War Stories

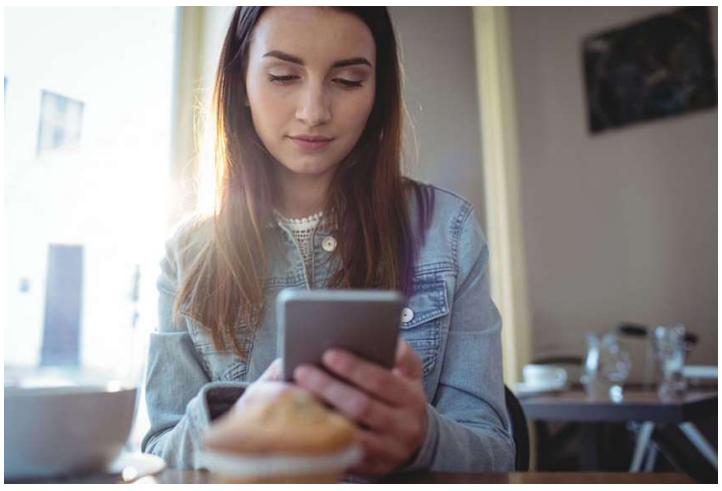
1.1.1

Hijacked People

Sarah stopped by her favorite coffee shop to grab her afternoon drink. She placed her order, paid the clerk, and waited while the baristas worked furiously to fulfill the backup of orders. Sarah pulled out her phone, opened the wireless client, and connected to what she assumed was the coffee shop's free wireless network.

However, sitting in a corner of the store, a hacker had just set up an open "rogue" wireless hotspot posing as the coffee shop's wireless network. When Sarah logged onto her bank's website, the hacker hijacked her session and gained access to her bank accounts. Another term for rogue wireless hotspots is "evil twin" hotspots.

Search the internet on "evil twin hotspots" to learn more about this security threat.

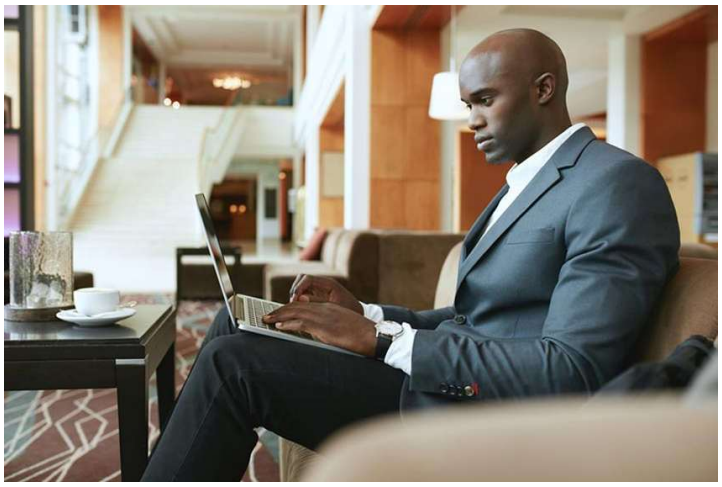


1.1.2

Ransomed Companies

Rashid, an employee in the finance department of a major publicly held corporation, receives an email from his CEO with an attached PDF. The PDF is about the company's third quarter earnings. Rashid does not remember his department creating the PDF. His curiosity is piqued, so he opens the attachment.

The same scenario plays out across the organization as dozens of other employees are successfully enticed to click the attachment. When the PDF opens, ransomware is installed on the employees' computers and begins the process of gathering and encrypting corporate data. The goal of the attackers is financial gain, because they hold the company's data for ransom until they are paid.



1.1.3

Targeted Nations

Some of today's malware is so sophisticated and expensive to create that security experts believe only a nation state or group of nations could possibly have the influence and funding to create it. Such malware can be targeted to attack a nation's vulnerable infrastructure, such as the water system or power grid.

This was the purpose of the Stuxnet worm, which infected USB drives. These drives were carried by five Iranian component vendors into a secure facility that they supported. Stuxnet was designed to infiltrate Windows operating systems and then target Step 7 software. Step 7 was developed by Siemens for their programmable logic controllers (PLCs). Stuxnet was looking for a specific model of the Siemens PLCs that controls the centrifuges in uranium processing facilities. The worm was transmitted from the infected USB drives into the PLCs and eventually damaged many of these centrifuges.

Zero Days, a film released in 2016, documents what is known about the development and deployment of the Stuxnet targeted malware attack. Search for Zero Days to find the film or information about the film.

1.1.4

Video - Anatomy of an Attack

Watch this video to view details of a complex attack.

3:38

1.1.5

Lab - Installing the Virtual Machines

In this lab, you will install VirtualBox on your personal computer. You will then download and install the CyberOps Workstation Virtual Machine (VM).

CyberOps Workstation VM MD5 Checksum: 6a70f156715f85c09fbb859c80c4b6c5 SHA512 Checksum: 2cc44d6585001d99bce5dfc19ed5ef920714ca03

Security Onion VM MD5 Checksum: 8d65135641b9c94e788909026805ad6b SHA512 Checksum: aaca24b0036be5d61dd42a0b3503403e18ae0e12

Installing the Virtual...

1.1.6

Lab - Cybersecurity Case Studies

In this lab, you will analyze the given cases and answer questions about them.

Cybersecurity Cas...

1.0 Introduction

1.2 Threat Actors

Show Menu