Warning: Ransomware is spreading through fake malicious Windows updates

Named Magniber, this dangerous ransomware strain has been around on the internet for a while, and ranks in the dangerous group with its diverse infectivity.

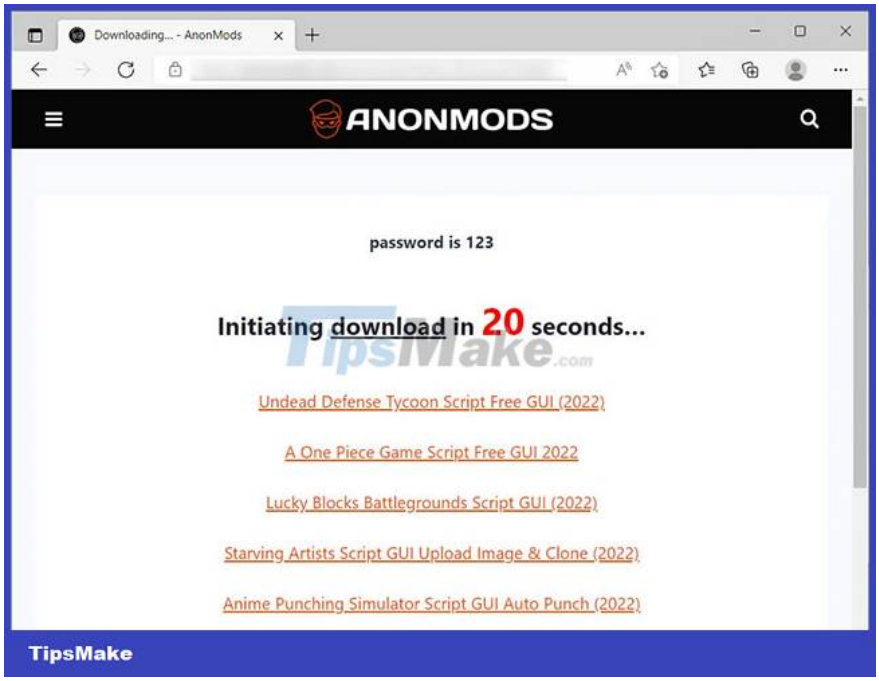
International security researchers have just made an urgent announcement about a campaign to spread ransomware through fake Windows 10 updates.

Named Magniber, this dangerous ransomware strain has been around on the internet for a while, and ranks in the dangerous group with its diverse infectivity. Back in 2021, Magniber was used by a group of malicious actors in the infamous PrintNightmare exploit campaign. As recently as January 2022, this ransomware strain was also recorded spreading through Microsoft Edge and Chrome at a rapid rate.

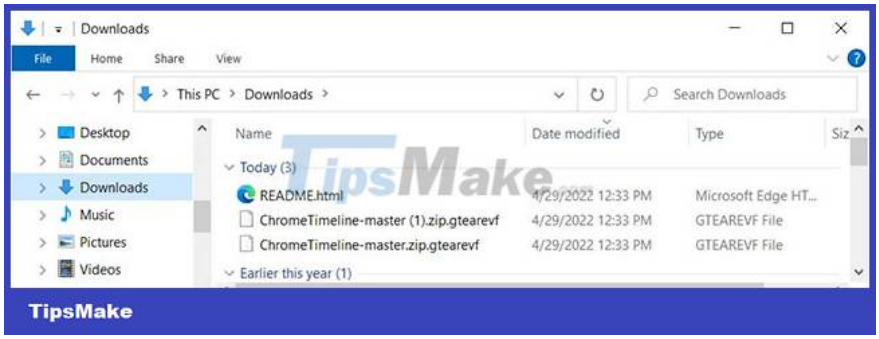
According to the latest report from, this new Magniber infection campaign does not seem to be limited to a specific region or territory. There have been a series of recorded cases of infection scattered in many countries around the world. The common feature is that malicious code is implanted in malicious Windows 10 updates, but designed to look like the real thing, and some of them even have a fake ID knowledge base (KB) attached to increase the theory. dress. Reported instances of fake updates include:

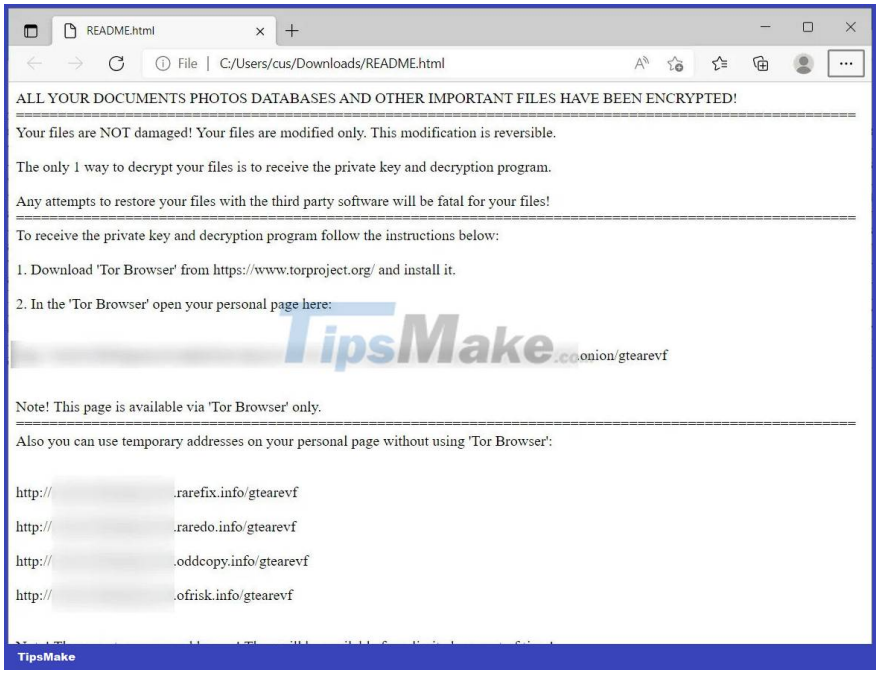
1. Win10.0_System_Upgrade_Software.msi
2. Security_Upgrade_Software_Win10.0.msi
3. System.Upgrade.Win10.0-KB47287134.msi
4. System.Upgrade.Win10.0-KB82260712.msi
5. System.Upgrade.Win10.0-KB18062410.msi
6. System.Upgrade.Win10.0-KB66846525.msi

These malicious updates are being spread unlimitedly via pirated, fake websites. Such as in the screenshot below.

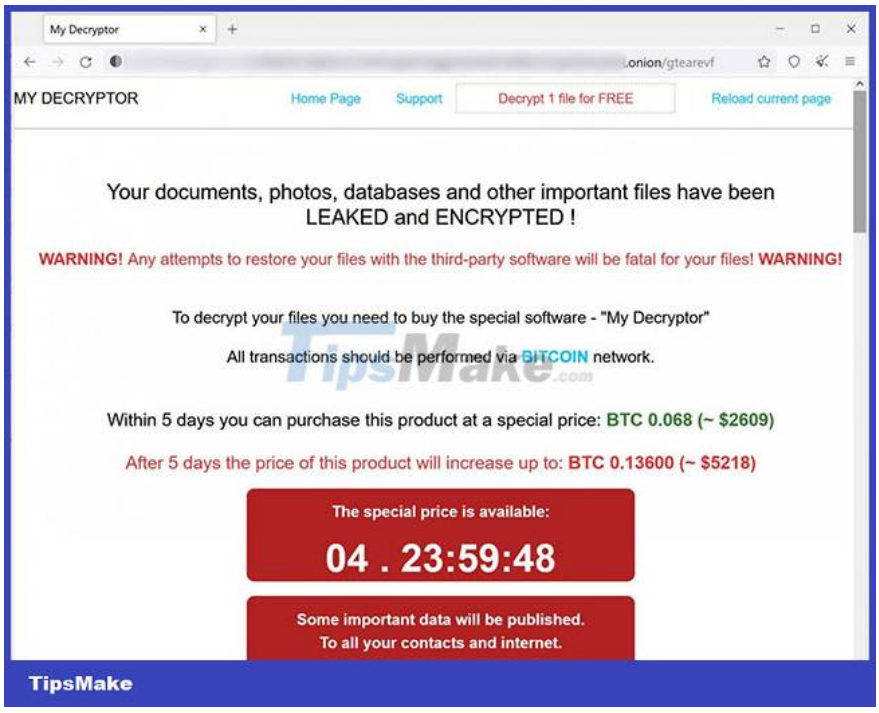


After successfully infecting malicious files are installed on the victim's system, they will continue to delete backups of encrypted drives and generate a "README" HTML file containing a ransom note (recognized by the victim). shown in the image below):





On the ransom payment website, the malicious actor will ask the victim to pay around 2,600 USD or 0.068 bitcoin (BTC) to get back the encrypted data. The ransom will double if the victim does not pay after 5 days.



To protect yourself from Magniber and a similar infection campaign, it's best to stay away from unofficial sources of Windows update downloads. Instead, download new updates from Windows Update itself. Alternatively, you can also search for standalone updates on the Microsoft Update Catalog website.

You finished reading the article "**Warning: Ransomware is spreading through fake malicious Windows updates**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.