

Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20250315



Inhaltsverzeichnis

1 Editorial	2
2 Security-News	3
2.1 Heise - Security-Alert	3
3 Sicherheitslücken	3
3.1 EPSS	3
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit	3
3.2 BSI - Warn- und Informationsdienst (WID)	5
3.3 Sicherheitslücken Meldungen von Tenable	9
4 Die Hacks der Woche	11
4.0.1 Information Stealer. Wie funktionieren sie?	12
5 Cyberangriffe: (Mär)	13
6 Ransomware-Erpressungen: (Mär)	14
7 Quellen	24
7.1 Quellenverzeichnis	24
8 Impressum	25

1 Editorial

Guten Morgen,

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

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

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

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

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

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

Ihr Cyberwald-Team

2 Security-News

2.1 Heise - Security-Alert

3 Sicherheitslücken

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

3.1 EPSS

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

3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2025-0108	0.967640000	0.997990000	Link
CVE-2024-9474	0.974550000	0.999800000	Link
CVE-2024-9465	0.937960000	0.993700000	Link
CVE-2024-9463	0.959940000	0.996400000	Link
CVE-2024-8963	0.966010000	0.997630000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-7593	0.967730000	0.998010000	Link
CVE-2024-6670	0.900620000	0.990980000	Link
CVE-2024-5910	0.967120000	0.997880000	Link
CVE-2024-55956	0.968970000	0.998320000	Link
CVE-2024-53704	0.960740000	0.996540000	Link
CVE-2024-5217	0.945850000	0.994500000	Link
CVE-2024-50623	0.969520000	0.998470000	Link
CVE-2024-50603	0.927520000	0.992810000	Link
CVE-2024-4879	0.950100000	0.995030000	Link
CVE-2024-4577	0.953780000	0.995470000	Link
CVE-2024-4358	0.926010000	0.992720000	Link
CVE-2024-41713	0.955390000	0.995680000	Link
CVE-2024-40711	0.964240000	0.997250000	Link
CVE-2024-4040	0.966350000	0.997730000	Link
CVE-2024-38856	0.946330000	0.994570000	Link
CVE-2024-36401	0.961790000	0.996690000	Link
CVE-2024-3400	0.959660000	0.996340000	Link
CVE-2024-3273	0.937240000	0.993640000	Link
CVE-2024-32113	0.938440000	0.993750000	Link
CVE-2024-28995	0.970760000	0.998800000	Link
CVE-2024-28987	0.957000000	0.995910000	Link
CVE-2024-27348	0.961750000	0.996690000	Link
CVE-2024-27198	0.970340000	0.998690000	Link
CVE-2024-24919	0.966210000	0.997670000	Link
CVE-2024-23897	0.973580000	0.999570000	Link
CVE-2024-2389	0.928740000	0.992900000	Link
CVE-2024-23692	0.967310000	0.997930000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-21893	0.960410000	0.996480000	Link
CVE-2024-21887	0.973690000	0.999610000	Link
CVE-2024-20767	0.966090000	0.997660000	Link
CVE-2024-1709	0.957060000	0.995920000	Link
CVE-2024-1212	0.946600000	0.994590000	Link
CVE-2024-0986	0.954890000	0.995610000	Link
CVE-2024-0195	0.962680000	0.996900000	Link
CVE-2024-0012	0.969610000	0.998500000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 14 Mar 2025

[NEU] [kritisch] Flowise: Schwachstelle ermöglicht Codeausführung

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

- [Link](#)

—

Fri, 14 Mar 2025

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

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

- [Link](#)

—

Fri, 14 Mar 2025

[UPDATE] [hoch] GitLab: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in GitLab ausnutzen, um Informationen preiszugeben, beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, Daten zu manipulieren und einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

—

Fri, 14 Mar 2025

[NEU] [hoch] Ruby SAML: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Ruby SAML ausnutzen, um Sicherheitsvorkehrungen zu umgehen und um einen Denial of Service Zustand herbeizuführen.

- [Link](#)

—

Fri, 14 Mar 2025

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

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

- [Link](#)

—

Fri, 14 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](#)

—

Fri, 14 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](#)

—

Fri, 14 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](#)

—

Fri, 14 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](#)

—

Fri, 14 Mar 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](#)

—

Fri, 14 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](#)

—

Fri, 14 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](#)

—

Fri, 14 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](#)

—

Fri, 14 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](#)

—

Fri, 14 Mar 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](#)

—

Fri, 14 Mar 2025

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

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

- [Link](#)

—

Fri, 14 Mar 2025

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

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

- [Link](#)

—

Fri, 14 Mar 2025

[UPDATE] [hoch] Apache Tomcat: Schwachstelle ermöglicht Manipulation, Codeausführung und Offenlegung von Daten

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Apache Tomcat ausnutzen, um beliebigen Programmcode auszuführen, Dateien zu manipulieren oder Informationen offenzulegen.

- [Link](#)

—

Thu, 13 Mar 2025

[UPDATE] [hoch] Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um Spoofing-Angriffe durchzuführen, Sicherheitsmaßnahmen zu umgehen, erhöhte Privilegien zu erlangen, einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen, Daten zu manipulieren, beliebigen Code auszuführen oder nicht spezifizierte Auswirkungen zu verursachen.

- [Link](#)

—

Thu, 13 Mar 2025

[NEU] [hoch] Cisco IOS XR: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Cisco IOS XR ausnutzen, um Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand herbeizuführen, erhöhte Rechte zu erlangen, beliebigen Code auszuführen und Daten zu manipulieren.

- [Link](#)

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
3/14/2025	[FreeBSD : Gitlab – Vulnerabilities (a435609c-ffd5-11ef-b4e4-2cf05da270f3)]	critical
3/14/2025	[Debian dsa-5878 : libapache2-mod-php8.2 - security update]	critical
3/14/2025	[RHEL 9 : webkit2gtk3 (RHSA-2024:9553)]	critical
3/14/2025	[Amazon Linux 2023 : bpftool, kernel, kernel-devel (ALAS2023-2025-876)]	high
3/14/2025	[Amazon Linux 2 : kernel (ALASKERNEL-5.10-2025-082)]	high
3/14/2025	[Amazon Linux 2023 : bpftool, kernel, kernel-devel (ALAS2023-2025-864)]	high
3/14/2025	[Amazon Linux 2 : kernel (ALAS-2024-2696)]	high
3/14/2025	[Adobe Substance 3D Sampler 0.0.x < 5.0 Multiple Vulnerabilities (APSB25-16)]	high
3/14/2025	[Adobe Substance 3D Designer 14.1.1 Multiple Vulnerabilities (APSB25-22)]	high
3/14/2025	[SUSE SLES12 Security Update : google-osconfig-agent (SUSE-SU-2025:0852-1)]	high
3/14/2025	[openSUSE 15 Security Update : rubygem-rack-1_6 (SUSE-SU-2025:0858-1)]	high
3/14/2025	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2025:0856-1)]	high
3/14/2025	[FreeBSD : shibboleth-sp – Parameter manipulation allows the forging of signed SAML messages (0b43fac4-005d-11f0-a540-6cc21735f730)]	high
3/14/2025	[Fedora 40 : xorg-x11-server (2025-fd490bcdcd)]	high
3/14/2025	[Fedora 40 : thunderbird (2025-4b50cd66a5)]	high
3/14/2025	[SUSE SLES15 Security Update : kernel (SUSE-SU-2025:0855-1)]	high
3/14/2025	[Oracle Linux 7 : kernel (ELSA-2025-1281)]	high

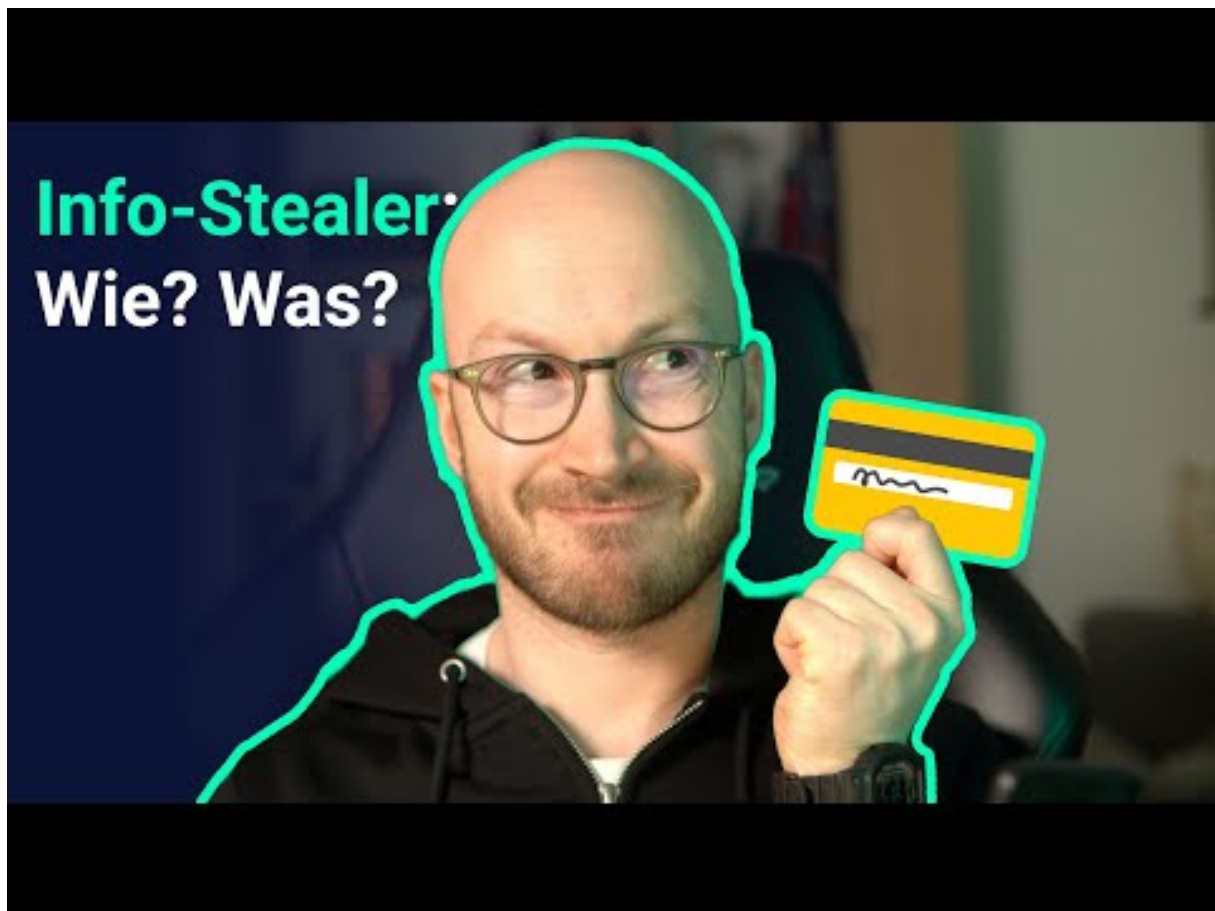
Datum	Schwachstelle	Bewertung
3/14/2025	[AlmaLinux 9 : kernel (ALSA-2025:2627)]	high
3/14/2025	[Adobe Substance 3D Modeler 0.0.x < 1.21.0 Multiple Vulnerabilities (APSB25-21)]	high
3/14/2025	[Siemens Teamcenter Multiple Vulnerabilities (SSA-050438)]	high
3/14/2025	[Juniper Junos OS DoS (JSA88100)]	high
3/14/2025	[Security Update for Microsoft Visual Studio Code (March 2025)]	high
3/14/2025	[Security Updates for Microsoft Visual Studio 2022 17.8 / 17.10 / 17.12 / 17.13 Products (March 2025)]	high
3/14/2025	[Security Updates for Microsoft Visual Studio 2019 16.11 Products (March 2025)]	high
3/14/2025	[Security Updates for Microsoft Visual Studio 2017 15.9 Products (March 2025)]	high
3/14/2025	[Security Updates for Microsoft Office Products (March 2025)]	high
3/14/2025	[Security Updates for Microsoft Excel Products (March 2025)]	high
3/14/2025	[Security Updates for Microsoft Access Products (March 2025)]	high
3/14/2025	[Security Updates for Microsoft Word Products (March 2025)]	high
3/14/2025	[RHEL 9 : webkit2gtk3 (RHSA-2024:9638)]	high
3/13/2025	[Siemens SCALANCE X-200RNA Switch Devices Improper Input Validation (CVE-2016-0797)]	high
3/13/2025	[Siemens SCALANCE X-200RNA Switch Devices Improper Restriction of Operations within the Bounds of a Memory Buffer (CVE-2016-0778)]	high
3/13/2025	[Siemens SCALANCE X-200RNA Switch Devices Concurrent Execution using Shared Resource with Improper Synchronization (CVE-2015-1791)]	high
3/13/2025	[Siemens SCALANCE X-200RNA Switch Devices Exposure of Sensitive Information to an Unauthorized Actor (CVE-2015-3193)]	high

Datum	Schwachstelle	Bewertung
3/13/2025	[Siemens SCALANCE X-200RNA Switch Devices Improper Input Validation (CVE-2016-6515)]	high
3/13/2025	[Siemens SCALANCE X-200RNA Switch Devices NULL Pointer Dereference (CVE-2015-3194)]	high
3/13/2025	[Siemens SCALANCE X-200RNA Switch Devices Use After Free (CVE-2015-6564)]	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
2025-03-13	Mairie de Murça	[PRT]	Link
2025-03-12	Edesur Dominicana	[DOM]	Link
2025-03-11	YAP Health Services	[FSM]	Link
2025-03-09	Aerticket	[DEU]	Link
2025-03-07	Crystal D	[USA]	Link
2025-03-06	Bikur Rofeh	[ISR]	Link
2025-03-05	Ålands Centralandelslag (ÅCA)	[FIN]	Link
2025-03-05	Endless Mountains Health Systems (EMHS)	[USA]	Link
2025-03-05	Fachhochschule Nordwestschweiz	[CHE]	Link
2025-03-04	Unikorn Semiconductor Corp.	[TWN]	Link
2025-03-04	Stadtwerke Schwerte	[DEU]	Link
2025-03-04	Adina Hotels	[AUS]	Link
2025-03-03	Whitman Hospital and Medical Clinics	[USA]	Link
2025-03-03	Mission, Texas	[USA]	Link
2025-03-03	Brucha	[AUT]	Link
2025-03-03	Vranken-Pommery Monopole	[FRA]	Link
2025-03-02	HomeTeamNS	[SGP]	Link
2025-03-02	POLSA (Polish Space Agency)	[POL]	Link
2025-03-02	Adval Tech Group	[CHE]	Link
2025-03-02	Penn-Harris-Madison school district	[USA]	Link
2025-03-02	Ivinhema	[BRA]	Link
2025-03-02	Berkeley Research Group (BRG)	[USA]	Link
2025-03-01	National Presto Industries, Inc.	[USA]	Link
2025-03-01	TFE Hotels	[AUS]	Link

6 Ransomware-Erpressungen: (Mär)

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-14	[yeanshalle.de]	incransom	Link
2025-03-14	[Perrigo Company]	termite	Link
2025-03-14	[Fulcrum Lifting]	lynx	Link
2025-03-14	[argusdatainsights.de]	safepay	Link
2025-03-14	[idcconstruction.com]	ransomhub	Link
2025-03-14	[Domina Entrega Total]	akira	Link
2025-03-14	[jennyoo.com]	ransomhub	Link
2025-03-14	[Unicorr Packaging Group]	akira	Link
2025-03-14	[iaai.com - Washington DC DMV]	babuk2	Link
2025-03-14	[Indiv Usa]	lynx	Link
2025-03-14	[Bancroft Wines]	incransom	Link
2025-03-14	[Tryon]	lynx	Link
2025-03-14	[The Ministry of National Defense - mod.gov.vn (NavyVietnam)]	babuk2	Link
2025-03-14	[movistar.com.pe]	babuk2	Link
2025-03-14	[JAGGEDPEAK.COM]	clop	Link
2025-03-14	[RACKSPACE.COM]	clop	Link
2025-03-14	[LIPPERTENT.COM]	clop	Link
2025-03-14	[GARANIMALS.COM]	clop	Link
2025-03-13	[Portland Street Honda]	medusa	Link
2025-03-13	[Karen S Pouliot]	medusa	Link
2025-03-14	[mdm-insurance.com]	abyss	Link
2025-03-14	[Cothron's Security Professionals]	rhysida	Link
2025-03-13	[www.raymond.in]	ransomhub	Link
2025-03-13	[dtrglaw.com]	ransomhub	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-13	[World Wide Fittings]	qilin	Link
2025-03-12	[rixos.com]	embargo	Link
2025-03-13	[Taiwan - Mackay Hospital]	babuk2	Link
2025-03-13	[cch.org.tw - Changhua Christian Hospital]	babuk2	Link
2025-03-13	[nuclep.gov.br. Nuclep Brazil]	babuk2	Link
2025-03-14	[parliament.iq]	babuk2	Link
2025-03-14	[web.asia.edu.tw - Taiwan (Asia University)]	babuk2	Link
2025-03-14	[Intelligence Bureau of the Joint Staff Department of the Central Military Commission China]	babuk2	Link
2025-03-14	[Indian military and government defense 20TB]	babuk2	Link
2025-03-13	[fstlogistics.com]	lynx	Link
2025-03-13	[Harrells.com]	lynx	Link
2025-03-13	[SL Tennessee Information]	play	Link
2025-03-13	[Backes]	play	Link
2025-03-13	[Best Cheer Stone]	play	Link
2025-03-14	[Terralogic]	secp0	Link
2025-03-13	[University Diagnostic Medical Imaging, PC (udmi.net)]	fog	Link
2025-03-12	[El Camino Real Academy (elcaminorealacademy)]	fog	Link
2025-03-13	[Iraqi Ministry of Finance]	babuk2	Link
2025-03-13	[Iraqi Council of Ministers]	babuk2	Link
2025-03-12	[Ascoma Group]	akira	Link
2025-03-03	[Raja Ferry Port Public Company Limited]	nightspire	Link
2025-03-08	[Far East Consortium International Limited]	nightspire	Link
2025-03-03	[Business Ledger Limited]	nightspire	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-01	[Tohpe Corporation]	nightspire	Link
2025-03-12	[Hydro-Vacuum S.A.]	nightspire	Link
2025-03-12	[marinabaysands.com - Singapore Hotel (Internal Server)]	babuk2	Link
2025-03-12	[Yushin America, Inc]	qilin	Link
2025-03-12	[PACOMARTINEZ]	akira	Link
2025-03-12	[SMG Bahamas]	akira	Link
2025-03-12	[extremepformance.com]	funksec	Link
2025-03-12	[hitekgroup.in india Finance]	babuk2	Link
2025-03-12	[Indastrial Acceptance Corporation]	akira	Link
2025-03-12	[tempel.com]	cactus	Link
2025-03-12	[thermoid.com]	cactus	Link
2025-03-12	[baillie.com]	cactus	Link
2025-03-12	[CAHOKIA CUSD 187 SCHOOL DISTRICT]	qilin	Link
2025-03-12	[India's telecommunication network]	babuk2	Link
2025-03-12	[Best Telecom Laos]	akira	Link
2025-03-12	[CNQC]	akira	Link
2025-03-12	[Peerless Food Equipment]	akira	Link
2025-03-12	[Helmut Hölbling Spedition GmbH]	akira	Link
2025-03-12	[urban1.com]	cactus	Link
2025-03-12	[rocketstores.com]	cactus	Link
2025-03-12	[www.visualisation.one]	ransomhub	Link
2025-03-10	[HOST Software Entwicklung und Consulting GmbH]	qilin	Link
2025-03-12	[HYPONAMIRU]	arcusmedia	Link
2025-03-12	[HYPERNOVA TELECOM]	arcusmedia	Link
2025-03-12	[unimore.it]	funksec	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-12	[Baykar Turkish defense company C4I and artificial intelligence]	babuk2	Link
2025-03-11	[tradingacademy.com]	safepay	Link
2025-03-11	[ultimateclasslimo.com]	safepay	Link
2025-03-11	[havenresorts.com]	safepay	Link
2025-03-11	[lgipr.com]	safepay	Link
2025-03-11	[jockeysalud.com.pe]	safepay	Link
2025-03-11	[motomecanica.com]	safepay	Link
2025-03-11	[cali.losolivos.co]	safepay	Link
2025-03-11	[Skyward Specialty Insurance]	killsec	Link
2025-03-11	[Trymata]	killsec	Link
2025-03-03	[Gaines County, Texas]	qilin	Link
2025-03-11	[Springfield Water and Sewer Commission]	lynx	Link
2025-03-11	[Suder&Suder]	qilin	Link
2025-03-11	[Longue Vue Club]	lynx	Link
2025-03-11	[Taking stock of February 2025]	akira	Link
2025-03-11	[WAUGH & GOODWIN, LLP]	akira	Link
2025-03-11	[airexplore.aero Company]	babuk2	Link
2025-03-11	[Veristat]	akira	Link
2025-03-11	[Edesur Dominicana]	hunters	Link
2025-03-11	[All4Labels - Global Packaging Group]	akira	Link
2025-03-11	[Essex County OB/GYN Associates]	incransom	Link
2025-03-11	[Princeton Hydro]	akira	Link
2025-03-11	[isee-eg.com]	funksec	Link
2025-03-11	[fnnde.gov.br brazilian government]	babuk2	Link
2025-03-11	[wapda.gov.pk]	babuk2	Link
2025-03-11	[lexmark.com Company]	babuk2	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-10	[Wilkinson Rogers (wilkinsonrogers.com)]	fog	Link
2025-03-11	[forvismazars.com.fr (mazars.fr)]	babuk2	Link
2025-03-10	[Magnolia Manor (magnoliamanor.com)]	fog	Link
2025-03-10	[petstop.com Company]	babuk2	Link
2025-03-10	[misaludhealth.com]	babuk2	Link
2025-03-10	[bank.pingan.com (CN)]	babuk2	Link
2025-03-10	[Access to Indian Ministry of Defence and Military Secret (DRDO) documents By Babuk Locker ...]	babuk2	Link
2025-03-10	[fredsalvuccicorp.com]	kairos	Link
2025-03-10	[Mandarin.com.br]	babuk2	Link
2025-03-10	[Callico Distributors, Inc.]	akira	Link
2025-03-10	[Pacific Honda Company]	akira	Link
2025-03-10	[Arcusin]	akira	Link
2025-03-10	[www.hexosys.com]	ransomhub	Link
2025-03-10	[Safe-Strap Company, LLC]	akira	Link
2025-03-10	[Fickling & Company]	akira	Link
2025-03-07	[GPS 909]	akira	Link
2025-03-10	[mazars.fr]	babuk2	Link
2025-03-10	[Dacas Argentina]	qilin	Link
2025-03-05	[Cotswold Fayre]	dragonforce	Link
2025-03-05	[Vercoe Insurance Brokers]	dragonforce	Link
2025-03-05	[Steel Dynamics UK]	dragonforce	Link
2025-03-05	[E Leet Woodworking]	dragonforce	Link
2025-03-04	[Customer Management Systems]	medusa	Link
2025-03-06	[CPI Books]	medusa	Link
2025-03-09	[ACTi Corporation]	lynx	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-09	[BerksBar.org]	incransom	Link
2025-03-09	[baldaufarchitekten.de]	incransom	Link
2025-03-09	[klabs.it]	funksec	Link
2025-03-03	[Salemerode.com]	flocker	Link
2025-03-09	[State Bar of Texas (www.texasbar.com)]	incransom	Link
2025-03-09	[Greenwood Village South GVS]	incransom	Link
2025-03-07	[prelco.ca]	qilin	Link
2025-03-07	[KH OneStop]	qilin	Link
2025-03-09	[Jerue Companies]	play	Link
2025-03-09	[Syma-System]	play	Link
2025-03-09	[Compound Solutions]	play	Link
2025-03-09	[T J Machine & Tool]	play	Link
2025-03-09	[Gevril]	play	Link
2025-03-09	[Peak Season]	play	Link
2025-03-09	[Yorke & Curtis]	play	Link
2025-03-09	[Buckley BalaWilson Mew]	play	Link
2025-03-09	[Holiday Comfort]	play	Link
2025-03-09	[Clawson Honda]	play	Link
2025-03-09	[Dectron]	play	Link
2025-03-09	[Nor Arc]	play	Link
2025-03-09	[British virgin islands London Office]	rhysida	Link
2025-03-05	[Changhua Christian Hospital]	crazyhunter	Link
2025-03-05	[Huacheng Electric]	crazyhunter	Link
2025-03-05	[Mackay Hospital]	crazyhunter	Link
2025-03-05	[Asia University Hospital]	crazyhunter	Link
2025-03-05	[Asia University]	crazyhunter	Link
2025-03-06	[mitchellmcnutt.com]	ransomhub	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-08	[univ-rennes.fr]	funksec	Link
2025-03-05	[Tech NH]	lynx	Link
2025-03-07	[Allworx]	bianlian	Link
2025-03-07	[Minnesota Orthodontics]	bianlian	Link
2025-03-07	[REYCOTEL]	arcusmedia	Link
2025-03-07	[total-ps.com]	ransomhub	Link
2025-03-07	[Hancock Public School]	interlock	Link
2025-03-07	[lofotenseafood.com]	lynx	Link
2025-03-07	[ADDA (adda.io)]	ransomexx	Link
2025-03-07	[Swift Haulage Berhad]	akira	Link
2025-03-07	[Aj Taylor Electrical Contractors Ltd]	sarcoma	Link
2025-03-07	[Sittab INC]	akira	Link
2025-03-07	[wheats.com]	ransomhub	Link
2025-03-07	[srmg.com.au]	ransomhub	Link
2025-03-07	[sorbonne-universite.fr]	funksec	Link
2025-03-06	[RFA Decor]	akira	Link
2025-03-05	[www.portlandschools.org]	ransomhub	Link
2025-03-05	[www.hinton.ca]	ransomhub	Link
2025-03-05	[www.convention.qc.ca]	ransomhub	Link
2025-03-06	[hickorylaw.com]	ransomhub	Link
2025-03-06	[lovesac.com]	ransomhub	Link
2025-03-06	[agi.net]	monti	Link
2025-03-06	[Adval Tech]	lynx	Link
2025-03-06	[WJCC Public Schools (wjccschools.org)]	fog	Link
2025-03-06	[Connekted, Inc.]	qilin	Link
2025-03-06	[Naples Heritage Golf & Country Club]	incransom	Link
2025-03-06	[Ministry of Foreign Affairs of Ukraine]	qilin	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-06	[Oberlin Cable Co-op (oberlin.net)]	fog	Link
2025-03-06	[Elite Advanced Laser Corporation]	akira	Link
2025-03-05	[1X Internet]	fog	Link
2025-03-05	[Bizcode]	fog	Link
2025-03-05	[Manning Publications Co.]	fog	Link
2025-03-05	[Engikam]	fog	Link
2025-03-05	[FHNW]	fog	Link
2025-03-05	[Aeonsparx]	fog	Link
2025-03-05	[Flightsim studio]	fog	Link
2025-03-05	[Neopoly]	fog	Link
2025-03-05	[Kr3m]	fog	Link
2025-03-05	[InfoReach]	fog	Link
2025-03-05	[Euranova]	fog	Link
2025-03-05	[Inelmatic]	fog	Link
2025-03-05	[Kotliva]	fog	Link
2025-03-05	[Blue Planet]	fog	Link
2025-03-05	[Eumetsat]	fog	Link
2025-03-05	[Melexis]	fog	Link
2025-03-06	[City government office in Van (Turkey) - van.bel.tr]	skira	Link
2025-03-06	[Law Diary (USA)]	skira	Link
2025-03-06	[Carruth Compliance Consulting]	skira	Link
2025-03-06	[CCL Products India]	skira	Link
2025-03-06	[Krisala Developer (India)]	skira	Link
2025-03-05	[The 19 biggest gitlabs]	fog	Link
2025-03-05	[willms-fleisch.de]	safepay	Link
2025-03-05	[Pervedant]	lynx	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-05	[SCOLARO FETTER GRIZANTI & McGOUGH, P.C. (scolaro.com)]	fog	Link
2025-03-05	[www.black-star.fr]	ransomhub	Link
2025-03-05	[Adrenalina]	akira	Link
2025-03-05	[Cyncly Company]	akira	Link
2025-03-05	[City Plumbing & Electric Supply Co]	akira	Link
2025-03-03	[www.japanrebuilt.jp]	ransomhub	Link
2025-03-04	[www.sunsweet.com]	ransomhub	Link
2025-03-05	[Best Collateral, Inc.]	rhysida	Link
2025-03-04	[Chicago Doorways, LLC]	qilin	Link
2025-03-05	[Schmiedetechnik Plettenberg GmbH & Co KG]	lynx	Link
2025-03-04	[365labs - Security Corp]	monti	Link
2025-03-04	[PFS Grupo - Plan de igualdad, Sostenibilidad]	qilin	Link
2025-03-04	[Pampili (pampili.com.br)]	fog	Link
2025-03-04	[Keystone Pacific Property Management LLC]	bianlian	Link
2025-03-04	[Mosley Glick O'Brien, Inc.]	bianlian	Link
2025-03-04	[FANTIN group]	akira	Link
2025-03-04	[Grupo Baston Aerosol (baston.com.br)]	fog	Link
2025-03-04	[Ray Fogg Corporate Properties]	akira	Link
2025-03-04	[goencon.com]	ransomhub	Link
2025-03-04	[Seabank Group]	lynx	Link
2025-03-04	[Tata Technologies]	hunters	Link
2025-03-04	[Wendy Wu Tours]	killsec	Link
2025-03-04	[rockhillwc.com]	qilin	Link
2025-03-04	[bpmmicro.com]	qilin	Link
2025-03-04	[peruzzi.com]	qilin	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-04	[IOVATE.COM]	clop	Link
2025-03-04	[Legal Aid Society of Salt Lake]	bianlian	Link
2025-03-04	[Ewald Consulting]	bianlian	Link
2025-03-04	[Netcom-World]	apos	Link
2025-03-04	[InternetWay]	apos	Link
2025-03-04	[cimenyan.desa.id]	funksec	Link
2025-03-03	[familychc.com]	ransomhub	Link
2025-03-03	[andreyevengineering.com]	ransomhub	Link
2025-03-03	[drvitenas.com]	kairos	Link
2025-03-03	[usarice.com]	kairos	Link
2025-03-03	[Sunnking SustainableSolutions]	akira	Link
2025-03-03	[LINKGROUP]	arcusmedia	Link
2025-03-03	[Openreso]	arcusmedia	Link
2025-03-03	[Itapeseg]	arcusmedia	Link
2025-03-03	[logic insectes]	arcusmedia	Link
2025-03-03	[RJ IT Solutions]	arcusmedia	Link
2025-03-03	[Grafitec]	arcusmedia	Link
2025-03-03	[synaptic.co.tz]	arcusmedia	Link
2025-03-03	[quigleyeye.com]	cactus	Link
2025-03-03	[La Unión]	lynx	Link
2025-03-03	[Central McGowan (centralmcgowan.com)]	fog	Link
2025-03-03	[Klesk Metal Stamping Co (kleskmetalstamping.com)]	fog	Link
2025-03-03	[Forstenlechner Installationstechnik]	akira	Link
2025-03-03	[ceratec.com]	abyss	Link
2025-03-02	[Pre Con Industries]	play	Link
2025-03-02	[IT-IQ Botswana]	play	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-02	[North American Fire Hose]	play	Link
2025-03-02	[Couri Insurance Agency]	play	Link
2025-03-02	[Optometrics]	play	Link
2025-03-02	[International Process Plants]	play	Link
2025-03-02	[Ganong Bros]	play	Link
2025-03-02	[FM.GOB.AR]	monti	Link
2025-03-02	[gruppocogesi.org]	lockbit3	Link
2025-03-02	[Bell Ambulance]	medusa	Link
2025-03-02	[Workforce Group]	killsec	Link
2025-03-01	[germancentre.sg]	incransom	Link
2025-03-01	[JEFFREYCOURT.COM]	clop	Link
2025-03-01	[APTEAN.COM]	clop	Link
2025-03-01	[Wayne County, Michigan]	interlock	Link
2025-03-01	[The Smeg Group]	interlock	Link
2025-03-01	[Newton & Associates, Inc]	rhysida	Link

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
- 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

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