

---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20250210



## 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>4</b>
3.1 EPSS . . . . .	4
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit . . . . .	5
3.2 BSI - Warn- und Informationsdienst (WID) . . . . .	6
3.3 Sicherheitslücken Meldungen von Tenable . . . . .	10
<b>4 Die Hacks der Woche</b>	<b>11</b>
4.0.1 Wo gehyped wird fallen Späne. Öffentliche Datenbank bei Deepseek . . . . .	12
<b>5 Cyberangriffe: (Feb)</b>	<b>13</b>
<b>6 Ransomware-Erpressungen: (Feb)</b>	<b>13</b>
<b>7 Quellen</b>	<b>20</b>
7.1 Quellenverzeichnis . . . . .	20
<b>8 Impressum</b>	<b>21</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

#### ***Defekter Sicherheitspatch für HCL BigFix Server Automation repariert***

Angreifer können HCL BigFix SA per DoS-Attacke abschießen. Ein überarbeitetes Sicherheitsupdate soll das Problem nun lösen.

- [Link](#)

—

#### ***Cisco stopft Sicherheitslücken in mehreren Produkten – auch kritische***

In mehreren Produkten hat Cisco Sicherheitslücken entdeckt und warnt in Sicherheitsmitteilungen davor. Updates stehen bereit.

- [Link](#)

—

#### ***Quartalssicherheitsupdates: F5 rüstet BIG-IP-Appliances gegen mögliche Angriffe***

Die F5-Entwickler haben mehrere Sicherheitslücken in unter anderem BIG-IP Next und BIG-IQ geschlossen. Es kann zur Ausführung von Schadcode kommen.

- [Link](#)

—

#### ***CISA warnt vor Angriffen auf Linux, Apache OFBiz, .NET und Paessler PRTG***

Die US-amerikanische Cybersicherheitsbehörde CISA warnt vor beobachteten Angriffen auf Lücken in Linux, Apache OFBiz, .NET und Paessler PRTG.

- [Link](#)

—

#### ***HP: Kritische Lücken in Universal-Druckertreiber ermöglichen Codeschmuggel***

HP hat die Universal-Druckertreiber für PCL 6 und Postscript aktualisiert. Die Updates schließen kritische Sicherheitslücken.

- [Link](#)

—

#### ***Netgear: Nighthawk Pro Gaming-Router mit Schadcode-Leck***

Netgear warnt vor Codeschmuggel-Lücken in Nighthawk Pro Gaming-Routern. Zudem haben einige Router nach Support-Ende eine Sicherheitslücke.

- [Link](#)

—

#### ***Veeam Backup: Codeschmuggel durch MitM-Lücke im Updater möglich***

Veeam Backup enthält einen Updater, der für Man-in-the-Middle-Attacken anfällig ist. Angreifer können Schadcode einschleusen.

- [Link](#)

---

***Zugriffsmanagement: HPE Aruba Networking CPPM ist verwundbar***

Netzwerkadmins sollten HPE Aruba Networking ClearPass Policy Manager aus Sicherheitsgründen aktualisieren.

- [Link](#)

---

***Support ausgelaufen: Keine Sicherheitsupdates mehr für attackierte Zyxel-Router***

Derzeit hat es eine Mirai-Botnet-Malware auf bestimmte Routermodelle von Zyxel abgesehen. Weil der Support ausgelaufen ist, müssen Admins jetzt handeln.

- [Link](#)

---

***Patchday Android: Angreifer nutzen Kernel-Sicherheitslücke aus***

Es sind wichtige Sicherheitsupdates für Android 12, 12L, 13, 14 und 15 erschienen. Angreifer können Geräte kompromittieren.

- [Link](#)

---

### 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-2024-9474	0.974800000	0.999860000	<a href="#">Link</a>
CVE-2024-9465	0.943220000	0.994130000	<a href="#">Link</a>
CVE-2024-9463	0.961860000	0.996680000	<a href="#">Link</a>
CVE-2024-8963	0.967240000	0.997840000	<a href="#">Link</a>
CVE-2024-7593	0.971650000	0.998990000	<a href="#">Link</a>
CVE-2024-6893	0.938390000	0.993660000	<a href="#">Link</a>
CVE-2024-6670	0.904230000	0.991040000	<a href="#">Link</a>
CVE-2024-5910	0.962890000	0.996900000	<a href="#">Link</a>
CVE-2024-55956	0.967520000	0.997900000	<a href="#">Link</a>
CVE-2024-5217	0.933860000	0.993180000	<a href="#">Link</a>
CVE-2024-50623	0.969230000	0.998340000	<a href="#">Link</a>
CVE-2024-4879	0.934670000	0.993270000	<a href="#">Link</a>
CVE-2024-4577	0.958420000	0.996110000	<a href="#">Link</a>
CVE-2024-4358	0.925270000	0.992470000	<a href="#">Link</a>
CVE-2024-41713	0.957210000	0.995900000	<a href="#">Link</a>
CVE-2024-40711	0.963400000	0.997000000	<a href="#">Link</a>
CVE-2024-4040	0.969020000	0.998290000	<a href="#">Link</a>
CVE-2024-38856	0.942880000	0.994100000	<a href="#">Link</a>
CVE-2024-36401	0.955950000	0.995710000	<a href="#">Link</a>
CVE-2024-3400	0.964000000	0.997130000	<a href="#">Link</a>
CVE-2024-3273	0.937410000	0.993570000	<a href="#">Link</a>
CVE-2024-32113	0.933050000	0.993120000	<a href="#">Link</a>
CVE-2024-28995	0.965000000	0.997320000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-28987	0.961930000	0.996690000	<a href="#">Link</a>
CVE-2024-27348	0.960260000	0.996410000	<a href="#">Link</a>
CVE-2024-27198	0.968000000	0.998020000	<a href="#">Link</a>
CVE-2024-24919	0.960980000	0.996520000	<a href="#">Link</a>
CVE-2024-23897	0.973540000	0.999550000	<a href="#">Link</a>
CVE-2024-2389	0.900180000	0.990770000	<a href="#">Link</a>
CVE-2024-23692	0.964470000	0.997230000	<a href="#">Link</a>
CVE-2024-21893	0.956970000	0.995850000	<a href="#">Link</a>
CVE-2024-21887	0.973220000	0.999480000	<a href="#">Link</a>
CVE-2024-20767	0.965330000	0.997390000	<a href="#">Link</a>
CVE-2024-1709	0.957220000	0.995900000	<a href="#">Link</a>
CVE-2024-1212	0.937140000	0.993540000	<a href="#">Link</a>
CVE-2024-0986	0.955530000	0.995650000	<a href="#">Link</a>
CVE-2024-0195	0.962680000	0.996850000	<a href="#">Link</a>
CVE-2024-0012	0.969980000	0.998540000	<a href="#">Link</a>

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

Fri, 07 Feb 2025

#### **[NEU] [UNGEPATCHT] [kritisch] ProFTPD: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in ProFTPD ausnutzen, um eigenen Code auszuführen.

- [Link](#)

—

Fri, 07 Feb 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](#)

—

Fri, 07 Feb 2025

**[NEU] [hoch] Moxa Switch (EDS, ICS, IKS und SDS): Schwachstelle ermöglicht Denial of Service**

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in Moxa Switches ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

—

Fri, 07 Feb 2025

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

Ein entfernter anonymen oder lokaler Angreifer kann diese Schwachstelle ausnutzen, um beliebigen Code auszuführen, Spoofing-Angriffe durchzuführen, vertrauliche Informationen offenzulegen, Daten zu manipulieren und einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

—

Fri, 07 Feb 2025

**[NEU] [hoch] Microsoft Dynamics 365: Schwachstelle ermöglicht Privilegieneskalation**

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Microsoft Dynamics 365 ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Fri, 07 Feb 2025

**[UPDATE] [hoch] bzip2: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode mit den Rechten des Dienstes**

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in bzip2 ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen.

- [Link](#)

—

Fri, 07 Feb 2025

**[UPDATE] [kritisch] Sophos XG Firewall: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in Sophos XG Firewall ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 07 Feb 2025

**[UPDATE] [hoch] wget: Schwachstelle ermöglicht Offenlegung von Informationen**

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in wget ausnutzen, um Informationen offenzulegen.

- [Link](#)



—

Fri, 07 Feb 2025

**[UPDATE] [kritisch] Microsoft Office: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in verschiedenen Microsoft Office Anwendungen ausnutzen, um beliebigen Code auszuführen, seine Privilegien zu eskalieren oder vertrauliche Informationen offenzulegen.

- [Link](#)

—

Fri, 07 Feb 2025

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

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

- [Link](#)

—

Fri, 07 Feb 2025

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

Ein entfernter Angreifer kann mehrere Schwachstellen in GitLab ausnutzen, um seine Privilegien zu erhöhen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand zu erzeugen oder einen Cross-Site-Scripting-Angriff durchzuführen.

- [Link](#)

—

Fri, 07 Feb 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](#)

—

Fri, 07 Feb 2025

**[UPDATE] [hoch] Mozilla Firefox und Thunderbird: Mehrere Schwachstellen**

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen preiszugeben, Sicherheitsmaßnahmen zu umgehen oder Cross-Site-Scripting- oder Spoofing-Angriffe durchzuführen.

- [Link](#)

—

Fri, 07 Feb 2025

**[UPDATE] [hoch] Mozilla Firefox und Thunderbird: Mehrere Schwachstellen**

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox

ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen preiszugeben, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu erzeugen oder Spoofing-Angriffe durchzuführen.

- [Link](#)

—

Fri, 07 Feb 2025

**[UPDATE] [hoch] Google Chrome / Microsoft Edge: Mehrere Schwachstellen**

Ein entfernter, anonymes Angreifer kann mehrere Schwachstellen in Google Chrome / Microsoft Edge ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, einen Spoofing-Angriff durchzuführen oder nicht spezifizierte Auswirkungen zu verursachen.

- [Link](#)

—

Fri, 07 Feb 2025

**[UPDATE] [hoch] F5 BIG-IP: Mehrere Schwachstellen**

Ein Angreifer kann diese Schwachstellen ausnutzen, um beliebige Systembefehle auszuführen, Sicherheitsmaßnahmen zu umgehen, Cross-Site-Scripting-Angriffe durchzuführen und einen Denial-of-Service-Zustand zu erzeugen.

- [Link](#)

—

Thu, 06 Feb 2025

**[NEU] [hoch] Cisco IOS, IOS XE and IOS XR: Mehrere Schwachstellen ermöglichen Denial of Service**

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Cisco IOS, Cisco IOS XE und Cisco IOS XR ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

—

Thu, 06 Feb 2025

**[UPDATE] [hoch] Oracle MySQL: Mehrere Schwachstellen**

Ein entfernter, anonymes oder authentisierter Angreifer kann mehrere Schwachstellen in Oracle MySQL ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- [Link](#)

—

Thu, 06 Feb 2025

**[NEU] [hoch] Apache Camel for Spring Boot: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Apache Camel, Red Hat Enterprise Linux und Red Hat Integration ausnutzen, um beliebigen Code auszuführen und Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

—

Thu, 06 Feb 2025

**[NEU] [hoch] Golang Go: Mehrere Schwachstellen**

Ein lokaler Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um Informationen offenzulegen, oder Code auszuführen.

- [Link](#)

—

### 3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
2/8/2025	[Fedora 40 : firefox (2025-2e627d0672)]	critical
2/8/2025	[Fedora 41 : clevis-pin-tpm2 / dbus-secwrap / envision / fido-device-onboard / etc (2025-f8be7978e3)]	critical
2/8/2025	[CBL Mariner 2.0 Security Update: freetype (CVE-2020-15999)]	critical
2/8/2025	[Slackware Linux 15.0 / current gnutls Multiple Vulnerabilities (SSA:2025-039-01)]	critical
2/7/2025	[AlmaLinux 9 : keepalived (ALSA-2025:0917)]	critical
2/7/2025	[AlmaLinux 9 : mingw-glib2 (ALSA-2025:0936)]	critical
2/7/2025	[AlmaLinux 9 : bzip2 (ALSA-2025:0925)]	critical
2/7/2025	[Slackware Linux 15.0 / current libtasn1 Vulnerability (SSA:2025-038-01)]	critical
2/7/2025	[FreeBSD : mozilla – multiple vulnerabilities (20485d27-e540-11ef-a845-b42e991fc52e)]	critical
2/7/2025	[FreeBSD : mozilla – multiple vulnerabilities (f7ca4ff7-e53f-11ef-a845-b42e991fc52e)]	critical
2/7/2025	[Nutanix AOS : Multiple Vulnerabilities (NXSA-AOS-6.10.1)]	critical
2/7/2025	[Debian dla-4045 : thunderbird - security update]	critical
2/7/2025	[Debian dla-4044 : firefox-esr - security update]	critical
2/9/2025	[Fedora 40 : php-phpseclib (2025-b38cbff99d)]	high

Datum	Schwachstelle	Bewertung
2/9/2025	[Fedora 40 : vaultwarden (2025-7fd2f66440)]	high
2/9/2025	[Fedora 40 : rust-routinator (2025-46db4ee37e)]	high
2/9/2025	[Debian dla-4047 : libipa-hbac-dev - security update]	high
2/8/2025	[Fedora 41 : vaultwarden (2025-41f4056b0e)]	high
2/8/2025	[Fedora 40 : jpegxl (2025-35a8167b88)]	high
2/8/2025	[Fedora 41 : php-phpseclib (2025-91d6e174d9)]	high
2/8/2025	[CBL Mariner 2.0 Security Update: vim (CVE-2024-22667)]	high
2/7/2025	[PDF-XChange Editor < 10.5.0.393 Multiple Vulnerabilities]	high
2/7/2025	[Cisco IOS XE Software SNMP DoS (cisco-sa-snmp-dos-sdxnSUcW)]	high
2/7/2025	[Cisco IOS Software SNMP DoS (cisco-sa-snmp-dos-sdxnSUcW)]	high
2/7/2025	[AlmaLinux 9 : buildah (ALSA-2025:0923)]	high
2/7/2025	[AlmaLinux 9 : podman (ALSA-2025:0922)]	high
2/7/2025	[FreeBSD : libcaca – Multiple vulnerabilities (c10b639c-e51c-11ef-9e76-4ccc6adda413)]	high
2/7/2025	[FreeBSD : cacti – Multiple vulnerabilities (e7974ca5-e4c8-11ef-aab3-40b034429ecf)]	high
2/7/2025	[Debian dsa-5860 : affs-modules-6.1.0-21-4kc-malta-di - security update]	high

## 4 Die Hacks der Woche

mit Martin Haunschmid

#### 4.0.1 Wo gehyped wird fallen Späne. Öffentliche Datenbank bei Deepseek



[Zum Youtube Video](#)

## 5 Cyberangriffe: (Feb)

Datum	Opfer	Land	Information
2025-02-07	Transcend Information, Inc.	[TWN]	<a href="#">Link</a>
2025-02-05	IMI	[GBR]	<a href="#">Link</a>
2025-02-03	Lee Enterprises	[USA]	<a href="#">Link</a>
2025-02-02	Top-Medien	[CHE]	<a href="#">Link</a>
2025-02-02	Mayer Steel Pipe Corporation	[TWN]	<a href="#">Link</a>
2025-02-02	Nan Ya PCB (KunShan) Corp.	[TWN]	<a href="#">Link</a>
2025-02-02	Université des Bahamas	[BHS]	<a href="#">Link</a>
2025-02-01	CESI	[FRA]	<a href="#">Link</a>

## 6 Ransomware-Erpressungen: (Feb)

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-10	[Upstate Glass Tempering]	sarcoma	<a href="#">Link</a>
2025-02-10	[Saied Music]	sarcoma	<a href="#">Link</a>
2025-02-09	[Kitty cookies]	kraken	<a href="#">Link</a>
2025-02-09	[www.cdprojekt.com]	kraken	<a href="#">Link</a>
2025-02-09	[www.mgl.law]	kraken	<a href="#">Link</a>
2025-02-09	[www.fudpucker.com]	kraken	<a href="#">Link</a>
2025-02-09	[ctntelco.com]	kraken	<a href="#">Link</a>
2025-02-09	[iRidge Inc.]	fog	<a href="#">Link</a>
2025-02-09	[Maxvy Technologies Pvt]	fog	<a href="#">Link</a>
2025-02-09	[Universitatea Politehnica din Bucuresti]	fog	<a href="#">Link</a>
2025-02-09	[Hpisd.org]	ransomhub	<a href="#">Link</a>
2025-02-09	[wwcsd.net]	ransomhub	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-09	[Israel Police]	handala	<a href="#">Link</a>
2025-02-09	[Gitlabs: Universitatea Politehnica din Bucuresti, Maxvy Technologies Pvt, iRidge Inc.]	fog	<a href="#">Link</a>
2025-02-08	[Substitute Teacher Service]	cicada3301	<a href="#">Link</a>
2025-02-08	[SAKAI SOUKEN Co.]	hunters	<a href="#">Link</a>
2025-02-08	[cmr24]	stormous	<a href="#">Link</a>
2025-02-08	[phidac.be]	funksec	<a href="#">Link</a>
2025-02-07	[3SS]	fog	<a href="#">Link</a>
2025-02-07	[Fligno]	fog	<a href="#">Link</a>
2025-02-07	[Chalmers tekniska högskola]	fog	<a href="#">Link</a>
2025-02-07	[herbalcanadaonline.com]	funksec	<a href="#">Link</a>
2025-02-07	[Gitlabs: Chalmers tekniska högskola, Fligno, 3SS]	fog	<a href="#">Link</a>
2025-02-06	[teamues.com]	ransomhub	<a href="#">Link</a>
2025-02-07	[iaaglobal.org]	funksec	<a href="#">Link</a>
2025-02-07	[Tropical Foods Company Inc]	akira	<a href="#">Link</a>
2025-02-07	[sautech.edu]	ransomhub	<a href="#">Link</a>
2025-02-07	[autogedal.ro]	funksec	<a href="#">Link</a>
2025-02-07	[nldappraisals.com]	qilin	<a href="#">Link</a>
2025-02-07	[renmarkfinacial.com]	qilin	<a href="#">Link</a>
2025-02-06	[lowernazareth.com]	safepay	<a href="#">Link</a>
2025-02-06	[northernresponse.com]	cactus	<a href="#">Link</a>
2025-02-06	[savoiesfoods.com]	cactus	<a href="#">Link</a>
2025-02-06	[zsattorneys.com]	ransomhub	<a href="#">Link</a>
2025-02-06	[NG-BLU Networks]	akira	<a href="#">Link</a>
2025-02-06	[Presence From Innovation (PFI)]	akira	<a href="#">Link</a>
2025-02-06	[Robertshaw]	hunters	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-05	[HARADA]	qilin	<a href="#">Link</a>
2025-02-06	[DIEM]	fog	<a href="#">Link</a>
2025-02-06	[Top Systems]	fog	<a href="#">Link</a>
2025-02-06	[eConceptions]	fog	<a href="#">Link</a>
2025-02-06	[Gitlabs: eConceptions, Top Systems, DIEM]	fog	<a href="#">Link</a>
2025-02-05	[McCORMICK TAYLOR]	qilin	<a href="#">Link</a>
2025-02-05	[corehandf.com]	threeam	<a href="#">Link</a>
2025-02-05	[Dash Business]	bianlian	<a href="#">Link</a>
2025-02-05	[Hall Chadwick]	bianlian	<a href="#">Link</a>
2025-02-05	[NESCTC Security Services]	bianlian	<a href="#">Link</a>
2025-02-05	[Shinsung Delta Tech]	lynx	<a href="#">Link</a>
2025-02-05	[Banfi Vintners]	lynx	<a href="#">Link</a>
2025-02-05	[annegrady.org]	ransomhub	<a href="#">Link</a>
2025-02-05	[rablighting.com]	qilin	<a href="#">Link</a>
2025-02-05	[boostheat.com]	apt73	<a href="#">Link</a>
2025-02-05	[rattelacademy.com]	funksec	<a href="#">Link</a>
2025-02-05	[cara.com.my]	funksec	<a href="#">Link</a>
2025-02-05	[Mid-State Machine & Fabricating Corp]	play	<a href="#">Link</a>
2025-02-04	[casperstruck.com]	kairos	<a href="#">Link</a>
2025-02-04	[medicalreportsltd.com]	kairos	<a href="#">Link</a>
2025-02-01	[LUA Coffee]	fog	<a href="#">Link</a>
2025-02-01	[GFZ Helmholtz Centre for Geosciences]	fog	<a href="#">Link</a>
2025-02-01	[PT. ITPRENEUR INDONESIA TECHNOLOGY]	fog	<a href="#">Link</a>
2025-02-04	[Devlion]	fog	<a href="#">Link</a>
2025-02-04	[SOLEIL]	fog	<a href="#">Link</a>
2025-02-04	[hemio.de]	fog	<a href="#">Link</a>
2025-02-03	[Madia]	fog	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-03	[X-lab group]	fog	<a href="#">Link</a>
2025-02-03	[Bolin Centre for Climate Research]	fog	<a href="#">Link</a>
2025-02-04	[Gitlabs: hemio.de, SOLEIL, Devlion]	fog	<a href="#">Link</a>
2025-02-04	[mielectric.com.br]	akira	<a href="#">Link</a>
2025-02-04	[engineeredequip.com]	akira	<a href="#">Link</a>
2025-02-04	[emin.cl]	akira	<a href="#">Link</a>
2025-02-04	[alphascriptrx.com]	akira	<a href="#">Link</a>
2025-02-04	[premierop.com]	akira	<a href="#">Link</a>
2025-02-04	[acesaz.com]	akira	<a href="#">Link</a>
2025-02-04	[mipa.com.br]	akira	<a href="#">Link</a>
2025-02-04	[usm-americas.com]	akira	<a href="#">Link</a>
2025-02-04	[feheq.com]	akira	<a href="#">Link</a>
2025-02-04	[stewartautosales.com]	akira	<a href="#">Link</a>
2025-02-04	[milleraa.com]	akira	<a href="#">Link</a>
2025-02-04	[jsfrental.com]	akira	<a href="#">Link</a>
2025-02-04	[summitmovinghouston.com]	akira	<a href="#">Link</a>
2025-02-04	[dwgp.com]	akira	<a href="#">Link</a>
2025-02-04	[easycom.com]	akira	<a href="#">Link</a>
2025-02-04	[alfa.com.co]	akira	<a href="#">Link</a>
2025-02-04	[westernwoodsinc.com]	akira	<a href="#">Link</a>
2025-02-04	[viscira.com]	akira	<a href="#">Link</a>
2025-02-04	[elitt-sas.fr]	akira	<a href="#">Link</a>
2025-02-04	[cfctech.com]	akira	<a href="#">Link</a>
2025-02-04	[armellini.com]	akira	<a href="#">Link</a>
2025-02-04	[mbacomputer.com]	akira	<a href="#">Link</a>
2025-02-04	[directex.net]	akira	<a href="#">Link</a>
2025-02-04	[360energy.com.ar]	akira	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-04	[saludsa.com.ec]	akira	<a href="#">Link</a>
2025-02-04	[intercomp.com.mt]	akira	<a href="#">Link</a>
2025-02-04	[C & R Molds Inc]	bianlian	<a href="#">Link</a>
2025-02-04	[Commercial Solutions]	bianlian	<a href="#">Link</a>
2025-02-04	[www.aymcdonald.com]	ransomhub	<a href="#">Link</a>
2025-02-04	[capstoneins.ca]	ransomhub	<a href="#">Link</a>
2025-02-04	[clarkfreightways.com]	ransomhub	<a href="#">Link</a>
2025-02-04	[mistralsolutions.com]	apt73	<a href="#">Link</a>
2025-02-04	[India car owners]	apt73	<a href="#">Link</a>
2025-02-04	[Alshu, Eshoo]	ransomhouse	<a href="#">Link</a>
2025-02-04	[kksp.com]	qilin	<a href="#">Link</a>
2025-02-04	[brainsystem.eu]	funksec	<a href="#">Link</a>
2025-02-04	[Taking stock of 2024	Part 2]	akira
2025-02-04	[esle.eu]	funksec	<a href="#">Link</a>
2025-02-04	[forum-rainbow-rp.forumotion.eu]	funksec	<a href="#">Link</a>
2025-02-04	[mgainnovation.com]	cactus	<a href="#">Link</a>
2025-02-04	[cornwelltools.com]	cactus	<a href="#">Link</a>
2025-02-04	[rashtiandrashti.com]	cactus	<a href="#">Link</a>
2025-02-04	[alojaimi.com]	ransomhub	<a href="#">Link</a>
2025-02-04	[www.aswgr.com]	ransomhub	<a href="#">Link</a>
2025-02-04	[heartlandrvs.com]	ransomhub	<a href="#">Link</a>
2025-02-04	[gaheritagefcu.org]	ransomhub	<a href="#">Link</a>
2025-02-04	[SSMC]	cicada3301	<a href="#">Link</a>
2025-02-04	[Rivers Casino and Rush Street Gaming]	cicada3301	<a href="#">Link</a>
2025-02-04	[Asterra Properties]	cicada3301	<a href="#">Link</a>
2025-02-04	[Caliente Construction]	cicada3301	<a href="#">Link</a>
2025-02-04	[C2S Technologies Inc.]	everest	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-04	[ITSS]	everest	<a href="#">Link</a>
2025-02-03	[brewsterfiredepartment.org]	safepay	<a href="#">Link</a>
2025-02-03	[Dickerson & Nieman Realtors]	play	<a href="#">Link</a>
2025-02-03	[Sheridan Nurseries]	play	<a href="#">Link</a>
2025-02-03	[The Hill Brush]	play	<a href="#">Link</a>
2025-02-03	[DPC Development]	play	<a href="#">Link</a>
2025-02-03	[Woodway USA]	play	<a href="#">Link</a>
2025-02-03	[Daniel Island Club]	play	<a href="#">Link</a>
2025-02-03	[QGS Development]	play	<a href="#">Link</a>
2025-02-03	[Gitlabs: Bolin Centre for Climate Research, X-lab group, Madia]	fog	<a href="#">Link</a>
2025-02-03	[gruppozaccaria.it]	lockbit3	<a href="#">Link</a>
2025-02-03	[Karadeniz Holding (karadenizholding.com)]	fog	<a href="#">Link</a>
2025-02-03	[www.wongfleming.com]	ransomhub	<a href="#">Link</a>
2025-02-03	[smithmidland.com]	ransomhub	<a href="#">Link</a>
2025-02-03	[www.origene.com]	ransomhub	<a href="#">Link</a>
2025-02-03	[Denton Regional Suicide Prevention Coalition]	qilin	<a href="#">Link</a>
2025-02-03	[fasttrackcargo.com]	funksec	<a href="#">Link</a>
2025-02-03	[Ponte16 Hotel & Casino]	killsec	<a href="#">Link</a>
2025-02-03	[Elslaw.com ( EARLY , LUCARELLI , SWEENEY & MEISENKOTHEN LAW )]	qilin	<a href="#">Link</a>
2025-02-03	[DRI Title & Escrow]	qilin	<a href="#">Link</a>
2025-02-03	[DPA Auctions]	qilin	<a href="#">Link</a>
2025-02-03	[Altair Travel]	qilin	<a href="#">Link</a>
2025-02-03	[Civil Design, Inc]	qilin	<a href="#">Link</a>
2025-02-03	[The Gatesworth Senior Living St. Louis]	qilin	<a href="#">Link</a>
2025-02-03	[GOVirtual-it.com ( VIRTUAL IT )]	qilin	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-03	[coel.com.mx]	apt73	<a href="#">Link</a>
2025-02-03	[Alford Walden Law]	qilin	<a href="#">Link</a>
2025-02-03	[Pasco Systems]	qilin	<a href="#">Link</a>
2025-02-03	[MPP Group of Companies]	qilin	<a href="#">Link</a>
2025-02-03	[Pineland community service board]	spacebears	<a href="#">Link</a>
2025-02-02	[usuhs.edu]	lockbit3	<a href="#">Link</a>
2025-02-02	[Four Eye Clinics]	abyss	<a href="#">Link</a>
2025-02-02	[jpcgroupinc.com]	abyss	<a href="#">Link</a>
2025-02-02	[hreu.eu]	funksec	<a href="#">Link</a>
2025-02-02	[Tosaf]	handala	<a href="#">Link</a>
2025-02-02	[turbomp]	stormous	<a href="#">Link</a>
2025-02-02	[Cyrious Software]	bianlian	<a href="#">Link</a>
2025-02-02	[Medical Associates of Brevard]	bianlian	<a href="#">Link</a>
2025-02-02	[Civic Committee]	bianlian	<a href="#">Link</a>
2025-02-02	[Ayres Law Firm]	bianlian	<a href="#">Link</a>
2025-02-02	[Growth Acceleration Partners]	bianlian	<a href="#">Link</a>
2025-02-01	[fiberskynet.net]	funksec	<a href="#">Link</a>
2025-02-01	[tirtaraharja.co.id]	funksec	<a href="#">Link</a>
2025-02-01	[Gitlabs: PT. ITPRENEUR INDONESIA TECHNOLOGY, GFZ Helmholtz Centre for Geosciences, LUA Cof...]	fog	<a href="#">Link</a>
2025-02-01	[myisp.live]	funksec	<a href="#">Link</a>
2025-02-01	[DATACONSULTANTS.COM]	clop	<a href="#">Link</a>
2025-02-01	[CHAMPIONHOMES.COM]	clop	<a href="#">Link</a>
2025-02-01	[CIERANT.COM]	clop	<a href="#">Link</a>
2025-02-01	[DATATRAC.COM]	clop	<a href="#">Link</a>
2025-02-01	[Nano Health]	killsec	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-01	[St. Nicholas School]	8base	<a href="#">Link</a>
2025-02-01	[Héron]	8base	<a href="#">Link</a>
2025-02-01	[Tan Teck Seng Electric (Co) Pte Ltd]	8base	<a href="#">Link</a>
2025-02-01	[High Learn Ltd]	8base	<a href="#">Link</a>
2025-02-01	[CAMRIDGEPORT]	spacebears	<a href="#">Link</a>
2025-02-01	[Falcon Gaming]	arcusmedia	<a href="#">Link</a>
2025-02-01	[Eascon]	arcusmedia	<a href="#">Link</a>
2025-02-01	[Utilissimo Transportes]	arcusmedia	<a href="#">Link</a>
2025-02-01	[GATTELLI SpA]	arcusmedia	<a href="#">Link</a>
2025-02-01	[Technico]	arcusmedia	<a href="#">Link</a>
2025-02-01	[Wireless Solutions (Morris.Domain)]	lynx	<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.