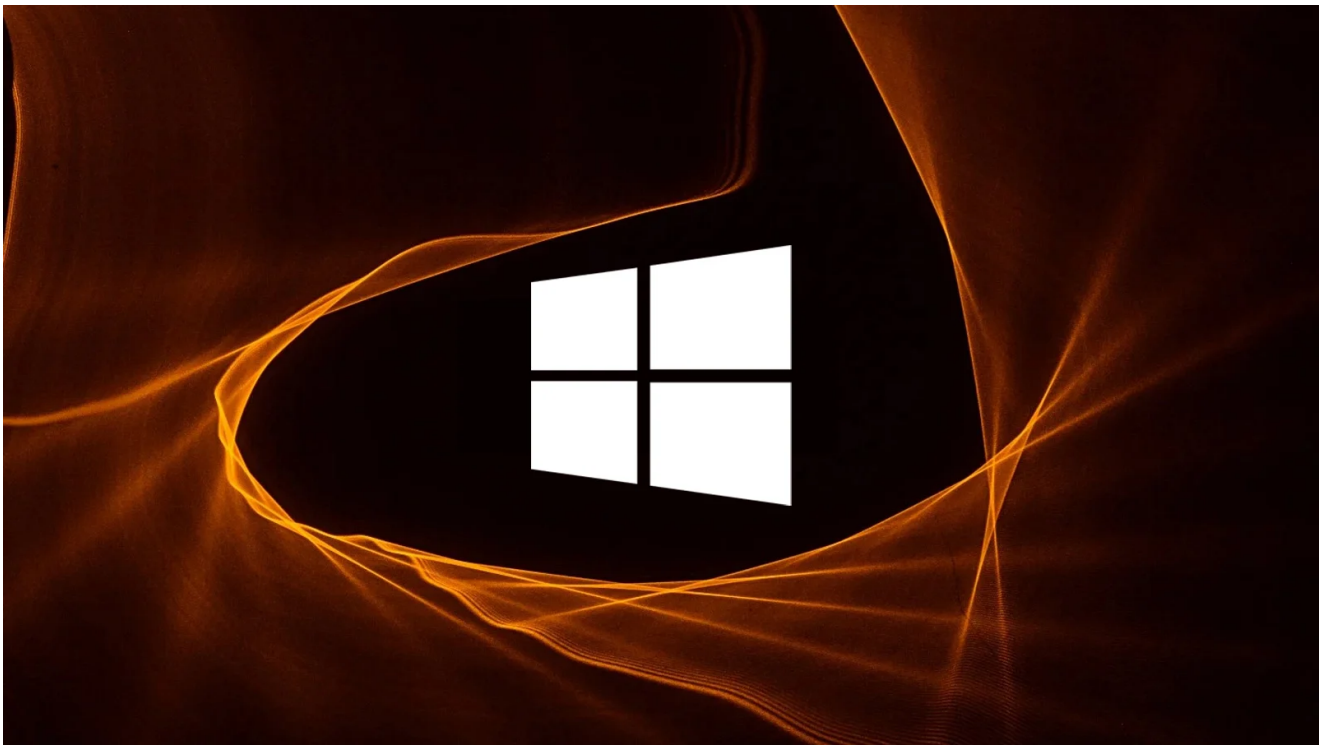
Fake Windows 10 updates infect you with Magniber ransomware

bleepingcomputer.com/news/security/fake-windows-10-updates-infect-you-with-magniber-ransomware/

Lawrence Abrams

By
Lawrence Abrams

- April 30, 2022
- 10:18 AM
- 7



Fake Windows 10 updates are being used to distribute the Magniber ransomware in a massive campaign that started earlier this month.

Over the past few days, BleepingComputer has received a surge of requests for help regarding a ransomware infection targeting users worldwide.

While researching the campaign, we discovered a topic in our forums where readers report becoming infected by the Magniber ransomware after installing what is believed to be Windows 10 cumulative or security update.

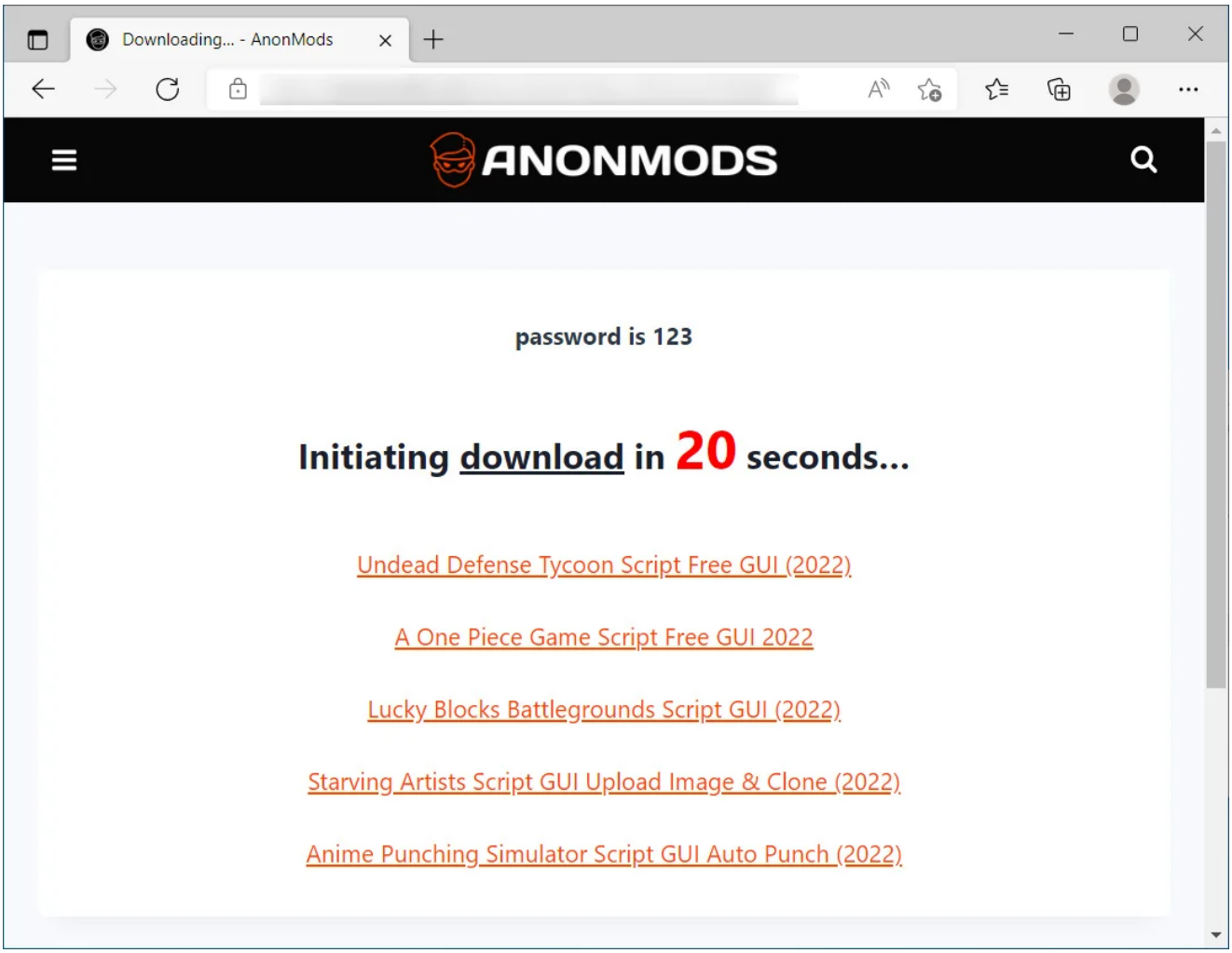
These updates are distributed under various names, with Win10.0_System_Upgrade_Software.msi [VirusTotal] and Security_Upgrade_Software_Win10.0.msi being the most common.

Other downloads pretend to be Windows 10 cumulative updates, using fake knowledge base articles, as shown below.

```
System.Upgrade.Win10.0-KB47287134.msi
System.Upgrade.Win10.0-KB82260712.msi
System.Upgrade.Win10.0-KB18062410.msi
System.Upgrade.Win10.0-KB66846525.msi
```

Based on the submissions to VirusTotal, this campaign appears to have started on April 8th, 2022 and has seen massive distribution worldwide since then.

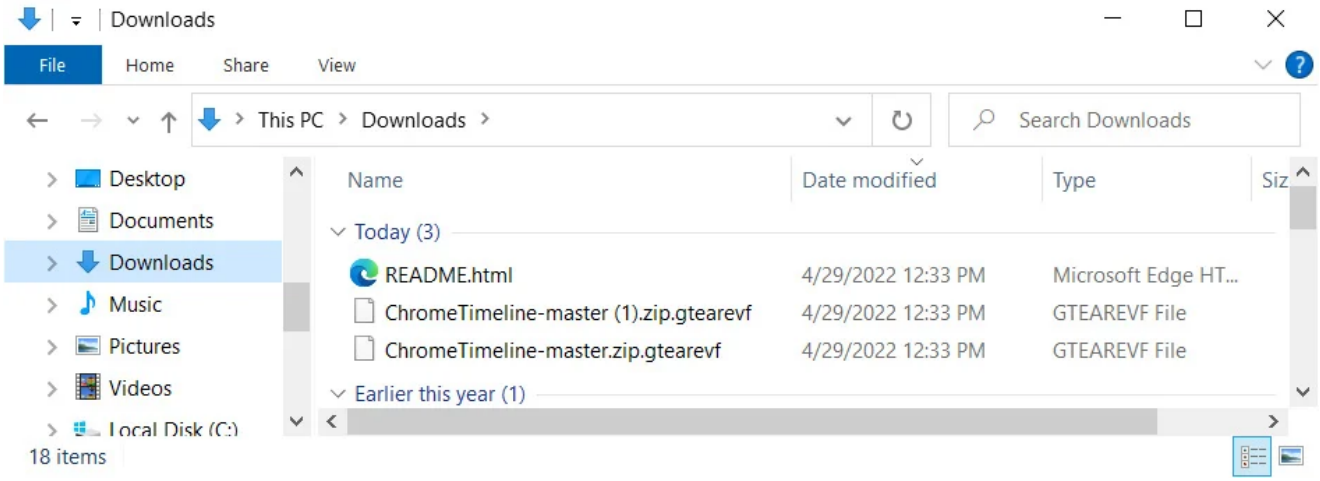
While it's not 100% clear how the fake Windows 10 updates are being promoted, the downloads are distributed from fake warez and crack sites.



Fake warez and crack sites pushing Magniber

Source: BleepingComputer

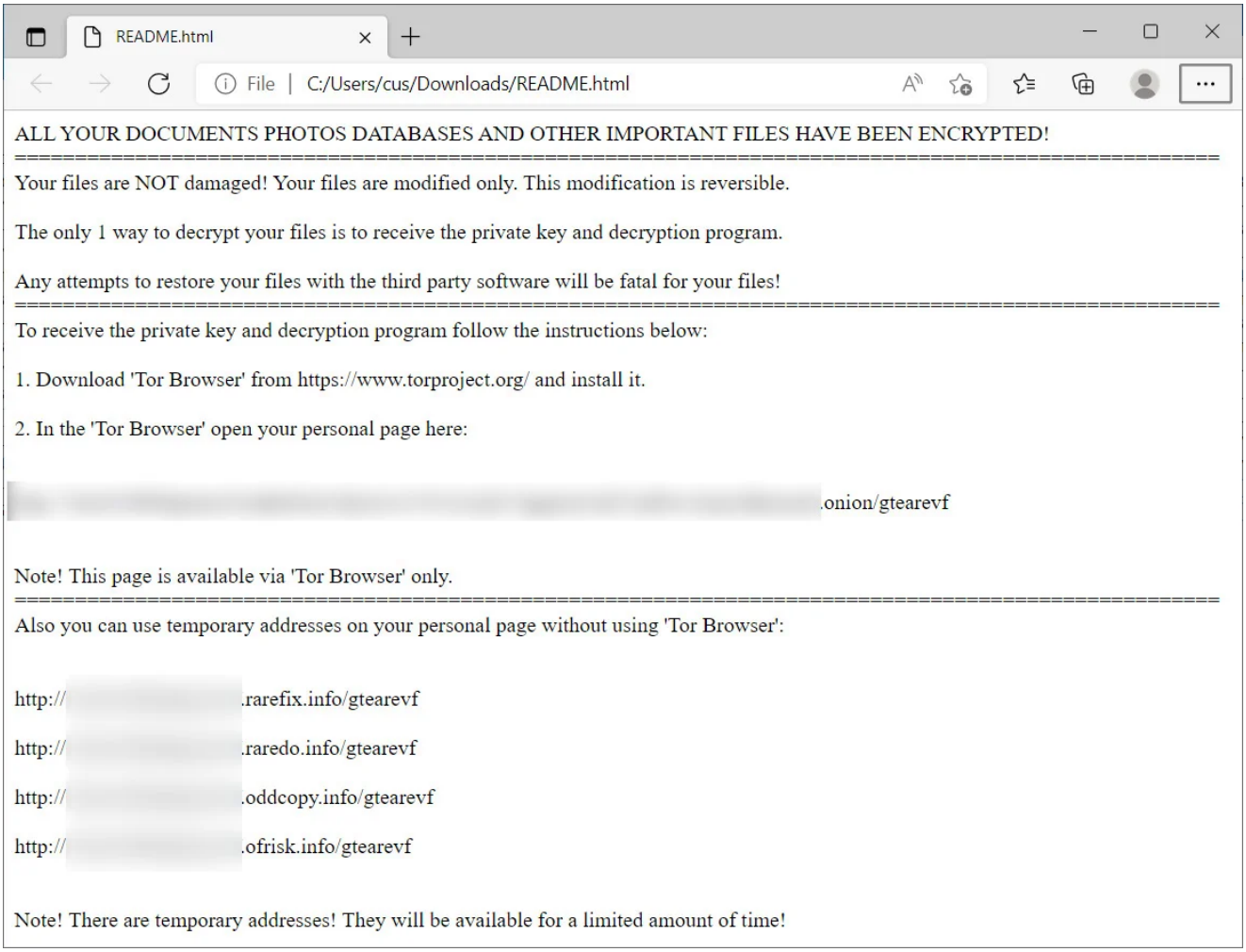
Once installed, the ransomware will delete shadow volume copies and then encrypt files. When encrypting files, the ransomware will append a random 8-character extension, such as .gtearevf, as shown below.



Files encrypted by Magniber

Source: BleepingComputer

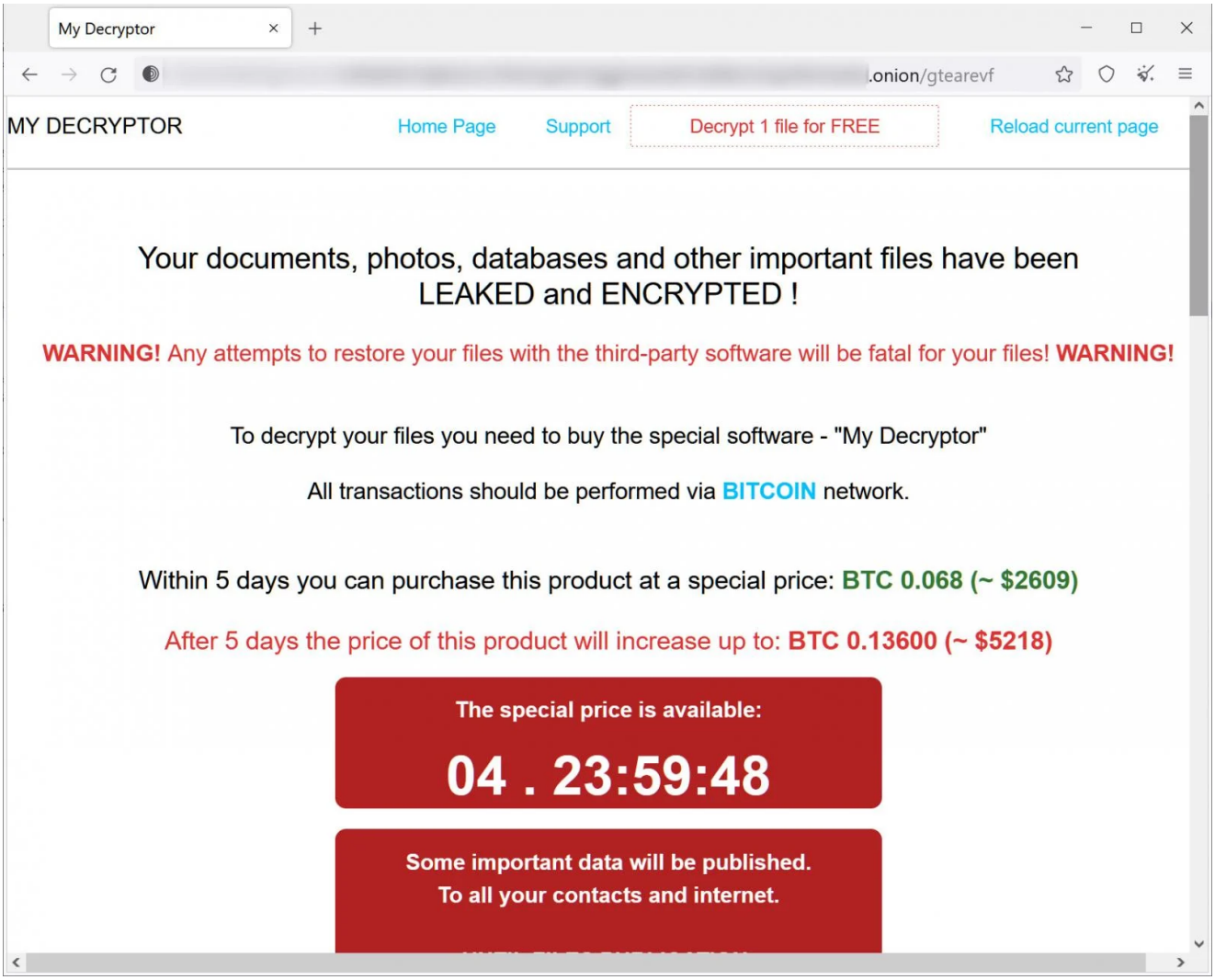
The ransomware also creates ransom notes named **README.html** in each folder that contains instructions on how to access the Magniber Tor payment site to pay a ransom.



Magniber ransom note

Source: BleepingComputer

The Magniber payment site is titled 'My Decryptor' and will allow a victim to decrypt one file for free, contact 'support,' or determine the ransom amount and bitcoin address victims should make a payment.



Magniber Tor payment site

Source: BleepingComputer

From payment pages seen by BleepingComputer, most ransom demands have been approximately $2,500 or 0.068 bitcoins.

Magniber is considered secure, meaning that it does not contain any weaknesses that can be exploited to recover files for free.

Unfortunately, this campaign primarily targets students and consumers rather than enterprise victims, causing the ransom demand to be too expensive for many victims.

Related Articles:

Windows 10 KB5011831 update released with 26 bug fixes, improvements

Windows 10 KB5012599 and KB5012591 updates released

Windows 11 KB5013943 update causes 0xc0000135 application errors

Microsoft May 2022 Patch Tuesday fixes 3 zero-days, 75 flaws

Windows 11 KB5013943 update fixes screen flickers and .NET app issues

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.