SOPHOS

ho.Systeme

Sophos Adaptive AI-Native Cybersecurity Platform

Behalten Sie jede Bedrohung im Griff

Stefan Liß
Senior Sales Engineer

Sophos Active Adversary Report 2026

661 cases

investigated by Sophos X-Ops between November 1, 2024 and October 31, 2025.

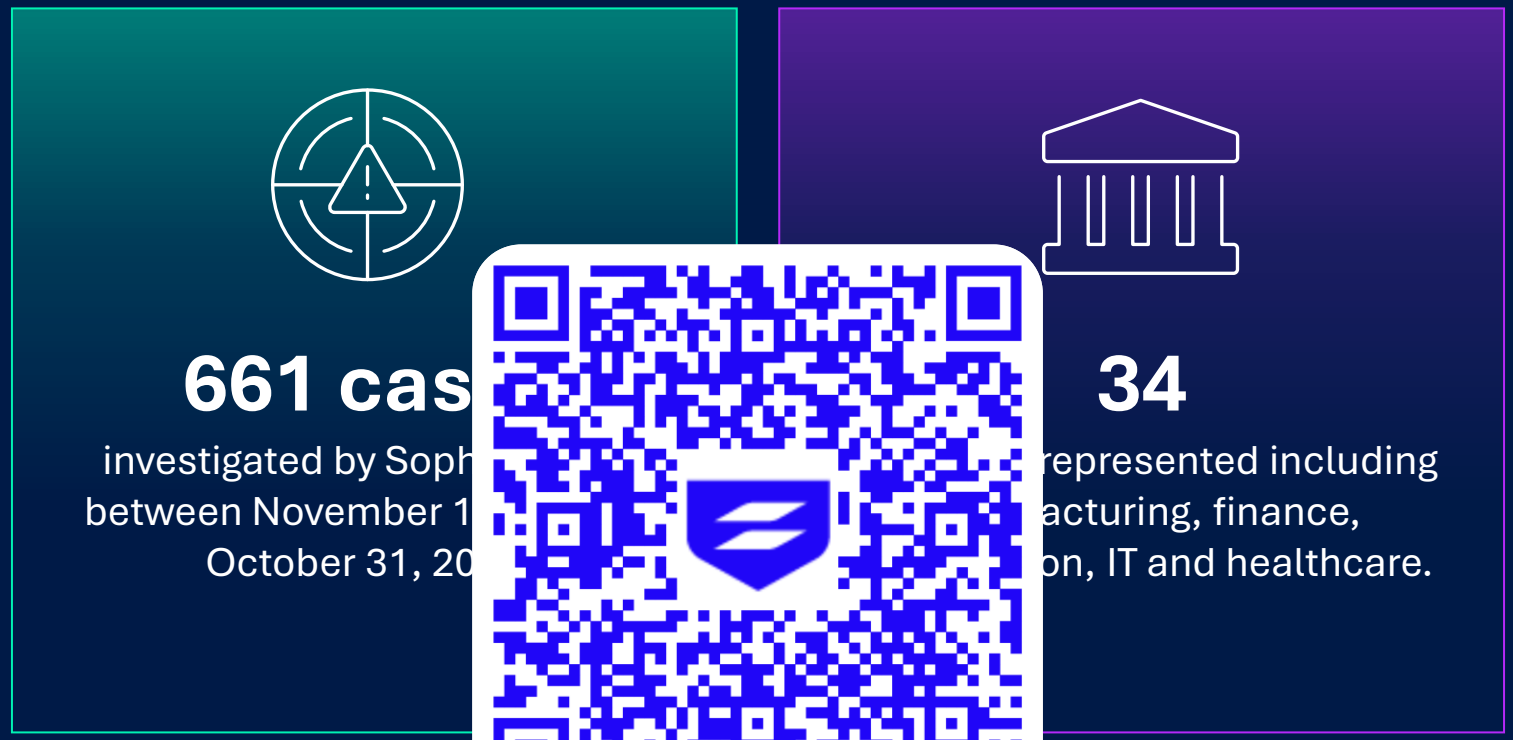
34

industries represented including manufacturing, finance, construction, IT and healthcare.

https://www.sophos.com/de-de/press/press-releases/sophos-active-adversary-report-2026-identity-attacks-dominate-as-threat-groups-proliferate

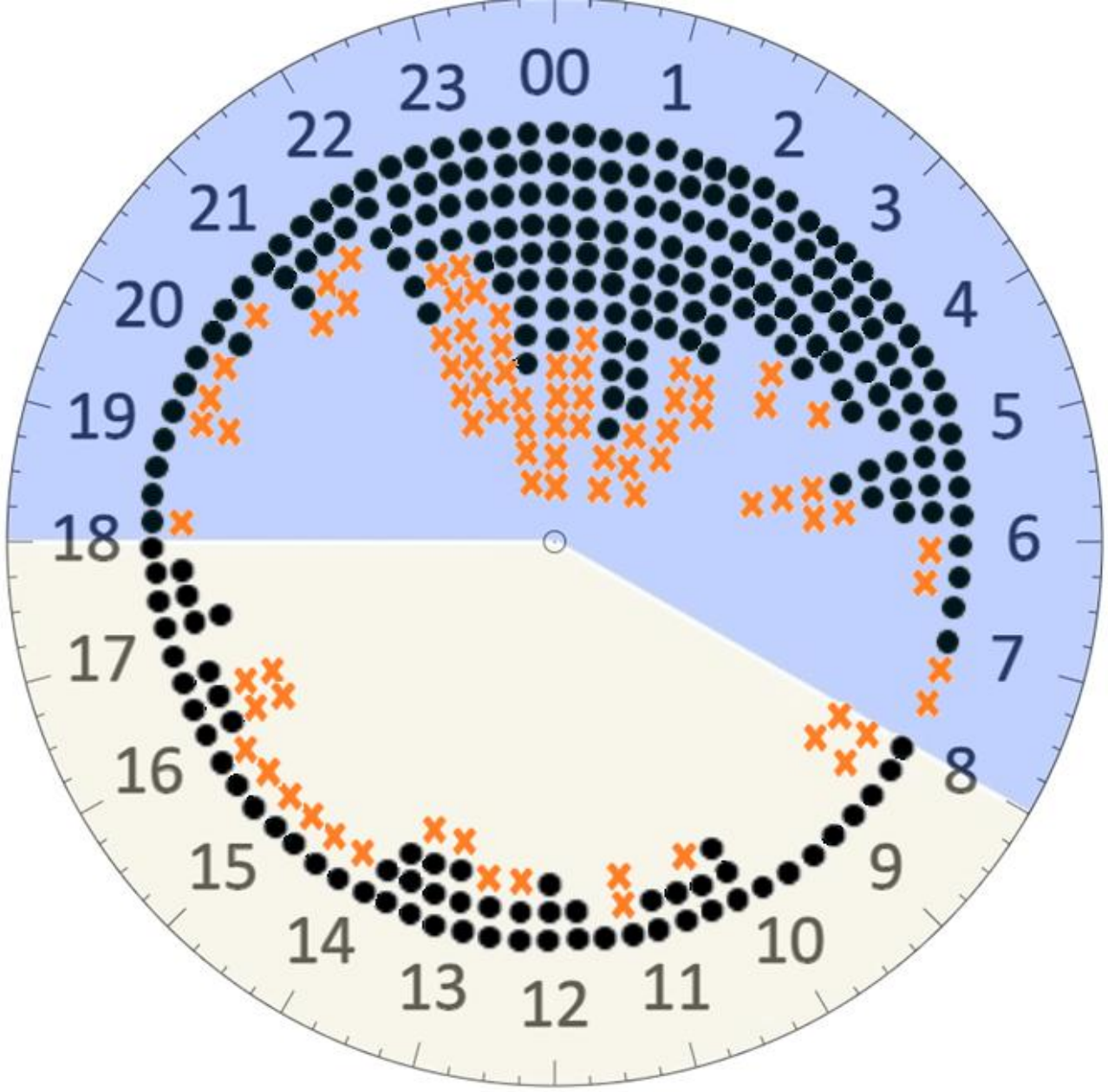
SOPHOS

Sophos Active Adversary Report 2026



https://www.sophos.com/de-de/press/press-releases/sophos-active-adversary-report-2026-identity-attacks-dominate-as-threat-groups-proliferate

SOPHOS


00
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
Business hours in target time zone (8am-6pm Mon-Fri)
Before / after business hours in target time zone
Workweek attacks
Weekend attacks (6pm Fri-12am Mon)

SOPHOS

Resultat Nr. 1:

Resultat Nr. 1:

Identität ist der größte Angriffsvektor

SOPHOS

“In 67% aller Fälle brechen Angreifer nicht ein, sie loggen sich ein”

Durch gestohlene Zugangsdaten und Passwörter in Daten-Leaks

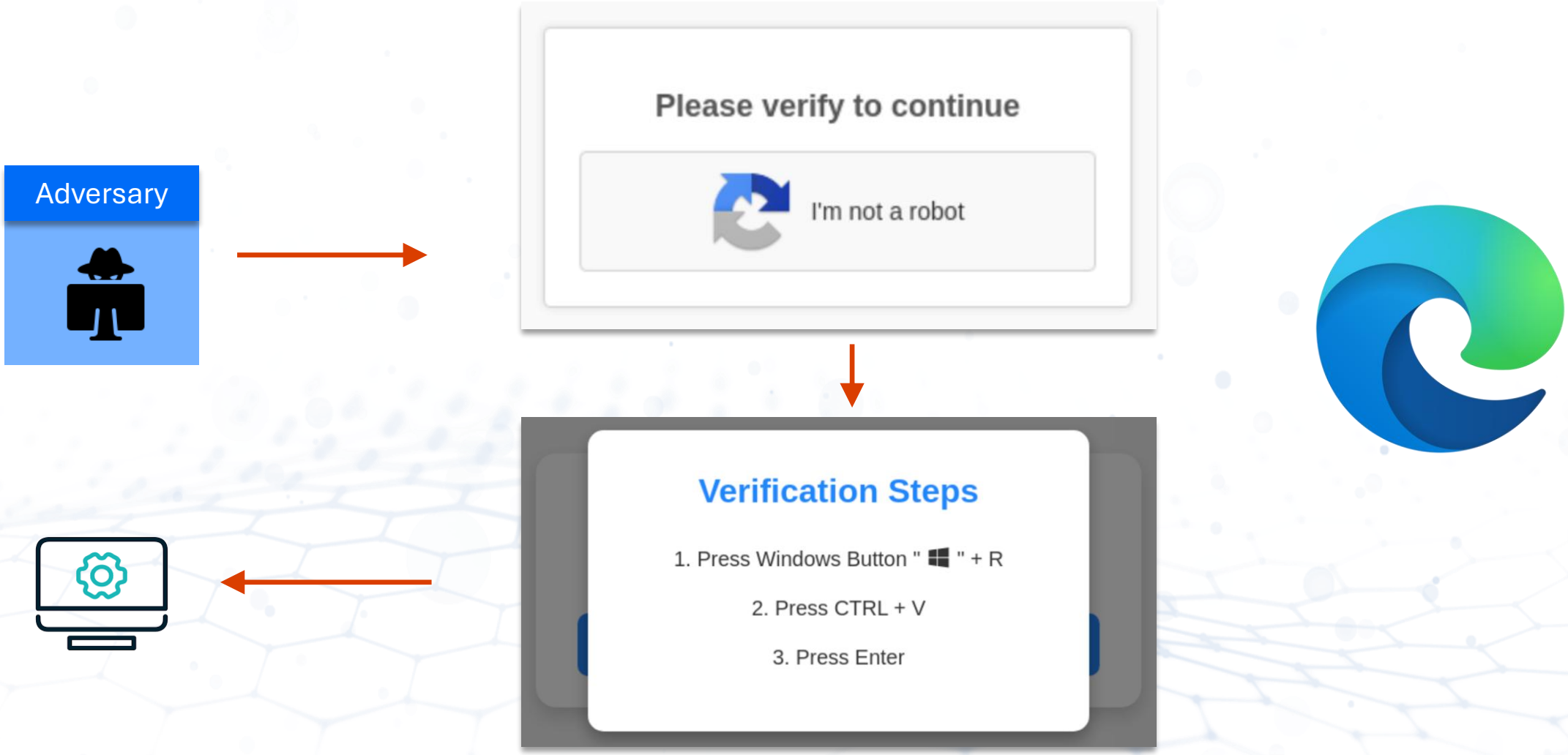
SOPHOS

Summary of key findings

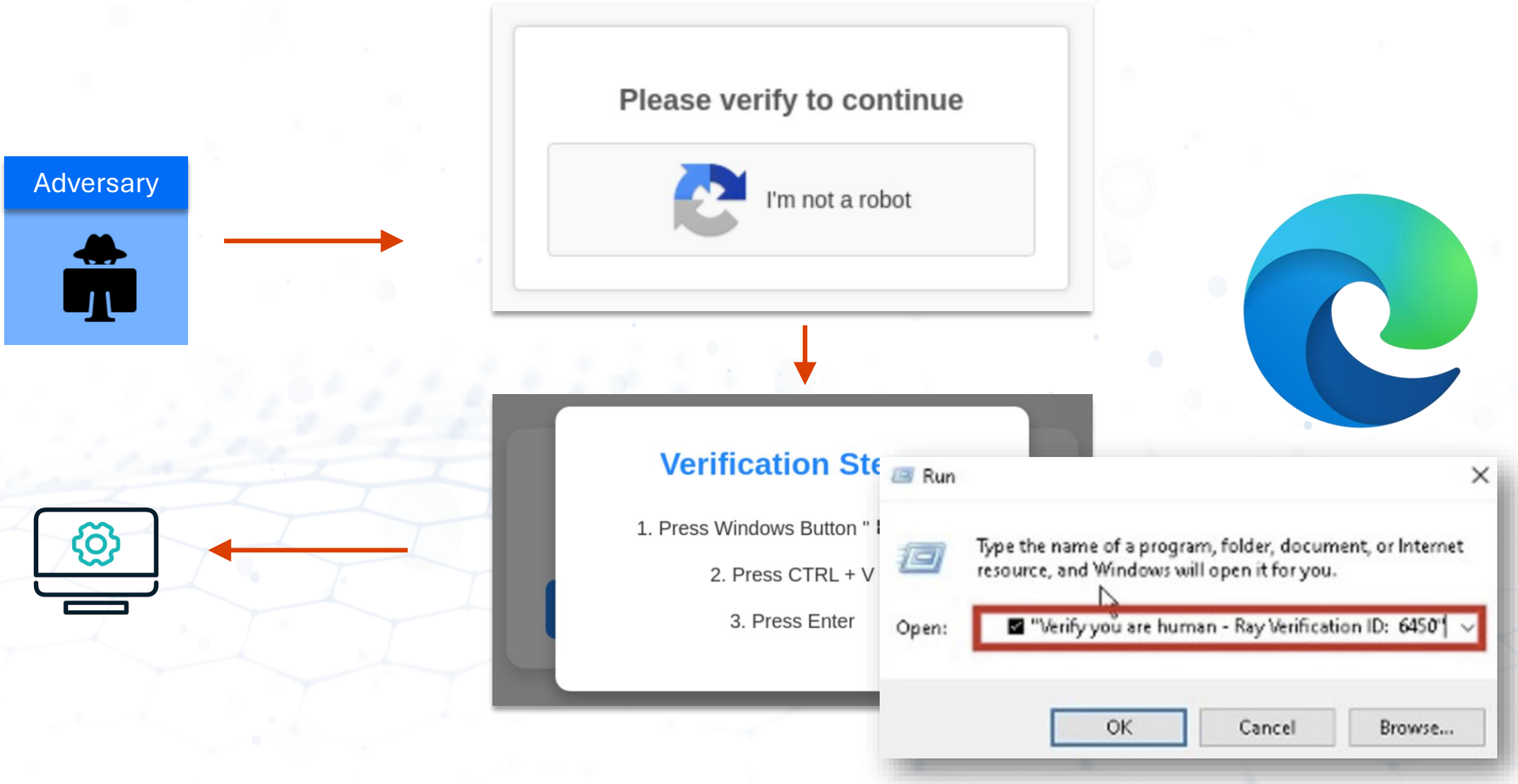
1. Identity is now the primary attack vector.
2. Ransomware is an evening, night and weekend activity.
3. Firewall vulnerabilities remain a high-impact entry point.
4. Attackers are getting faster at attacking Active Directory (AD).
5. Lack of telemetry creates headwinds for defenders.

SOPHOS

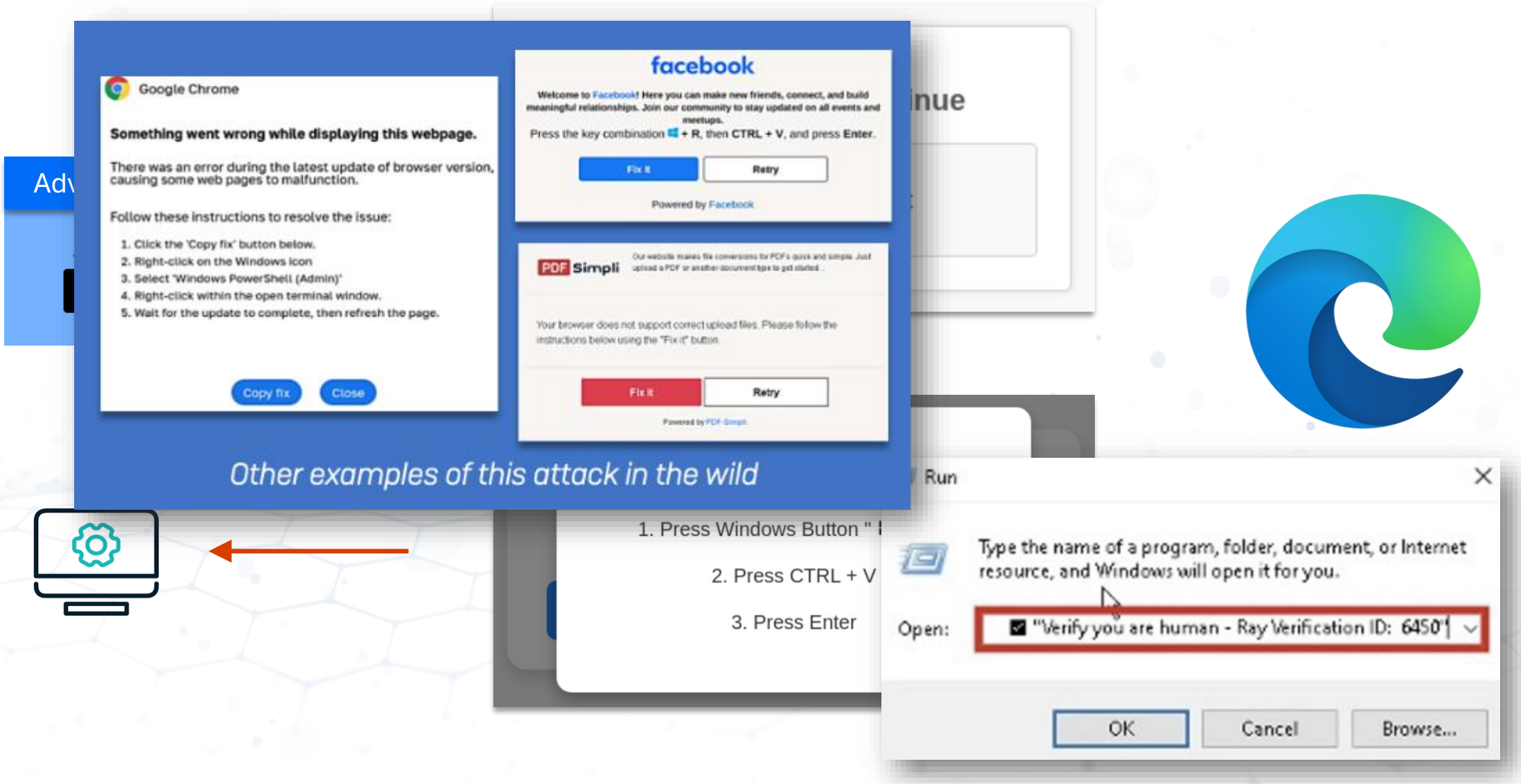
ClickFix Phishing (aka Fake CAPTCHA)



ClickFix Phishing (aka Fake CAPTCHA)



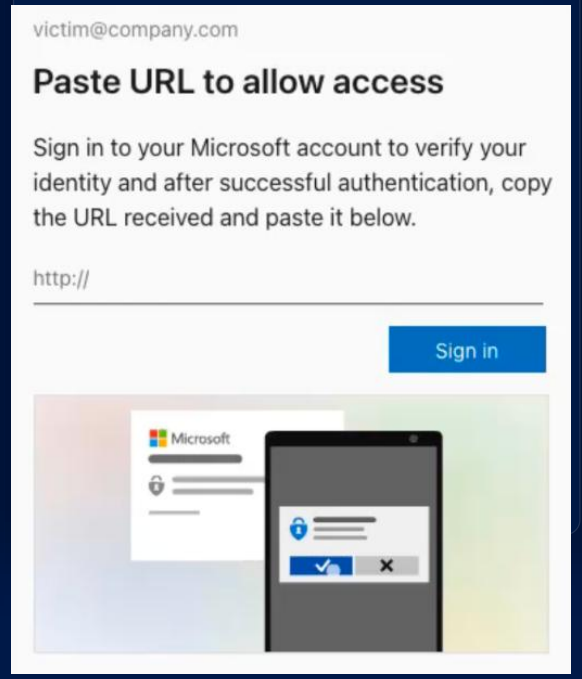
ClickFix Phishing (aka Fake CAPTCHA)



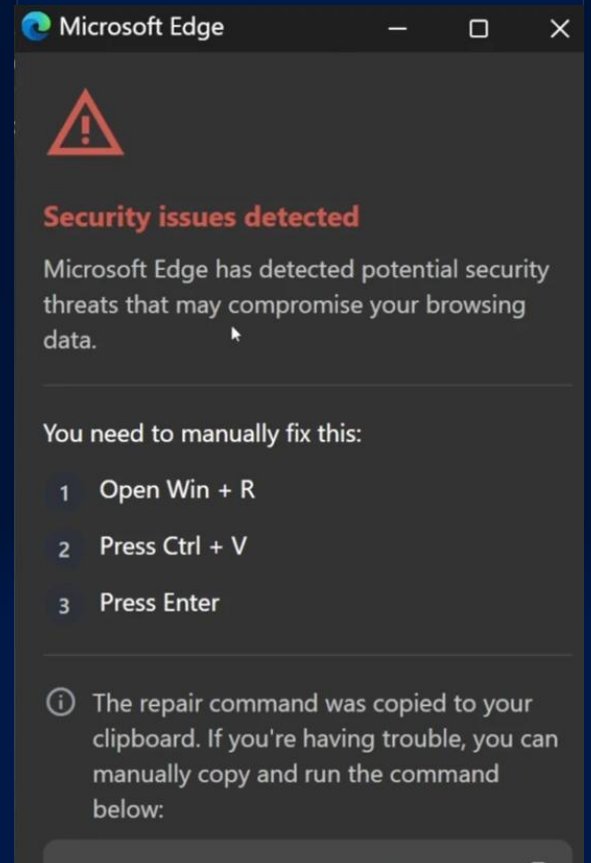
Battlefield Browser!

ClickFix

ConsentFix



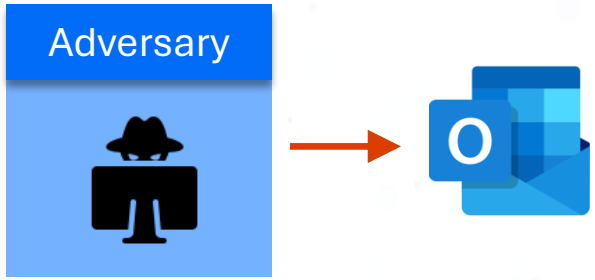
CrashFix



Device Code

SOPHOS

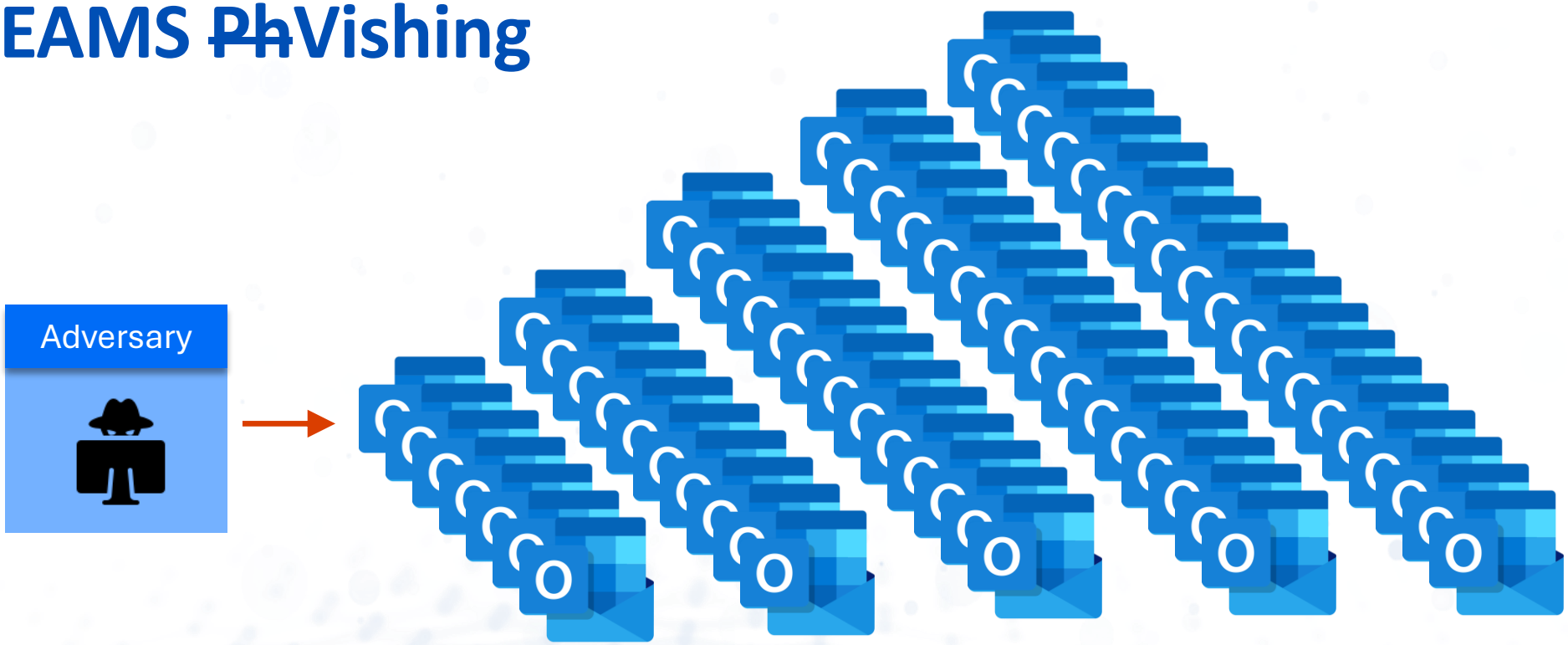
TEAMS ~~Ph~~Vishing



https://news.sophos.com/en-us/2025/01/21/sophos-mdr-tracks-two-ransomware-campaigns-using-email-bombing-microsoft-teams-vishing/

SOPHOS

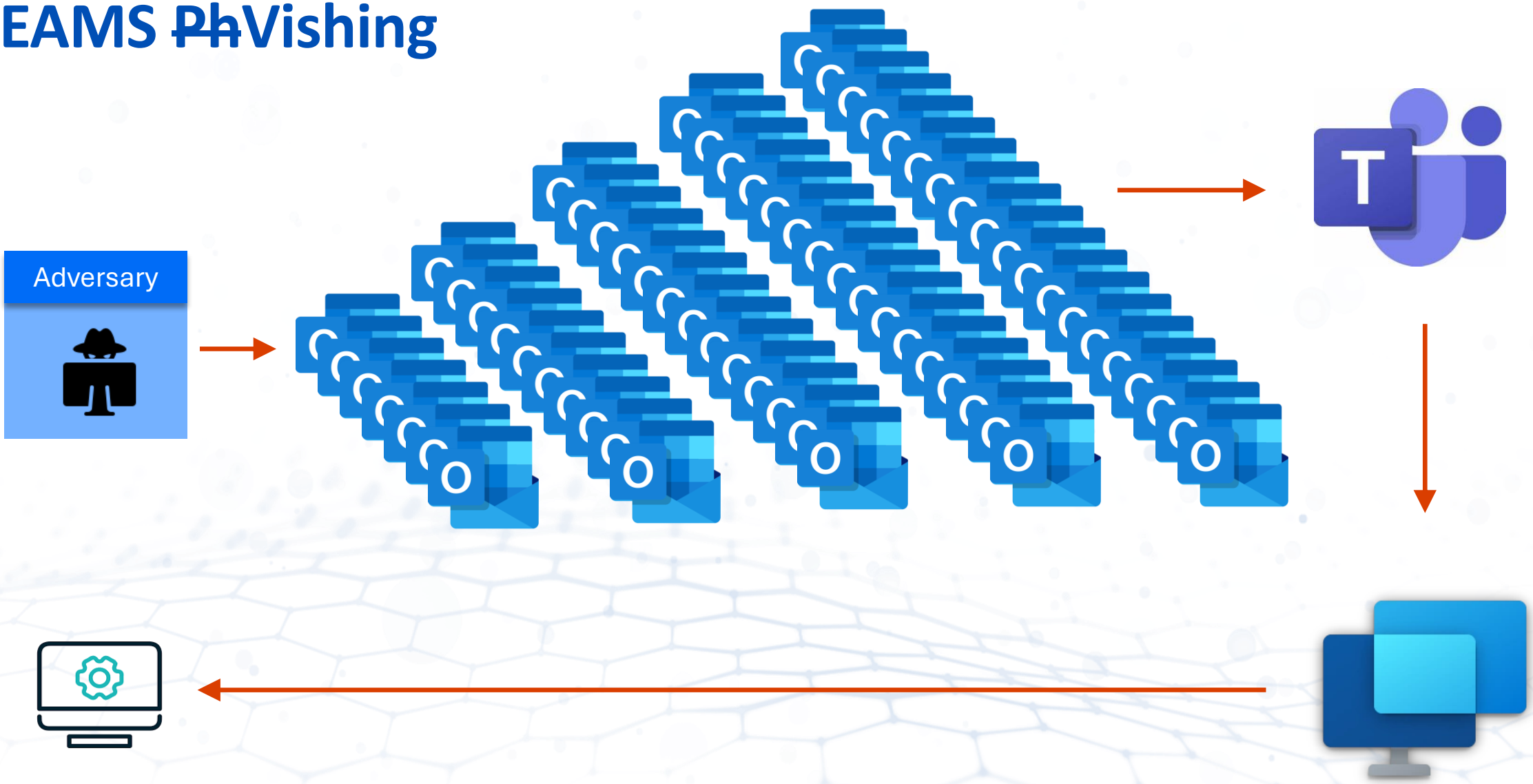
TEAMS ~~Ph~~Vishing



https://news.sophos.com/en-us/2025/01/21/sophos-mdr-tracks-two-ransomware-campaigns-using-email-bombing-microsoft-teams-vishing/

SOPHOS

TEAMS ~~Ph~~Vishing



https://news.sophos.com/en-us/2025/01/21/sophos-mdr-tracks-two-ransomware-campaigns-using-email-bombing-microsoft-teams-vishing/

SOPHOS CENTRAL PLATFORM

Managed by Customers | Managed by Partners | Managed by Sophos

SERVICES

MANAGED SERVICES

- MDR
- Incident Response
- Vulnerability Management
- Professional Services

ADVISORY SERVICES

- Penetration Testing
- Security Assessments
- Red Team Exercises
- Incident Readiness

THREAT PREVENTION AND CONTROLS

CONTROLS

- Endpoint
- Firewall
- Identity
- Email
- Network
- Web Browser

INTEGRATIONS

350+ Third Party Integrations

SECURITY OPERATIONS

- XDR
- SIEM
- EDR
- ITDR
- NDR
- SOAR

THREAT INTELLIGENCE

SOPHOS X-OPS

- Adversary Tracking
- Threat Research
- Breach Forensics
- Malware Analysis
- Industry Collaboration

AI, AUTOMATION & ENGINEERING

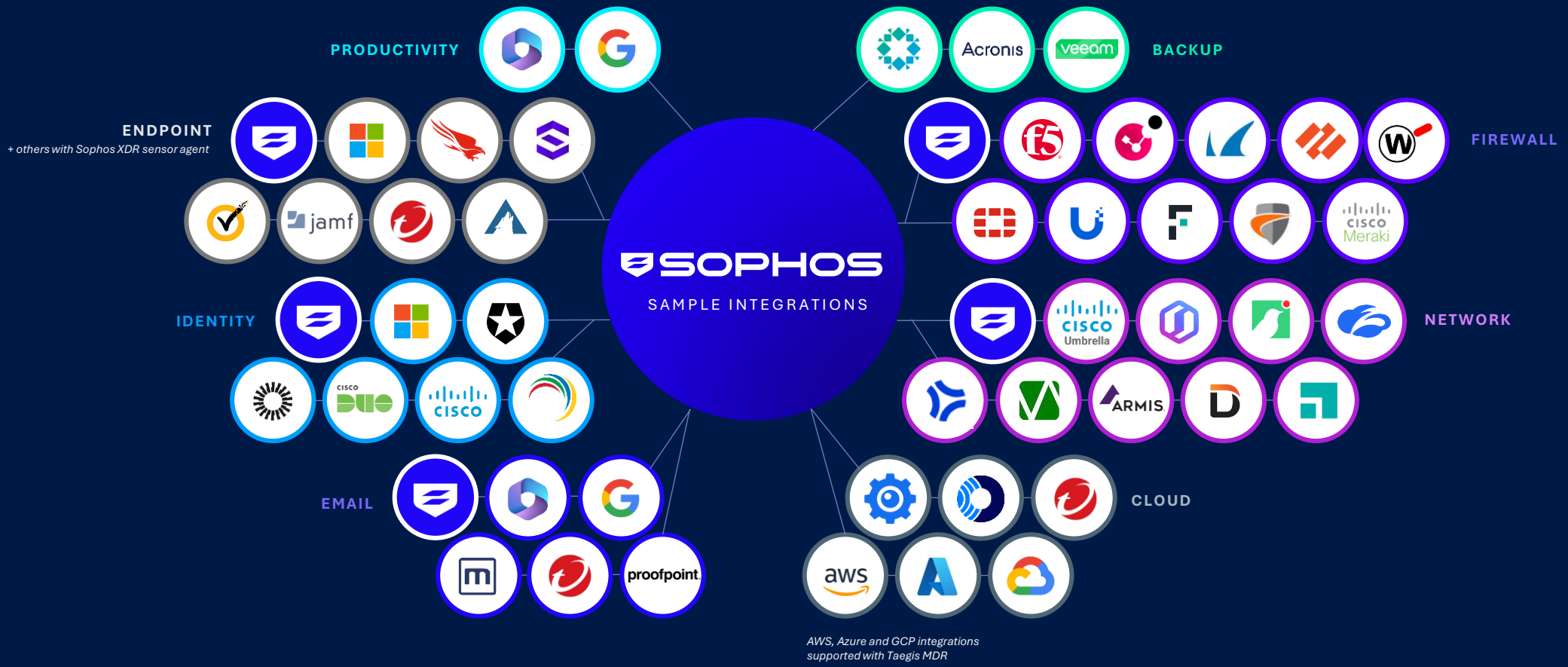
- Adaptive Attack Protection
- Critical Attack Warning
- Security Analytics
- Detection Logic
- Threat Protection

DATA LAKE

AI-ASSISTED & AGENTIC WORKFLOWS

Visibility across all attack surfaces

Our analysts can leverage your existing technology investments to detect and respond to threats.



SOPHOS

Neu: Sophos Workspace Protection

Alle erforderlichen Schutzfunktionen in einer einzigen Lösung integriert

Protected Browser

ZTNA

DNS Protection

EMS

Bereitstellen oder nur das nutzen, was gebraucht wird

SOPHOS

Sophos Identity Threat Detection and Response (ITDR)

Ganzheitlicher Ansatz, das Identitätsrisiko in der Organisation zu reduzieren

Reduziert die Identity Angriffsfläche

Kontinuierlicher Scan von Microsoft Entra ID nach Identity Sicherheitslücken und Fehlkonfigurationen

Minimiert das Risiko kompromittierter Zugangsdaten

Benachrichtigung, wenn Zugangsdaten im Darknet auftauchen

Identifiziert riskantes Nutzerverhalten

Monitoring und Alarmierung bei ungewöhnlichen Benutzeraktivtäten

Sophos ITDR Add-on zu Sophos XDR und Sophos MDR

SOPHOS

SOPHOS MDR THREAT CASE

Backup Server Compromise Thwarted

ADVERSARY BEHAVIOR

The attacker begins an SSL VPN session on the **customer's Sophos Firewall**, then accesses a Veaam backup server, both via legacy accounts with previously compromised credentials and from an out-of-region IP address.

The attacker attempts to create a new user account with administrative privileges on the Veeam Backup Service.

THREAT DETECTION

10:11 UTC
Sophos MDR flags this suspicious combination of commands on the Veeam backup server and a case is automatically created.

10:20 UTC
The case is triaged and escalated to High Severity. The customer has Sophos MDR's **"Authorize"** response mode enabled, allowing Sophos to act immediately on their behalf.

INVESTIGATION

10:28 UTC
A Sophos MDR analyst isolates the Veeam backup server and discovers the VPN session on the customer's Sophos Firewall.

10:38 UTC
Sophos MDR terminates the VPN session and disables the attacker's user account.

10:40 UTC
Sophos MDR calls the customer and elevates the case to Critical, initiating Incident Response.

RESPONSE

11:00 UTC
Customer confirms the accounts were from a decommissioned IT provider.

Sophos MDR provides remediation guidance and confirms completion with the customer, including resetting credentials, disabling legacy accounts, blocking attacker IP addresses, deploying MFA, and upgrading the Veeam Backup Service to the latest secure version.

SOPHOS

Microsoft M365

Example Response Actions

Block/enable user sign-in

Lock down a user's Microsoft 365/Azure account to stop adversaries using stolen credentials.

Terminate active sessions

Instantly revoke active sessions to eject adversaries and prevent reuse of stolen session tokens.

Disable suspicious inbox rules

Remove malicious inbox rules often used in business email compromise (BEC) attacks

SOPHOS MDR THREAT CASE

Adversary-in-the-Middle Attack with Response Actions

Case Creation: August 13, 2025 | 16:54 UTC

A proprietary Sophos detection rule identifies an Adversary-in-the-Middle attack (Axios user agent).

Response: August 13, 2025 | 16:55 UTC

Microsoft O365 response actions are automatically executed, **disabling sign-in and terminating active sessions** for the compromised user account; the activity is immediately escalated to the customer.

Remediation: August 14, 2025 | 06:48 UTC

Once the customer has confirmed that the user's password has been reset, the Sophos MDR analyst re-enables user sign-in to restore access to the O365 account.

SOPHOS

Sophos MDR

35,000 +
MDR customers globally

A vast, diverse customer base provides unparalleled intelligence and proactive threat defense.

1,101
Investigations completed daily

Our highly skilled experts monitor, triage, investigate, and respond to threats on your behalf.

231
Advanced attacks stopped every day

Learnings from attacks stopped by Sophos MDR drive enhancements to proactive protection.

Global analyst coverage

Tested. Recognized. Trusted.

Gartner Peer Insights Customers' Choice 2024
Customers' Choice

MITRE ATT&CK®
Top Performer

FROST & SULLIVAN
Leader

Gartner Peer Insights™
Highest-Rated

G2 Grid® Reports
Highest-Rated

SOPHOS

SOPHOS

DEFEAT CYBERATTACKS