


---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20250215



## 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 Alte S3-Buckets ausgraben, Sachen hacken ☒ . . . . .	12
<b>5 Cyberangriffe: (Feb)</b>	<b>13</b>
<b>6 Ransomware-Erpressungen: (Feb)</b>	<b>13</b>
<b>7 Quellen</b>	<b>29</b>
7.1 Quellenverzeichnis . . . . .	29
<b>8 Impressum</b>	<b>31</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

#### ***Palo Alto PAN-OS: Exploit-Code für hochriskante Lücke aufgetaucht***

Im Betriebssystem PAN-OS für Firewalls von Palo Alto Networks klaffen Sicherheitslücken. Für eine davon gibt es bereits Exploit-Code.

- [Link](#)

—

#### ***Sicherheitslücke: Angreifer können PostgreSQL-Datenbanken attackieren***

Ein Sicherheitspatch schließt eine Schadcode-Lücke im Datenbankmanagementsystem PostgreSQL.

- [Link](#)

—

#### ***Progress Telerik und Loadmaster: Updates dichten Sicherheitslecks ab***

In Loadmaster und Telerik von Progress hat der Hersteller hochriskante Schwachstellen entdeckt. Updates bessern sie aus.

- [Link](#)

—

#### ***Lexmark warnt vor Sicherheitslücken in Drucker-Software und -Firmware***

Lexmark hat Sicherheitslücken in Drucker-Firmware und Begleitsoftware gefunden. Updates stehen bereit, um sie zu schließen.

- [Link](#)

—

#### ***Sicherheitslücken: Gitlab-Entwickler raten zu zügigem Update***

Gitlab ist unter anderem für DoS-Attacken anfällig. Außerdem können vertrauliche Informationen leaken.

- [Link](#)

—

#### ***Patchday: Intel schließt Sicherheitslücken in CPUs und Grafiktreibern***

Es sind wichtige Updates für verschiedene Produkte von Intel erschienen. Admins sollten sie zeitnah installieren.

- [Link](#)

—

#### ***Fortinet: Angriffe auf Schwachstellen laufen, Updates für diverse Produkte***

Fortinet hat für zahlreiche Produkte Sicherheitsupdates veröffentlicht. Mindestens eine Lücke wird bereits attackiert.

- [Link](#)

—

***Adobe-Patchday: Schadcode-Sicherheitslücken gefährden Illustrator & Co.***

Angreifer können an mehreren Sicherheitslücken in Anwendungen von Adobe ansetzen, um Computer zu kompromittieren.

- [Link](#)

—

***Ivanti: Kritische Codeschmuggel-Lücken in VPN und CSA***

In Ivanti VPN-Software ICS, IPS und ISAC sowie in Ivanti CSA klaffen kritische Sicherheitslecks. Angreifer können Schadcode unterjubeln.

- [Link](#)

—

***Microsoft-Patchday: Angreifer attackieren Windows und löschen Daten***

Es sind wichtige Sicherheitsupdates für Azure, Office, Windows und Co. erschienen. Es gibt bereits Attacken. Weitere können bevorstehen.

- [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	0.999850000	<a href="#">Link</a>
CVE-2024-9465	0.943220000	0.994140000	<a href="#">Link</a>
CVE-2024-9463	0.961860000	0.996690000	<a href="#">Link</a>
CVE-2024-8963	0.967240000	0.997850000	<a href="#">Link</a>
CVE-2024-7593	0.971650000	0.999010000	<a href="#">Link</a>
CVE-2024-6893	0.938390000	0.993690000	<a href="#">Link</a>
CVE-2024-6670	0.904230000	0.991080000	<a href="#">Link</a>
CVE-2024-5910	0.962890000	0.996900000	<a href="#">Link</a>
CVE-2024-55956	0.969490000	0.998420000	<a href="#">Link</a>
CVE-2024-5217	0.933860000	0.993240000	<a href="#">Link</a>
CVE-2024-50623	0.969520000	0.998430000	<a href="#">Link</a>
CVE-2024-50603	0.924330000	0.992450000	<a href="#">Link</a>
CVE-2024-4879	0.934670000	0.993320000	<a href="#">Link</a>
CVE-2024-4577	0.958420000	0.996120000	<a href="#">Link</a>
CVE-2024-4358	0.925270000	0.992520000	<a href="#">Link</a>
CVE-2024-41713	0.957210000	0.995910000	<a href="#">Link</a>
CVE-2024-40711	0.962170000	0.996750000	<a href="#">Link</a>
CVE-2024-4040	0.969020000	0.998300000	<a href="#">Link</a>
CVE-2024-38856	0.950120000	0.994940000	<a href="#">Link</a>
CVE-2024-36401	0.955950000	0.995730000	<a href="#">Link</a>
CVE-2024-3400	0.964000000	0.997130000	<a href="#">Link</a>
CVE-2024-3273	0.937410000	0.993610000	<a href="#">Link</a>
CVE-2024-32113	0.933050000	0.993170000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-28995	0.965000000	0.997350000	<a href="#">Link</a>
CVE-2024-28987	0.961930000	0.996700000	<a href="#">Link</a>
CVE-2024-27348	0.960260000	0.996420000	<a href="#">Link</a>
CVE-2024-27198	0.969340000	0.998380000	<a href="#">Link</a>
CVE-2024-24919	0.960980000	0.996530000	<a href="#">Link</a>
CVE-2024-23897	0.973540000	0.999550000	<a href="#">Link</a>
CVE-2024-2389	0.900180000	0.990820000	<a href="#">Link</a>
CVE-2024-23692	0.964390000	0.997240000	<a href="#">Link</a>
CVE-2024-21893	0.956970000	0.995860000	<a href="#">Link</a>
CVE-2024-21887	0.973220000	0.999490000	<a href="#">Link</a>
CVE-2024-20767	0.965330000	0.997420000	<a href="#">Link</a>
CVE-2024-1709	0.957220000	0.995910000	<a href="#">Link</a>
CVE-2024-1212	0.937140000	0.993570000	<a href="#">Link</a>
CVE-2024-0986	0.955530000	0.995670000	<a href="#">Link</a>
CVE-2024-0195	0.962680000	0.996850000	<a href="#">Link</a>
CVE-2024-0012	0.969980000	0.998550000	<a href="#">Link</a>

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

Fri, 14 Feb 2025

#### **[UPDATE] [hoch] Apple Mac OS: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstelle in Apple Mac OS ausnutzen, um Code mit Kernel Privilegien auszuführen, Sicherheitsvorkehrungen zu umgehen, einen Denial of Service Angriff durchzuführen oder vertrauliche Daten einzusehen.

- [Link](#)

—

Fri, 14 Feb 2025

#### **[UPDATE] [hoch] IEEE WPA2: Mehrere Schwachstellen**

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in IEEE WPA2 ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Fri, 14 Feb 2025

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

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

- [Link](#)

—

Fri, 14 Feb 2025

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

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

- [Link](#)

—

Fri, 14 Feb 2025

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in OpenSSL ausnutzen, um beliebigen Programmcode mit den Rechten des Dienstes auszuführen, Sicherheitsvorkehrungen zu umgehen, Dateien zu manipulieren oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

—

Fri, 14 Feb 2025

**[UPDATE] [hoch] AMD Prozessoren: Mehrere Schwachstellen ermöglichen Offenlegung von Informationen**

Ein Angreifer kann mehrere Schwachstellen im AMD Prozessoren ausnutzen, um Informationen offenzulegen.

- [Link](#)

—

Fri, 14 Feb 2025

**[UPDATE] [hoch] AMD Prozessoren: Mehrere Schwachstellen**

Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in AMD Prozessoren ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen und Daten zu manipulieren.

- [Link](#)



—

Fri, 14 Feb 2025

**[UPDATE] [hoch] Grafana: Schwachstelle ermöglicht Übernahme von Benutzerkonto**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Grafana ausnutzen, um ein Benutzerkonto zu übernehmen.

- [Link](#)

—

Fri, 14 Feb 2025

**[UPDATE] [hoch] AMD Prozessoren: Mehrere Schwachstellen**

Ein lokaler Angreifer kann mehrere Schwachstellen in AMD Prozessoren ausnutzen, um beliebigen Programmcode auszuführen oder Informationen offenzulegen.

- [Link](#)

—

Fri, 14 Feb 2025

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

Ein lokaler Angreifer kann eine Schwachstelle in BusyBox ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 14 Feb 2025

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

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

- [Link](#)

—

Fri, 14 Feb 2025

**[UPDATE] [kritisch] Apache ActiveMQ: Schwachstelle ermöglicht Codeausführung**

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

- [Link](#)

—

Fri, 14 Feb 2025

**[UPDATE] [hoch] Apache ActiveMQ: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Apache ActiveMQ ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 14 Feb 2025

**[UPDATE] [hoch] EDK2 NetworkPkg IP stack implementation: Mehrere Schwachstellen**

Ein Angreifer aus dem angrenzenden Netzwerk oder ein entfernter, anonym Angreifer kann mehrere Schwachstellen in der EDK2 NetworkPkg IP stack implementation ausnutzen, um beliebigen Programmcode auszuführen, vertrauliche Informationen offenzulegen und einen Denial of Service Zustand auszulösen.

- [Link](#)

—

Fri, 14 Feb 2025

**[UPDATE] [hoch] PostgreSQL JDBC Driver: Schwachstelle ermöglicht SQL-Injection**

Ein entfernter, anonym Angreifer kann eine Schwachstelle in PostgreSQL JDBC Driver ausnutzen, um eine SQL-Injection durchzuführen.

- [Link](#)

—

Fri, 14 Feb 2025

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

Ein lokaler Angreifer kann eine Schwachstelle in less ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 14 Feb 2025

**[UPDATE] [hoch] GNU libc: Schwachstelle ermöglicht Codeausführung**

Ein Angreifer kann eine Schwachstelle in GNU libc ausnutzen, um einen Denial-of-Service-Zustand zu verursachen, Code auszuführen oder seine Privilegien zu erweitern.

- [Link](#)

—

Fri, 14 Feb 2025

**[UPDATE] [hoch] RADIUS: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen**

Ein lokaler Angreifer kann eine Schwachstelle im RADIUS Protokoll ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Fri, 14 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, 14 Feb 2025

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

Ein Angreifer kann mehrere Schwachstellen in Redis ausnutzen, um einen Denial of Service Angriff durchzuführen oder Code auszuführen.

- [Link](#)

### 3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
2/14/2025	[RockyLinux 8 : firefox (RLSA-2025:1283)]	critical
2/14/2025	[RockyLinux 8 : bzip2 (RLSA-2025:0733)]	critical
2/14/2025	[RockyLinux 8 : grafana (RLSA-2025:0401)]	critical
2/14/2025	[RockyLinux 8 : keepalived (RLSA-2025:0743)]	critical
2/14/2025	[RockyLinux 8 : thunderbird (RLSA-2025:1292)]	critical
2/14/2025	[Ivanti Policy Secure 22.x < 22.7R1.3 RCE]	critical
2/14/2025	[Ivanti Connect Secure 22.x < 22.7R2.4 Multiple Vulnerabilities]	critical
2/14/2025	[Ivanti Connect Secure 22.x < 22.7R2.6 Multiple Vulnerabilities]	critical
2/14/2025	[RockyLinux 8 : kernel-rt (RLSA-2025:1067)]	high
2/14/2025	[RockyLinux 8 : unbound (RLSA-2025:0837)]	high
2/14/2025	[RockyLinux 8 : libsoup (RLSA-2025:0838)]	high
2/14/2025	[RockyLinux 8 : container-tools:rhel8 (RLSA-2025:1372)]	high
2/14/2025	[RockyLinux 8 : .NET 9.0 (RLSA-2025:0382)]	high
2/14/2025	[RockyLinux 8 : glibc (RLSA-2024:3269)]	high
2/14/2025	[RockyLinux 9 : nodejs:20 (RLSA-2025:1443)]	high
2/14/2025	[RockyLinux 9 : git-lfs (RLSA-2025:0673)]	high
2/14/2025	[RockyLinux 8 : git-lfs (RLSA-2025:0845)]	high

Datum	Schwachstelle	Bewertung
2/14/2025	[RockyLinux 8 : kernel (RLSA-2025:1068)]	high
2/14/2025	[Security Updates for Microsoft Visio Products C2R (February 2025)]	high
2/14/2025	[Security Updates for Microsoft Access Products C2R (February 2025)]	high
2/14/2025	[Security Updates for Microsoft Excel Products C2R (February 2025)]	high
2/14/2025	[Security Updates for Microsoft Word Products C2R (February 2025)]	high
2/14/2025	[Security Updates for Microsoft Office Products C2R (February 2024)]	high
2/14/2025	[Oracle Linux 9 : libxml2 (ELSA-2025-1350)]	high
2/14/2025	[Oracle Linux 8 : container-tools:ol8 (ELSA-2025-1372)]	high
2/14/2025	[RHEL 9 : kpatch-patch-5_14_0-427_13_1, kpatch-patch-5_14_0-427_31_1, and kpatch-patch-5_14_0-427_44_1 (RHSA-2025:1434)]	high
2/14/2025	[RHEL 9 : kpatch-patch-5_14_0-284_52_1, kpatch-patch-5_14_0-284_79_1, and kpatch-patch-5_14_0-284_92_1 (RHSA-2025:1437)]	high
2/14/2025	[RHEL 9 : nodejs:20 (RHSA-2025:1443)]	high
2/14/2025	[AlmaLinux 9 : libxml2 (ALSA-2025:1350)]	high
2/14/2025	[RHEL 9 : kpatch-patch-5_14_0-503_15_1 (RHSA-2025:1433)]	high
2/14/2025	[Oracle Linux 9 : nodejs:20 (ELSA-2025-1443)]	high

## 4 Die Hacks der Woche

mit Martin Haunschmid

#### 4.0.1 Alte S3-Buckets ausgraben, Sachen hacken ☒



[Zum Youtube Video](#)

## 5 Cyberangriffe: (Feb)

Datum	Opfer	Land	Information
2025-02-13	Eckert & Ziegler SE	[DEU]	<a href="#">Link</a>
2025-02-13	Université de la Bundeswehr	[DEU]	<a href="#">Link</a>
2025-02-11	Port of Oostende	[BEL]	<a href="#">Link</a>
2025-02-11	Ville de Tulln	[AUT]	<a href="#">Link</a>
2025-02-10	LUP-Kliniken	[DEU]	<a href="#">Link</a>
2025-02-10	City of Tarrant	[USA]	<a href="#">Link</a>
2025-02-10	Sault Tribe, Kewadin Casinos	[USA]	<a href="#">Link</a>
2025-02-10	Secrétariat de la Conférence des évêques allemands (Deutsche Bischofskonferenz)	[DEU]	<a href="#">Link</a>
2025-02-09	Williamsburg James City County Public Schools	[USA]	<a href="#">Link</a>
2025-02-08	FORTUNE ELECTRIC CO.,LTD	[TWN]	<a href="#">Link</a>
2025-02-07	Transcend Information, Inc.	[TWN]	<a href="#">Link</a>
2025-02-05	IMI	[GBR]	<a href="#">Link</a>
2025-02-05	REMSA Health	[USA]	<a href="#">Link</a>
2025-02-04	Pinehurst Radiology	[USA]	<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
2025-02-11	[Hydronic & Steam Equipment]	play	<a href="#">Link</a>
2025-02-11	[Ratioparts]	play	<a href="#">Link</a>
2025-02-11	[CST Corp]	play	<a href="#">Link</a>
2025-02-14	[Heritage South Credit Union]	embargo	<a href="#">Link</a>
2025-02-14	[Primaveras]	akira	<a href="#">Link</a>
2025-02-08	[www.calspa.it]	ransomhub	<a href="#">Link</a>
2025-02-14	[Nelson & Townsend, CPA's]	akira	<a href="#">Link</a>
2025-02-14	[Castle Rock Construction Company]	akira	<a href="#">Link</a>
2025-02-14	[Genus]	akira	<a href="#">Link</a>
2025-02-14	[Window World of Raleigh]	akira	<a href="#">Link</a>
2025-02-14	[F.TECH R&D NORTH AMERICA INC.]	qilin	<a href="#">Link</a>
2025-02-14	[Go Strictly]	akira	<a href="#">Link</a>
2025-02-14	[Bethany Lutheran Church]	qilin	<a href="#">Link</a>
2025-02-10	[GANRO]	lynx	<a href="#">Link</a>
2025-02-14	[Regency Media]	akira	<a href="#">Link</a>
2025-02-14	[brockbanks.co.uk]	ransomhub	<a href="#">Link</a>
2025-02-14	[The Agency]	rhysida	<a href="#">Link</a>
2025-02-13	[Shields Facilities Maintenance]	play	<a href="#">Link</a>
2025-02-13	[ADULLACT]	fog	<a href="#">Link</a>
2025-02-13	[Ayomi]	fog	<a href="#">Link</a>
2025-02-13	[Omydoo]	fog	<a href="#">Link</a>
2025-02-13	[Gitlabs: Omydoo, Ayomi, ADULLACT]	fog	<a href="#">Link</a>
2025-02-13	[Aspire Rural Health System]	bianlian	<a href="#">Link</a>
2025-02-13	[leonardo.com]	threeam	<a href="#">Link</a>
2025-02-13	[Mozo Grau (mozo-grau.com)]	fog	<a href="#">Link</a>
2025-02-13	[CoMo-Industrial Engineering]	akira	<a href="#">Link</a>
2025-02-13	[enventuregt.com]	ransomhub	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-13	[snoqualmietribe.us]	ransomhub	<a href="#">Link</a>
2025-02-13	[vadatech.com]	qilin	<a href="#">Link</a>
2025-02-13	[Nippon Steel USA]	bianlian	<a href="#">Link</a>
2025-02-13	[Financial Services of America, Inc.]	bianlian	<a href="#">Link</a>
2025-02-13	[Layfield & Borel CPA's L.L.C]	bianlian	<a href="#">Link</a>
2025-02-13	[Dain, Torpy, Le Ray, Wiest & Garner, P.C.]	bianlian	<a href="#">Link</a>
2025-02-13	[Dan Eckman CPA]	akira	<a href="#">Link</a>
2025-02-12	[Elite Advanced LaserCorporation]	akira	<a href="#">Link</a>
2025-02-12	[Obex Medical]	killsec	<a href="#">Link</a>
2025-02-12	[Cache Valley ENT]	medusa	<a href="#">Link</a>
2025-02-12	[JP Express]	medusa	<a href="#">Link</a>
2025-02-12	[Central District Health Department]	medusa	<a href="#">Link</a>
2025-02-12	[morrisgroup.co]	clop	<a href="#">Link</a>
2025-02-05	[stjerome.org]	safepay	<a href="#">Link</a>
2025-02-12	[Therma Seal Insulation Systems]	ciphbit	<a href="#">Link</a>
2025-02-12	[Squeezer-software]	fog	<a href="#">Link</a>
2025-02-12	[Spacemanic]	fog	<a href="#">Link</a>
2025-02-12	[INGV]	fog	<a href="#">Link</a>
2025-02-12	[Gitlabs: INGV, Spacemanic, Squeezer-software]	fog	<a href="#">Link</a>
2025-02-12	[Quality Home Health Care]	qilin	<a href="#">Link</a>
2025-02-12	[avtovelomoto.by]	funksec	<a href="#">Link</a>
2025-02-12	[alderconstruction.com]	ransomhub	<a href="#">Link</a>
2025-02-12	[steveallcorn.remax.com]	ransomhub	<a href="#">Link</a>
2025-02-12	[bergconst.com]	ransomhub	<a href="#">Link</a>
2025-02-12	[burdickpainting.com]	ransomhub	<a href="#">Link</a>
2025-02-12	[columbiacabinets.com]	ransomhub	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-12	[ekvallbyrne.com]	ransomhub	<a href="#">Link</a>
2025-02-12	[krmcustomhomes.com]	ransomhub	<a href="#">Link</a>
2025-02-12	[lateralending.com]	ransomhub	<a href="#">Link</a>
2025-02-12	[minnesotaexteriors.com]	ransomhub	<a href="#">Link</a>
2025-02-12	[rogerspetro.com]	ransomhub	<a href="#">Link</a>
2025-02-12	[sundanceliving.com]	ransomhub	<a href="#">Link</a>
2025-02-12	[thejdkgroup.com]	ransomhub	<a href="#">Link</a>
2025-02-12	[twncomm.com]	ransomhub	<a href="#">Link</a>
2025-02-12	[Vicky Foods]	akira	<a href="#">Link</a>
2025-02-12	[Hess (hess-gmbh.de)]	fog	<a href="#">Link</a>
2025-02-12	[TJKM]	qilin	<a href="#">Link</a>
2025-02-03	[askgs.ma]	ransomhub	<a href="#">Link</a>
2025-02-12	[slchc.edu]	ransomhub	<a href="#">Link</a>
2025-02-12	[weathersa.co.za]	ransomhub	<a href="#">Link</a>
2025-02-12	[Erie Management Group, LLC]	qilin	<a href="#">Link</a>
2025-02-12	[curtisint.com]	cactus	<a href="#">Link</a>
2025-02-12	[britannicahome.com]	cactus	<a href="#">Link</a>
2025-02-12	[uniquehd.com]	cactus	<a href="#">Link</a>
2025-02-12	[tomsmithindustries.com]	qilin	<a href="#">Link</a>
2025-02-04	[Accelerator]	dragonforce	<a href="#">Link</a>
2025-02-04	[O&S Associates]	dragonforce	<a href="#">Link</a>
2025-02-12	[Leading Edge Specialized Dentistry]	rhysida	<a href="#">Link</a>
2025-02-12	[Hammond Trucking & Excavation]	rhysida	<a href="#">Link</a>
2025-02-12	[BH Aircraft Company, Inc.]	rhysida	<a href="#">Link</a>
2025-02-12	[My New Jersey Dentist]	rhysida	<a href="#">Link</a>
2025-02-12	[Town Counsel Law & Litigation]	rhysida	<a href="#">Link</a>
2025-02-06	[MICRO MANUFACTURING]	medusalocker	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-05	[The Brown & Hurley Group]	lynx	<a href="#">Link</a>
2025-02-11	[Tie Down Engineering]	play	<a href="#">Link</a>
2025-02-11	[Monroe Transportation Services Inc]	play	<a href="#">Link</a>
2025-02-11	[Kensington Glass Arts]	play	<a href="#">Link</a>
2025-02-11	[EAC Consulting]	play	<a href="#">Link</a>
2025-02-11	[Baltimore Country Club]	play	<a href="#">Link</a>
2025-02-11	[Jildor Shoes]	play	<a href="#">Link</a>
2025-02-11	[Mainline Information Systems]	play	<a href="#">Link</a>
2025-02-11	[Fastighetsservice AB]	play	<a href="#">Link</a>
2025-02-11	[CESI]	termite	<a href="#">Link</a>
2025-02-11	[Shinn Fu Company of America]	play	<a href="#">Link</a>
2025-02-11	[ROCK SOLID Stabilization & Reclamation]	play	<a href="#">Link</a>
2025-02-11	[Cold Storage Manufacturing]	play	<a href="#">Link</a>
2025-02-11	[Neaton Auto Products Manufacturing]	play	<a href="#">Link</a>
2025-02-11	[Saint George's College (saintgeorge.cl)]	fog	<a href="#">Link</a>
2025-02-11	[Aurora Public Schools (aurorak12.org)]	fog	<a href="#">Link</a>
2025-02-11	[Natures Organics]	medusa	<a href="#">Link</a>
2025-02-11	[Paignton Zoo]	medusa	<a href="#">Link</a>
2025-02-11	[SRP Companies]	medusa	<a href="#">Link</a>
2025-02-11	[lacold.com]	clap	<a href="#">Link</a>
2025-02-11	[The University of Notre Dame Australia (nd.edu.au)]	fog	<a href="#">Link</a>
2025-02-11	[Prime Trust Financial]	akira	<a href="#">Link</a>
2025-02-01	[sehma.com]	threeam	<a href="#">Link</a>
2025-02-11	[I.B.G SPA]	sarcoma	<a href="#">Link</a>
2025-02-11	[Idi-trucking-inc]	sarcoma	<a href="#">Link</a>
2025-02-11	[Wisper Reimer Ingenieure GmbH]	sarcoma	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-11	[Unimicron]	sarcoma	<a href="#">Link</a>
2025-02-11	[Logix Corporate Solutions]	killsec	<a href="#">Link</a>
2025-02-11	[sole technology]	monti	<a href="#">Link</a>
2025-02-10	[primesourcestaffing.com]	ransomhub	<a href="#">Link</a>
2025-02-04	[The Children's Center Of Hamden]	incransom	<a href="#">Link</a>
2025-02-10	[komline.com]	ransomhub	<a href="#">Link</a>
2025-02-10	[bazcooil.com]	ransomhub	<a href="#">Link</a>
2025-02-10	[sdfab.com]	ransomhub	<a href="#">Link</a>
2025-02-10	[kaplanstahler.com]	ransomhub	<a href="#">Link</a>
2025-02-04	[www.jsp.com]	ransomhub	<a href="#">Link</a>
2025-02-10	[ekonom.com]	cllop	<a href="#">Link</a>
2025-02-10	[editel.eu]	cllop	<a href="#">Link</a>
2025-02-10	[derrytransport.com]	cllop	<a href="#">Link</a>
2025-02-10	[dana-co.com]	cllop	<a href="#">Link</a>
2025-02-10	[designndesigninc.com]	cllop	<a href="#">Link</a>
2025-02-10	[daatagroup.com]	cllop	<a href="#">Link</a>
2025-02-10	[dunnriteproducts.com]	cllop	<a href="#">Link</a>
2025-02-10	[d2go.io]	cllop	<a href="#">Link</a>
2025-02-10	[dynastyfootwear.com]	cllop	<a href="#">Link</a>
2025-02-10	[dxc.com]	cllop	<a href="#">Link</a>
2025-02-10	[dundasjafine.com]	cllop	<a href="#">Link</a>
2025-02-10	[drexel.ca]	cllop	<a href="#">Link</a>
2025-02-10	[donlen.com]	cllop	<a href="#">Link</a>
2025-02-10	[dlfna.com]	cllop	<a href="#">Link</a>
2025-02-04	[directex.net]	cllop	<a href="#">Link</a>
2025-02-10	[diazfoods.com]	cllop	<a href="#">Link</a>
2025-02-10	[detecno.com]	cllop	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-10	[deltaenterprise.com]	clon	<a href="#">Link</a>
2025-02-10	[deltachildren.com]	clon	<a href="#">Link</a>
2025-02-10	[decescente.com]	clon	<a href="#">Link</a>
2025-02-10	[dbetances.com]	clon	<a href="#">Link</a>
2025-02-10	[datapakservices.com]	clon	<a href="#">Link</a>
2025-02-10	[coglans.com]	clon	<a href="#">Link</a>
2025-02-10	[cycle.local]	clon	<a href="#">Link</a>
2025-02-10	[cassinfo.com]	clon	<a href="#">Link</a>
2025-02-10	[claw.local]	clon	<a href="#">Link</a>
2025-02-10	[cgdc.cottong.local]	clon	<a href="#">Link</a>
2025-02-10	[cps.k12.il.us]	clon	<a href="#">Link</a>
2025-02-10	[conbraco.com]	clon	<a href="#">Link</a>
2025-02-10	[clearon.com]	clon	<a href="#">Link</a>
2025-02-10	[crestmills.com]	clon	<a href="#">Link</a>
2025-02-10	[cranebsu.com]	clon	<a href="#">Link</a>
2025-02-10	[covetra.com]	clon	<a href="#">Link</a>
2025-02-10	[connexion-informatique.fr]	clon	<a href="#">Link</a>
2025-02-10	[compasshealthbrands.com]	clon	<a href="#">Link</a>
2025-02-10	[collectionxiix.com]	clon	<a href="#">Link</a>
2025-02-10	[coghlans.com]	clon	<a href="#">Link</a>
2025-02-10	[codagami.com]	clon	<a href="#">Link</a>
2025-02-10	[cmcoldstores.com]	clon	<a href="#">Link</a>
2025-02-10	[classicaccessories.com]	clon	<a href="#">Link</a>
2025-02-10	[cinema1.ca]	clon	<a href="#">Link</a>
2025-02-10	[cherokeedistributing.com]	clon	<a href="#">Link</a>
2025-02-10	[chemstarcop.com]	clon	<a href="#">Link</a>
2025-02-10	[challenger.com]	clon	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-10	[cesarcastillo.com]	cllop	<a href="#">Link</a>
2025-02-10	[cedarsfoods.com]	cllop	<a href="#">Link</a>
2025-02-10	[cathayhome.com]	cllop	<a href="#">Link</a>
2025-02-10	[catchuplogistics.com]	cllop	<a href="#">Link</a>
2025-02-10	[castlewoodapparel.com]	cllop	<a href="#">Link</a>
2025-02-10	[carlsondistributing.com]	cllop	<a href="#">Link</a>
2025-02-10	[Enfin]	killsec	<a href="#">Link</a>
2025-02-10	[Recievership Specialists]	bianlian	<a href="#">Link</a>
2025-02-10	[abcapital.com.ph]	lockbit3	<a href="#">Link</a>
2025-02-10	[Allen & Pinnix]	akira	<a href="#">Link</a>
2025-02-10	[The Pawn]	akira	<a href="#">Link</a>
2025-02-10	[Polstermöbel Oelsa GmbH]	sarcoma	<a href="#">Link</a>
2025-02-03	[Grail Springs Retreat]	medusa	<a href="#">Link</a>
2025-02-05	[Rural Health Services]	medusa	<a href="#">Link</a>
2025-02-07	[Adler Shine LLP]	medusa	<a href="#">Link</a>
2025-02-07	[SimonMed Imaging]	medusa	<a href="#">Link</a>
2025-02-08	[PAD Aviation Technics GmbH]	medusa	<a href="#">Link</a>
2025-02-10	[Serenity Salon & Spa]	medusa	<a href="#">Link</a>
2025-02-10	[Michael's Hair Body Mind]	medusa	<a href="#">Link</a>
2025-02-10	[Greenwich Medical Spa]	medusa	<a href="#">Link</a>
2025-02-10	[Capital Cell Global (CCG)]	killsec	<a href="#">Link</a>
2025-02-10	[ASRAM Medical College and Hospita]	killsec	<a href="#">Link</a>
2025-02-10	[CAPITALFINEMEATS.COM]	cllop	<a href="#">Link</a>
2025-02-10	[CALIFORNIARAINLA.COM]	cllop	<a href="#">Link</a>
2025-02-10	[CAINEWAREHOUSING.COM]	cllop	<a href="#">Link</a>
2025-02-10	[BARCOMADE.COM]	cllop	<a href="#">Link</a>
2025-02-10	[BEINOGLUO.GR]	cllop	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-10	[BIAGIBROS.COM]	clon	<a href="#">Link</a>
2025-02-10	[BSIEDI.COM]	clon	<a href="#">Link</a>
2025-02-10	[BOZICKDIST.COM]	clon	<a href="#">Link</a>
2025-02-10	[BOWANDARROWPET.COM]	clon	<a href="#">Link</a>
2025-02-10	[BOSSCHAIR.COM]	clon	<a href="#">Link</a>
2025-02-10	[BESTBRANDSINC.COM]	clon	<a href="#">Link</a>
2025-02-10	[BERKSHIREINC.COM]	clon	<a href="#">Link</a>
2025-02-10	[BENSONMILLS.COM]	clon	<a href="#">Link</a>
2025-02-10	[BENBECKER.EU]	clon	<a href="#">Link</a>
2025-02-10	[BAYSIDENH.COM]	clon	<a href="#">Link</a>
2025-02-10	[BARRETTDISTRIBUTION.COM]	clon	<a href="#">Link</a>
2025-02-10	[BACKYARDDISCOVERY.COM]	clon	<a href="#">Link</a>
2025-02-10	[ALEGACY.COM]	clon	<a href="#">Link</a>
2025-02-10	[AURORAIMPORTING.COM]	clon	<a href="#">Link</a>
2025-02-10	[ARLAN.NL]	clon	<a href="#">Link</a>
2025-02-10	[ARKIEJIGS.COM]	clon	<a href="#">Link</a>
2025-02-10	[APOLLOCORP.COM]	clon	<a href="#">Link</a>
2025-02-10	[AOL.COM AJ MISSERT INC]	clon	<a href="#">Link</a>
2025-02-10	[ANNABELLECANDY.COM]	clon	<a href="#">Link</a>
2025-02-10	[ANDROSNA.COM]	clon	<a href="#">Link</a>
2025-02-10	[ANDREWSDISTRIBUTING.COM]	clon	<a href="#">Link</a>
2025-02-10	[AMSINO.COM]	clon	<a href="#">Link</a>
2025-02-10	[AMERICANLIGHTING.COM]	clon	<a href="#">Link</a>
2025-02-10	[ALPADVANTAGE.COM]	clon	<a href="#">Link</a>
2025-02-10	[ALLTECH.COM]	clon	<a href="#">Link</a>
2025-02-10	[ALLIANCEMERCANTILE.COM]	clon	<a href="#">Link</a>
2025-02-10	[AIRLIQUIDE.COM]	clon	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-10	[AGILITYAUTOPARTS.COM]	clon	<a href="#">Link</a>
2025-02-10	[AFFINITYCANADA.COM]	clon	<a href="#">Link</a>
2025-02-10	[ACTIAN.COM]	clon	<a href="#">Link</a>
2025-02-10	[ACPIDEAS.COM]	clon	<a href="#">Link</a>
2025-02-10	[ACCEM.COM]	clon	<a href="#">Link</a>
2025-02-10	[ABCOPRODUCTS.COM]	clon	<a href="#">Link</a>
2025-02-10	[3PLSOFTWARE.COM]	clon	<a href="#">Link</a>
2025-02-10	[Brockway Hair Design]	medusa	<a href="#">Link</a>
2025-02-10	[True World Foods]	medusa	<a href="#">Link</a>
2025-02-10	[MEDES College]	medusa	<a href="#">Link</a>
2025-02-03	[Glow Medi Spa]	medusa	<a href="#">Link</a>
2025-02-10	[3FINITY.NET]	clon	<a href="#">Link</a>
2025-02-10	[1888MILLS.COM]	clon	<a href="#">Link</a>
2025-02-10	[CXTSOFTWARE.COM]	clon	<a href="#">Link</a>
2025-02-10	[UNIEKINC.COM]	clon	<a href="#">Link</a>
2025-02-10	[STORKCRAFT.COM]	clon	<a href="#">Link</a>
2025-02-10	[COMPANY's_PART1]	clon	<a href="#">Link</a>
2025-02-10	[Old National Events Plaza]	akira	<a href="#">Link</a>
2025-02-09	[Marshall Motor Holdings]	lynx	<a href="#">Link</a>
2025-02-10	[Albright Institute]	killsec	<a href="#">Link</a>
2025-02-10	[WhoHire]	killsec	<a href="#">Link</a>
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>

Datum	Opfer	Ransomware-Gruppe	Webseite
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>
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	[renmarkfinancial.com]	qilin	<a href="#">Link</a>
2025-02-06	[lowernazareth.com]	safepay	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
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>
2025-02-04	[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>

Datum	Opfer	Ransomware-Gruppe	Webseite
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>
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>

Datum	Opfer	Ransomware-Gruppe	Webseite
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>
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>

Datum	Opfer	Ransomware-Gruppe	Webseite
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>
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>

Datum	Opfer	Ransomware-Gruppe	Webseite
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>
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>

Datum	Opfer	Ransomware-Gruppe	Webseite
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>
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.