Principles of Analyzing .NET Ransomware Malware

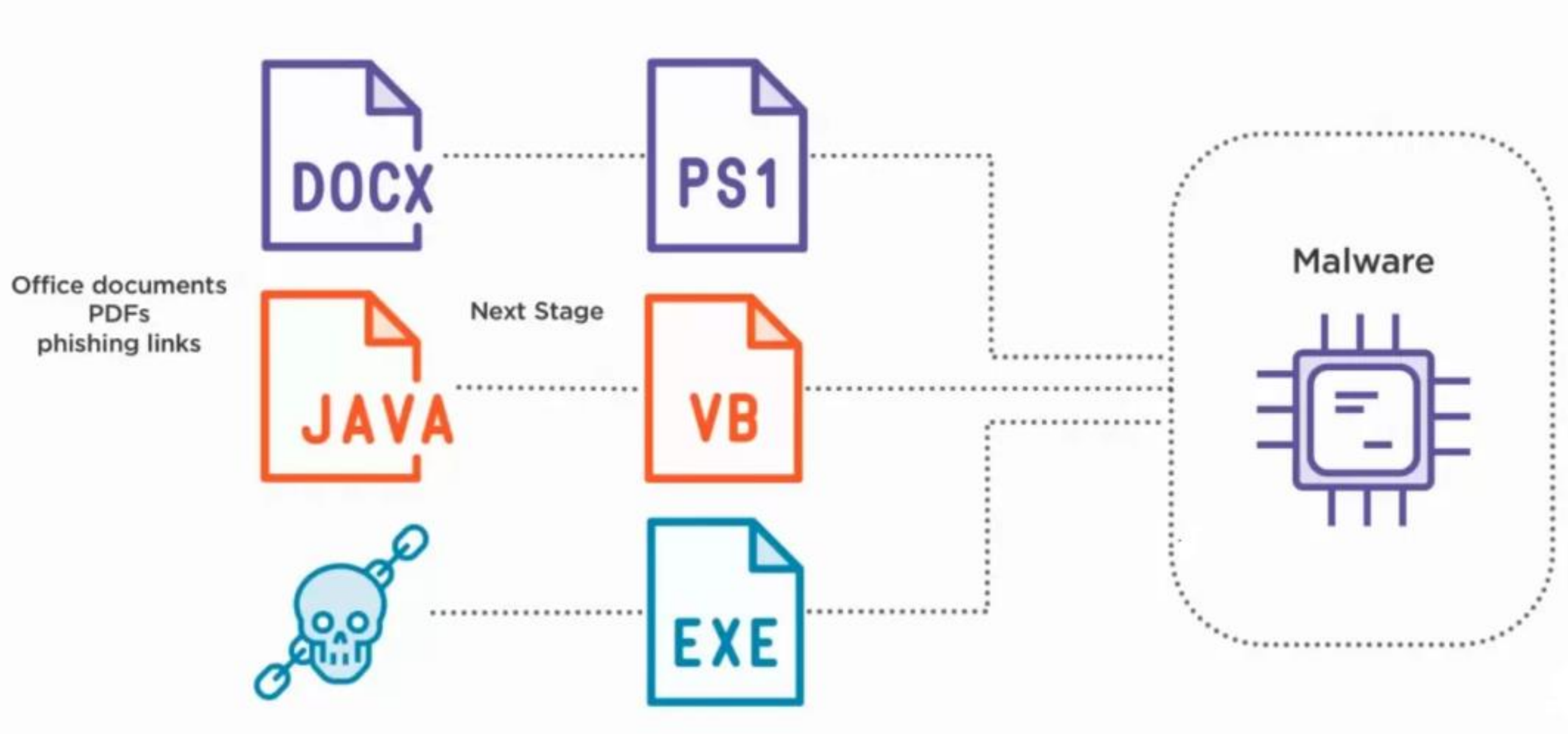
What is ransomware

Ransomware is a malware that restricts access to data by encrypting files or locking computer screens and attempts to extort money from victims in the form of cryptocurrencies.

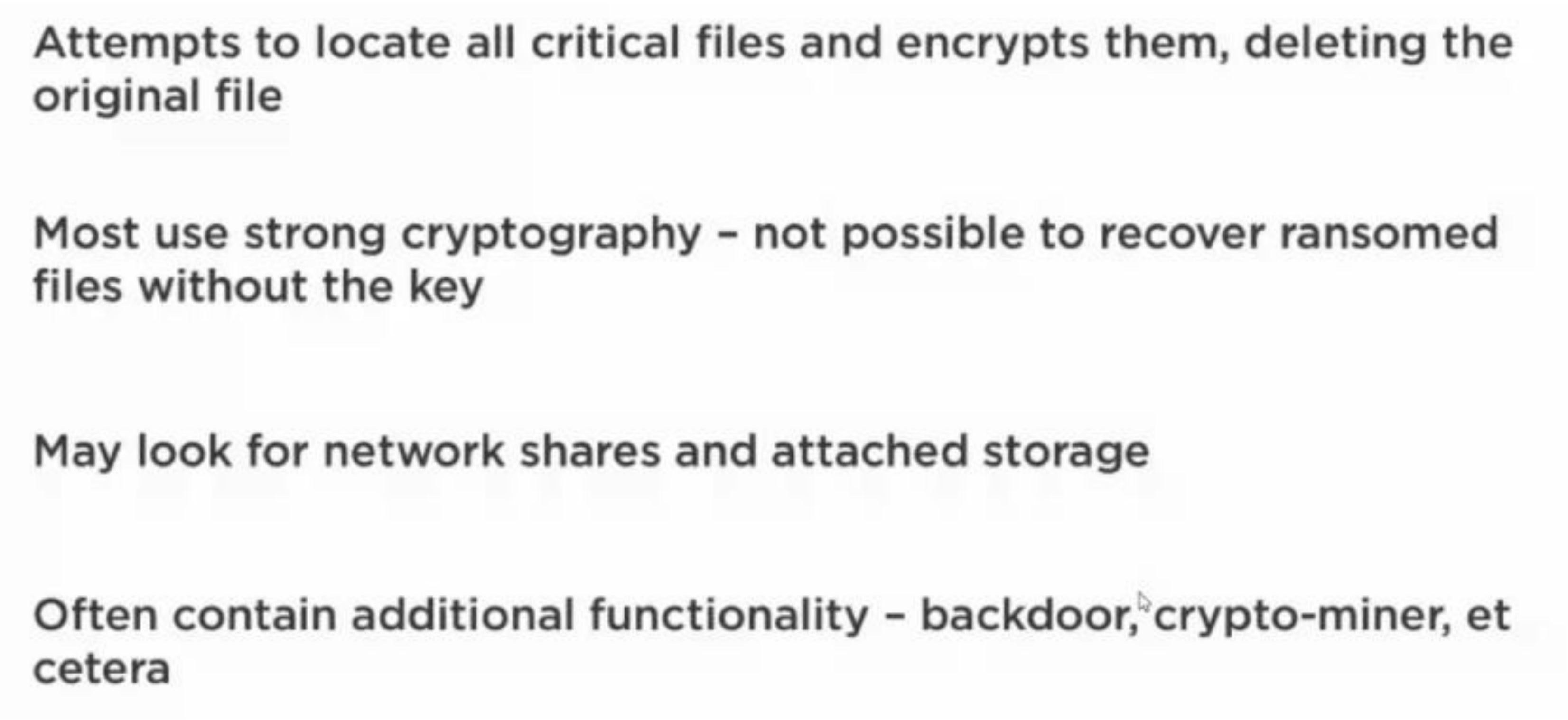
After encrypting the files, it displays a ransom note with instructions of how to pay and recover the files in one of the following ways:

- desktop wallpaper
- website
- pop up message

Typical Stages of a Malware Attack



Features of Ransomware



- Attempts to locate all critical files and encrypts them, deleting the original file
- Most use strong cryptography – not possible to recover ransomed files without the key
- May look for network shares and attached storage
- Often contain additional functionality – backdoor, crypto-miner, et cetera

Instructions for Lab

Download the file PS_DotNet_RealWorld_Ransomware.zip from the Resource section for this lesson.

Use a Virtual Machine. This is real ransomware.

Password to unzip is:

crackinglessons.com

Workflow for Analyzing Ransomware

- Check hash with virustotal
- Check strings
- Dynamic Analysis
- Use dnSpy to reverse engineer
    - Defeat any Anti-Analysis Mechanisms
    - Find Indicators of Compromise (IoCs)

Thank you