Ransomware - part2

Lecture (6)

Information Security Department

2nd Class- First Course

28 November 2023

By

Assist. Lecturer : **Nuha Kareem Hameed**

Email : NuhaKareem@uobabylon.edu.iq

- Ransomware Is Evolving

- Ransomware is a rapidly evolving threat. As ransomware attacks continue to cause greater economic impacts, the patterns of attacks are changing to "**quality over quantity**." This is possible due to more highly targeted attacks, using ransomware variants like Ryuk, on medium to large organizations with a greater ability to pay.

Ransomware: reasons of rapid growth

- Several factors have contributed to the rapid growth and evolution of ransomware, including :

1. digital transformation initiatives (which greatly increases the number of potential entry points and the ability for attacks to propagate),
2. the rise of Bitcoin (enabling easy and virtually untraceable payments to cybercriminals),
3. and the emergence of **Ransomware-as-a-Service** (RaaS; see the next slide), which makes it easy for practically anyone to use ransomware.

Ransomware-as-a-Service Is an Emerging Threat

- RaaS has emerged as a new threat that literally makes it as easy as "one, two, three" for practically anyone with limited technical skills to become a cybercriminal. For example, **Tox** — one of the earliest known RaaS offerings, first discovered in May 2015 — can be downloaded from **the dark web** using a **Tor browser ,**
- and then set up as follows:

1. Enter a ransom amount.
2. Create a ransom note.
3. Type a CAPTCHA so that the creators of Tox know you're not a bot.

- RaaS software is typically available to download for free or for a small fee. The real profit for the creators of RaaS software is in the cut they take of the ransom payments that are collected — typically from 5 percent to 30 percent.

Dark web and Tor browser

- **Dark web definition**
  - ✓The dark web is the hidden collective of internet sites only accessible by a specialized web browser. It is used for keeping internet activity anonymous and private, which can be helpful in both legal and illegal applications.
  - ✓**What can be found in dark web?**
  - ✓**Is the dark web illegal?**
  - ✓**VPN vs. Tor browser**

- **Tor browser**
  - ✓The Tor Browser is a web browser that anonymizes your web traffic using the Tor network, making it easy to protect your identity online.
  - ✓Tor Browser is also **illegal** in authoritarian regimes that want to prevent citizens from reading, publishing, and communicating anonymously

Paying a Ransom Doesn’t Solve Your Security Problems

- There’s also no guarantee that the perpetrator didn’t install other malware or exploit kits to facilitate future cyberattacks against your organization.
- A copy of your files may also have been exfiltrated for other purposes, such as selling your organization’s **sensitive information** on the dark web.

Paying a Ransom Doesn't Solve Your Security Problems

- In most cases, your files will be decrypted if you pay the ransom, but there's no guarantee.

- Although it's in the cybercriminals' best interests to restore your files if you pay the ransom (if a ransomware campaign gains a reputation for not decrypting files when the ransom is paid, then there is no reason for future victims to pay the ransom), **there's no honor among thieves**.

- This is particularly true with the emergence of RaaS because a "**newbie**" cybercriminal may not see the bigger picture. Also, if the encryption key doesn't work for some reason, you can't just call customer service!

Prevent based on packet inspection

- Most ransomware relies on a robust C2 communications infrastructure, for example, to transmit encryption keys and payment messages. By preventing an attacker from connecting with ransomware that has infected its network, an organization can stop a successful ransomware attack. If, for example, the attacker is unable to send encryption keys to an infected endpoint or instruct a victim on how to send a ransom payment, the ransomware attack will fail.

Prevent based on DNS

- As the following Table shows, many ransomware variants rely heavily on DNS for C2 communications. In some cases, a Tor (The Onion Router) browser is also used for C2 communications. Therefore, it's important to be able to block both types of communications, using a method like a proxy

C2 Communications Examples in Ransomware

Name	Encryption Key	Payment Message
Locky	DNS	DNS
TeslaCrypt	DNS	DNS
CryptoWall	DNS	DNS
TorrentLocker	DNS	DNS
PadCrypt	DNS	DNS, Tor
CTB-Locker	DNS, Tor	DNS
FAKBEN	DNS	DNS, Tor
PayCrypt	DNS	DNS
KeyRanger	DNS, Tor	DNS

BACKUP

- Keep at least three copies of your company's data.
- Store two backup copies on different devices or storage media.
- Keep at least one backup copy off-site and offline or otherwise not accessible other than physically. Get the basics right: back up data regularly.

Other Anti-ransomware Solutions

- Build a Layered Security Architecture Based on Open Standards.
- Leverage Cloud-Based, Real-Time Threat Intelligence.
- Automate Security Actions to Reduce Response Time.
- Embed Security throughout in Network Environment.
- Reduce Complexity in Security Environment.