

# RANSOMWARE

AFFECTS MOST ORGANIZATIONS

## TOP SECURITY PRIORITIES



## MISPLACED OPTIMISM

# 79%

of respondents are confident in their capabilities to prevent a ransomware attack in the next 12 months...

...but there's misalignment between defense priorities and evolving attack methods – which have shifted away from breached credentials to malware-stolen cookies that enable session hijacking

## RANKED PRIORITIES FROM RESPONDENTS DON'T ALIGN WITH ATTACK METHODS

**10TH ON THE LIST OF COUNTERMEASURES:**  
Monitoring for compromised web session cookies & tokens

**PERCEIVED LOWEST RISK ENTRYPOINT:**  
Stolen cookies

**LEAST PRIORITIZED AUTHENTICATION PRACTICES:**  
Automating workflows to remediate exposed passwords and cookies



**SURVEY SAYS!**  
Look deeper at your malware problem

# 81%

OF SURVEYED ORGANIZATIONS AFFECTED AT LEAST ONCE IN THE PAST 12 MONTHS



# NEARLY ONE-THIRD

of North American and European ransomware victim companies had an infostealer infection prior



# BUT JUST 19%

of organizations are prioritizing improved visibility and remediation of exposed credentials and malware-exfiltrated data...

...LEAVING THE DOOR WIDE OPEN FOR FOLLOW-ON ATTACKS

## RANSOMWARE IS A MALWARE PROBLEM AT ITS CORE

which means that preventing ransomware attacks must start with proper and robust **malware remediation**.

..... [DOWNLOAD THE FULL REPORT](#) ▶▶▶