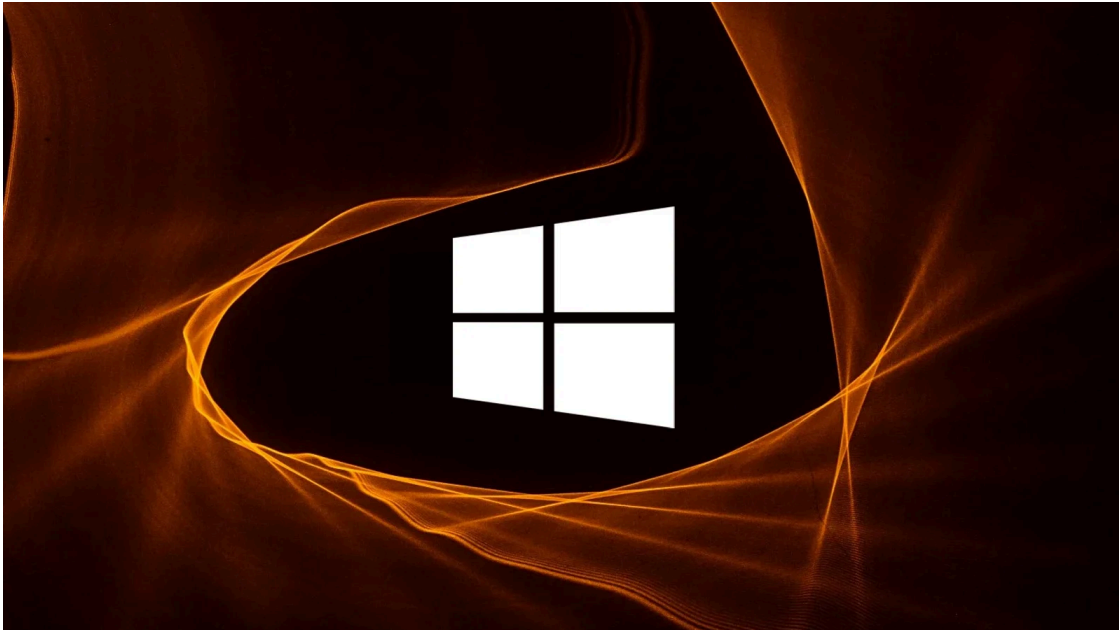


Fake Windows 10 updates infect you with Magniber ransomware

By Lawrence Abrams

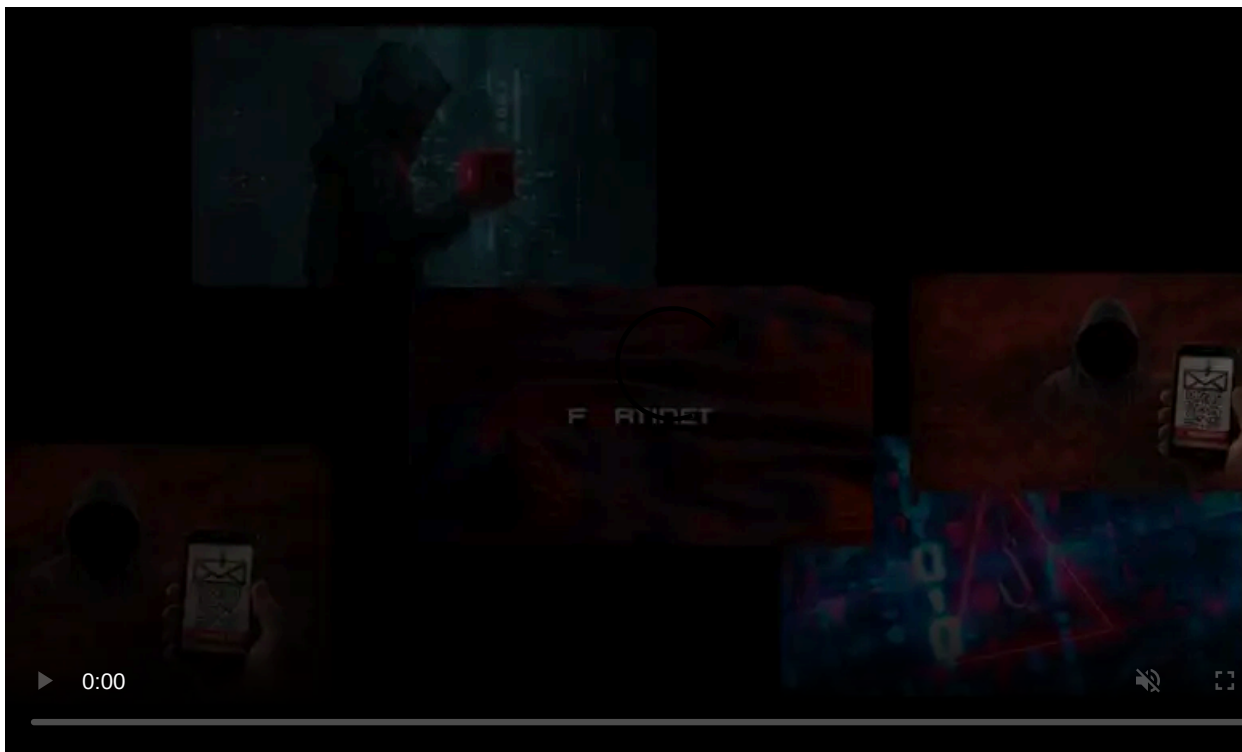
Published: 2022-04-30 · Archived: 2026-04-05 21:38:39 UTC



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.



Visit Advertiser website [GO TO PAGE](#)

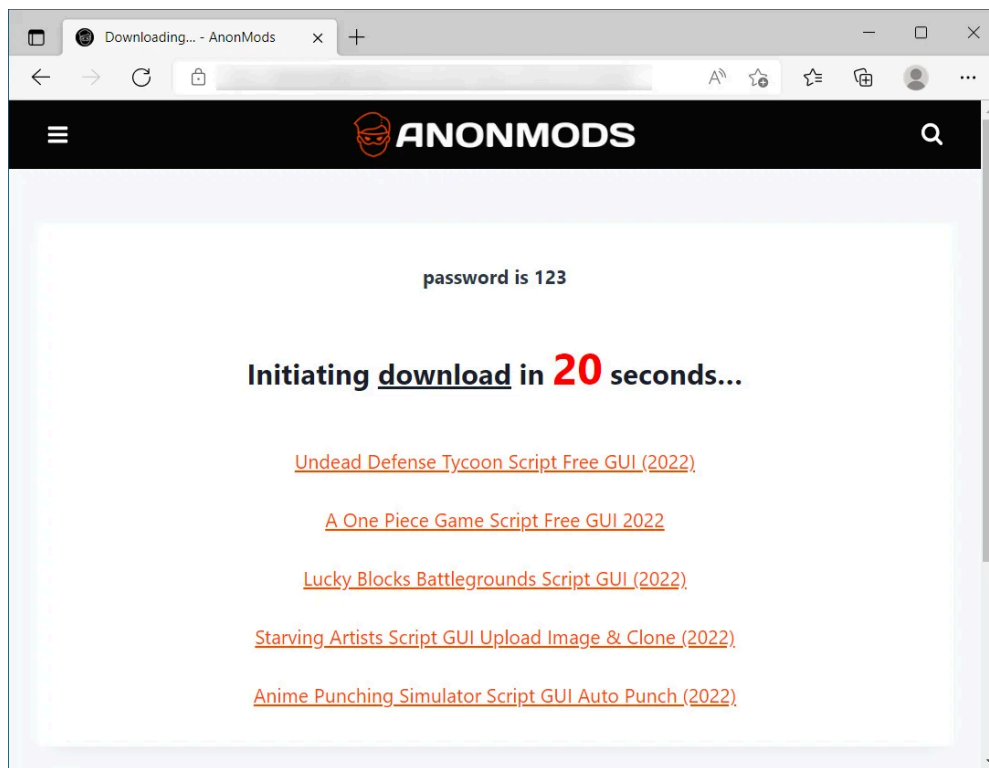
These updates are distributed under various names, with Win10.0_System_Upgrade_Software.msi [[VirusTotal](#)] and Security_Upgrade_Software_Win10.0.msi being the most common.

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.

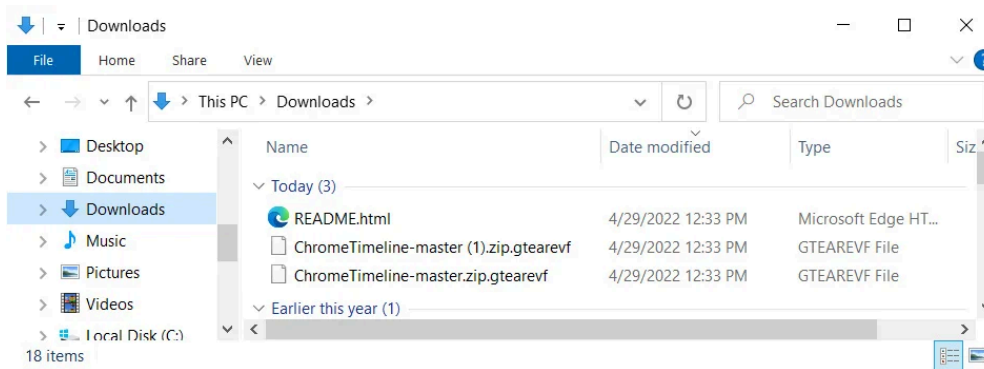
While it's not 100% clear how the fake Windows 10 updates are being promoted, the downloads are distributed from fake warez and crack sites.



Fake warez and crack sites pushing Magniber

Source: *BleepingComputer*

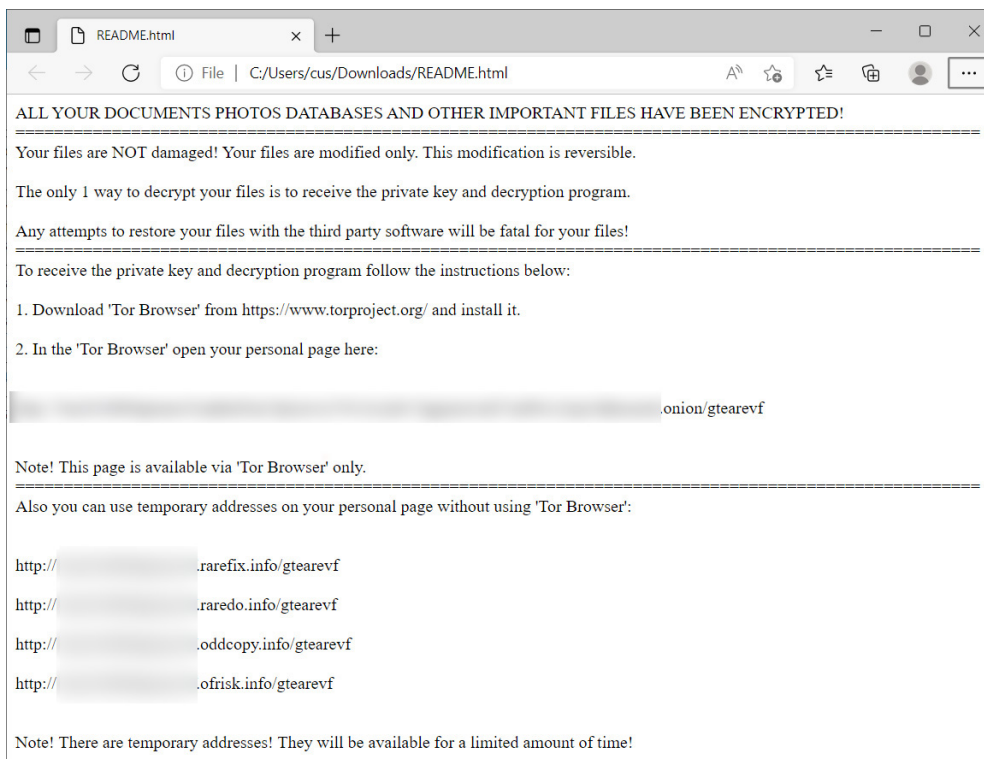
Once installed, the ransomware will delete shadow volume copies and then encrypt files. When encrypting files, the ransomware will append a random 8-character extension, such as .gtearevf, as shown below.



Files encrypted by Magniber

Source: *BleepingComputer*

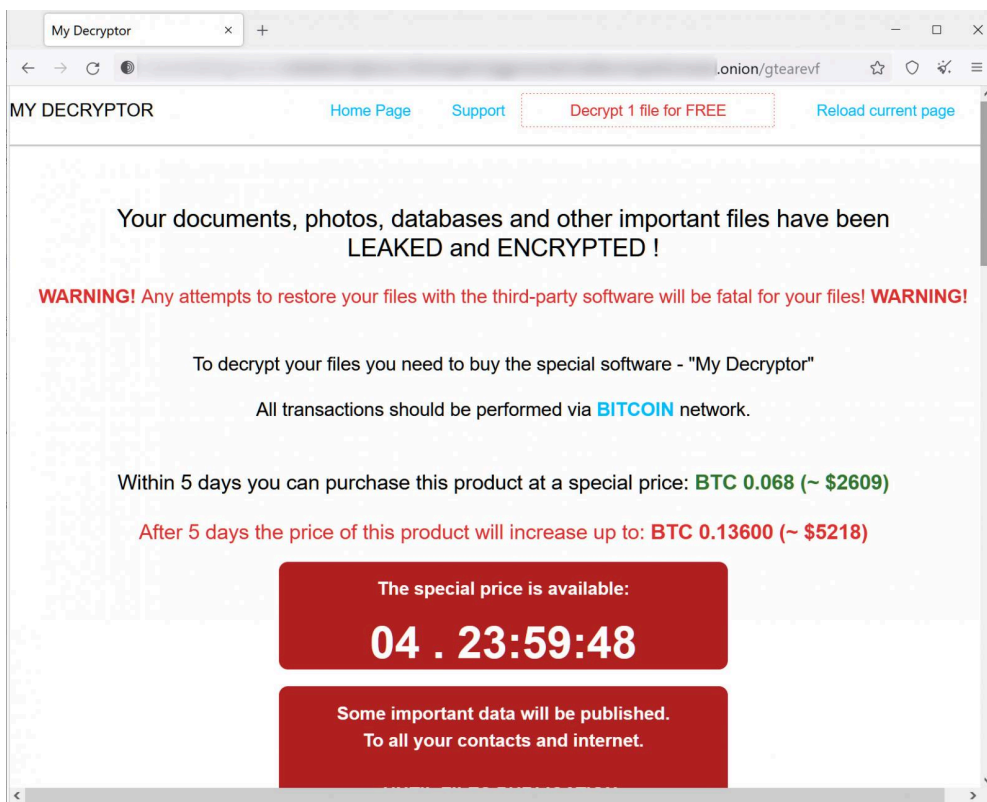
The ransomware also creates ransom notes named **README.html** in each folder that contains instructions on how to access the Magniber Tor payment site to pay a ransom.



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.



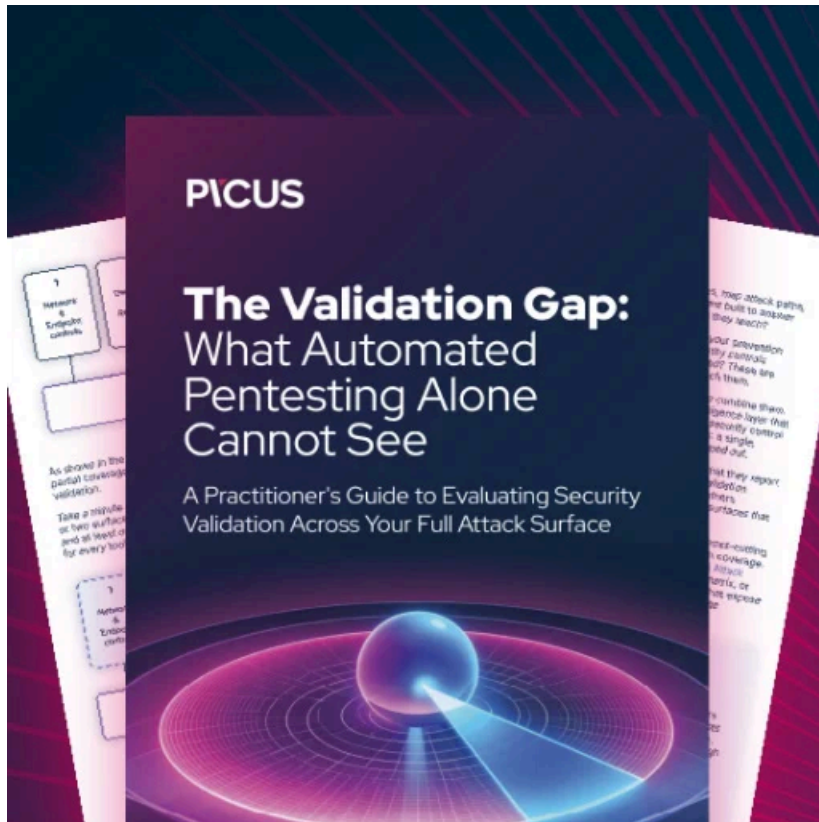
Magniber Tor payment site

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.



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/fake-windows-10-updates-infect-you-with-magniber-ransomware/>