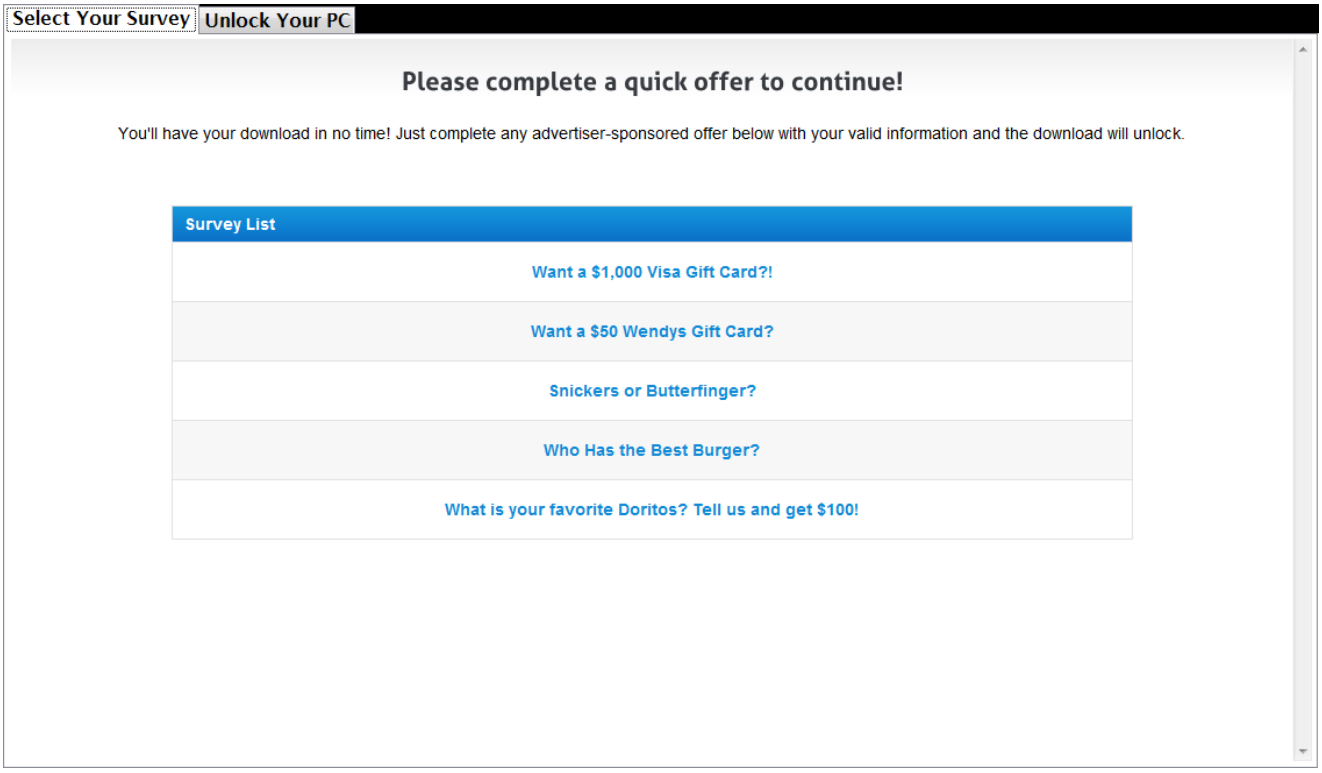
In-Dev Ransomware forces you do to Survey before unlocking Computer

bleepingcomputer.com/news/security/in-dev-ransomware-forces-you-do-to-survey-before-unlocking-computer

By
Lawrence Abrams

- October 27, 2016
- 02:56 PM
- 1

As if surveys aren't already annoying, a new ransomware utilizes the FileIce survey platform to force you to do surveys before unlocking your computer. First discovered by GData security researcher Karsten Hahn, this ransomware is currently in development and is most likely not being actively distributed at this time.



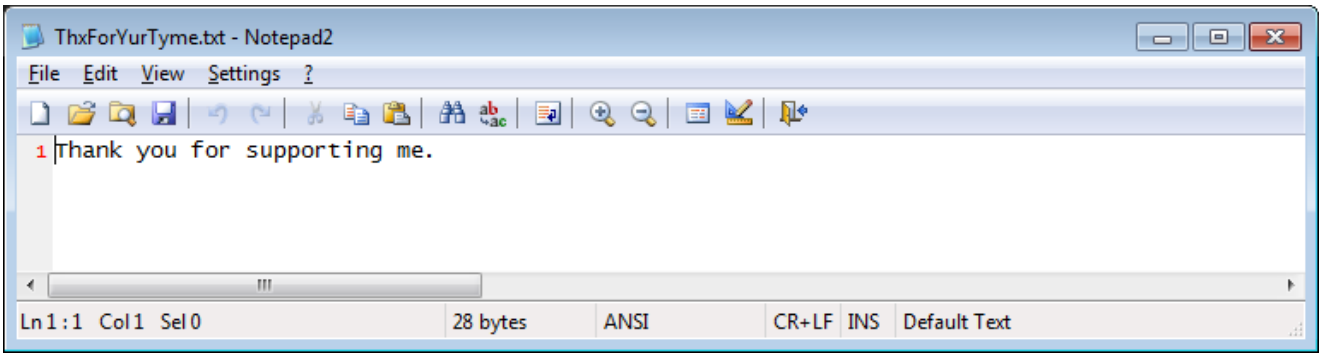
Select Your Survey Screen

When the malware is started it will display a Select Your Survey form as shown above that contains numerous surveys you can select in order to unlock the computer. The ransomware retrieves these surveys from the URL www.fileice.net/download.php?t=regular&file=3lhzu as shown in the source code below.

```
// Token: 0x0600006C RID: 108 RVA: 0x00003D80 File Offset: 0x00002180
private void Form1_Load(object sender, EventArgs e)
{
    eWebbrowser eWebbrowser = new eWebbrowser();
    this.wb = eWebbrowser;
    eWebbrowser.Dock = DockStyle.Fill;
    eWebbrowser.IsWebBrowserContextMenuEnabled = false;
    eWebbrowser.ScriptErrorsSuppressed = true;
    this.SurveyList.Controls.Add(eWebbrowser);
    eWebbrowser.Navigate("http://www.fileice.net/download.php?t=regular&file=3lhzu");
}
```

Source showing the form retrieving the Surveys

When a user completes a survey, it will download a file called ThxForYurTyme.txt, which displays the message "Thank you for supporting me.".



Thank You File

My guess is that this file will eventually contain a code that will be used to unlock and remove the lock screen.

Not all features are functional

Since this ransomware is currently in development mode, it contains source code to perform a variety of functions that do not work as of yet. For example, though it does create an autostart so the programs starts when you login, it also contains numerous other features that do not work right. For example, it contains code to disable Ctrl+Alt+Del and code to set a variety of Windows policies to make it more difficult to remove, but they failed to be created on my test.

The policies that it attempts to enable are:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System "DisableTaskMgr" = 1
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
"DisableLockWorkstation" = 1
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
"DisableChangePassword" = 1
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer "NoClose" = 1
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer "NoLogoff" = 1
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
"HideFastUserSwitching" = 1
```

What makes it truly show that it is still in development is the Unlock Your PC screen. This screen contains numerous debugging options that can be used to test the ransomware.

Unlock Your PC Screen

For example, the **startup** button will enable the autostart entry for the ransomware, the **Close** button will terminate the process, the **Clear Ctrl Alt** checkbox will enable or disable the policies, and the **Disable keys** button will attempt to hook the keyboard so that the keys do not work.

Like many other ransomware infections that are discovered, there is a good chance that this ransomware will never make it into distribution. If it does, though, it will be easily defeated.

Files associated with the Survey Ransomware:

```
C:\Users\User\Downloads\ThxForYurTyme.txt
C:\seo\Sdchost.exe
```

Registry entries associated with the Survey Ransomware

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Sdchost      C:\seo\Sdchost.exe
```

Network traffic associated with the Survey Ransomware

```
http://www.fileice.net/download.php?t=regular&file=3lhzu
```

Hashes:

SHA256: 60fba97585c3a48720bffdb1e11fb5be537e6b6344220015bc9740d084f58c0b

Related Articles:

Indian airline SpiceJet's flights impacted by ransomware attack

US Senate: Govt’s ransomware fight hindered by limited reporting

New RansomHouse group sets up extortion market, adds first victims

Ransomware attack exposes data of 500,000 Chicago students

The Week in Ransomware - May 20th 2022 - Another one bites the dust

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.