# Ransomware

With Marcelle Lee


## Got Ransomware?

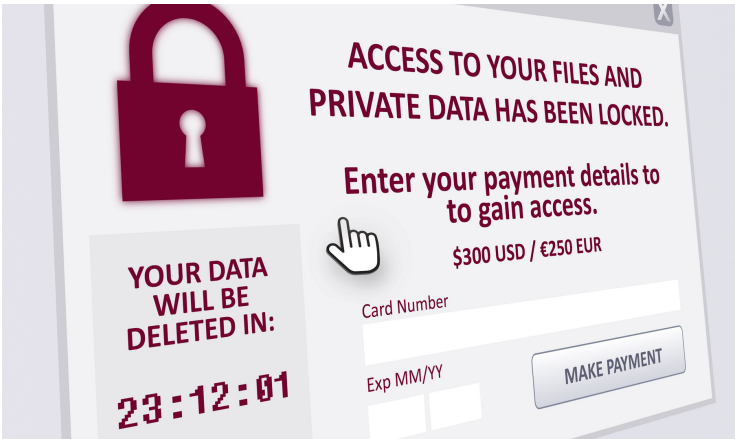
Reports of ransomware attacks have frequented news headlines lately. These attacks reportedly cost the global economy an estimated $20 billion in 2021, with the average cost of each successful attack being $4.62 million.

By vertical, Secureworks" team responded to the most incidents in manufacturing companies, followed by technology, credit unions, education, healthcare, the financial industry, and business services. But why should you be concerned about ransomware?

Ransomware is a type of malware that captures the victim's files and other sensitive data with a threat to publish or destroy it if a ransom is not paid. A cyber threat has several components. It consists of intent, capability, and opportunity. Intent is the desire to cause an effect, such as harming a company or stealing data. Capability is the ability to perform the aforementioned act. Opportunity is having a time or event that allows the act to be performed.

In an interview with the Cybersecurity Association of Maryland, Security Researcher Marcelle Lee stated, "Ransomware is becoming so prevalent; the boundaries that were in place about organizations not being targeted if they were providing medical services, or they were a school or something like that, that's all flown out the window now, so anybody is fair game."

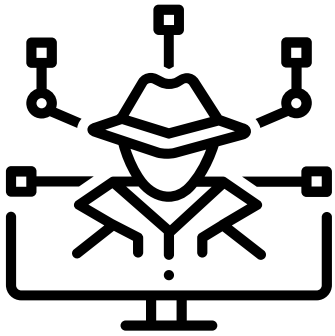
The banking industry alone has seen a 1318% increase in ransomware attacks in 2021. Many other industries have taken devastating blows to their finances and infrastructure because of the recent increase of ransomware attacks.




The ecosystem of ransomware attacks has changed significantly. For example, AIDS ransomware was developed in 1989 by a biologist and written in QuickBASIC 3.0. It featured symmetric encryption and targeted delivery was via floppy disks. The ransom was relatively low and payment was requested in the form of a cashier's check sent by snail mail.

In contrast, REvil's ransomware was developed by GOLD SOUTHFIELD, a cybercriminal threat group, and was distributed as Ransomware as a Service (RaaS). It utilizes both symmetric and asymmetric encryption. Stolen data is uploaded to a website that is accessible if the ransom is not paid in a name-and-shame style. The ransom is usually extremely high and payment is expected via cryptocurrency.

One major issue caused by ransomware attacks is damage to brand and reputation. While paying the ransom of an attack is expensive, the financial damage caused by maring a company's reputation can be even greater. In 2017, the WannaCry ransomware attack indirectly cost the NHS $116.4 million (£92m) and resulted in 19,000 canceled appointments. Target CEO, President, and Chairman Gregg Steinhafel resigned from all of his positions after a massive data breach in 2014. Additionally, almost one in four Chief Information Security Officers (CISOs) resign after just one year at a company.




Lee said that, “One of the key trends that we’ve been following is the emergence of what is called naming and shaming, which is where ransomware groups will ransom your environment… but before they do that, they will exfiltrate data from your environment and also hold that hostage as well.” She stated that 3,500 victim organizations have been publicly named and shamed on threat group websites—a number only expected to increase.

The best way to protect yourself and your company from ransomware is to follow these tips:

1. Look before you click: one popular way of deploying ransomware is through emails--always verify that links and attachments are from legitimate people and not infected.
2. Always use antivirus software: the best protection against ransomware is prevention because once the ransomware has captured your files, it can be extremely difficult to get them back without paying the ransom.
3. Have good backups of all important files: if you have a backup of your files, there is less of a chance you will have to pay the ransom.
4. Keep all systems up to date: old programs allow for viruses to access your computer through holes in security left unpatched by old versions of a software. Make sure to install patches to software when they are released by its developers.
5. Utilize MFA: Multi-factor authentication makes it substantially more difficult for your accounts to be hacked and your identity to be stolen.
6. Implement an EDR solution: Endpoint Detection and Response solutions are an important part of an incident response plan, which every team should have and test in case of cyber attacks.
7. Manage accounts and assets: know what needs to be defended and do not allow all users to run as administrators.