PHISHING & RANSOMWARE

WHAT IS IT?

It is alarming how easily an organisation can have its data stolen. This is conducted by attackers in **five simple steps**: reconnaissance, weaponization, delivery, installation and propagation.

1. Attackers gather info and identify contacts through publicly available sources such as social media and company website.
2. Then, they use the gathered intelligence to prepare a believable story and customise the **malware-infected email** to target individuals.
3. The unsuspecting email recipient **infects their own workstation** by clicking on link or opening an attachment.
4. Malware spreads throughout company estate using network connections, **encrypting data** essential to daily operations and effectively paralysing the entire organisation.
5. Finally, attackers demand a **payment** for returning the data to its original state.

KEY FACTS

40 secs

A company is hit with ransomware every 40 seconds [1]

71%

71% of companies targeted by ransomware have been infected [2]

80%

80% of infected businesses lost access to data for over two days [3]

[1] https://smallbiztrends.com/2016/04/cyber-attacks-target-small-business.html
[2] https://www.websecurity.symantec.com/security-topics/istr-2017-infographic
[3] https://securityintelligence.com/20-eye-opening-cybercrime-statistics/