CYREN BY DATA443

Understanding Ransomware

What is Ransomware?

ran·som·ware — noun

Ransomware is a type of malicious software (malware) that threatens to publish or blocks access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker. In many cases, the ransom demand comes with a deadline.

1 Criminal sends email with phishing URL or malicious attachment

2 Malicious attachment could contain a phishing URL or a trojan

3 Phishing URL leads to web page designed to steal credentials or drive-by download of a trojan

4 Credentials or trojan malware allow attacker to have remote access to organization's network

5 Attackers access network and navigate the environment, looking for the most impactful systems to hit with ransomware

6 In a double-extortion scam, attackers steal data before encrypting it with ransomware

7 Bitcoin Payment

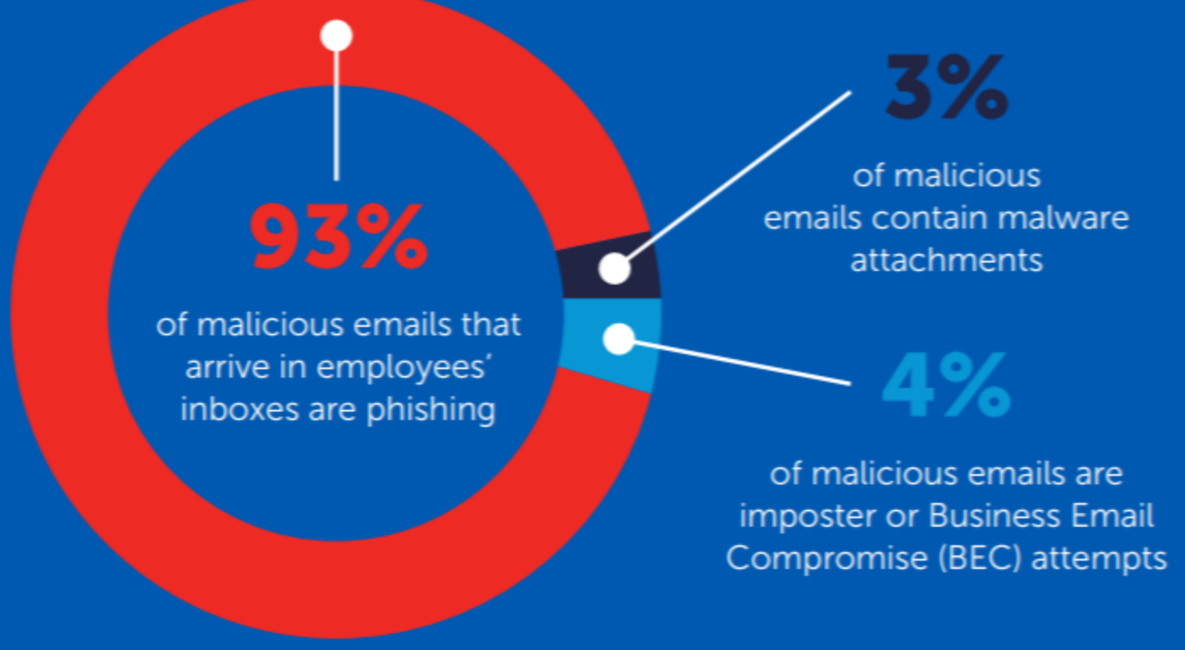
Phishing leads to ransomware

93% of malicious emails that arrive in employees' inboxes are phishing

4% of malicious emails are imposter or Business Email Compromise (BEC) attempts

3% of malicious emails contain malware attachments

— data from July 1-31, 2021
Cyren Incident Response Services



Phishing is evasive. Cyren Inbox Security finds and eliminates phishing before attackers use it to infect your network with ransomware and BEC attacks.

- Simple but powerful add-on for Office 365
- Continuously scan inboxes for threats
- Automatically delete attacks from all mailboxes
- Reduce reliance on users to spot suspicious messages

"...we were also curious what kind of data was the fastest to be compromised, and that turns out to be **Credentials**. This is particularly the case in Phishing, which typically goes after the victim's credentials for use in gaining further access to their chosen victim organization."

— 2021 Verizon Data Breach Investigations Report