

The Evolution of RANSOMWARE

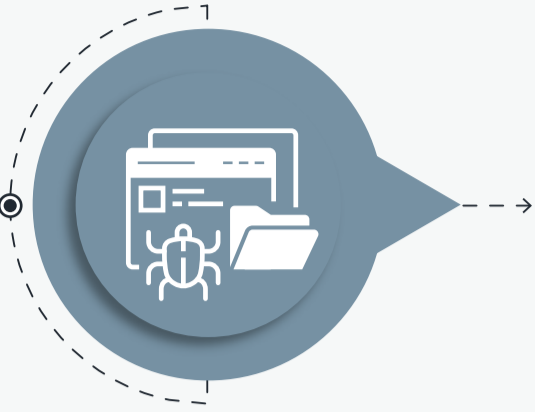
2020

1989



ENCRYPTION

Victims pay to regain access to computer systems after key files get encrypted. This is the original ransomware attack.



DATA THEFT

EXTORTION: Hackers steal and threaten to release sensitive information if a ransom is not paid.



DENIAL OF SERVICE (DOS):

Ransomware gangs launch denial of service attacks that bring down a victim's public websites.

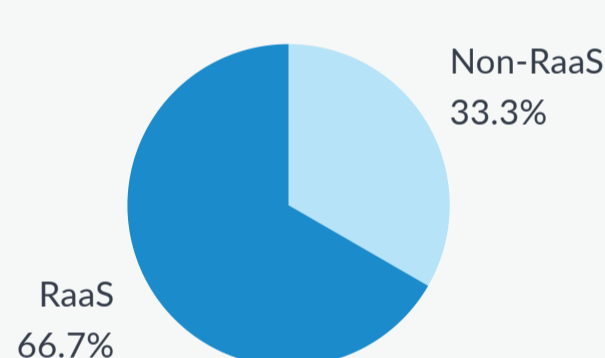
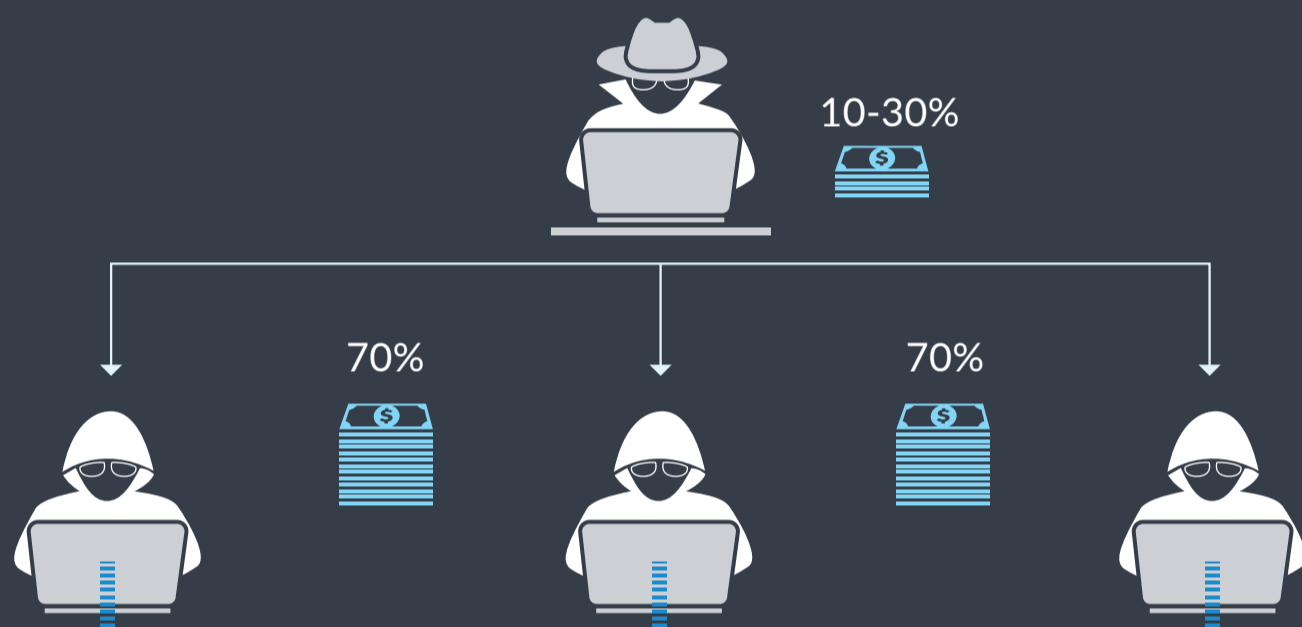


HARASSMENT:

Cybercriminals contact customers, business partners, employees, and media to tell them the organization was hacked.

RANSOMWARE AS A SERVICE (RaaS)

Ransomware as a Service (RaaS) is a lucrative business model where ransomware authors create code and then sell it to other cybercriminals, charging a % of the ransom they reap from using it. This reduces overhead, making ransomware attacks easier and cheaper to conduct.

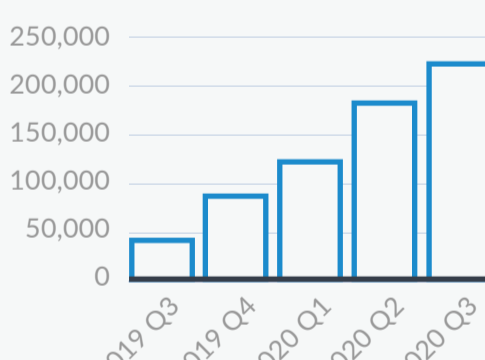


2 OUT OF 3
Ransomware attacks are facilitated by the RaaS setups



CYBERCRIME PAYS

RaaS providers generally take a 20% - 30% cut of the ransom profit generated.



The average ransom payment in Q1 2021 was \$220,298, which was 43% higher than the previous quarter.

ARE YOU PREPARED?

Is your vulnerability management software up to the challenge of today's emerging threats?



EARLY THREAT DETECTION

Can your VM solution quickly and accurately scan vulnerabilities and alert you to security gaps before criminals slip through them?



ACCURATE RESULTS

Does your VM detect threats correlate assets with 99.9% accuracy or are you wading through false alerts?

ALWAYS WATCHING

Do you have continuous monitoring of your entire network that detects anomalous behavior to identify 0-day attacks?

If You Can't Answer Yes to All of the Above
YOU HAVE SECURITY GAPS

To avoid costly, damaging ransomware attacks, you have to think like an attacker. Your best defense is a proactive cybersecurity strategy. You need a vulnerability manager that empowers your team to identify and prioritize weaknesses fast, before they can be exploited. Learn more about [Frontline VM from Digital Defense](#).