

---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20250313



## Inhaltsverzeichnis

<b>1 Editorial</b>	<b>2</b>
<b>2 Security-News</b>	<b>3</b>
2.1 Heise - Security-Alert . . . . .	3
<b>3 Sicherheitslücken</b>	<b>3</b>
3.1 EPSS . . . . .	3
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit . . . . .	3
3.2 BSI - Warn- und Informationsdienst (WID) . . . . .	5
3.3 Sicherheitslücken Meldungen von Tenable . . . . .	8
<b>4 Die Hacks der Woche</b>	<b>10</b>
4.0.1 Information Stealer. Wie funktionieren sie? . . . . .	11
<b>5 Cyberangriffe: (Mär)</b>	<b>12</b>
<b>6 Ransomware-Erpressungen: (Mär)</b>	<b>12</b>
<b>7 Quellen</b>	<b>22</b>
7.1 Quellenverzeichnis . . . . .	22
<b>8 Impressum</b>	<b>23</b>

## 1 Editorial

Guten Morgen,

willkommen zum Cybersecurity Morgenreport von Cyberwald, Ihrem täglichen Begleiter in der Welt der IT-Sicherheit. Als nicht-kommerzielles Projekt ist es unser Anliegen, Awareness und Wissen rund um das Thema Cybersecurity kostenlos zu vermitteln. In der heutigen digitalen Welt ist es für Unternehmen von entscheidender Bedeutung, sich über aktuelle Sicherheitsrisiken zeitnah zu informieren. Cyberbedrohungen entwickeln sich ständig weiter und können erhebliche Schäden verursachen, wenn sie nicht rechtzeitig erkannt und abgewehrt werden. Durch die Nutzung aktueller Informationen können Unternehmen ihre IT-Sicherheitsmaßnahmen stärken und sich effektiv gegen diese Bedrohungen schützen.

Unser Ziel ist es, Ihnen, den IT-Verantwortlichen, einen kompakten und leicht verständlichen Überblick über aktuelle Sicherheitsrisiken zu geben. Wir präsentieren Ihnen täglich Sicherheitsmeldungen und Berichte über neue Sicherheitslücken, die Ihre Systeme und Daten bedrohen könnten.

Darüber hinaus listen wir aktuelle Cyberangriffe und Ransomware-Vorfälle auf. Dies ist von besonderer Bedeutung, da es Unternehmen ermöglicht, sich auf mögliche Supply-Chain- und Phishing-Angriffe vorzubereiten. Durch das Verständnis der Methoden und Taktiken, die von Cyberkriminellen verwendet werden, können Unternehmen ihre Verteidigungsmaßnahmen entsprechend anpassen und stärken.

Für den Cybersecurity Morgenreport greifen wir automatisiert auf öffentliche Informationsquellen zu, filtern und sortieren diese Informationen, um sie Ihnen in einer übersichtlichen Form zur Verfügung zu stellen. Wir bemühen uns, die Inhalte so verständlich wie möglich zu gestalten und vorzugsweise vollständig in deutscher Sprache wiederzugeben. Bei Bedarf übersetzen wir die öffentlichen Informationen und fassen sie durch eine KI zusammen.

Der Cybersecurity Morgenreport ist ein dynamisches Projekt. Wir passen und erweitern unsere Inhalte ständig, um Ihnen die relevantesten und aktuellsten Informationen zu liefern. Derzeit befinden wir uns im Alpha-Stadium des Projekts und freuen uns über Ihr Feedback und Ihre Anregungen.

Wir hoffen, dass der Cybersecurity Morgenreport Ihnen hilft, Ihre IT-Sicherheitsmaßnahmen zu verbessern und Ihre Systeme vor den ständig wechselnden Bedrohungen zu schützen. Bleiben Sie sicher und informiert mit dem Cybersecurity Morgenreport von Cyberwald.

Ihr Cyberwald-Team

## 2 Security-News

### 2.1 Heise - Security-Alert

## 3 Sicherheitslücken

Eine Sicherheitslücke oder Schwachstelle ist ein Fehler in einer Software oder Hardware, der es einem Angreifer ermöglicht, in ein Computersystem einzudringen und Schaden anzurichten. Diese Lücke stellt eine Bedrohung für die Sicherheit des Systems dar, da sie ausgenutzt werden kann, um das System zu kompromittieren. Sicherheitslücken entstehen oft durch unzureichenden Schutz des Computers vor Netzwerkangriffen, zum Beispiel durch fehlende Firewall oder andere Sicherheitssoftware. Auch Programmierfehler im Betriebssystem, Webbrowser oder anderen Anwendungen können Sicherheitslücken verursachen. Bekannte Sicherheitslücken sollten daher so schnell wie möglich durch das Einspielen eines Patches geschlossen werden, um die Angriffsfläche der IT-Systeme zu verringern.

### 3.1 EPSS

Das Exploit Prediction Scoring System wird für eine bekannte Software-Sicherheitslücke / CVE auf einer Skala von 0 (0%) bis 1 (100%) angegeben und soll die Wahrscheinlichkeit für das Auftreten eines Exploits in naher Zukunft darstellen. Ein höherer Wert bedeutet eine höhere Wahrscheinlichkeit, dass eine Schwachstelle in naher Zukunft ausgenutzt wird. EPSS kann auch als Rahmen für die Priorisierung von Schwachstellen unter Verwendung einer Kombination von Metriken betrachtet werden. Es soll Unternehmen dabei helfen, ihre Ressourcen effizienter zu verteilen und alle relevanten Cyber-Risiken zu minimieren.

#### 3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2025-0108	0.967640000	0.997970000	<a href="#">Link</a>
CVE-2024-9474	0.974550000	0.999800000	<a href="#">Link</a>
CVE-2024-9465	0.939910000	0.993880000	<a href="#">Link</a>
CVE-2024-9463	0.961860000	0.996700000	<a href="#">Link</a>
CVE-2024-8963	0.966010000	0.997640000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-7593	0.967730000	0.997990000	<a href="#">Link</a>
CVE-2024-6670	0.904230000	0.991230000	<a href="#">Link</a>
CVE-2024-5910	0.967120000	0.997860000	<a href="#">Link</a>
CVE-2024-55956	0.968970000	0.998310000	<a href="#">Link</a>
CVE-2024-53704	0.960740000	0.996530000	<a href="#">Link</a>
CVE-2024-5217	0.945850000	0.994490000	<a href="#">Link</a>
CVE-2024-50623	0.969520000	0.998470000	<a href="#">Link</a>
CVE-2024-50603	0.927520000	0.992800000	<a href="#">Link</a>
CVE-2024-4879	0.950100000	0.995020000	<a href="#">Link</a>
CVE-2024-4577	0.951770000	0.995220000	<a href="#">Link</a>
CVE-2024-4358	0.921450000	0.992390000	<a href="#">Link</a>
CVE-2024-41713	0.955390000	0.995680000	<a href="#">Link</a>
CVE-2024-40711	0.964240000	0.997240000	<a href="#">Link</a>
CVE-2024-4040	0.966350000	0.997730000	<a href="#">Link</a>
CVE-2024-38856	0.941790000	0.994050000	<a href="#">Link</a>
CVE-2024-36401	0.961880000	0.996710000	<a href="#">Link</a>
CVE-2024-3400	0.958850000	0.996200000	<a href="#">Link</a>
CVE-2024-3273	0.937240000	0.993630000	<a href="#">Link</a>
CVE-2024-32113	0.938440000	0.993730000	<a href="#">Link</a>
CVE-2024-28995	0.970760000	0.998800000	<a href="#">Link</a>
CVE-2024-28987	0.957000000	0.995900000	<a href="#">Link</a>
CVE-2024-27348	0.961750000	0.996680000	<a href="#">Link</a>
CVE-2024-27198	0.970340000	0.998680000	<a href="#">Link</a>
CVE-2024-24919	0.966210000	0.997680000	<a href="#">Link</a>
CVE-2024-23897	0.973580000	0.999570000	<a href="#">Link</a>
CVE-2024-2389	0.928740000	0.992880000	<a href="#">Link</a>
CVE-2024-23692	0.967310000	0.997920000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-21893	0.960410000	0.996470000	<a href="#">Link</a>
CVE-2024-21887	0.973690000	0.999610000	<a href="#">Link</a>
CVE-2024-20767	0.964870000	0.997370000	<a href="#">Link</a>
CVE-2024-1709	0.957060000	0.995910000	<a href="#">Link</a>
CVE-2024-1212	0.946600000	0.994580000	<a href="#">Link</a>
CVE-2024-0986	0.954890000	0.995610000	<a href="#">Link</a>
CVE-2024-0195	0.962680000	0.996890000	<a href="#">Link</a>
CVE-2024-0012	0.969610000	0.998490000	<a href="#">Link</a>

### 3.2 BSI - Warn- und Informationsdienst (WID)

Wed, 12 Mar 2025

**[UPDATE] [hoch] libxml2: Mehrere Schwachstellen**

Ein lokaler Angreifer kann mehrere Schwachstellen in libxml2 ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen oder einen nicht näher spezifizierten Angriff zu starten.

- [Link](#)

—

Wed, 12 Mar 2025

**[NEU] [hoch] Linux Kernel: Mehrere Schwachstellen ermöglichen Denial of Service**

Ein Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um einen Denial of Service Zustand herbeizuführen und um nicht näher beschriebene Auswirkungen zu verursachen.

- [Link](#)

—

Wed, 12 Mar 2025

**[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um einen Denial of Service Zustand herbeizuführen oderum einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

—

Wed, 12 Mar 2025

**[NEU] [hoch] Microsoft Azure: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Microsoft Azure und Microsoft Azure CLI ausnutzen, um erhöhte Privilegien zu erlangen oder beliebigen Programmcode auszuführen.

- [Link](#)

—

Wed, 12 Mar 2025

**[NEU] [kritisch] Webkit / Apple : Schwachstelle ermöglicht Umgehung von Sicherheitsmechanismen**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Webkit und in Apple iOS, Apple iPadOS, Apple macOS und Apple Safari ausnutzen, um Sicherheitsmechanismen zu umgehen.

- [Link](#)

—

Wed, 12 Mar 2025

**[NEU] [hoch] FreeType: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in FreeType ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Wed, 12 Mar 2025

**[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Privilegieneskalation**

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Wed, 12 Mar 2025

**[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Privilegieneskalation**

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Wed, 12 Mar 2025

**[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen**

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand zu verursachen und seine Privilegien zu erweitern.

- [Link](#)

—

Wed, 12 Mar 2025

**[UPDATE] [hoch] Linux Kernel (vmwgfx): Mehrere Schwachstellen**

Ein lokaler Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um Informationen offenzulegen und um seine Privilegien zu erweitern.

- [Link](#)

—

Wed, 12 Mar 2025

**[UPDATE] [hoch] FreeRDP: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff**

Ein Angreifer kann mehrere Schwachstellen in FreeRDP ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

—

Wed, 12 Mar 2025

**[UPDATE] [hoch] FreeRDP: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in FreeRDP ausnutzen, um Sicherheitsvorkehrungen zu umgehen oder einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

—

Wed, 12 Mar 2025

**[UPDATE] [hoch] Apple macOS: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apple macOS ausnutzen, um seine Privilegien zu erhöhen, einen Denial-of-Service-Zustand herbeizuführen, Spoofing-Angriffe durchzuführen, Daten zu ändern, Sicherheitsmaßnahmen zu umgehen und vertrauliche Informationen offenzulegen

- [Link](#)

—

Wed, 12 Mar 2025

**[UPDATE] [hoch] bluez: Schwachstelle ermöglicht Codeausführung**

Ein Angreifer aus einem angrenzenden Netzwerk kann eine Schwachstelle in bluez ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Wed, 12 Mar 2025

**[UPDATE] [hoch] Oracle Java SE: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Oracle Java SE ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- [Link](#)

—

Wed, 12 Mar 2025

**[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen ermöglichen Denial of Service**



Ein Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um einen Denial of Service Angriff durchzuführen oder nicht näher beschriebene Auswirkungen zu erzielen.

- [Link](#)

—

Wed, 12 Mar 2025

**[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen ermöglichen Denial of Service**

Ein Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um einen Denial of Service Zustand oder andere, nicht näher beschriebene Auswirkungen zu verursachen.

- [Link](#)

—

Wed, 12 Mar 2025

**[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen**

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um erhöhte Privilegien zu erlangen oder einen Denial of Service auszulösen.

- [Link](#)

—

Wed, 12 Mar 2025

**[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Linux und Ubuntu Linux ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Wed, 12 Mar 2025

**[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen**

Ein entfernter Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- [Link](#)

—

---

### 3.3 Sicherheitslücken Meldungen von Tenable

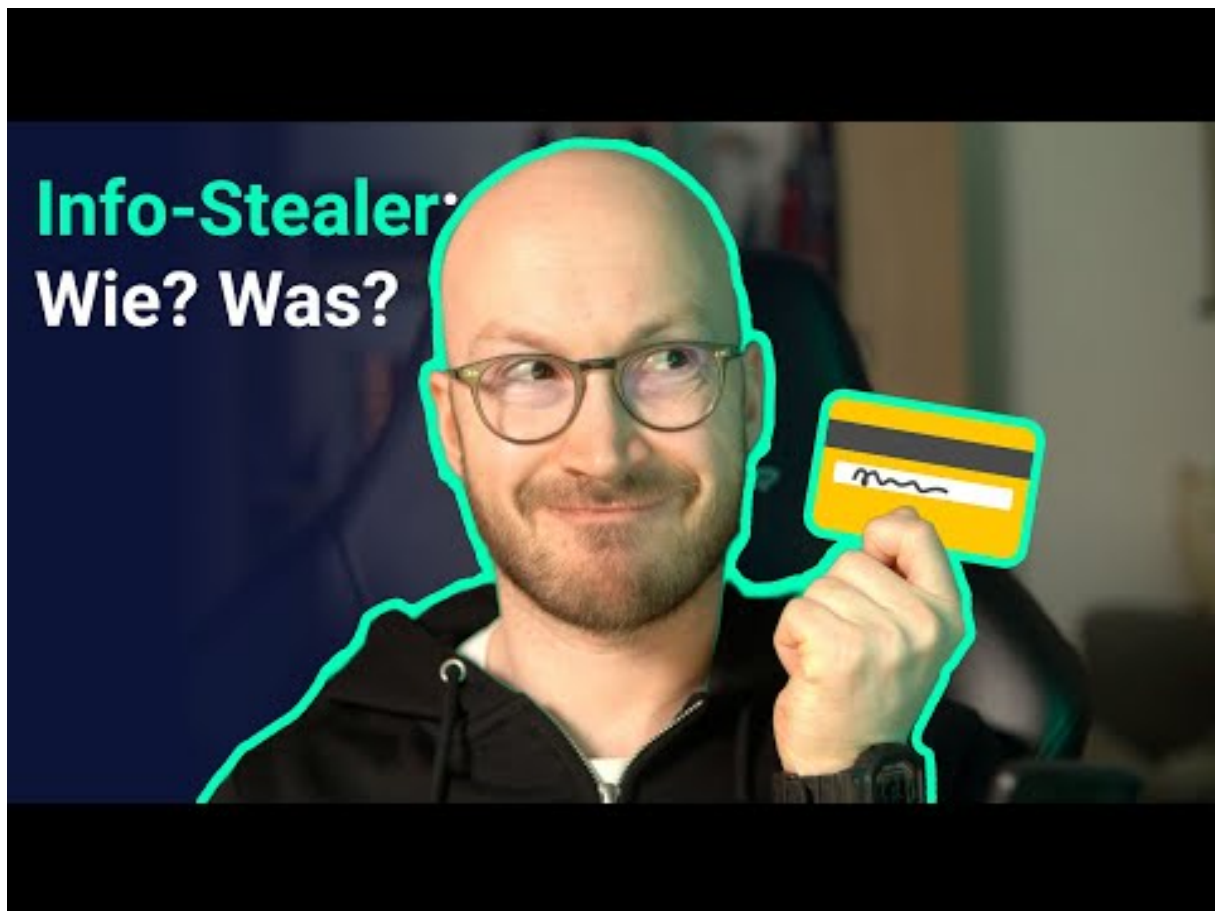
Datum	Schwachstelle	Bewertung
3/12/2025	[SPIP CMS < 4.1.16 / 4.2.x < 4.2.13 / 4.3.x < 4.3.0-alpha2 Remote Code Execution]	critical
3/12/2025	[Fedora 41 : thunderbird (2025-bd6664e83b)]	critical
3/12/2025	[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS : Netatalk vulnerabilities (USN-7347-1)]	critical
3/11/2025	[Ubuntu 24.04 LTS : FreeRDP vulnerabilities (USN-7341-1)]	critical
3/11/2025	[RHEL 8 : webkit2gtk3 (RHSA-2024:9646)]	critical
3/11/2025	[RHEL 8 : webkit2gtk3 (RHSA-2024:9636)]	critical
3/11/2025	[RHEL 8 : webkit2gtk3 (RHSA-2024:9679)]	critical
3/12/2025	[Apache Tomcat 11.0.0-M1 < 11.0.3 Remote Code Execution]	high
3/12/2025	[Apache Tomcat 10.1.0-M1 < 10.1.35 Remote Code Execution]	high
3/12/2025	[Apache Tomcat 9.0.0-M1 < 9.0.99 Remote Code Execution]	high
3/12/2025	[SimpleHelp Unauthenticated Path Traversal]	high
3/12/2025	[SUSE SLES15 Security Update : kernel (SUSE-SU-2025:0201-2)]	high
3/12/2025	[SUSE SLES15 Security Update : kernel (SUSE-SU-2025:0833-2)]	high
3/12/2025	[FreeBSD : chromium – multiple security fixes (a02a6d94-fe53-11ef-85f3-a8a1599412c6)]	high
3/12/2025	[SUSE SLES15 Security Update : kernel (SUSE-SU-2025:0835-1)]	high
3/12/2025	[SUSE SLES15 Security Update : kernel (SUSE-SU-2025:0577-2)]	high
3/12/2025	[SUSE SLES15 Security Update : kernel (SUSE-SU-2025:0833-1)]	high
3/12/2025	[SUSE SLES12 Security Update : kernel (SUSE-SU-2025:0834-1)]	high
3/12/2025	[Oracle Linux 9 : kernel (ELSA-2025-2627)]	high
3/12/2025	[Ubuntu 22.04 LTS / 24.04 LTS / 24.10 : .NET vulnerability (USN-7345-1)]	high

Datum	Schwachstelle	Bewertung
3/12/2025	[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : OpenSC vulnerabilities (USN-7346-1)]	high
3/12/2025	[HPE Insight Remote Support XXE (CVE-2024-53675)]	high
3/12/2025	[Palo Alto Networks PAN-OS 10.1.x < 10.1.14-h11 / 10.2.x < 10.2.5 / 11.0.x < 11.0.2 Vulnerability]	high
3/12/2025	[Microsoft Edge (Chromium) < 134.0.3124.66 Multiple Vulnerabilities]	high
3/12/2025	[AlmaLinux 8 : firefox (ALSA-2025:2452)]	high
3/12/2025	[Debian dsa-5877 : chromium - security update]	high
3/12/2025	[Siemens InsydeH2O Plaintext Storage of a Password (CVE-2021-38489)]	high
3/11/2025	[Debian dla-4084 : libmodbus-dev - security update]	high
3/11/2025	[Ubuntu 16.04 LTS : Linux kernel vulnerabilities (USN-7332-2)]	high
3/11/2025	[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7342-1)]	high
3/11/2025	[Ubuntu 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities (USN-7344-1)]	high
3/11/2025	[Security Updates for Microsoft Office Products (March 2025) (macOS)]	high

## 4 Die Hacks der Woche

mit Martin Haunschmid

#### 4.0.1 Information Stealer. Wie funktionieren sie?



[Zum Youtube Video](#)

## 5 Cyberangriffe: (Mär)

Datum	Opfer	Land	Information
2025-03-09	Aerticket	[DEU]	<a href="#">Link</a>
2025-03-07	Crystal D	[USA]	<a href="#">Link</a>
2025-03-06	Bikur Rofeh	[ISR]	<a href="#">Link</a>
2025-03-05	Ålands Centralandelslag (ÅCA)	[FIN]	<a href="#">Link</a>
2025-03-05	Endless Mountains Health Systems (EMHS)	[USA]	<a href="#">Link</a>
2025-03-05	Fachhochschule Nordwestschweiz	[CHE]	<a href="#">Link</a>
2025-03-04	Unikorn Semiconductor Corp.	[TWN]	<a href="#">Link</a>
2025-03-04	Stadtwerke Schwerte	[DEU]	<a href="#">Link</a>
2025-03-04	Adina Hotels	[AUS]	<a href="#">Link</a>
2025-03-03	Whitman Hospital and Medical Clinics	[USA]	<a href="#">Link</a>
2025-03-03	Mission, Texas	[USA]	<a href="#">Link</a>
2025-03-03	Brucha	[AUT]	<a href="#">Link</a>
2025-03-02	HomeTeamNS	[SGP]	<a href="#">Link</a>
2025-03-02	POLSA (Polish Space Agency)	[POL]	<a href="#">Link</a>
2025-03-02	Adval Tech Group	[CHE]	<a href="#">Link</a>
2025-03-02	Penn-Harris-Madison school district	[USA]	<a href="#">Link</a>
2025-03-02	Ivinhema	[BRA]	<a href="#">Link</a>
2025-03-02	Berkeley Research Group (BRG)	[USA]	<a href="#">Link</a>
2025-03-01	National Presto Industries, Inc.	[USA]	<a href="#">Link</a>
2025-03-01	TFE Hotels	[AUS]	<a href="#">Link</a>

## 6 Ransomware-Erpressungen: (Mär)

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-13	[University Diagnostic Medical Imaging, PC (udmi.net)]	fog	<a href="#">Link</a>
2025-03-12	[El Camino Real Academy (elcaminorealacademy)]	fog	<a href="#">Link</a>
2025-03-13	[Iraqi Ministry of Finance]	babuk2	<a href="#">Link</a>
2025-03-13	[Iraqi Council of Ministers]	babuk2	<a href="#">Link</a>
2025-03-12	[Ascoma Group]	akira	<a href="#">Link</a>
2025-03-03	[Raja Ferry Port Public Company Limited]	nightspire	<a href="#">Link</a>
2025-03-08	[Far East Consortium International Limited]	nightspire	<a href="#">Link</a>
2025-03-03	[Business Ledger Limited]	nightspire	<a href="#">Link</a>
2025-03-01	[Tohpe Corporation]	nightspire	<a href="#">Link</a>
2025-03-12	[Hydro-Vacuum S.A.]	nightspire	<a href="#">Link</a>
2025-03-12	[marinabaysands.com - Singapore Hotel (Internal Server)]	babuk2	<a href="#">Link</a>
2025-03-12	[Yushin America, Inc]	qilin	<a href="#">Link</a>
2025-03-12	[PACOMARTINEZ]	akira	<a href="#">Link</a>
2025-03-12	[SMG Bahamas]	akira	<a href="#">Link</a>
2025-03-12	[extremepperformance.com]	funksec	<a href="#">Link</a>
2025-03-12	[hitekgroup.in india Finance]	babuk2	<a href="#">Link</a>
2025-03-12	[Industrial Acceptance Corporation]	akira	<a href="#">Link</a>
2025-03-12	[tempel.com]	cactus	<a href="#">Link</a>
2025-03-12	[thermoid.com]	cactus	<a href="#">Link</a>
2025-03-12	[baillie.com]	cactus	<a href="#">Link</a>
2025-03-12	[CAHOKIA CUSD 187 SCHOOL DISTRICT]	qilin	<a href="#">Link</a>
2025-03-12	[India's telecommunication network]	babuk2	<a href="#">Link</a>
2025-03-12	[Best Telecom Laos]	akira	<a href="#">Link</a>
2025-03-12	[CNQC]	akira	<a href="#">Link</a>
2025-03-12	[Peerless Food Equipment]	akira	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-12	[Babuk Locker 2.0 affiliate program 2025]	babuk2	<a href="#">Link</a>
2025-03-12	[Helmut Hölbling Spedition GmbH]	akira	<a href="#">Link</a>
2025-03-12	[urban1.com]	cactus	<a href="#">Link</a>
2025-03-12	[rocketstores.com]	cactus	<a href="#">Link</a>
2025-03-12	[www.visualisation.one]	ransomhub	<a href="#">Link</a>
2025-03-10	[HOST Software Entwicklung und Consulting GmbH]	qilin	<a href="#">Link</a>
2025-03-12	[HYPONAMIRU]	arcusmedia	<a href="#">Link</a>
2025-03-12	[HYPERNOVA TELECOM]	arcusmedia	<a href="#">Link</a>
2025-03-12	[unimore.it]	funksec	<a href="#">Link</a>
2025-03-12	[Baykar Turkish defense company C4I and artificial intelligence]	babuk2	<a href="#">Link</a>
2025-03-11	[tradingacademy.com]	safepay	<a href="#">Link</a>
2025-03-11	[ultimateclasslimo.com]	safepay	<a href="#">Link</a>
2025-03-11	[havenresorts.com]	safepay	<a href="#">Link</a>
2025-03-11	[lgipr.com]	safepay	<a href="#">Link</a>
2025-03-11	[jockeysalud.com.pe]	safepay	<a href="#">Link</a>
2025-03-11	[motomecanica.com]	safepay	<a href="#">Link</a>
2025-03-11	[cali.losolivos.co]	safepay	<a href="#">Link</a>
2025-03-11	[Skyward Specialty Insurance]	killsec	<a href="#">Link</a>
2025-03-11	[Trymata]	killsec	<a href="#">Link</a>
2025-03-03	[Gaines County, Texas]	qilin	<a href="#">Link</a>
2025-03-11	[Springfield Water and Sewer Commission]	lynx	<a href="#">Link</a>
2025-03-11	[Suder&Suder]	qilin	<a href="#">Link</a>
2025-03-11	[Longue Vue Club]	lynx	<a href="#">Link</a>
2025-03-11	[Taking stock of February 2025]	akira	<a href="#">Link</a>
2025-03-11	[WAUGH & GOODWIN, LLP]	akira	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-11	[airexplore.aero Company]	babuk2	<a href="#">Link</a>
2025-03-11	[Veristat]	akira	<a href="#">Link</a>
2025-03-11	[Edesur Dominicana]	hunters	<a href="#">Link</a>
2025-03-11	[All4Labels - Global Packaging Group]	akira	<a href="#">Link</a>
2025-03-11	[Essex County OB/GYN Associates]	incransom	<a href="#">Link</a>
2025-03-11	[Princeton Hydro]	akira	<a href="#">Link</a>
2025-03-11	[isee-eg.com]	funksec	<a href="#">Link</a>
2025-03-11	[fnde.gov.br brazilian government]	babuk2	<a href="#">Link</a>
2025-03-11	[wapda.gov.pk]	babuk2	<a href="#">Link</a>
2025-03-11	[lexmark.com Company]	babuk2	<a href="#">Link</a>
2025-03-10	[Wilkinson Rogers (wilkinsonrogers.com)]	fog	<a href="#">Link</a>
2025-03-11	[forvismazars.com.fr ( mazars.fr )]	babuk2	<a href="#">Link</a>
2025-03-10	[Magnolia Manor (magnoliamanor.com)]	fog	<a href="#">Link</a>
2025-03-10	[petstop.com Company]	babuk2	<a href="#">Link</a>
2025-03-10	[misaludhealth.com]	babuk2	<a href="#">Link</a>
2025-03-10	[bank.pingan.com (CN)]	babuk2	<a href="#">Link</a>
2025-03-10	[Access to Indian Ministry of Defence and Military Secret (DRDO) documents By Babuk Locker ...]	babuk2	<a href="#">Link</a>
2025-03-10	[fredsalvuccicorp.com]	kairos	<a href="#">Link</a>
2025-03-10	[Mandarin.com.br]	babuk2	<a href="#">Link</a>
2025-03-10	[Callico Distributors, Inc.]	akira	<a href="#">Link</a>
2025-03-10	[Pacific Honda Company]	akira	<a href="#">Link</a>
2025-03-10	[Arcusin]	akira	<a href="#">Link</a>
2025-03-10	[www.hexosys.com]	ransomhub	<a href="#">Link</a>
2025-03-10	[Safe-Strap Company, LLC]	akira	<a href="#">Link</a>
2025-03-10	[Fickling & Company]	akira	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-07	[GPS 909]	akira	<a href="#">Link</a>
2025-03-10	[mazars.fr]	babuk2	<a href="#">Link</a>
2025-03-10	[Dacas Argentina]	qilin	<a href="#">Link</a>
2025-03-05	[Cotswold Fayre]	dragonforce	<a href="#">Link</a>
2025-03-05	[Vercoe Insurance Brokers]	dragonforce	<a href="#">Link</a>
2025-03-05	[Steel Dynamics UK]	dragonforce	<a href="#">Link</a>
2025-03-05	[E Leet Woodworking]	dragonforce	<a href="#">Link</a>
2025-03-04	[Customer Management Systems]	medusa	<a href="#">Link</a>
2025-03-06	[CPI Books]	medusa	<a href="#">Link</a>
2025-03-09	[ACTi Corporation]	lynx	<a href="#">Link</a>
2025-03-09	[BerksBar.org]	incransom	<a href="#">Link</a>
2025-03-09	[baldaufarchitekten.de]	incransom	<a href="#">Link</a>
2025-03-09	[klabs.it]	funksec	<a href="#">Link</a>
2025-03-03	[Salemerode.com]	flocker	<a href="#">Link</a>
2025-03-09	[State Bar of Texas (www.texasbar.com)]	incransom	<a href="#">Link</a>
2025-03-09	[Greenwood Village South GVS]	incransom	<a href="#">Link</a>
2025-03-07	[prelco.ca]	qilin	<a href="#">Link</a>
2025-03-07	[KH OneStop]	qilin	<a href="#">Link</a>
2025-03-09	[Jerue Companies]	play	<a href="#">Link</a>
2025-03-09	[Syma-System]	play	<a href="#">Link</a>
2025-03-09	[Compound Solutions]	play	<a href="#">Link</a>
2025-03-09	[T J Machine & Tool]	play	<a href="#">Link</a>
2025-03-09	[Gevril]	play	<a href="#">Link</a>
2025-03-09	[Peak Season]	play	<a href="#">Link</a>
2025-03-09	[Yorke & Curtis]	play	<a href="#">Link</a>
2025-03-09	[Buckley BalaWilson Mew]	play	<a href="#">Link</a>
2025-03-09	[Holiday Comfort]	play	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-09	[Clawson Honda]	play	<a href="#">Link</a>
2025-03-09	[Dectron]	play	<a href="#">Link</a>
2025-03-09	[Nor Arc]	play	<a href="#">Link</a>
2025-03-09	[British virgin islands London Office]	rhysida	<a href="#">Link</a>
2025-03-05	[Changhua Christian Hospital]	crazyhunter	<a href="#">Link</a>
2025-03-05	[Huacheng Electric]	crazyhunter	<a href="#">Link</a>
2025-03-05	[Mackay Hospital]	crazyhunter	<a href="#">Link</a>
2025-03-05	[Asia University Hospital]	crazyhunter	<a href="#">Link</a>
2025-03-05	[Asia University]	crazyhunter	<a href="#">Link</a>
2025-03-06	[mitchellmcnutt.com]	ransomhub	<a href="#">Link</a>
2025-03-08	[univ-rennes.fr]	funksec	<a href="#">Link</a>
2025-03-05	[Tech NH]	lynx	<a href="#">Link</a>
2025-03-07	[Allworx]	bianlian	<a href="#">Link</a>
2025-03-07	[Minnesota Orthodontics]	bianlian	<a href="#">Link</a>
2025-03-07	[REYCOTEL]	arcusmedia	<a href="#">Link</a>
2025-03-07	[total-ps.com]	ransomhub	<a href="#">Link</a>
2025-03-07	[Hancock Public School]	interlock	<a href="#">Link</a>
2025-03-07	[lofotenseafood.com]	lynx	<a href="#">Link</a>
2025-03-07	[ADDA (adda.io)]	ransomexx	<a href="#">Link</a>
2025-03-07	[Swift Haulage Berhad]	akira	<a href="#">Link</a>
2025-03-07	[Aj Taylor Electrical Contractors Ltd]	sarcoma	<a href="#">Link</a>
2025-03-07	[Sittab INC]	akira	<a href="#">Link</a>
2025-03-07	[wheats.com]	ransomhub	<a href="#">Link</a>
2025-03-07	[srmg.com.au]	ransomhub	<a href="#">Link</a>
2025-03-07	[sorbonne-universite.fr]	funksec	<a href="#">Link</a>
2025-03-06	[RFA Decor]	akira	<a href="#">Link</a>
2025-03-05	[www.portlandschools.org]	ransomhub	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-05	[www.hinton.ca]	ransomhub	<a href="#">Link</a>
2025-03-05	[www.convention.qc.ca]	ransomhub	<a href="#">Link</a>
2025-03-06	[hickorylaw.com]	ransomhub	<a href="#">Link</a>
2025-03-06	[lovesac.com]	ransomhub	<a href="#">Link</a>
2025-03-06	[agi.net]	monti	<a href="#">Link</a>
2025-03-06	[Adval Tech]	lynx	<a href="#">Link</a>
2025-03-06	[WJCC Public Schools (wjccschools.org)]	fog	<a href="#">Link</a>
2025-03-06	[Connekted, Inc.]	qilin	<a href="#">Link</a>
2025-03-06	[Naples Heritage Golf & Country Club]	incransom	<a href="#">Link</a>
2025-03-06	[Ministry of Foreign Affairs of Ukraine]	qilin	<a href="#">Link</a>
2025-03-06	[Oberlin Cable Co-op (oberlin.net)]	fog	<a href="#">Link</a>
2025-03-06	[Elite Advanced Laser Corporation]	akira	<a href="#">Link</a>
2025-03-05	[1X Internet]	fog	<a href="#">Link</a>
2025-03-05	[Bizcode]	fog	<a href="#">Link</a>
2025-03-05	[Manning Publications Co.]	fog	<a href="#">Link</a>
2025-03-05	[Engikam]	fog	<a href="#">Link</a>
2025-03-05	[FHNW]	fog	<a href="#">Link</a>
2025-03-05	[Aeonsparx]	fog	<a href="#">Link</a>
2025-03-05	[Flightsim studio]	fog	<a href="#">Link</a>
2025-03-05	[Neopoly]	fog	<a href="#">Link</a>
2025-03-05	[Kr3m]	fog	<a href="#">Link</a>
2025-03-05	[InfoReach]	fog	<a href="#">Link</a>
2025-03-05	[Euranova]	fog	<a href="#">Link</a>
2025-03-05	[Inelmatic]	fog	<a href="#">Link</a>
2025-03-05	[Kotliva]	fog	<a href="#">Link</a>
2025-03-05	[Blue Planet]	fog	<a href="#">Link</a>
2025-03-05	[Eumetsat]	fog	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-05	[Melexis]	fog	<a href="#">Link</a>
2025-03-06	[City government office in Van (Turkey) - van.bel.tr]	skira	<a href="#">Link</a>
2025-03-06	[Law Diary (USA)]	skira	<a href="#">Link</a>
2025-03-06	[Carruth Compliance Consulting]	skira	<a href="#">Link</a>
2025-03-06	[CCL Products India]	skira	<a href="#">Link</a>
2025-03-06	[Krisala Developer (India)]	skira	<a href="#">Link</a>
2025-03-05	[The 19 biggest gitlabs]	fog	<a href="#">Link</a>
2025-03-05	[willms-fleisch.de]	safepay	<a href="#">Link</a>
2025-03-05	[Pervedant]	lynx	<a href="#">Link</a>
2025-03-05	[SCOLARO FETTER GRIZANTI & McGOUGH, P.C. (scolaro.com)]	fog	<a href="#">Link</a>
2025-03-05	[www.black-star.fr]	ransomhub	<a href="#">Link</a>
2025-03-05	[Adrenalina]	akira	<a href="#">Link</a>
2025-03-05	[Cyncly Company]	akira	<a href="#">Link</a>
2025-03-05	[City Plumbing & Electric Supply Co]	akira	<a href="#">Link</a>
2025-03-03	[www.japanrebuilt.jp]	ransomhub	<a href="#">Link</a>
2025-03-04	[www.sunsweet.com]	ransomhub	<a href="#">Link</a>
2025-03-05	[Best Collateral, Inc.]	rhysida	<a href="#">Link</a>
2025-03-04	[Chicago Doorways, LLC]	qilin	<a href="#">Link</a>
2025-03-05	[Schmiedetechnik Plettenberg GmbH & Co KG]	lynx	<a href="#">Link</a>
2025-03-04	[365labs - Security Corp]	monti	<a href="#">Link</a>
2025-03-04	[PFS Grupo - Plan de igualdad, Sostenibilidad]	qilin	<a href="#">Link</a>
2025-03-04	[Pampili (pampili.com.br)]	fog	<a href="#">Link</a>
2025-03-04	[Keystone Pacific Property Management LLC]	bianlian	<a href="#">Link</a>
2025-03-04	[Mosley Glick O'Brien, Inc.]	bianlian	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-04	[FANTIN group]	akira	<a href="#">Link</a>
2025-03-04	[Grupo Baston Aerossol (baston.com.br)]	fog	<a href="#">Link</a>
2025-03-04	[Ray Fogg Corporate Properties]	akira	<a href="#">Link</a>
2025-03-04	[goencon.com]	ransomhub	<a href="#">Link</a>
2025-03-04	[Seabank Group]	lynx	<a href="#">Link</a>
2025-03-04	[Tata Technologies]	hunters	<a href="#">Link</a>
2025-03-04	[Wendy Wu Tours]	killsec	<a href="#">Link</a>
2025-03-04	[rockhillwc.com]	qilin	<a href="#">Link</a>
2025-03-04	[bpmmicro.com]	qilin	<a href="#">Link</a>
2025-03-04	[peruzzi.com]	qilin	<a href="#">Link</a>
2025-03-04	[IOVATE.COM]	clop	<a href="#">Link</a>
2025-03-04	[Legal Aid Society of Salt Lake]	bianlian	<a href="#">Link</a>
2025-03-04	[Ewald Consulting]	bianlian	<a href="#">Link</a>
2025-03-04	[Netcom-World]	apos	<a href="#">Link</a>
2025-03-04	[InternetWay]	apos	<a href="#">Link</a>
2025-03-04	[cimenyan.desa.id]	funksec	<a href="#">Link</a>
2025-03-03	[familychc.com]	ransomhub	<a href="#">Link</a>
2025-03-03	[andreyengineering.com]	ransomhub	<a href="#">Link</a>
2025-03-03	[drvitenas.com]	kairos	<a href="#">Link</a>
2025-03-03	[usarice.com]	kairos	<a href="#">Link</a>
2025-03-03	[Sunnking SustainableSolutions]	akira	<a href="#">Link</a>
2025-03-03	[LINKGROUP]	arcusmedia	<a href="#">Link</a>
2025-03-03	[Openreso]	arcusmedia	<a href="#">Link</a>
2025-03-03	[Itapeseg]	arcusmedia	<a href="#">Link</a>
2025-03-03	[logic insectes]	arcusmedia	<a href="#">Link</a>
2025-03-03	[RJ IT Solutions]	arcusmedia	<a href="#">Link</a>
2025-03-03	[Grafitec]	arcusmedia	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-03	[synaptic.co.tz]	arcusmedia	<a href="#">Link</a>
2025-03-03	[quigleyeye.com]	cactus	<a href="#">Link</a>
2025-03-03	[La Unión]	lynx	<a href="#">Link</a>
2025-03-03	[Central McGowan (centralmcgowan.com)]	fog	<a href="#">Link</a>
2025-03-03	[Klesk Metal Stamping Co (kleskmetalstamping.com)]	fog	<a href="#">Link</a>
2025-03-03	[Forstenlechner Installationstechnik]	akira	<a href="#">Link</a>
2025-03-03	[ceratec.com]	abyss	<a href="#">Link</a>
2025-03-02	[Pre Con Industries]	play	<a href="#">Link</a>
2025-03-02	[IT-IQ Botswana]	play	<a href="#">Link</a>
2025-03-02	[North American Fire Hose]	play	<a href="#">Link</a>
2025-03-02	[Couri Insurance Agency]	play	<a href="#">Link</a>
2025-03-02	[Optometrics]	play	<a href="#">Link</a>
2025-03-02	[International Process Plants]	play	<a href="#">Link</a>
2025-03-02	[Ganong Bros]	play	<a href="#">Link</a>
2025-03-02	[FM.GOB.AR]	monti	<a href="#">Link</a>
2025-03-02	[gruppocogesi.org]	lockbit3	<a href="#">Link</a>
2025-03-02	[Bell Ambulance]	medusa	<a href="#">Link</a>
2025-03-02	[Workforce Group]	killsec	<a href="#">Link</a>
2025-03-01	[germancentre.sg]	incransom	<a href="#">Link</a>
2025-03-01	[JEFFREYCOURT.COM]	clop	<a href="#">Link</a>
2025-03-01	[APTEAN.COM]	clop	<a href="#">Link</a>
2025-03-01	[Wayne County, Michigan]	interlock	<a href="#">Link</a>
2025-03-01	[The Smeg Group]	interlock	<a href="#">Link</a>
2025-03-01	[Newton & Associates, Inc]	rhysida	<a href="#">Link</a>

## 7 Quellen

### 7.1 Quellenverzeichnis

- 1) Cyberwatch - <https://github.com/Casualtek/Cyberwatch>
- 2) Ransomware.live - <https://data.ransomware.live>
- 3) Heise Security Alerts! - <https://www.heise.de/security/alerts/>
- 4) First EPSS - <https://www.first.org/epss/>
- 5) BSI WID - <https://wid.cert-bund.de/>
- 6) Tenable Plugins - <https://www.tenable.com/plugins/>
- 7) Exploit - [packetstormsecurity.com](https://packetstormsecurity.com)
- 8) 0-Day - <https://www.zerodayinitiative.com/rss/published/>
- 9) Die Hacks der Woche - <https://martinhaunschmid.com/videos>

## 8 Impressum



***Herausgeber:***

Marlon Hübner  
Brückenstraße 3  
57629 Höchstenbach

***E-Mail***

[info@cyberwald.com](mailto:info@cyberwald.com)

Cyberwald ist ein privates, nicht-kommerzielles Projekt zur Förderung des Bewusstseins für Cybersicherheit.