The State of Threats: Safeguarding the Health System Against Various Modes of Attacks

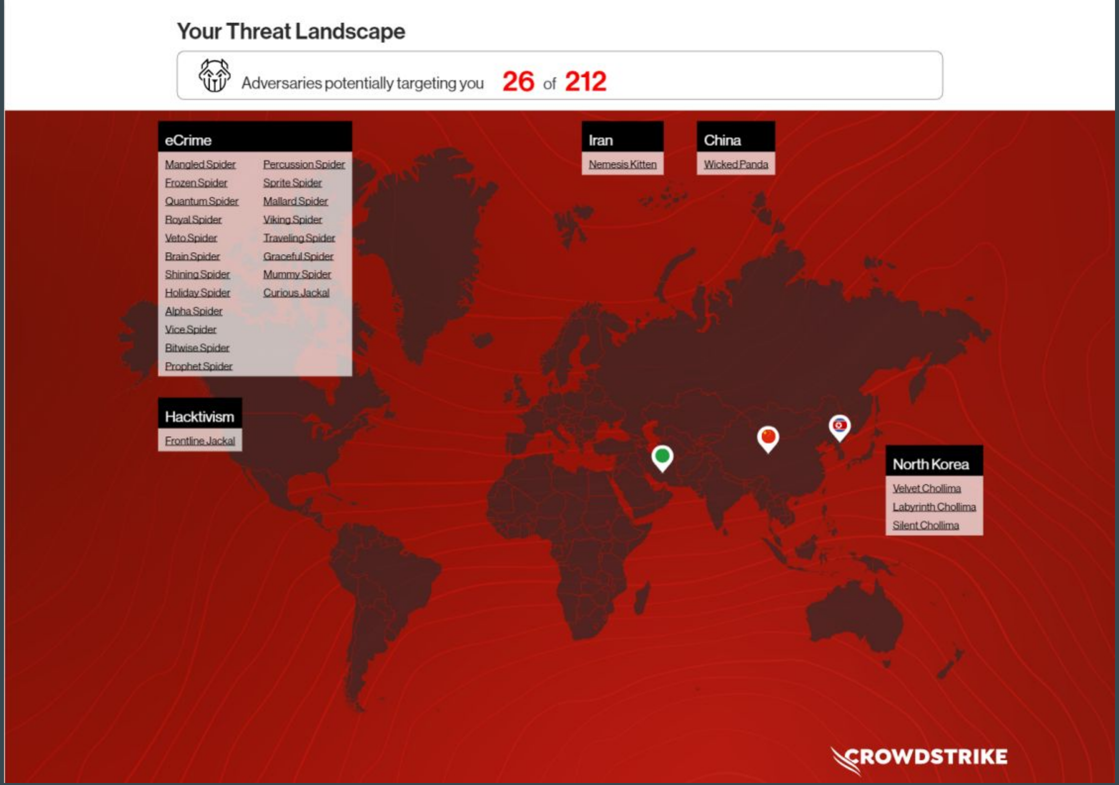
•••

Presented By:
Farheen Ali, Sonia Daneshwar, Jacob Jones, Tyler Ramos

April 25th, 2023

State of Threats

- CrowdStrike tracks 26 threat actors actively targeting mid sized hospitals
- File Exfiltration
- Ransomware
- Information Exfiltration
- Monetary Exfiltration



Your Threat Landscape

Adversaries potentially targeting you 26 of 212

eCrime

- Mangled Spider
- Frozen Spider
- Quantum Spider
- Royal Spider
- Veto Spider
- Brain Spider
- Shining Spider
- Holiday Spider
- Alpha Spider
- Vice Spider
- Bitwise Spider
- Prophet Spider
- Percussion Spider
- Sprite Spider
- Mallard Spider
- Viking Spider
- Traveling Spider
- Graceful Spider
- Mummy Spider
- Curious Jackal

Iran

- Nemesis Kitten

China

- Wicked Panda

Hacktivism

- Frontline Jackal

North Korea

- Velvet Chollima
- Labyrinth Chollima
- Silent Chollima

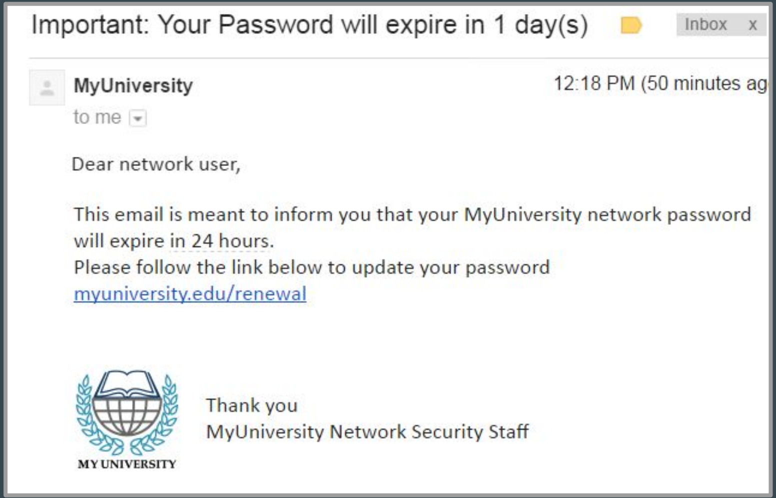
Real Events

- Hospital Almost Gives Child an Overdose
- Baby’s Life Cut Short Due to Ransomware Attack
- Hospital “Unable” to Treat German Women

Modes of Attacks

Phishing

- Phishing is the practice of infecting a seemingly innocuous email with malicious links.
- Phishing links are made to look very convincing, and try to impersonate an organization or person with credibility.



Important: Your Password will expire in 1 day(s)

MyUniversity

12:18 PM (50 minutes ag

to me

Dear network user,

This email is meant to inform you that your MyUniversity network password will expire in 24 hours.
Please follow the link below to update your password
myuniversity.edu/renewal

Thank you
MyUniversity Network Security Staff

Ransomware Attacks

- Malware is injected into a network to infect and encrypt sensitive data, and this data is then held hostage until a ransom is paid.
- Malware, or malicious software, is a blanket term for any kind of computer software with malicious intent.
- Phishing is typically used to inject malware into a system.

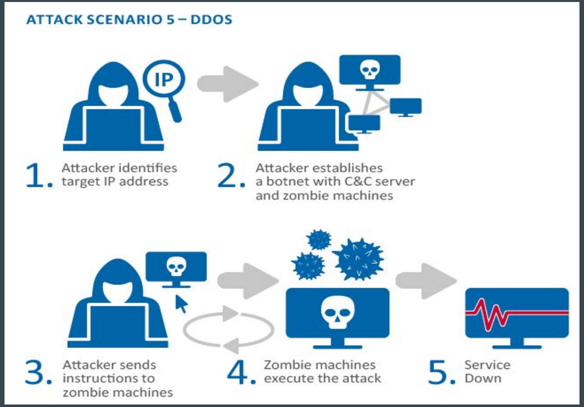
Modes of Attacks

Data Breaches

- Breaches are at a disproportionately large amount in the healthcare industry.
- In 2020, the average number of data breaches that occurred every day in the healthcare sector was 1.76.
- This threat landscape could facilitate indirect access to sensitive data, such as:
  - Social security numbers
  - Credit card numbers
  - Medical device intellectual property

DDoS Attacks

- A Distributed-Denial-Of-Service attack is when many fake connection requests are sent to the targeted server, forcing it to go offline.
- A botnet can be created in a hospital that recruits all IoT devices to participate in the attack.


ATTACK SCENARIO 5 – DDOS
IP
1. Attacker identifies target IP address
2. Attacker establishes a botnet with C&C server and zombie machines
3. Attacker sends instructions to zombie machines
4. Zombie machines execute the attack
5. Service Down

How Can The Healthcare System Prepare?

- Future breaches are always inevitable but hospitals can make it harder to happen..
- Require staff to take training in cybersecurity, with a focus on phishing attempts through email, and social engineering.
  - The Canadian Internet Registration Authority does training that simulates phishing attacks, which has resulted in a decrease on malicious links being clicked by two-thirds.
- The Cybersecurity and Infrastructure Security Agency suggested to use a the 3-2-1-backup method:
  - Keep **3** copies of your data - 1 primary and 2 backups
  - Have **2** different media types -- protects against different types of hazards
  - **1** copy off-site for disaster recovery.
- Companies should opt for physical devices with security embedded in it already.

RESOURCES

https://www.wired.co.uk/article/ransomware-hospital-death-germany

https://online.maryville.edu/blog/healthcare-cybersecurity/

https://www.wired.co.uk/article/ransomware-hospital-death-germany

https://www.wsj.com/articles/ransomware-hackers-hospital-first-alleged-death-11633008116

https://www.nbcnews.com/tech/security/ransomware-attacks-hospitals-take-toll-patients-rcna54090

https://www.crowdstrike.com/adversaries

https://www.upguard.com/blog/biggest-cyber-threats-in-healthcare

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6989022/

https://www.malwarebytes.com/malware

Images used

https://www.imperva.com/learn/wp-content/uploads/sites/13/2019/01/phishing-attack-email-example.png