Defending Against Ransomware

Beyond a Step-by-Step Blueprint

Javier Perez

veeam

Agenda

Introduction

Ransomware Trends Report

Ransomware Incident Response

Recommendations

Nice to Meet You

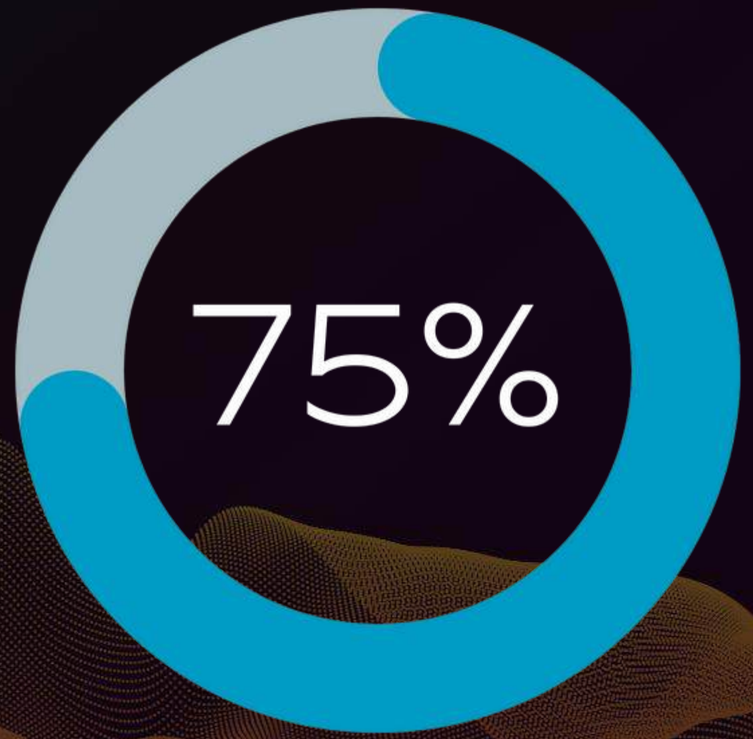
Javier Perez

Sr. Director of Product Marketing and Evangelism at Veeam Software

javierperez.mozello.com

www.linkedin.com/in/javierperez

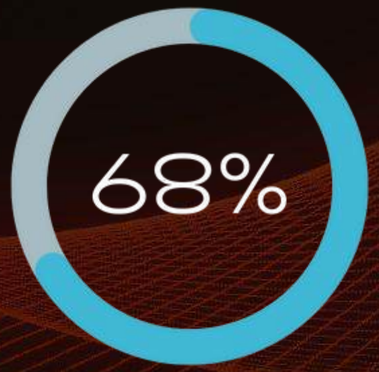
The Era of Cyberattacks



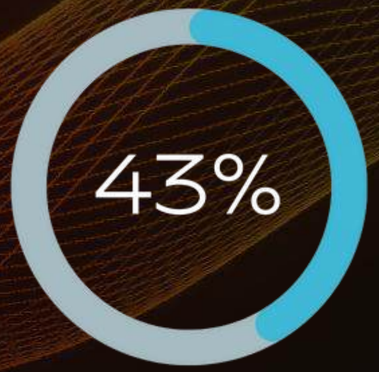
75% of organizations suffered at least one ransomware attack in 2023, most report getting hit more than once

The Ransomware Trends Report

of ransomware attacks targeted backup respositories



of financial impact is beyond the ransom payment



of affected data won’t be recovered

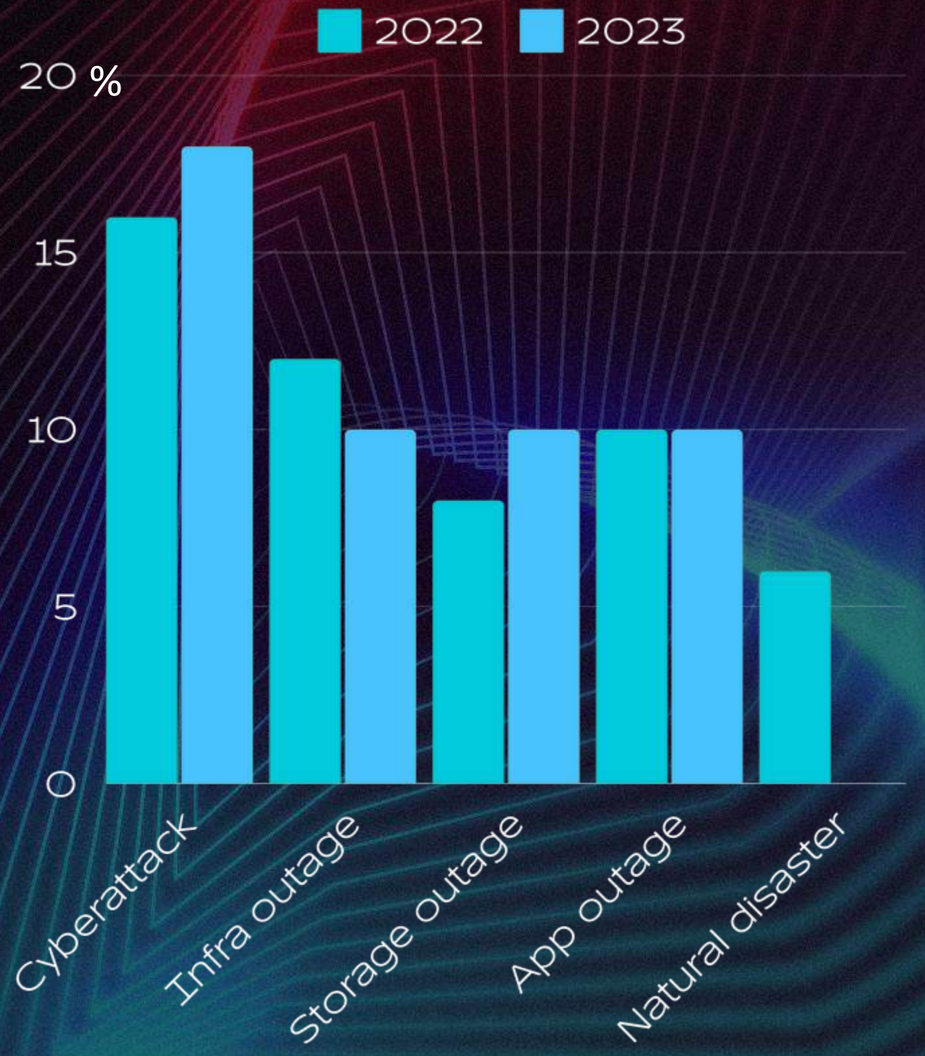
of organizations paid the ransom but couldn’t recover

veeam

Most Common and Most Impactful

Fourth Year

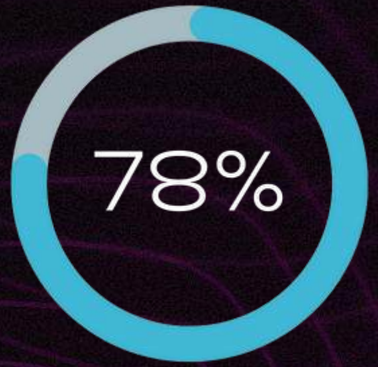
in a row cyberattacks were the most common & most impactful cause of outage



Cyber Extortion

Encrypting & Exfiltrating Data

Growing cases of exfiltration and double extortion



of cyber attacks involved confirmed exfiltration

of cyber attacks involved encryption

Source: Q2 20024 Coveware Quarterly TTP Report

veeam

Assistance and Documentation

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

National Cyber Security Centre

- Australian Cyber Security Centre
- Canadian Centre for Cyber Security
- Germany’s Federal Office for Information Security
- Netherlands’ National Cyber Security Centre
- New Zealand’s National Cyber Security Centre
- Korea Internet & Security Agency
- Israel’s National Cyber Directorate
- Japan’s National Center of Incident Readiness and Strategy for Cybersecurity
- Cyber Security Agency of Singapore

Plenty of Blue-Prints

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE National Cybersecurity Center of Excellence

HKCERT Hong Kong Computer Emergency Response Team Coordination Centre 香港電腦保安事故協調中心

- Mobilize response team (forensics, legal, insurance, etc.)
- Network segmentation, containment
- Work with forensics expert
- Restore backup or preserved data
- Notify law enforcement
- Notify affected parties

- Avoid paying ransom
- Isolate/disconnect infected systems
- Use trusted decryption tools
- Use cleanup tools to remove ransom
- Restore backups
- Deploy intrusion detection tools
- Report the incident to HKCERT

Recognize Ransomware

- Lost access to systems
- Can’t open files
- Files with a different extension
- Screen blocking access
- Ransom note

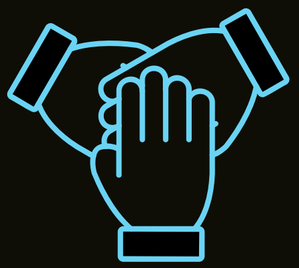
Incident Response: Stay Calm

Alert Security/Incident Response Team

- Contact Cyber Insurance (if you have it)
- Contact your Legal team
- Contact third-party IR teams

Collect artifacts

- Ransom note, sample encrypted files, malware



Incident Response: Stay Calm

Focus and Containment

- Identify affected systems and data
- Change Admin passwords
- Isolate endpoints
- Understand how much time do you have (RTO, RPO)
- Communicate internally
- Look at your insurance policy

Incident Response: Assessment

Identify Encryption

- Extensions, can you decrypt?
- Identify which data is important, and which one can be lost

Find you backups

- Are your backups encrypted?
- Can you recover from clean backups?

Expert's Assistance

- Identify encryption, threat actor group
- Forecast recoverable data

Incident Response: Engage

Respond to Threat Actor

- Are they still in your network?
- Proof of Exfiltration
- Information about breach
- Decryption verification

Negotiate

- You don’t have to pay
- Reduce scope and reduce price

Incident Response: Negotiate

- Assume that any communication will become public
- Professional negotiation, respectful and unemotional
- Bring an expert negotiator
- There’s no way to enforce terms of negotiation
- Paying ransom does not guarantee delivery of keys or deletion of exfiltrated data
- Payments to threat actors in certain countries could be illegal

Incident Response: Recovery

Prioritize applications to recover

Restore from Backup

- Available backups
- Clean backups
- Time to recover
- Cost of recovery

Rebuild Systems and Data

- Capability to rebuild
- Time to rebuild
- Cost to rebuild
- Risks of rebuild

Document prioritization and where to recover to

Incident Response: Decision

Impact Assessment

- Life and Safety Impact
- Operational Impact
- Financial Impact
- Sales Impact
- Reputation Impact
- Consider Length of Time

Incident Response: Decision

If you are going to pay

- The network is contained and secure, resetted passwords
- Malicious software is removed from impacted systems
- Backup recovery options exhausted
- Rebuild options exhausted
- Law enforcement notified
- Regulators notified

Expert Incident Response

Rapid Assessment

- Scan affected systems
- Collection of forensic data
- Inventory of systems affected

Forecast Outcome

- Forensic triage
- Identify corrupted files
- Identify non-encrypted files
- Ransomware family verification
- Compare against previous cases

Analysis

- Identify TTPs (MITRE ATT&CK)
- Timeline, dwell time, compromise, and attack
- Recommendations and negotiation strategy

veeam

Final Actions

- Document Lessons Learned
- Updated response plans and procedures for future events
- Consider sharing lessons learned and IOCs with Cyber Security Organizations

Thank You!

Javier Perez

Sr. Director of Product Marketing and Evangelism at Veeam Software

javierperez.mozello.com

www.linkedin.com/in/javierperez