Malware Analysis: Ransomware

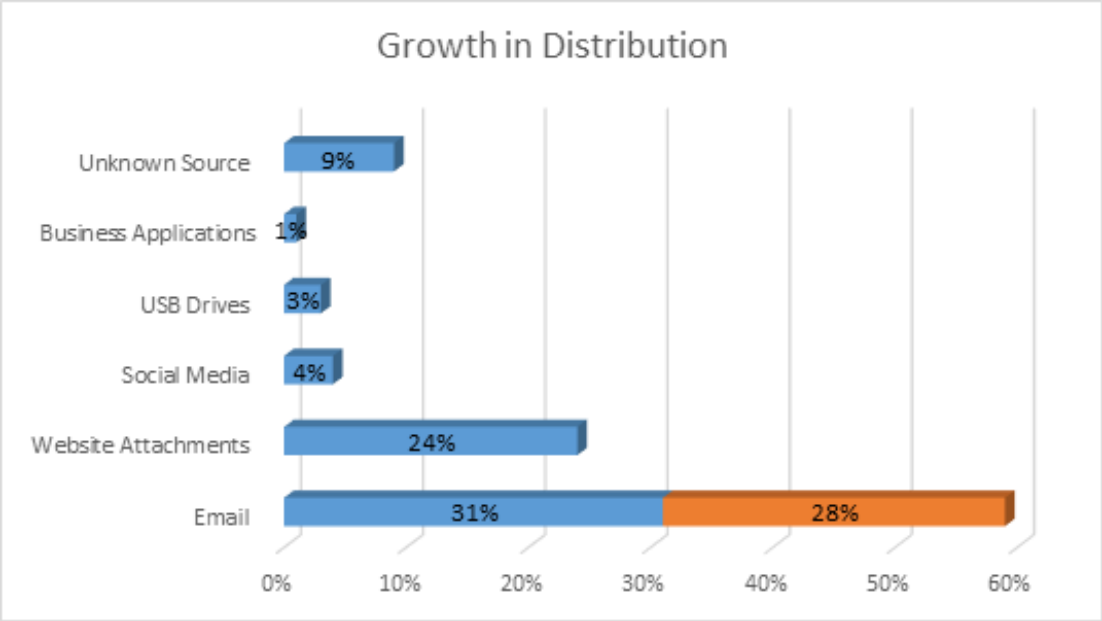
What is ransomware?

- Ransomware is a type of malware that prevents users from accessing their system or files unless money (a ransom) is paid.

Two types of ransomware:

- **Encryption-based Ransomware**
  - Designed to encrypt system files and demand payment to provide the victim with the key that can decrypt the blocked content
- **Locker Ransomware**
  - Locks the victim out of the operating system making it impossible to access the desktop and any apps or files

How it spreads



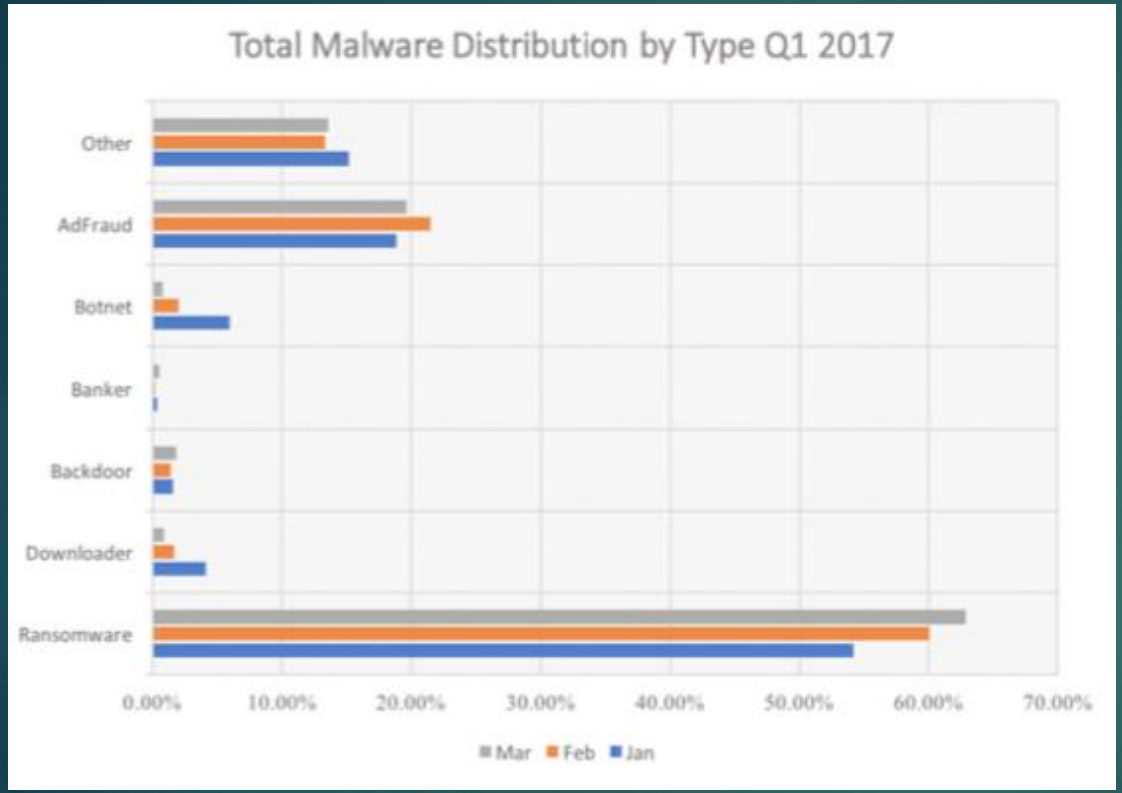
- Phishing email attachments have become the #1 delivery vehicle for Ransomware. A review by IBM Security found that the quantity of Ransomware-infected emails expanded 6,000 percent as compared to 2016.

Source: IBM Security

Payment

- **Bitcoins**
  - An electronic currency that is managed by its users
  - No intermediaries (e.g. Banks)
  - No personal information is necessary for processing transactions
  - Maintains the anonymity of both parties in a transaction

- **Other**
  - iTunes and Amazon gift cards

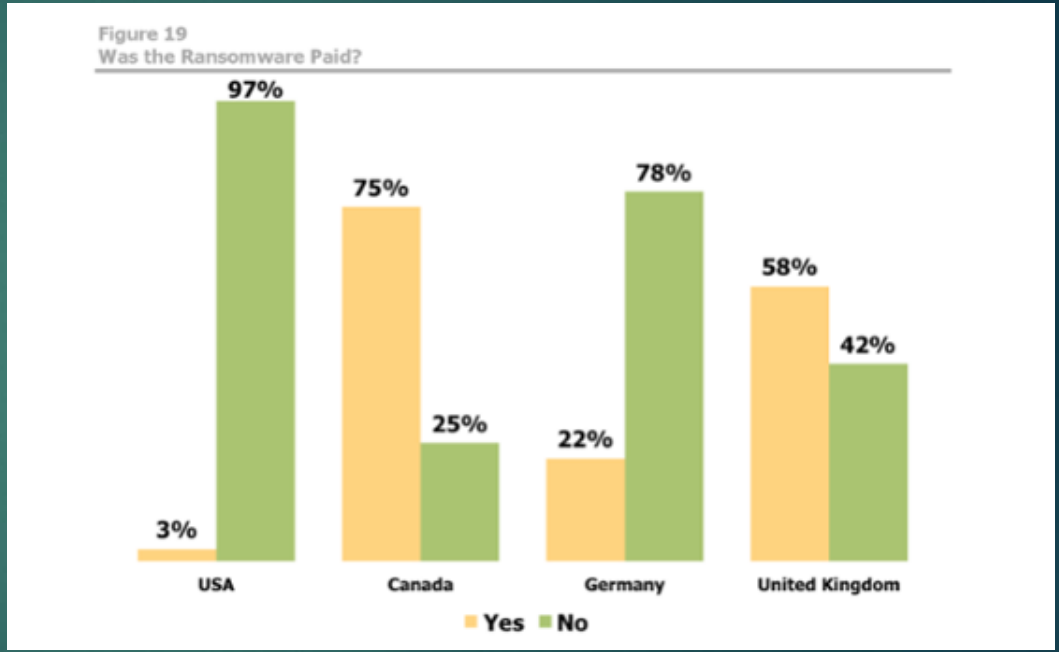


Source: Malwarebytes

- Ransomware continues to be the most heavily utilized type of malware by the most popular methods of distribution, both exploit kits and malicious spam (malspam).

Who Pays the Ransom?

- Very few organizations actually pay the ransom, even after successful attacks — results from an Osterman Research survey conducted with Ransomware victims indicated that only 3 percent of U.S. companies paid up.



Source: Osterman Research

WannaCry

- Encryption-based ransomware
- Infected more than 230,000 computers in over 150 countries in a single day.
- It searches for and encrypts 176 different file types.
- If payment is not made after seven days it claims the encrypted files will be deleted.
- It propagates using EternalBlue, an exploit of Windows' SMB protocol.

Major Organizations Affected by WannaCry

- The UK's National Health Service
- FedEx
- Nissan
- Renault
- The Chinese Public Security Bureau
- Chinese Universities
- Hitachi (Japanese electronics maker)
- Police in Andhra Pradesh, India
- Russian banks, telecom providers, the railway system, and the interior ministry

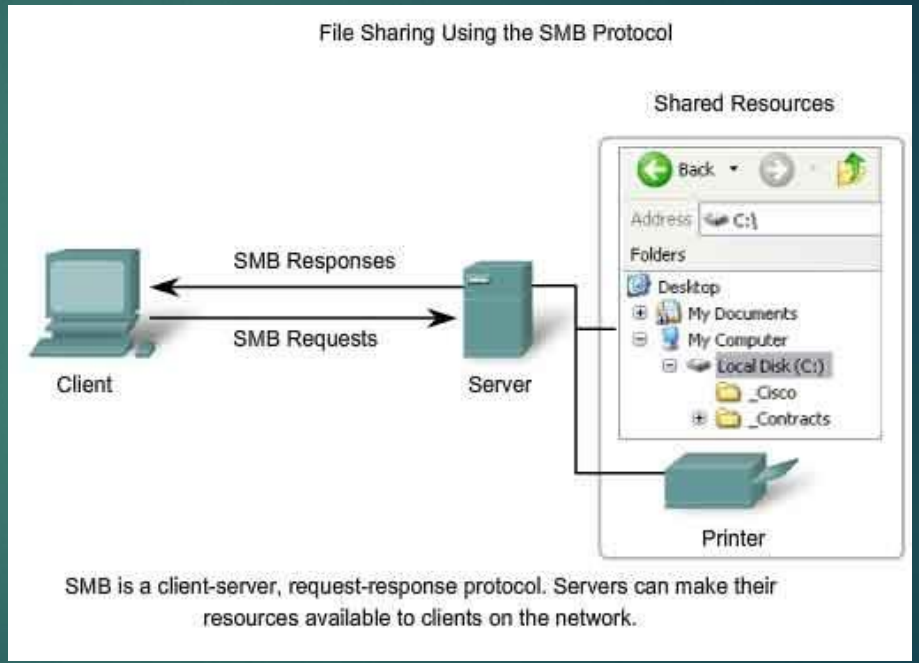
Why Ransomware Creators Targets Businesses

- Attackers know that a successful infection can cause major business disruptions, increasing their chances of getting paid
- Ransomware can affect servers and cloud-based file-sharing systems, directly affecting the business's core
- Cyber criminals know that businesses would rather not report an infection for fear or legal consequences and brand damage

Source: www.heimdalsecurity.com

Server Message Block (SMB) Protocol

- A network file sharing protocol implemented in Microsoft Windows
- Using the SMB Protocol, an application or program can access files on a remote server
- Programs can read, create, and update files on a remote server



Kill Switch

- An emergency mechanism used to shut down or disable machinery, a device or a program.
- Designed to completely and quickly abort and operation.
- WannaCry contains a kill switch designed to shut down the program and prevent its spreading across a network.
- WannaCry's kill switch was found and activated by 22-year-old Marcus Hutchins, a web security researcher in England.

Resources

- https://blog.barkly.com/ransomware-statistics-2017
- https://heimdalsecurity.com/blog/what-is-ransomware-protection/#ransomwaredefinition
- https://www.trendmicro.com/vinfo/us/security/definition/ransomware
- https://blogs.systweak.com/2017/05/ransomware-statistics-2017-at-a-glance/
- https://venturebeat.com/2017/02/19/ransomware-has-exploded-because-of-bitcoins-anonymity/
- http://whatis.techtarget.com/definition/kill-switch
- https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html
- https://www.bleepingcomputer.com/news/security/wannacry-ransomware-version-with-second-kill-switch-detected-and-shut-down/
- http://www.techrepublic.com/pictures/gallery-10-major-organizations-affected-by-the-wannacry-ransomware-attack/