Avast Business

Avast partner educational series

Ransomware & cryptominer

16 September 2021

Avast Business

About the author

Rob Krug,
Senior Security Architect,
Avast Business

Rob has been in the network engineering and security space for over 30 years. His background includes extensive work with telecommunications, network design and management, and most importantly, network security. Specializing in security vulnerabilities, Rob has extensive experience in cryptography, ethical hacking, and reverse engineering of malware. Rob served in the U.S. Navy and also worked as a Data Security Analyst and Director of Engineering for multiple international service providers and vendors. Rob has designed, implemented, and maintained some of the most complex and secure networks imaginable.

Ransomware

Ransomware is a malicious software which encrypts files on your computer or completely locks you out. It is spread by hackers who then demand a ransom, usually $300-500/GPB/EUR, preferably paid in bitcoins), claiming that you'll receive the decryption key to recover your files if you pay. It's also often combined with a time limit, creating a sense of urgency. Ransomware comes in all shapes and sizes. Some variants are more harmful than others, but they all have one thing in common - the ransom.

When it comes to ransomware, anyone can be a target. For example, WannaCry took advantage of a Windows vulnerability to spread and infect more than 200,000 users as well as 10,000 companies, public authorities, and organizations worldwide. The first recorded ransomware attack occurred in 1989, so this concept is not entirely new.

Is ransomware a virus?

No, ransomware is not the same as a virus. Viruses infect your files/software and have the ability to replicate themselves. However, ransomware simply scrambles your files in order to render them unusable and then demands that you pay up.

How Ransomware Infects Your PC

From malicious email attachments and fake links to social media scams, ransomware spreads quickly and hits hard. Here's how it gets on your computer:

Social Engineering

- A fancy term for tricking people to download malware from a fake attachment or link
- Disguised as ordinary documents such as bills, notices, receipts, CVs, etc. and they appear to be from a reputable company/person/institution

Malvertising

- Paid ads that deliver ransomware, viruses, and malware
- Hackers will even buy ad space on popular websites and social media to get their hands on your data

Avast Business

Exploit Kits

- Prewritten code wrapped nicely in a ready-to-use hacking tool
- Designed to exploit vulnerabilities and security holes caused by out-of-date software regardless if it's a general OS or a third-party app

Drive-by Downloads

- Dangerous files you never asked for
- Some malicious websites take advantage of out-of-date software/apps to silently download malware in the background while you're browsing an innocent-looking website

Preventing Ransomware

Back up your important files

Back up your files on external drives, the Cloud, or both. With so many free cloud storage services out there, you really have no excuse. To be extra safe, choose a service with version histories. That way, if anything bad ever happens to your account, you can easily restore it to a previous version.

Use an up-to-date antivirus software

Antivirus software offers essential protection against anything trying to mess with your computer. It also offers proactive security measures instead of common reactive or passive procedures other tools might offer.

Keep your operating system updated

If you remember when we talked about WannaCry earlier, you will already know that security updates are vital for your computer's safety. Out-of-date software makes you more vulnerable to all kinds of malware, including ransomware.

Should I pay the Ransom?

Hackers don't discriminate. Their only goal is to infect as many computers as possible because that's how they make money. Victims will pay hundreds of thousands of dollars to recover data.

You're dealing with scammers here, so paying the ransom doesn't guarantee anything. Paying encourages the hackers to come back harder and demand more money.

Simply put - no, you should not pay the ransom. Instead, keep preventive measures in mind and prepare for the worst just in case.

Avast Business

Cryptominer or Crypojacking

These types of malware are often related to ransomware, since they use the same attack vectors to infect a system or network. The big difference is that these types of malware do not encrypt your local files and send you a ransom note as soon as they are done. They turn the infected system into a continuous money making machine for the hacker by mining cryptocurrencies in the background without you noticing.

Cryptojacking doesn't even require significant technical skills - you can actually buy "out-of-the-box" cryptominer toolkits on the Dark Net for as low as $30.

Due to the complex nature of cryptominers, the best protection against this type of threat is similar to what you use to protect against ransomware. Additionally, another helpful precaution is to educate users and staff to be aware of suspicious links or a sudden change within the system or network performance/behavior.

About Avast Business

Avast delivers all-in-one cybersecurity solutions for today's modern workplace, providing total peace of mind. Avast provides integrated, 100% cloud-based endpoint and network security solutions for businesses and IT service providers. Backed by the largest, most globally dispersed threat detection network, the Avast Business security portfolio makes it easy and affordable to secure, manage, and monitor complex networks. Our easy-to-deploy cloud security solutions are built to offer maximum protection businesses can count on. For more information about our cloud-based cybersecurity solutions, visit **www.avast.com/business**.