Home

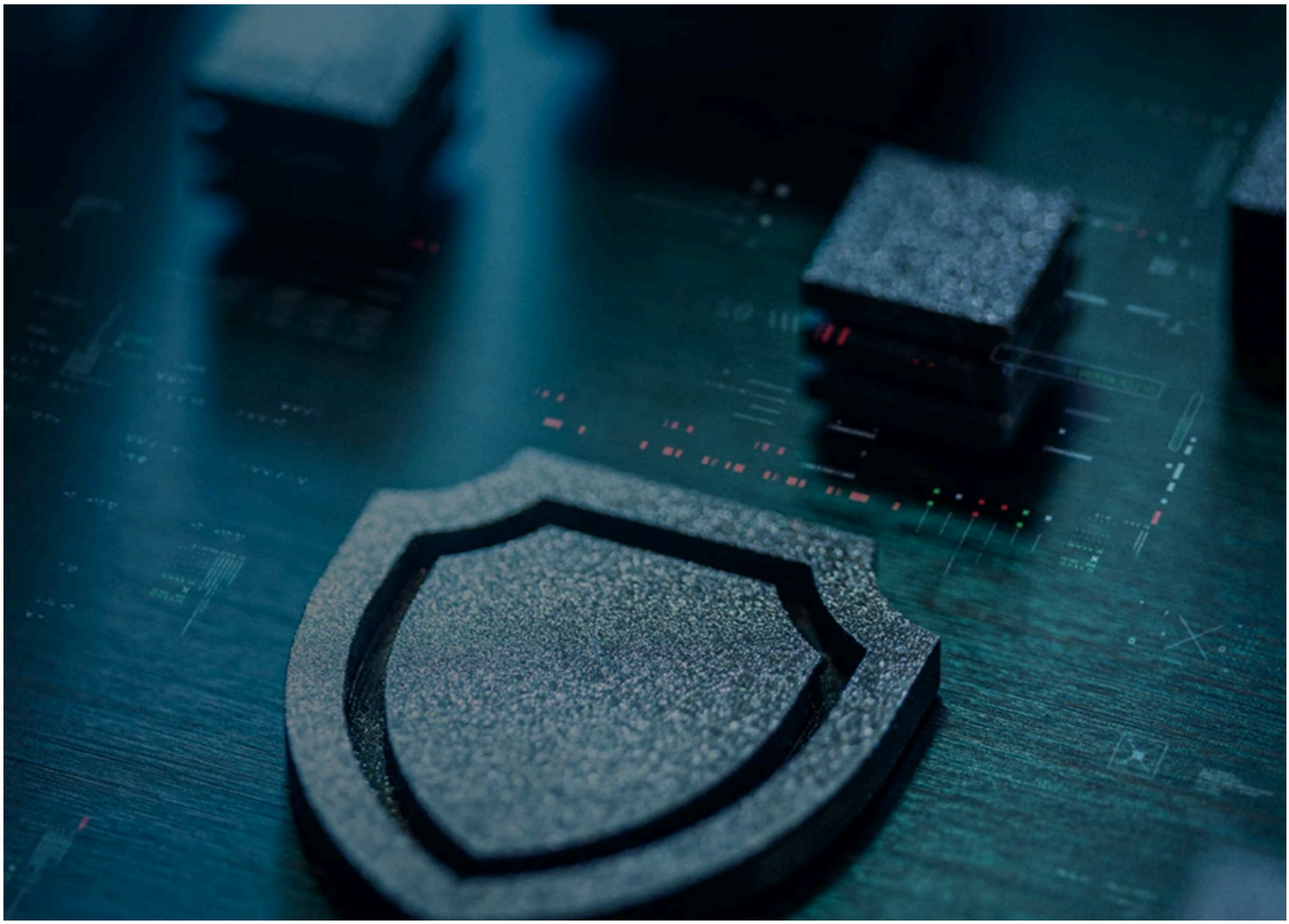
Cyber Shield blogs

Turning threat intelligence into cyber insight

Find expert-curated threat intelligence discoveries, technical breakdowns, and proactive defense insights directly from the Atos Threat Research Center(TRC).

Our cybersecurity services >

Digital Security Magazine >





The Threat Research Center content is currently being migrated to this platform. Previously published research articles will be progressively restored over the coming days. We apologize for any inconvenience during this transition.

Articles

- Mimori Ransomware is new. Its operators probably are not. >
- Inside INC ransomware: Behind AI-Driven operations >
- Eclipse ransomware - Tradecraft exposed through a leaked C2 server >
- EtherRAT distribution spoofing administrative tools via GitHub Facades >

Campaign KCPhoenix: Inside Silver Fox's latest ValleyRAT chain >

From prompt to phish >

Living off DENO >

Behind the fake AnyDesk: Tracking a Silver Fox-Linked ValleyRAT Campaign >

Exploiting trust in the vendor - cybersecurity provided binary turned malicious >

Abuse of Apache APISIX: Misconfigurations in the wild >

ASAR archives: An overlooked blind spot >

When installing AI turns risky: The rising scale of the campaigns targeting Claude code users >

Rising usage of Apple Developer Certificates for signing Windows malware >

Malicious Proxyware Campaign distributed via Microsoft Store >

Domain Spoofing >

Anatomy of access: Windows device objects from a security perspective >

Investigating a new Click-fix variant >

Distributed Denial of 2023? >

Writeup Drive Hackthebox >

From zero to certificate hero. The 5 Steps to a mature Certificate Lifecycle Management >

Insider Threat – What if the Big Bad Wolf was already in? >

CA/Browser Forum S/MIME Certificate Requirements: what is it and what to do about it? >

Snake Malware >

Cl0p Ransomware Group activity related to data leaks from GoAnywhere MFT >

Are privacy-enhancing technologies the holy grail to privacy? >

10 security tips to protect your organizations against ransomware >

The Invisible Danger of Exposed QR Codes and Account Recovery Artifacts >

Missing TLS Certificate Validation leading to RCE >

DLL Hijacking in EfficientLab Controlio (cloud-based employee monitoring service) >

Broken Access Control in Config Endpoint in LiteLLM >

Exposed Private Key of X.509 Certificate in SAP HANA Cockpit & SAP HANA Database Explorer >

Improper Enforcement of Locked Accounts in WebUI (SSO) in Kiuwan SAST on-premise (KOP) & cloud/SaaS >

Broken Access Control in Open WebUI >

Local Privilege Escalation in Vienna Assistant (MacOS) – Vienna Symphonic Library >

Multiple Privilege Escalation Vulnerabilities in Arturia Software Center MacOS >

Multiple vulnerabilities in PEGA Infinity platform >

Making Vulnerable Drivers Exploitable Without Hardware – The BYOVD Perspective >

Analysis of Ivanti 0-days, CVE-2023-46805 and CVE-2024-21887 >

Citrix NetScaler flaw exposing sensitive data >

Using EDR telemetry for offensive research >

Downfall Vulnerability (CVE-2022-40982) >

Roaming and racing to get SYSTEM – CVE-2023-37250 >

Detailed analysis of the Zero-Day vulnerability in MOVEit transfer >

Creating persistent local privilege escalation with temporarily elevated legitimate installers >

Attacking local self-protection mechanisms – a case study of CVE-2019-3613 and CVE-2022-3859 >

Outlaw APT group – From initial access to crypto mining >

BumbleBee hunting with a Velociraptor >

SOCCRATES – Automation and Orchestration of Security Operations >

How to build an agile SOC? >

AI-based detections in SOC >

CISO's perspectives – The 4 recommendations to sleep without a worry >

Ethical Boundaries of Independent Security Research in the Consumer Pet Tracking Ecosystem >

Multiple Vulnerabilities in Quanos Content Solutions SCHEMA ST4 >

Multiple Critical Vulnerabilities in Sprecher Automation SPRECON-E-C/-E-P/-E-T3 >

Broken Access Control in syracom AG Secure Login (2FA) for Atlassian >

Multiple Vulnerabilities in Wertheim SafeController Hardware for VAULT ROOMS

Multiple Critical Vulnerabilities in Wertheim SafeController Software for VAULT ROOMS >

Local Privilege Escalation in Slate Digital Connect (macOS) >

Hardcoded Root Cloud Credentials in Application Binaries in Silver Leaf Technologies >

Multiple Local Privilege Escalation Vulnerabilities in Waves Audio >

Privilege Escalation via Binary Planting in Genetec-provided RabbitMQ >

A tale of several hijacks and what it taught me about runtime-driven testing >

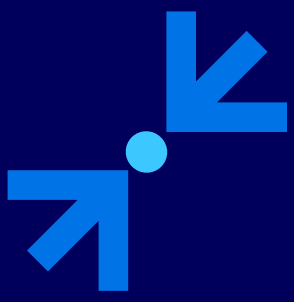
Multiple cross-site scripting vulnerabilities in VertiGIS WebOrderSystem >

Improper device certificate validation enables AiTM attacks in Siemens SICAM Toolbox II device communication >

Subscribe to Cyber shield blogs to stay one step ahead of evolving threats

Receive expert-curated threat intelligence discoveries, technical breakdowns, and proactive defense insights directly from the Atos Threat Research Center (TRC).

Loading form...



Discover our Cybersecurity Services

and get in touch with our experts to discuss how we can help transform your IT infrastructure.

Services >

Industries >

News and Insights >

About us >

Careers >

Follow us and interact

© 2026 Atos Group. All rights reserved. Accessibility Statement Terms of use Integrity Line Privacy

Cookie Settings Contact us

ATOS GROUP

Accelerating intelligence