Case Study

Watering Hole Attack

International Civil Aviation Organization (ICAO)

Attack Category: Watering Hole Attack

Examples: Cross-site Scripting(XSS), SQL Injection, DNS cache poisoning, Malvertising, Zero-day exploits

1. Description: Watering Hole Attacks function with the attacker profiling the victim to see what types of webpages they visit, testing these webpages for vulnerabilities, injecting malicious code into the webpages that have vulnerabilities that can be exploited, and waiting for that code to infect its intended user.

2. In 2021, zero-day exploits were involved in 66% of all malware[1]. Cross-site scripting placed third on OWASP's top ten list of application security risks[2].

Citations:
1: Comparitech
https://www.comparitech.com/blog/information-security/cybersecurity-vulnerability-statistics/
2: OWASP
https://owasp.org/www-project-top-ten/

Company Description and Breach Summary

International Civil Aviation Organization(ICAO) is an agency within the United Nations that concerns itself with air navigation, infrastructure, flight procedures, the prevention of unlawful actions, and the facilitation of procedures for border crossing.

In November of 2016, the ICAO suffered the largest attack in its history that gave the attackers domain administrator and system administrator level access throughout the organization and, in turn, were able to turn the ICAO website into another watering hole to infect other targeted users. One of the UN’s 192 members, Turkey, was infected within 30 minutes of the ICAO attack.

Timeline

1. Event 1
   On Nov. 22 2016 the breach was flagged and reported by an outside agency to the ICAO.
2. Event 2
   The ICAO website becomes the host for another watering hole attack infecting the Turkish treasury board's website.
3. Event 3
   The information and communications team of the ICAO dismissed deadline of noon on the 23rd of November to take the servers offline.
4. Event 4
   Six weeks after the breach discovery, an ICAO Nordic delegate had an unauthorized email sent from her account, which was downplayed
5. Event 5
   An investigation into the breach had shown that the ICAO's own anti-virus software had detected the malware a year prior
6. Event 6
   ICAO's chief of communications made claims that "ICAO has made robust improvements to its cybersecurity posture and approaches"

Vulnerabilities

The major vulnerabilities stem from the initial malware spread from the watering hole attack, which then turn the ICAO into a secondary watering hole, to the reluctance of the ICT to enact recommended steps, to downplaying the security concerns of people whose credentials had been abused.

Vulnerability 1

The initial watering hole attack was not contained, and the servers were not taken offline, which gave the attackers plenty of time to embed and take advantage of the ICAO systems.

Vulnerability 2

Turning the ICAO web presence into another watering hole vector allowed for UN members to also become infected as well as being able to infect their visitors.

Vulnerability 3

The reluctance of the ICT gave the attackers more time than they should have had to embed themselves into the ICAO systems and take advantage of the administrative access they had taken control of.

Vulnerability 4

By downplaying the severity of the credential theft and not investigating the ICAO had either allowed the attackers to take over more systems, or allowed for new attackers to gain access to their system.

Costs and Prevention

Costs

- Given that the team dedicated to ensuring the security of the ICAO "acted with intent to disguise the source, nature and impact of a breach of the ICAO network“ had kept their jobs, there is potentially still an immeasurable cost to the internal data of the ICAO
- The response of the ICAO shows an organization that favored maintaining internal status quo instead of working towards repairing its security infrastructure and public image

Prevention

- All potentially infected systems should have been taken offline and/or isolated.
- The attack and response should have been willingly put to closer scrutiny both through third-party security vendors as well as any applicable government agency.
- Anti-virus software should be more closely monitored.
- Actions taken to secure systems should be adequately documented and published.