



20. Mai 2026

17. Bechtle
IT-Forum
Thüringen
Steigerwald Stadion Erfurt

20
26



Apple Geräte effektiv verwalten und schützen

Stefan Bartram

Jamf Software Deutschland GmbH

Test Name

04.09.2024







QR Code Phishing - Quishing



15. April 2025 ⌚ 8 Min #Laden

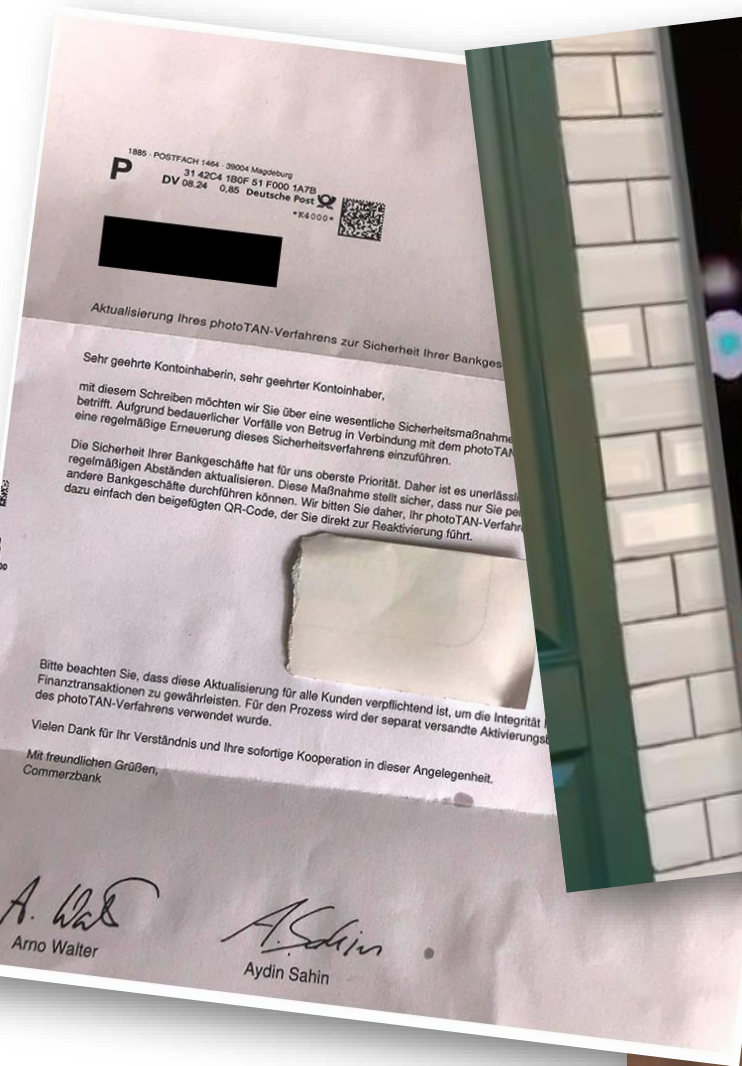
Vorsicht Quishing: Wie man gefälschte QR-Codes an der Ladesäule erkennt

QR-Codes begegnen uns heute überall: auf Plakaten, in Restaurants, beim Ticketkauf – und auch an Ladesäulen für Elektroautos. Die kleinen, schwarz-weißen Quadrate haben viele Vorteile, werden jedoch immer häufiger von Kriminellen für das sogenannte Quishing genutzt. Wir erklären, wie die Betrugsmasche funktioniert und wie man gefälschte QR-Codes erkennt und sich schützen kann.

Kriminelle nutzen Quishing mittlerweile auch, um E-Auto-Fahrer*innen vor allem beim Bezahlen an öffentlichen Ladesäulen zu täuschen. Dabei nutzen sie manipulierte QR-Codes, um ihre Opfer auf gefälschte Webseiten zu lotsen und sensible Daten abzugreifen. Neben E-Mail-Adressen und Passwörtern haben es die Kriminellen vor allem auf Kreditkartendaten abgesehen. Die Zeitschrift Auto Motor und Sport berichtete bereits über erste Fälle, auch der ADAC und die Verbraucherzentrale warnen vor einer steigenden Gefahr.

Warum Schutz für Devices wichtig ist.

QR Code Phishing - Quishing



Warum Schutz für Devices wichtig ist.

Angriffe auf Smartphones

bechtle

NEWS > CYBERSECURITY AND DATA PROTECTION

Brussels spyware bombshell: Surveillance software found on officials

EU Parliament defense committee email says.

Apple alerts users in 92 nations to mercenary spyware attacks

Manish Singh @refsrc / 6:54 AM GMT+2 • April 11, 2024

Apple lässt wieder Piraten-Software in den App Store

Schon in der Vergangenheit waren problematische iPhone-Anwendungen bei Apples App Review "durchgerutscht". Nun kam es zu einem neuerlichen Fall.

🔒 🔊 🖨️ 💬 29

EINFALLSTOR SMARTPHONE: WIE HACKERANGRIFFE AUF HANDYS UNTERNEHMEN BEDROHEN

Juli 5, 2025 | Hackerangriff, Cybersisiko, IT-Sicherheit | 0



Smartphones erleichtern vieles, öffnen aber auch Einfallstore für Hacker. Cyberangriffe über Apps, Messenger oder WLAN-Netze haben in den vergangenen Jahren deutlich zugenommen. Prominentes Opfer: Jeff Bezos. Das Handy des Amazon-Gründers wurde über ein WhatsApp-Video mit Schadsoftware infiziert, die Daten ausspionierte. Lesen Sie hier, welche Angriffsmethoden beliebt sind und wie sich Unternehmen schützen können.

Angriffe auf Handys im Minutentakt

Das Smartphone hat für viele Menschen den herkömmlichen Computer als Zugangsgerät zum

Golem | Followed by 20+ million | Anmelden

SPIONAGE AUF DEM IPHONE
Neue Sp...

The Hacker News | #1 Trusted Cybersecurity News Platform

WIZ SECURING AI AGENTS 101
A Quick Intro for Security Teams

WhatsApp Patches Zero-Click Exploit Targeting iOS and macOS Devices
Zero-Day / Vulnerability
Aug 30, 2025 | Ravie Lakshmanan

DEFENDING THE WORLD'S MOST SENSITIVE NETWORKS
LEARN THE SECRET OF ELITE SOCS

Another Day, Another Firewall Patch
It's time to reduce cost and complexity
REMOVE YOUR ATTACK SURFACE

Trending News
Hackers Abuse Blockchain Smart Contracts to Spread Malware via Infected WordPress Sites

WhatsApp has addressed a security vulnerability in its messaging apps for Apple iOS and macOS that it said may have been exploited in the wild in conjunction with a recently disclosed Apple flaw in targeted zero-day attacks.

The vulnerability, CVE-2025-55177 (CVSS score: 5.4), relates to a case of insufficient authorization of linked device synchronization messages. Internal researchers on the WhatsApp Security Team have been credited with discovering and rerating the bug.

The Meta-owned company said the issue "could have allowed an unrelated user to trigger processing of content from an arbitrary URL on a target's device."

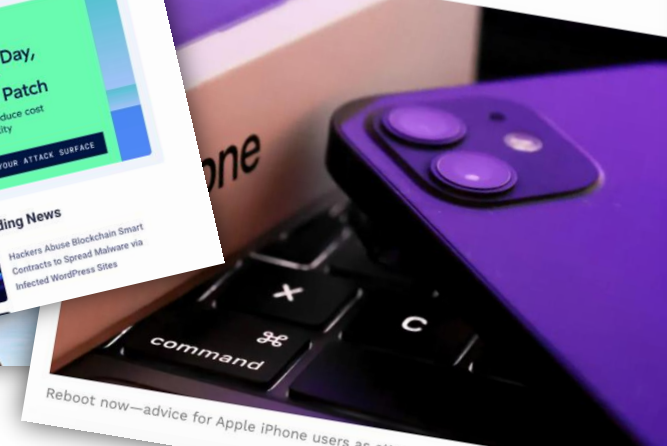
Politicians have been taking their...
FEBRUARY 21, 2024 1:01 PM CET
BY ANTOANETA ROUSSI

FORBES > INNOVATION > CYBERSECURITY

Reboot Your iPhone—Warning As Hackers Target Apple Users

Zak Doffman Contributor @ Zak Doffman writes about security, surveillance and privacy.

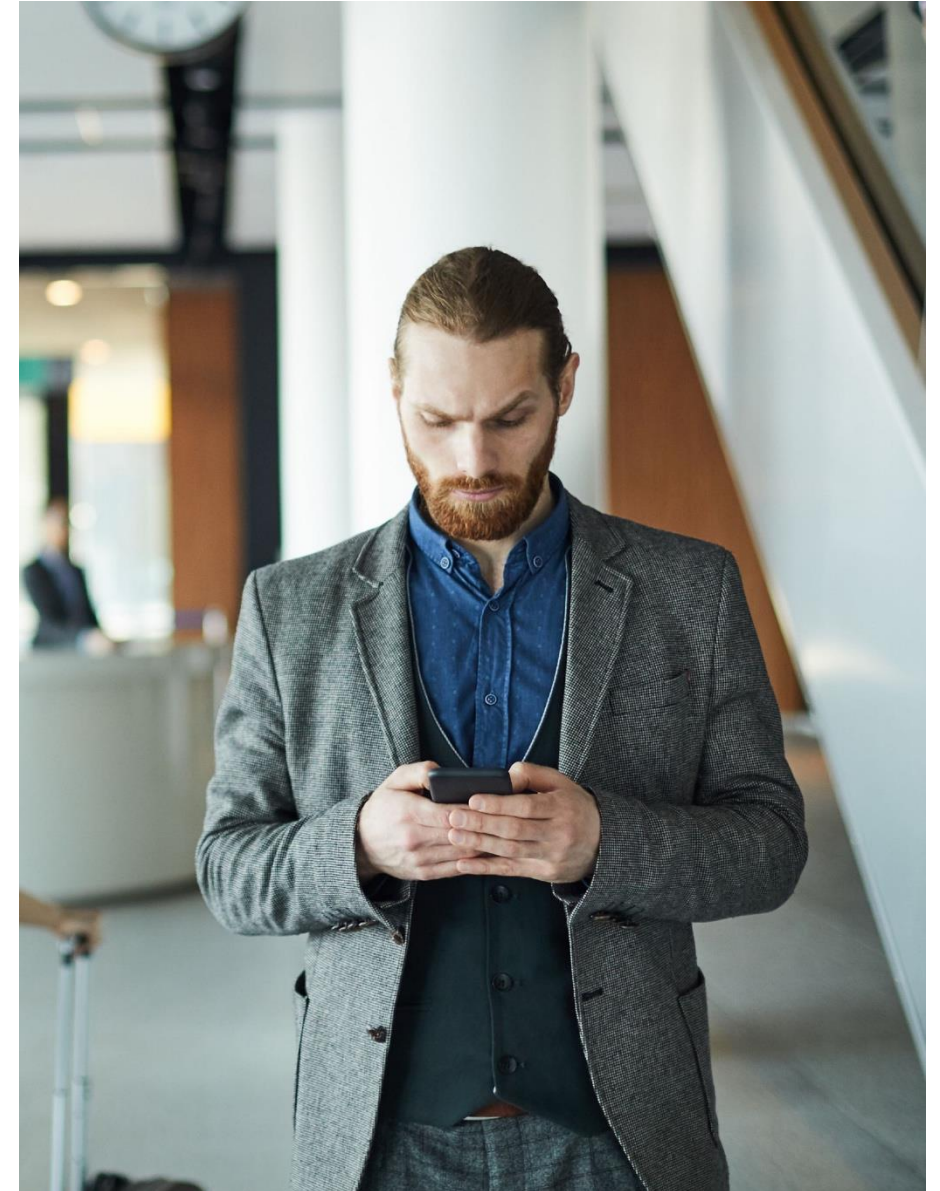
dated Nov 2, 2024, 09:43am EDT



Absicherung von Smartphones hat andere Herausforderungen

Die Nutzung von iPhones, iPads bzw. Androids auf der ganzen Welt führt dazu, dass finanzstarke und nationalstaatliche Akteure ihren Fokus neu ausrichten.

- ▶ Zielgerichtete Spionageprogramme entwickeln sich rasant weiter
- ▶ **Phishing-Angriffe** sind auf dem Handy 50% erfolgreicher
- ▶ Gezielte Nutzer sind **überall mit dem Unternehmen verbunden**
- ▶ **Side-Loading-Apps für iOS können die Bedrohungslandschaft verändern**



Smartphones sind das schwächste Glied

2FA

Wie es eigentlich sein sollte



Login



2FA-Token vom **zweiten** Gerät



Unternehmensdaten

Same FA

Wie es auf dem Handy ist



Login

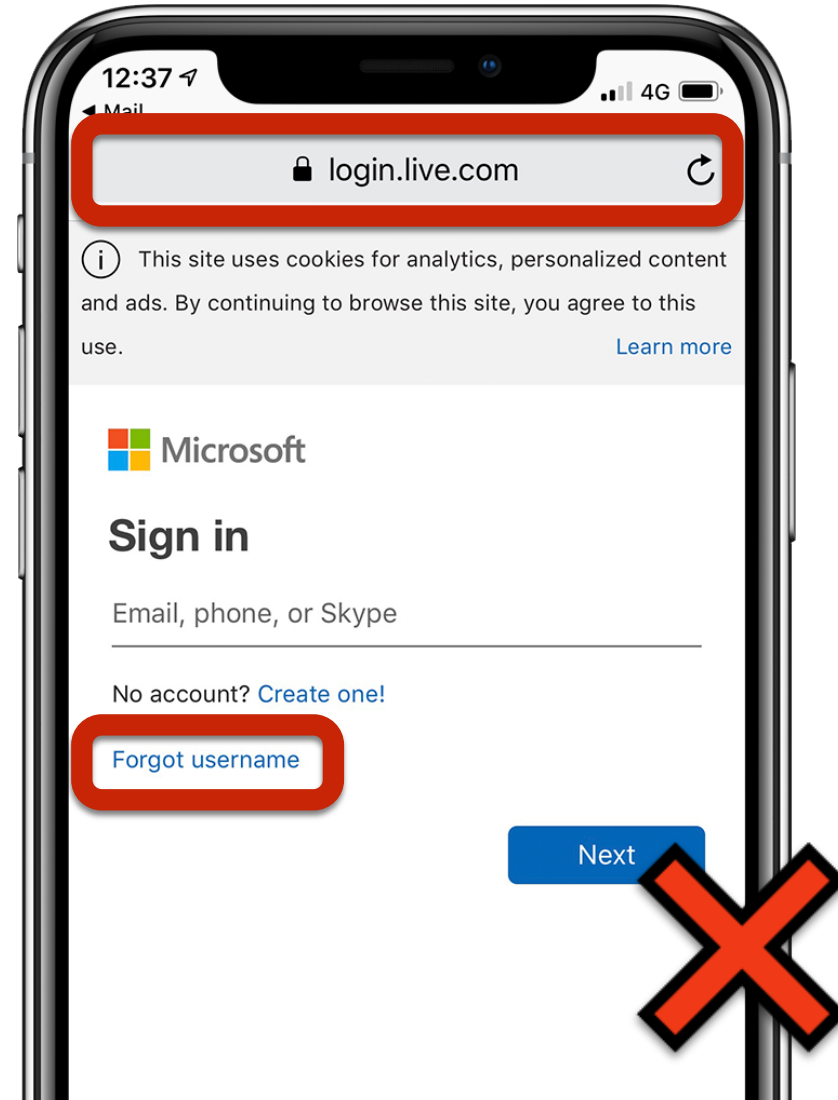
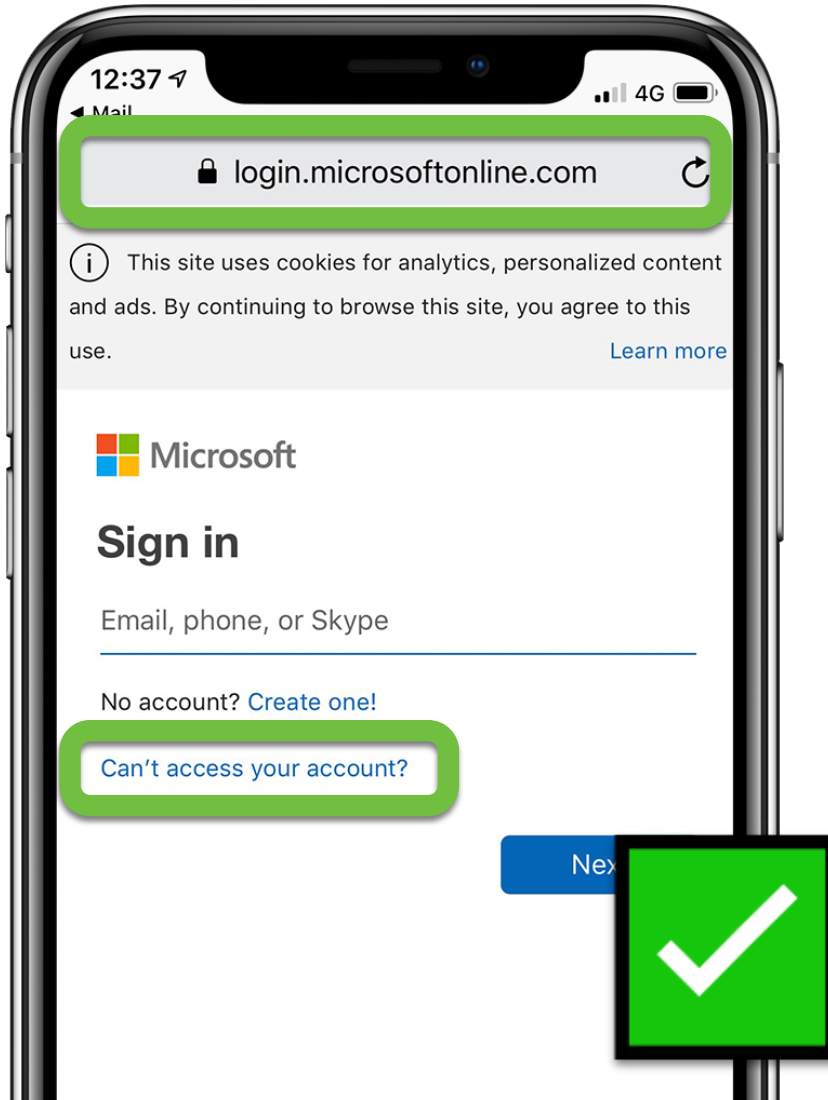


2FA-Token auf **demselben** Gerät



Unternehmensdaten

Welche Anmeldeseite ist echt?



Analysen mobiler Malware

Jamf Threat Labs discovers apps that leak credentials

Two mobile apps available for download were found leaking personally identifiable information. Jamf Threat Labs investigates.

September 17 2025 by Jamf Threat Labs



Author: Michal Rajčan

During Jamf Threat Labs continuous threat investigation we came across two apps leaking credentials and Personally Identifiable Information (PII). One is from a Malaysian

Predator's kill switch: undocumented anti-analysis techniques in iOS spyware

A deep dive into the error code taxonomy and detection mechanisms that prior research didn't cover.

January 14 2026 by Jamf Threat Labs

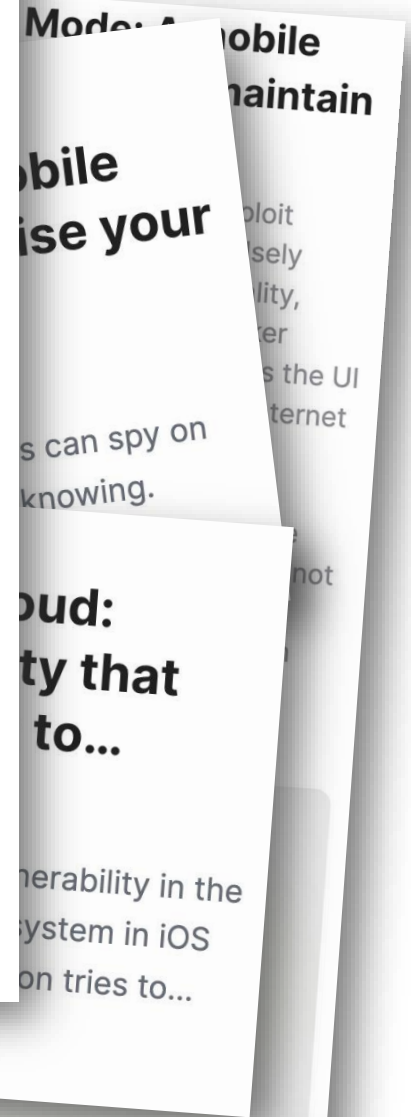
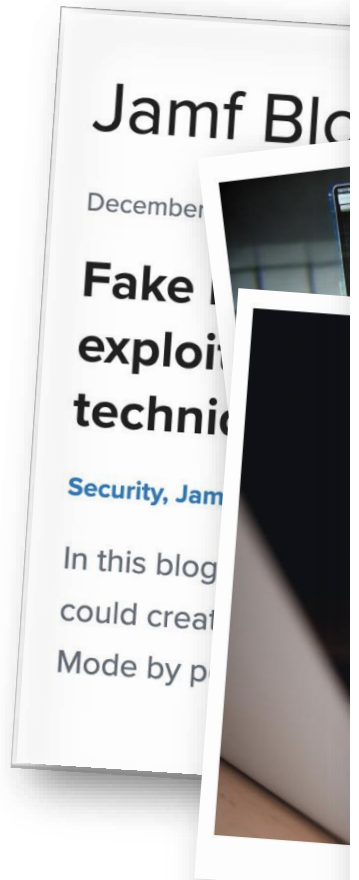


By: Shen Yuan and Nir Avraham

Introduction

In December 2025, Google's Threat Intelligence Group (GTIG) published extensive research on Intellexa's Predator

[Read More](#) →



Mac ist kein Nischenprodukt mehr

Key Trends bei Cyberangriffen in Unternehmen

- Mac ist kein Nischenprodukt mehr
 - Mac Marktanteil ist von 2024 auf 2025 um 16,4% gewachsen auf fast 10%
 - Edas größte Wachstum im Markt
- Infostealers entwickeln sich und stehlen mehr daten als jeh zuvor
- APT-Gruppen haben weiterhin ein Auge auf macOS (Advanced Persistent Threats)
- Mac und Windows Computer sind unterschiedlich
 - Gatekeeper
 - System Integrity Protection (SIP)
 - Transparency, Consent and Control (TCC)

Basis des Reports:

- 26.000 individuelle Malware Beispiele wurden in 2025 von Jamf Threat Labs in die Datenbank aufgenommen



Key Findings

44%

of devices have malicious network traffic

Attackers are always trying to compromise your devices. Detecting and containing malicious traffic requires constant diligence — and the right tools.

41%

of devices have critically out-of-date operating systems

Enforcing minimum software versions ensures devices have the latest patches, reducing the number of known exploitable vulnerabilities.

50%

of malware affecting Mac were trojans

Trojans topped the charts, increasing by over 33 percentage points since 2024. They are back doors into your systems, leaving lasting damage.

73%

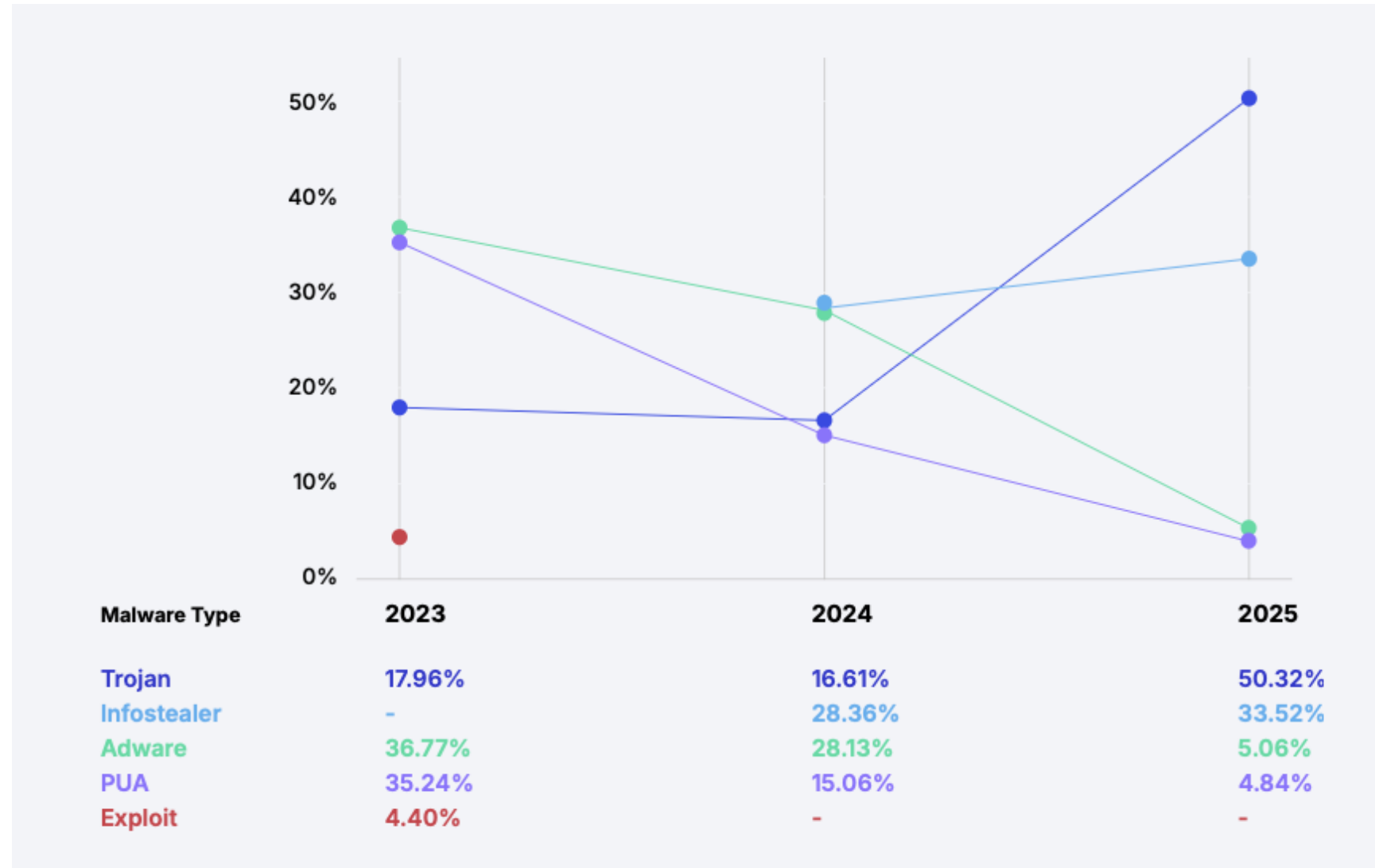
of devices have vulnerable apps

Apps can contain vulnerable libraries, suffer supply chain compromises or mishandle data. Knowing what's installed is critical to managing risk.

Malware Trends

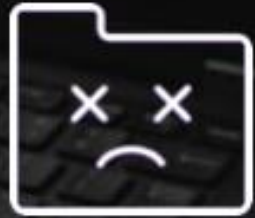
- Trojaner – der größte Gewinner:
 - Anstieg von Trojaner-Angriffen auf 50,32% in 2025

- Infostealers – von Null auf ein Drittel:
 - Von irrelevant in 2023 auf 33,52% in 2025 gewachsen
 - Infostealers stehlen Zugangsdaten, Passwörter, Krypto-Wallets und andere sensible Daten



**MDM alone won't cut
it anymore.**

***Endpoints need security capabilities
that are "built right in"***



**Windows
first security
tools**




**Lack of
real-time
visibility**



**Patching
and OS
delays**

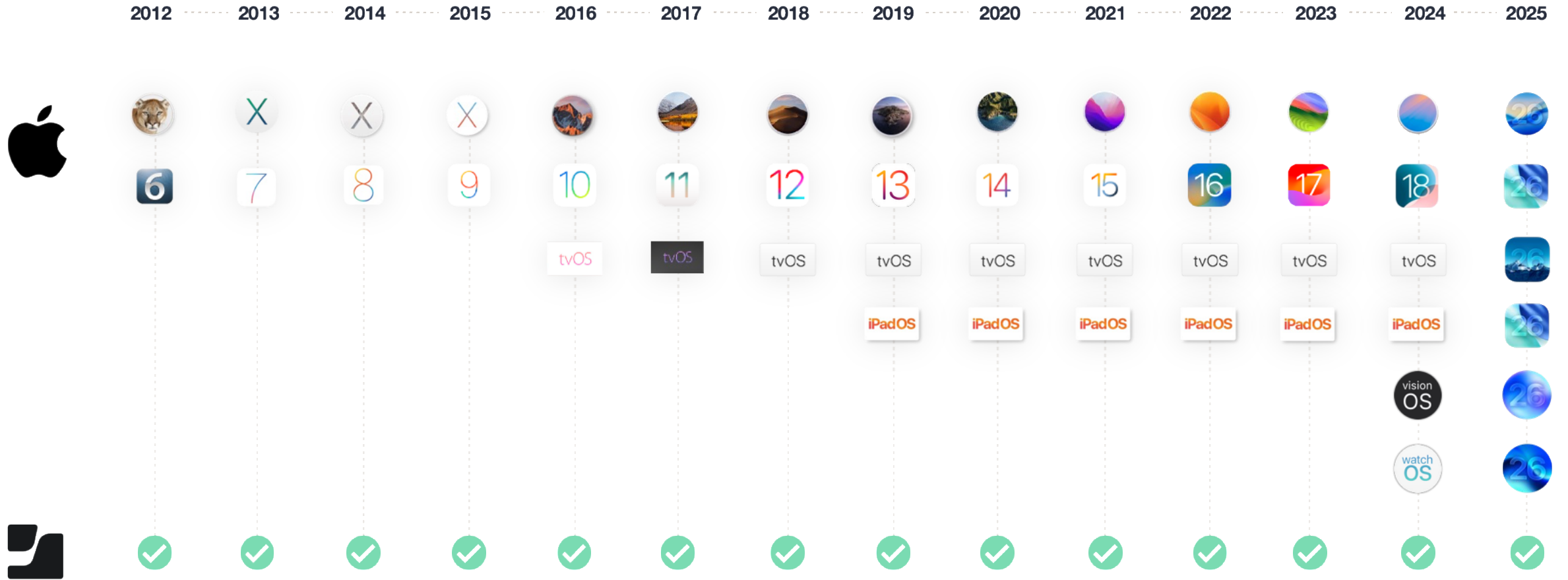
Software Update

This Mac is enrolled in the
Apple Developer Beta
Program  **jamf**
Details...

Device Management, Secure Device, and Secure Access



Same-Day Support



Features, die der Mac bietet und die Genutzt werden sollten

- Zero-Touch Deployment
- Audit against industry benchmarks
- Vollständige Ausnutzung von Declarative Device Management
- Same-Day Support
- Nur autorisierte Nutzer mit compliant Devices können auf Arbeitsressourcen zugreifen
- Real-time security data
- Web Protection
- Endpoint threat prevention

Die Grenzen von "normaler" Security

**Mobile Threat
Defense**



**Advanced
detection &
forensics**

Jamf Mobile Forensic

Erkennt die raffiniertesten mobilen Angriffe

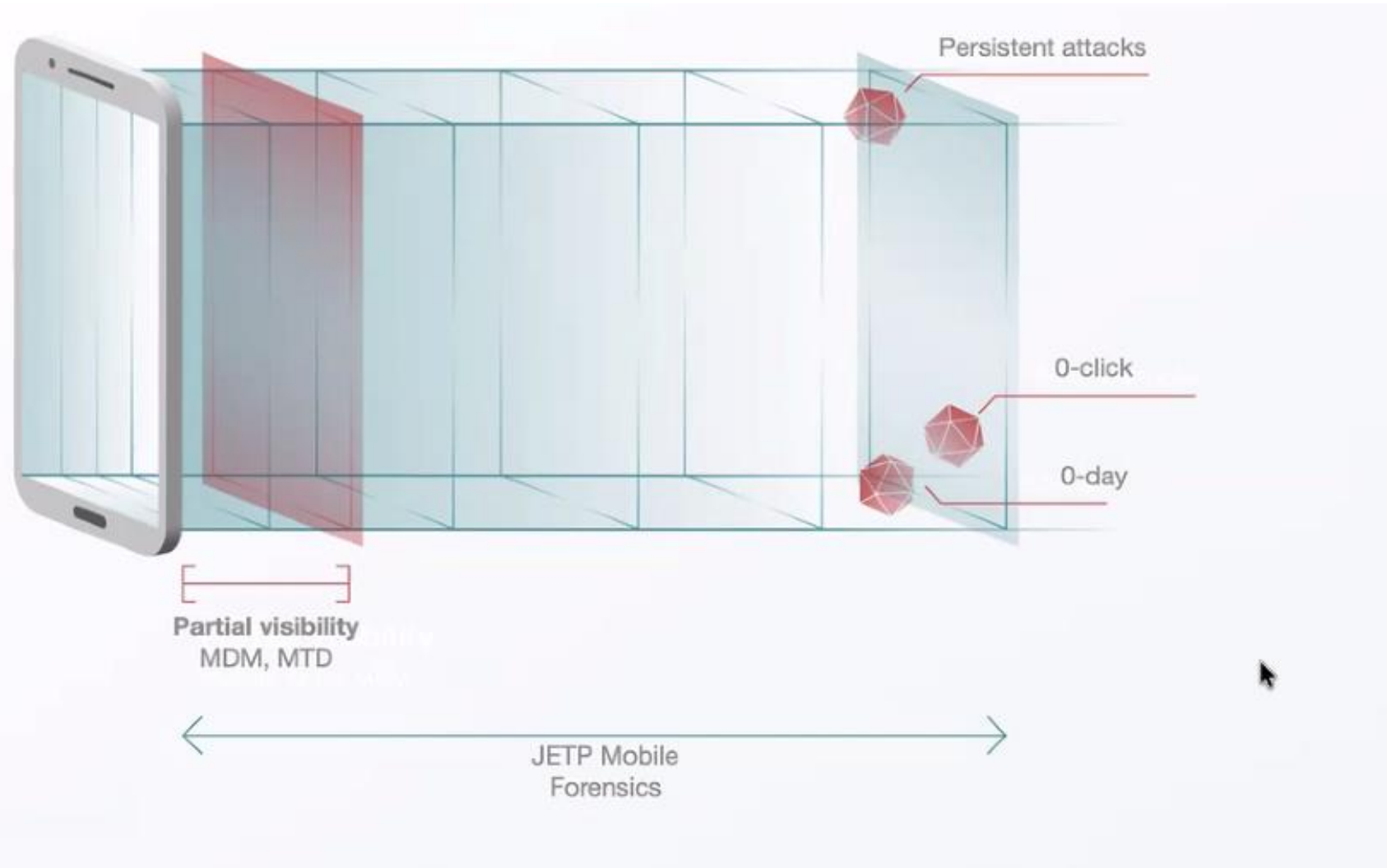
Erstellt eine Zeitleiste mit verdächtigen Ereignissen

Auswahl von Angriffen, die erkannt werden

- Zero- or 1-Click Attacks
- Advanced Persistent Threats (APT)
- Exploits and Payloads
- Indicators of Compromise (IoC)
- Suspicious Errors und Reboots



Jamf Mobile Forensic Advantage: Data Depth



Beacon by Jamf Threat Labs

Dedicated threat hunting service for macOS environments.

Our years of Mac expertise on Mac threat vectors allows us a deep understanding of:

- The tactics, techniques and procedures of macOS threat actors
- How to identify and analyze gaps in macOS configurations
- The macOS vulnerabilities that threat-actors exploit



Manage and Secure Apple at Work

75,900+

Active Jamf customers

32.8M+

Devices running Jamf

100k+

Jamf Nation members

7 of the Top 10

Technology companies as ranked by Fortune

of the Top 25

Most valuable brands as ranked by Forbes

15 of the Top 15

Largest U.S. banks by total assets according to bankrate.com

MARKET VALIDATION

IDC MarketScape Worldwide Unified Endpoint Management Software for Apple Devices



