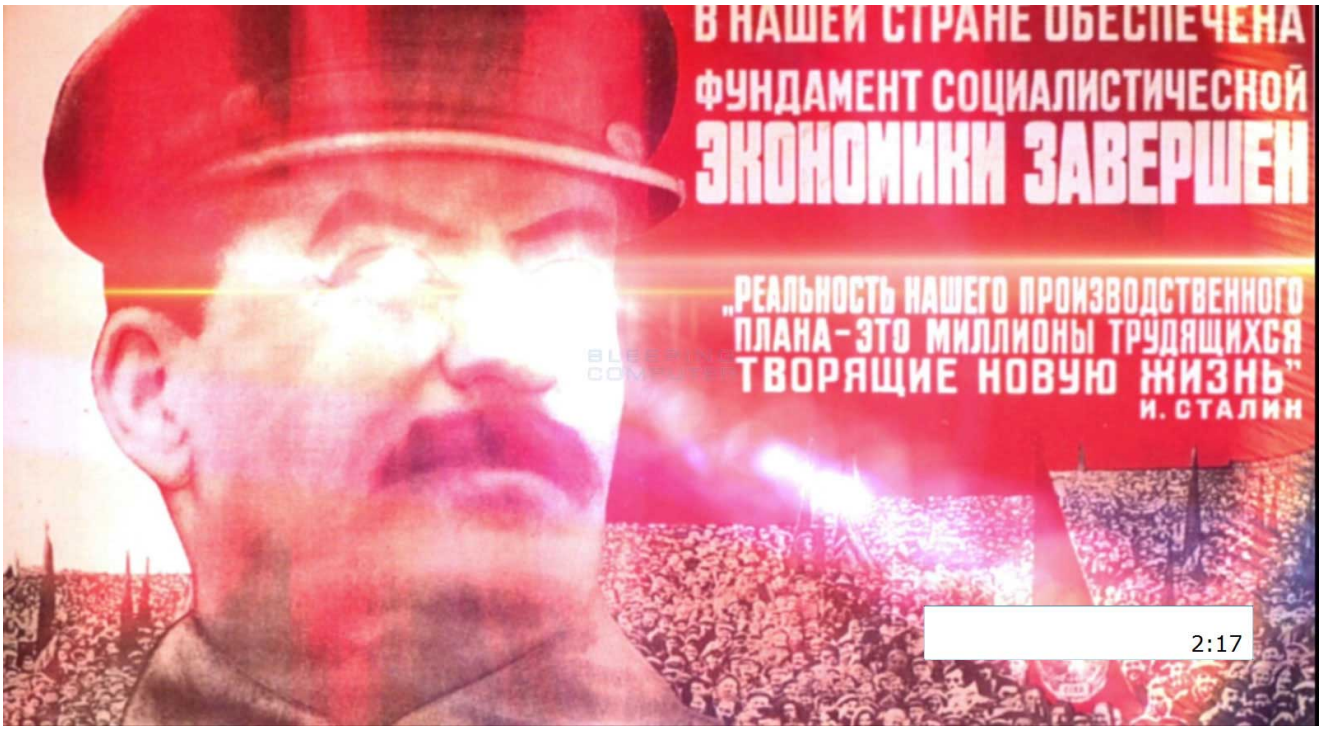
StalinLocker Deletes Your Files Unless You Enter the Right Code

bleepingcomputer.com/news/security/stalinlocker-deletes-your-files-unless-you-enter-the-right-code

By
Lawrence Abrams

- May 14, 2018
- 06:26 PM
- 0

A new in-development screenlocker/wiper called StalinLocker, or StalinScreamer, was discovered by MalwareHunterTeam that gives you 10 minutes to enter a code or it will try to delete the contents of the drives on the computer. While running, it will display screen that shows Stalin while playing the USSR anthem and displaying a countdown until files are deleted.



StalinLocker/StalinScreamer Lock Screen

When executed, StalinLocker will perform the following actions:

- Extract the "USSR_Anthem.mp3" file to the %UserProfile%\AppData\Local folder and play it. This anthem is the same one heard in this YouTube video, but of much worse quality.
- It will copy itself to %UserProfile%\AppData\Local\stalin.exe and create an autorun called "Stalin" that starts the screenlocker/wiper when the user logs into the computer.

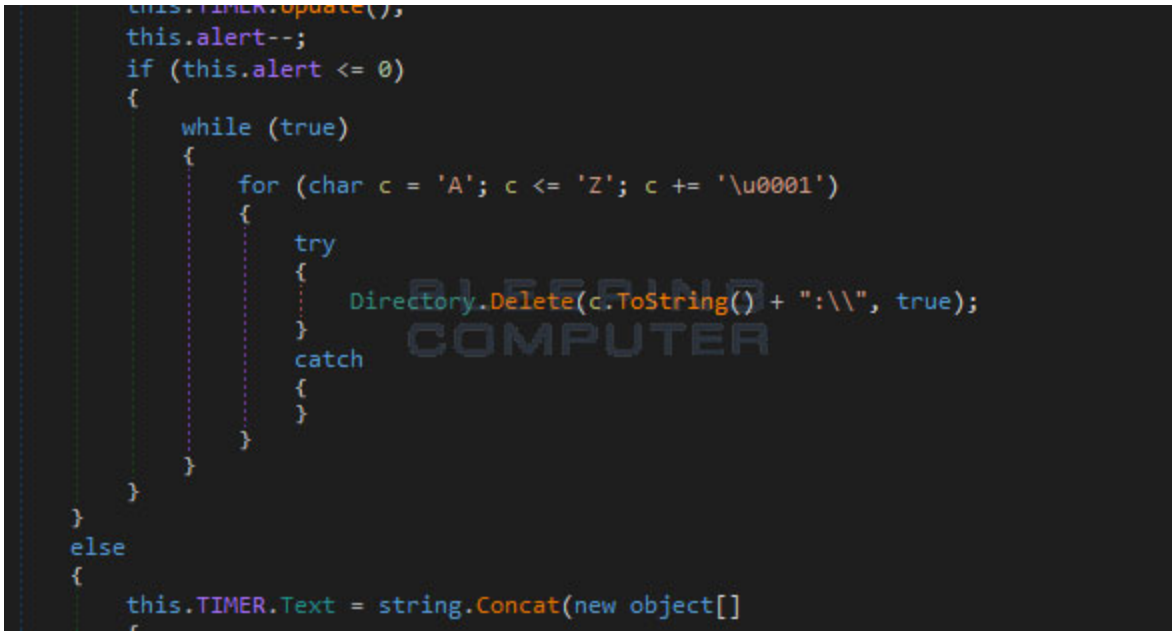
- It will create %UserProfile%\AppData\Local\fl.dat and write the current amount of seconds left divided by 3. So each time you start the program, the countdown is significantly less.
- Attempt to terminate processes other than Skype or Discord.
- Terminate Explorer.exe and taskmgr.exe.
- Tries to create a Scheduled Task called "Driver Update" to launch Stalin.exe. This part of the code is currently throwing errors.

StalinLocker will then display the above lock screen that contains a 10 minutes countdown until your files are deleted or you enter a code. According to MalwareHunterTeam, this code is derived by subtracting the current date of when the program was executed by the date 1922.12.30. If the user enters the correct code, the wiper will exit and delete the autorun.

```
private void KeyBox_TextChanged(object sender, EventArgs e)
{
    try
    {
        if (int.Parse(this.KeyBox.Text) == (this.n - this.dt).Days)
        {
            this.timer1.Stop();
            this.timer2.Stop();
            this.timer3.Stop();
            this.timer4.Stop();
            this.guessed = true;
            MessageBox.Show("Правильный ключ", "Уведомление", MessageBoxButtons.OK, MessageBoxIcon.Asterisk);
            try
            {
                using (TaskService taskService = new TaskService())
                {
                    taskService.get_RootFolder().DeleteTask("Driver Update", true);
                }
            }
            catch
            {
            }
            try
            {
                RegistryKey expr_AD = Registry.LocalMachine.OpenSubKey("SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\\", true);
                expr_AD.DeleteSubKey("Stalin");
                expr_AD.Close();
```


Enter Code Source

On the other hand, if the code is not entered by the time the countdown reaches zero, the screenlocker will attempt to delete all of the files on each drive letter found on the computer. This is done by going through all drive letters from A to Z and deleting any that are accessible as shown below.



Source code to delete files on drive letters A-Z

This wiper is currently in development, but could easily be made into a workable state. Thankfully, most security vendors are detecting this either through definitions or heuristics, so make sure that you have an anti-virus program installed and updated to the latest definitions.

Related Articles:

Beware: Onyx ransomware destroys files instead of encrypting them

IOCs

Hashes:

```
SHA256: 853177d9a42fab0d8d62a190894de5c27ec203240df0d9e70154a675823adf04
```

Associated Files:

```
%UserProfile%\AppData\Local\fl.dat
%UserProfile%\AppData\Local\stalin.exe
%UserProfile%\AppData\Local\USSR_Anthem.mp3
```

Associated Registry Entries:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Stalin
%UserProfile%\AppData\Local\stalin.exe
```


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.

- Previous Article
- Next Article

You may also like: