Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20250311

Inhaltsverzeichnis

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	0.997970000	Link
CVE-2024-9474	0.974550000	0.999800000	Link
CVE-2024-9465	0.939910000	0.993880000	Link
CVE-2024-9463	0.961860000	0.996710000	Link
CVE-2024-8963	0.966010000	0.997650000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-7593	0.967730000	0.997990000	Link
CVE-2024-6670	0.904230000	0.991220000	Link
CVE-2024-5910	0.967120000	0.997860000	Link
CVE-2024-55956	0.968970000	0.998310000	Link
CVE-2024-53704	0.960740000	0.996530000	Link
CVE-2024-5217	0.945850000	0.994490000	Link
CVE-2024-50623	0.969520000	0.998470000	Link
CVE-2024-50603	0.924330000	0.992560000	Link
CVE-2024-4879	0.950100000	0.995020000	Link
CVE-2024-4577	0.951770000	0.995220000	Link
CVE-2024-4358	0.921450000	0.992370000	Link
CVE-2024-41713	0.955390000	0.995680000	Link
CVE-2024-40711	0.964240000	0.997240000	Link
CVE-2024-4040	0.967700000	0.997980000	Link
CVE-2024-38856	0.941790000	0.994050000	Link
CVE-2024-36401	0.961880000	0.996720000	Link
CVE-2024-3400	0.958850000	0.996200000	Link
CVE-2024-3273	0.937240000	0.993630000	Link
CVE-2024-32113	0.938440000	0.993730000	Link
CVE-2024-28995	0.970760000	0.998800000	Link
CVE-2024-28987	0.957000000	0.995900000	Link
CVE-2024-27348	0.960910000	0.996550000	Link
CVE-2024-27198	0.970470000	0.998720000	Link
CVE-2024-24919	0.963920000	0.997140000	Link
CVE-2024-23897	0.973580000	0.999570000	Link
CVE-2024-2389	0.928740000	0.992870000	Link
CVE-2024-23692	0.967310000	0.997910000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-21893	0.960410000	0.996460000	Link
CVE-2024-21887	0.973690000	0.999600000	Link
CVE-2024-20767	0.964870000	0.997370000	Link
CVE-2024-1709	0.957060000	0.995920000	Link
CVE-2024-1212	0.946600000	0.994580000	Link
CVE-2024-0986	0.954890000	0.995610000	Link
CVE-2024-0195	0.962680000	0.996900000	Link
CVE-2024-0012	0.969610000	0.998490000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Mon, 10 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

—

Mon, 10 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

—

Mon, 10 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

—

Mon, 10 Mar 2025

[NEU] [hoch] Apache OFBiz: Schwachstelle ermöglicht Codeausführung

Ein Angreifer kann eine Schwachstelle in Apache OFBiz ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Mon, 10 Mar 2025

[NEU] [hoch] QNAP NAS (QuLog Center, QTS, QuTS hero): Mehrere Schwachstellen

Ein entfernter anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in QNAP NAS ausnutzen, um Informationen preiszugeben, Daten zu verändern, beliebigen Code auszuführen und möglicherweise einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Mon, 10 Mar 2025

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

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um einen Spoofing-Angriff durchzuführen, beliebigen Code auszuführen, Dateien zu manipulieren, vertrauliche Informationen offenzulegen oder Cross-Site-Scripting-Angriffe durchzuführen.

- Link

—

Mon, 10 Mar 2025

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Mozilla Thunderbird ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsmaßnahmen zu umgehen, Daten zu manipulieren, einen Denial-of-Service-Zustand zu erzeugen und vertrauliche Informationen preiszugeben.

- Link

—

Mon, 10 Mar 2025

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen preiszugeben oder einen Cross-Site-Scripting-Angriff durchzuführen.

- Link

—

Mon, 10 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

—

Mon, 10 Mar 2025

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Firefox ESR und Thunderbird ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, vertrauliche Informationen preiszugeben, Sicherheitsmaßnahmen zu umgehen oder Spoofing-Angriffe durchzuführen.

- Link

—

Mon, 10 Mar 2025

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

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

- Link

—

Mon, 10 Mar 2025

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen preiszugeben, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu erzeugen oder Spoofing-Angriffe durchzuführen.

- Link

—

Mon, 10 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

—

Mon, 10 Mar 2025

[UPDATE] [hoch] OpenSSH: Mehrere Schwachstellen

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

- Link

—

Mon, 10 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

—

Mon, 10 Mar 2025

[UPDATE] [hoch] Google Chrome / Microsoft Edge: Mehrere Schwachstellen ermöglichen Denial of Service

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome / Microsoft Edge ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Fri, 07 Mar 2025

[UPDATE] [hoch] Google Chrome / Microsoft Edge: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome / Microsoft Edge ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- Link

—

Fri, 07 Mar 2025

[UPDATE] [hoch] Kibana: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Fri, 07 Mar 2025

[NEU] [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

—

Fri, 07 Mar 2025

[UPDATE] [hoch] Ansible: Mehrere Schwachstellen ermöglichen Ausführen von beliebigem Programmcode

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Ansible ausnutzen, um

beliebigen Programmcode auszuführen.
- Link
—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
3/10/2025	[Apache Tomcat 9.0.0.M1 < 9.0.99]	critical
3/10/2025	[Apache Tomcat 10.1.0.M1 < 10.1.35]	critical
3/10/2025	[Apache Tomcat 11.0.0.M1 < 11.0.3]	critical
3/10/2025	[Debian dla-4079 : openvpn - security update]	critical
3/10/2025	[Google Chrome < 134.0.6998.88 Multiple Vulnerabilities]	critical
3/10/2025	[Google Chrome < 134.0.6998.89 Multiple Vulnerabilities]	critical
3/10/2025	[Google Chrome < 134.0.6998.89 Multiple Vulnerabilities]	critical
3/10/2025	[Google Chrome < 134.0.6998.88 Multiple Vulnerabilities]	critical
3/10/2025	[RHEL 9 : firefox (RHSA-2025:2359)]	critical
3/10/2025	[RHEL 8 : firefox (RHSA-2025:2452)]	critical
3/10/2025	[Debian dsa-5876 : thunderbird - security update]	critical
3/10/2025	[FreeBSD : electron33 – multiple vulnerabilities (6ba9e26e-c9c6-49f7-ae43-47e5864f0b66)]	critical
3/10/2025	[Debian dla-4081 : thunderbird - security update]	critical
3/10/2025	[CBL Mariner 2.0 Security Update: kernel (CVE-2024-56603)]	high
3/10/2025	[CBL Mariner 2.0 Security Update: kernel (CVE-2024-56581)]	high
3/10/2025	[Azure Linux 3.0 Security Update: kernel (CVE-2024-56704)]	high
3/10/2025	[CBL Mariner 2.0 Security Update: kernel (CVE-2024-56627)]	high
3/10/2025	[Azure Linux 3.0 Security Update: kernel (CVE-2024-56581)]	high
3/10/2025	[CBL Mariner 2.0 Security Update: kernel (CVE-2024-56640)]	high

Datum	Schwachstelle	Bewertung
3/10/2025	[Fedora 40 : python-spotipy (2025-2215919645)]	high
3/10/2025	[Fedora 40 : chromium (2025-762804f16e)]	high
3/10/2025	[Fedora 41 : python-spotipy (2025-fba1b24e4b)]	high
3/10/2025	[Fedora 40 : vim (2025-6452f3da4b)]	high
3/10/2025	[openSUSE 15 Security Update : chromium (openSUSE-SU-2025:0084-1)]	high
3/10/2025	[Fedora 41 : chromium (2025-e94782e579)]	high
3/10/2025	[Fedora 41 : qt6-qtwebengine (2025-c858874183)]	high
3/10/2025	[Fedora 40 : podman-tui (2025-dcf429359c)]	high
3/10/2025	[Fedora 41 : podman-tui (2025-736781dc2a)]	high
3/10/2025	[Fedora 41 : buildah (2025-f7524afa1f)]	high
3/10/2025	[RHEL 7 : kernel-aarch64 (RHSA-2017:0372)]	high
3/10/2025	[Ubuntu 16.04 LTS / 18.04 LTS : X.Org X Server vulnerabilities (USN-7299-2)]	high
3/10/2025	[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : LibreOffice vulnerability (USN-7337-1)]	high
3/10/2025	[SUSE SLES15 Security Update : buildah (SUSE-SU-2025:0812-1)]	high
3/10/2025	[SUSE SLES15 Security Update : buildah (SUSE-SU-2025:0813-1)]	high
3/10/2025	[SUSE SLES15 / openSUSE 15 Security Update : buildah (SUSE-SU-2025:0811-1)]	high
3/10/2025	[Debian dla-4080 : libaws-bin - security update]	high
3/10/2025	[Oracle Linux 9 : tigervnc (ELSA-2025-2500)]	high

4 Die Hacks der Woche

mit Martin Haunschmid

4.0.1 Private video

Vorschaubild Zum Youtube Video

5 Cyberangriffe: (Mär)

Datum	Opfer	Land	Information
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
2025-03-02	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

6 Ransomware-Erpressungen: (Mär)

Datum	Opfer	Ransomware-Grupppe	Webseite
2025-03-11	[isee-eg.com]	funksec	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2025-03-11	[fnde.gov.br brazilian government]	babuk2	Link
2025-03-11	[wapda.gov.pk By Babuk Locker 2.0]	babuk2	Link
2025-03-11	[lexmark.com Company]	babuk2	Link
2025-03-10	[Wilkinson Rogers (wilkinsonrogers.com)]	fog	Link
2025-03-11	[forvismazars.com.fr (mazars.fr) By Babuk Locker 2.0]	babuk2	Link
2025-03-10	[Magnolia Manor (magnoliamanor.com)]	fog	Link
2025-03-10	[petstop.com Company]	babuk2	Link
2025-03-10	[misaludhealth.com By Babuk Locker 2.0]	babuk2	Link
2025-03-10	[bank.pingan.com (CN) By Babuk Locker 2.0]	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 By Babuk Locker 2.0]	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

Datum	Opfer	Ransomware-Grupppe	Webseite
2025-03-04	[Customer Management Systems]	medusa	Link
2025-03-06	[CPI Books]	medusa	Link
2025-03-09	[ACTi Corporation]	lynx	Link
2025-03-09	[emperors.edu]	incransom	Link
2025-03-09	[wog-kaiserbaeder.de]	incransom	Link
2025-03-09	[BerksBar.org]	incransom	Link
2025-03-09	[williampevear.com]	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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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
2025-03-04	[www.cdg.us]	qilin	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	[ACDC Express]	lynx	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
2025-03-06	[Tugwell Pump & Supply]	lynx	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
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	[Dynamic Closures]	lynx	Link
2025-03-06	[Naples Heritage Golf & Country Club]	incransom	Link
2025-03-06	[Ministry of Foreign Affairs of Ukraine]	qilin	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
2025-03-04	[FANTIN group]	akira	Link
2025-03-04	[Grupo Baston Aerossol (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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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.