9 of the most dangerous Viruses & malware threats in 2024

Provided by:

Avast

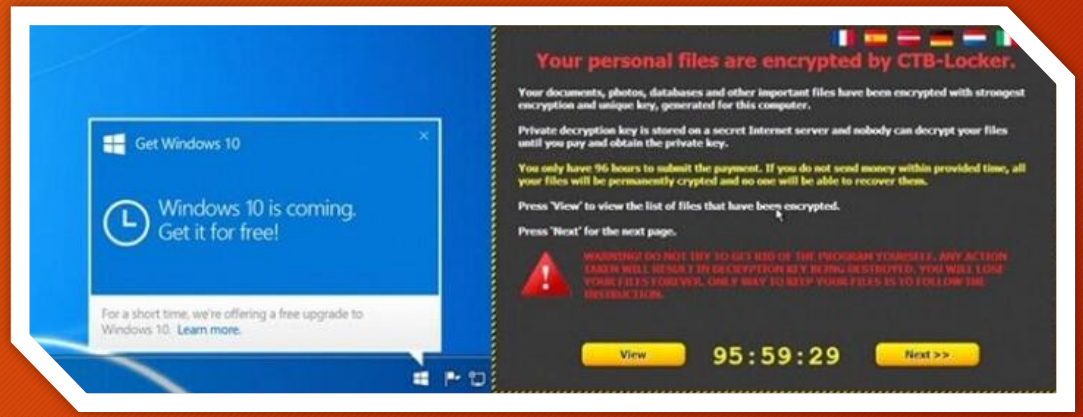
Viruses and malware are continually advancing, becoming more sophisticated and dangerous over time. From ransomware that denies access to your files to spyware that monitors your every action, navigating the digital world without protection is fraught with risks. The most destructive malware can compromise your most sensitive information, such as financial credentials, personal photos, and identification documents

1.Clop Ransomware

- Clop is a dangerous ransomware variant of CryptoMix, targeting Windows users. It disables over 600 Windows processes, including security tools like Windows Defender, leaving systems defenseless.
- Clop has advanced to attack entire networks, not just individual devices. Notably, Maastricht University in the Netherlands had its Windows network encrypted, forcing it to pay a ransom.

2.Fake Windows Updates (Hidden Ransomware)

- Hackers use fake emails urging users to install "urgent" Windows updates, tricking them into downloading ransomware disguised as '.exe' files.
- One such ransomware, “Cyborg,” encrypts all files and demands a ransom for their release. Many email providers and basic antivirus programs fail to detect these threats, making robust internet security essential to stay protected.



3. Zeus Gameover

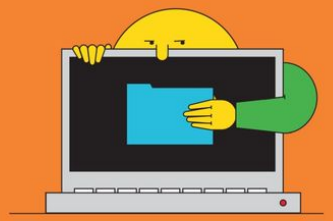
- Zeus Gameover, a Trojan from the “Zeus” malware family, targets sensitive banking details to steal funds. Unlike typical malware, it operates without a centralized command server, making it nearly impossible to trace or disrupt. Instead, it uses independent servers to exfiltrate stolen data, leaving victims without recourse.

RaaS (Ransomware as a Service)

- Ransomware as a Service (RaaS) is a dark web industry where hackers for hire launch ransomware attacks for clients with no technical skills. Its rise is alarming, making ransomware attacks accessible to virtually anyone.

Fleeceware

- Fleeceware refers to mobile apps that charge exorbitant subscription fees, even after being uninstalled. Though not a direct security threat, it’s a deceptive practice affecting millions of Android users, exploiting unsuspecting victims for profit.



IoT Device Attacks

- As IoT devices like smart speakers and doorbells grow in popularity, hackers exploit their weak security to steal valuable data, including passwords and banking info. Many IoT devices lack proper security due to limited storage, making them easy targets.
- Hackers can also use cameras and microphones to spy, even through smart baby monitors. Unsecured IoT devices can serve as entry points into corporate networks, allowing malware to spread across systems.

Social Engineering/Phishing Attacks

- Cybercriminals exploit human psychology to bypass security protocols. In social engineering attacks, hackers impersonate trusted individuals to trick customer support into revealing sensitive information.
- Phishing is a common form of this attack, where fraudulent emails or messages lead victims to fake websites designed to steal login credentials or install malware. Since phishing preys on trust, it can result in severe data breaches and financial losses, requiring no technical skills—just deception.

Cryptojacking

- Cryptojacking malware hijacks a device's computing power to mine cryptocurrencies like Bitcoin. This process slows down the device as it contributes to generating new coins.
- Although cryptojacking attacks have decreased in recent years due to falling cryptocurrency values, the rise of Bitcoin and other currencies in 2024 makes this threat lucrative for cybercriminals, ensuring its continued existence.

Artificial Intelligence (AI) Attacks

As AI tools become more accessible, hackers can use the same technology to execute powerful cyberattacks. While AI and machine learning enhance cybersecurity, they can also be weaponized for large-scale hacking.
As these technologies evolve, cybercriminals are likely to develop more advanced and destructive AI-driven malware, making future attacks faster and more impactful.

Common Signs of a Malware Infection

- **Slow Performance**: Your device becomes sluggish, with slow startups or app load times.
- **Frequent Crashes**: Programs or your system crash often, showing error messages or the blue screen of death.
- **Pop-up Ads**: Increased pop-up ads, even when your browser is closed, typically due to adware.
- **Unfamiliar Programs**: Unwanted programs appear on your device, often starting automatically.
- **Changes to Browser Settings**: Unapproved changes to your homepage or search engine settings.
- **Unusual Network Activity**: High network usage, even when not online, indicating possible data theft or cryptojacking.
- **Overheating**: Your device overheats from malware running in the background.
- **Disabled Security Software**: Antivirus or firewall is disabled without your consent.

Recognizing these signs helps you act quickly to protect your data.

How to defend yourself?

- Your sensitive data, bank details, personal photos, and private messages—how much are they worth to you? They’re priceless.
- So, how are you protecting yourself from the latest malware and cyberattacks?
- Many people rely on basic antivirus software or a few security tools. But the reality is, most antivirus programs can't provide complete protection against new and evolving threats. You may still be vulnerable to the latest viruses and malware.
- To truly safeguard your devices and data, you need **Avast**—one of the most advanced and reliable antivirus solutions for PC, Mac, Android, and iOS