


---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20250430



## 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) . . . . .	9
3.3 Sicherheitslücken Meldungen von Tenable . . . . .	12
<b>4 Die Hacks der Woche</b>	<b>14</b>
4.0.1 Information Stealer. Wie funktionieren sie? . . . . .	15
<b>5 Cyberangriffe: (Apr)</b>	<b>16</b>
<b>6 Ransomware-Erpressungen: (Apr)</b>	<b>17</b>
<b>7 Quellen</b>	<b>34</b>
7.1 Quellenverzeichnis . . . . .	34
<b>8 Impressum</b>	<b>36</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

#### ***Apple AirPlay: Sicherheitsforscher warnen vor gravierenden Lücken***

Schwachstellen erlauben die Übernahme von AirPlay-Geräten, warnen Sicherheitsforscher. Für iPhones & Co gibt es Patches, bei anderer Hardware wird es knifflig.

- [Link](#)

—

#### ***Docker: Rechteausweitungslücke in Desktop für Windows***

Angreifer können ihre Rechte durch ein Sicherheitsleck in Docker Desktop für Windows ausweiten. Ein Update korrigiert das.

- [Link](#)

—

#### ***Seiko-Epson-Druckertreiber ermöglicht Rechteausweitung auf System***

Die Windows-Druckertreiber für Seiko-Epson-Drucker enthalten eine hochriskante Lücke, die Angreifern die Ausweitung ihrer Rechte ermöglicht.

- [Link](#)

—

#### ***Attackierte SAP-Lücke: Hunderte verwundbare Server im Netz***

Am Freitag hat SAP eine bereits angegriffene Sicherheitslücke in SAP Netweaver gepatcht. Noch immer sind hunderte Server verwundbar.

- [Link](#)

—

#### ***Angriffe auf Sicherheitslücken in Commvault, Brocade Fabric OS und Active! Mail***

Angreifer nehmen junge Schwachstellen in Commvault, Brocade Fabric OS und Active! Mail ins Visier und kompromittieren Systeme.

- [Link](#)

—

#### ***Sicherheitslücken: Attacken auf Lernplattform Moodle können bevorstehen***

Mehrere Softwareschwachstellen gefährden Moodle-Instanzen. Sicherheitsupdates stehen zum Download bereit.

- [Link](#)

—

#### ***Sicherheitsupdate: Unbefugte Zugriffe auf Spring Boot möglich***

Admins sollten Softwareentwicklungsumgebungen mit Spring Boot aus Sicherheitsgründen auf den aktuellen Stand bringen.

- [Link](#)

---

**Connectwise Screenconnect: Hochriskante Codeschmuggel-Lücke**

In Connectwise Screenconnect schließt der Hersteller mit einem Update eine als hohes Risiko eingestufte Schadcode-Lücke.

- [Link](#)

---

**Sicherheitsupdate: Nvidia-Grafikkartentreiber unter Linux angreifbar**

Drei Sicherheitslücken gefährden PCs mit einer Grafikkarte von Nvidia. Im schlimmsten Fall kann Schadcode auf Linux-Systeme gelangen.

- [Link](#)

---

**SAP patcht attackierte, kritische Schwachstelle außer der Reihe**

Eine kritische Sicherheitslücke nötigt SAP zum Update außer der Reihe. Sie wird bereits in freier Wildbahn angegriffen.

- [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-2025-29927	0.925570000	0.997200000	<a href="#">Link</a>
CVE-2025-24813	0.929580000	0.997570000	<a href="#">Link</a>
CVE-2025-0282	0.920990000	0.996810000	<a href="#">Link</a>
CVE-2025-0108	0.935650000	0.998190000	<a href="#">Link</a>
CVE-2024-9989	0.911880000	0.996100000	<a href="#">Link</a>
CVE-2024-9935	0.928150000	0.997410000	<a href="#">Link</a>
CVE-2024-9474	0.942830000	0.999250000	<a href="#">Link</a>
CVE-2024-9465	0.942440000	0.999140000	<a href="#">Link</a>
CVE-2024-9463	0.942590000	0.999200000	<a href="#">Link</a>
CVE-2024-9264	0.923200000	0.996990000	<a href="#">Link</a>
CVE-2024-9234	0.925020000	0.997160000	<a href="#">Link</a>
CVE-2024-9047	0.914320000	0.996290000	<a href="#">Link</a>
CVE-2024-9014	0.923220000	0.997000000	<a href="#">Link</a>
CVE-2024-8963	0.943480000	0.999450000	<a href="#">Link</a>
CVE-2024-8856	0.914410000	0.996300000	<a href="#">Link</a>
CVE-2024-8517	0.905320000	0.995660000	<a href="#">Link</a>
CVE-2024-8504	0.923140000	0.996980000	<a href="#">Link</a>
CVE-2024-8503	0.930440000	0.997680000	<a href="#">Link</a>
CVE-2024-8190	0.927840000	0.997390000	<a href="#">Link</a>
CVE-2024-7954	0.939410000	0.998660000	<a href="#">Link</a>
CVE-2024-7928	0.914030000	0.996260000	<a href="#">Link</a>
CVE-2024-7593	0.943990000	0.999690000	<a href="#">Link</a>
CVE-2024-7120	0.912160000	0.996110000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-6911	0.927560000	0.997360000	<a href="#">Link</a>
CVE-2024-6782	0.937140000	0.998350000	<a href="#">Link</a>
CVE-2024-6781	0.932170000	0.997870000	<a href="#">Link</a>
CVE-2024-6670	0.944670000	0.999930000	<a href="#">Link</a>
CVE-2024-6646	0.915540000	0.996390000	<a href="#">Link</a>
CVE-2024-5932	0.941040000	0.998920000	<a href="#">Link</a>
CVE-2024-5910	0.908210000	0.995860000	<a href="#">Link</a>
CVE-2024-5806	0.907610000	0.995820000	<a href="#">Link</a>
CVE-2024-57727	0.934600000	0.998070000	<a href="#">Link</a>
CVE-2024-56145	0.915340000	0.996360000	<a href="#">Link</a>
CVE-2024-55956	0.922660000	0.996940000	<a href="#">Link</a>
CVE-2024-55591	0.929980000	0.997620000	<a href="#">Link</a>
CVE-2024-53704	0.936990000	0.998340000	<a href="#">Link</a>
CVE-2024-53677	0.921710000	0.996860000	<a href="#">Link</a>
CVE-2024-5217	0.941960000	0.999070000	<a href="#">Link</a>
CVE-2024-51567	0.942610000	0.999200000	<a href="#">Link</a>
CVE-2024-51378	0.939560000	0.998690000	<a href="#">Link</a>
CVE-2024-5084	0.907680000	0.995820000	<a href="#">Link</a>
CVE-2024-50623	0.939920000	0.998760000	<a href="#">Link</a>
CVE-2024-50603	0.942460000	0.999150000	<a href="#">Link</a>
CVE-2024-50498	0.922440000	0.996910000	<a href="#">Link</a>
CVE-2024-50379	0.919360000	0.996700000	<a href="#">Link</a>
CVE-2024-4956	0.939760000	0.998730000	<a href="#">Link</a>
CVE-2024-48914	0.909810000	0.995960000	<a href="#">Link</a>
CVE-2024-4885	0.942780000	0.999240000	<a href="#">Link</a>
CVE-2024-4879	0.943360000	0.999410000	<a href="#">Link</a>
CVE-2024-48307	0.909650000	0.995950000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-48248	0.931910000	0.997850000	<a href="#">Link</a>
CVE-2024-47575	0.909990000	0.995970000	<a href="#">Link</a>
CVE-2024-47176	0.916890000	0.996480000	<a href="#">Link</a>
CVE-2024-46938	0.915900000	0.996420000	<a href="#">Link</a>
CVE-2024-4577	0.943760000	0.999560000	<a href="#">Link</a>
CVE-2024-45519	0.941500000	0.998990000	<a href="#">Link</a>
CVE-2024-45388	0.915030000	0.996340000	<a href="#">Link</a>
CVE-2024-45216	0.939010000	0.998610000	<a href="#">Link</a>
CVE-2024-45195	0.940810000	0.998900000	<a href="#">Link</a>
CVE-2024-4443	0.932760000	0.997940000	<a href="#">Link</a>
CVE-2024-4439	0.909450000	0.995930000	<a href="#">Link</a>
CVE-2024-44000	0.920120000	0.996770000	<a href="#">Link</a>
CVE-2024-4358	0.942540000	0.999180000	<a href="#">Link</a>
CVE-2024-43451	0.906830000	0.995760000	<a href="#">Link</a>
CVE-2024-43425	0.926940000	0.997300000	<a href="#">Link</a>
CVE-2024-42640	0.904770000	0.995620000	<a href="#">Link</a>
CVE-2024-4257	0.922930000	0.996960000	<a href="#">Link</a>
CVE-2024-41713	0.939620000	0.998700000	<a href="#">Link</a>
CVE-2024-41107	0.929020000	0.997500000	<a href="#">Link</a>
CVE-2024-4040	0.944120000	0.999720000	<a href="#">Link</a>
CVE-2024-40348	0.919180000	0.996680000	<a href="#">Link</a>
CVE-2024-39914	0.926650000	0.997280000	<a href="#">Link</a>
CVE-2024-38856	0.943660000	0.999530000	<a href="#">Link</a>
CVE-2024-38816	0.924030000	0.997050000	<a href="#">Link</a>
CVE-2024-38112	0.917790000	0.996550000	<a href="#">Link</a>
CVE-2024-37032	0.924680000	0.997120000	<a href="#">Link</a>
CVE-2024-36412	0.927520000	0.997360000	<a href="#">Link</a>



CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-36401	0.944180000	0.999750000	<a href="#">Link</a>
CVE-2024-36104	0.938050000	0.998490000	<a href="#">Link</a>
CVE-2024-3552	0.932020000	0.997850000	<a href="#">Link</a>
CVE-2024-3495	0.932990000	0.997960000	<a href="#">Link</a>
CVE-2024-34470	0.932220000	0.997880000	<a href="#">Link</a>
CVE-2024-34102	0.943580000	0.999500000	<a href="#">Link</a>
CVE-2024-3400	0.942860000	0.999260000	<a href="#">Link</a>
CVE-2024-3273	0.944020000	0.999700000	<a href="#">Link</a>
CVE-2024-3272	0.937910000	0.998470000	<a href="#">Link</a>
CVE-2024-32651	0.913070000	0.996180000	<a href="#">Link</a>
CVE-2024-32113	0.934460000	0.998060000	<a href="#">Link</a>
CVE-2024-31982	0.941010000	0.998920000	<a href="#">Link</a>
CVE-2024-31851	0.914260000	0.996280000	<a href="#">Link</a>
CVE-2024-31850	0.909130000	0.995920000	<a href="#">Link</a>
CVE-2024-31849	0.919840000	0.996740000	<a href="#">Link</a>
CVE-2024-31848	0.927370000	0.997330000	<a href="#">Link</a>
CVE-2024-31750	0.926850000	0.997290000	<a href="#">Link</a>
CVE-2024-3094	0.910420000	0.996000000	<a href="#">Link</a>
CVE-2024-30255	0.921870000	0.996870000	<a href="#">Link</a>
CVE-2024-29973	0.936960000	0.998330000	<a href="#">Link</a>
CVE-2024-29972	0.915290000	0.996360000	<a href="#">Link</a>
CVE-2024-29895	0.930810000	0.997730000	<a href="#">Link</a>
CVE-2024-29824	0.943660000	0.999520000	<a href="#">Link</a>

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

Tue, 29 Apr 2025

**[NEU] [hoch] Redmine.org Redmine: Mehrere Schwachstellen**

Ein lokaler Angreifer kann mehrere Schwachstellen in Redmine.org Redmine ausnutzen, um Informationen offenzulegen, einen Cross-Site Scripting Angriff durchzuführen und weitere, nicht spezifizierte Auswirkungen zu verursachen.

- [Link](#)

—

Tue, 29 Apr 2025

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

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erweitern, einen Denial of Service Zustand auszulösen und mehrere nicht spezifizierte Angriffe durchzuführen.

- [Link](#)

—

Tue, 29 Apr 2025

**[UPDATE] [hoch] Red Hat FUSE: Mehrere Schwachstellen**

Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat FUSE ausnutzen, um vertrauliche Informationen offenzulegen, beliebigen Code auszuführen, einen Denial of Service Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, Daten und Informationen zu manipulieren und seine Privilegien zu erweitern.

- [Link](#)

—

Tue, 29 Apr 2025

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

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

- [Link](#)

—

Tue, 29 Apr 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](#)

—

Tue, 29 Apr 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](#)

—

Tue, 29 Apr 2025

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

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in PHP ausnutzen, um vertrauliche Informationen preiszugeben, beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu erzeugen und einen Spoofing-Angriff durchzuführen.

- [Link](#)

—

Tue, 29 Apr 2025

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

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um einen Denial of Service Angriff durchzuführen und um seine Privilegien zu erhöhen.

- [Link](#)

—

Tue, 29 Apr 2025

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

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

- [Link](#)

—

Tue, 29 Apr 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](#)

—

Tue, 29 Apr 2025

**[UPDATE] [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](#)

—

Tue, 29 Apr 2025

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

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um erhöhte Privilegi-

en zu erlangen oder einen Denial of Service auszulösen.

- [Link](#)

—

Tue, 29 Apr 2025

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

Ein lokaler Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um Dateien zu manipulieren oder seine Rechte zu erweitern.

- [Link](#)

—

Tue, 29 Apr 2025

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

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erweitern, um beliebigen Programmcode auszuführen oder einen Denial of Service auszulösen.

- [Link](#)

—

Tue, 29 Apr 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](#)

—

Tue, 29 Apr 2025

**[UPDATE] [hoch] Red Hat Enterprise Linux (Quarkus): Mehrere Schwachstellen**

Ein entfernter Angreifer kann mehrere Schwachstellen in Quarkus auf Red Hat Enterprise Linux ausnutzen, um Informationen offenzulegen, oder einen Denial of Service auszulösen.

- [Link](#)

—

Tue, 29 Apr 2025

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

Ein Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um nicht spezifizierte Auswirkungen zu erzeugen oder einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

—

Tue, 29 Apr 2025

**[UPDATE] [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](#)

---

Tue, 29 Apr 2025

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

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um erhöhte Rechte zu erlangen, beliebigen Code auszuführen, Spoofing-Angriffe durchzuführen, einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen preiszugeben oder andere nicht spezifizierte Angriffe durchzuführen.

- [Link](#)

---

Tue, 29 Apr 2025

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

Ein entfernter anonymmer Angreifer kann mehrere Schwachstellen im Linux-Kernel ausnutzen, um einen 'Denial of Service'-Zustand zu erzeugen oder andere nicht spezifizierte Angriffe durchzuführen.

- [Link](#)

---

### 3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
4/29/2025	[FreeBSD : h11 accepts some malformed Chunked-Encoding bodies (df126e23-24fa-11f0-ab92-f02f7497ecda)]	critical
4/29/2025	[Google Chrome < 136.0.7103.48 Multiple Vulnerabilities]	critical
4/29/2025	[Google Chrome < 136.0.7103.48 Multiple Vulnerabilities]	critical
4/29/2025	[Amazon Linux 2 : firefox (ALASFIREFOX-2025-037)]	critical
4/29/2025	[Amazon Linux 2023 : firefox (ALAS2023-2025-943)]	high
4/29/2025	[Amazon Linux 2023 : java-17-amazon-corretto, java-17-amazon-corretto-devel, java-17-amazon-corretto-headless (ALAS2023-2025-954)]	high
4/29/2025	[Amazon Linux 2023 : java-24-amazon-corretto, java-24-amazon-corretto-devel, java-24-amazon-corretto-headless (ALAS2023-2025-951)]	high

Datum	Schwachstelle	Bewertung
4/29/2025	[Amazon Linux 2023 : bpftool, kernel6.12, kernel6.12-modules-extra (ALAS2023-2025-948)]	high
4/29/2025	[Amazon Linux 2023 : redis6, redis6-devel (ALAS2023-2025-950)]	high
4/29/2025	[Amazon Linux 2023 : java-11-amazon-corretto, java-11-amazon-corretto-devel, java-11-amazon-corretto-headless (ALAS2023-2025-955)]	high
4/29/2025	[Amazon Linux 2023 : libsoup, libsoup-devel (ALAS2023-2025-946)]	high
4/29/2025	[Amazon Linux 2023 : libsoup3, libsoup3-devel (ALAS2023-2025-941)]	high
4/29/2025	[Amazon Linux 2 : kernel (ALASKERNEL-5.10-2025-090)]	high
4/29/2025	[Amazon Linux 2 : containerd (ALASECS-2025-060)]	high
4/29/2025	[Amazon Linux 2023 : bpftool, kernel6.12, kernel6.12-modules-extra (ALAS2023-2025-940)]	high
4/29/2025	[Amazon Linux 2 : java-11-openjdk (ALASJAVA-OPENJDK11-2025-011)]	high
4/29/2025	[Amazon Linux 2 : runc (ALASECS-2025-062)]	high
4/29/2025	[Amazon Linux 2 : docker (ALASECS-2025-059)]	high
4/29/2025	[Amazon Linux 2 : kernel (ALASKERNEL-5.4-2025-100)]	high
4/29/2025	[Amazon Linux 2 : runc (ALASECS-2025-058)]	high
4/29/2025	[Amazon Linux 2 : containerd (ALASDOCKER-2025-061)]	high
4/29/2025	[Amazon Linux 2 : runfinch-finch (ALASDOCKER-2025-057)]	high
4/29/2025	[Amazon Linux 2 : runc (ALASDOCKER-2025-059)]	high
4/29/2025	[Amazon Linux 2 : docker (ALASDOCKER-2025-060)]	high
4/29/2025	[Amazon Linux 2 : kernel (ALASKERNEL-5.15-2025-070)]	high
4/29/2025	[Amazon Linux 2 : runc (ALASNITRO-ENCLAVES-2025-055)]	high
4/29/2025	[Amazon Linux 2 : runc (ALASECS-2025-064)]	high
4/29/2025	[Amazon Linux 2 : docker (ALASECS-2025-061)]	high

Datum	Schwachstelle	Bewertung
4/29/2025	[Amazon Linux 2 : docker (ALASDOCKER-2025-058)]	high
4/29/2025	[Amazon Linux 2 : redis (ALASREDIS6-2025-012)]	high
4/29/2025	[Amazon Linux 2 : docker (ALASNITRO-ENCLAVES-2025-059)]	high
4/29/2025	[Amazon Linux 2 : java-11-openjdk (ALASJAVA-OPENJDK11-2025-012)]	high
4/29/2025	[Amazon Linux 2 : docker (ALASNITRO-ENCLAVES-2025-057)]	high
4/29/2025	[Amazon Linux 2 : docker (ALASNITRO-ENCLAVES-2025-054)]	high
4/29/2025	[Amazon Linux 2 : containerd (ALASNITRO-ENCLAVES-2025-058)]	high
4/29/2025	[Amazon Linux 2 : runc (ALASNITRO-ENCLAVES-2025-056)]	high
4/29/2025	[Amazon Linux 2 : docker (ALASECS-2025-055)]	high
4/29/2025	[Slackware Linux 15.0 / current mozilla-thunderbird Multiple Vulnerabilities (SSA:2025-119-02)]	high

## 4 Die Hacks der Woche

mit Martin Haunschmid

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



[Zum Youtube Video](#)



## 5 Cyberangriffe: (Apr)

Datum	Opfer	Land	Information
2025-04-28	DuPage County sheriff's office, circuit clerk's office and courthouse	[USA]	<a href="#">Link</a>
2025-04-28	Doctors Hospital	[CYM]	<a href="#">Link</a>
2025-04-27	JFL Hospital	[VIR]	<a href="#">Link</a>
2025-04-26	Hitachi Vantara	[JPN]	<a href="#">Link</a>
2025-04-25	MTN Group	[ZAF]	<a href="#">Link</a>
2025-04-25	Swiss Post Cargo Deutschland	[DEU]	<a href="#">Link</a>
2025-04-25	Nova Scotia Power	[CAN]	<a href="#">Link</a>
2025-04-23	guentiger.de GmbH	[DEU]	<a href="#">Link</a>
2025-04-22	Oettinger	[DEU]	<a href="#">Link</a>
2025-04-21	Aigües de Mataró	[ESP]	<a href="#">Link</a>
2025-04-20	City of Abilene	[USA]	<a href="#">Link</a>
2025-04-20	Marks & Spencer	[GBR]	<a href="#">Link</a>
2025-04-20	Santa Fe ISD	[USA]	<a href="#">Link</a>
2025-04-19	SK Telecom	[KOR]	<a href="#">Link</a>
2025-04-18	Groupe INDIGO	[FRA]	<a href="#">Link</a>
2025-04-17	William Buck	[AUS]	<a href="#">Link</a>
2025-04-17	Service public de Wallonie	[BEL]	<a href="#">Link</a>
2025-04-17	Limestone District School Board	[CAN]	<a href="#">Link</a>
2025-04-17	Centre hospitalier de Pézenas	[FRA]	<a href="#">Link</a>
2025-04-17	Tokai University	[JPN]	<a href="#">Link</a>
2025-04-17	Safety21	[ITA]	<a href="#">Link</a>
2025-04-17	Versa Networks	[USA]	<a href="#">Link</a>
2025-04-16	Layer-Grosshandel	[DEU]	<a href="#">Link</a>
2025-04-15	Rhône FM	[CHE]	<a href="#">Link</a>

Datum	Opfer	Land	Information
2025-04-14	Administration communale de Jemeppe-sur-Sambre	[BEL]	<a href="#">Link</a>
2025-04-14	Schweizerische Zentralverein für das Blindenwesen	[CHE]	<a href="#">Link</a>
2025-04-13	Western New Mexico University	[USA]	<a href="#">Link</a>
2025-04-12	DaVita Inc.	[USA]	<a href="#">Link</a>
2025-04-12	Groupe 3R	[CHE]	<a href="#">Link</a>
2025-04-10	Oregon Department of Environmental Quality (DEQ)	[USA]	<a href="#">Link</a>
2025-04-09	SIAPA (Sistema Intermunicipal de los Servicios de Agua Potable y Alcantarillado)	[MEX]	<a href="#">Link</a>
2025-04-09	Nippon Life India Asset Management Limited	[IND]	<a href="#">Link</a>
2025-04-09	Bertie County Schools	[USA]	<a href="#">Link</a>
2025-04-08	Visionary Holdings Inc.	[CAN]	<a href="#">Link</a>
2025-04-07	Sensata Technologies	[USA]	<a href="#">Link</a>
2025-04-07	Eu-Rec GmbH	[DEU]	<a href="#">Link</a>
2025-04-06	Toppan Next Tech (TNT)	[SGP]	<a href="#">Link</a>
2025-04-06	Fall River Public Schools	[USA]	<a href="#">Link</a>
2025-04-05	Optimax Technology	[TWN]	<a href="#">Link</a>
2025-04-03	Manchester Credit Union	[GBR]	<a href="#">Link</a>
2025-04-02	Bureau du défenseur public fédéral de l'Arizona	[USA]	<a href="#">Link</a>

## 6 Ransomware-Erpressungen: (Apr)

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-28	[Ushio]	termite	<a href="#">Link</a>
2025-04-29	[Coop UQAM]	rhysida	<a href="#">Link</a>
2025-04-29	[National Steel City]	play	<a href="#">Link</a>
2025-04-29	[PermaCold Engineering]	play	<a href="#">Link</a>
2025-04-29	[Missouri Pipe Fittings]	play	<a href="#">Link</a>
2025-04-29	[Cooper Global Chauffeured]	play	<a href="#">Link</a>
2025-04-29	[BOLL Logistik]	play	<a href="#">Link</a>
2025-04-29	[Gorham Sand & Gravel]	play	<a href="#">Link</a>
2025-04-29	[southernagllc.com]	lynx	<a href="#">Link</a>
2025-04-29	[SoloVue]	qilin	<a href="#">Link</a>
2025-04-29	[SJERP]	nova	<a href="#">Link</a>
2025-04-28	[Hpital Glengarry Memorial Hospital (clglen.local)]	incransom	<a href="#">Link</a>
2025-04-28	[David Mills CPA, LLC]	lynx	<a href="#">Link</a>
2025-04-25	[w8textil]	nightspire	<a href="#">Link</a>
2025-04-27	[csspv]	nightspire	<a href="#">Link</a>
2025-04-23	[Melco Capital Pte. Ltd.]	nightspire	<a href="#">Link</a>
2025-04-28	[Kramer Green Zuckerman Greene and Buchsbaum]	akira	<a href="#">Link</a>
2025-04-23	[rawafid]	nova	<a href="#">Link</a>
2025-04-28	[Tolerance Masters]	akira	<a href="#">Link</a>
2025-04-10	[hasbco Company]	nova	<a href="#">Link</a>
2025-04-14	[Al-Hejailan Group]	nova	<a href="#">Link</a>
2025-04-15	[NewHotel cloud]	nova	<a href="#">Link</a>
2025-04-15	[ARRCO LSM]	nova	<a href="#">Link</a>
2025-04-16	[Bio-Clima Service]	nova	<a href="#">Link</a>
2025-04-16	[bettininformatica - suporteon]	nova	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-22	[agromate]	nova	<a href="#">Link</a>
2025-04-28	[LaBella Associates]	rhysida	<a href="#">Link</a>
2025-04-23	[HELUKABEL]	nova	<a href="#">Link</a>
2025-04-27	[DIALOG]	nova	<a href="#">Link</a>
2025-04-03	[CCHC Healthcare]	qilin	<a href="#">Link</a>
2025-04-28	[Bioprofarma Bagó S.A]	gunra	<a href="#">Link</a>
2025-04-21	[Whitley Law Firm]	qilin	<a href="#">Link</a>
2025-04-28	[Minnesota Lawyers Mutual Insurance]	hunters	<a href="#">Link</a>
2025-04-28	[RC Manubhai]	qilin	<a href="#">Link</a>
2025-04-27	[FMT Consultants]	play	<a href="#">Link</a>
2025-04-27	[Mantel Machine Products]	play	<a href="#">Link</a>
2025-04-27	[Scientel Solutions]	play	<a href="#">Link</a>
2025-04-27	[Haas & Associates]	play	<a href="#">Link</a>
2025-04-27	[Crawford Door Sales]	play	<a href="#">Link</a>
2025-04-27	[www.southlandscs.com]	qilin	<a href="#">Link</a>
2025-04-22	[Matthews Law]	medusa	<a href="#">Link</a>
2025-04-22	[Phelps United]	medusa	<a href="#">Link</a>
2025-04-24	[Conditioned Air Corporation]	medusa	<a href="#">Link</a>
2025-04-24	[Appalachian Regional Commission]	medusa	<a href="#">Link</a>
2025-04-27	[KLINGER Italy]	gunra	<a href="#">Link</a>
2025-04-27	[DIALOG company]	ralord	<a href="#">Link</a>
2025-04-25	[Sisnet, Costa Rica]	nightspire	<a href="#">Link</a>
2025-04-26	[MDB]	rhysida	<a href="#">Link</a>
2025-04-26	[Seneca Gaming & Entertainment]	nitrogen	<a href="#">Link</a>
2025-04-25	[Stadtwerke Schwerte GmbH]	nitrogen	<a href="#">Link</a>
2025-04-25	[M'AR De AR Hotels]	nitrogen	<a href="#">Link</a>
2025-04-25	[DYNAMIS Insurance]	akira	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-25	[corporateflight.com]	lynx	<a href="#">Link</a>
2025-04-25	[shgcpa.com]	lynx	<a href="#">Link</a>
2025-04-25	[Kenworth Del Sur]	hunters	<a href="#">Link</a>
2025-04-25	[J. SCHNEEBERGER Maschinen AG]	akira	<a href="#">Link</a>
2025-04-25	[Kasb Bank - K-Trade]	hunters	<a href="#">Link</a>
2025-04-25	[Santa Cruz Properties]	akira	<a href="#">Link</a>
2025-04-25	[Cohn Lifland Pearlman Herrmann and Knopf]	akira	<a href="#">Link</a>
2025-04-25	[DaVita]	interlock	<a href="#">Link</a>
2025-04-25	[Madison School District Schools]	interlock	<a href="#">Link</a>
2025-04-25	[EU victim]	devman	<a href="#">Link</a>
2025-04-25	[Advanced Simulation Technology inc. (ASTi)]	silent	<a href="#">Link</a>
2025-04-25	[impactcanada.com]	lynx	<a href="#">Link</a>
2025-04-24	[pay4freight.com]	lynx	<a href="#">Link</a>
2025-04-24	[greatplainstransport.com]	lynx	<a href="#">Link</a>
2025-04-24	[buildingmaterialspecialties.com]	lynx	<a href="#">Link</a>
2025-04-24	[friscochamber.com]	lynx	<a href="#">Link</a>
2025-04-24	[Pacific Metallurgical]	blacksuit	<a href="#">Link</a>
2025-04-24	[The Fortune Society]	blacksuit	<a href="#">Link</a>
2025-04-24	[Dress To]	akira	<a href="#">Link</a>
2025-04-24	[end2endtechnologies]	lynx	<a href="#">Link</a>
2025-04-24	[Oversea Casing]	akira	<a href="#">Link</a>
2025-04-23	[Fogelman Management Group]	akira	<a href="#">Link</a>
2025-04-24	[Vicarage Court Solicitors]	lynx	<a href="#">Link</a>
2025-04-24	[arkansasprimarycare.com]	incransom	<a href="#">Link</a>
2025-04-24	[Fleet Canada]	silent	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-24	[China Harbour Engeneiring Company]	devman	<a href="#">Link</a>
2025-04-23	[HELUKABEL company]	ralord	<a href="#">Link</a>
2025-04-24	[thederbyhighschool.co.uk]	kairos	<a href="#">Link</a>
2025-04-21	[MFR CULTIVONS LES REUSSITES, France]	nightspire	<a href="#">Link</a>
2025-04-23	[rawafid company]	ralord	<a href="#">Link</a>
2025-04-06	[tecnologias.mspz2.gob.ec]	babuk2	<a href="#">Link</a>
2025-04-23	[Farmo Res]	lynx	<a href="#">Link</a>
2025-04-23	[coloradopulmonary.com]	kairos	<a href="#">Link</a>
2025-04-23	[Two Kings Casino Resort]	anubis	<a href="#">Link</a>
2025-04-23	[Rayle Electric Membership Corporation]	akira	<a href="#">Link</a>
2025-04-23	[Milicic]	rhapsida	<a href="#">Link</a>
2025-04-23	[Varela Hermanos]	gunra	<a href="#">Link</a>
2025-04-23	[Dar Al Teb]	gunra	<a href="#">Link</a>
2025-04-23	[Shinko Shoji]	gunra	<a href="#">Link</a>
2025-04-23	[Versa Networks]	silent	<a href="#">Link</a>
2025-04-23	[ESP Associates]	silent	<a href="#">Link</a>
2025-04-23	[lemi-group]	incransom	<a href="#">Link</a>
2025-04-23	[N8XT]	crypto24	<a href="#">Link</a>
2025-04-23	[www.unitedcaps.com]	qilin	<a href="#">Link</a>
2025-04-23	[Mafi]	hunters	<a href="#">Link</a>
2025-04-22	[Jet Ice]	play	<a href="#">Link</a>
2025-04-18	[M-POWER Information, Taiwan]	nightspire	<a href="#">Link</a>
2025-04-13	[promenade-village-dental, Canada]	nightspire	<a href="#">Link</a>
2025-04-22	[Independent Financial Services]	play	<a href="#">Link</a>
2025-04-22	[The Human Bean]	play	<a href="#">Link</a>
2025-04-22	[All Book Covers]	play	<a href="#">Link</a>
2025-04-22	[Suburban Carting]	play	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-17	[Springer & Steinberg]	lynx	<a href="#">Link</a>
2025-04-22	[Diedrich Coffee]	akira	<a href="#">Link</a>
2025-04-22	[franklin nursing home]	incransom	<a href="#">Link</a>
2025-04-22	[Asesoría Bieito]	cicada3301	<a href="#">Link</a>
2025-04-22	[Natilait]	cicada3301	<a href="#">Link</a>
2025-04-22	[Amazon Transportes]	cicada3301	<a href="#">Link</a>
2025-04-10	[Bacton Transport Services]	ransomhouse	<a href="#">Link</a>
2025-04-10	[amethystgroup.co.uk]	lynx	<a href="#">Link</a>
2025-04-22	[parrishleasing.com]	qilin	<a href="#">Link</a>
2025-04-22	[R&N Manufacturing]	lynx	<a href="#">Link</a>
2025-04-22	[Acos Favorit]	rhysida	<a href="#">Link</a>
2025-04-22	[agromate company]	ralord	<a href="#">Link</a>
2025-04-21	[Machu PicchuFoods]	akira	<a href="#">Link</a>
2025-04-21	[Auren part 1]	akira	<a href="#">Link</a>
2025-04-21	[Auren part 2]	akira	<a href="#">Link</a>
2025-04-21	[ZB ZIMMERMANN UND BECKERGmbH]	akira	<a href="#">Link</a>
2025-04-10	[C-Mec]	ransomhouse	<a href="#">Link</a>
2025-04-13	[Richmond CPA]	qilin	<a href="#">Link</a>
2025-04-21	[MASHBURN CONSTRUCTION]	akira	<a href="#">Link</a>
2025-04-21	[The law firm of Rochelle McCullough, L.L.P]	akira	<a href="#">Link</a>
2025-04-21	[Bindi SpA]	akira	<a href="#">Link</a>
2025-04-18	[TrussWorks International]	akira	<a href="#">Link</a>
2025-04-21	[Dominion Lending Centres]	qilin	<a href="#">Link</a>
2025-04-21	[Sinalisa Segurança Viária Ltda]	sarcoma	<a href="#">Link</a>
2025-04-21	[Pharma Force]	hunters	<a href="#">Link</a>
2025-04-21	[tuttoperlufficio.eu]	lockbit3	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-15	[Accueil - Site Officiel de la commune d'Ardon]	nightspire	<a href="#">Link</a>
2025-04-19	[The Michelson Organization]	qilin	<a href="#">Link</a>
2025-04-20	[Premier Meats South Africa]	devman	<a href="#">Link</a>
2025-04-20	[Feel Four]	devman	<a href="#">Link</a>
2025-04-20	[Singapour Victim]	devman	<a href="#">Link</a>
2025-04-20	[Honk Kong Victim]	devman	<a href="#">Link</a>
2025-04-20	[China Harbour Engeneiring Company]	devman	<a href="#">Link</a>
2025-04-16	[Iris ID]	dragonforce	<a href="#">Link</a>
2025-04-16	[City of Grove]	dragonforce	<a href="#">Link</a>
2025-04-16	[Lithium Americas Nevada]	medusa	<a href="#">Link</a>
2025-04-19	[MRC de Maskinongé - district]	medusa	<a href="#">Link</a>
2025-04-20	[FAKO-M Getränke]	sarcoma	<a href="#">Link</a>
2025-04-13	[ChangShen Hospital, Taiwan]	nightspire	<a href="#">Link</a>
2025-04-16	[bettininformatica - suporteon company]	ralord	<a href="#">Link</a>
2025-04-18	[April, 18, 2025: Independent Title Agency, LLC ("ITA") (USA hacked. 932.4 GiB is for selli...)]	skira	<a href="#">Link</a>
2025-04-18	[Independent Title Agency, LLC ("ITA") (USA)]	skira	<a href="#">Link</a>
2025-04-18	[Agencia Browne y Espinoza]	akira	<a href="#">Link</a>
2025-04-18	[Heinz Hammer Vertragswerkstatt (Mercedes-Benz car dealer)]	akira	<a href="#">Link</a>
2025-04-01	[[EVIDENCE PACK 2] Telecontrol]	ransomhouse	<a href="#">Link</a>
2025-04-18	[Bosshard-farben.ch]	cloak	<a href="#">Link</a>
2025-04-18	[Hubbard, McIlwain, & Brakefield, P.C.]	akira	<a href="#">Link</a>
2025-04-18	[Tänzer GmbH]	akira	<a href="#">Link</a>
2025-04-18	[Toppan Next]	akira	<a href="#">Link</a>
2025-04-18	[Global Media Group]	nitrogen	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-18	[Hayward Quartz Technology]	akira	<a href="#">Link</a>
2025-04-14	[Wilmington Personal Injury Lawyer - DPLAW]	nightspire	<a href="#">Link</a>
2025-04-11	[Compliance Consulting Group]	nightspire	<a href="#">Link</a>
2025-04-04	[Mid-America POOL RENOVATION, Inc]	nightspire	<a href="#">Link</a>
2025-04-17	[1sthealthinc.com]	qilin	<a href="#">Link</a>
2025-04-17	[Sally B Gold]	lynx	<a href="#">Link</a>
2025-04-17	[HOPI]	hunters	<a href="#">Link</a>
2025-04-17	[Enflame Technology]	killsec	<a href="#">Link</a>
2025-04-17	[yankeetrails.com]	qilin	<a href="#">Link</a>
2025-04-17	[universalwindow.com]	qilin	<a href="#">Link</a>
2025-04-17	[bertie.k12.nc.us]	qilin	<a href="#">Link</a>
2025-04-17	[Kaye Lifestyle Homes]	sarcoma	<a href="#">Link</a>
2025-04-17	[TRALFO Srl Trasporti e Spedizioni]	sarcoma	<a href="#">Link</a>
2025-04-17	[Schultz Industries Inc.]	sarcoma	<a href="#">Link</a>
2025-04-17	[Manchester Credit Union]	sarcoma	<a href="#">Link</a>
2025-04-17	[Ju Percussion Group]	sarcoma	<a href="#">Link</a>
2025-04-12	[VIÑUELAS ABOGADOS]	spacebears	<a href="#">Link</a>
2025-04-15	[EVERTECH INSTRUMENTAL CO., LTD]	spacebears	<a href="#">Link</a>
2025-04-16	[itec-gmbh.com]	safepay	<a href="#">Link</a>
2025-04-16	[heinrich-steinhardt.de]	safepay	<a href="#">Link</a>
2025-04-16	[hurst-schroeder.de]	safepay	<a href="#">Link</a>
2025-04-16	[helixtools.co.uk]	safepay	<a href="#">Link</a>
2025-04-16	[heilbronn.de]	safepay	<a href="#">Link</a>
2025-04-16	[getriebetech.de]	safepay	<a href="#">Link</a>
2025-04-16	[kirkel.de]	safepay	<a href="#">Link</a>
2025-04-16	[extremefire.com.au]	safepay	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-16	[foerster-schwanau.de]	safepay	<a href="#">Link</a>
2025-04-16	[eichele-bau.de]	safepay	<a href="#">Link</a>
2025-04-16	[frapack.de]	safepay	<a href="#">Link</a>
2025-04-16	[aqhch.com.cn]	lockbit3	<a href="#">Link</a>
2025-04-16	[Koninklijke Ahold Delhaize N.V.]	incransom	<a href="#">Link</a>
2025-04-07	[niemann.de]	safepay	<a href="#">Link</a>
2025-04-16	[www.nelson.edu]	qilin	<a href="#">Link</a>
2025-04-16	[Bio-Clima Service]	ralord	<a href="#">Link</a>
2025-04-16	[Red Chamber]	play	<a href="#">Link</a>
2025-04-16	[d-line-it.com]	kairos	<a href="#">Link</a>
2025-04-16	[Lamberti Group]	akira	<a href="#">Link</a>
2025-04-16	[Feldman & Lopez]	lynx	<a href="#">Link</a>
2025-04-16	[Hyalogic]	lynx	<a href="#">Link</a>
2025-04-16	[aeamg.org.br]	lockbit3	<a href="#">Link</a>
2025-04-16	[ende.bo]	lockbit3	<a href="#">Link</a>
2025-04-16	[Dale Partners Architects]	akira	<a href="#">Link</a>
2025-04-16	[Anfarm Hellas]	akira	<a href="#">Link</a>
2025-04-16	[D'Granel]	akira	<a href="#">Link</a>
2025-04-08	[shengyusteel.com]	underground	<a href="#">Link</a>
2025-04-15	[semex.com]	underground	<a href="#">Link</a>
2025-04-15	[McElwee Firm]	lynx	<a href="#">Link</a>
2025-04-14	[KraftKisarna]	dragonforce	<a href="#">Link</a>
2025-04-14	[Pryor Morrow]	dragonforce	<a href="#">Link</a>
2025-04-14	[Pratt Homes]	dragonforce	<a href="#">Link</a>
2025-04-15	[Setpoint Systems]	dragonforce	<a href="#">Link</a>
2025-04-14	[Pawnee Heights Unified School District]	medusa	<a href="#">Link</a>
2025-04-16	[iblinfo.de]	incransom	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-15	[a-1freeman]	qilin	<a href="#">Link</a>
2025-04-15	[Astra Products]	lynx	<a href="#">Link</a>
2025-04-15	[Lake HVAC]	lynx	<a href="#">Link</a>
2025-04-15	[ARRCO LSM]	ralord	<a href="#">Link</a>
2025-04-15	[spscompanies.com]	lynx	<a href="#">Link</a>
2025-04-15	[nevadareadymix.com]	lynx	<a href="#">Link</a>
2025-04-15	[Heierli]	akira	<a href="#">Link</a>
2025-04-15	[Bolivar Insulation]	akira	<a href="#">Link</a>
2025-04-15	[King Industries Inc.]	akira	<a href="#">Link</a>
2025-04-15	[PEÑA BRIONES MCDANIEL & CO.]	akira	<a href="#">Link</a>
2025-04-15	[Inductors Inc.]	akira	<a href="#">Link</a>
2025-04-15	[NewHotel cloud company]	ralord	<a href="#">Link</a>
2025-04-15	[trocaire.edu]	incransom	<a href="#">Link</a>
2025-04-15	[Oregon Department of Environmental Quality]	rhysida	<a href="#">Link</a>
2025-04-14	[NL Olson & Associates]	qilin	<a href="#">Link</a>
2025-04-14	[CDI]	qilin	<a href="#">Link</a>
2025-04-14	[Waller]	play	<a href="#">Link</a>
2025-04-09	[Cortez Resources]	play	<a href="#">Link</a>
2025-04-14	[Comport Technology Solutions]	play	<a href="#">Link</a>
2025-04-14	[Merri-Makers]	play	<a href="#">Link</a>
2025-04-14	[Voigt-Abernathy Company]	play	<a href="#">Link</a>
2025-04-03	[Destination Toronto]	play	<a href="#">Link</a>
2025-04-14	[James & Sons Fine Jewelers]	play	<a href="#">Link</a>
2025-04-14	[Al-Hejailan Group]	ralord	<a href="#">Link</a>
2025-04-14	[Caputo]	akira	<a href="#">Link</a>
2025-04-14	[Agricola Da Quinta De Corona]	akira	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-14	[STUMPF MÜLLER Biberach]	akira	<a href="#">Link</a>
2025-04-14	[Oklahoma Steel & Wire]	akira	<a href="#">Link</a>
2025-04-14	[Orthopaedic Specialists of Connecticut]	incransom	<a href="#">Link</a>
2025-04-14	[MENTAL HEALTH]	incransom	<a href="#">Link</a>
2025-04-10	[REFFINDO-PT Pupk Indonesia]	nightspire	<a href="#">Link</a>
2025-04-13	[FEELFOUR]	devman	<a href="#">Link</a>
2025-04-13	[Med institute]	devman	<a href="#">Link</a>
2025-04-13	[Bangkok Electronics Co., Ltd]	devman	<a href="#">Link</a>
2025-04-13	[Tawasol]	devman	<a href="#">Link</a>
2025-04-13	[Texas Construction Firm]	devman	<a href="#">Link</a>
2025-04-13	[Optimax Technology]	devman	<a href="#">Link</a>
2025-04-13	[CALTON.COM]	cllop	<a href="#">Link</a>
2025-04-01	[STORT]	nightspire	<a href="#">Link</a>
2025-04-04	[Sistel Connections]	nightspire	<a href="#">Link</a>
2025-04-01	[InterLOGIC Inc]	nightspire	<a href="#">Link</a>
2025-04-01	[Secretaria de Educacion de Veracruz, SEV]	nightspire	<a href="#">Link</a>
2025-04-06	[Nicera]	nightspire	<a href="#">Link</a>
2025-04-08	[Emotrans Chile]	nightspire	<a href="#">Link</a>
2025-04-08	[Zaphira Uniformes]	nightspire	<a href="#">Link</a>
2025-04-03	[Audit Accounting Advisory Taxes]	nightspire	<a href="#">Link</a>
2025-04-03	[Condista]	dragonforce	<a href="#">Link</a>
2025-04-07	[Precision Textiles]	dragonforce	<a href="#">Link</a>
2025-04-07	[Coulter & Tateoka]	dragonforce	<a href="#">Link</a>
2025-04-09	[Miller & Caggiano]	dragonforce	<a href="#">Link</a>
2025-04-09	[Service Trade SpA]	dragonforce	<a href="#">Link</a>
2025-04-09	[Harris Steel]	dragonforce	<a href="#">Link</a>
2025-04-12	[Ossman Consultants Limited]	dragonforce	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-08	[McFarland Commercial Insurance Services]	medusa	<a href="#">Link</a>
2025-04-08	[Bridgebank Limited]	medusa	<a href="#">Link</a>
2025-04-08	[Pulse Urgent Care]	medusa	<a href="#">Link</a>
2025-04-08	[National Association for Stock Car Auto Racing]	medusa	<a href="#">Link</a>
2025-04-12	[Fall River Public Schools]	medusa	<a href="#">Link</a>
2025-04-13	[intelliloan.com]	lockbit3	<a href="#">Link</a>
2025-04-13	[FEELFOUR]	qilin	<a href="#">Link</a>
2025-04-12	[All4Labels -Global Packaging Group]	akira	<a href="#">Link</a>
2025-04-11	[Chickenshed]	incransom	<a href="#">Link</a>
2025-04-12	[visionproducts.llc]	lockbit3	<a href="#">Link</a>
2025-04-12	[acimfunds.com]	lockbit3	<a href="#">Link</a>
2025-04-12	[MS SUPPLY CHAIN SOLUTIONS (MALAYSIA) SDN. BHD]	qilin	<a href="#">Link</a>
2025-04-12	[Mapaex]	qilin	<a href="#">Link</a>
2025-04-12	[CMC Corperation]	crypto24	<a href="#">Link</a>
2025-04-12	[Dimension Composite]	rhysida	<a href="#">Link</a>
2025-04-12	[bilbie.com.au]	lynx	<a href="#">Link</a>
2025-04-11	[Bjørklund]	termite	<a href="#">Link</a>
2025-04-11	[C?l????t Group]	play	<a href="#">Link</a>
2025-04-10	[Batesville Products,Inc.]	akira	<a href="#">Link</a>
2025-04-11	[Colmar Industrial Supplies]	lynx	<a href="#">Link</a>
2025-04-04	[Restaurant Associates]	lynx	<a href="#">Link</a>
2025-04-11	[Imagineering Finishing Technologies]	incransom	<a href="#">Link</a>
2025-04-10	[On IT]	termite	<a href="#">Link</a>
2025-04-10	[Sfrent.net]	play	<a href="#">Link</a>
2025-04-10	[The Study]	play	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-02	[Codinter]	play	<a href="#">Link</a>
2025-04-10	[PAC Strapping Products]	play	<a href="#">Link</a>
2025-04-10	[New York Sports Club]	play	<a href="#">Link</a>
2025-04-10	[hasbco Company]	ralord	<a href="#">Link</a>
2025-04-10	[ModulusGroup,Ludi-SFM]	crypto24	<a href="#">Link</a>
2025-04-10	[inspec-international.com]	incransom	<a href="#">Link</a>
2025-04-10	[TMA Group of Companies]	sarcoma	<a href="#">Link</a>
2025-04-10	[SeproTec Multilingual Solutions]	akira	<a href="#">Link</a>
2025-04-10	[Harvest]	RunSomeWares	<a href="#">Link</a>
2025-04-07	[3P Corporation]	spacebears	<a href="#">Link</a>
2025-04-10	[sk.com]	qilin	<a href="#">Link</a>
2025-04-10	[Algas Engineering Pte Ltd - Algas Engineering]	qilin	<a href="#">Link</a>
2025-04-09	[Správa služeb hlavního města Prahy]	cicada3301	<a href="#">Link</a>
2025-04-07	[Potomac Financial Services]	hellcat	<a href="#">Link</a>
2025-04-09	[Dumont Telephone]	akira	<a href="#">Link</a>
2025-04-09	[Bangkok Electronics Co., Ltd]	qilin	<a href="#">Link</a>
2025-04-09	[Simms Sigal Linwood Inc.]	akira	<a href="#">Link</a>
2025-04-09	[Hotell Euroopa]	akira	<a href="#">Link</a>
2025-04-09	[Consonic]	akira	<a href="#">Link</a>
2025-04-09	[ccso2014.local(sheriffs)]	incransom	<a href="#">Link</a>
2025-04-09	[Yozgat City Hospital]	bert	<a href="#">Link</a>
2025-04-08	[physiciansmedicalbilling.net]	lockbit3	<a href="#">Link</a>
2025-04-08	[Taxplan]	crypto24	<a href="#">Link</a>
2025-04-08	[Mochtar Karuwin Komar: Indonesian law firm - MKK]	crypto24	<a href="#">Link</a>
2025-04-08	[technoforte software pvt ltd]	crypto24	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-08	[International Busines Service]	crypto24	<a href="#">Link</a>
2025-04-08	[Iris Neofinanciera]	crypto24	<a href="#">Link</a>
2025-04-08	[RFMS, Inc.]	kairos	<a href="#">Link</a>
2025-04-08	[www.gchd.org]	qilin	<a href="#">Link</a>
2025-04-08	[Third Avenue Management]	metaencryptor	<a href="#">Link</a>
2025-04-08	[crystal-d.com]	lockbit3	<a href="#">Link</a>
2025-04-08	[Bauer-Walser AG]	akira	<a href="#">Link</a>
2025-04-08	[Gruppo C.R S.p.a]	sarcoma	<a href="#">Link</a>
2025-04-08	[FKS Group]	sarcoma	<a href="#">Link</a>
2025-04-08	[Coop57]	incransom	<a href="#">Link</a>
2025-04-08	[The Fullerton Hotelsand Resorts]	akira	<a href="#">Link</a>
2025-04-08	[Thiekon Constructie]	incransom	<a href="#">Link</a>
2025-04-07	[Doman Building Materials Group]	interlock	<a href="#">Link</a>
2025-04-07	[galesburg.org]	kairos	<a href="#">Link</a>
2025-04-07	[Privat-Spitex Schweiz GmbH]	qilin	<a href="#">Link</a>
2025-04-07	[CVTE]	hellcat	<a href="#">Link</a>
2025-04-01	[Telecontrol]	ransomhouse	<a href="#">Link</a>
2025-04-04	[Metal Sales Manufacturing Corporation]	morpheus	<a href="#">Link</a>
2025-04-06	[asiapacificex.com]	lockbit3	<a href="#">Link</a>
2025-04-07	[TIME Group]	akira	<a href="#">Link</a>
2025-04-07	[ASOLO DOLCE SAS]	akira	<a href="#">Link</a>
2025-04-07	[SMYK]	akira	<a href="#">Link</a>
2025-04-07	[sunbayhotel.com]	qilin	<a href="#">Link</a>
2025-04-06	[Dubai Company]	devman	<a href="#">Link</a>
2025-04-06	[Texas Construction Firm]	devman	<a href="#">Link</a>
2025-04-06	[Optimax Technology]	devman	<a href="#">Link</a>
2025-04-01	[National Electronic Transit (N.E.T)]	dragonforce	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-01	[Altara]	dragonforce	<a href="#">Link</a>
2025-04-04	[IACC Holdings]	dragonforce	<a href="#">Link</a>
2025-04-04	[Texla Energy Management]	dragonforce	<a href="#">Link</a>
2025-04-01	[Krypton Solutions]	medusa	<a href="#">Link</a>
2025-04-01	[FS Tool Corporation]	medusa	<a href="#">Link</a>
2025-04-06	[Groupe Delcourt]	hunters	<a href="#">Link</a>
2025-04-06	[Hofmann Fördertechnik GmbH]	hunters	<a href="#">Link</a>
2025-04-06	[IDS Infotech]	hunters	<a href="#">Link</a>
2025-04-06	[grupotersa.com.mx]	lockbit3	<a href="#">Link</a>
2025-04-06	[graphiquedefrance.com]	lockbit3	<a href="#">Link</a>
2025-04-06	[Swiss Capitals Group]	rhysida	<a href="#">Link</a>
2025-04-04	[National Ticket Company]	bert	<a href="#">Link</a>
2025-04-05	[Eagle Distilleries]	cicada3301	<a href="#">Link</a>
2025-04-05	[caschile.cl]	VanHelsing	<a href="#">Link</a>
2025-04-05	[Optimax Technology]	qilin	<a href="#">Link</a>
2025-04-05	[ABITL Finishing]	play	<a href="#">Link</a>
2025-04-03	[L&S Mechanical (Reuploaded)]	spacebears	<a href="#">Link</a>
2025-04-05	[Racami]	hellcat	<a href="#">Link</a>
2025-04-05	[Asseco]	hellcat	<a href="#">Link</a>
2025-04-05	[LeoVegas AB]	hellcat	<a href="#">Link</a>
2025-04-05	[Nexia Poyiadjis IT]	hunters	<a href="#">Link</a>
2025-04-05	[Blackmon Mooring]	hunters	<a href="#">Link</a>
2025-04-05	[Apex Logistics International]	sarcoma	<a href="#">Link</a>
2025-04-05	[FUJIFILM]	sarcoma	<a href="#">Link</a>
2025-04-03	[Latronica Law Firm, P.C]	morpheus	<a href="#">Link</a>
2025-04-04	[Fraser Trebilcock]	play	<a href="#">Link</a>
2025-04-04	[Drive Products]	interlock	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-04	[Sinari's software POC]	qilin	<a href="#">Link</a>
2025-04-04	[DELOPT]	akira	<a href="#">Link</a>
2025-04-04	[Source Photonics]	frag	<a href="#">Link</a>
2025-04-04	[AWM Alliance Real Estate Group Ltd.]	akira	<a href="#">Link</a>
2025-04-04	[RORZE Technology Inc.]	akira	<a href="#">Link</a>
2025-04-04	[Sansone Group]	hunters	<a href="#">Link</a>
2025-04-04	[Parker Fabrication, Inc]	akira	<a href="#">Link</a>
2025-04-04	[Henna Chevrolet]	akira	<a href="#">Link</a>
2025-04-04	[National Sign corp]	hunters	<a href="#">Link</a>
2025-04-04	[raymurray.com]	qilin	<a href="#">Link</a>
2025-04-04	[dgr.at]	qilin	<a href="#">Link</a>
2025-04-04	[yumaspazio.com]	qilin	<a href="#">Link</a>
2025-04-04	[The ToolShed]	sarcoma	<a href="#">Link</a>
2025-04-04	[turkish defense military]	babuk2	<a href="#">Link</a>
2025-04-04	[rheinmetall.com (Rheinmetall Defence)]	babuk2	<a href="#">Link</a>
2025-04-04	[Woodmen Valley Chapel]	sarcoma	<a href="#">Link</a>
2025-04-04	[Cherokee County School District]	interlock	<a href="#">Link</a>
2025-04-03	[gangotreehomes.com (RealEstate)]	babuk2	<a href="#">Link</a>
2025-04-03	[Secret plans of Indian army]	babuk2	<a href="#">Link</a>
2025-04-03	[Bangladesh Armed Forces (BangLadesh Army)]	babuk2	<a href="#">Link</a>
2025-04-03	[Saudi Arabian military and government internal center]	babuk2	<a href="#">Link</a>
2025-04-03	[Hellenic Airforce]	babuk2	<a href="#">Link</a>
2025-04-03	[Gem-Dandy Accessories]	akira	<a href="#">Link</a>
2025-04-03	[Fuller Metric Parts]	akira	<a href="#">Link</a>
2025-04-03	[ezbuy.sg (Singapore Shopping)]	babuk2	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-03	[Iran gas service system]	babuk2	<a href="#">Link</a>
2025-04-03	[kfar hatta medical center - Lebanon]	babuk2	<a href="#">Link</a>
2025-04-03	[Polizia italia mail access]	babuk2	<a href="#">Link</a>
2025-04-03	[zalora.sg (Singapore Shopping)]	babuk2	<a href="#">Link</a>
2025-04-02	[Hop Industries]	play	<a href="#">Link</a>
2025-04-02	[Parvin-Clauss Sign Company]	play	<a href="#">Link</a>
2025-04-02	[aosense.com - AO Sense INC.]	babuk2	<a href="#">Link</a>
2025-04-02	[Alton Steel]	lynx	<a href="#">Link</a>
2025-04-02	[navy-mil-bd]	babuk2	<a href="#">Link</a>
2025-04-02	[Taking stock of March 2025]	akira	<a href="#">Link</a>
2025-04-02	[Socarpor]	akira	<a href="#">Link</a>
2025-04-02	[Naza TTDI Sdn Bhd]	akira	<a href="#">Link</a>
2025-04-02	[Mikado Publicis]	akira	<a href="#">Link</a>
2025-04-02	[Entech Sales & Service, LLC]	akira	<a href="#">Link</a>
2025-04-02	[Prima Power]	akira	<a href="#">Link</a>
2025-04-02	[Clarity Ventures]	rhysida	<a href="#">Link</a>
2025-04-02	[crownlaboratories.com]	abyss	<a href="#">Link</a>
2025-04-02	[caliendoarchitects.com]	qilin	<a href="#">Link</a>
2025-04-02	[Brügger Architekten AG]	killsec	<a href="#">Link</a>
2025-04-02	[Royal Saudi Air Force]	killsec	<a href="#">Link</a>
2025-04-02	[Collective Architecture]	killsec	<a href="#">Link</a>
2025-04-02	[IMA Global]	killsec	<a href="#">Link</a>
2025-04-02	[US BioTek Laboratories]	killsec	<a href="#">Link</a>
2025-04-02	[drdo.gov.in]	babuk2	<a href="#">Link</a>
2025-04-01	[uniproof.com.br]	babuk2	<a href="#">Link</a>
2025-04-01	[DG2 Design]	anubis	<a href="#">Link</a>
2025-04-01	[The Loretto Hospital]	incransom	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-01	[(UPDATE) - whitecapcanada.com]	babuk2	<a href="#">Link</a>
2025-04-01	[Bamar Plastics, Inc.]	akira	<a href="#">Link</a>
2025-04-01	[Mercury Integrated Manufacturing]	akira	<a href="#">Link</a>
2025-04-01	[Alora Pharmaceuticals, LLC]	morpheus	<a href="#">Link</a>
2025-04-01	[747 Studios]	killsec	<a href="#">Link</a>
2025-04-01	[BenefitElect]	killsec	<a href="#">Link</a>
2025-04-01	[Ocuco]	killsec	<a href="#">Link</a>
2025-04-01	[Workers Informática Ltda]	killsec	<a href="#">Link</a>
2025-04-01	[Testima Engineering]	killsec	<a href="#">Link</a>
2025-04-01	[Brella]	killsec	<a href="#">Link</a>
2025-04-01	[Fancy Films]	killsec	<a href="#">Link</a>
2025-04-01	[Lendco]	killsec	<a href="#">Link</a>
2025-04-01	[Nydegger + Finger AG]	killsec	<a href="#">Link</a>
2025-04-01	[Dorel Home]	killsec	<a href="#">Link</a>
2025-04-01	[Hexicor]	killsec	<a href="#">Link</a>
2025-04-01	[AAPG]	killsec	<a href="#">Link</a>
2025-04-01	[Hanna Global Solutions]	killsec	<a href="#">Link</a>
2025-04-01	[Flagship Press Flagship Press]	killsec	<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.