Active Adversary Behaviors 2023

Insights into the latest attacker behaviors based on attacks remediated by Sophos Incident Responders

Álvaro Fernández
Director Comercial Sophos
Alvaro.fernadez@sophos.com

SOPHOS

Who Is the Sophos X-Ops Incident Response Team?

Who

Core Team

50 Digital Forensic Specialists
35 Deployment Engineers

Backed by:

150+ MDR SOC Analysts
400 Malware Analysts in SophosLabs

What

Immediate Response

Quickly triage, contain, and neutralize active threats

Threat Removal

Eject adversaries from your estate to prevent further damage

Analysis of 232 Incident Response Cases

2022 – 1H 2023

2022

152 incident response cases

81% from sub-1000 organizations

22 sectors represented

35 nations represented

1H 2023

80 incident response cases

88% from sub-1000 organizations

25 sectors represented

34 nations represented

Who Are Active Adversaries?

Who

Active adversaries are highly skilled cybercriminals, often equipped with sophisticated software and networking skills.

How

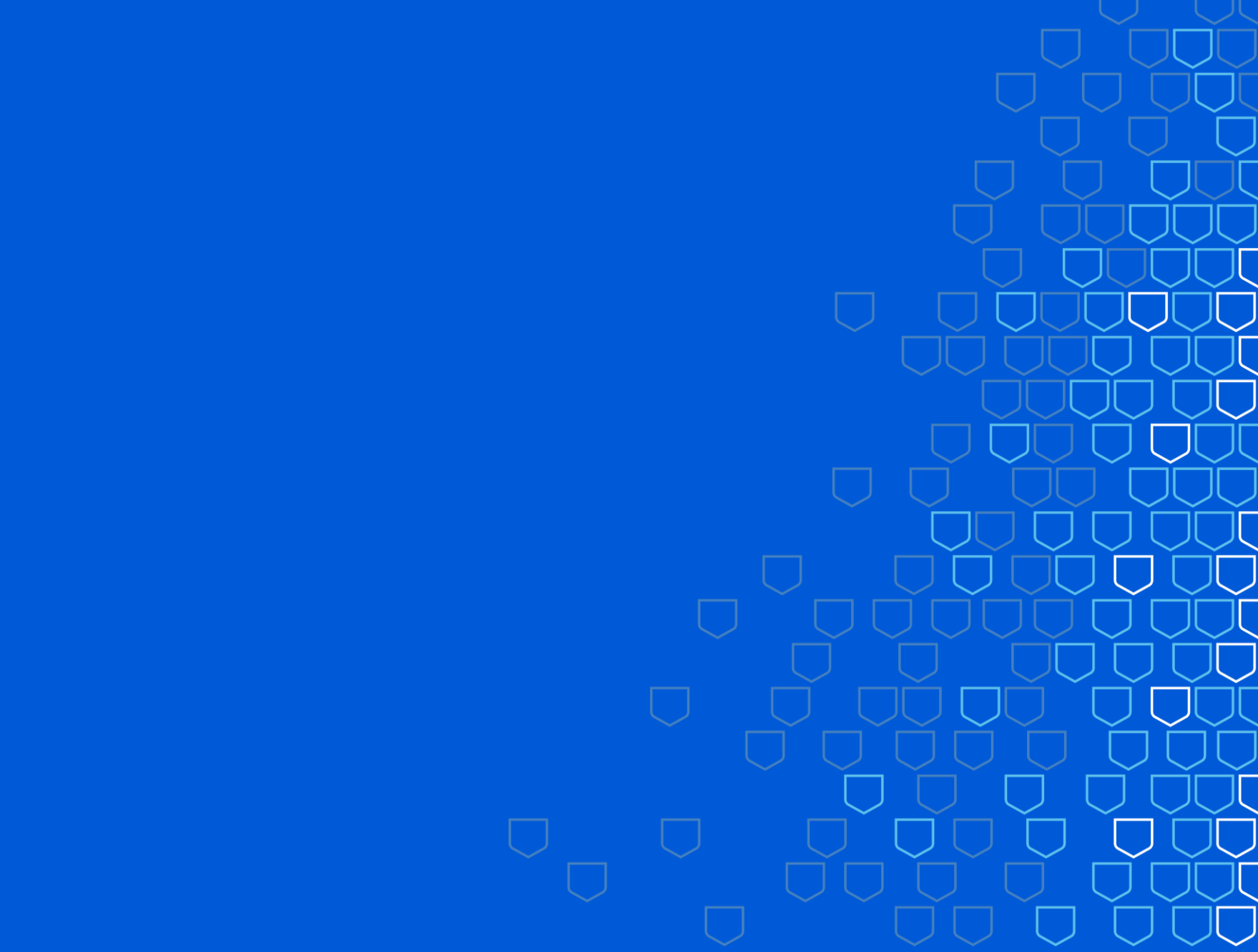
They gain entry, evade detection and **continuously adapt their techniques**, using hands-on keyboard and AI-assisted methods to circumvent preventative security controls and execute their attack.

Prevalence

23% of organizations have experienced an attack involving an Active Adversary in the last year.

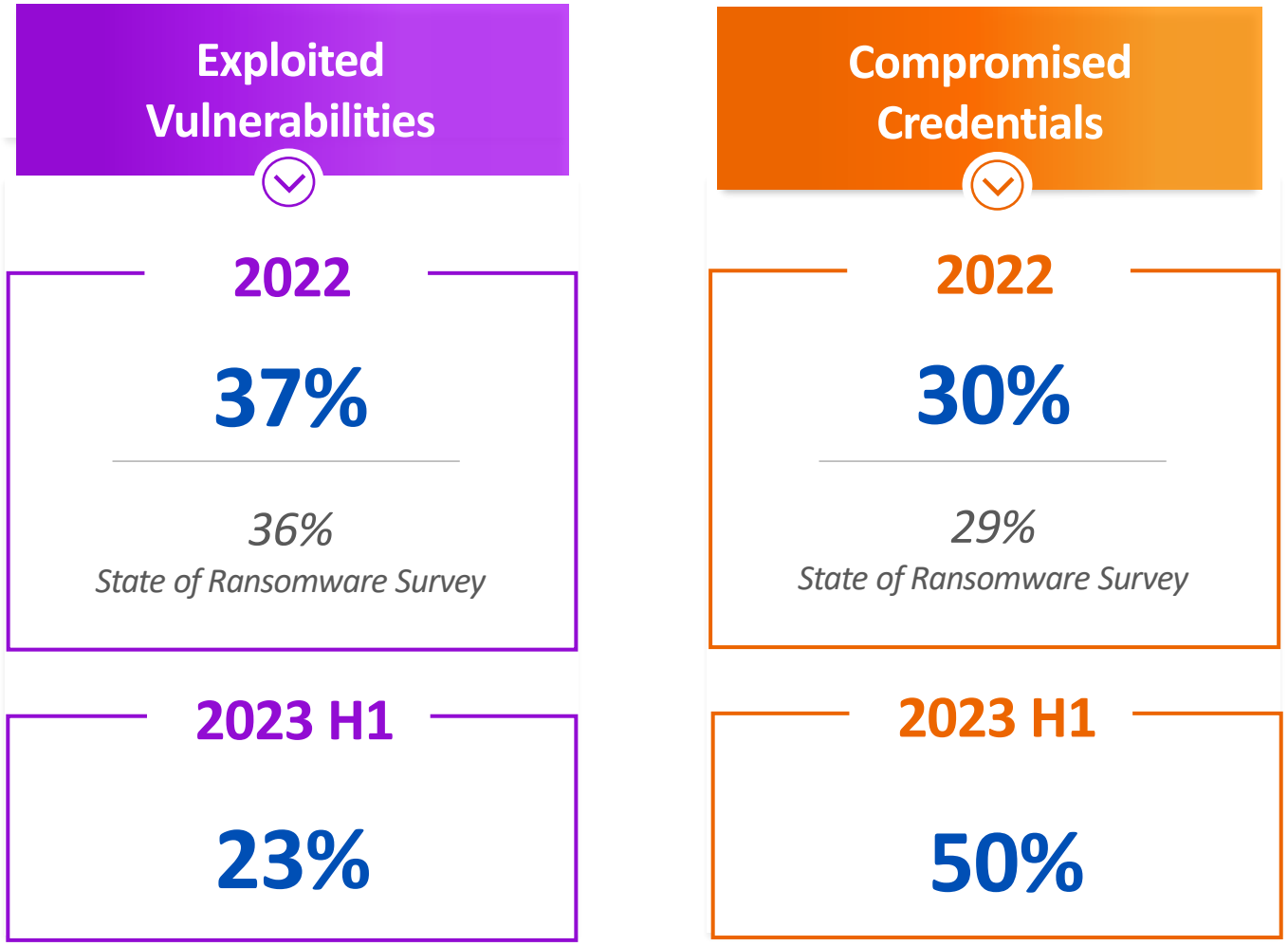
Source: The State of Cybersecurity 2023, Sophos. Survey of 3,000 IT leaders across 14 countries

Getting In



SOPHOS

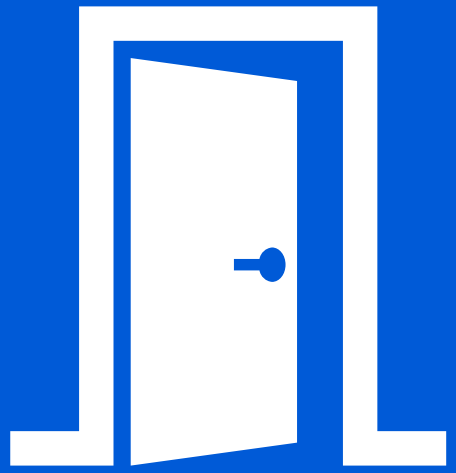
Evolving Attack Vectors



Source: The State of Ransomware 2023, Sophos (n=1,974 organizations hit by ransomware in the last year); Active Adversary Report for Business Leaders, 2023, Sophos (n=152); Active Adversary Report for Tech Leaders, 2023, Sophos (n=80)

SOPHOS

Lack of MFA leaves the door open to adversaries



39%

Of incidents we remediated in the first half of 2023 did not have multi-factor authentication (MFA) configured.

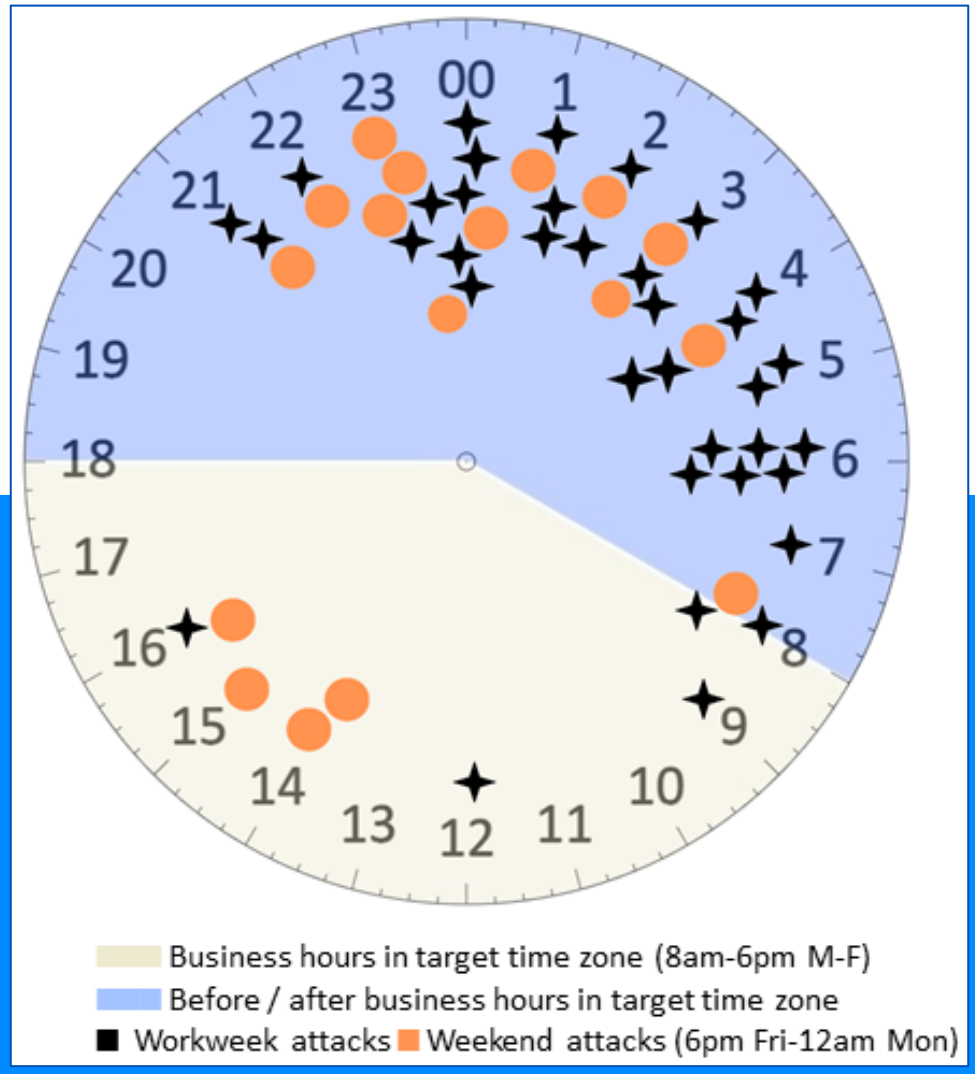
Source: Active Adversary Report for Tech Leaders, 2023, Sophos (n=80)

SOPHOS

Attackers Target Off-Hours

91% of ransomware attacks start outside standard work hours

9 in 10 attacks occur outside 8am to 6pm on a weekday.

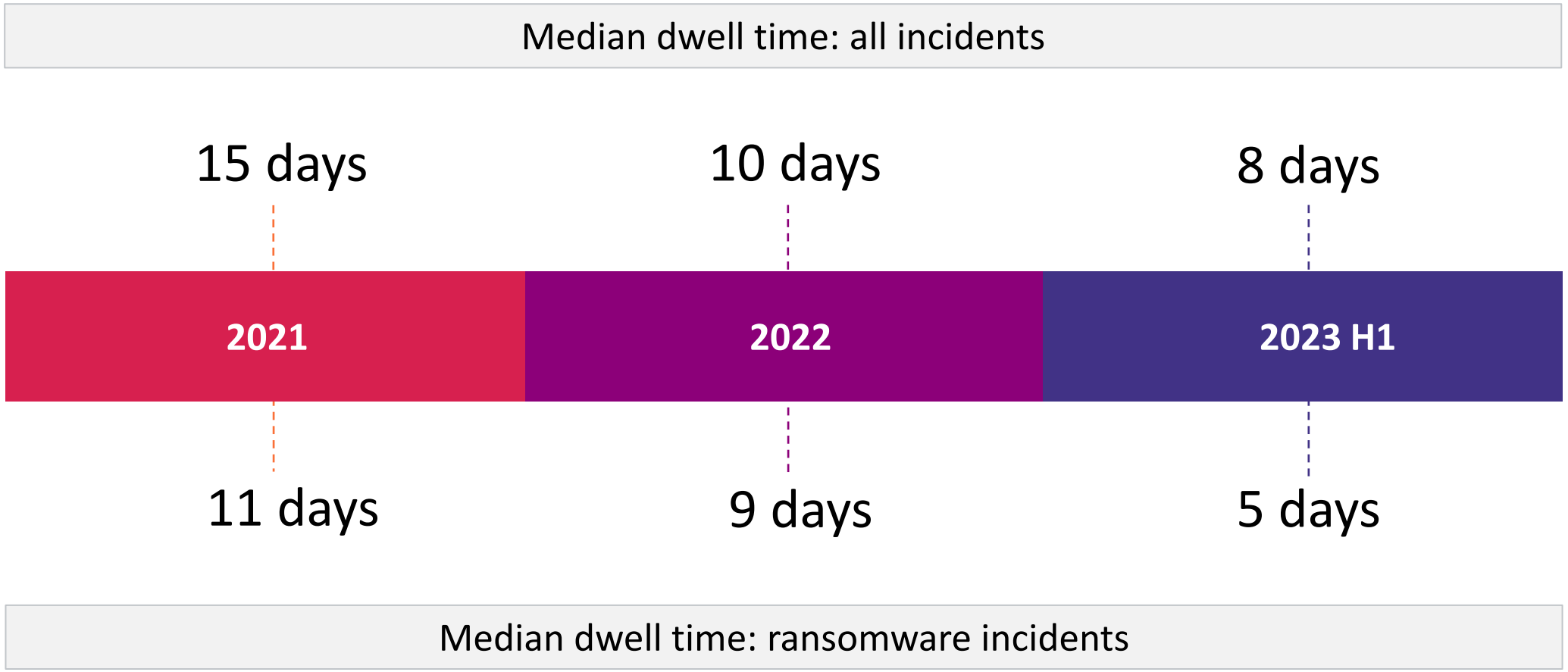


Source: Active Adversary Report for Tech Leaders, 2023, Sophos (n=52)

SOPHOS

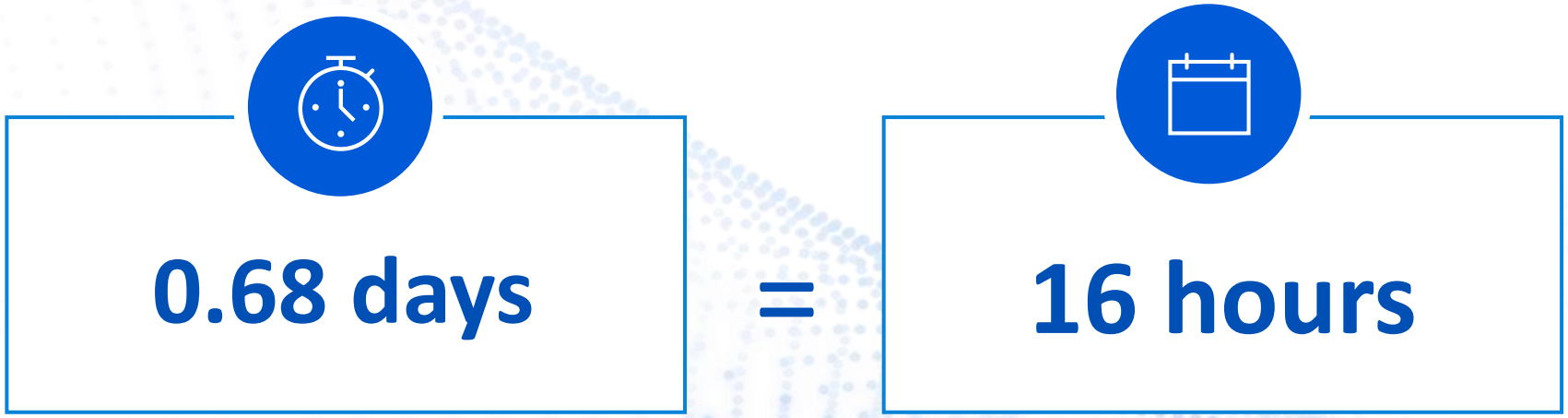
Once Inside …

Adversaries Are Speeding Up



Source: Active Adversary Playbook 2022, Sophos (n=144); Active Adversary Report for Business Leaders, 2023, Sophos (n=152); Active Adversary Report for Tech Leaders, 2023, Sophos (n=80)

The Race to Active Directory

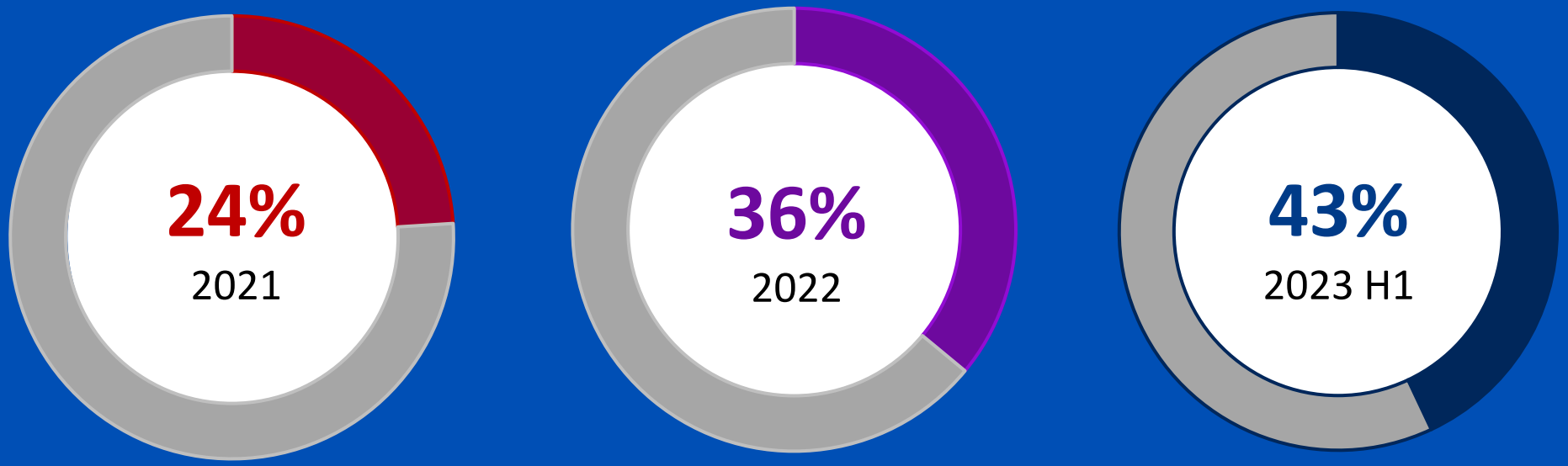


Median Time-to-Active-Directory for attacks in 2023 H1

Source: Active Adversary Report for Tech Leaders, 2023, Sophos (n=80)

Disabling Protection Is Now Commonplace

Percentage of Active Directory compromises where adversaries disable protection



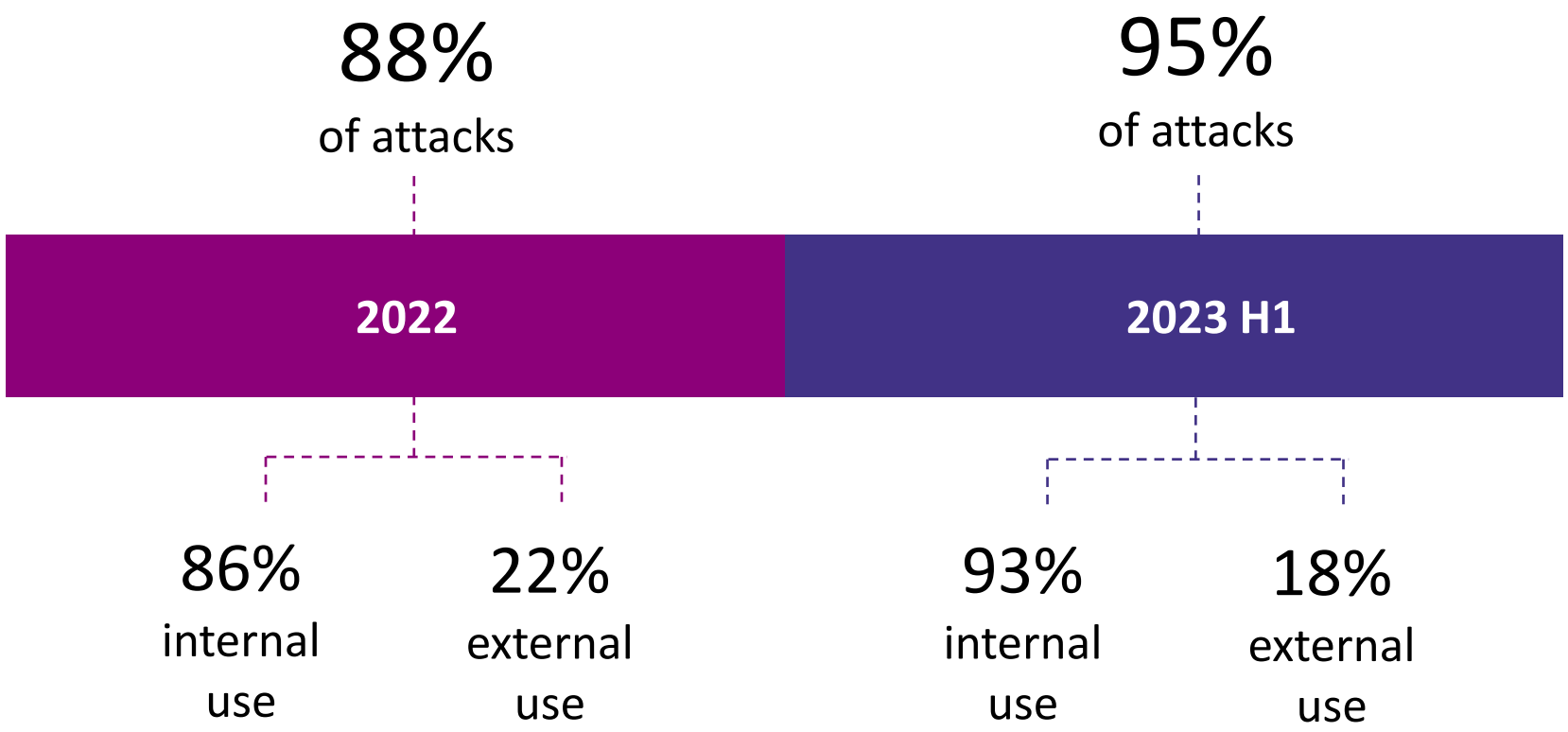
Source: Active Adversary Playbook 2022, Sophos (n=144); Active Adversary Report for Business Leaders, 2023, Sophos (n=152); Active Adversary Report for Tech Leaders, 2023, Sophos (n=80)

Living off the Land (i.e., exploiting legitimate IT tools)

Top 10 Living off the Land Binaries (LOLBins) observed in the dataset

Rank	5 Days or Less	Greater than 5 Days	Rank
1	RDP	RDP	1
2	PowerShell	PowerShell	2
3	PsExec	cmd.exe	3
4	cmd.exe	PsExec	4
5	Task Scheduler	Net.exe	5
6	net.exe	Task Scheduler	6
7	rundll32.exe	rundll32.exe	7
8	ping.exe	WMI	8
9	reg.exe	Ping.exe	9
10	vssadmin.exe	whoami.exe	10

Ubiquity of RDP in Attacks



Source: Active Adversary Report for Business Leaders, 2023, Sophos (n=152); Active Adversary Report for Tech Leaders, 2023, Sophos (n=80)

Why isn’t cybersecurity working?

SOPHOS

Peter Firstbrook | Gartner

Distinguished VP Analyst

> **“Nobody has enough people to do security…you have to deliver it as a service. It’s not enough to sell software because most buyers don’t have the people who can use it. We see a huge interest in managed security services — because this whole security market is becoming far too complicated for the average organization.”**

Peter Firstbrook | Gartner

Distinguished VP Analyst

“Nadie tiene suficiente gente para ocuparse de la seguridad... hay que ofrecerla como un servicio. No basta con vender software porque la mayoría de los compradores no cuentan con las personas que puedan utilizarlo. Vemos un enorme interés en los servicios de seguridad gestionados, porque todo este mercado de la seguridad se está volviendo demasiado complicado para la organización promedio.”

How Sophos Delivers Cybersecurity as a Service

MANAGED SECURITY SERVICES

- MDR — Sophos MDR Complete
- MDR — Sophos MDR Essentials
- MDR — Sophos MDR for Microsoft Defender
- IR — Sophos IR Services
- NDR — Sophos NDR

A COMPREHENSIVE AND EXTENSIBLE PLATFORM

Sophos Adaptive Cybersecurity Ecosystem

Sophos Central

SECURITY SOLUTIONS AND CONTROL POINTS

- XDR — Sophos XDR
- Fw — Sophos Firewall
- Em — Sophos Email
- Ep — Sophos Endpoint
- Cld — Sophos Cloud
- Fac — Sophos Factory

Sophos MDR: Industry-Leading Openness and Flexibility

Sophos MDR

Compatible with your environment
We can use our tools, another vendor's tools or any combination of the two

Compatible with your needs
Whether you need full-scale incident response or assistance making more accurate decisions

Compatible with your business
Our team has deep experience hunting threats targeting organizations in every industry

Sophos

- XDR Sophos XDR
- Fw Sophos Firewall
- Cld Sophos Cloud
- NDR Sophos NDR
- Em Sophos Email
- Ep Sophos Endpoint

Endpoint

Microsoft, CROWDSTRIKE, SentinelOne, TREND MICRO, Symantec (A Division of Broadcom), Trellix, Malwarebytes, BlackBerry CYLANCE

Firewall

paloalto NETWORKS, FORTINET, CHECK POINT, CISCO, SONICWALL

Cloud SaaS

aws, Azure, Google Cloud, orca security

Email

Microsoft 365, mimecast, proofpoint

Identity

Microsoft [Azure IDP, ATA], okta, DUO, ManageEngine

Network

DARKTRACE, THINKST CANARY, Skyhigh Security

SOPHOS

- XDR Sophos XDR
- Ep Sophos Endpoint
- Fw Sophos Firewall
- Cld Sophos Cloud
- NDR Sophos NDR
- Em Sophos Email

Endpoint

Microsoft
CROWDSTRIKE
SentinelOne
TREND MICRO
Symantec. A Division of Broadcom
BlackBerry. CYLANCE.

Firewall

paloalto NETWORKS
FORTINET
CHECK POINT
cisco
SONICWALL
WatchGuard

Identity

Microsoft
okta
DUO
ManageEngine

Email

Microsoft
proofpoint.
mimecast

Productivity

Microsoft
Google Workspace

Network

DARKTRACE
VECTRA
THINKST CANARY

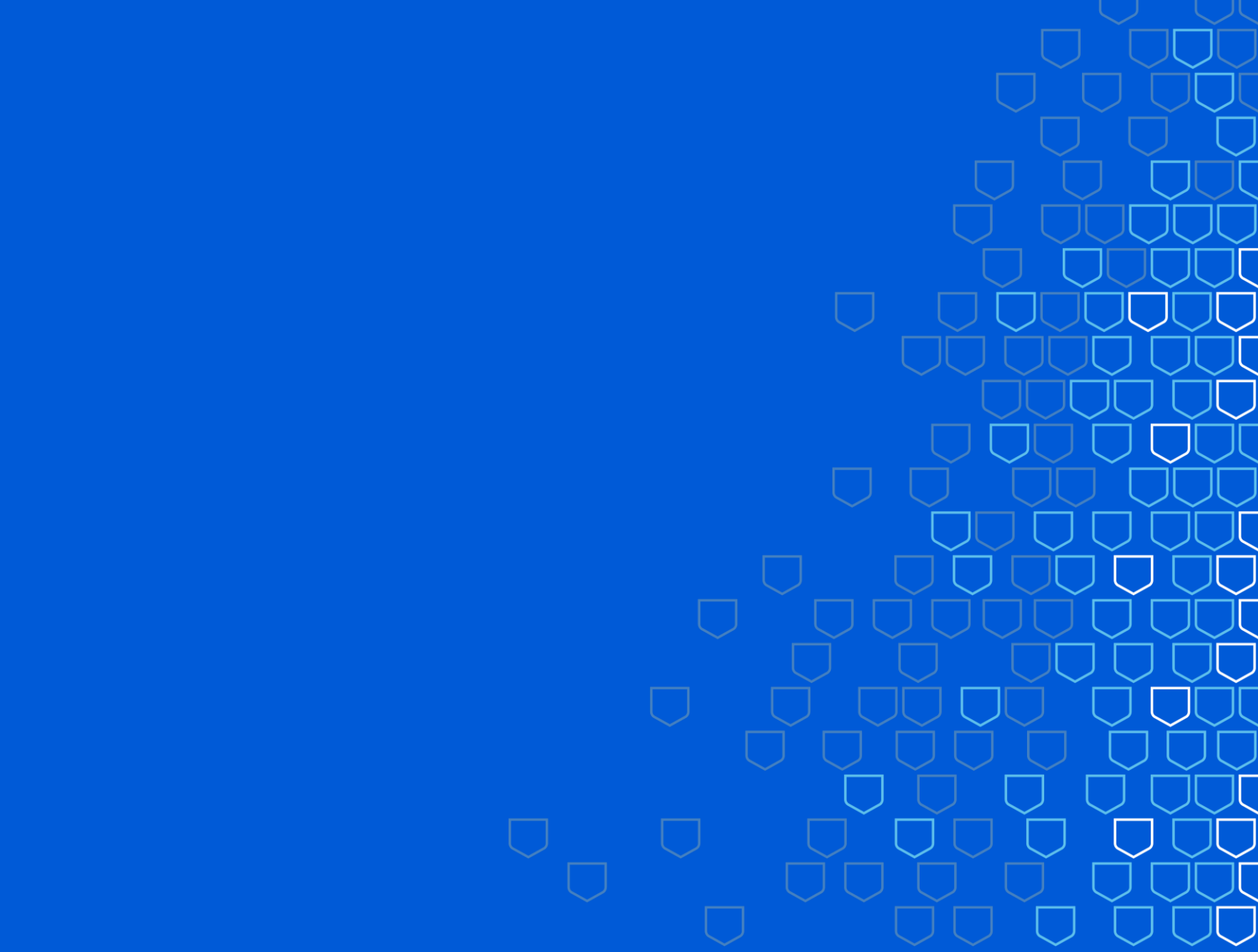
Cloud

Microsoft
aws
Google Cloud
orca security

Backup / Data Security

VEEAM

Takeaways



Key Actions for Defenders

- **Increase friction wherever possible**
  - Robust, layered defenses
  - MFA
  - Vulnerability management
  - Lock down RDP – and actively monitor for abuse
  - Limit tools that can be present on systems and their scope
- **Protect everything**
  - Adversaries *will* find the unmanaged or under-protected machine
- **Always be watching**
  - Attackers deliberately target off-hours and weak spots
- **Be ready to investigate and respond**
  - Planning is good, but you need to be *prepared* to act immediately

Learn More

Insights and advice to help defenders secure their organizations

- news.sophos.com/threat-research
- @SophosXOps
- https://infosec.exchange/@SophosXOps

Articles, reports, videos and more

SOPHOS

Services and products to detect and stop Active Adversaries

- 24/7 managed detection and response
- Adaptive endpoint protection
- Incident Response support

Start a free trial and speak to our team

SOPHOS