Chapter 4

An Experimental Analysis on Detection of Corona Virus Malware Attacks and Its Preventive Measures

Soumi Banerjee
Department of Information Technology, Ramrao Adik Institute of Technology, India

Swapnil Shinde
Department of Information Technology, Ramrao Adik Institute of Technology, India

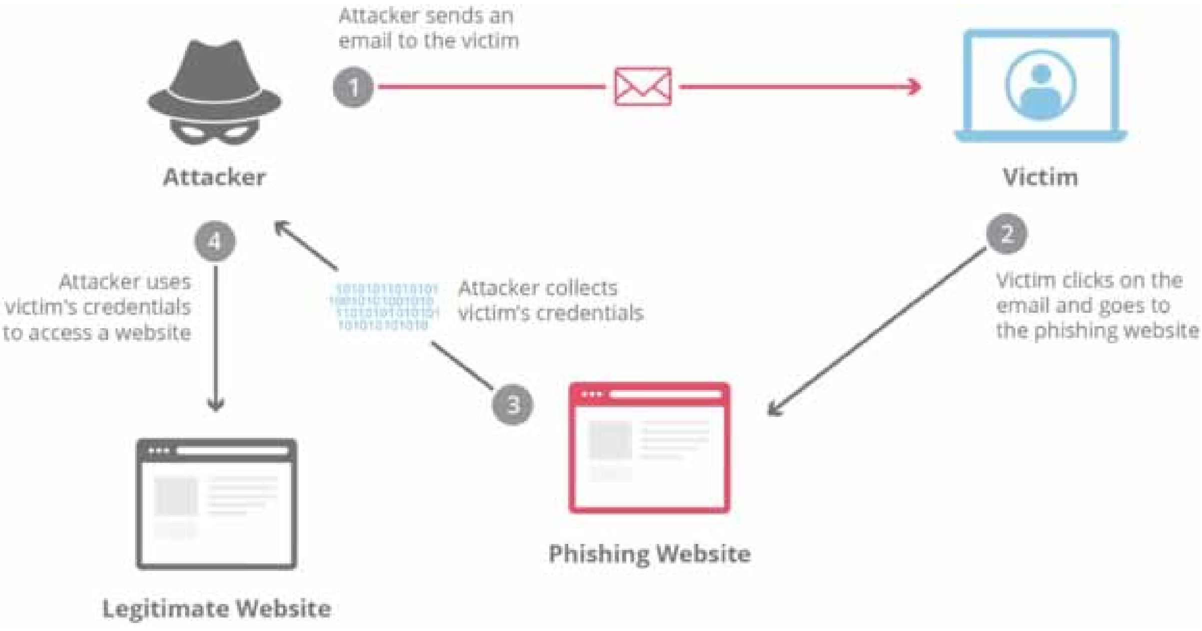
Anita Patil
https://orcid.org/0000-0002-2161-7128
Department of Information Technology, Ramrao Adik Institute of Technology, India

ABSTRACT

Coronavirus has affected China massively. This creates dread among the peoples in the world. Cyber criminals tend to take advantage of fear through malicious activities. Cyber criminals generate a phishing and spam campaign to trick the people in the name of Coronavirus. According to current analysis, the criminals hide malware behind different documents that are shared for creating awareness for the people regarding Coronavirus. Kaspersky technologies discovered that such documents contain viruses, trojans, worms, etc. (malwares) that can infect other files on victims' systems and corrupt or encrypt them. In this chapter, the nature, behavior, and types of different malware and their impacts are analyzed. An analysis is performed on how attackers' attacks using that malware to misuse the victim's data and what the techniques used to perform the attack are. In this chapter, an experimental analysis is performed to detect these attacks, and also measures and guidelines are proposed to prevent these types of attacks.

DOI: 10.4018/978-1-7998-5728-0.ch004

Figure 1. Steps of Phishing attack


Attacker sends an email to the victim
1
Attacker
Victim
2
Victim clicks on the email and goes to the phishing website
3
Attacker collects victim's credentials
4
Attacker uses victim's credentials to access a website
Phishing Website
Legitimate Website

INTRODUCTION

Cybercrime involves crime using computers, network, internet communication and any digital devices connected to the Internet. Cybercrimes are performed by the criminals having bad intention to damage, steal or modify data or information stored in computer or any other digital devices. There are several types of cybercrime attack. Phishing attack is one of the type of cybercrime attack. Some examples of cyber-attacks are discussed below:

a. Denial-of-Service (DoS): sends flood of packets to exhaust the resource.
b. Man-in-Middle Attack: here attacker act as intruder between server and client communication.
c. Phishing Attack: In this type of attack, the attacker sends spam and malicious email that pretend to be from trusted network.
d. Password Attack: In this type of attack, hacker tries to crack the password.
e. SQL Injection Attack: Here hacker tries to hack database by executing invalid SQL queries.
f. Cross-Site Scripting: Here cyber-criminal runs some script on a vulnerable web browser and hack the web browser.
g. Eavesdropping Attack: In this type of attack, the attacker grasps some confidential information that an individual is sending through network.
h. Malware Attack: Cyber criminal's motive is to spread malware like virus, trojan, worms etc. to a victim's system or network.

Phishing attack is a type of cyber-attack where cybercriminal collect or gather the information or credentials like user name and password and other details through fake websites or spam emails. Phish-