

Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20250203



Inhaltsverzeichnis

1 Editorial	2
2 Security-News	3
2.1 Heise - Security-Alert	3
3 Sicherheitslücken	4
3.1 EPSS	4
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit	5
3.2 BSI - Warn- und Informationsdienst (WID)	5
3.3 Sicherheitslücken Meldungen von Tenable	8
4 Die Hacks der Woche	10
4.0.1 Riskanter Tippfehler bei Mastercard	11
5 Cyberangriffe: (Feb)	12
6 Ransomware-Erpressungen: (Feb)	12
7 Quellen	13
7.1 Quellenverzeichnis	13
8 Impressum	14

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

SimpleHelp RMM: Angriffe auf Sicherheitslücken beobachtet

In SimpleHelp RMM missbrauchen Angreifer Sicherheitslücken, um Netzwerke zu kompromittieren. Updates stehen bereit.

- [Link](#)

Schadcode-Schlupfloch in Dell NetWorker geschlossen

Angreifer können an mehreren Sicherheitslücken in Dells Backuplösung NetWorker ansetzen. Sicherheitsupdates stehen zum Download bereit.

- [Link](#)

Zoho ManageEngine Applications Manager: Sicherheitslücke verschafft Admin-Rechte

Zohocorp warnt vor einer Schwachstelle in ManageEngine Applications Manager. Angreifer können sich Admin-Rechte verschaffen.

- [Link](#)

VMware Aria Operations: Angreifer können Zugangsdaten auslesen

Broadcom warnt vor Sicherheitslücken in VMware Aria Operations, durch die Angreifer etwa Zugangsdaten ausspähen können. Updates stehen bereit.

- [Link](#)

Warten auf Patch: Das Admin-Interface Voyager für Laravel-Apps ist verwundbar

Sicherheitsforscher warnen vor möglichen Attacken auf Voyager. Bislang haben sich die Entwickler zu den Sicherheitslücken nicht geäußert.

- [Link](#)

Mirai-Botnetz: Angreifer attackieren Zyxel-Router und Mitel-SIP-Phones

Derzeit attackieren Angreifer Geräte von Mitel und Zyxel. Für betroffenen Zyxel-Router gibt es bislang kein Sicherheitsupdate.

- [Link](#)

Angreifer können Dell Enterprise Sonic Distribution kompromittieren

In Dells Enterprise Sonic Distribution können Angreifer eine Sicherheitslücke missbrauchen, um Geräte zu kompromittieren.

- [Link](#)

VMware: Hochriskante SQL-Injection-Lücke gefährdet Avi Load Balancer

Broadcom warnt vor einer SQL-Injection-Lücke in VMware Avi Load Balancer. Angreifer können unbefugt auf die Datenbank zugreifen.

- [Link](#)

Industrielle Kontrollsysteme: Attacken auf kritische Infrastrukturen möglich

Es sind wichtige Sicherheitsupdates für industriellen Steuerungssysteme von unter anderem Rockwell und Schneider erschienen.

- [Link](#)

Teamviewer: Sicherheitsleck ermöglicht Angreifern die Ausweitung ihrer Rechte

Teamviewer warnt vor einer Schwachstelle in den Windows-Versionen der Fernwartungssoftware, die Angreifern die Rechteauserweiterung ermöglicht.

- [Link](#)

3 Sicherheitslücken

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

3.1 EPSS

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

Es soll Unternehmen dabei helfen, ihre Ressourcen effizienter zu verteilen und alle relevanten Cyber-Risiken zu minimieren.

3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
-----	------	-----------	-----------------------

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 31 Jan 2025

[NEU] [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, 31 Jan 2025

[UPDATE] [hoch] Red Hat Enterprise Linux und 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](#)

—

Fri, 31 Jan 2025

[UPDATE] [hoch] PHP: Schwachstelle ermöglicht Offenlegung von Informationen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in PHP ausnutzen, um Informationen offenzulegen.

- [Link](#)

—

Fri, 31 Jan 2025

[NEU] [hoch] Rockwell Automation FactoryTalk AssetCentre: Mehrere Schwachstellen ermöglichen Erlangen von Benutzerrechten

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Rockwell Automation FactoryTalk AssetCentre ausnutzen, um Benutzerrechte zu erlangen.

- [Link](#)

—
Fri, 31 Jan 2025

[UPDATE] [hoch] Oracle Java SE: Mehrere Schwachstellen

Ein entfernter, anonymes Angreifer kann mehrere Schwachstellen in Oracle Java SE ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- [Link](#)

—
Fri, 31 Jan 2025

[NEU] [hoch] VMware Aria Operations, VMware Aria Operations for Logs und VMware Cloud Foundation:: Mehrere Schwachstellen

Ein entfernter authentisierter Angreifer kann mehrere Schwachstellen in VMware Aria Operations for Logs, VMware Aria Operations und VMware Cloud Foundation ausnutzen, um Informationen preiszugeben, erhöhte Berechtigungen zu erlangen und einen Cross-Site-Scripting-Angriff durchzuführen.

- [Link](#)

—
Fri, 31 Jan 2025

[UPDATE] [hoch] IBM QRadar SIEM: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in IBM QRadar SIEM ausnutzen, um seine Privilegien zu erweitern, Administratorrechte zu erlangen, beliebigen Programmcode auszuführen, Informationen offenzulegen, Dateien zu manipulieren oder Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—
Fri, 31 Jan 2025

[UPDATE] [hoch] Python: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Python ausnutzen, um einen Denial of Service Angriff durchzuführen und Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

—
Fri, 31 Jan 2025

[UPDATE] [hoch] Red Hat Enterprise Linux: Schwachstelle in unbound

Ein entfernter, anonymes Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um eine laufende Instanz zu manipulieren, Informationen offenzulegen oder einen Denial-of-Service auszulösen.

- [Link](#)

—
Fri, 31 Jan 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](#)

—

Fri, 31 Jan 2025

[UPDATE] [hoch] Oracle MySQL: Mehrere Schwachstellen

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

- [Link](#)

—

Fri, 31 Jan 2025

[UPDATE] [hoch] Red Hat Enterprise Linux (git-lfs): Schwachstelle ermöglicht Erlangen von Benutzerrechten

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux bezüglich git-lfs ausnutzen, um Benutzerrechte zu erlangen.

- [Link](#)

—

Fri, 31 Jan 2025

[UPDATE] [hoch] Vaultwarden: Mehrere Schwachstellen

Ein entfernter, anonymer oder authentifizierter Angreifer kann mehrere Schwachstellen in Vaultwarden ausnutzen, um Dateien zu manipulieren, beliebigen Code auszuführen und sich erhöhte Rechte zu verschaffen.

- [Link](#)

—

Fri, 31 Jan 2025

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

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

- [Link](#)

—

Fri, 31 Jan 2025

[UPDATE] [hoch] Apple macOS, iPadOS und iOS: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Apple macOS, Apple iPadOS und Apple iOS ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, beliebigen Code auszuführen, sensible Daten offenzulegen, Dateien zu manipulieren, erhöhte Rechte zu erlangen - einschließlich Root-Rechte, Sicherheitsmaßnahmen zu umgehen und einen Spoofing-Angriff zu starten.

- [Link](#)

—

Fri, 31 Jan 2025

[UPDATE] [hoch] Google Chrome/ Microsoft Edge: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Google Chrome/ Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 31 Jan 2025

[NEU] [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, 30 Jan 2025

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

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

- [Link](#)

—

Thu, 30 Jan 2025

[UPDATE] [hoch] Oracle MySQL: Mehrere Schwachstellen

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

- [Link](#)

—

Thu, 30 Jan 2025

[NEU] [hoch] Microsoft GitHub Enterprise: Schwachstelle ermöglicht Offenlegung von Informationen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Microsoft GitHub Enterprise ausnutzen, um Informationen offenzulegen.

- [Link](#)

—

3.3 Sicherheitslücken Meldungen von Tenable

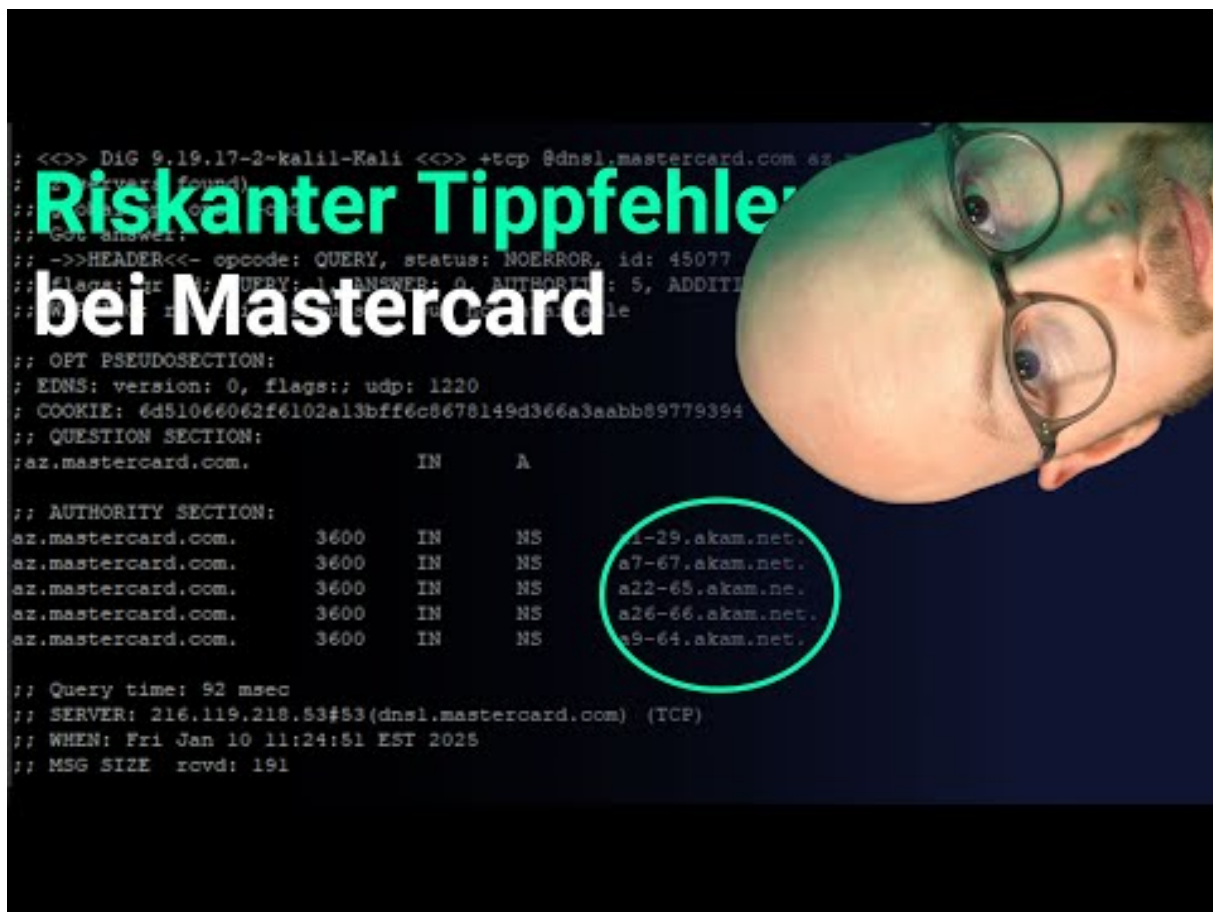
Datum	Schwachstelle	Bewertung
2/1/2025	[Debian dla-4039 : ffmpeg - security update]	critical
1/31/2025	[ServiceNow Platform Input Validation (CVE-2024-4879) (Direct Check)]	critical
1/30/2025	[Wiesemann & Theis ComServer Series Missing Authentication for Critical Function (CVE-2022-42785)]	critical
2/2/2025	[FreeBSD : qt6-webengine – Multiple vulnerabilities (72b8729e-e134-11ef-9e76-4ccc6adda413)]	high
2/1/2025	[Fedora 41 : nodejs20 (2025-76fc32d433)]	high
2/1/2025	[Fedora 41 : rust-routinator (2025-bbabead4d7)]	high
2/1/2025	[CBL Mariner 2.0 Security Update: libxml2 (CVE-2022-49043)]	high
2/1/2025	[CBL Mariner 2.0 Security Update: git-lfs (CVE-2024-53263)]	high
2/1/2025	[Fedora 40 : chromium (2025-82ba6b8dc5)]	high
2/1/2025	[Fedora 41 : jpegxl (2025-6e4727185c)]	high
2/1/2025	[Fedora 40 : nodejs20 (2025-54958ff9e2)]	high
2/1/2025	[IBM WebSphere Application Server Liberty 20.0.0.12 < 24.0.0.11 DoS (7173097)]	high
1/31/2025	[Fedora 41 : java-21-openjdk (2025-9f92cbc27f)]	high
1/31/2025	[Fedora 40 : expat (2024-2462a2fc4c)]	high
1/31/2025	[JetBrains Rider 2024.1.x < 2024.1.7 / 2024.2.x < 2024.2.8 / 2024.3.x < 2024.3.4 Local Privilege Escalation (CVE-2025-23385)]	high
1/31/2025	[Security Updates for Microsoft Excel Products C2R (January 2025)]	high
1/31/2025	[Security Updates for Microsoft Word Products C2R (January 2025)]	high
1/31/2025	[Security Updates for Microsoft Access Products C2R (January 2025)]	high
1/31/2025	[Security Updates for Microsoft Office Products C2R (January 2024)]	high

Datum	Schwachstelle	Bewertung
1/31/2025	[Security Updates for Microsoft Visio Products C2R (January 2025)]	high
1/31/2025	[FreeBSD : chromium – multiple security fixes (186101b4-dfa6-11ef-8c1c-a8a1599412c6)]	high
1/31/2025	[AlmaLinux 8 : git-lfs (ALSA-2025:0845)]	high
1/31/2025	[AlmaLinux 8 : unbound (ALSA-2025:0837)]	high
1/31/2025	[AlmaLinux 8 : libsoup (ALSA-2025:0838)]	high
1/31/2025	[Debian dla-4038 : dcmthk - security update]	high
1/30/2025	[Ubuntu 24.10 : Linux kernel (Oracle) vulnerabilities (USN-7238-2)]	high
1/30/2025	[Ubuntu 20.04 LTS : Linux kernel (Azure) Unknown kernel vulnerabilities (USN-7235-2)]	high
1/30/2025	[Ubuntu 18.04 LTS : Linux kernel (HWE) vulnerabilities (USN-7234-2)]	high
1/30/2025	[Ubuntu 14.04 LTS / 18.04 LTS : Linux kernel (Azure) vulnerabilities (USN-7233-2)]	high
1/30/2025	[Debian dla-4036 : debian-security-support - security update]	high
1/30/2025	[Debian dsa-5856 : redis - security update]	high
1/30/2025	[Wiesemann & Theis ComServer Use of Insufficiently Random Values (CVE-2022-42787)]	high
1/30/2025	[Wiesemann & Theis ComServer Series Authentication Bypass by Spoofing (CVE-2022-4098)]	high
1/30/2025	[Ubiquiti Networks UniFi Improper Access Control (CVE-2016-7792)]	high

4 Die Hacks der Woche

mit Martin Haunschmid

4.0.1 Riskanter Tippfehler bei Mastercard



[Zum Youtube Video](#)

5 Cyberangriffe: (Feb)

Datum	Opfer	Land	Information
2025-02-02	Top-Medien	[CHE]	Link

6 Ransomware-Erpressungen: (Feb)

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-03	[Pineland community service board]	spacebears	Link
2025-02-02	[usuhs.edu]	lockbit3	Link
2025-02-02	[Four Eye Clinics]	abyss	Link
2025-02-02	[jpcgroupinc.com]	abyss	Link
2025-02-02	[hreu.eu]	funksec	Link
2025-02-02	[Tosaf]	handala	Link
2025-02-02	[turbomp]	stormous	Link
2025-02-02	[Cyrious Software]	bianlian	Link
2025-02-02	[Medical Associates of Brevard]	bianlian	Link
2025-02-02	[Civic Committee]	bianlian	Link
2025-02-02	[Ayres Law Firm]	bianlian	Link
2025-02-02	[Growth Acceleration Partners]	bianlian	Link
2025-02-01	[fiberskynet.net]	funksec	Link
2025-02-01	[tirtaraharja.co.id]	funksec	Link
2025-02-01	[Gitlabs: PT. ITPRENEUR INDONESIA TECHNOLOGY, GFZ Helmholtz Centre for Geosciences, LUA Cof...]	fog	Link
2025-02-01	[myisp.live]	funksec	Link
2025-02-01	[Zamzow's]	lynx	Link
2025-02-01	[DATACONSULTANTS.COM]	clap	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-01	[CHAMPIONHOMES.COM]	clon	Link
2025-02-01	[CIERANT.COM]	clon	Link
2025-02-01	[DATATRAC.COM]	clon	Link
2025-02-01	[Nano Health]	killsec	Link
2025-02-01	[St. Nicholas School]	8base	Link
2025-02-01	[Héron]	8base	Link
2025-02-01	[Tan Teck Seng Electric (Co) Pte Ltd]	8base	Link
2025-02-01	[High Learn Ltd]	8base	Link
2025-02-01	[CAMRIDGEPORT]	spacebears	Link
2025-02-01	[Falcon Gaming]	arcusmedia	Link
2025-02-01	[Eascon]	arcusmedia	Link
2025-02-01	[Utilissimo Transportes]	arcusmedia	Link
2025-02-01	[GATTELLI SpA]	arcusmedia	Link
2025-02-01	[Technico]	arcusmedia	Link
2025-02-01	[Wireless Solutions (Morris.Domain)]	lynx	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.