Ransomware: Evaluation of Mitigation and Prevention Techniques

Juanjose Rodriguez-Cardenas
Kennesaw State University

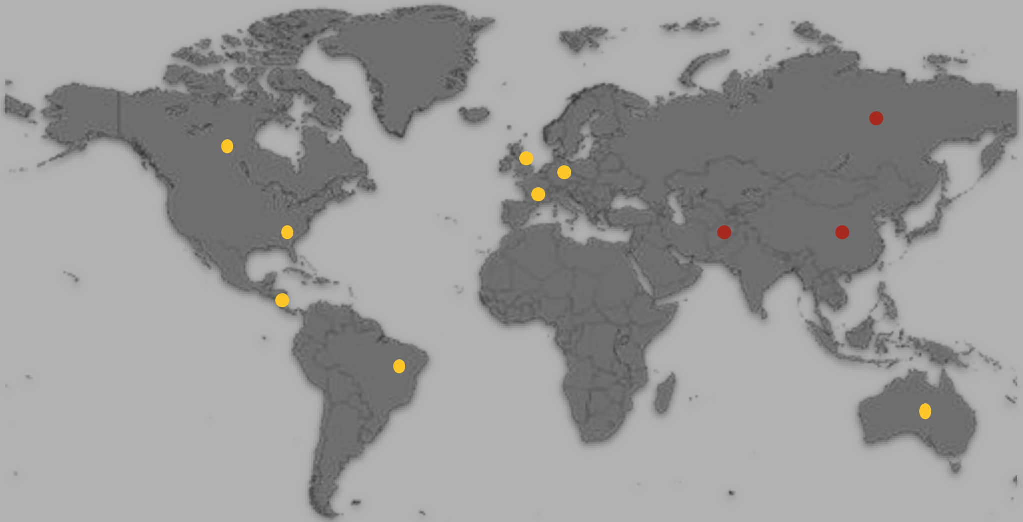
Ransomware: Evaluation of Mitigation and Prevention Techniques

Institute for Cyber Workforce Development
Department of Information Technology

Dr. Hossain Shahriar - Mentor
Juan Rodriguez Cardenas – Undergraduate B.S Cybersecurity

Global Overview

- ❑ Russia
- ❑ Iran
- ❑ North Korea



Legend

🔴 Threat actor

🟡 Targets

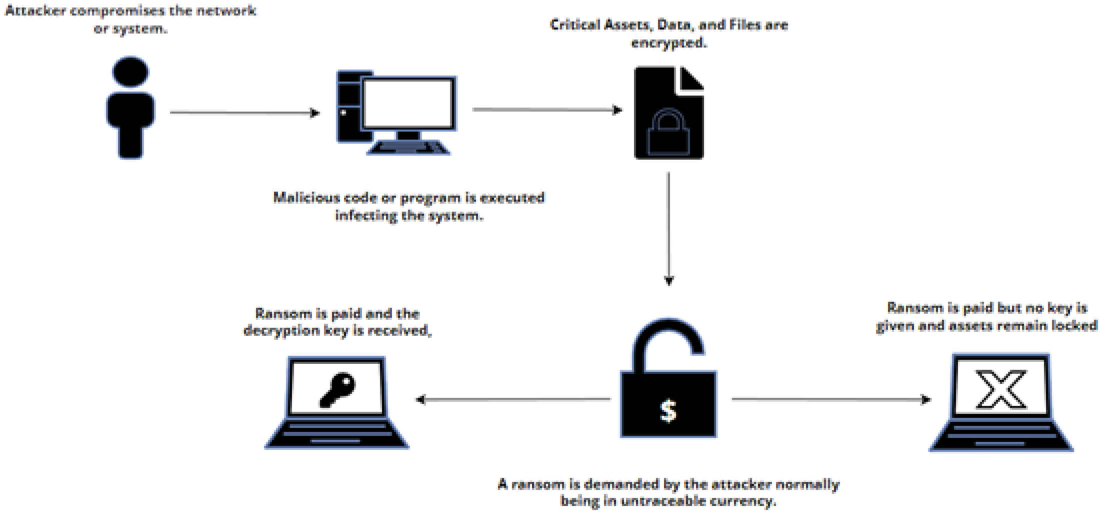
Countries Organizations affected

- United States 47%
- Italy 8%
- Australia 8%
- Brazil 6%
- Germany 6%

Most affected Nations

- Israel
- South Korea
- U.K

Procedure



Attacker compromises the network or system.

Malicious code or program is executed infecting the system.

Critical Assets, Data, and Files are encrypted.

A ransom is demanded by the attacker normally being in untraceable currency.

Ransom is paid and the decryption key is received,

Ransom is paid but no key is given and assets remain locked

Why?

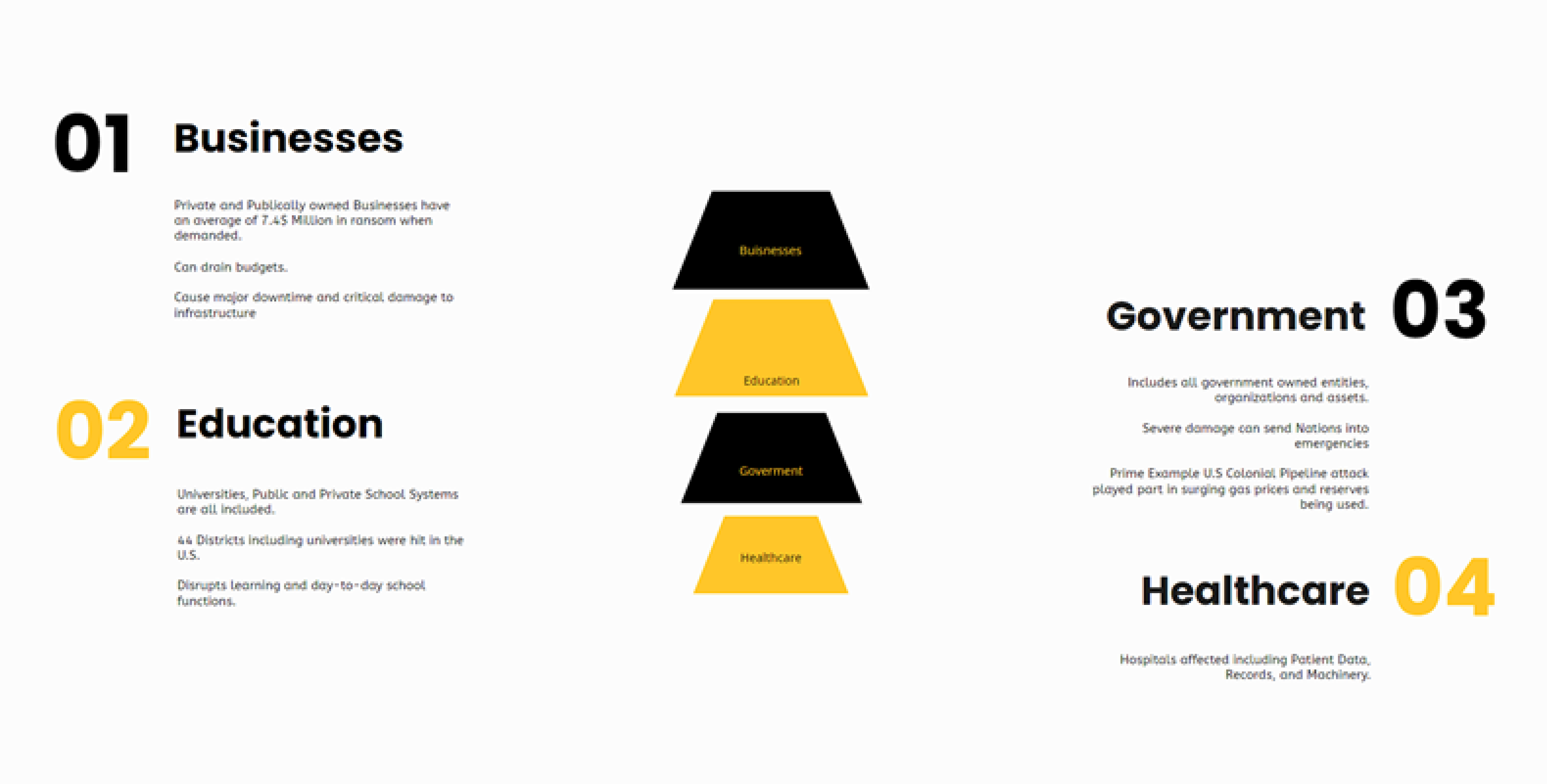
- Responsible for roughly 14$ Billion in damages in 2022 alone
- Targets Organizations and other critical infrastructure from varying industries
- Threat to National Security for both Citizen and Officials
- Drains Budgets and unrecoverable downtime

Classes of Malware Detection

- Static: Examines ransomware malware by not executing the actual binary files. They just use static data such as PE Headers, URLS, and File Hash. Some open-source tools that can allow us to test it are VirusTotal. Static analysis is easy to implement and can detect simple malware. However, it is not very efficient against sophisticated well-developed malware. AI has helped to improve its detection methods.

- Dynamic: Uses abnormal data from compiled ransomware attacks/events to detect attacks. Packet collection and data collection from the infected system and a command control (C2) server can be used with Random Forest (RF) machine learning algorithm to detect more accurate attacks.

Industries



01 Businesses

Private and Publically owned Businesses have an average of 7.45 Million in ransom when demanded.

Can drain budgets.

Cause major downtime and critical damage to infrastructure

02 Education

Universities, Public and Private School Systems are all included.

44 Districts including universities were hit in the U.S.

Disrupts learning and day-to-day school functions.

Government 03

Includes all government owned entities, organizations and assets.

Severe damage can send Nations into emergencies

Prime Example U.S Colonial Pipeline attack played part in surging gas prices and reserves being used.

Healthcare 04

Hospitals affected including Patient Data, Records, and Machinery.

Removal and Prevention

Fix Management: Ensure all Workstations, both Physical and Virtual, including servers are up to date on the latest Operating System patches.

Antivirus: Update and constantly run anti-virus, gather points of interest, and confirm whether it is malware or not and how it has been distinguished in previous weeks.

Email Gateway

- Most PCs can be signed in into experimental mode by squeezing F8 key before the windows begin. Check framework registry, run, assignment chief, and framework arrangements.

-Task supervisor: In this element, there is a tab called process that demonstrates all the running programs: It's prescribed to stop suspicious and obscure files.

-Check : %localAppData%, %ProgramData%.

Future Directions

- Understanding Counter-Offensive measures
- Dynamic detection through AI
- How Generative Text AI's such as ChatGPT can implement more volatile increases of attacks. Without attackers knowing much.

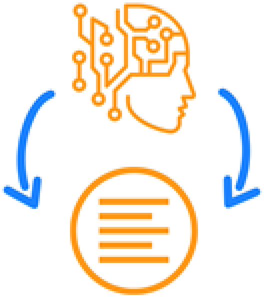


Image retrieved via; https://eskritor.com/