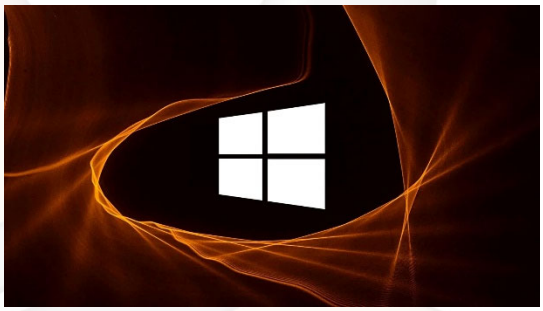
Fake Windows 10 Updates Infect You With Magniber Ransomware



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, there's been a surge of attacks regarding a ransomware infection targeting users worldwide.

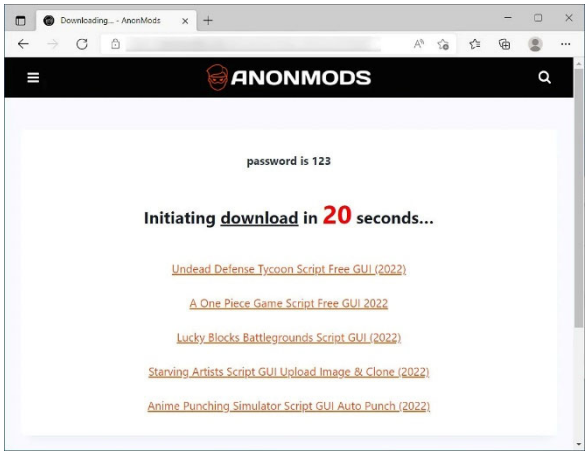
Research done on the ransomware shows users becoming infected by the Magniber ransomware after installing what is believed to be Windows 10 cumulative or security update.

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.

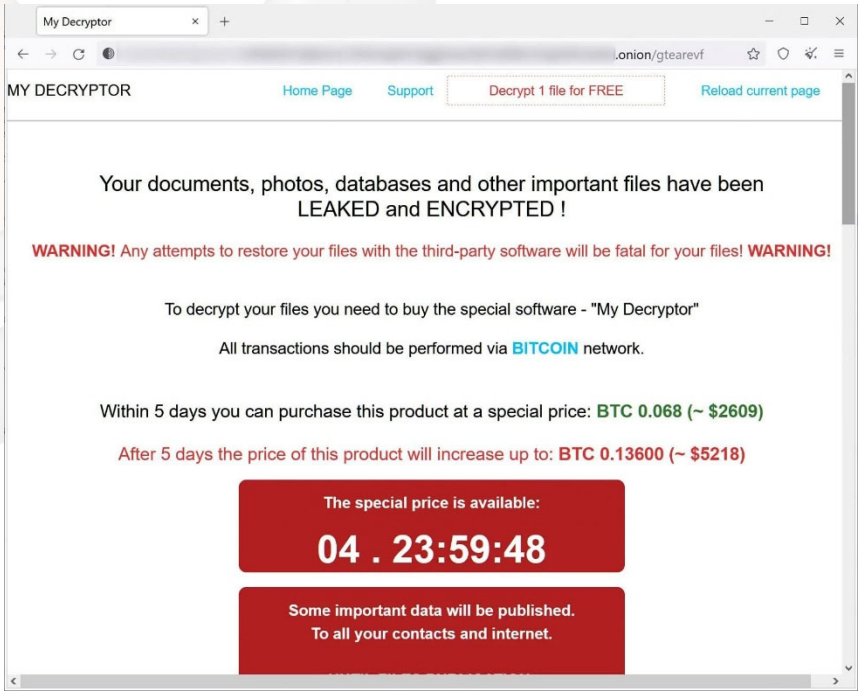


While it's not 100% clear how the fake Windows 10 updates are being promoted, the downloads are distributed from fake warez and crack sites.

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.

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.

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.



From payment pages seen, most ransom demands have started at $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.

To protect yourself from such a campaign, it is best to avoid such unofficial sources of downloading Windows updates and directly download them via your settings. You can also look for standalone updates on the Microsoft Update Catalog website.