Ransomware Lifecycle and How to be Ready for it!
About me!

Safa Aktepe
Sr. Security Engineer

Law Enforcement 2011 - 2016
Higher-Ed 2016 - 2020
Corporate 2020 - Present

Master's in Information Assurance and Security
Certifications: GCFA, GCFE, AWS CCP, Nuix
What we will cover?

What is Ransomware?
- Definition of Ransomware, Well-known Ransomwares, Advanced Threat Groups

Lifecycle of Ransomware
- Stages of a Ransomware Attack, Commonly Used TTPs, Motivations

How to be protected?
- Best Practices to be Secure and Protected for potential attacks
What is a Ransomware?

Type of malicious software designed to block access to a computer system or files by encrypting them until a sum of money is paid.
What is the motivation of Ransomware attacks?
Well-Known Advanced Threat Groups with Ransomware Attacks
Percentage of the Top 10 Types of Reported Ransomware

- Sodinokibi (REvil): 14.2%
- Conti V2: 10.2%
- Lockbit: 7.5%
- Clop: 7.1%
- Egregor: 5.3%
- Avaddon: 4.4%
- Ryuk: 4%
- Darkside: 3.5%
- Suncrypt: 3.1%
- Netwalker: 3.1%
- Phobos: 2.7%
The Cost of Ransomware for Businesses (in Billions)

2019: $11.5

2021: $20

2031 (est.): $265
Ransomware Attack Stages
Most Common Techniques for Initial Access

- **Phishing Emails**
  - Mass Email Campaigns, Targeted Spear Phishing attacks

- **Credential Attacks**
  - Brute Force Attacks, Password Spraying Attacks etc.

- **Vulnerability Exploitation**
  - Zero-Day Attacks, Abuse of Misconfigured Systems, Known Vulnerability Exploitations

- **Malware**
  - Malwares, Rootkits, Droppers
They got the access! What is next?

- Establish Persistence Mechanism
- Discover the compromised network/system
- Privilege Escalation
- Lateral Movement
Final Stage!!!

- Exfiltrate Data
- Destroy Backups
- Encrypt
What we can do???
Best Practices to Prevent Initial Access

- Multi-Factor Authentication
- Strong Passwords
- Cybersecurity Awareness
- Update and Patch Applications
- Malware Protection (AV, EDR)
- Network Security and Monitoring
Best Practices to Prevent Persistence and Lateral Movement
(In addition to the previous items)

- Limit the number of Admin Accounts
- Additional Monitoring on Admin Accounts
- Additional Protection and Monitoring for Domain Controllers and Mission Critical Systems
Best Practices to Prevent/Minimize the Impact
(In addition to the previous items)

- Multiple Backups in Different Locations (Online and Offline)
- Additional Monitoring and Protection for Backup Servers
- Additional Monitoring for Egress/Outbound Data Transfers (Especially in big size)
- Additional Protection and Monitoring for Domain Controllers and Mission Critical Systems
Thank you!
References

- https://www.cisa.gov/stopransomware
- https://www.trendmicro.com/vinfo/us/security/definition/ransomware
- https://www.cognyte.com/blog/ransomware_2021/
- https://www.cloudwards.net/ransomware-statistics/
- https://www.deepwatch.com/blog/anatomy-of-ransomware-attack/
- https://www.cybertalk.org/2022/02/14/the-anatomy-of-a-ransomware-attack-in-2022/
- https://krebsonsecurity.com/2021/05/a-closer-look-at-the-darkside-ransomware-gang/