New Voldemort/Nagini Ransomware Virus Infection

By Alex Dimchev

Published: 2016-09-27 · Archived: 2026-04-05 21:50:25 UTC

A new ransomware by the name of Voldemort(or Nagini) has appeared. It's yet another dangerous virus with a goofy exterior. The virus locks the screen of infected computers and puts a picture of Lord Voldemort as a wallpaper. The virus doesn't add extensions to encrypted files.

Voldemort Ransomware Virus – What To Expecto?

The virus was discovered by Michael Gillespie. The virus was named after a few files referencing **Voldemort,** the main villain of the **Harry Potter** franchise. One of the virus's file names is **"Nagini.exe."** Another is named **voldemort.horcrux.**

Voldemort Ransomware is still in development as of now, but a finished version may be released soon. The virus will most likely be distributed with the help of email spam (not owl mail, sadly.) The virus is developed by someone called **"Colosseum."** It's unknown is it's a single person or a group of malware developers.

Voldemort Ransomware – Technical details

The **Voldemort** virus uses a strong **RSA** encryption algorithm. The ransomware includes instructions to its victims. The message reads:

> Done Encrypting!
> Enter your credit card:
> Get key!
> Enter key to decrypt the files:
> Decrypt Now!

Voldemort ransomware aims to encrypt specific files. The extensions targeted the virus are:

> .bmp, .doc, .jpeg, .jpg, .png, .pdf, .pptx, .xls, .xlsx, .exe

Once the victim PC is infected, **Voldemort** will create its files in the following directories:

> C:\Temp\voldemort.horcrux
> *Username*\1.exe
> *Username*\Nagini.exe

The virus remains fairly mysterious as of now. There's not a lot of data to go on since **Voldemort** isn't widely distributed yet.

Voldemort Ransomware Virus – Conclusion

Don’t underestimate Voldemort just because of its name. The virus can prove very dangerous if the crooks behind it start a distribution campaign. Voldemort isn’t the only virus with a weird name. Here are a few examples of the cyber-criminal imagination:

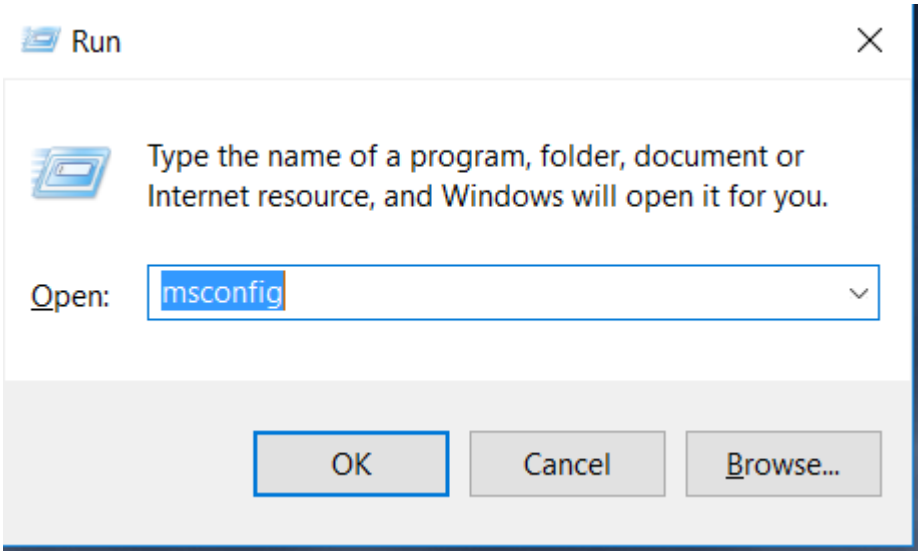
- Hitler Ransomware – A fake ransomware virus named after the Führer.
- PokemonGo ransomware – a Pikachu-faced ransomware virus masking as the hit app
- Bart2 – a virus named after the brat from The Simpsons

Just in case the virus proves dangerous, we’ll leave malware removal instructions at the end of this article. With their help, you’ll be able to combat the **Voldemort/Nagini** ransomware virus. There’s no magic spell that can remove **Voldemort** ransomware. If you want to remove it, you’re going to have to go the muggle route and download an anti-malware tool or remove it by hand.

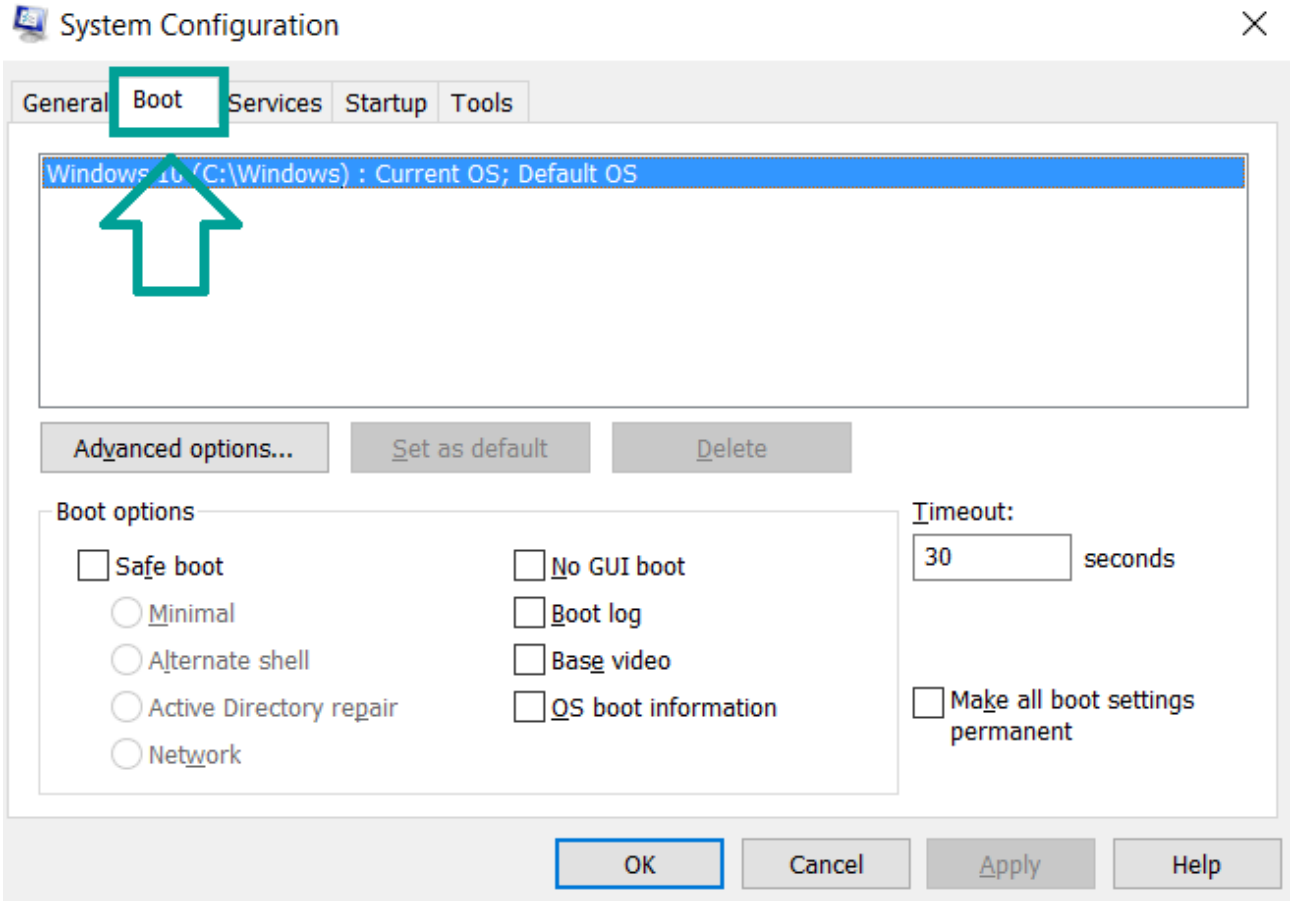
Try to Load Your PC in Safe Mode

For various Windows OS’s:
1) Hit **WIN Key + R**

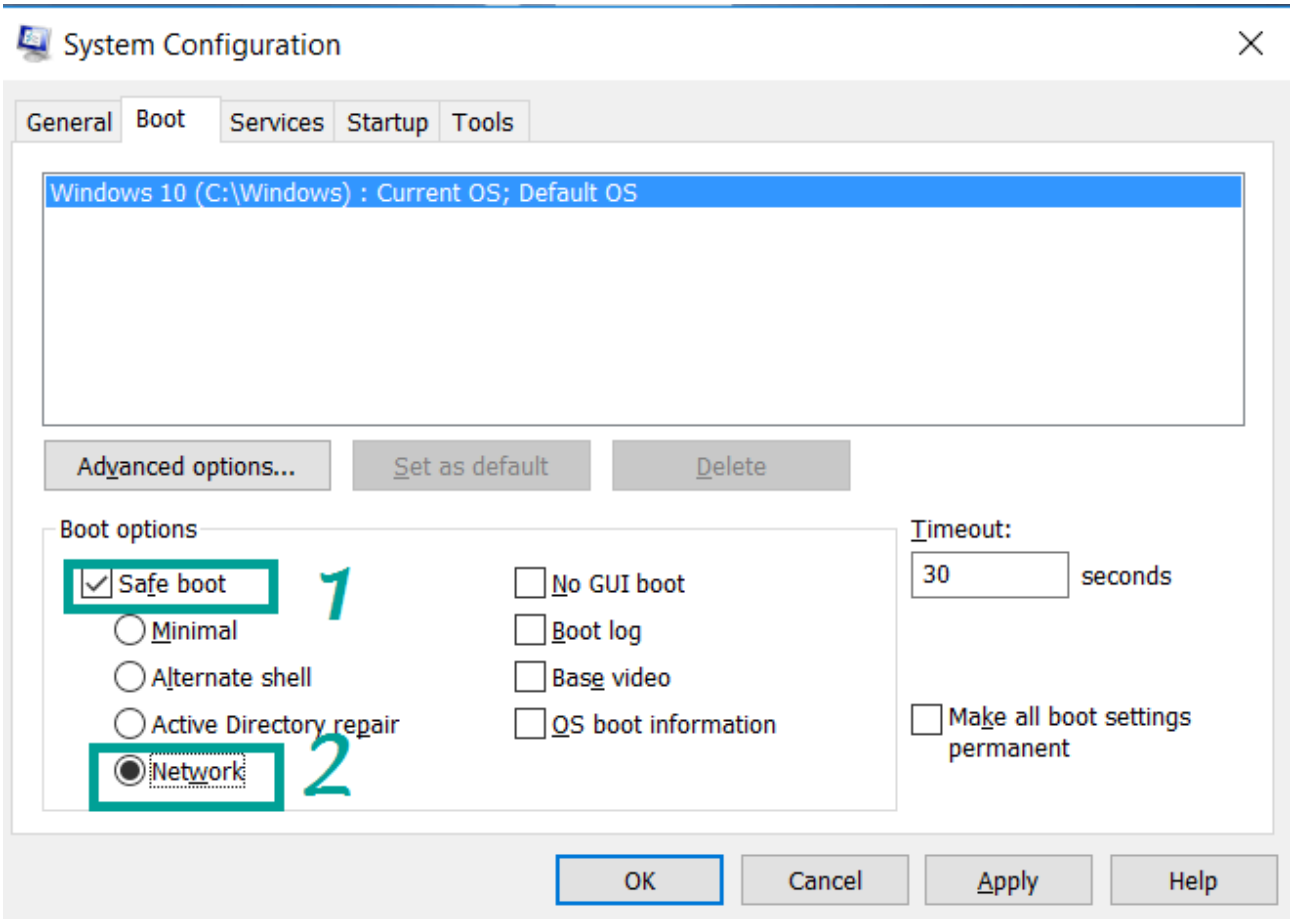
2) A Run window will appear. In it, write “msconfig” and then press Enter.



3) A Configuration box shall appear. In it Choose the menu named “Boot”.



4) Choose the **Safe Boot** preference and then go to Network under it to tick it.



Eliminate the malicious processes

1) hit the following key combination: **CTRL+ESC+SHIFT**
2) Get over to **Processes.**
3) Choose the suspicious process if you have found it and then right click it after which click on “Open File Location.”
4) End the malicious process by again right-clicking and choosing “End Process”.

Delete registry objects created by the Voldemort ransomware virus.

For all Windows versions:
1) Again type simultaneously the **Windows Button + R.** key combination.
2) In the type box, write “regedit”(without the inverted comas) and hit Enter.
3) Type the **CTRL+F** key combination and then write the malicious name in the search type field to locate the malicious executable.
4) In case you have discovered registry keys and values related to the name, you should delete them, but be careful not to delete legitimate keys.

Recover files encrypted by Voldemort.

If you want to try recovering files yourself, you have several options:
Option One: By using Windows’s System Restore

1) Hit the **Windows Button + R.** key combination.
2) After the “Run” Window pops up, write “rstrui” and hit on the Enter button.
3) Choose a restore point and continue.

IMPORTANT: If you want to be more effective, we strongly suggest booting in safe mode if you are to do this!

Option Two: By using Windows’s Shadow Volume Copies

To access shadow volume copies you may require a program, **like Shadow Explorer.** Install it, open it and make it scan for shadow copies. If you have them enabled, this method will work, in case the crypto-virus has not deleted them.

Option Three: By using various Recovery Software

This option will not ensure maximum effectiveness and recovery rate but still, you may restore several files. Most data recovery programs are available for free online, simply Google “Data Recovery Software”.

Prevent viruses from damaging your files in the future.

To protect your important data, we suggest that you store it in the cloud. Programs that makes online backup possible also enable you to schedule auto backup on different time periods and this way, even if you lose your data, you can find it uploaded in securely encrypted account, access to which only you have.

Author : Alex Dimchev

Alex Dimchev is a beat writer for Best Security Search. When he's not busy researching cyber-security matters, he enjoys sports and writing about himself in third person.
