.tmp.1.dr, tmpAFBA.tmp.1.dr, tmp4D35.tmp.1.dr, tm p7EB6.tmp.1.dr, tmp6FB4.tmp.1.dr, tmpE939.tmp.1.dr, tmp1B56.tmp.1.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/ac/?q=	tmp1B56.tmp.1.dr	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	workalone.exe, 00000001.00000002.4128359 43.000000000432F000.00000004.00000800.00 020000.00000000.sdmp, workalone.exe, 000 00001.00000003.372893673.000000000695E00 0.00000004.00000800.00020000.00000000.sdmp, tmp10B8.tmp.1.dr, tmpE08F.tmp.1.dr, tmp4D74.tm p.1.dr, tmp10E8.tmp.1.dr, tmp6FE4.tmp.1.dr, tmp407 5.tmp.1.dr, tmpAFBA.tmp.1.dr, tmp4D35.tmp.1.dr, tm p7EB6.tmp.1.dr, tmp6FB4.tmp.1.dr, tmpE939.tmp.1.dr, tmp1B56.tmp.1.dr	false		high
http://ns.adobe.cobj	workalone.exe, 00000001.00000003.3855174 83.0000000008C81000.00000004.00000800.00 020000.00000000.sdmp, workalone.exe, 000 00001.00000003.404595530.0000000008C9100 0.00000004.00000800.00020000.00000000.sdmp, workalone.exe, 00000001.00000003.404434533.000 0000008C90000.00000004.00000800.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous	workalone.exe, 00000001.00000002.4064539 54.0000000003051000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://tempuri.org/Endpoint/CheckConnectResponse	workalone.exe, 00000001.00000002.4064539 54.0000000003051000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.datacontract.org/2004/07/	workalone.exe, 00000001.00000002.4074841 96.000000000318C000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Endpoint/EnvironmentSettings	workalone.exe, 00000001.00000002.4064539 54.0000000003051000.00000004.00000800.00 020000.00000000.sdmp, workalone.exe, 000 00001.00000002.406713080.000000000309F00 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/t_	workalone.exe, 00000001.00000002.4067130 80.000000000309F000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ip.sb/geoip%USERPEnvironmentROFILE%	workalone.exe, 00000000.00000002.2702493 52.00000000039F9000.00000004.00000800.00 020000.00000000.sdmp, workalone.exe, 000 00001.00000000.262815044.000000000040200 0.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/soap/envelope/	workalone.exe, 00000001.00000002.4067130 80.000000000309F000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://saleshor12.duckdns.org:46539	workalone.exe, 00000001.00000002.4064539 54.0000000003051000.00000004.00000800.00 020000.00000000.sdmp, workalone.exe, 000 00001.00000002.406918576.00000000030E100 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://search.yahoo.com?fr=crmas_sfpf	workalone.exe, 00000001.00000002.4128359 43.000000000432F000.00000004.00000800.00 020000.00000000.sdmp, workalone.exe, 000 00001.00000003.372893673.000000000695E00 0.00000004.00000800.00020000.00000000.sdmp, tmp10B8.tmp.1.dr, tmpE08F.tmp.1.dr, tmp4D74.tm p.1.dr, tmp10E8.tmp.1.dr, tmp6FE4.tmp.1.dr, tmp407 5.tmp.1.dr, tmpAFBA.tmp.1.dr, tmp4D35.tmp.1.dr, tm p7EB6.tmp.1.dr, tmp6FB4.tmp.1.dr, tmpE939.tmp.1.dr, tmp1B56.tmp.1.dr	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	tmp1B56.tmp.1.dr	false		high
http://schemas.xmlsoap.org/soap/envelope/D	workalone.exe, 00000001.00000002.4067130 80.000000000309F000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://saleshor12.duckdns.org	workalone.exe, 00000001.00000002.4074841 96.000000000318C000.00000004.00000800.00 020000.00000000.sdmp, workalone.exe, 000 00001.00000002.406918576.00000000030E100 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://tempuri.org/	workalone.exe, 00000001.00000002.4067130 80.000000000309F000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Endpoint/CheckConnect	workalone.exe, 00000001.00000002.4064539 54.0000000003051000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	workalone.exe, 00000001.00000002.412835943.000000000432F000.00000004.00000800.00020000.00000000.sdmp, workalone.exe, 00000001.00000003.372893673.000000000695E000.00000004.00000800.00020000.00000000.sdmp, tmp10B8.tmp.1.dr, tmpE08F.tmp.1.dr, tmp4D74.tmp.1.dr, tmp10E8.tmp.1.dr, tmp6FE4.tmp.1.dr, tmp4075.tmp.1.dr, tmpAFBA.tmp.1.dr, tmp4D35.tmp.1.dr, tmp7EB6.tmp.1.dr, tmp6FB4.tmp.1.dr, tmpE939.tmp.1.dr, tmp1B56.tmp.1.dr	false		high
http://ns.adobe.c/g	workalone.exe, 00000001.00000003.385517483.0000000008C81000.00000004.00000800.00020000.00000000.sdmp, workalone.exe, 00000001.00000003.404595530.0000000008C91000.00000004.00000800.00020000.00000000.sdmp, workalone.exe, 00000001.00000003.404434533.0000000008C90000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Endpoint/VerifyUpdateResponse	workalone.exe, 00000001.00000002.406453954.0000000003051000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Endpoint/SetEnviron	workalone.exe, 00000001.00000002.407484196.000000000318C000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	workalone.exe, 00000001.00000002.412835943.000000000432F000.00000004.00000800.00020000.00000000.sdmp, workalone.exe, 00000001.00000003.372893673.000000000695E000.00000004.00000800.00020000.00000000.sdmp, tmp10B8.tmp.1.dr, tmpE08F.tmp.1.dr, tmp4D74.tmp.1.dr, tmp10E8.tmp.1.dr, tmp6FE4.tmp.1.dr, tmp4075.tmp.1.dr, tmpAFBA.tmp.1.dr, tmp4D35.tmp.1.dr, tmp7EB6.tmp.1.dr, tmp6FB4.tmp.1.dr, tmpE939.tmp.1.dr, tmp1B56.tmp.1.dr	false		high
http://tempuri.org/Endpoint/SetEnvironment	workalone.exe, 00000001.00000002.407484196.000000000318C000.00000004.00000800.00020000.00000000.sdmp, workalone.exe, 00000001.00000002.406918576.00000000030E100.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Endpoint/SetEnvironmentResponse	workalone.exe, 00000001.00000002.406453954.0000000003051000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Endpoint/GetUpdates	workalone.exe, 00000001.00000002.406918576.00000000030E1000.00000004.00000800.00020000.00000000.sdmp, workalone.exe, 00000001.00000002.406713080.000000000309F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://ac.ecosia.org/autocomplete?q=	tmp1B56.tmp.1.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfp	workalone.exe, 00000001.00000002.412835943.000000000432F000.00000004.00000800.00020000.00000000.sdmp, workalone.exe, 00000001.00000003.372893673.000000000695E000.00000004.00000800.00020000.00000000.sdmp, tmp10B8.tmp.1.dr, tmpE08F.tmp.1.dr, tmp4D74.tmp.1.dr, tmp10E8.tmp.1.dr, tmp6FE4.tmp.1.dr, tmp4075.tmp.1.dr, tmpAFBA.tmp.1.dr, tmp4D35.tmp.1.dr, tmp7EB6.tmp.1.dr, tmp6FB4.tmp.1.dr, tmpE939.tmp.1.dr, tmp1B56.tmp.1.dr	false		high
http://https://api.ipify.orgcookies//settinString.Removeg	workalone.exe, 00000000.00000002.270249352.00000000039F9000.00000004.00000800.00020000.00000000.sdmp, workalone.exe, 00000001.00000000.262815044.000000000040200.00000040.00000400.00020000.00000000.sdmp	true	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing	workalone.exe, 00000001.00000002.406453954.0000000003051000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/fault	workalone.exe, 00000001.00000002.406453954.0000000003051000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Endpoint/GetUpdatesResponse	workalone.exe, 00000001.00000002.406453954.0000000003051000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Endpoint/EnvironmentSettingsResponse	workalone.exe, 00000001.00000002.406453954.0000000003051000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Endpoint/VerifyUpdate	workalone.exe, 00000001.00000002.406453954.0000000003051000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/0	workalone.exe, 00000001.00000002.4064539 54.0000000003051000.00000004.00000800.00 020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http:// schemas.xmlsoap.org/ws/2005/05/identity/claims/nam e	workalone.exe, 00000001.00000002.4064539 54.0000000003051000.00000004.00000800.00 020000.00000000.sdmp	false		high
http:// https://cdn.ecosia.org/assets/images/ico/favicon.icohttp s://www.ecosia.org/search?q=	tmp1B56.tmp.1.dr	false		high
http://schemas.xmlsoap.org/soap/actor/next	workalone.exe, 00000001.00000002.4064539 54.0000000003051000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://ns.ado/1	workalone.exe, 00000001.00000003.3855174 83.0000000008C81000.00000004.00000800.00 020000.00000000.sdmp, workalone.exe, 000 00001.00000003.404595530.0000000008C9100 0.00000004.00000800.00020000.00000000.sdmp, workalone.exe, 00000001.00000003.404434533.000 0000008C90000.00000004.00000800.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://saleshor12.duckdns.org:	workalone.exe, 00000001.00000002.4074841 96.000000000318C000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
85.208.136.178	saleshor12.duckdns.org	Germany		33657	CMCSUS	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756291
Start date and time:	2022-11-30 00:06:06 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 33s
Hypervisor based Inspection enabled:	false

Copyright Joe Security LLC 2022

Report type:	light
Sample file name:	workalone.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	20
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@15/29@5/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 104.26.12.31, 104.26.13.31, 172.67.75.172
- Excluded domains from analysis (whitelisted): api.ip.sb.cdn.cloudflare.net, fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
00:07:08	Task Scheduler	Run new task: Nafifas path: "C:\Users\user\AppData\Roaming\svchost\svchost.exe"
00:07:54	API Interceptor	95x Sleep call for process: workalone.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\workalone.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	612
Entropy (8bit):	5.33730556823153
Encrypted:	false
SSDEEP:	12:Q3La/hhkvoDLI4MWuCqDLI4MWuPk21xzAbDLI4M9XKbbDLI4MWuPJKiUrRZ9I0Z7:MLUE4K5E4Ks2vsXE4qXKDE4KhK3VZ9p7
MD5:	F06804B809C3212C7F29ABA89E9FAF16
SHA1:	B49ED216A41EA579FF109A4BA44A8E62C2B1A3BB
SHA-256:	E63AFB84BF09F02C3C19978966E610BEE5C14099B1A65C8B34E426ABC127ECB7
SHA-512:	53ED48D5233FD6318320264400ACBD451A7C6B10BB2A11C2B95F51C3838708835D1016B417748E7C50023BAF179AC94CCAAE230C71AC073D0233765409341D49
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.Management, 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..

C:\Users\user\AppData\Local\Temp\tmp10B8.tmp

Process:	C:\Users\user\Desktop\workalone.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\tmp10E8.tmp

Process:	C:\Users\user\Desktop\workalone.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false

Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\tmp1B45.tmp

Process:	C:\Users\user\Desktop\workalone.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 2, database pages 23, cookie 0x19, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.7876734657715041
Encrypted:	false
SSDEEP:	48:43KzOIIY3HzrkNSs8LKvUf9KnmlG0UX9q4lCm+KLka+yJqhM0ObVEq8Ma0D0HOlx:Sq0NFeymDlGD9qlm+KL2y0Obn8MouO
MD5:	CF7758A2FF4A94A5D589DEBAED38F82E
SHA1:	D3380E70D0CAEB9AD78D14DD970EA480E08232B8
SHA-256:	6CA783B84D01BFCF9AA7185D7857401D336BAD407A182345B97096E1F2502B7F
SHA-512:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804CBF
Malicious:	false
Preview:	SQLite format 3.....@ .....[5..... ....

C:\Users\user\AppData\Local\Temp\tmp1B56.tmp

Process:	C:\Users\user\Desktop\workalone.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\tmp4075.tmp

Process:	C:\Users\user\Desktop\workalone.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\tmp4D35.tmp

Process:	C:\Users\user\Desktop\workalone.exe

File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\tmp4D74.tmp

Process:	C:\Users\user\Desktop\workalone.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\tmp6FB4.tmp

Process:	C:\Users\user\Desktop\workalone.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\tmp6FE4.tmp

Process:	C:\Users\user\Desktop\workalone.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3

SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\tmp7EB6.tmp

Process:	C:\Users\user\Desktop\workalone.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\tmp82DA.tmp

Process:	C:\Users\user\Desktop\workalone.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 2, database pages 23, cookie 0x19, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.7876734657715041
Encrypted:	false
SSDEEP:	48:43KzOIIY3HzrkNSs8LKvUf9KnmlG0UX9q4lCm+KLka+yJqhM0ObVEq8Ma0D0HOlx:Sq0NFeymDlGD9qlm+KL2y0Obn8MouO
MD5:	CF7758A2FF4A94A5D589DEBAED38F82E
SHA1:	D3380E70D0CAEB9AD78D14DD970EA480E08232B8
SHA-256:	6CA783B84D01BFCF9AA7185D7857401D336BAD407A182345B97096E1F2502B7F
SHA-512:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804CB F
Malicious:	false
Preview:	SQLite format 3.....@ .....[5..... ....

C:\Users\user\AppData\Local\Temp\tmp8319.tmp

Process:	C:\Users\user\Desktop\workalone.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 2, database pages 23, cookie 0x19, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.7876734657715041
Encrypted:	false
SSDEEP:	48:43KzOIIY3HzrkNSs8LKvUf9KnmlG0UX9q4lCm+KLka+yJqhM0ObVEq8Ma0D0HOlx:Sq0NFeymDlGD9qlm+KL2y0Obn8MouO
MD5:	CF7758A2FF4A94A5D589DEBAED38F82E
SHA1:	D3380E70D0CAEB9AD78D14DD970EA480E08232B8
SHA-256:	6CA783B84D01BFCF9AA7185D7857401D336BAD407A182345B97096E1F2502B7F
SHA-512:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804CB F
Malicious:	false

Preview:	SQLite format 3.....@ .....[5..... ....

C:\Users\user\AppData\Local\Temp\tmp93B7.tmp	
Process:	C:\Users\user\Desktop\workalone.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.691266297898928
Encrypted:	false
SSDEEP:	24:VFl0HyrVqOHKWeRhsGhMtSCTPacJ7pZeZLF8M7y+b:VFl0HyrVqOqNRhHkTaW73Q58yy+b
MD5:	7D4E714F4EDA4631DCA8D420338392F1
SHA1:	536B4BCBAB5C780738EE2D562D16AB532C9D8E68
SHA-256:	841F74A72A1D21F63E4039906E93A4FD9E70EC517385DDEE855033A9A17FE94A
SHA-512:	FEB2EEC88720FF040794CD273A7B4A07DD5AC1E6CD9A9235A098F1FB3A1C50385B37E376764C927978961A0EE4AC1C591F197494D82D71B35EAA3780956CB1A 3
Malicious:	false
Preview:	AQRFEVRTGLRPNVUMAMHTYETEVGDENHEHZDAQRXZQCDHHLTUZIEJRCQGGPRQWBIYWADWJEZTAELERKZUDZJHSFVIUPBTJVGKYQFWVMPTQUZUZZS OJNBOABYGRCYMPSQARVQUZQVCNVECXPCBIEBYWXWSRMTKFKBEHRJGIPFMOYSZMEELAQPGBHDTUPVXJROQBNFXLTFTPQHVAGKBRLNHZRZVUTEGA NMGKVRFJJNOMKLVMQNTHIORPQCPGNIZSOYKXAQJCOPIGBQRJINVPIRVOHHCOGWQPXWQEGDKAHJASRIJBIMZDOWPSCSZZQNZFPNLCIRCXKLGBVX KUJASQXRHFULXFGHARZKMVRSMXPJPUDKEQXOSCEBAKVRLNKSSEVKXVMESKRHMKSXSUKELGCEYTRDUXROEARVKPGFZHNSDRPAQVQVSCJPHBVIRZ PYJKRBBZNOUQWXJMMJNDFWGGJPGQMMWRHVVMGZTXMHGJMPQFKEKIAULKOFHNCPDGWVUWIVKGZHFAQVQOBPOUZZTMTUXLURTPHPWR VYABSKGEOJTHCTJYEQSHAVPELOSNLRXFRVWMHJRZTZLGKGNKELBIANUAYANWKNNJPQUXDOBXLYTGIGYZMXXBSVTKCOWSZHFODTFONXVLBRUGJK EZMTIRWSGAANCFOWQHTMLCODGMRHITYHVPOCCXAYGLOXHITQDUATUBKLPLHFHTHTEONDGTWZOQVYRUABLZCNSDXFSTUTQJACVNWW CLMGVDGIDXECYLUJKBUKWQQUERSQSLBAKCXGRYMXSMUPSLSRDICMSQOGBWCATEAACXPGZFMXCSVNIZUQRAQEWTFWYKNKMGGMAZDJ HXXORIHLHSPMGKAWZUQOKTRGEGDEPETKDTOVQKFNIASUNQNVNPECXIFOSOXOYCRVRJAKLVRMRCMTVZUHFLJPYFXCUSTATJHRIINTHARIAPEKFS UPRLIGJHIMRLJERLFFTZAQPSMLNNQSZLYNDGBIYC

C:\Users\user\AppData\Local\Temp\tmpA720.tmp	
Process:	C:\Users\user\Desktop\workalone.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.698711683401115
Encrypted:	false
SSDEEP:	24:qKHpKPokvebe5xXL3g76mBU/gS2JBbl20lS7pnXk:RpcjnxbW7TYgS2nbzlS7pnXk
MD5:	47643CE7571E0C995094D7CE5F2005D7
SHA1:	40D42828B2F68C625EBD884FB8AF5B20F5A1DF9C
SHA-256:	1D642D4EC7BC821B0FFA28C3F2702C875C922139D8001EADD664EBCCF8D321B3
SHA-512:	3AAD0470C01D2609662C0B8D146BA79132B404C669C22032D085233E2D30725797AC2E15A11F54DFE00E4B6CA6E914E3439D4775B3AF6D782334FE9424F485A5
Malicious:	false
Preview:	HMPPSXQPQVZTKYGXRLZXZQHGCZSWFSMKAZTFZQVPBWYDEIQOYRZBKZROCVLLNDGOXMZATHCHJWBWCKMDMUVOMUCFYNBSIKMCOOAG LUHDSCAREEEQGTRYCAFLTFVCHREFHJJALACUPWFTGZJJVRRQBVOZGXIEUBTJBNHNAXRWAWTUYQZIZWPARDBZBFGZUBQQPINOCLFOLDPTMWQVUU BDSNGDFVMEOTHPNKBOMDPGLFXUXBXHUOTYRPUQTUJPKLUSNTISPNFAHVFBBWEWJQFBJFCDDWUUKCQJNEKMUTJEZKKMXXOCBOVMCG GYTPDYBYYFVGHQJJBCDHYWPXJUJWPNURQCUHPTATLFRAOGUCJWWSBAITHVPDRYRFCTPIWHJVKSAXOIPKHISTBCDZISGIVPPYDJLJWFRNVNCWIO INKYQLAFVLCPSGCZABGNTUVGEDQZGQNDECUBPLLOYUYTHXDNNCAXKLHFZXBBAWBICFREGZBLZZMPWRLUSXUNEXAKLSJETGNCJTTGSNPPSHZUKZ DHHYHBBWKJUSIBAKGKHQJINZHCWLBCIIUGTVVLNEZXUBIPUVRAILLENTRJYFNIBHNOUNYAIFQBNUMFUSXNGITFIFZKTSFAQXDYVBIUCIUYJIGJ TIJHWTPPRJQVSBHHUXLZRPPJOWJAPSVQQVKLFHKXZRPEJBFXNKVNBCPMLRQGCJINKLLBJVROFAFCDRFCDAMIDEYSZDWNLUMJZXGWKOIKNAYVXP YRZWMBNAAFKFOPCVNGUECOARMDWJVYVUQQAFEGKCYXVVGXPHPEVOMRADTQDTJSHAKHPNNOGUDWBRXDJFEMSJTJUJKHZONBLGDCDD UDTRQKPOFACELSKHFSBPKXKDGWOKSDBAMWLKXEAOOHWVOAQZGZCNSDWOXSHPTFMVMYQXTRNMUPZSFQXOQLPUFJWHWTXXIRMQXDPV AJKHMSCGTFVJKECYILRMHGFBWQKUNTRVZTBJQJAKTSJUIDOLPL

C:\Users\user\AppData\Local\Temp\tmpA760.tmp	
Process:	C:\Users\user\Desktop\workalone.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.69486718145169
Encrypted:	false
SSDEEP:	24:XvKYeI9D5UOyoiaxIKgpZ9ONvMyTONN5ZjJH1U:yyD6yxILZ9OtTT+XRG
MD5:	E63B196AE0D5F7670244FB1347D75EFC
SHA1:	1C17108AC7E5263674836BAD67AE44D8C3C6890B
SHA-256:	D8C0D7B9CDFC72CAAB0A7687299B6734708E98C6DD088CDB0FF1A659E294B49D

SHA-512:	63345352964E1BD19AC843F82820E9B29C5BA991A002AB9B3164E1AA10B6D88BFA0DFAFA2E91E584835BA89B6A1770140AC14EA0B4B64E6C3BF8CDA34C9698AC
Malicious:	false
Preview:	LIJDSFKJZGBDGXNCCVBULCELYCDFJRIXKMFPVDHHKPYEYOXKFYMNEETRQHXLDRVBOTNERMYOYUJOPHUSKFPWBGKNJYBGZTTHNKGNUZWATSMORY BOIKBFSVUUMZNDYXOYKYUKGRNFVRQOPBEEIPDGTPBXCNLKHMGPHFCEQOUTEDGJZTMFUUGECZETRSODGZCJVQEAMRZADPDVQRANZO SHTGPOXPXGXXQDJVYZOCNXDECWJISPPIJOZUBSSKPGODUHTISNESPZRLELINJJYOXSBFTVUDENIBRDIMMGFIQNDGUSXDBHQNJRYLFTZGOCELKZ GOQQKNDPFAMTXHBKHJYXYEGLJLANRMMTCVEFYRTWLXIMCCHDWVOLGVUWRNLSIBMLMBKVSYLKXRTMZROHVHCRDBCODTPNVQMBPRJG BGOOFVGDIERMXUFETJQWDXSQQFMQAZGGRVNRCUOAVYJDIMQETJOANIIDEGJCHEFRSNVBQAQBBUTTMXBTJXRHLSOCTPPBIKPXITOOCINTVZYAVQ LVOOZWSOPLYJPOTKFKIKEHIDDPCDDEPKVDYQAVTVBFYYWCGUKGIDVLQSIPXISDEDNJWONTSILFUGUYMKQLKEJGOOCBYSXDFHNFHHWGLXWWQKSS OHSSTZLRZVRHZVBZGGEZQFSIWQQPMILSPBAMPAGAHHVJJCITDTJRZTRBEXSXOVDKONGLMSWBAOOYAFISJHKEYUKIWXBFUDUMVQRELEPVTNQBAL AQOEAEFVPIKNYIPNICGKQFRVXNQUEFULLOYWMHOMUFEMHYNKNWMAOBGWSECZOKWISDOIKSUVWBGWPNAMFUHBRWEJQPHFPEKIRLAE PTBNRQEUVXXIZSSOOEFEETUMNPSVEAKOXVYHAOIXBEYBVXDJXZCNDVOPZLARFFUSXUOWXQBKDLINBWBQLXLHHNIXZEPCNHFEIZUZSTXWFUITSB KYSELMNKNBBDQMNLAIOSKYHCWGFPNUXAFSRHOWYH

C:\Users\user\AppData\Local\Temp\tmpA790.tmp

Process:	C:\Users\user\Desktop\workalone.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.694142261581685
Encrypted:	false
SSDEEP:	24:f9GDi2EYjkpBrLp83PYbuFr5oKIQppDgX+qrctnWyd3z+g8BHGZ:yEYjkpZYwS/oKluA+qriTjEBHe
MD5:	E9AA17F314E072EBB015265FB63E77C0
SHA1:	1233B76350B8181FFFC438B62002C02B4AE79000
SHA-256:	F66078FCFEC2D71549136CC8B5B4EE7D33C4994E0A4E3E7C11F5ADCD819D0436
SHA-512:	719E659924CE585E4DD8CEA9BC6B5371AD810999022F874F380F50C7153D3AE97CC934E3173EF06573CAEE6CBC835A668C4D7DC2ADE597B1B0D200FCBAC67A1
Malicious:	false
Preview:	WSHEJMDVQCWJPIIWMEHEPOBRYLOZOHFMDEEYYASRZPHJZGFNCKWIQSPBUMWBCKDMTEBFINALYAFGJUQXINNGDKSDBFBQLHYZRLLDJYSVNXVIEP IYHZGOTARYUNPFNZVRVVWIOWWFIFWCHVVHXNGKFNRNLVVSOPOMGZCDQUWJFARKTCAVVDPTCPNIDLRGSLNKZTVRAJAILYGDVIAAGIVKXRCRTRZJ PKATKZAWRJTPVLTDNBDIRDWCCHBTEVEGYPYDTGSMLUDQXMQCAVHLYMRKPCVHQHMGNCGBZKOUKCCBHQPSIYIJGDVOYJJJRQLDKNVUEXDKCTANSM CHJUBIODALXWUAFPSECIRPCAEPPBACCLXBZAEDKJHLGOICLSKBQEGFCVDQOFKKAJPCTRIXBNPUDXKHSSXTDTQZSFEWHTHKFNJWHOEXGCYSYWIH FSMYJIYEESDQFMESLFQFBUJNXHWFNXIDWEUDMVGFDXPTRRRNPARVUGZAYZRHNTXHZAPBLWMHFSSHMXCYMAGONQNLTCAVPZPCAKJRMGEPDIFETD NSXWPDVMAZGTTCLNRREMVTBLOGKASYOATUDXLJKIYPPDNLZIZMWWFFDVMUFCTZZOFJORNAMGQBAFGCPTDCZBKTIGYDSCSPMIEXAMGICZNTFVNR PLGPMBXJHNCQSYNMGGPKIQJNDBDUBVIVXFILKXZXHODXZAYIDEIMZZMKQNQNBCCMZNFBKSYULDGKOMQZDUQMUVTBBTUTRZMIOZGDEUPHCDKJQD SGBXYNWPWTHYVLGGYNOBJJKAZSTKJSBCHVCLGWYHCNILYSCYCHTGYOGMNGWDZAVDCOVKWJPWVNTTKFTSHAAXLYUEWEVGETFCFTLK WTQCVAMBWYOYJVXNPSSWXJXUZDXJOZNTBLIZLLJQXYNILILMHHONBPAPFMVWEMHIHAGMOXTIBNNEBGCVSZEZTMJVDXSVACSKTAVTFOOSEHZQGT OUSCIQBVIWZGABQNZGJE

C:\Users\user\AppData\Local\Temp\tmpA7C0.tmp

Process:	C:\Users\user\Desktop\workalone.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.691266297898928
Encrypted:	false
SSDEEP:	24:VFl0HyrVqOHKWeRhsGhMtSCTPacJ7pZeZLF8M7y+b:VFl0HyrVqOqNRhHkTaW73Q58yy+b
MD5:	7D4E714F4EDA4631DCA8D420338392F1
SHA1:	536B4BCBAB5C780738EE2D562D16AB532C9D8E68
SHA-256:	841F74A72A1D21F63E4039906E93A4FD9E70EC517385DDEE855033A9A17FE94A
SHA-512:	FEB2EEC88720FF040794CD273A7B4A07DD5AC1E6CD9A9235A098F1FB3A1C50385B37E376764C927978961A0EE4AC1C591F197494D82D71B35EAA3780956CB1A3
Malicious:	false
Preview:	AQRFEVRTGLRPNVUMAMHTYETEVGDENHEHZDAQRXZQCDHHLTUZIEJRCQGGPRQWBIYWADWJEZTAELERKZUDZJHSFVIUPBTJVGKYQFWVMPTQUZUZZS OJNBOABYGRCYMPSQARVQUZQVCNVECXPCBIEBYWXWSRMTKFKBEHRJGIPFMOYSZMEELAQPGBHDTUPVXJROQBNFXLTFTPQHVAGKBRLNHZRZVUTEGA NMGKVRFJJNOMKLVMQNTHIORPQCPGNIZSOYKXAQJCOPIGBQRJINVPIRVOHHCOGWQPXWQEGDKAHJASRIJBIMZDOWPSCSZZQNZFPNLCIRCXKLGBVX KUJASQXRHFULXFGHARZKMVRSMXPJPUDKEQXOSCEBAKVRLNKSSEVKXVMESKRHMKSXSUKELGCEYTRDUXROEARVKPGFZHNSDRPAQVQVSCJPHBVIRZ PYJKRBBZNOUQWXJMMJNDFWGGJPGQMMWRHVVMGZTXMHGJMPQFKEKIAULKOFHNCPDGWVUWIVKGZHFAQVQOBPOUZZTMTUXLURTPHPWR VYABSKGEOJTHCTJYEQSHAVPELOSNLRXFRVWMHJRZTZLGKGNKELBIANUAYANWKNNJPQUXDOBXLYTGIGYZMXXBSVTKCOWSZHFODTFONXVLBRUGJK EZMTIRWSGAANCFOWQHTMLCODGMRHITYHVPOCCXAYGLOXHITQDUATUBKLPLHFHTHTEONDGTWZOQVYRUABLZCNSDXFSTUTQJACVNWW CLMGVDGIDXECYLUJKBUKWQQUERSQSLBAKCXGRYMXSMUPSLSRDICMSQOGBWCATEAACXPGZFMXCSVNIZUQRAQEWTFWYKNKMGGMAZDJ HXXORIHLHSPMGKAWZUQOKTRGEGDEPETKDTOVQKFNIASUNQNVNPECXIFOSOXOYCRVRJAKLVRMRCMTVZUHFLJPYFXCUSTATJHRIINTHARIAPEKFS UPRLIGJHIMRLJERLFFTZAQPSMLNNQSZLYNDGBIYC

C:\Users\user\AppData\Local\Temp\tmpA7F0.tmp

Process:	C:\Users\user\Desktop\workalone.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped

Size (bytes):	1026
Entropy (8bit):	4.698711683401115
Encrypted:	false
SSDEEP:	24:qKHpKPokvebe5xXL3g76mBU/gS2JBbl20IS7pnXk:RpcjnxbW7TYgS2nbzIS7pnXk
MD5:	47643CE7571E0C995094D7CE5F2005D7
SHA1:	40D42828B2F68C625EBD884FB8AF5B20F5A1DF9C
SHA-256:	1D642D4EC7BC821B0FFA28C3F2702C875C922139D8001EADD664EBCCF8D321B3
SHA-512:	3AAD0470C01D2609662C0B8D146BA79132B404C669C22032D085233E2D30725797AC2E15A11F54DFE00E4B6CA6E914E3439D4775B3AF6D782334FE9424F485A5
Malicious:	false
Preview:	HMPPSXQPQVZTKYGXRLZXZQHGCZSWFSMKAZTFZQVPBWYDEIQOYRZBKZROCVLLNDGOXMZATHCHJWBWCKMDMUVOMUCFYNBSIKMCOOAG LUHDSCAREEEQGTRYCAFLTFVCHREFHJJALACUPWFTGZJJVRRQBVOZGXIEUBTJBNHNAXRWAWTUYQZIZWPARDBZBFGZUBQQPINOCLFOLDPTMWQVUU BDSNGDFVMEOTHPNKBOMDPGLFXUXBXHUOTYRPUQTUJPKLUSNTISPNFAHVFBBWEWJQFBJFCDDWUUKCQJNEKMUTJEZKKMXXOCBOVMCG GYTPDYBYYFVGHQJJBCDHYWPXJUJWPNURQCUHPTATLFRAOGUCJWWSBAITHVPDRYRFCTPIWHJVKSAXOIPKHISTBCDZISGIVPPYDJLJWFRNVNCWIO INKYQLAFVLCPSGCZABGNTUVGEDQZGQNDECUBPLLOYUYTHXDNNCAXKLHFZXBBAWBICFREGZBLZZMPWRLUSXUNEXAKLSJETGNCJTTGSNPPSHZUKZ DHHYHBBWKJUSIBAKGKHQJINZHCWLBCIIUGTVVLNEZXUBIPUVRAILLENTRJYFNIBHNOUNYAIFQBNUMFUSXNGITFIFZKTSFAQXDYVBIUCIUYJIGJ TIJHWTPPRJQVSBHHUXLZRPPJOWJAPSVQQVKLFHKXZRPEJBFXNKVNBCPMLRQGCJINKLLBJVROFAFCDRFCDAMIDEYSZDWNLUMJZXGWKOIKNAYVXP YRZWMBNAAFKFOPCVNGUECOARMDWJVYVUQQAFEGKCYXVVGXPHPEVOMRADTQDTJSHAKHPNNOGUDWBRXDJFEMSJTJUJKHZONBLGDCDD UDTRQKPOFACELSKHFSBPKXKDGWOKSDBAMWLKXEAOOHWVOAQZGZCNSDWOXSHPTFMVMYQXTRNMUPZSFQXOQLPUFJWHWTXXIRMQXDPV AJKHMSCGTFVJKECYILRMHGFBWQKUNTRVZTBJQJAKTSJUIDOLPL

C:\Users\user\AppData\Local\Temp\tmpA81F.tmp

Process:	C:\Users\user\Desktop\workalone.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.69486718145169
Encrypted:	false
SSDEEP:	24:XvKYeI9D5UOyoiaxIKgpZ9ONvMyTONN5ZjJH1U:yyD6yxILZ9OtTT+XRG
MD5:	E63B196AE0D5F7670244FB1347D75EFC
SHA1:	1C17108AC7E5263674836BAD67AE44D8C3C6890B
SHA-256:	D8C0D7B9CDFC72CAAB0A7687299B6734708E98C6DD088CDB0FF1A659E294B49D
SHA-512:	63345352964E1BD19AC843F82820E9B29C5BA991A002AB9B3164E1AA10B6D88BFA0DFAFA2E91E584835BA89B6A1770140AC14EA0B4B64E6C3BF8CDA34C9698AC
Malicious:	false
Preview:	LIJDSFKJZGBDGXNCCVBULCELYCDFJRIXKMFPVDHHKPYEYOXKFYMNEETRQHXLDRVBOTNERMYOYUJOPHUSKFPWBGKNJYBGZTTHNKGNUZWATSMORY BOIKBFSVUUMZNDYXOYKYUKGRNFVRQOPBEEIPDGTPBXCNLKHMGPHFCEQOUTEDGJZTMFUUGECZETRSODGZCJVQEAMRZADPDVQRANZO SHTGPOXPXGXXQDJVYZOCNXDECWJISPPIJOZUBSSKPGODUHTISNESPZRLELINJJYOXSBFTVUDENIBRDIMMGFIQNDGUSXDBHQNJRYLFTZGOCELKZ GOQQKNDPFAMTXHBKHJYXYEGLJLANRMMTCVEFYRTWLXIMCCHDWVOLGVUWRNLSIBMLMBKVSYLKXRTMZROHVHCRDBCODTPNVQMBPRJG BGOOFVGDIERMXUFETJQWDXSQQFMQAZGGRVNRCUOAVYJDIMQETJOANIIDEGJCHEFRSNVBQAQBBUTTMXBTJXRHLSOCTPPBIKPXITOOCINTVZYAVQ LVOOZWSOPLYJPOTKFKIKEHIDDPCDDEPKVDYQAVTVBFYYWCGUKGIDVLQSIPXISDEDNJWONTSILFUGUYMKQLKEJGOOCBYSXDFHNFHHWGLXWWQKSS OHSSTZLRZVRHZVBZGGEZQFSIWQQPMILSPBAMPAGAHHVJJCITDTJRZTRBEXSXOVDKONGLMSWBAOOYAFISJHKEYUKIWXBFUDUMVQRELEPVTNQBAL AQOEAEFVPIKNYIPNICGKQFRVXNQUEFULLOYWMHOMUFEMHYNKNWMAOBGWSECZOKWISDOIKSUVWBGWPNAMFUHBRWEJQPHFPEKIRLAE PTBNRQEUVXXIZSSOOEFEETUMNPSVEAKOXVYHAOIXBEYBVXDJXZCNDVOPZLARFFUSXUOWXQBKDLINBWBQLXLHHNIXZEPCNHFEIZUZSTXWFUITSB KYSELMNKNBBDQMNLAIOSKYHCWGFPNUXAFSRHOWYH

C:\Users\user\AppData\Local\Temp\tmpA820.tmp

Process:	C:\Users\user\Desktop\workalone.exe
File Type:	ASCII text, with very long lines (1024), with CRLF line terminators
Category:	dropped
Size (bytes):	1026
Entropy (8bit):	4.694142261581685
Encrypted:	false
SSDEEP:	24:f9GDi2EYjkpBrLp83PYbuFr5oKIQppDgX+qrctnWyd3z+g8BHGZ:yEYjkpZYwS/oKluA+qriTjEBHe
MD5:	E9AA17F314E072EBB015265FB63E77C0
SHA1:	1233B76350B8181FFFC438B62002C02B4AE79000
SHA-256:	F66078FCFEC2D71549136CC8B5B4EE7D33C4994E0A4E3E7C11F5ADCD819D0436
SHA-512:	719E659924CE585E4DD8CEA9BC6B5371AD810999022F874F380F50C7153D3AE97CC934E3173EF06573CAEE6CBC835A668C4D7DC2ADE597B1B0D200FCBAC67A1
Malicious:	false
Preview:	WSHEJMDVQCWJPIIWMEHEPOBRYLOZOHFMDEEYYASRZPHJZGFNCKWIQSPBUMWBCKDMTEBFINALYAFGJUQXINNGDKSDBFBQLHYZRLLDJYSVNXVIEP IYHZGOTARYUNPFNZVRVVWIOWWFIFWCHVVHXNGKFNRNLVVSOPOMGZCDQUWJFARKTCAVVDPTCPNIDLRGSLNKZTVRAJAILYGDVIAAGIVKXRCRTRZJ PKATKZAWRJTPVLTDNBDIRDWCCHBTEVEGYPYDTGSMLUDQXMQCAVHLYMRKPCVHQHMGNCGBZKOUKCCBHQPSIYIJGDVOYJJJRQLDKNVUEXDKCTANSM CHJUBIODALXWUAFPSECIRPCAEPPBACCLXBZAEDKJHLGOICLSKBQEGFCVDQOFKKAJPCTRIXBNPUDXKHSSXTDTQZSFEWHTHKFNJWHOEXGCYSYWIH FSMYJIYEESDQFMESLFQFBUJNXHWFNXIDWEUDMVGFDXPTRRRNPARVUGZAYZRHNTXHZAPBLWMHFSSHMXCYMAGONQNLTCAVPZPCAKJRMGEPDIFETD NSXWPDVMAZGTTCLNRREMVTBLOGKASYOATUDXLJKIYPPDNLZIZMWWFFDVMUFCTZZOFJORNAMGQBAFGCPTDCZBKTIGYDSCSPMIEXAMGICZNTFVNR PLGPMBXJHNCQSYNMGGPKIQJNDBDUBVIVXFILKXZXHODXZAYIDEIMZZMKQNQNBCCMZNFBKSYULDGKOMQZDUQMUVTBBTUTRZMIOZGDEUPHCDKJQD SGBXYNWPWTHYVLGGYNOBJJKAZSTKJSBCHVCLGWYHCNILYSCYCHTGYOGMNGWDZAVDCOVKWJPWVNTTKFTSHAAXLYUEWEVGETFCFTLK WTQCVAMBWYOYJVXNPSSWXJXUZDXJOZNTBLIZLLJQXYNILILMHHONBPAPFMVWEMHIHAGMOXTIBNNEBGCVSZEZTMJVDXSVACSKTAVTFOOSEHZQGT OUSCIQBVIWZGABQNZGJE

C:\Users\user\AppData\Local\Temp\tmpAFBA.tmp	
Process:	C:\Users\user\Desktop\workalone.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\tmpB611.tmp	
Process:	C:\Users\user\Desktop\workalone.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 2, database pages 23, cookie 0x19, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.7876734657715041
Encrypted:	false
SSDEEP:	48:43KzOIIY3HzrkNSs8LKvUf9KnmlG0UX9q4lCm+KLka+yJqhM0ObVEq8Ma0D0HOlx:Sq0NFeymDlGD9qlm+KL2y0Obn8MouO
MD5:	CF7758A2FF4A94A5D589DEBAED38F82E
SHA1:	D3380E70D0CAEB9AD78D14DD970EA480E08232B8
SHA-256:	6CA783B84D01BFCF9AA7185D7857401D336BAD407A182345B97096E1F2502B7F
SHA-512:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804CB F
Malicious:	false
Preview:	SQLite format 3.....@ .....[5..... ....

C:\Users\user\AppData\Local\Temp\tmpB641.tmp	
Process:	C:\Users\user\Desktop\workalone.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 2, database pages 23, cookie 0x19, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.7876734657715041
Encrypted:	false
SSDEEP:	48:43KzOIIY3HzrkNSs8LKvUf9KnmlG0UX9q4lCm+KLka+yJqhM0ObVEq8Ma0D0HOlx:Sq0NFeymDlGD9qlm+KL2y0Obn8MouO
MD5:	CF7758A2FF4A94A5D589DEBAED38F82E
SHA1:	D3380E70D0CAEB9AD78D14DD970EA480E08232B8
SHA-256:	6CA783B84D01BFCF9AA7185D7857401D336BAD407A182345B97096E1F2502B7F
SHA-512:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804CB F
Malicious:	false

Preview:	SQLite format 3.....@ .....[5.....

C:\Users\user\AppData\Local\Temp\tmpE08F.tmp

Process:	C:\Users\user\Desktop\workalone.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*

C:\Users\user\AppData\Local\Temp\tmpE6B7.tmp

Process:	C:\Users\user\Desktop\workalone.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 2, database pages 23, cookie 0x19, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.7876734657715041
Encrypted:	false
SSDEEP:	48:43KzOIIY3HzrkNSs8LKvUf9KnmlG0UX9q4lCm+KLka+yJqhM0ObVEq8Ma0D0HOlx:Sq0NFeymDlGD9qlm+KL2y0Obn8MouO
MD5:	CF7758A2FF4A94A5D589DEBAED38F82E
SHA1:	D3380E70D0CAEB9AD78D14DD970EA480E08232B8
SHA-256:	6CA783B84D01BFCF9AA7185D7857401D336BAD407A182345B97096E1F2502B7F
SHA-512:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804CBF
Malicious:	false
Preview:	SQLite format 3.....@ .....[5.....

C:\Users\user\AppData\Local\Temp\tmpE939.tmp

Process:	C:\Users\user\Desktop\workalone.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*

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

Process:	C:\Windows\SysWOW64\cmd.exe

File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	348672
Entropy (8bit):	5.276672751026678
Encrypted:	false
SSDEEP:	3072:kd4jFS378hlr02cpbHrxfV0WzJsQuJpnpvcPavg3igp06mLkXDQWmE6:W378ib70cWpnv2+6mLkzQE6
MD5:	68F42F485ECE93306BEF1E4084D3052E
SHA1:	C63F1A56D12A0ACBF5E9A354D8A66C6E17AF2309
SHA-256:	5D526BE000146CF9CF94F7EF6F4E86929D508E17CA483B03D4ECBD2D52E071C9
SHA-512:	75E09E7505039A7EB0D0652666F3ED258D50C2536BB3877C2E1503E69700AAE6A8014EF6B8F4F7F41BFA11F857CF0240F1A950F66395D19AE12707DB863C1242
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...PT.c.....R.....Fp... .....@.. ....@.....o..J..... ....H.....text...LP... ...R..... ..`.rsrc.....T.....@..@.rel oc.....P.....@..B.....,p.....H.....a.....p.....(W...*.0..U.....~.... ....(t....-.&~....~....(.....(....&..,&.#.+..+..~.....(....~.....(....s X...z.*.....66.....0.....~Y....:....&sZ....9....&~.....~.... ....(t....:}...&&&~.....~.... ....(t....-l&&&~.....~....~.... ....(t....(.....,M&&&~.....,G&&&.-..9.....~.....(....&~....(....&...-.8h... (....8|...(....+.(....+.(....+.&...,....9#....*.8'.....0..^.....-i~....~...

C:\Users\user\AppData\Roaming\svchost\svchost.exe:Zone.Identifier

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.276672751026678
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	workalone.exe
File size:	348672
MD5:	68f42f485ece93306bef1e4084d3052e
SHA1:	c63f1a56d12a0acbf5e9a354d8a66c6e17af2309
SHA256:	5d526be000146cf9cf94f7ef6f4e86929d508e17ca483b03d4ecbd2d52e071c9
SHA512:	75e09e7505039a7eb0d0652666f3ed258d50c2536bb3877c2e1503e69700aae6a8014ef6b8f4f7f41bfa11f857cf0240f1a950f66395d19ae12707db863c1242
SSDEEP:	3072:kd4jFS378hlr02cpbHrxfV0WzJsQuJpnpvcPavg3igp06mLkXDQWmE6:W378ib70cWpnv2+6mLkzQE6
TLSH:	747439267384DF26C79223B7C6035BA002184C197785EE76A4E529FC94A1FFAD9CF193
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...PT.c.....R.....Fp... .....@.. .....@.....

File Icon

Icon Hash:	64c68eb2b3b686c4

Static PE Info

General

Entrypoint:	0x427046
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x63865450 [Tue Nov 29 18:49:52 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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
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 2022

Instruction
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	0x26ffc	0x4a	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x28000	0x2faa4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x58000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x2504c	0x25200	False	0.8109743265993266	data	7.585773646811085	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x28000	0x2faa4	0x2fc00	False	0.08600908049738219	data	2.4474216242910125	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x58000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x280b4	0x13ca	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x294a2	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 67584		
RT_ICON	0x39cee	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 38016		
RT_ICON	0x431ba	0x67e8	Device independent bitmap graphic, 80 x 160 x 32, image size 26560		
RT_ICON	0x499c6	0x5488	Device independent bitmap graphic, 72 x 144 x 32, image size 21600		
RT_ICON	0x4ee72	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16896		
RT_ICON	0x530be	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600		
RT_ICON	0x5568a	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224		
RT_ICON	0x56756	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400		
RT_ICON	0x57102	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088		
RT_GROUP_ICON	0x575b8	0x92	data		
RT_VERSION	0x57686	0x1f8	data	English	United States
RT_MANIFEST	0x578ba	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Copyright Joe Security LLC 2022

Imports

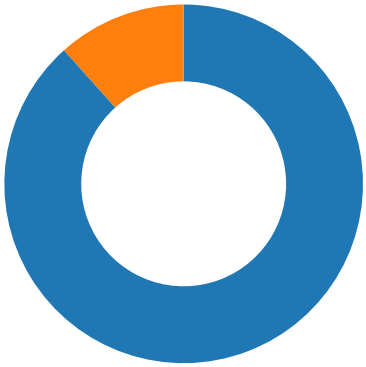
DLL	Import
mscoree.dll	_CorExeMain

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:07:25.722348928 CET	49685	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:07:25.752378941 CET	46539	49685	85.208.136.178	192.168.2.3
Nov 30, 2022 00:07:25.752796888 CET	49685	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:07:26.016802073 CET	49685	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:07:26.088752985 CET	46539	49685	85.208.136.178	192.168.2.3
Nov 30, 2022 00:07:26.213782072 CET	46539	49685	85.208.136.178	192.168.2.3
Nov 30, 2022 00:07:26.218960047 CET	49685	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:07:26.290599108 CET	46539	49685	85.208.136.178	192.168.2.3
Nov 30, 2022 00:07:26.380656004 CET	46539	49685	85.208.136.178	192.168.2.3
Nov 30, 2022 00:07:26.424237013 CET	49685	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:07:34.937004089 CET	49685	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:07:34.972991943 CET	46539	49685	85.208.136.178	192.168.2.3
Nov 30, 2022 00:07:35.004894972 CET	49685	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:07:35.055725098 CET	46539	49685	85.208.136.178	192.168.2.3
Nov 30, 2022 00:07:35.055794954 CET	46539	49685	85.208.136.178	192.168.2.3
Nov 30, 2022 00:07:35.055846930 CET	46539	49685	85.208.136.178	192.168.2.3
Nov 30, 2022 00:07:35.055901051 CET	46539	49685	85.208.136.178	192.168.2.3
Nov 30, 2022 00:07:35.056029081 CET	49685	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:07:35.056374073 CET	49685	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:07.861217022 CET	49685	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:07.890326023 CET	46539	49685	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:07.890465021 CET	49685	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:08.012422085 CET	49687	46539	192.168.2.3	85.208.136.178

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:08:08.040680885 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.040882111 CET	49687	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:08.051173925 CET	49687	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:08.118521929 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.179694891 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.181700945 CET	49687	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:08.210653067 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.212898016 CET	49687	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:08.242925882 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.243597984 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.243987083 CET	49687	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:08.272692919 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.272722960 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.273192883 CET	49687	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:08.273495913 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.273772001 CET	49687	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:08.274296045 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.300961971 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.301352024 CET	49687	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:08.301760912 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.301800013 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.302026987 CET	49687	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:08.302115917 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.302129030 CET	49687	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:08.302516937 CET	49687	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:08.302608967 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.302635908 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.302661896 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.302783012 CET	49687	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:08.304261923 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.329659939 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.329730988 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.329937935 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.330197096 CET	49687	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:08.330393076 CET	49687	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:08.330487013 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.331543922 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.331660986 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.331897974 CET	49687	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:08.332432032 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.332724094 CET	49687	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:08.333273888 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.333509922 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.333692074 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.333694935 CET	49687	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:08.333961010 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.334039927 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.334115982 CET	49687	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:08.335695982 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.335901022 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.357816935 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.358990908 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.359028101 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.359174967 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.359221935 CET	49687	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:08.359349966 CET	49687	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:08.359509945 CET	49687	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:08.359599113 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.359643936 CET	46539	49687	85.208.136.178	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:08:08.359833002 CET	49687	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:08.360557079 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.361654997 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.361905098 CET	49687	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:08.362641096 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.362689018 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.362763882 CET	49687	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:08.363637924 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.364617109 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.365525007 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.365761995 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.365890026 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.365921021 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.365948915 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.365995884 CET	49687	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:08.366144896 CET	49687	46539	192.168.2.3	85.208.136.178
Nov 30, 2022 00:08:08.366528034 CET	46539	49687	85.208.136.178	192.168.2.3
Nov 30, 2022 00:08:08.367007971 CET	46539	49687	85.208.136.178	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 30, 2022 00:07:25.575783014 CET	63722	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:07:25.687061071 CET	53	63722	8.8.8.8	192.168.2.3
Nov 30, 2022 00:07:35.732409954 CET	65522	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:07:35.763092995 CET	59869	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:08:07.898642063 CET	54397	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:08:08.008116007 CET	53	54397	8.8.8.8	192.168.2.3
Nov 30, 2022 00:08:10.978208065 CET	59324	53	192.168.2.3	8.8.8.8
Nov 30, 2022 00:08:11.086960077 CET	53	59324	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 30, 2022 00:07:25.575783014 CET	192.168.2.3	8.8.8.8	0x9fd4	Standard query (0)	saleshor12 .duckdns.org	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:07:35.732409954 CET	192.168.2.3	8.8.8.8	0x7e82	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:07:35.763092995 CET	192.168.2.3	8.8.8.8	0x48a3	Standard query (0)	api.ip.sb	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:08:07.898642063 CET	192.168.2.3	8.8.8.8	0xe5fe	Standard query (0)	saleshor12 .duckdns.org	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:08:10.978208065 CET	192.168.2.3	8.8.8.8	0x3609	Standard query (0)	saleshor12 .duckdns.org	A (IP address)	IN (0x0001)	false

DNS Answers

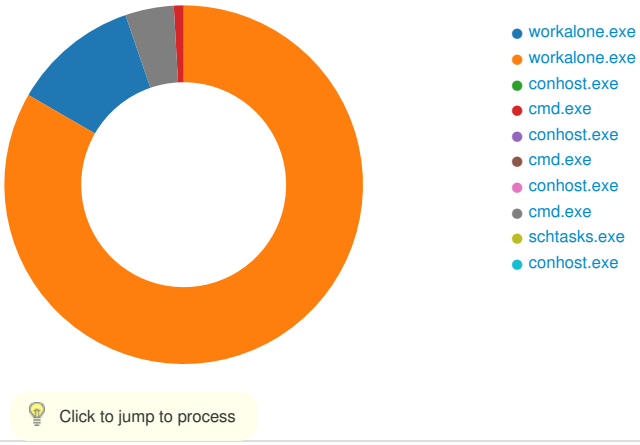
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 30, 2022 00:07:25.687061071 CET	8.8.8.8	192.168.2.3	0x9fd4	No error (0)	saleshor12 .duckdns.org		85.208.136.178	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:07:35.754019976 CET	8.8.8.8	192.168.2.3	0x7e82	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 00:07:35.783816099 CET	8.8.8.8	192.168.2.3	0x48a3	No error (0)	api.ip.sb	api.ip.sb.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 30, 2022 00:08:08.008116007 CET	8.8.8.8	192.168.2.3	0xe5fe	No error (0)	saleshor12 .duckdns.org		85.208.136.178	A (IP address)	IN (0x0001)	false
Nov 30, 2022 00:08:11.086960077 CET	8.8.8.8	192.168.2.3	0x3609	No error (0)	saleshor12 .duckdns.org		85.208.136.178	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- saleshor12.duckdns.org:46539

Statistics

Behavior



System Behavior

Analysis Process: workalone.exe PID: **5836**, Parent PID: **3452**

General

Target ID:	0
Start time:	00:06:58
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\workalone.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\workalone.exe
Imagebase:	0x590000
File size:	348672 bytes
MD5 hash:	68F42F485ECE93306BEF1E4084D3052E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000000.00000002.270249352.00000000039F9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.270249352.00000000039F9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_f54632eb, Description: unknown, Source: 00000000.00000002.270249352.00000000039F9000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

Analysis Process: workalone.exe PID: **5956**, Parent PID: **5836**

General

Target ID:	1
Start time:	00:07:06
Start date:	30/11/2022
Path:	C:\Users\user\Desktop\workalone.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\workalone.exe
Imagebase:	0xd20000
File size:	348672 bytes
MD5 hash:	68F42F485ECE93306BEF1E4084D3052E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000000.262815044.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000000.262815044.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_f54632eb, Description: unknown, Source: 00000001.00000000.262815044.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000001.00000002.406713080.000000000309F000.00000004.00000800.00020000.00000000.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	6D3BCF06	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	6D3BCF06	unknown
C:\Users\user\AppData\Local\Temp\tmpE6B7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp1B45.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp82DA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp8319.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpB611.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpB641.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpE939.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp1B56.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp4D35.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp4D74.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp7EB6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpAFBA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE08F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp10B8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp10E8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp4075.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp6FB4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp6FE4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp93B7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpA720.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpA760.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpA790.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpA7C0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpA7F0.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpA81F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpA820.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C207038	GetTempFileNameW
C:\Users\user\AppData\Local\Yandex	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C20BEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Yandex\YaAddon	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C20BEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1B45.tmp	success or wait	1	6C206A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpE6B7.tmp	success or wait	1	6C206A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp8319.tmp	success or wait	1	6C206A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp82DA.tmp	success or wait	1	6C206A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpB641.tmp	success or wait	1	6C206A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpB611.tmp	success or wait	1	6C206A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp1B56.tmp	success or wait	1	6C206A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpE939.tmp	success or wait	1	6C206A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp4D74.tmp	success or wait	1	6C206A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp4D35.tmp	success or wait	1	6C206A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpAFBA.tmp	success or wait	1	6C206A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp7EB6.tmp	success or wait	1	6C206A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp10B8.tmp	success or wait	1	6C206A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpE08F.tmp	success or wait	1	6C206A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp4075.tmp	success or wait	1	6C206A95	DeleteFileW

Copyright Joe Security LLC 2022

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp10E8.tmp	success or wait	1	6C206A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp6FE4.tmp	success or wait	1	6C206A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp6FB4.tmp	success or wait	1	6C206A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp93B7.tmp	success or wait	1	6C206A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpA720.tmp	success or wait	1	6C206A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpA760.tmp	success or wait	1	6C206A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpA790.tmp	success or wait	1	6C206A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpA7C0.tmp	success or wait	1	6C206A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpA7F0.tmp	success or wait	1	6C206A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpA81F.tmp	success or wait	1	6C206A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpA820.tmp	success or wait	1	6C206A95	DeleteFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

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	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D395705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D39CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D395705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C201B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C201B4F	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	6D2F03DE	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	2	6C201B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	28	6C201B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	6C201B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp1B45.tmp	unknown	49152	success or wait	1	6C201B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	2	6C201B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp8319.tmp	unknown	49152	success or wait	1	6C201B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpB641.tmp	unknown	49152	success or wait	1	6C201B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	3	6C201B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	3	6C201B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp1B56.tmp	unknown	94208	success or wait	1	6C201B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp4D74.tmp	unknown	94208	success or wait	1	6C201B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpAFBA.tmp	unknown	94208	success or wait	1	6C201B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	2	6C201B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	2	6C201B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp10B8.tmp	unknown	94208	success or wait	1	6C201B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp4075.tmp	unknown	94208	success or wait	1	6C201B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp6FE4.tmp	unknown	94208	success or wait	1	6C201B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmp93B7.tmp	unknown	4096	success or wait	1	6C201B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA720.tmp	unknown	4096	success or wait	1	6C201B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA760.tmp	unknown	4096	success or wait	1	6C201B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA790.tmp	unknown	4096	success or wait	1	6C201B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA7C0.tmp	unknown	4096	success or wait	1	6C201B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA7F0.tmp	unknown	4096	success or wait	1	6C201B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA81F.tmp	unknown	4096	success or wait	1	6C201B4F	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA820.tmp	unknown	4096	success or wait	1	6C201B4F	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **5964**, Parent PID: **5956**

General

Target ID:	2
Start time:	00:07:06
Start date:	30/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **5972**, Parent PID: **5836**

General

Target ID:	3
Start time:	00:07:06
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd" /c mkdir "C:\Users\user\AppData\Roaming\svchost
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\svchost	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	BBFE7	CreateDirectoryW

Analysis Process: conhost.exe PID: **6020**, Parent PID: **5972**

General	
Target ID:	4
Start time:	00:07:07
Start date:	30/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **6040**, Parent PID: **5836**

General	
Target ID:	5
Start time:	00:07:07
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"cmd" /c schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\user\AppData\Roaming\svchost\svchost.exe'" /f
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6072**, Parent PID: **6040**

General	
Target ID:	6
Start time:	00:07:07
Start date:	30/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: **6080**, Parent PID: **5836**

General	
Target ID:	7
Start time:	00:07:07
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd" /c copy "C:\Users\user\Desktop\workalone.exe" "C:\Users\user\AppData\Roaming\svchost\svchost.exe
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\svchost\svchost.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	B4E97	CopyFileExW
C:\Users\user\AppData\Roaming\svchost\svchost.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	B4E97	CopyFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\svchost\svchost.exe	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 50 54 fd 63 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 08 00 00 52 02 00 00 fd 02 00 00 00 00 00 46 70 02 00 00 20 00 00 00 fd 02 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 fd 05 00 00 02 00 00 00 00 00 00 02 00 40 fd 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.$PELPTcRFp @ @	success or wait	3	B4E97	CopyFileExW
C:\Users\user\AppData\Roaming\svchost\svchost.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	B4E97	CopyFileExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\workalone.exe	unknown	512	success or wait	1	B5742	ReadFile

Copyright Joe Security LLC 2022

Analysis Process: schtasks.exe PID: **6108**, Parent PID: **6040**

General	
Target ID:	8
Start time:	00:07:07
Start date:	30/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /create /sc minute /mo 1 /tn "Nafifas" /tr "'C:\Users\user\AppData\Roaming\svchost\svchost.exe'" /f
Imagebase:	0x960000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **6124**, Parent PID: **6080**

General	
Target ID:	9
Start time:	00:07:08
Start date:	30/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly

Copyright Joe Security LLC 2022