Difference between Killware and Ransomware

It can be easy to confuse killware and ransomware because they are somewhat similar in name. Some websites also define killware as a type of ransomware.

At this point, most people are familiar with ransomware. These fast-growing and damaging cyberattacks have repeatedly made headlines, but even more dangerous types of attacks are beginning to emerge. Businesses and consumers now have to worry about killware.

However, some people claim that there are some commonalities between these two types of malware. So what is the difference between killware and ransomware?

What is Killware?

If you look up the definition of killware, you'll find a number of different answers. Some sources say it is ransomware that 'kills' your software, and others define it as ransomware that threatens violence in exchange for ransom. But the most widely accepted definition: Killware is any cyber attack that causes physical harm, whether deadly or not.

Harmful or even deadly cyberattacks may seem far-fetched, but they are increasingly likely. As people rely more on Internet of Things (IoT) devices, hackers can cause more damage by taking control of them.

Imagine a hospital using IoT-connected medical equipment. Cybercriminals can break into those devices and turn them off, endangering people's lives. Additionally, hackers can infiltrate an Internet-connected power grid

to shut off all power in an area when severe weather occurs.

Killware has become a reality. In a 2021 cyberattack in Florida, an attacker broke into a water treatment plant to increase the amount of sodium hydroxide in the water supply to dangerous levels, CNN reported. The facility noticed the attack and quickly returned everything to normal, but it could have poisoned thousands if not noticed.

What's the difference between Killware and Ransomware?

It can be easy to confuse killware and ransomware because they are somewhat similar in name. Some websites also define killware as a type of ransomware. Although there can be a combination of the two, they are separate things.

The biggest difference is the purpose of the attacks. Ransomware attacks can have serious consequences but are financially motivated. Attackers try to extort money from people by threatening to leak or delete sensitive information. Killware attacks aim to cause physical harm to people and typically do not involve money or data.

Despite these differences, killware and ransomware can be more or less similar. An attack that threatens to harm someone by endangering an IoT device if they do not pay a ransom would be ransomware and killware. Both types of malware also begin with an attacker gaining access to the system without the user realizing it.

How to prevent Killware

Killware can be scary - and not just because of its name - but there are steps you can take to protect yourself. A great place to start is by securing any IoT devices you have, as killware attacks tend to target these devices. To do that, you can:

1. .
2. Enable multi-factor authentication.
3. Turn on automatic updates.
4. Consider hosting IoT devices on separate networks so they are not at risk of lateral movement.

If any of your electronic devices have communication features that you don't use, turn off those settings. These features may be convenient, but the more connections a device has, the more potential vulnerabilities there are. You should also check your WiFi router to make sure you have WPA-2 or WPA-3 encryption.

Good anti-malware programs can detect malware before it causes any damage. If you don't want to pay for the premium version, you can enhance built-in security by enabling regular malware scanning and blocking unrecognized apps.

Phishing can bypass security software if it tricks you into making mistakes, so it's best to learn how to detect these attempts as well. To stay safe from phishing:

1. Never click on unnecessary links.
2. Double check the email address.
3. Be suspicious of any messages that are unusually urgent or from companies you've never heard of.

Prevention is always best, but sometimes, like in the 2021 Florida water center attack, killware doesn't become apparent until it becomes active. That's why it's important to always be on the lookout for suspicious activity. As soon as you notice something unusual with any smart home devices or accounts, adjust them and change your login information.