


---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20250321



## Inhaltsverzeichnis

<b>1 Editorial</b>	<b>2</b>
<b>2 Security-News</b>	<b>3</b>
2.1 Heise - Security-Alert . . . . .	3
<b>3 Sicherheitslücken</b>	<b>3</b>
3.1 EPSS . . . . .	3
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit . . . . .	3
3.2 BSI - Warn- und Informationsdienst (WID) . . . . .	7
3.3 Sicherheitslücken Meldungen von Tenable . . . . .	11
<b>4 Die Hacks der Woche</b>	<b>12</b>
4.0.1 Information Stealer. Wie funktionieren sie? . . . . .	13
<b>5 Cyberangriffe: (Mär)</b>	<b>14</b>
<b>6 Ransomware-Erpressungen: (Mär)</b>	<b>15</b>
<b>7 Quellen</b>	<b>31</b>
7.1 Quellenverzeichnis . . . . .	31
<b>8 Impressum</b>	<b>32</b>

## 1 Editorial

Guten Morgen,

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

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

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

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

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

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

Ihr Cyberwald-Team

## 2 Security-News

### 2.1 Heise - Security-Alert

## 3 Sicherheitslücken

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

### 3.1 EPSS

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

#### 3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2025-0108	0.924750000	0.997430000	<a href="#">Link</a>
CVE-2024-9474	0.939550000	0.998800000	<a href="#">Link</a>
CVE-2024-9465	0.937890000	0.998640000	<a href="#">Link</a>
CVE-2024-9463	0.919600000	0.997010000	<a href="#">Link</a>
CVE-2024-8963	0.941140000	0.999010000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-8517	0.905300000	0.996170000	<a href="#">Link</a>
CVE-2024-8504	0.916220000	0.996770000	<a href="#">Link</a>
CVE-2024-8503	0.920200000	0.997070000	<a href="#">Link</a>
CVE-2024-8190	0.915170000	0.996710000	<a href="#">Link</a>
CVE-2024-7954	0.934920000	0.998300000	<a href="#">Link</a>
CVE-2024-7593	0.939590000	0.998810000	<a href="#">Link</a>
CVE-2024-6782	0.929590000	0.997820000	<a href="#">Link</a>
CVE-2024-6670	0.943090000	0.999370000	<a href="#">Link</a>
CVE-2024-5932	0.937400000	0.998590000	<a href="#">Link</a>
CVE-2024-5806	0.929880000	0.997830000	<a href="#">Link</a>
CVE-2024-57727	0.918790000	0.996940000	<a href="#">Link</a>
CVE-2024-55956	0.908330000	0.996290000	<a href="#">Link</a>
CVE-2024-55591	0.906810000	0.996230000	<a href="#">Link</a>
CVE-2024-53704	0.910910000	0.996420000	<a href="#">Link</a>
CVE-2024-5217	0.936890000	0.998530000	<a href="#">Link</a>
CVE-2024-51567	0.939930000	0.998850000	<a href="#">Link</a>
CVE-2024-51378	0.932710000	0.998110000	<a href="#">Link</a>
CVE-2024-50623	0.940480000	0.998920000	<a href="#">Link</a>
CVE-2024-50603	0.933410000	0.998180000	<a href="#">Link</a>
CVE-2024-4956	0.936560000	0.998490000	<a href="#">Link</a>
CVE-2024-4885	0.936750000	0.998520000	<a href="#">Link</a>
CVE-2024-4879	0.941130000	0.999000000	<a href="#">Link</a>
CVE-2024-47575	0.912870000	0.996550000	<a href="#">Link</a>
CVE-2024-4577	0.943760000	0.999630000	<a href="#">Link</a>
CVE-2024-45519	0.933670000	0.998220000	<a href="#">Link</a>
CVE-2024-45216	0.920980000	0.997140000	<a href="#">Link</a>
CVE-2024-45195	0.940290000	0.998900000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-4443	0.912490000	0.996520000	<a href="#">Link</a>
CVE-2024-4358	0.940870000	0.998970000	<a href="#">Link</a>
CVE-2024-41713	0.930790000	0.997910000	<a href="#">Link</a>
CVE-2024-4040	0.942450000	0.999220000	<a href="#">Link</a>
CVE-2024-40348	0.922050000	0.997200000	<a href="#">Link</a>
CVE-2024-39914	0.914110000	0.996620000	<a href="#">Link</a>
CVE-2024-38856	0.941840000	0.999110000	<a href="#">Link</a>
CVE-2024-36401	0.943720000	0.999600000	<a href="#">Link</a>
CVE-2024-36104	0.930810000	0.997910000	<a href="#">Link</a>
CVE-2024-3552	0.912890000	0.996560000	<a href="#">Link</a>
CVE-2024-3495	0.916030000	0.996750000	<a href="#">Link</a>
CVE-2024-34470	0.922580000	0.997240000	<a href="#">Link</a>
CVE-2024-34102	0.943470000	0.999520000	<a href="#">Link</a>
CVE-2024-3400	0.943400000	0.999480000	<a href="#">Link</a>
CVE-2024-3273	0.942130000	0.999140000	<a href="#">Link</a>
CVE-2024-3272	0.930690000	0.997910000	<a href="#">Link</a>
CVE-2024-32709	0.902690000	0.996010000	<a href="#">Link</a>
CVE-2024-32113	0.939340000	0.998780000	<a href="#">Link</a>
CVE-2024-31982	0.934840000	0.998300000	<a href="#">Link</a>
CVE-2024-31851	0.923600000	0.997360000	<a href="#">Link</a>
CVE-2024-31850	0.927050000	0.997570000	<a href="#">Link</a>
CVE-2024-31849	0.915310000	0.996720000	<a href="#">Link</a>
CVE-2024-31848	0.915310000	0.996720000	<a href="#">Link</a>
CVE-2024-3094	0.909890000	0.996340000	<a href="#">Link</a>
CVE-2024-29973	0.934290000	0.998270000	<a href="#">Link</a>
CVE-2024-29972	0.908270000	0.996280000	<a href="#">Link</a>
CVE-2024-29895	0.936520000	0.998480000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-29824	0.936130000	0.998430000	<a href="#">Link</a>
CVE-2024-2961	0.929030000	0.997750000	<a href="#">Link</a>
CVE-2024-29269	0.918300000	0.996900000	<a href="#">Link</a>
CVE-2024-29059	0.916430000	0.996790000	<a href="#">Link</a>
CVE-2024-28995	0.942870000	0.999310000	<a href="#">Link</a>
CVE-2024-28987	0.939530000	0.998790000	<a href="#">Link</a>
CVE-2024-2879	0.931170000	0.997940000	<a href="#">Link</a>
CVE-2024-28255	0.913600000	0.996580000	<a href="#">Link</a>
CVE-2024-27956	0.919980000	0.997040000	<a href="#">Link</a>
CVE-2024-27954	0.919300000	0.996990000	<a href="#">Link</a>
CVE-2024-27348	0.938630000	0.998700000	<a href="#">Link</a>
CVE-2024-27292	0.900780000	0.995910000	<a href="#">Link</a>
CVE-2024-27199	0.944440000	0.999900000	<a href="#">Link</a>
CVE-2024-27198	0.945820000	1.000000000	<a href="#">Link</a>
CVE-2024-25852	0.927360000	0.997600000	<a href="#">Link</a>
CVE-2024-25600	0.922190000	0.997210000	<a href="#">Link</a>
CVE-2024-24919	0.942890000	0.999310000	<a href="#">Link</a>
CVE-2024-23917	0.942750000	0.999290000	<a href="#">Link</a>
CVE-2024-23897	0.943510000	0.999530000	<a href="#">Link</a>
CVE-2024-2389	0.943810000	0.999640000	<a href="#">Link</a>
CVE-2024-23692	0.943360000	0.999470000	<a href="#">Link</a>
CVE-2024-2330	0.916970000	0.996810000	<a href="#">Link</a>
CVE-2024-22120	0.924530000	0.997420000	<a href="#">Link</a>
CVE-2024-22024	0.936170000	0.998440000	<a href="#">Link</a>
CVE-2024-21893	0.943200000	0.999410000	<a href="#">Link</a>
CVE-2024-21887	0.943920000	0.999700000	<a href="#">Link</a>
CVE-2024-21762	0.907240000	0.996240000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-21683	0.922010000	0.997190000	<a href="#">Link</a>
CVE-2024-21650	0.920760000	0.997110000	<a href="#">Link</a>
CVE-2024-21413	0.925630000	0.997490000	<a href="#">Link</a>
CVE-2024-20767	0.938210000	0.998680000	<a href="#">Link</a>
CVE-2024-1709	0.940610000	0.998940000	<a href="#">Link</a>
CVE-2024-1698	0.925630000	0.997490000	<a href="#">Link</a>
CVE-2024-1561	0.901790000	0.995970000	<a href="#">Link</a>
CVE-2024-1512	0.923180000	0.997330000	<a href="#">Link</a>
CVE-2024-13160	0.916310000	0.996780000	<a href="#">Link</a>
CVE-2024-13159	0.925980000	0.997530000	<a href="#">Link</a>
CVE-2024-12356	0.921460000	0.997160000	<a href="#">Link</a>
CVE-2024-1212	0.929150000	0.997770000	<a href="#">Link</a>
CVE-2024-11680	0.931700000	0.998010000	<a href="#">Link</a>
CVE-2024-10924	0.925170000	0.997450000	<a href="#">Link</a>

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

Thu, 20 Mar 2025

#### **[UPDATE] [hoch] Red Hat Enterprise Linux und and OpenShift (go-git): Mehrere Schwachstellen**

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux in der Grafana Komponente ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen preiszugeben und einen Denial-of-Service-Zustand zu erzeugen.

- [Link](#)

—

Thu, 20 Mar 2025

#### **[UPDATE] [hoch] Red Hat Enterprise Linux (Advanced Cluster Management): Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux Advanced Cluster Management ausnutzen, um Sicherheitsmaßnahmen zu umgehen und einen Denial-of-Service-Zustand zu



verursachen.

- [Link](#)

—

Thu, 20 Mar 2025

**[UPDATE] [hoch] PostgreSQL: Schwachstelle ermöglicht SQL Injection und Codeausführung**

Ein entfernter, anonymmer Angreifer kann eine Schwachstelle in PostgreSQL ausnutzen, um eine SQL Injection durchzuführen und in der Folge beliebigen Programmcode auszuführen.

- [Link](#)

—

Thu, 20 Mar 2025

**[UPDATE] [hoch] Microsoft Windows/Windows Server: Mehrere Schwachstellen**

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in Microsoft Windows Server, Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2, Microsoft Windows 10, Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows, Microsoft Windows Server 2022 und Microsoft Windows 11 ausnutzen, um beliebigen Programmcode auszuführen, seine Rechte zu erweitern, zu spoofen, Sicherheitsmaßnahmen zu umgehen, Informationen offenzulegen oder einen Denial of Service auszulösen .

- [Link](#)

—

Thu, 20 Mar 2025

**[NEU] [hoch] Veeam Backup & Replication: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Veeam Backup & Replication ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Thu, 20 Mar 2025

**[NEU] [hoch] ESRI ArcGIS Portal: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen**

Ein entfernter, anonymmer Angreifer kann eine Schwachstelle in ESRI ArcGIS Portal ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Thu, 20 Mar 2025

**[NEU] [hoch] IBM InfoSphere Information Server: Schwachstelle ermöglicht Privilegieneskalation**

Ein lokaler Angreifer kann eine Schwachstelle in IBM InfoSphere Information Server ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Thu, 20 Mar 2025

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

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in verschiedenen SAP Produkten ausnutzen, um dadurch die Vertraulichkeit, Verfügbarkeit und die Integrität der Anwendung zu gefährden.

- [Link](#)

—

Thu, 20 Mar 2025

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in ffmpeg ausnutzen, um einen Denial of Service Angriff durchzuführen, vertrauliche Informationen offenzulegen oder beliebigen Code auszuführen.

- [Link](#)

—

Thu, 20 Mar 2025

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

Ein entfernter Angreifer kann mehrere Schwachstellen in Docker ausnutzen, um seine Privilegien zu erhöhen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen oder Dateien zu manipulieren.

- [Link](#)

—

Thu, 20 Mar 2025

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

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

- [Link](#)

—

Thu, 20 Mar 2025

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

Ein entfernter Angreifer kann mehrere Schwachstellen in PostgreSQL ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, Daten zu manipulieren oder vertrauliche Informationen preiszugeben.

- [Link](#)

—

Thu, 20 Mar 2025

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

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

- [Link](#)

—

Thu, 20 Mar 2025

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

Ein Angreifer kann mehrere Schwachstellen in Rsync ausnutzen, um vertrauliche Informationen preiszugeben, sich erhöhte Rechte zu verschaffen und Daten zu manipulieren.

- [Link](#)

—

Thu, 20 Mar 2025

**[UPDATE] [hoch] libxml2: Schwachstelle ermöglicht remote Code Execution**

Ein lokaler Angreifer kann eine Schwachstelle in libxml2 ausnutzen, um einen Code auszuführen.

- [Link](#)

—

Thu, 20 Mar 2025

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

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

- [Link](#)

—

Thu, 20 Mar 2025

**[UPDATE] [hoch] Red Hat Enterprise Linux (Podman und Buildah): Schwachstelle ermöglicht Manipulation von Dateien**

Ein lokaler Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um Dateien zu manipulieren.

- [Link](#)

—

Thu, 20 Mar 2025

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

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

- [Link](#)

—

Thu, 20 Mar 2025

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

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

- [Link](#)

—

Thu, 20 Mar 2025

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

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

- [Link](#)

### 3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
3/20/2025	[Azure Linux 3.0 Security Update: expat / python3 (CVE-2024-45491)]	critical
3/20/2025	[Azure Linux 3.0 Security Update: expat / python3 (CVE-2024-45492)]	critical
3/20/2025	[Azure Linux 3.0 Security Update: xorg-x11-server / xorg-x11-server-Xwayland (CVE-2025-26598)]	high
3/20/2025	[Azure Linux 3.0 Security Update: libxml2 (CVE-2025-27113)]	high
3/20/2025	[Azure Linux 3.0 Security Update: xorg-x11-server / xorg-x11-server-Xwayland (CVE-2025-26601)]	high
3/20/2025	[Azure Linux 3.0 Security Update: xorg-x11-server / xorg-x11-server-Xwayland (CVE-2025-26597)]	high
3/20/2025	[Azure Linux 3.0 Security Update: libxml2 (CVE-2025-24928)]	high
3/20/2025	[Azure Linux 3.0 Security Update: xorg-x11-server / xorg-x11-server-Xwayland (CVE-2025-26599)]	high
3/20/2025	[Azure Linux 3.0 Security Update: libxml2 (CVE-2024-56171)]	high
3/20/2025	[Azure Linux 3.0 Security Update: kernel (CVE-2024-56605)]	high
3/20/2025	[CBL Mariner 2.0 Security Update: ruby (CVE-2025-27219)]	high
3/20/2025	[Azure Linux 3.0 Security Update: python3 (CVE-2024-4032)]	high

Datum	Schwachstelle	Bewertung
3/20/2025	[Azure Linux 3.0 Security Update: xorg-x11-server / xorg-x11-server-Xwayland (CVE-2025-26595)]	high
3/20/2025	[Azure Linux 3.0 Security Update: cert-manager / cf-cli / docker-buildx / docker-compose / kubernetes / kubevirt / moby-compose (CVE-2025-22869)]	high
3/20/2025	[Azure Linux 3.0 Security Update: libxml2 (CVE-2024-25062)]	high
3/20/2025	[Azure Linux 3.0 Security Update: vim (CVE-2025-27423)]	high
3/20/2025	[Azure Linux 3.0 Security Update: kernel (CVE-2024-56606)]	high
3/20/2025	[Azure Linux 3.0 Security Update: expat / python3 (CVE-2024-45490)]	high
3/20/2025	[Azure Linux 3.0 Security Update: xorg-x11-server / xorg-x11-server-Xwayland (CVE-2025-26600)]	high
3/20/2025	[Azure Linux 3.0 Security Update: cmake / nghttp2 / nodejs / nodejs18 (CVE-2023-35945)]	high
3/20/2025	[Azure Linux 3.0 Security Update: kernel (CVE-2024-50051)]	high
3/20/2025	[Azure Linux 3.0 Security Update: azcopy / blobfuse2 / cert-manager / containerized-data-importer / coredns (CVE-2025-22868)]	high
3/20/2025	[Azure Linux 3.0 Security Update: python-virtualenv (CVE-2024-53899)]	high
3/20/2025	[Azure Linux 3.0 Security Update: kernel (CVE-2024-56650)]	high
3/20/2025	[Azure Linux 3.0 Security Update: erlang (CVE-2025-26618)]	high
3/20/2025	[Azure Linux 3.0 Security Update: kernel (CVE-2024-56614)]	high

## 4 Die Hacks der Woche

mit Martin Haunschmid

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



[Zum Youtube Video](#)

## 5 Cyberangriffe: (Mär)

Datum	Opfer	Land	Information
2025-03-17	Keding Enterprises Co., Ltd.	[TWN]	<a href="#">Link</a>
2025-03-17	Sozialholding der Stadt Mönchengladbach	[DEU]	<a href="#">Link</a>
2025-03-17	Virgin Islands Lottery (VIL)	[VIR]	<a href="#">Link</a>
2025-03-16	Mairie de Kirkel	[DEU]	<a href="#">Link</a>
2025-03-16	Atchison County	[USA]	<a href="#">Link</a>
2025-03-16	Ascom	[CHE]	<a href="#">Link</a>
2025-03-16	James Pascoe	[NZL]	<a href="#">Link</a>
2025-03-15	Strafford County	[USA]	<a href="#">Link</a>
2025-03-14	Spar Gruppe Schweiz	[CHE]	<a href="#">Link</a>
2025-03-13	Mairie de Murça	[PRT]	<a href="#">Link</a>
2025-03-13	Pelham School District	[USA]	<a href="#">Link</a>
2025-03-12	Edesur Dominicana	[DOM]	<a href="#">Link</a>
2025-03-12	Prefeitura Municipal de Palmeira	[BRA]	<a href="#">Link</a>
2025-03-11	YAP Health Services	[FSM]	<a href="#">Link</a>
2025-03-11	Derby Police Department	[USA]	<a href="#">Link</a>
2025-03-09	Aerticket	[DEU]	<a href="#">Link</a>
2025-03-07	Crystal D	[USA]	<a href="#">Link</a>
2025-03-06	Bikur Rofeh	[ISR]	<a href="#">Link</a>
2025-03-05	Ålands Centralandelslag (ÅCA)	[FIN]	<a href="#">Link</a>
2025-03-05	Endless Mountains Health Systems (EMHS)	[USA]	<a href="#">Link</a>
2025-03-05	Fachhochschule Nordwestschweiz	[CHE]	<a href="#">Link</a>
2025-03-05	St Albert the Great College	[MLT]	<a href="#">Link</a>
2025-03-04	Unikorn Semiconductor Corp.	[TWN]	<a href="#">Link</a>
2025-03-04	Stadtwerke Schwerte	[DEU]	<a href="#">Link</a>
2025-03-04	Adina Hotels	[AUS]	<a href="#">Link</a>
2025-03-03	Whitman Hospital and Medical Clinics	[USA]	<a href="#">Link</a>

Datum	Opfer	Land	Information
2025-03-03	Mission, Texas	[USA]	<a href="#">Link</a>
2025-03-03	Brucha	[AUT]	<a href="#">Link</a>
2025-03-03	Vranken-Pommery Monopole	[FRA]	<a href="#">Link</a>
2025-03-02	HomeTeamNS	[SGP]	<a href="#">Link</a>
2025-03-02	POLSA (Polish Space Agency)	[POL]	<a href="#">Link</a>
2025-03-02	Adval Tech Group	[CHE]	<a href="#">Link</a>
2025-03-02	Penn-Harris-Madison school district	[USA]	<a href="#">Link</a>
2025-03-02	Ivinhema	[BRA]	<a href="#">Link</a>
2025-03-02	Berkeley Research Group (BRG)	[USA]	<a href="#">Link</a>
2025-03-01	National Presto Industries, Inc.	[USA]	<a href="#">Link</a>
2025-03-01	TFE Hotels	[AUS]	<a href="#">Link</a>

## 6 Ransomware-Erpressungen: (Mär)

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-21	[exostar.com TOP Defense AS]	babuk2	<a href="#">Link</a>
2025-03-21	[Our Official telegram channel babak Locker 2.0]	babuk2	<a href="#">Link</a>
2025-03-21	[Standard Capital Securities (Pvt) Backoffice - Pakistan Stock Market Data Vault]	babuk2	<a href="#">Link</a>
2025-03-17	[www.mslglobalexp.com]	ransomhub	<a href="#">Link</a>
2025-03-20	[mohrss.gov.cn ( Ministry of Human Resources and Social Security )]	babuk2	<a href="#">Link</a>
2025-03-20	[amazon.com]	babuk2	<a href="#">Link</a>
2025-03-18	[L&S Mechanical]	spacebears	<a href="#">Link</a>
2025-03-02	[Whittaker & Company]	spacebears	<a href="#">Link</a>
2025-03-20	[www.janvier-labs.com]	ransomhub	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-17	[National Safety Council]	medusa	<a href="#">Link</a>
2025-03-17	[Augusta Industrial Services, Inc.]	medusa	<a href="#">Link</a>
2025-03-19	[Champions Group]	medusa	<a href="#">Link</a>
2025-03-19	[J McCann & Co Ltd]	medusa	<a href="#">Link</a>
2025-03-19	[Big Horn County School District #4]	medusa	<a href="#">Link</a>
2025-03-20	[Obra Play]	killsec	<a href="#">Link</a>
2025-03-20	[interiseworld.com]	killsec	<a href="#">Link</a>
2025-03-20	[Instituto de Ojos]	killsec	<a href="#">Link</a>
2025-03-20	[Oag.state.va.us]	cloak	<a href="#">Link</a>
2025-03-20	[Wr-recht.de]	cloak	<a href="#">Link</a>
2025-03-20	[Baltimorecityschools]	cloak	<a href="#">Link</a>
2025-03-20	[Land Planners]	akira	<a href="#">Link</a>
2025-03-20	[Auren]	akira	<a href="#">Link</a>
2025-03-20	[Newtown Friends School (newtownfriends.org)]	fog	<a href="#">Link</a>
2025-03-20	[fr.sodexo.com]	babuk2	<a href="#">Link</a>
2025-03-20	[Corporate access, up to Shipping Apps in QATAR]	babuk2	<a href="#">Link</a>
2025-03-20	[woqod.com]	babuk2	<a href="#">Link</a>
2025-03-20	[mof.go.th - Ministry of Finance (Thailand)]	babuk2	<a href="#">Link</a>
2025-03-20	[ZB ZIMMERMANN UND BECKER GmbH]	akira	<a href="#">Link</a>
2025-03-20	[Cargills Bank]	hunters	<a href="#">Link</a>
2025-03-20	[Luff Industries]	qilin	<a href="#">Link</a>
2025-03-20	[Megacentro]	hunters	<a href="#">Link</a>
2025-03-20	[smic.mi.th (Thailand Intelligence Agency)]	babuk2	<a href="#">Link</a>
2025-03-20	[www.kvhealth.net]	kraken	<a href="#">Link</a>
2025-03-19	[www.gob.ve]	babuk2	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-19	[Access Panel Financial Technology Company (Thailand)]	babuk2	<a href="#">Link</a>
2025-03-19	[United States County Palm Beach Government]	babuk2	<a href="#">Link</a>
2025-03-19	[Municipal taxation Secretariat Access - Brazil Government]	babuk2	<a href="#">Link</a>
2025-03-19	[Intelligence Bureau of the Joint Staff Department of the Central Military Commission...]	babuk2	<a href="#">Link</a>
2025-03-19	[rac.gov.my]	babuk2	<a href="#">Link</a>
2025-03-19	[nimapinfotech.com]	babuk2	<a href="#">Link</a>
2025-03-17	[controlledair.com]	ransomhub	<a href="#">Link</a>
2025-03-19	[Q railing]	play	<a href="#">Link</a>
2025-03-19	[www.medsrx.com]	VanHelsing	<a href="#">Link</a>
2025-03-07	[Los Madroños Hospital]	qilin	<a href="#">Link</a>
2025-03-19	[The Ely Company, Inc.]	akira	<a href="#">Link</a>
2025-03-19	[Machu Picchu Foods]	akira	<a href="#">Link</a>
2025-03-19	[LINC Systems]	akira	<a href="#">Link</a>
2025-03-19	[VEST LLC]	akira	<a href="#">Link</a>
2025-03-19	[Palomino Petroleum]	lynx	<a href="#">Link</a>
2025-03-18	[warmsworth.doncaster.sch.uk]	incransom	<a href="#">Link</a>
2025-03-18	[alphaoil.ca]	incransom	<a href="#">Link</a>
2025-03-19	[CD]	monti	<a href="#">Link</a>
2025-03-19	[Gloria Cales]	monti	<a href="#">Link</a>
2025-03-18	[newhollandwood.com]	incransom	<a href="#">Link</a>
2025-03-18	[Coopertruni]	arcusmedia	<a href="#">Link</a>
2025-03-18	[THX Transport]	arcusmedia	<a href="#">Link</a>
2025-03-18	[Kiribati Government]	arcusmedia	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-18	[Atos-racks.com]	VanHelsing	<a href="#">Link</a>
2025-03-18	[AMICIO]	lynx	<a href="#">Link</a>
2025-03-18	[Ted Hosmer Enterprises]	rhysida	<a href="#">Link</a>
2025-03-18	[51talk.com]	lockbit3	<a href="#">Link</a>
2025-03-18	[esaote.com]	babuk2	<a href="#">Link</a>
2025-03-18	[nstda.or.th]	babuk2	<a href="#">Link</a>
2025-03-18	[pajak.go.id]	babuk2	<a href="#">Link</a>
2025-03-18	[dukcapil.kemendagri.go.id (SIK DUKCAPIL MINISTRY OF HOME AFFAIRS OF INDONESIA)]	babuk2	<a href="#">Link</a>
2025-03-18	[semaphore.asso.fr]	funksec	<a href="#">Link</a>
2025-03-13	[PTS Group]	qilin	<a href="#">Link</a>
2025-03-18	[whitecapcanada.com]	babuk2	<a href="#">Link</a>
2025-03-18	[JAMEL CONTAINERS LLC]	akira	<a href="#">Link</a>
2025-03-18	[Cleveland Municipal Court]	qilin	<a href="#">Link</a>
2025-03-18	[hcahealthcare.com INC.]	babuk2	<a href="#">Link</a>
2025-03-18	[SAGETRA INC.]	akira	<a href="#">Link</a>
2025-03-18	[gaertnerhof-jeutter.de]	incransom	<a href="#">Link</a>
2025-03-18	[sp.tnitelecom.com]	babuk2	<a href="#">Link</a>
2025-03-18	[Otelier.io]	babuk2	<a href="#">Link</a>
2025-03-18	[expertdata.com.au]	incransom	<a href="#">Link</a>
2025-03-18	[airtelligence.com]	incransom	<a href="#">Link</a>
2025-03-18	[highwirepress.com]	babuk2	<a href="#">Link</a>
2025-03-18	[Harcourts Prime Properties]	killsec	<a href="#">Link</a>
2025-03-07	[Far East Consortium]	nightspire	<a href="#">Link</a>
2025-03-16	[Bridgewater Retirement Community]	nightspire	<a href="#">Link</a>
2025-03-17	[Electronics For Imaging]	hellcat	<a href="#">Link</a>
2025-03-17	[www.baxterlaboratories.com]	ransomhub	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-17	[ccktech.com]	ransomhub	<a href="#">Link</a>
2025-03-17	[Lepant Law Office]	qilin	<a href="#">Link</a>
2025-03-17	[Worldlawn Power Equipment]	qilin	<a href="#">Link</a>
2025-03-17	[Diode Technologies]	qilin	<a href="#">Link</a>
2025-03-17	[terrell.k12.ga.us]	safepay	<a href="#">Link</a>
2025-03-03	[oneill.com]	ransomhub	<a href="#">Link</a>
2025-03-17	[www.jhayber.com]	ransomhub	<a href="#">Link</a>
2025-03-17	[RAE (Real Academia Española) (rae.es)]	fog	<a href="#">Link</a>
2025-03-17	[Solist]	akira	<a href="#">Link</a>
2025-03-17	[CableVision]	hunters	<a href="#">Link</a>
2025-03-12	[www.cityofbellville.com]	VanHelsing	<a href="#">Link</a>
2025-03-17	[assaabloy.com]	cactus	<a href="#">Link</a>
2025-03-17	[kyb.com]	cactus	<a href="#">Link</a>
2025-03-17	[PIBOR ISO SA]	akira	<a href="#">Link</a>
2025-03-17	[SMC Corporation]	qilin	<a href="#">Link</a>
2025-03-17	[KIU System Solutions]	apos	<a href="#">Link</a>
2025-03-17	[taobao.com]	babuk2	<a href="#">Link</a>
2025-03-17	[This entry has been removed following a request from the company]	babuk2	<a href="#">Link</a>
2025-03-17	[March, 6, 2025: City government office in Van (Turkey) van.bel.tr hacked. 7.4 TiB is for s...]	skira	<a href="#">Link</a>
2025-03-17	[icmr.gov.in]	babuk2	<a href="#">Link</a>
2025-03-16	[Ministry Of Defense of the Republic Of Korea]	babuk2	<a href="#">Link</a>
2025-03-16	[JD.com Inc (Chinese)]	babuk2	<a href="#">Link</a>
2025-03-16	[KD Panels]	crazyhunter	<a href="#">Link</a>
2025-03-16	[Kairav Chemofarbe Industries]	trinity	<a href="#">Link</a>
2025-03-16	[consultoria-consultores.es]	trinity	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-16	[ROBONG-WINMINI]	trinity	<a href="#">Link</a>
2025-03-16	[Lake Psychological Services]	trinity	<a href="#">Link</a>
2025-03-16	[CANAM Realty Group]	trinity	<a href="#">Link</a>
2025-03-16	[CNS]	trinity	<a href="#">Link</a>
2025-03-16	[la-z-boy]	trinity	<a href="#">Link</a>
2025-03-15	[sitro.com.au]	incransom	<a href="#">Link</a>
2025-03-15	[www.ameda.com]	ransomhub	<a href="#">Link</a>
2025-03-16	[SRP Companies (Second lock! + Company scam!)]	medusa	<a href="#">Link</a>
2025-03-16	[Coldwell Banker D'Ann Harper, REALTORS]	medusa	<a href="#">Link</a>
2025-03-15	[Kleen-Pak Products]	dragonforce	<a href="#">Link</a>
2025-03-15	[Moncaro]	dragonforce	<a href="#">Link</a>
2025-03-16	[DTS -services]	dragonforce	<a href="#">Link</a>
2025-03-16	[Florida Department of Transportation (FDOT)]	babuk2	<a href="#">Link</a>
2025-03-16	[Orange.com]	babuk2	<a href="#">Link</a>
2025-03-16	[Courageous Home Care]	hunters	<a href="#">Link</a>
2025-03-10	[Tanaka Electronics Taiwan Co.,LTD]	nightspire	<a href="#">Link</a>
2025-03-05	[Waihong Environmental Services Limited]	nightspire	<a href="#">Link</a>
2025-03-12	[Wilson Re Limited]	nightspire	<a href="#">Link</a>
2025-03-16	[MESS sales srl]	sarcoma	<a href="#">Link</a>
2025-03-15	[Ascom Holding AG]	hellcat	<a href="#">Link</a>
2025-03-15	[Ricardo Rodriguez]	qilin	<a href="#">Link</a>
2025-03-15	[Belarus E-commerce & Energy Data]	babuk2	<a href="#">Link</a>
2025-03-15	[nrru.ac.th - University]	babuk2	<a href="#">Link</a>
2025-03-14	[yeanshalle.de]	incransom	<a href="#">Link</a>
2025-03-14	[Perrigo Company]	termite	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-14	[Fulcrum Lifting]	lynx	<a href="#">Link</a>
2025-03-14	[argusdatainsights.de]	safepay	<a href="#">Link</a>
2025-03-14	[idcconstruction.com]	ransomhub	<a href="#">Link</a>
2025-03-14	[Domina Entrega Total]	akira	<a href="#">Link</a>
2025-03-14	[jennyoo.com]	ransomhub	<a href="#">Link</a>
2025-03-14	[Unicorr Packaging Group]	akira	<a href="#">Link</a>
2025-03-14	[iaai.com - Washington DC DMV]	babuk2	<a href="#">Link</a>
2025-03-14	[Indiv Usa]	lynx	<a href="#">Link</a>
2025-03-14	[Tryon]	lynx	<a href="#">Link</a>
2025-03-14	[The Ministry of National Defense - mod.gov.vn (NavyVietnam)]	babuk2	<a href="#">Link</a>
2025-03-14	[movistar.com.pe]	babuk2	<a href="#">Link</a>
2025-03-14	[JAGGEDPEAK.COM]	clop	<a href="#">Link</a>
2025-03-14	[RACKSPACE.COM]	clop	<a href="#">Link</a>
2025-03-14	[LIPPERTENT.COM]	clop	<a href="#">Link</a>
2025-03-14	[GARANIMALS.COM]	clop	<a href="#">Link</a>
2025-03-13	[Portland Street Honda]	medusa	<a href="#">Link</a>
2025-03-13	[Karen S Pouliot]	medusa	<a href="#">Link</a>
2025-03-14	[mdm-insurance.com]	abyss	<a href="#">Link</a>
2025-03-14	[Cothron's Security Professionals]	rhysida	<a href="#">Link</a>
2025-03-13	[www.raymond.in]	ransomhub	<a href="#">Link</a>
2025-03-13	[dtrglaw.com]	ransomhub	<a href="#">Link</a>
2025-03-12	[rixos.com]	embargo	<a href="#">Link</a>
2025-03-13	[Taiwan - Mackay Hospital]	babuk2	<a href="#">Link</a>
2025-03-13	[cch.org.tw - Changhua Christian Hospital]	babuk2	<a href="#">Link</a>
2025-03-13	[nuclep.gov.br. Nuclep Brazil]	babuk2	<a href="#">Link</a>
2025-03-14	[parliament.iq]	babuk2	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-14	[web.asia.edu.tw - Taiwan (Asia University)]	babuk2	<a href="#">Link</a>
2025-03-14	[Intelligence Bureau of the Joint Staff Department of the Central Military Commission China]	babuk2	<a href="#">Link</a>
2025-03-14	[Indian military and government defense 20TB]	babuk2	<a href="#">Link</a>
2025-03-13	[fstlogistics.com]	lynx	<a href="#">Link</a>
2025-03-13	[Harrells.com]	lynx	<a href="#">Link</a>
2025-03-13	[SL Tennessee Information]	play	<a href="#">Link</a>
2025-03-13	[Backes]	play	<a href="#">Link</a>
2025-03-13	[Best Cheer Stone]	play	<a href="#">Link</a>
2025-03-14	[Terralogic]	secp0	<a href="#">Link</a>
2025-03-13	[University Diagnostic Medical Imaging, PC (udmi.net)]	fog	<a href="#">Link</a>
2025-03-12	[El Camino Real Academy (elcaminorealacademy)]	fog	<a href="#">Link</a>
2025-03-13	[Iraqi Ministry of Finance]	babuk2	<a href="#">Link</a>
2025-03-13	[Iraqi Council of Ministers]	babuk2	<a href="#">Link</a>
2025-03-12	[Ascoma Group]	akira	<a href="#">Link</a>
2025-03-03	[Raja Ferry Port Public Company Limited]	nightspire	<a href="#">Link</a>
2025-03-08	[Far East Consortium International Limited]	nightspire	<a href="#">Link</a>
2025-03-03	[Business Ledger Limited]	nightspire	<a href="#">Link</a>
2025-03-01	[Tohpe Corporation]	nightspire	<a href="#">Link</a>
2025-03-12	[Hydro-Vacuum S.A.]	nightspire	<a href="#">Link</a>
2025-03-12	[marinabaysands.com - Singapore Hotel (Internal Server)]	babuk2	<a href="#">Link</a>
2025-03-12	[Yushin America, Inc]	qilin	<a href="#">Link</a>
2025-03-12	[PACOMARTINEZ]	akira	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-12	[SMG Bahamas]	akira	<a href="#">Link</a>
2025-03-12	[extremepformance.com]	funksec	<a href="#">Link</a>
2025-03-12	[hitekgroup.in india Finance]	babuk2	<a href="#">Link</a>
2025-03-12	[Indastrial Acceptance Corporation]	akira	<a href="#">Link</a>
2025-03-12	[tempel.com]	cactus	<a href="#">Link</a>
2025-03-12	[thermoid.com]	cactus	<a href="#">Link</a>
2025-03-12	[baillie.com]	cactus	<a href="#">Link</a>
2025-03-12	[CAHOKIA CUSD 187 SCHOOL DISTRICT]	qilin	<a href="#">Link</a>
2025-03-12	[India's telecommunication network]	babuk2	<a href="#">Link</a>
2025-03-12	[Best Telecom Laos]	akira	<a href="#">Link</a>
2025-03-12	[CNQC]	akira	<a href="#">Link</a>
2025-03-12	[Peerless Food Equipment]	akira	<a href="#">Link</a>
2025-03-12	[Helmut Hölbling Spedition GmbH]	akira	<a href="#">Link</a>
2025-03-12	[urban1.com]	cactus	<a href="#">Link</a>
2025-03-12	[rocketstores.com]	cactus	<a href="#">Link</a>
2025-03-12	[www.visualisation.one]	ransomhub	<a href="#">Link</a>
2025-03-12	[HYPONAMIRU]	arcusmedia	<a href="#">Link</a>
2025-03-12	[HYPERNOVA TELECOM]	arcusmedia	<a href="#">Link</a>
2025-03-12	[unimore.it]	funksec	<a href="#">Link</a>
2025-03-12	[Baykar Turkish defense company C4I and artificial intelligence]	babuk2	<a href="#">Link</a>
2025-03-11	[tradingacademy.com]	safepay	<a href="#">Link</a>
2025-03-11	[ultimateclasslimo.com]	safepay	<a href="#">Link</a>
2025-03-11	[havenresorts.com]	safepay	<a href="#">Link</a>
2025-03-11	[lgipr.com]	safepay	<a href="#">Link</a>
2025-03-11	[jockeysalud.com.pe]	safepay	<a href="#">Link</a>
2025-03-11	[motomecanica.com]	safepay	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-11	[cali.losolivos.co]	safepay	<a href="#">Link</a>
2025-03-11	[Skyward Specialty Insurance]	killsec	<a href="#">Link</a>
2025-03-11	[Trymata]	killsec	<a href="#">Link</a>
2025-03-03	[Gaines County, Texas]	qilin	<a href="#">Link</a>
2025-03-11	[Springfield Water and Sewer Commission]	lynx	<a href="#">Link</a>
2025-03-11	[Suder&Suder]	qilin	<a href="#">Link</a>
2025-03-11	[Longue Vue Club]	lynx	<a href="#">Link</a>
2025-03-11	[Taking stock of February 2025]	akira	<a href="#">Link</a>
2025-03-11	[WAUGH & GOODWIN, LLP]	akira	<a href="#">Link</a>
2025-03-11	[airexplore.aero Company]	babuk2	<a href="#">Link</a>
2025-03-11	[Veristat]	akira	<a href="#">Link</a>
2025-03-11	[Edesur Dominicana]	hunters	<a href="#">Link</a>
2025-03-11	[All4Labels - Global Packaging Group]	akira	<a href="#">Link</a>
2025-03-11	[Essex County OB/GYN Associates]	incransom	<a href="#">Link</a>
2025-03-11	[Princeton Hydro]	akira	<a href="#">Link</a>
2025-03-11	[isee-eg.com]	funksec	<a href="#">Link</a>
2025-03-11	[fn.de.gov.br brazilian government]	babuk2	<a href="#">Link</a>
2025-03-11	[wapda.gov.pk]	babuk2	<a href="#">Link</a>
2025-03-11	[lexmark.com Company]	babuk2	<a href="#">Link</a>
2025-03-10	[Wilkinson Rogers (wilkinsonrogers.com)]	fog	<a href="#">Link</a>
2025-03-11	[forvismazars.com.fr ( mazars.fr )]	babuk2	<a href="#">Link</a>
2025-03-10	[Magnolia Manor (magnoliamanor.com)]	fog	<a href="#">Link</a>
2025-03-10	[petstop.com Company]	babuk2	<a href="#">Link</a>
2025-03-10	[misaludhealth.com]	babuk2	<a href="#">Link</a>
2025-03-10	[bank.pingan.com (CN)]	babuk2	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-10	[Access to Indian Ministry of Defence and Military Secret (DRDO) documents By Babuk Locker ...]	babuk2	<a href="#">Link</a>
2025-03-10	[fredsalvuccicorp.com]	kairos	<a href="#">Link</a>
2025-03-10	[Mandarin.com.br]	babuk2	<a href="#">Link</a>
2025-03-10	[Callico Distributors, Inc.]	akira	<a href="#">Link</a>
2025-03-10	[Pacific Honda Company]	akira	<a href="#">Link</a>
2025-03-10	[Arcusin]	akira	<a href="#">Link</a>
2025-03-10	[www.hexosys.com]	ransomhub	<a href="#">Link</a>
2025-03-10	[Safe-Strap Company, LLC]	akira	<a href="#">Link</a>
2025-03-10	[Fickling & Company]	akira	<a href="#">Link</a>
2025-03-07	[GPS 909]	akira	<a href="#">Link</a>
2025-03-10	[mazars.fr]	babuk2	<a href="#">Link</a>
2025-03-10	[Dacas Argentina]	qilin	<a href="#">Link</a>
2025-03-05	[Cotswold Fayre]	dragonforce	<a href="#">Link</a>
2025-03-05	[Vercoe Insurance Brokers]	dragonforce	<a href="#">Link</a>
2025-03-05	[Steel Dynamics UK]	dragonforce	<a href="#">Link</a>
2025-03-05	[E Leet Woodworking]	dragonforce	<a href="#">Link</a>
2025-03-04	[Customer Management Systems]	medusa	<a href="#">Link</a>
2025-03-06	[CPI Books]	medusa	<a href="#">Link</a>
2025-03-09	[ACTi Corporation]	lynx	<a href="#">Link</a>
2025-03-09	[BerksBar.org]	incransom	<a href="#">Link</a>
2025-03-09	[klabs.it]	funksec	<a href="#">Link</a>
2025-03-03	[Salemerode.com]	flocker	<a href="#">Link</a>
2025-03-09	[State Bar of Texas (www.texasbar.com)]	incransom	<a href="#">Link</a>
2025-03-09	[Greenwood Village South GVS]	incransom	<a href="#">Link</a>
2025-03-07	[prelco.ca]	qilin	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-09	[Jerue Companies]	play	<a href="#">Link</a>
2025-03-09	[Syma-System]	play	<a href="#">Link</a>
2025-03-09	[Compound Solutions]	play	<a href="#">Link</a>
2025-03-09	[T J Machine & Tool]	play	<a href="#">Link</a>
2025-03-09	[Gevril]	play	<a href="#">Link</a>
2025-03-09	[Peak Season]	play	<a href="#">Link</a>
2025-03-09	[Yorke & Curtis]	play	<a href="#">Link</a>
2025-03-09	[Buckley BalaWilson Mew]	play	<a href="#">Link</a>
2025-03-09	[Holiday Comfort]	play	<a href="#">Link</a>
2025-03-09	[Clawson Honda]	play	<a href="#">Link</a>
2025-03-09	[Dectron]	play	<a href="#">Link</a>
2025-03-09	[Nor Arc]	play	<a href="#">Link</a>
2025-03-09	[British virgin islands London Office]	rhysida	<a href="#">Link</a>
2025-03-05	[Changhua Christian Hospital]	crazyhunter	<a href="#">Link</a>
2025-03-05	[Huacheng Electric]	crazyhunter	<a href="#">Link</a>
2025-03-05	[Mackay Hospital]	crazyhunter	<a href="#">Link</a>
2025-03-05	[Asia University Hospital]	crazyhunter	<a href="#">Link</a>
2025-03-05	[Asia University]	crazyhunter	<a href="#">Link</a>
2025-03-06	[mitchellmcnutt.com]	ransomhub	<a href="#">Link</a>
2025-03-08	[univ-rennes.fr]	funksec	<a href="#">Link</a>
2025-03-05	[Tech NH]	lynx	<a href="#">Link</a>
2025-03-07	[Allworx]	bianlian	<a href="#">Link</a>
2025-03-07	[Minnesota Orthodontics]	bianlian	<a href="#">Link</a>
2025-03-07	[REYCOTEL]	arcusmedia	<a href="#">Link</a>
2025-03-07	[total-ps.com]	ransomhub	<a href="#">Link</a>
2025-03-07	[Hancock Public School]	interlock	<a href="#">Link</a>
2025-03-07	[lofotenseafood.com]	lynx	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-07	[ADDA (adda.io)]	ransomexx	<a href="#">Link</a>
2025-03-07	[Swift Haulage Berhad]	akira	<a href="#">Link</a>
2025-03-07	[Aj Taylor Electrical Contractors Ltd]	sarcoma	<a href="#">Link</a>
2025-03-07	[Sittab INC]	akira	<a href="#">Link</a>
2025-03-07	[wheats.com]	ransomhub	<a href="#">Link</a>
2025-03-07	[srmg.com.au]	ransomhub	<a href="#">Link</a>
2025-03-07	[sorbonne-universite.fr]	funksec	<a href="#">Link</a>
2025-03-06	[RFA Decor]	akira	<a href="#">Link</a>
2025-03-05	[www.portlandschools.org]	ransomhub	<a href="#">Link</a>
2025-03-05	[www.hinton.ca]	ransomhub	<a href="#">Link</a>
2025-03-05	[www.convention.qc.ca]	ransomhub	<a href="#">Link</a>
2025-03-06	[hickorylaw.com]	ransomhub	<a href="#">Link</a>
2025-03-06	[lovesac.com]	ransomhub	<a href="#">Link</a>
2025-03-06	[agi.net]	monti	<a href="#">Link</a>
2025-03-06	[Adval Tech]	lynx	<a href="#">Link</a>
2025-03-06	[WJCC Public Schools (wjccschools.org)]	fog	<a href="#">Link</a>
2025-03-06	[Connekted, Inc.]	qilin	<a href="#">Link</a>
2025-03-06	[Naples Heritage Golf & Country Club]	incransom	<a href="#">Link</a>
2025-03-06	[Ministry of Foreign Affairs of Ukraine]	qilin	<a href="#">Link</a>
2025-03-06	[Oberlin Cable Co-op (oberlin.net)]	fog	<a href="#">Link</a>
2025-03-06	[Elite Advanced Laser Corporation]	akira	<a href="#">Link</a>
2025-03-05	[1X Internet]	fog	<a href="#">Link</a>
2025-03-05	[Bizcode]	fog	<a href="#">Link</a>
2025-03-05	[Manning Publications Co.]	fog	<a href="#">Link</a>
2025-03-05	[Engikam]	fog	<a href="#">Link</a>
2025-03-05	[FHNW]	fog	<a href="#">Link</a>
2025-03-05	[Aeonsparx]	fog	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-05	[Flightsim studio]	fog	<a href="#">Link</a>
2025-03-05	[Neopoly]	fog	<a href="#">Link</a>
2025-03-05	[Kr3m]	fog	<a href="#">Link</a>
2025-03-05	[InfoReach]	fog	<a href="#">Link</a>
2025-03-05	[Euranova]	fog	<a href="#">Link</a>
2025-03-05	[Inelmatic]	fog	<a href="#">Link</a>
2025-03-05	[Kotliva]	fog	<a href="#">Link</a>
2025-03-05	[Blue Planet]	fog	<a href="#">Link</a>
2025-03-05	[Eumetsat]	fog	<a href="#">Link</a>
2025-03-05	[Melexis]	fog	<a href="#">Link</a>
2025-03-06	[City government office in Van (Turkey) - van.bel.tr]	skira	<a href="#">Link</a>
2025-03-06	[Law Diary (USA)]	skira	<a href="#">Link</a>
2025-03-06	[Carruth Compliance Consulting]	skira	<a href="#">Link</a>
2025-03-06	[CCL Products India]	skira	<a href="#">Link</a>
2025-03-06	[Krisala Developer (India)]	skira	<a href="#">Link</a>
2025-03-05	[The 19 biggest gitlabs]	fog	<a href="#">Link</a>
2025-03-05	[willms-fleisch.de]	safepay	<a href="#">Link</a>
2025-03-05	[Pervedant]	lynx	<a href="#">Link</a>
2025-03-05	[SCOLARO FETTER GRIZANTI & McGOUGH, P.C. (scolaro.com)]	fog	<a href="#">Link</a>
2025-03-05	[Adrenalina]	akira	<a href="#">Link</a>
2025-03-05	[Cyncly Company]	akira	<a href="#">Link</a>
2025-03-05	[City Plumbing & Electric Supply Co]	akira	<a href="#">Link</a>
2025-03-04	[www.sunsweet.com]	ransomhub	<a href="#">Link</a>
2025-03-05	[Best Collateral, Inc.]	rhysida	<a href="#">Link</a>
2025-03-04	[Chicago Doorways, LLC]	qilin	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-05	[Schmiedetechnik Plettenberg GmbH & Co KG]	lynx	<a href="#">Link</a>
2025-03-04	[365labs - Security Corp]	monti	<a href="#">Link</a>
2025-03-04	[PFS Grupo - Plan de igualdad, Sostenibilidad]	qilin	<a href="#">Link</a>
2025-03-04	[Pampili (pampili.com.br)]	fog	<a href="#">Link</a>
2025-03-04	[Keystone Pacific Property Management LLC]	bianlian	<a href="#">Link</a>
2025-03-04	[Mosley Glick O'Brien, Inc.]	bianlian	<a href="#">Link</a>
2025-03-04	[FANTIN group]	akira	<a href="#">Link</a>
2025-03-04	[Grupo Baston Aerossol (baston.com.br)]	fog	<a href="#">Link</a>
2025-03-04	[Ray Fogg Corporate Properties]	akira	<a href="#">Link</a>
2025-03-04	[goencon.com]	ransomhub	<a href="#">Link</a>
2025-03-04	[Seabank Group]	lynx	<a href="#">Link</a>
2025-03-04	[Tata Technologies]	hunters	<a href="#">Link</a>
2025-03-04	[Wendy Wu Tours]	killsec	<a href="#">Link</a>
2025-03-04	[rockhillwc.com]	qilin	<a href="#">Link</a>
2025-03-04	[bpmmicro.com]	qilin	<a href="#">Link</a>
2025-03-04	[peruzzi.com]	qilin	<a href="#">Link</a>
2025-03-04	[IOVATE.COM]	clop	<a href="#">Link</a>
2025-03-04	[Legal Aid Society of Salt Lake]	bianlian	<a href="#">Link</a>
2025-03-04	[Ewald Consulting]	bianlian	<a href="#">Link</a>
2025-03-04	[Netcom-World]	apos	<a href="#">Link</a>
2025-03-04	[InternetWay]	apos	<a href="#">Link</a>
2025-03-04	[cimenyan.desa.id]	funksec	<a href="#">Link</a>
2025-03-03	[familychc.com]	ransomhub	<a href="#">Link</a>
2025-03-03	[andreyevengineering.com]	ransomhub	<a href="#">Link</a>
2025-03-03	[drvitenas.com]	kairos	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-03	[usarice.com]	kairos	<a href="#">Link</a>
2025-03-03	[Sunnking SustainableSolutions]	akira	<a href="#">Link</a>
2025-03-03	[LINKGROUP]	arcusmedia	<a href="#">Link</a>
2025-03-03	[Openreso]	arcusmedia	<a href="#">Link</a>
2025-03-03	[Itapeseg]	arcusmedia	<a href="#">Link</a>
2025-03-03	[logic insectes]	arcusmedia	<a href="#">Link</a>
2025-03-03	[RJ IT Solutions]	arcusmedia	<a href="#">Link</a>
2025-03-03	[Grafitec]	arcusmedia	<a href="#">Link</a>
2025-03-03	[synaptic.co.tz]	arcusmedia	<a href="#">Link</a>
2025-03-03	[quigleyeye.com]	cactus	<a href="#">Link</a>
2025-03-03	[La Unión]	lynx	<a href="#">Link</a>
2025-03-03	[Central McGowan (centralmcgowan.com)]	fog	<a href="#">Link</a>
2025-03-03	[Klesk Metal Stamping Co (kleskmetalstamping.com)]	fog	<a href="#">Link</a>
2025-03-03	[Forstenlechner Installationstechnik]	akira	<a href="#">Link</a>
2025-03-03	[ceratec.com]	abyss	<a href="#">Link</a>
2025-03-02	[Pre Con Industries]	play	<a href="#">Link</a>
2025-03-02	[IT-IQ Botswana]	play	<a href="#">Link</a>
2025-03-02	[North American Fire Hose]	play	<a href="#">Link</a>
2025-03-02	[Couri Insurance Agency]	play	<a href="#">Link</a>
2025-03-02	[Optometrics]	play	<a href="#">Link</a>
2025-03-02	[International Process Plants]	play	<a href="#">Link</a>
2025-03-02	[Ganong Bros]	play	<a href="#">Link</a>
2025-03-02	[FM.GOB.AR]	monti	<a href="#">Link</a>
2025-03-02	[Bell Ambulance]	medusa	<a href="#">Link</a>
2025-03-02	[Workforce Group]	killsec	<a href="#">Link</a>
2025-03-01	[germancentre.sg]	incransom	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-01	[JEFFREYCOURT.COM]	clon	<a href="#">Link</a>
2025-03-01	[APTEAN.COM]	clon	<a href="#">Link</a>
2025-03-01	[Wayne County, Michigan]	interlock	<a href="#">Link</a>
2025-03-01	[The Smeg Group]	interlock	<a href="#">Link</a>
2025-03-01	[Newton & Associates, Inc]	rhysida	<a href="#">Link</a>

## 7 Quellen

### 7.1 Quellenverzeichnis

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



## 8 Impressum



***Herausgeber:***

Marlon Hübner  
Brückenstraße 3  
57629 Höchstenbach

***E-Mail***

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

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