Abstract

iMedPub Journals
www.imedpub.com

American Journal of Computer Science and Information Technology

2021
Vol.9 No.S1

Ransom wares: How to build it and how to protect from it

Sami Fakhfakh
Engineer/Ethical Hacker, Tunisia
Email: contact@sami-fakhfakh.com

Abstract

Ransom ware is a type of malware. It restricts access to the computer system that it infects or the data that it stores (often using encryption techniques), and demands a ransom be paid to the creator(s) of the malware. This is in order for the restriction to be removed. Some forms of ransom ware encrypt files on the system's hard disk. Others may simply lock the system and display messages intended to persuade the user to pay.

Ransomware first became popular in Russia. Now the use of ransomware scams has grown internationally. In June 2013, McAfee said it had collected over 250,000 unique samples of ransomware in the first three months of 2013. This is more than double the number of the previous year. CryptoLocker, a ransomware worm that surfaced in late-2013, had collected an estimated $3 million USD before it was taken down by authorities.

In May 2017, a piece of ransom ware called Wanna Cry spread around the world. It lasted four days and affected over 200,000 computers in 150 countries.[4] Only about $130,000 (USD) was ever paid in ransom, but the attack affected a lot of large companies and organizations. The United Kingdom's National Health Service (NHS) was hit hard by WannaCry. Hospitals could not access their files, and so many surgeries were cancelled and patients had to be turned away.[5] The NHS was especially at risk because it was using a version of the Windows operating system called Windows XP that Microsoft no longer supported.[6] This meant that Microsoft had not been sending out security updates for this version of Windows, leaving it open to the WannaCry virus. Other systems were affected even though they were running newer versions of Windows, because their users had not yet installed the most recent security updates. Even though it was not designed to actually damage computers or their files, WannaCry led to a lot of wasted time and money, showing how vulnerable the world still is to ransomware attacks.

nowadays, several companies, organizations or individuals are affected by a ransomware attack. in the philosophy of learning defense by attack. we will explain how this malware works, do a live code review example, test it on live and teach you how to protect yourself from it.

Biography

Dr. Sami fakhfakh was a black hat hacker when he was young, his passion for security and IT pushed him to devote his studies to IT and to continue his training to become a white hat hacker, now he is a computer engineer who works in Paris in the field of blockhain and who does freelance cybersecurity consulting .He had his license in fundamental sciences in computer science at the faculty of sciences of sfax (Tunisia) in 2017, to then go to an engineering cycle at ISTY (France) where he obtains his diploma in 2020 .Sami Fakhfakh was known as s-man hacker at the time