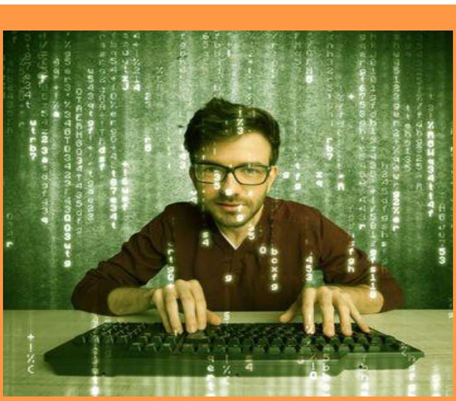
AJMS Global

# Newsletter

# Zero Day Attacks

## *Inside* THE ISSUE



## Background

A zero-day attack is a vulnerability in a system that is not yet found by the host of that system. Every single fix must be tailored to the problem, after diagnosing the vulnerability. Zero-day attacks become more common as technology advances, and more code is created

## Implications of Zero Day Attacks

Organizations which deal with highly valuable confidential information are usually the main targets for hackers to discover vulnerabilities  as those vulnerabilities can then be sold to malicious groups for a significant amount of money. These can have catastrophic consequences for the organization that has their security compromised, and their users who can have their private confidential information stolen. All of which can result in immeasurable losses

**Cases:**

- ❖ A zoom vulnerability zero-day attack was put up on the market for around half a million dollars at the beginning of the pandemic.
- ❖ Stuxnet was a worm that was used to target Iran’s uranium enrichment plants by taking advantage of the software running on the Industrial computers, the PLC’s, in the plant
- ❖ Sony’s zero-day attack which crippled its network and led to the release of sensitive corporate data on file sharing sites

## Ways to prevent it

- ❖ **Regular Pen tests**  by security analysts to find any possible vulnerabilities . These can be AI enabled
- ❖ **Ethical hackers** who works  to penetrate the defenses of organizations and then report the vulnerabilities
- ❖ There are organizations, such as ZDI, which offer **“bug bounties,” rewards** for anyone who happens to discover these exploits and pass on that information onto the vulnerable parties

## What is the Solution?

The solution to a zero-day attack, comes in the form of **patches to the software**. Once a zero-day exploit is used to attack an organization, the patching of that exploit becomes the number one priority of the organization. It can take an unreasonably long time to successfully create and roll out the patches, by when malicious groups will be able to steal information. Hence Prevention of such attacks are more effective