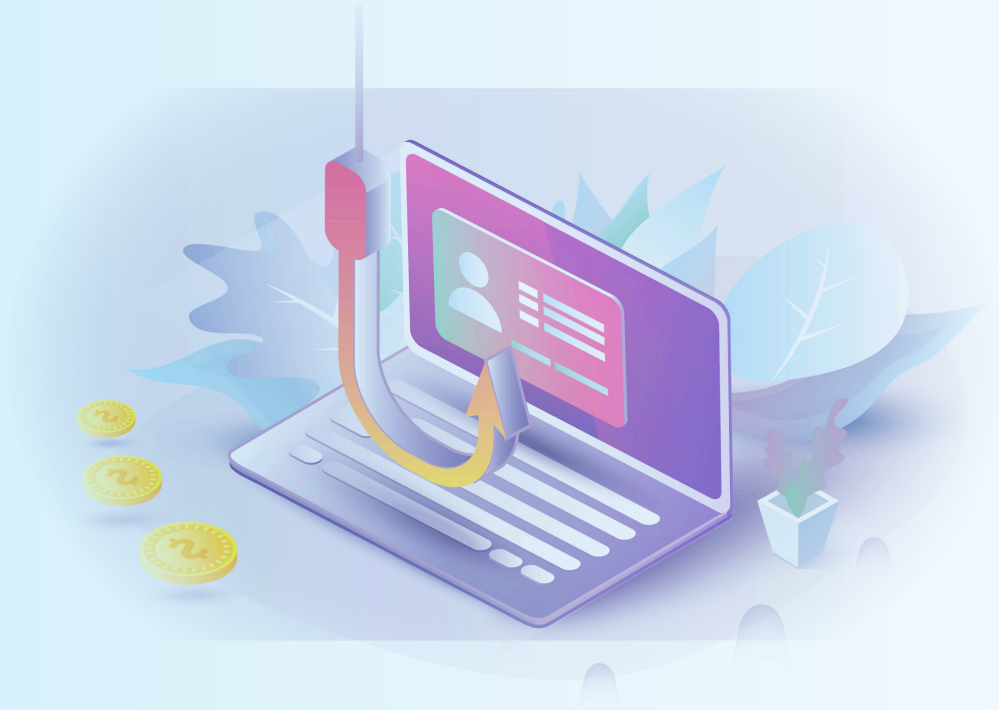
Poison Attacks 101

A comprehensive guide to poison attacks and how to best avoid them

White Paper



Computer Resources of America

Poison Attacks 101

Smart technology is everywhere. Not just in our offices, but even in our day-to-day lives with tools like Google Home and Alexa becoming a commonplace. With technology becoming smarter every minute, the risks are increasing by the minute as well. Cybercriminals are finding new ways to corrupt our IT networks to disrupt our businesses, hold our data hostage and even clear our personal bank accounts. Some of the more overt, commonly known acts of cybercrime include hacking, phishing, and ransomware attacks. This whitepaper discusses a lesser-known cybercrime--Poison attacks.

What are Poison attacks

Poison attacks are attacks on the ability of the system to make smart decisions. Think about this. How do systems make intelligent decisions? Based on the training or data they receive. This data is used to hone the artificial intelligence of the system to help make smart decisions. Poison attacks mess the very base--the training data set. Poison attacks basically skew the system's data model in such a way that the output is no longer as intended. They create a new normal for everything. Poison attacks are primarily backdoor attacks. In a backdoor poison attack, the attacker creates a loophole in the core data rule and trains the system to adhere to that rule so it can be exploited at a later time.

For example, let's say the access control for a particular file is set such that it will allow only those beyond the VP level to view the data. If someone changes the main parameter to include manager level in there, the core data set is violated and the system will not detect an intrusion by someone at the manager level, even if they log in with their credentials.

Poison attack methodologies

Poison attack methodologies typically fall into one of the following 4 categories.

- Logic corruption
- Data manipulation
- Data injection
- DNS Cache Poisoning

Logic corruption

In logic corruption, the attacker changes the basic logic used to make the system arrive at the output. It essentially changes the way the system learns, applies new rules and corrupts the system to do whatever the attacker wants.

Data manipulation

In data manipulation, as the name suggests, the attacker manipulates the data to extend data boundaries that result in backdoor entries that can be exploited later. Unlike logic corruption, the attacker doesn't have access to the logic, so they work with the existing rule and push data boundaries further with a view to accommodate them later.

Data injection

In data injection, the attacker inserts fake data into the actual data set to skew the data model and ultimately weaken the outcome. The weakened outcome then serves as an easy entryway for the attacker into the victim's system.

Protecting yourself against logic corruption, data manipulation, and data injection types of poison attacks

Data poisoning by way of logic corruption, data manipulation and data injection happens when the attacker finds a way to access your data set. The kind of poison attack varies depending on the level of access the attacker is able to achieve. Here's what you can do to ensure such access is prevented.

1. The data poisoning attacks discussed above adversely affect your IT system's machine learning capabilities. So, the first logical step would be to invest in a good machine learning malware detection tool. These tools are different from the typical anti-malware tools you get in the market and are specifically designed to prevent machine learning capability poisoning.

2. Always follow general IT security best practices such as-

    a. Training your employees to identify spam, phishing attempts, and possible malware attacks

    b. Following good password hygiene, which means never sharing passwords and only using passwords that meet the required security standards

    c. Having a powerful IT audit process, tracking and version control tools, so as to thwart any possible insider attacks

    d. Ensuring the physical security of your IT systems by way of biometric access, CCTV systems, etc.,

DNS Cache poisoning

In one of the most common poisoning attacks, the attacker poisons the DNS Cache with the aim of leading visitors to a fake website. In a DNS cache poisoning case, the attacker gains control of the DNS server and then manipulates cache data such that anyone typing the URL of the actual website is redirected to the fake one. This could be a phishing site where the attacker would have carefully laid out a trap to capture the unsuspecting victim's personal data or secure information. For example, the visitor thinks they are logging into their bank's website online, but are actually on the attacker's phishing site, where they enter the login credentials.

Protecting yourself against DNS poison attacks

Here are some ways to protect yourself and your customers from becoming victims of DNS poison attacks.

As discussed before, one of the most common poisoning attacks is the DNS attacks. Cybercriminals try to corrupt your DNS server using theirs. You can prevent this by bringing a trained professional onboard for your DNS server set-up. An expert will know to set up your DNS server such that it has a minimum relationship with other, external DNS servers, thus limiting your attacker's ability to corrupt your DNS server using theirs.

As a best practice, ensure that your DNS servers only store data related to your domain and not any other information. It is harder to corrupt the system when it focuses on a single element.

Another best practice is to ensure that you are up-to-date on all DNS security mechanisms and are using the most recent version of the DNS.

Ensure your site has, in layman terms, an SSL certificate and make sure it is HTTPS. Using encryption, a site with HTTPS protocol allows for a more secure connection between its server and the internet and is better at keeping cybercriminals out. Having an SSL certificate also ensures your site's name shows up alongside the URL in the address bar. This is an easy way for visitors to

identify if they are on a genuine site or not, thus helping them steer clear of phishing attacks and clone sites.

Data poisoning is one of the lesser-known and hence less talked about forms of cybercrime. But, it can inflict great damage--perhaps even more damage than the other obvious threats such as viruses and ransomware, because, unlike a Denial of Service (DoS) attack or a Ransomware attack where you know the moment the malware has hit your system, in a data poisoning attack, the malware is incorrect data that slithers into your system quietly like a snake and changes its overall functioning before delivering the big blow.

For more information please contact,

Computer Resources of America Phone:
2123764040 | Email: hello@consultcra.com