Acronis

Cyberthreat Landscape 2024:

The Middle East and Around the World

Kevin Reed

CISO
Acronis

#CyberFit

Acronis

29.1%

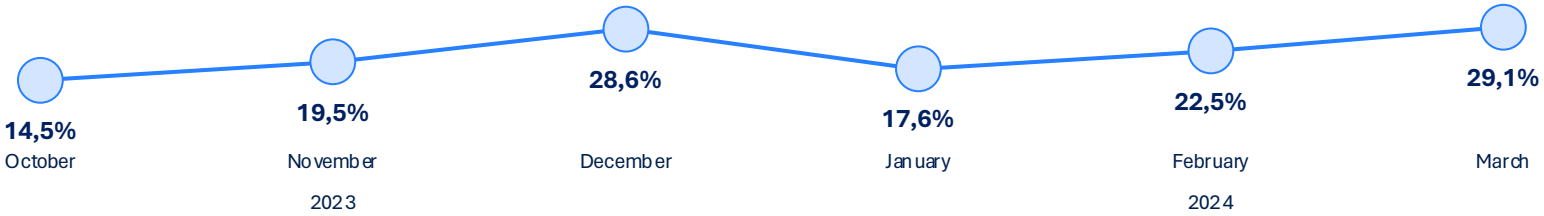
Malware detection rate, March 2024

Source: Acronis Cyber Protection Operation Center

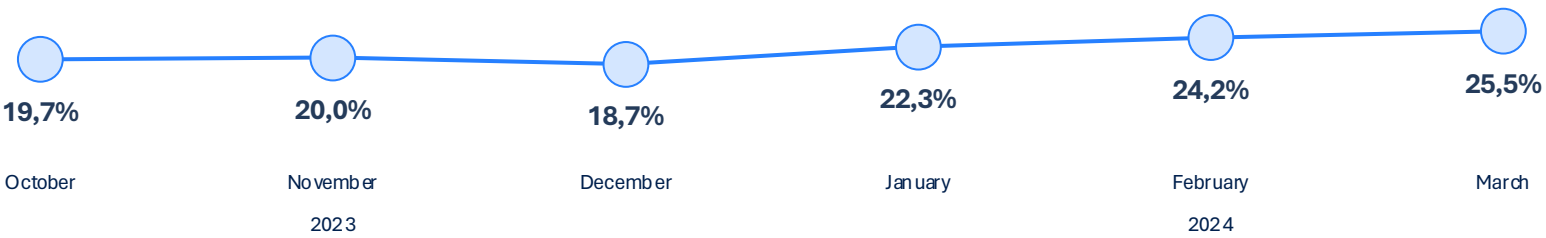
#CyberFit

Both malware and URL detection rate are growing

Malware detections



URL detections



Source: Acronis CPOC

Attack lifecycle

From the initial reconnaissance to deploying ransomware and data exfiltration

Attack lifecycle

Parsing LinkedIn, scanning IP addresses, open ports,
Web applications, doing DNS reconnaissance,
harvesting passwords dumps, gathering news…

Attack lifecycle

Attack Example

- Seven Seas is a global maritime services group that specializes in providing general ship supplies, stores, provisions, and leading technical maritime brands through its extensive global network.
- Profile:
  - 350 employees
  - Founded in 1996

SevenSeas

External reconnaissance → **Initial compromise** → Establishing persistence → Internal reconnaissance → Privilege escalation → Acting on objectives

Phishing attacks, public application exploitation, login with **valid leaked credentials**, AI-assisted social engineering

Attack lifecycle

Deploying remote access applications, purpose-built or off-the-shelf, repurposing legitimate remote access tools for persistence

Attack Example

- Saudia MRO MENA's leading provider of aviation services, specializes in end-to-end aircraft maintenance, repair, and overhaul solutions.
- Profile
  - 3100 employees
  - Founded in 1959

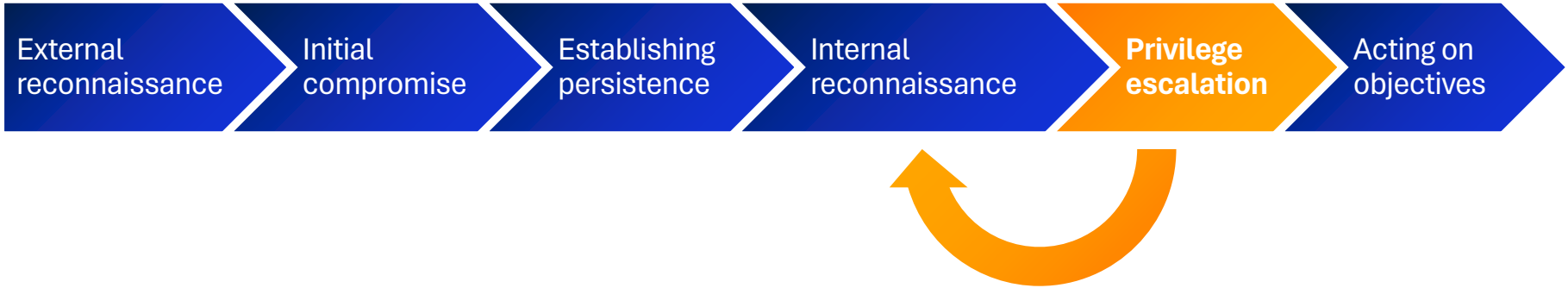
Saudia Technic

Attack lifecycle

Scanning internal assets, applications, harvesting credentials from local systems and networks shares, reviewing network diagrams and IT documentation

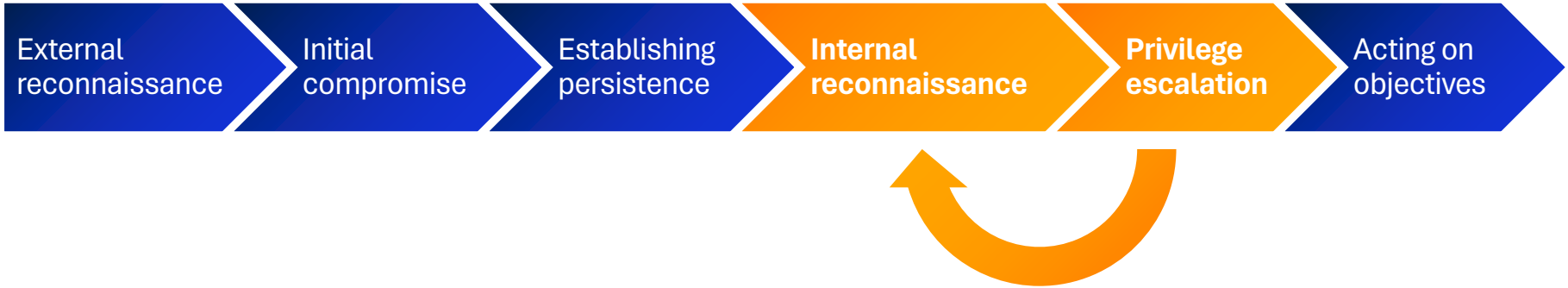
Attack lifecycle

Exploit internal applications to elevate privileges or reuse harvested admin credentials; monitor network traffic and sniff for weak authentication



Attack lifecycle

Exploit internal applications to elevate privileges or reuse harvested admin credentials; monitor network traffic and sniff for weak authentication



Al Firas falls victim of the LockBit group

Example Victim

- Al Firas an UAE construction company. Specializing in high-rise commercial and residential buildings, schools and universities and more, they have been a principal participant in the UAE building boom.
- Profile:
  - 57.3 M USD revenue
  - 250 employees
  - Founded in 1988

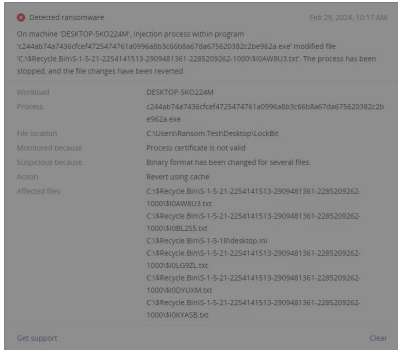
Threat vector and impact

- Attacked by: LockBit 3.0
- Timing: Attack likely December 2023 … confirmed on February 9, 2024.
- Impact: 2 TB of data exfiltrated.
- The ransomware request amount was not disclosed … no information if it was paid.

How Acronis protects

- **Active Protection** inside core Acronis Cyber Protect detects and blocks LockBit ransomware heuristically.
- Product needed: Acronis Cyber Protect.

Detection Screenshot



CPOC Statistics

*Malware detections:

29.1%

*Malicious URL was accessed:

25.5%

*normalized numbers, per unique machines in March 2024

Attack lifecycle

Exfiltrate data, encrypt files, deface the web site, wipe configuration, brick the hardware, collect credentials for future attacks, jump over to partner networks

Acronis

How technology can help solve a human problem.

#CyberFit

Defense lifecycle

From the initial compromise to deploying ransomware and data exfiltration

Defense lifecycle

Phishing protection: modern **AI-based anti-spam and anti-phishing** systems rank at 99.9% accuracy which may exceed the accuracy of a human being.

Vulnerability management: **risk-free updates** with pre-update automated backup.

Defense lifecycle

AI-powered **antimalware** solutions prevent establishing the initial foothold.

Defense lifecycle

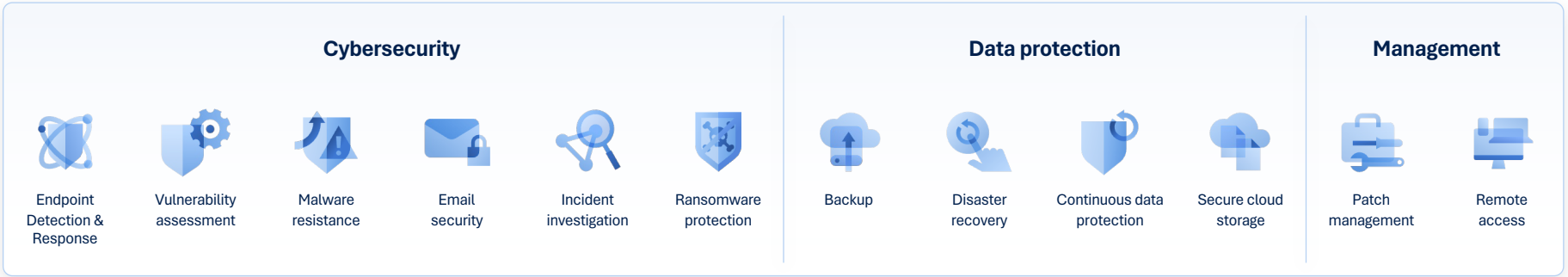
Endpoint detection and response (EDR) with automatic or managed remediation acting upon lateral movement detection. Compromised endpoint isolation and cloud-assisted forensics.

Defense lifecycle

Recovery from the recent local or off-site **backup** or activating cloud-based **disaster recovery** plan while performing **forensics analysis**

Natively integrated, higher efficient security built for MSPs and IT departments

Natively integrated, highly efficient security, data protection and management in a single solution



Ease of use

Single agent, single console and single policy for all services, and a single dashboard for monitoring

Operational efficiency

Mass management in multitenant environments designed for distributed, diverse customer infrastructure

Integration platform

Extensible and customizable platform to integrate all IT tools into single technology stack

Acronis

76%

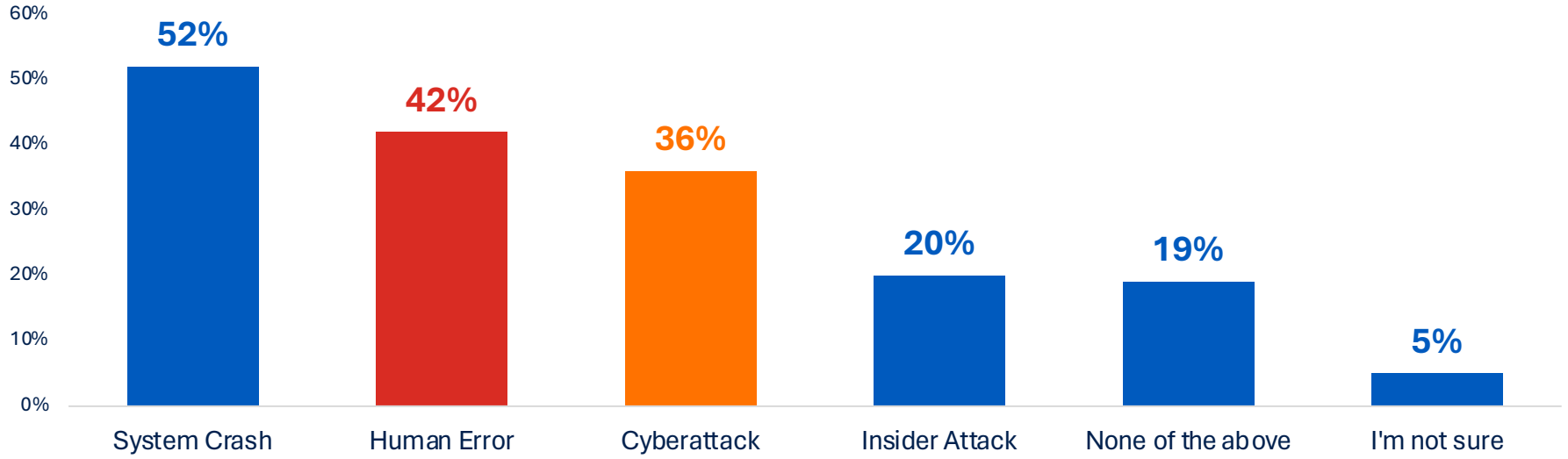
Has your organization experienced downtime?

Source: Acronis Cyber Protection Week Global Report 2022

#CyberFit

76% of companies experienced downtime

Has your organization experienced downtime due to any of the following in the past year?



Source: Acronis Cyber Protection Week Global Report 2022

Acronis

#CyberFit

Thank you!