paloalto NETWORKS | UNIT 42 BY PALO ALTO NETWORKS

THE GROWING RANSOMWARE THREAT

4 TRENDS AND INSIGHTS

Ransomware attacks can be devastating - regardless of whether a victim decides to pay. Business disruption, reputational harm, time lost while recovering from the incident, and regulatory/compliance ramifications can lead to higher costs and operational harm over the long term.

Palo Alto Networks Unit 42 Security Consulting and Threat Intelligence teams analyzed incident response cases we handled in combination with larger insights on the ransomware threat landscape, such as groups' activity on the Dark Web, to identify patterns and insights that could help organizations bolster their defenses against ransomware.

01 Costs Continue to Rise

As new ransomware groups join the fray, past players re-emerge and existing ransomware operators continue to attack – and push their victims to pay more.

$8.5M
Largest payment we observed in 2021

$2.2 M
Average ransom demand in 2021

144%
Increase since 2020

$541,000
Average ransom payment in 2021

02 Ransomware Groups are More Active than Ever

As new adversaries emerge, established players keep optimizing malware and building out capabilities to affect more types of systems, widening the scope of possible victims in the process.

Conti
Emerged in 2020, Became most active group in 2021

REvil/Sodinokibi
Second most active ransomware group during 2021

BlackCat
Surfaced in 2021. Its leak-site quickly jumped to seventh most active

LockBit
Rebranded as LockBit 2.0, claiming the fastest encryption software on the market

AvosLocker
Launched in June 2021 with slick marketing campaign (blue beetle logo, press releases to recruit affiliates)

Hello Kitty
This rapidly evolving group added a version of its malware that targets Linux computers in 2021

03 Evolving Tactics, Techniques and Procedures (TTPs)

Cybercriminals are constantly updating their tools and attack methods, while finding ways to optimize their business models to maximize profits.

Increased use of Zero-Day Vulnerabilities
helps threat actors take victims by surprise

Adoption of prolific ransomware as a service (RaaS) business model
lowers the technical bar for attacks and opens the door to more cybercriminals

Multiple Extortion Techniques
pressure victims to pay more and faster

35 NEW GROUPS
emerged using a double extortion model where victims' names are posted on Dark Web leak sites

2,566 VICTIMS
had names and proof of compromise publicly posted on ransomware leak sites

42 VULNERABILITIES
observed in 2021 across different technologies being used by ransomware operators

04 A Significant Global Problem

No region or industry is immune to ransomware attacks, and at least one victim from 90 different countries appeared on ransomware group's leak sites in 2021.

60% of ransomware victims located in the Americas

31% of ransomware victims in EMEA

9% JAPAC

How to Increase Your Ransomware Resilience

As ransomware threats grow and evolve, and groups continue to hone their tactics, it's more important than ever to bolster your defenses and improve your ransomware resilience. Unit 42 recommends the following steps:

1. Stay up-to-date on the evolving landscape
2. Understand the business impact of losing critical data
3. Assess your internal and external readiness
4. Review and test your incident response plan
5. Implement Zero Trust approach to secure your organization
6. Identify and shut down access to your exposed assets
7. Prevent known and unknown threats
8. Automate where possible
9. Secure cloud workloads
10. Reduce response time with incident response retainers

Get the 2022 Unit 42 Ransomware Threat Report for a deeper dive of the ransomware threat landscape, and gain actionable insights from security experts to help address your ransomware vulnerability.

Download the report

paloalto NETWORKS

© 2022 Palo Alto Networks, Inc. | All Rights Reserved.