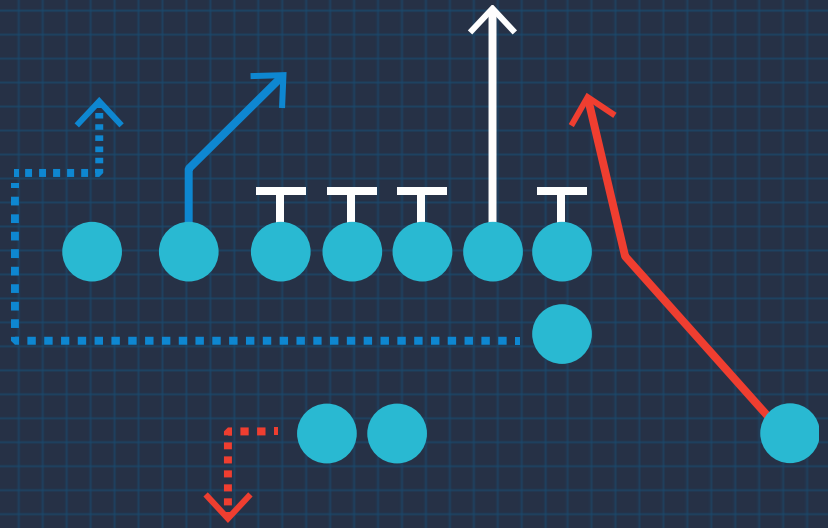
RANSOMWARE PROTECTION

SALES PLAYBOOK



Barracuda

Ransomware Trends

- Ransomware continued its upward trend with an almost 13% increase–a *rise as big as the last five years combined* (2022 DBIR)
- Allianz, a leading multi-national financial services company with 86 million customers, ranked cyber-incidents as the *#1 business threat* for 2022.
- According to Coveware, *82% of all ransomware attacks* are targeted at small business

Top actions and data varieties in breaches

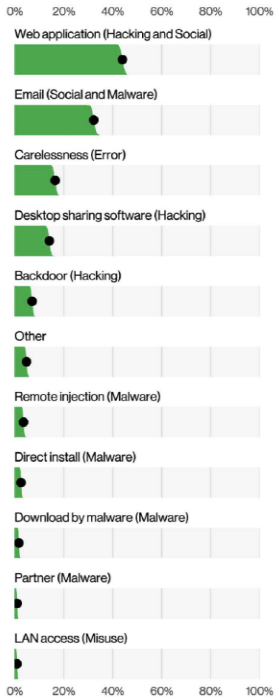


Figure 18. Top Action vectors in breaches (n=3,279)

Top actions in breaches are hacking and social engineering attacks.

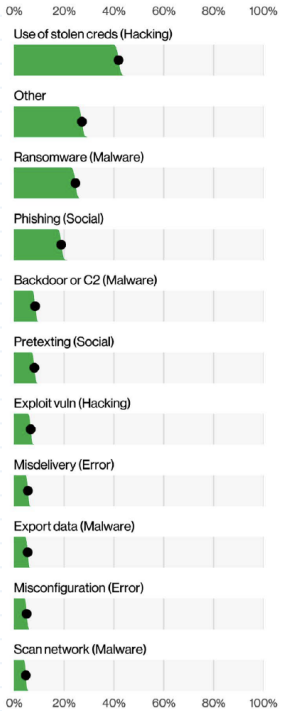


Figure 19. Top Action varieties in breaches (n=3,875)

Top data target in breaches is credentials.

Source: Verizon, 2022 Data Breach Investigation Report

Top actors and motives in breaches

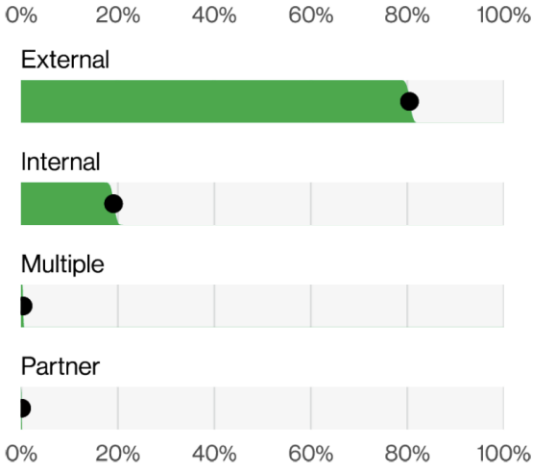
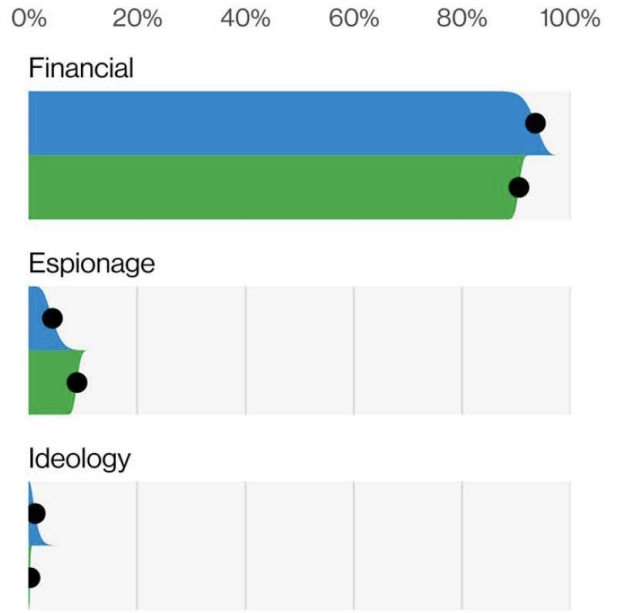


Figure 11. Actors in breaches (n=5,146)



Source: Verizon, 2022 Data Breach Investigation Report

Anatomy of a ransomware attack

Ransomware Protection Checklist

1. Protect your email.

Ransomware attacks often start with a phishing email to capture admin or user credentials.

1a	**Block phishing attacks** Attackers use social engineering tactics to bypass traditional email security. Use an email security solution that includes AI-enabled phishing and account takeover protection, as well as alerts when malicious activities are detected.	
1b	**Train users** Your users are your last line of defense against phishing attacks. Training needs to be an ongoing effort, as attacks often become more sophisticated over time.	
1c	**Implement remediation** Email attacks that evade email security and land in users' inboxes need to be addressed quickly. Choose an email security solution that enables proactive threat discovery and automates remediation.	

Email Protection

Use Case	Discovery questions	Solution pitch
Attackers use phishing to obtain user and admin credentials	• Have you been hit with targeted phishing attack or an account takeover? • Do you have sufficient account takeover protection in place? • Does your current email protection solution include AI-enabled phishing and account takeover protection?	**Barracuda Email Protection** multi-layered approach combines a secure email gateway, AI-powered fraud protection, advanced security awareness training and automated incident response. This results in comprehensive protection against all email threats from spam and malware to business email compromise and account takeover.
Attackers are using social engineering techniques to trick users into disclosing login credentials	• How are you currently training your employees to recognize and prevent phishing • and other social engineering attacks? • Do you have a security awareness training program in place? • How do you measure awareness improvement throughout your user population? • How do you keep security top of mind for all of your users?	**Barracuda Security Awareness Training** is an email security awareness and phishing simulation solution designed to protect your organization against targeted phishing attacks. Security Awareness Training trains employees to understand the latest social engineering phishing techniques, recognize subtle phishing clues, and prevent email fraud, data loss, and brand damage.
Threats are landing in user inboxes	• How do you discover threats in your users' email inboxes? • Does your current email security system adequately alert you when malicious activities are detected? • How long does it take you to respond and remove threats post-delivery?	**Barracuda Incident Response** automates incident response and provides remediation options to address issues faster and more efficiently. Admins can identify all impacted users and remove malicious email directly from their inboxes. Discovery and threat hunting tools help to identify post-delivery threats and initiate response.

Ransomware Protection Checklist

2. Secure your applications.

Attackers hack your web applications to gain access to your data.

2a	**Protect web applications** Applications often have open vulnerabilities that can be exploited to gain access to your data. Use an application security solution that defends against web application vulnerabilities such as OWASP Top 10, zero-day and brute force attacks.	☐
2b	**Protect access to applications** For internal applications, you should only allow access for authorized users and devices. Choose a zero trust access solution that enables role based access, multi-factor authentication and continuous verification of user and device identity.	☐
2c	**Prevent lateral movement on your network** If attackers gain access to your network, they often attempt to move laterally to find and infect data sources. You need a network firewall that protects both your on-prem and cloud networks with network segmentation and advanced security services.	☐

Application/ Access Protection

Use Case	Discovery questions	Solution pitch
• Attackers use open web application vulnerabilities to gain access to data or network • Attackers use brute force and credential stuffing attacks to gain access to data or network • Attackers use your web applications to spread ransomware to others	• How secure is your site? When was it last updated? • Do you have forms on your site? How do you prevent attacks through the forms? • Do you accept file uploads on your website? How do you secure against malware?	**Barracuda Cloud Application Protection** is a powerful, easy-to-use platform that protects applications everywhere. Capabilities include web application firewall, advanced bot protection, API protection and much more. • WAF-as-a-Service deploys in minutes to protect from web app vulnerabilities • Advanced bot protection stops brute force and credential stuffing attacks
• Attackers exploit stolen credentials to gain access to corporate applications and workloads	• Do your remote or contract workers use unmanaged or BYOD devices? • Do you have visibility into all the users and devices on the network? • Do you have visibility and an audit trail for who is access what when?	**Barracuda CloudGen Access** is a Zero Trust Access solution that continuously verifies that only the right person, with the right device, and the right permissions can access company resources. • Provides secure access to applications and workloads from any device and location
• If attackers manage to gain access to your network, they (or their malware) may move laterally to find data or other apps	• Is your corporate network divided into separate protected segments? • Do you have multi-factor authentication enabled for network access?	**Barracuda CloudGen Firewall** provides multi-layered security that blocks advanced threats, including zero-day attacks. It includes intrusion prevention and sandboxing. • Powerful network segmentation prevents lateral movement on the network.

Ransomware Protection Checklist

3. Back up your data.

Attackers encrypt your data and demand ransom.

3a	**Back up your data** You need to back up all of your data. Remember your on-prem data as well as data in the cloud/SaaS applications such as Office 365.	☐
3b	**Protect access to applications** Attackers often target your backups to prevent you from being able to recover your data. Encryption, access control, and IP restrictions are all important here. You want to make sure that accessing your data is easy for you, but difficult for attackers.	☐
3c	**Develop a recovery plan** If you are under attack, you need to be able to quickly deal with the attack, recover your data and avoid paying ransom. Consider not only your technical response, but also your business response. Test your plan in full before there is a problem. Forensics can be helpful in the aftermath of an attack to find vulnerabilities.	☐

Backup

Use Case	Discovery questions	Solution pitch
• If attackers are able to get through your defenses and encrypt your data, you need to be able to recover your data from backup to avoid paying ransom.	• Do you back up all your data? • How are you backing up your Microsoft 365 data?	Barracuda **Cloud-to-Cloud Backup (CCB)** is an easy-to-use SaaS solution that provides comprehensive, cost-effective, scalable backup and recovery for all your Microsoft 365 data, including Exchange Online, SharePoint, OneDrive, OneNote, and Teams.
• Even if you back up your data, attackers often target your backups to prevent you from being able to recover.	• How do you protect your backup admin credentials? • Do you have multi-factor authentication enabled for your backup admin access? • Is your backup easily accessible and identifiable on your network? • Are your backup stores encrypted in transit and at rest? • Do you have granular admin roles to restrict backup actions?	Protecting access to your backup data is crucial if you want to protect your data and recover after a ransomware attack. Choose backup solutions such as Barracuda Backup **(BBS)** and **Cloud-to-Cloud Backup (CCB)** to make sure that the backup and the access to the backup is secure.
• If you find yourself under a ransomware attack, you need to implement a recovery plan to avoid paying ransom and to get back to business quickly.	• Do you have a ransomware recovery plan developed? • Does you plan include both technical response and business response? • Have you tested your plan?	Choose a vendor like Barracuda to build a layered defense approach so that email and credentials are protected, web applications and access are secure and that your backups are defended. Consider using a managed service provider where appropriate

Resources

- ransomware webpage
  - https://www.barracuda.com/ransomware

- videos
- https://share.vidyard.com/watch/f17HWVAGChXkkS8PFH2gbS
- https://share.vidyard.com/watch/jms2Vqs7ojXBCEGtoSc6Xd

- blog posts
  - https://blog.barracuda.com/tag/ransomware/

- ransomware protection configuration tool and checklist
  - https://www.barracuda.com/ransomware/configurator
  - https://assets.barracuda.com/assets/docs/dms/checklist_ransomware.pdf