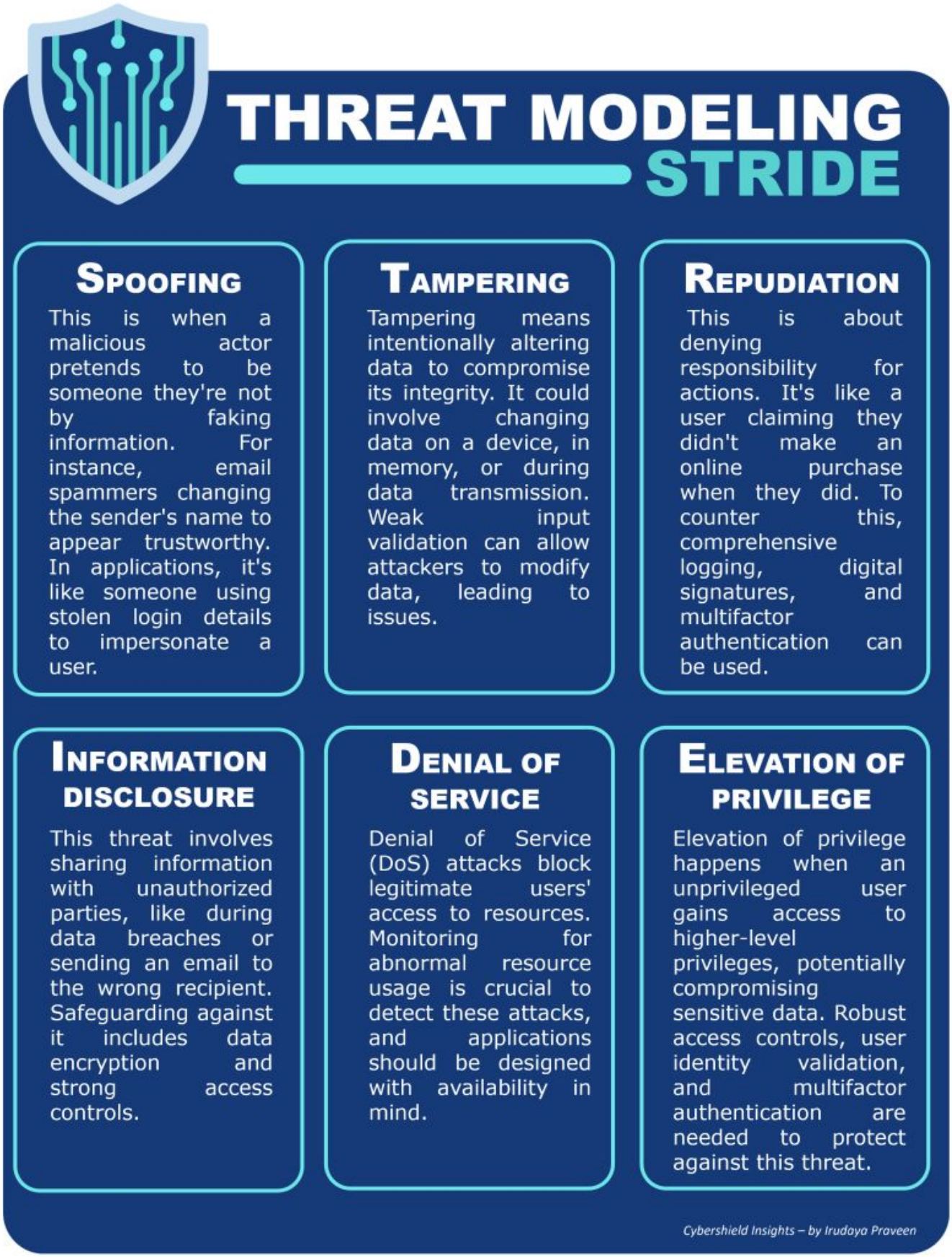
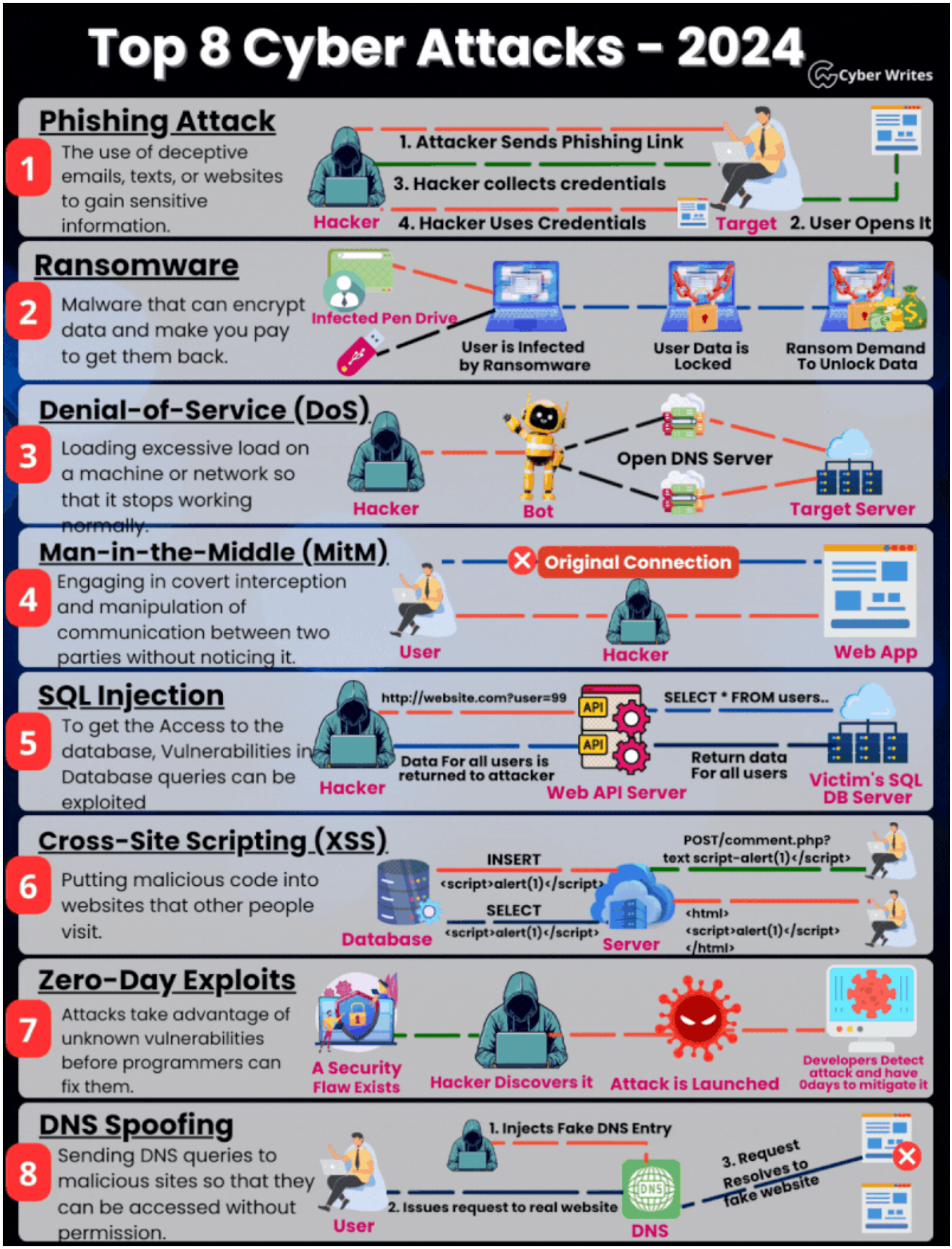
Threat Modeling




Top 8 Cyber Attacks - 2024
Cyber Writes
1
Phishing Attack
The use of deceptive emails, texts, or websites to gain sensitive information.
1. Attacker Sends Phishing Link
3. Hacker collects credentials
Hacker
4. Hacker Uses Credentials
Target
2. User Opens It
2
Ransomware
Malware that can encrypt data and make you pay to get them back.
Infected Pen Drive
User is Infected by Ransomware
User Data is Locked
Ransom Demand To Unlock Data
3
Denial-of-Service (DoS)
Loading excessive load on a machine or network so that it stops working normally.
Hacker
Bot
Open DNS Server
Target Server
4
Man-in-the-Middle (MitM)
Engaging in covert interception and manipulation of communication between two parties without noticing it.
Original Connection
User
Hacker
Web App
5
SQL Injection
To get the Access to the database, Vulnerabilities in Database queries can be exploited
http://website.com?user=99
API
API
SELECT * FROM users..
Hacker
Data For all users is returned to attacker
Web API Server
Return data For all users
Victim's SQL DB Server
6
Cross-Site Scripting (XSS)
Putting malicious code into websites that other people visit.
INSERT
<script>alert(1)</script>
SELECT
<script>alert(1)</script>
Database
Server
POST/comment.php?
text script-alert(1)</script>
<html>
<script>alert(1)</script>
</html>
7
Zero-Day Exploits
Attacks take advantage of unknown vulnerabilities before programmers can fix them.
A Security Flaw Exists
Hacker Discovers it
Attack is Launched
Developers Detect attack and have 0days to mitigate it
8
DNS Spoofing
Sending DNS queries to malicious sites so that they can be accessed without permission.
1. Injects Fake DNS Entry
2. Issues request to real website
DNS
3. Request Resolves to fake website
User

From:
https://wiki.fortier-family.com/ - **Warnaud's Wiki**

Permanent link:
https://wiki.fortier-family.com/cybersecurity/threats

Last update: **2024/02/02 06:54**