



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 Active Adversary Report 2026



661 cases

investigated by Sophos
between November 1, 2025
October 31, 2026

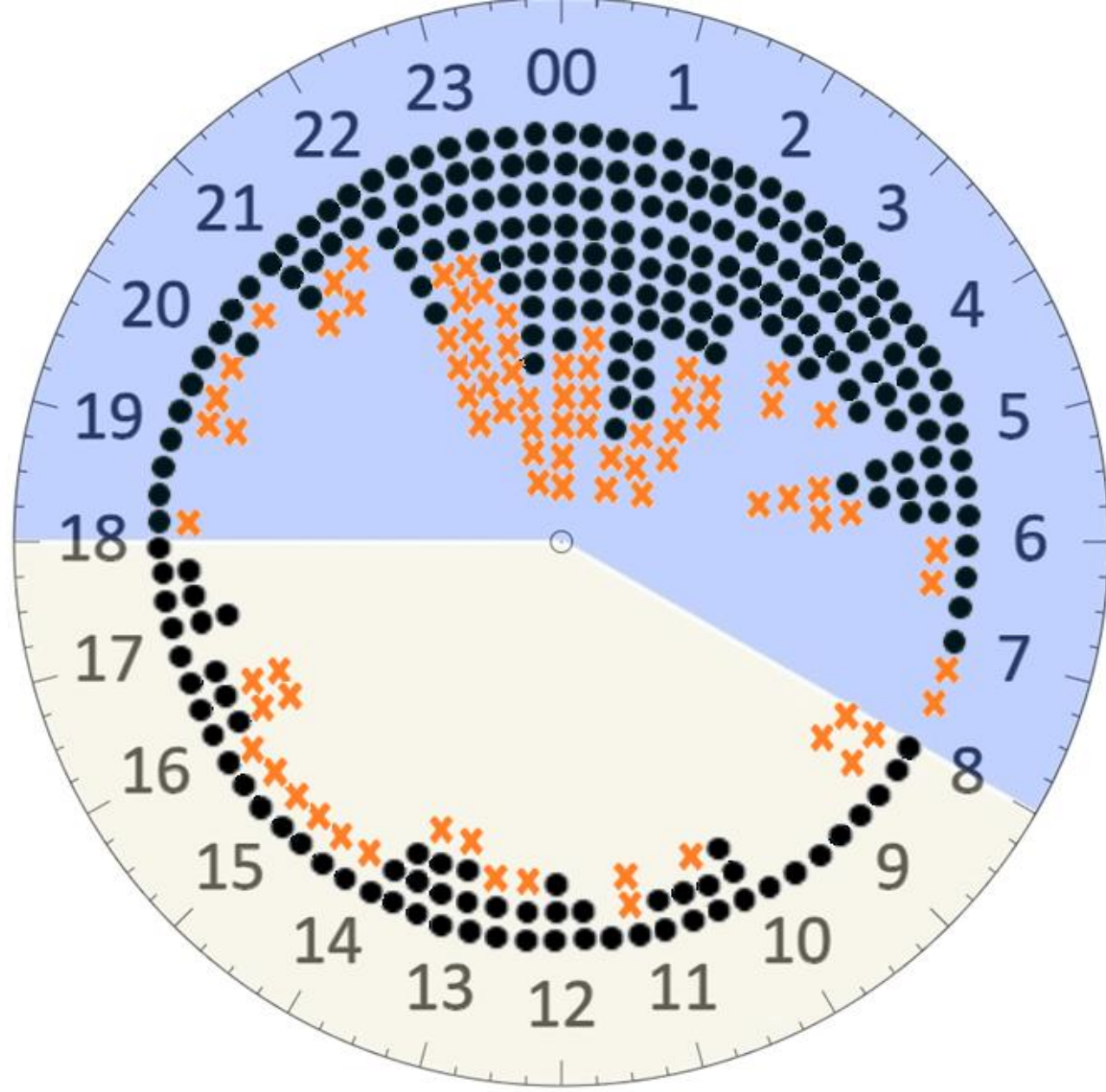


34

represented including
manufacturing, finance,
government, IT and healthcare.



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



- 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)

Resultat Nr. 1:

Resultat Nr. 1:

Identität ist der größte Angriffsvektor

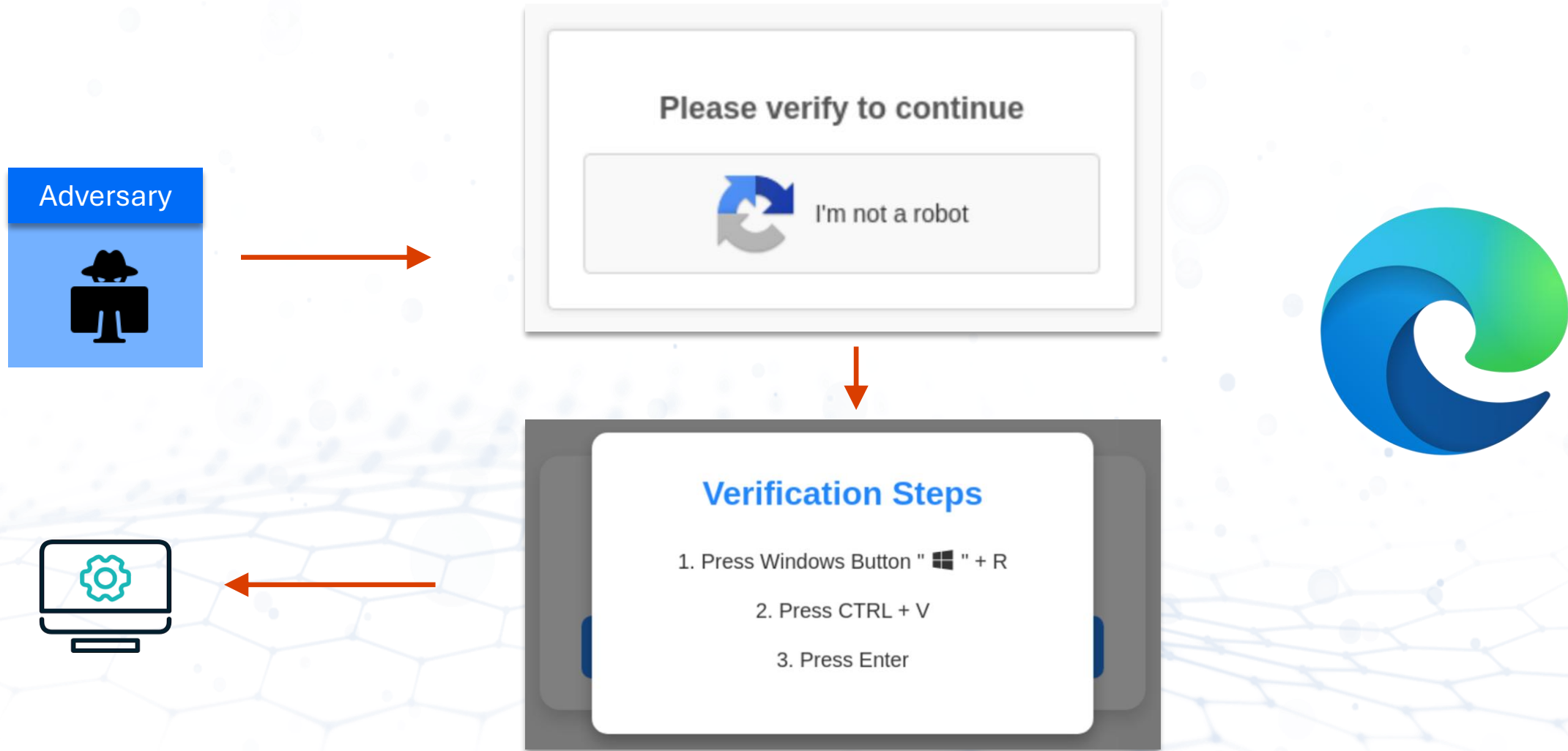
***“In 67% aller Fälle brechen Angreifer nicht ein,
sie loggen sich ein”***

***Durch gestohlene Zugangsdaten und
Passwörter in Daten-Leaks***

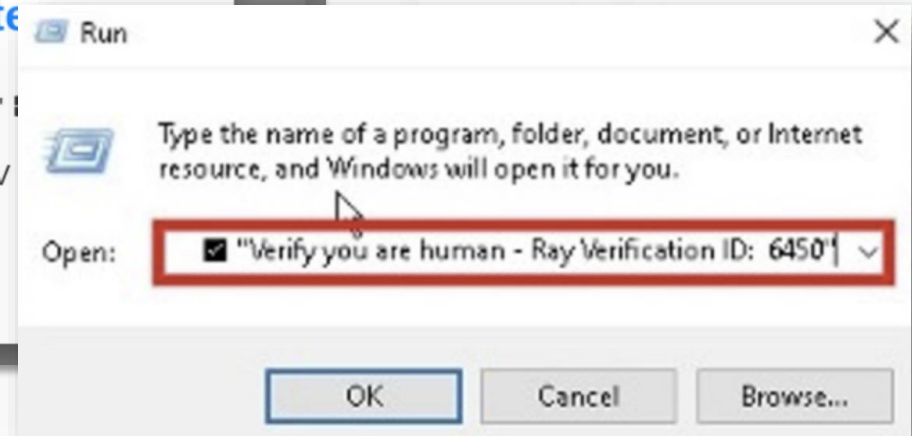
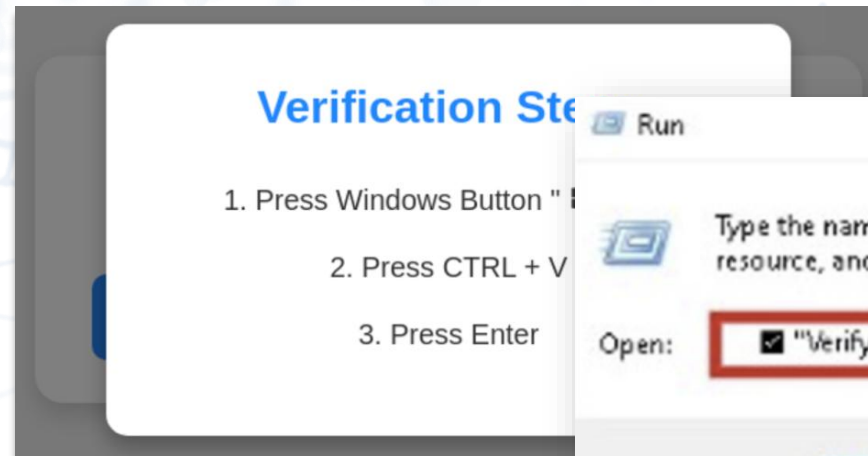
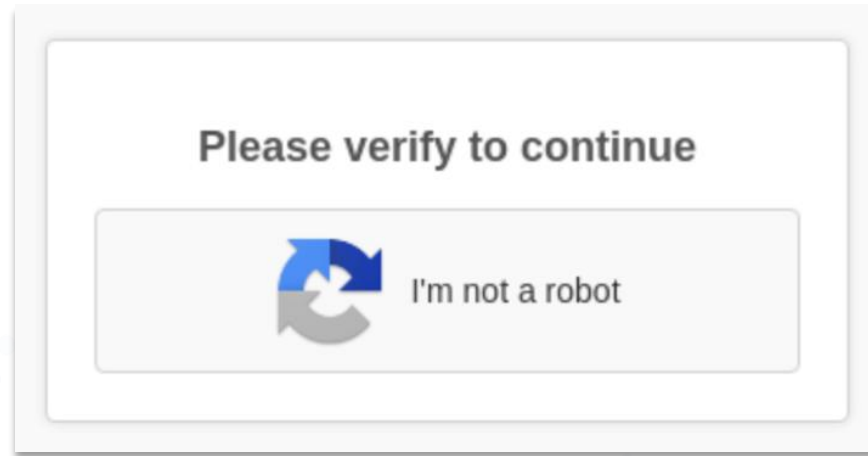
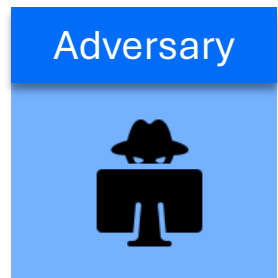
Summary of key findings

- 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.

ClickFix Phishing (aka Fake CAPTCHA)

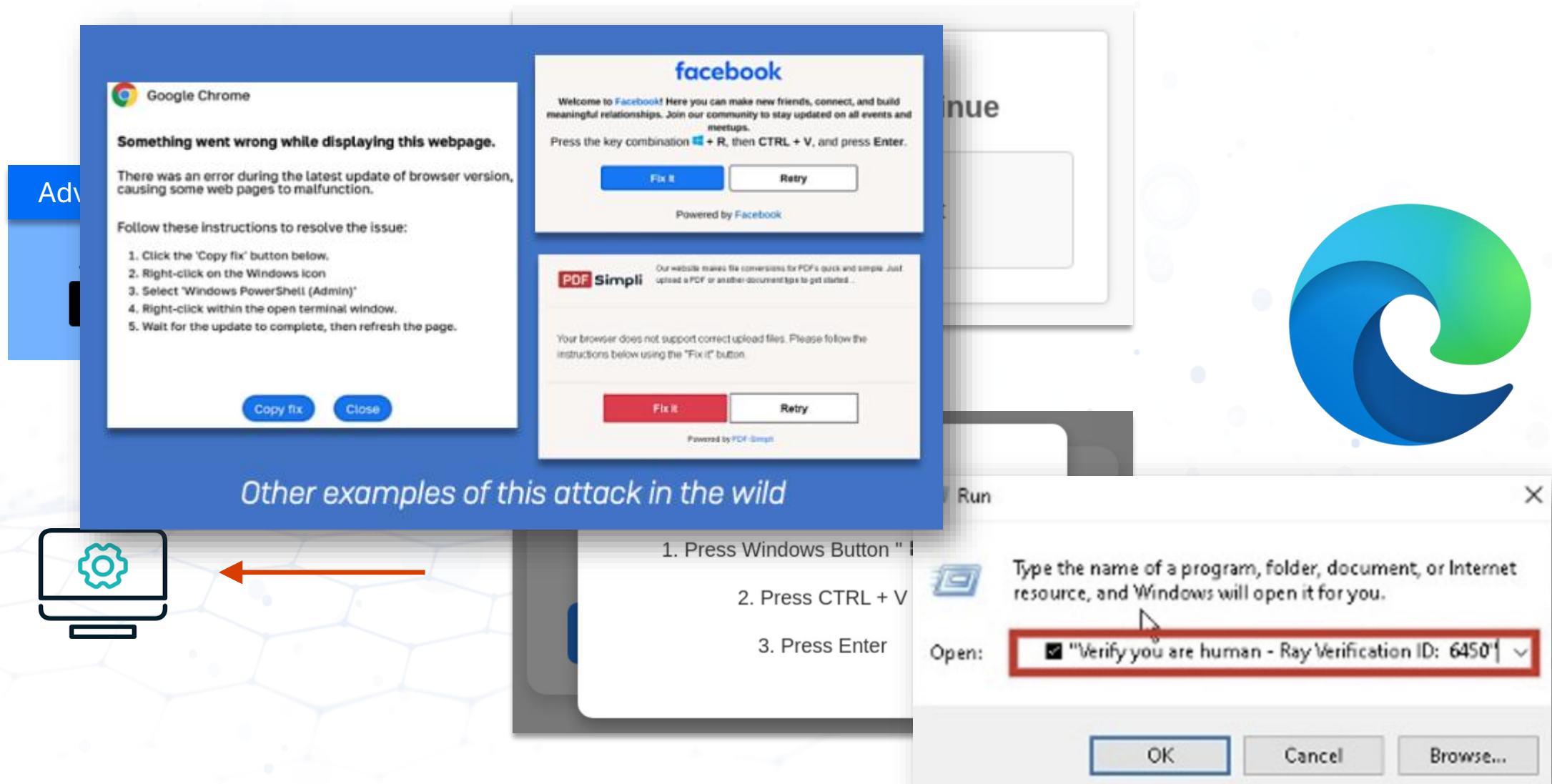


ClickFix Phishing (aka Fake CAPTCHA)



ClickFix Phishing (aka Fake CAPTCHA)

Adv



Google Chrome

Something went wrong while displaying this webpage.

There was an error during the latest update of browser version, causing some web pages to malfunction.

Follow these instructions to resolve the issue:

1. Click the 'Copy fix' button below.
2. Right-click on the Windows icon
3. Select 'Windows PowerShell (Admin)'
4. Right-click within the open terminal window.
5. Wait for the update to complete, then refresh the page.

Copy fix Close

facebook

Welcome to Facebook! Here you can make new friends, connect, and build meaningful relationships. Join our community to stay updated on all events and meetups.

Press the key combination **⌘ + R**, then **CTRL + V**, and press **Enter**.

Fix it Retry

Powered by Facebook

PDF Simpli

Our website makes file conversions for PDF's quick and simple. Just upload a PDF or another document type to get started.

Your browser does not support correct upload files. Please follow the instructions below using the "Fix it" button.

Fix it Retry

Powered by PDF-Simpli

Other examples of this attack in the wild

1. Press Windows Button "I"

2. Press CTRL + V

3. Press Enter

Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: ☒ "Verify you are human - Ray Verification ID: 64501" v

OK Cancel Browse...

Battlefield Browser!

ClickFix

Verification Steps

1. Press Windows Button "  " + R
2. Press CTRL + V
3. Press Enter

ConsentFix

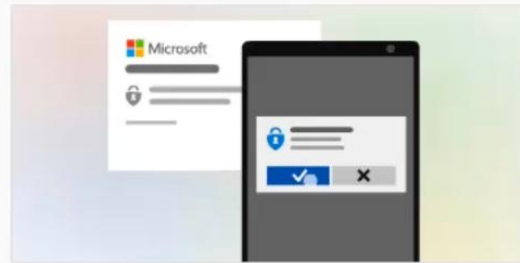
victim@company.com

Paste URL to allow access

Sign in to your Microsoft account to verify your identity and after successful authentication, copy the URL received and paste it below.

http://

Sign in



CrashFix

Microsoft Edge



Security issues detected

Microsoft Edge has detected potential security threats that may compromise your browsing data.

You need to manually fix this:

- 1 Open Win + R
- 2 Press Ctrl + V
- 3 Press Enter

 The repair command was copied to your clipboard. If you're having trouble, you can manually copy and run the command below:

Device Code

 Microsoft

Enter code to allow access

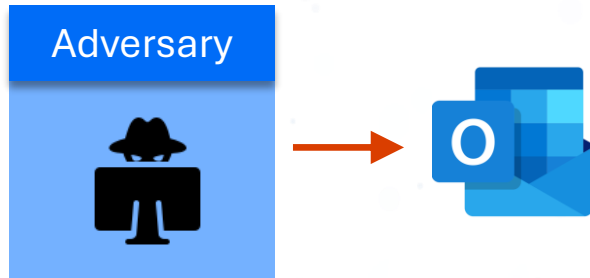
Once you enter the code displayed on your app or device, it will have access to your account.

Do not enter codes from sources you don't trust.

Code

Next

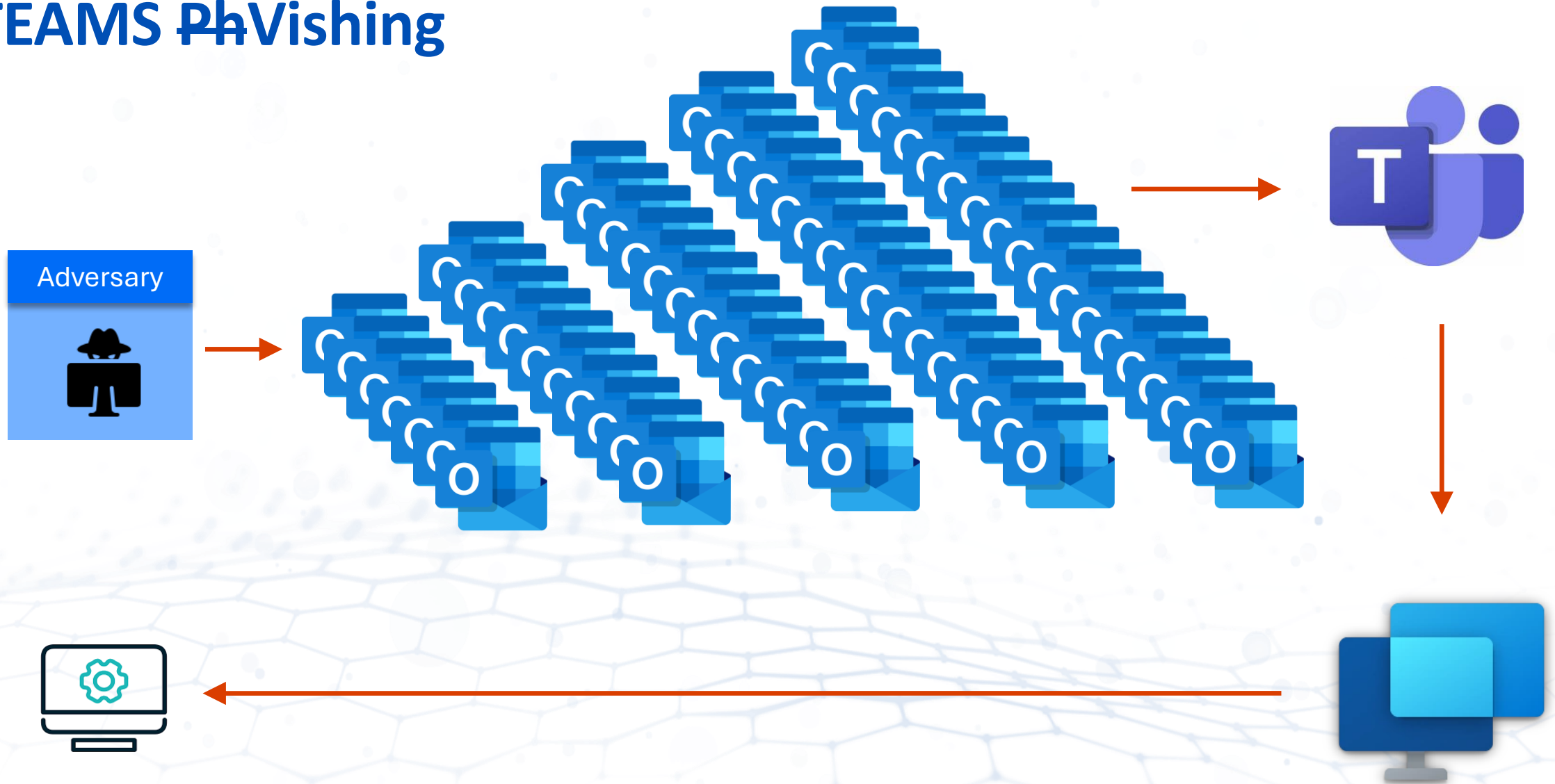
TEAMS Phishing



TEAMS PhVishing



TEAMS Phishing



SOPHOS CENTRAL PLATFORM

Managed by Customers | Managed by Partners | Managed by Sophos

MANAGED SERVICES

- MDR
- Incident Response
- Vulnerability Management
- Professional Services

ADVISORY SERVICES

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

SERVICES

CONTROLS

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

INTEGRATIONS

- 350+ Third Party Integrations

SECURITY OPERATIONS

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

THREAT PREVENTION AND CONTROLS

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

THREAT INTELLIGENCE

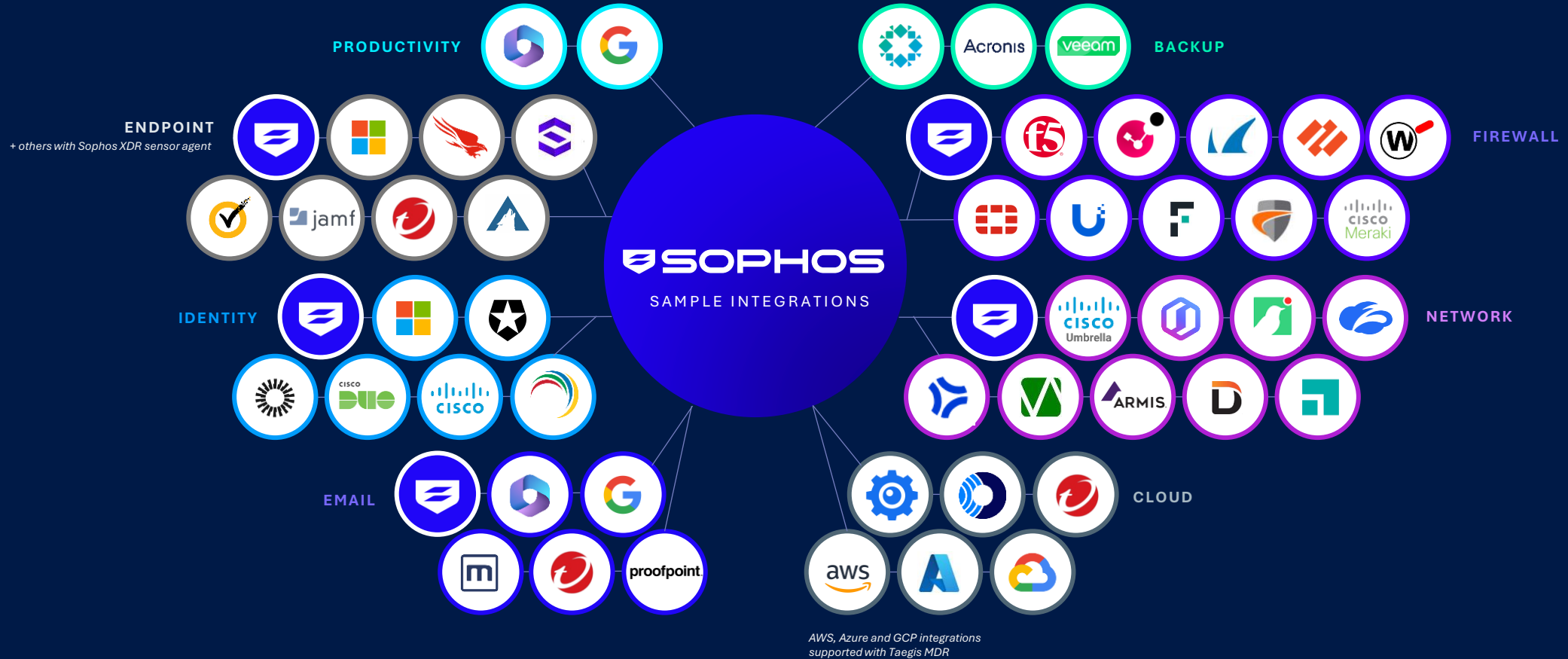
DATA LAKE



AI-ASSISTED & AGENTIC WORKFLOWS

Visibility across all attack surfaces

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



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 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
Benutzeraktivitäten

Sophos ITDR Add-on zu Sophos XDR und Sophos MDR

Backup Server Compromise Thwarted

ADVERSARY BEHAVIOR



The attacker begins an SSL VPN session on the **customer's Sophos Firewall**, then accesses a Veeam 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.



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 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.



Customers' Choice



Top Performer



Leader



Highest-Rated



Highest-Rated

