
Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20250219



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)	6
3.3 Sicherheitslücken Meldungen von Tenable	10
4 Die Hacks der Woche	12
4.0.1 Alte S3-Buckets ausgraben, Sachen hacken ☒	12
5 Cyberangriffe: (Feb)	13
6 Ransomware-Erpressungen: (Feb)	14
7 Quellen	33
7.1 Quellenverzeichnis	33
8 Impressum	34

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

Sicherheitsupdates Dell: BIOS- und NetWorker-Lücke geschlossen

Angrifer können Dell-PCs und -Software attackieren. Es kann Schadcode auf Geräte gelangen. Einer der Patches ist aber bislang nicht verfügbar.

- [Link](#)

—

Xerox Versalink: Multifunktionsdrucker geben Zugangsdaten preis

In den Versalink-Multifunktionsdruckern von Xerox wurden Schwachstellen entdeckt, durch die Angreifer Zugangsdaten abgreifen können.

- [Link](#)

—

Brocade SANnav: Angreifer können Zugangsdaten durch Sicherheitslecks erlangen

Broadcom warnt vor Sicherheitslücken in Brocade SANnav, durch die Angreifer unbefugt Zugang erlangen können. Aktualisierte Software schließt sie.

- [Link](#)

—

Winzip: Angreifer können durch Sicherheitsleck Schadcode einschleusen

Eine Schwachstelle in Winzip ermöglicht Angreifern, mit manipulierten Archiven beliebigen Code einzuschleusen. Ein Update korrigiert das.

- [Link](#)

—

HP-Laserdrucker ermöglichen Codeschmuggel durch Postscript-Sicherheitsleck

In zahlreichen HP-Laserdruckern können Angreifer eine Lücke beim Verarbeiten von Postscript zum Einschleusen von Schadcode missbrauchen.

- [Link](#)

—

Angriffe auf Sicherheitslücken in iOS, iPadOS, Mitel SIP-Phones und PAN-OS

IT-Forscher haben Angriffe auf Sicherheitslücken in iPadOS, Mitel SIP-Phones und PAN-OS beobachtet. Updates dichten die Sicherheitslecks ab.

- [Link](#)

—

Jetzt patchen! Angreifer kapern VPN-Verbindungen von Sonicwall-Firewalls

Derzeit finden Attacken auf Firewalls von Sonicwall statt. Sicherheitsupdates stehen zum Download bereit.

- [Link](#)

Palo Alto PAN-OS: Exploit-Code für hochriskante Lücke aufgetaucht

Im Betriebssystem PAN-OS für Firewalls von Palo Alto Networks klaffen Sicherheitslücken. Für eine davon gibt es bereits Exploit-Code.

- [Link](#)

Sicherheitslücke: Attacken auf PostgreSQL-Clients möglich

Ein Patch schließt eine Schadcode-Lücke, die unter bestimmten Voraussetzungen für Clients mit Zugriff auf PostgreSQL-Datenbanken gefährlich werden kann.

- [Link](#)

Progress Telerik und Loadmaster: Updates dichten Sicherheitslecks ab

In Loadmaster und Telerik von Progress hat der Hersteller hochriskante Schwachstellen entdeckt. Updates bessern sie aus.

- [Link](#)

3 Sicherheitslücken

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

3.1 EPSS

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

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

3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-9474	0.974800000	0.999850000	Link
CVE-2024-9465	0.943220000	0.994130000	Link
CVE-2024-9463	0.961860000	0.996700000	Link
CVE-2024-8963	0.967240000	0.997860000	Link
CVE-2024-7593	0.971450000	0.998980000	Link
CVE-2024-6893	0.938390000	0.993670000	Link
CVE-2024-6670	0.904230000	0.991090000	Link
CVE-2024-5910	0.962860000	0.996920000	Link
CVE-2024-55956	0.968970000	0.998290000	Link
CVE-2024-5217	0.930570000	0.992920000	Link
CVE-2024-50623	0.969520000	0.998430000	Link
CVE-2024-50603	0.924330000	0.992450000	Link
CVE-2024-4879	0.936740000	0.993500000	Link
CVE-2024-4577	0.958420000	0.996120000	Link
CVE-2024-4358	0.921450000	0.992290000	Link
CVE-2024-41713	0.957210000	0.995900000	Link
CVE-2024-40711	0.964240000	0.997220000	Link
CVE-2024-4040	0.969230000	0.998350000	Link
CVE-2024-38856	0.939580000	0.993800000	Link
CVE-2024-36401	0.961880000	0.996710000	Link
CVE-2024-3400	0.962560000	0.996840000	Link
CVE-2024-3273	0.937410000	0.993580000	Link
CVE-2024-32113	0.933050000	0.993170000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-28995	0.969950000	0.998540000	Link
CVE-2024-28987	0.961930000	0.996720000	Link
CVE-2024-27348	0.960030000	0.996380000	Link
CVE-2024-27198	0.969340000	0.998380000	Link
CVE-2024-24919	0.963920000	0.997130000	Link
CVE-2024-23897	0.973540000	0.999550000	Link
CVE-2024-2389	0.900180000	0.990820000	Link
CVE-2024-23692	0.964390000	0.997270000	Link
CVE-2024-21893	0.956970000	0.995850000	Link
CVE-2024-21887	0.973220000	0.999490000	Link
CVE-2024-20767	0.964870000	0.997340000	Link
CVE-2024-1709	0.957220000	0.995900000	Link
CVE-2024-1212	0.937140000	0.993550000	Link
CVE-2024-0986	0.955530000	0.995670000	Link
CVE-2024-0195	0.962680000	0.996870000	Link
CVE-2024-0012	0.969980000	0.998550000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Tue, 18 Feb 2025

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

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

- [Link](#)

—

Tue, 18 Feb 2025

[UPDATE] [hoch] PaloAlto Networks PAN-OS: Mehrere Schwachstellen

Ein entfernter anonymen oder authentisierter Angreifer kann mehrere Schwachstellen in PaloAlto

Networks PAN-OS ausnutzen, um Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen preiszugeben, Daten zu manipulieren und beliebigen Code auszuführen.

- [Link](#)

—

Tue, 18 Feb 2025

[NEU] [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](#)

—

Tue, 18 Feb 2025

[UPDATE] [hoch] docker: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in docker ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Tue, 18 Feb 2025

[NEU] [hoch] Dell NetWorker "Management Console": Schwachstelle ermöglicht Codeausführung

Ein anonymer Angreifer kann eine Schwachstelle in Dell NetWorker "Management Console" ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Tue, 18 Feb 2025

[NEU] [hoch] Juniper Session Smart Router: Schwachstelle ermöglicht Erlangen von Administratorrechten

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Juniper Session Smart Router ausnutzen, um Administratorrechte zu erlangen.

- [Link](#)

—

Tue, 18 Feb 2025

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

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

- [Link](#)

—

Tue, 18 Feb 2025

[UPDATE] [hoch] Node.js: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen preiszugeben, einen Denial-of-Service-Zustand herbeizuführen oder nicht näher spezifizierte Angriffe zu starten.

- [Link](#)

—

Tue, 18 Feb 2025

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

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

- [Link](#)

—

Tue, 18 Feb 2025

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

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

- [Link](#)

—

Tue, 18 Feb 2025

[UPDATE] [hoch] Red Hat Enterprise Linux (Fast Datapath): Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Tue, 18 Feb 2025

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode mit Administratorrechten

Ein lokaler Angreifer kann eine Schwachstelle im Kernel von Fedora Linux ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen.

- [Link](#)

—

Tue, 18 Feb 2025

[NEU] [hoch] Moodle: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Moodle ausnutzen, um SQL-Injection- und Cross-Site-Scripting-Angriffe durchzuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen preiszugeben oder andere nicht näher spezifizierte Auswirkungen zu verursachen.

- [Link](#)

—

Tue, 18 Feb 2025

[NEU] [hoch] Dell BIOS (Client Platform): Schwachstelle ermöglicht Privilegieneskalation

Ein lokaler Angreifer kann eine Schwachstelle in Dell BIOS ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Mon, 17 Feb 2025

[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um Sicherheitsvorkehrungen zu umgehen und um Dateien zu manipulieren.

- [Link](#)

—

Mon, 17 Feb 2025

[NEU] [hoch] HP LaserJet: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in HP LaserJet ausnutzen, um beliebigen Programmcode auszuführen, seine Rechte zu erweitern, oder einen DoS auszuführen.

- [Link](#)

—

Mon, 17 Feb 2025

[UPDATE] [hoch] IEEE WPA2: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in IEEE WPA2 ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Mon, 17 Feb 2025

[UPDATE] [hoch] AMD Prozessoren: Mehrere Schwachstellen ermöglichen Offenlegung von Informationen

Ein Angreifer kann mehrere Schwachstellen im AMD Prozessoren ausnutzen, um Informationen offenzulegen.

- [Link](#)

—

Mon, 17 Feb 2025

[UPDATE] [hoch] AMD Prozessoren: Mehrere Schwachstellen

Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in AMD Prozessoren ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen und Daten zu manipulieren.

- [Link](#)

Mon, 17 Feb 2025

[UPDATE] [hoch] Ruby: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Ruby ausnutzen, um einen Denial of Service Angriff durchzuführen, einen Cross-Site-Scripting-Angriff durchzuführen oder beliebigen Programmcode auszuführen.

- [Link](#)

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
2/18/2025	[Debian dla-4058 : libpam-pkcs11 - security update]	critical
2/18/2025	[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : Docker vulnerabilities (USN-7161-2)]	critical
2/18/2025	[Mozilla Firefox < 135.0.1]	critical
2/18/2025	[Mozilla Firefox < 135.0.1]	critical
2/18/2025	[Google Chrome < 133.0.6943.126 Multiple Vulnerabilities]	critical
2/18/2025	[Google Chrome < 133.0.6943.126 Multiple Vulnerabilities]	critical
2/18/2025	[RHEL 8 : bzip2 (RHSA-2025:0733)]	critical
2/17/2025	[Automated Logic WebCTRL Premium Server Unrestricted Upload of File with Dangerous Type (CVE-2024-8525)]	critical
2/17/2025	[Automated Logic WebCTRL Premium Server Unrestricted Upload of File with Dangerous Type (CVE-2024-8525)]	critical
2/17/2025	[Automated Logic WebCTRL Premium Server Unrestricted Upload of File with Dangerous Type (CVE-2024-8525)]	critical
2/18/2025	[RHEL 8 : redhat-ds:11 (RHSA-2025:1632)]	high
2/18/2025	[Debian dla-4057 : openssh-client - security update]	high
2/18/2025	[Debian dsa-5868 : openssh-client - security update]	high

Datum	Schwachstelle	Bewertung
2/18/2025	[Cisco IOS Software Intermediate System to Intermediate System DoS (cisco-sa-isis-sGjyOUHX)]	high
2/18/2025	[Cisco IOS XE Software Intermediate System to Intermediate System DoS (cisco-sa-isis-sGjyOUHX)]	high
2/18/2025	[RHEL 9 : Red Hat JBoss Enterprise Application Platform 7.4.21 (RHSA-2025:1638)]	high
2/18/2025	[RHEL 8 : Red Hat JBoss Enterprise Application Platform 7.4.21 (RHSA-2025:1637)]	high
2/18/2025	[RHEL 7 : Red Hat JBoss Enterprise Application Platform 7.4.21 (RHSA-2025:1636)]	high
2/18/2025	[AlmaLinux 8 : nodejs:22 (ALSA-2025:1611)]	high
2/18/2025	[AlmaLinux 9 : nodejs:22 (ALSA-2025:1613)]	high
2/18/2025	[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS / 24.10 : OpenSSH vulnerabilities (USN-7270-1)]	high
2/18/2025	[Ubuntu 14.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS : libsndfile vulnerabilities (USN-7273-1)]	high
2/18/2025	[Ubuntu 20.04 LTS / 22.04 LTS : virtualenv vulnerability (USN-7271-1)]	high
2/18/2025	[Ubuntu 20.04 LTS / 22.04 LTS / 24.04 LTS : Symfony vulnerabilities (USN-7272-1)]	high
2/18/2025	[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS : Atril vulnerabilities (USN-7274-1)]	high
2/18/2025	[RHEL 8 : RHUI 4.11 (RHSA-2025:1335)]	high
2/18/2025	[Siemens SIMATIC S7-1200 CPU Family Improper Resource Shutdown or Release (CVE-2025-24811)]	high
2/18/2025	[Schneider Electric Modicon M340 and BMXNOE0100/0110, BMXNOR0200H Exposure of Sensitive Information to an Unauthorized Actor (CVE-2024-12142)]	high
2/18/2025	[Schneider Electric Modicon M580 PLCs, BMENOR2200H and EVLink Pro AC Incorrect Calculation of Buffer Size (CVE-2024-11425)]	high

Datum	Schwachstelle	Bewertung
2/17/2025	[RHEL 9 : nodejs:22 (RHSA-2025:1613)]	high
2/17/2025	[RHEL 8 : nodejs:22 (RHSA-2025:1611)]	high
2/17/2025	[Schneider Electric PowerLogic HDPM6000 Authorization Bypass Through User-Controlled Key (CVE-2024-10497)]	high

4 Die Hacks der Woche

mit Martin Haunschmid

4.0.1 Alte S3-Buckets ausgraben, Sachen hacken ☒



[Zum Youtube Video](#)

5 Cyberangriffe: (Feb)

Datum	Opfer	Land	Information
2025-02-17	Appomattox County Public Schools	[USA]	Link
2025-02-13	Eckert & Ziegler SE	[DEU]	Link
2025-02-13	Université de la Bundeswehr	[DEU]	Link
2025-02-11	Port of Oostende	[BEL]	Link
2025-02-11	Ville de Tulln	[AUT]	Link
2025-02-11	Alf DaFrè	[ITA]	Link
2025-02-10	LUP-Kliniken	[DEU]	Link
2025-02-10	City of Tarrant	[USA]	Link
2025-02-10	Sault Tribe, Kewadin Casinos	[USA]	Link
2025-02-10	Secrétariat de la Conférence des évêques allemands (Deutsche Bischofskonferenz)	[DEU]	Link
2025-02-09	Williamsburg James City County Public Schools	[USA]	Link
2025-02-08	FORTUNE ELECTRIC CO.,LTD	[TWN]	Link
2025-02-07	Transcend Information, Inc.	[TWN]	Link
2025-02-07	Rainbow District School Board	[CAN]	Link
2025-02-05	IMI	[GBR]	Link
2025-02-05	REMSA Health	[USA]	Link
2025-02-04	Pinehurst Radiology	[USA]	Link
2025-02-03	Lee Enterprises	[USA]	Link
2025-02-02	Top-Medien	[CHE]	Link
2025-02-02	Mayer Steel Pipe Corporation	[TWN]	Link
2025-02-02	Nan Ya PCB (KunShan) Corp.	[TWN]	Link
2025-02-02	Université des Bahamas	[BHS]	Link
2025-02-01	CESI	[FRA]	Link

6 Ransomware-Erpressungen: (Feb)

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-19	[BeniPlus]	killsec	Link
2025-02-19	[Brolly]	killsec	Link
2025-02-19	[Help Me Grow Yolo]	killsec	Link
2025-02-19	[NimuSoft]	killsec	Link
2025-02-18	[footballticketnet.com]	funksec	Link
2025-02-18	[uniekinc.com]	cactus	Link
2025-02-18	[midwayimporting.com]	cactus	Link
2025-02-18	[revitalash.com]	cactus	Link
2025-02-18	[bestbrands.com]	cactus	Link
2025-02-07	[autogedal.ro]	apt73	Link
2025-02-18	[www.mwmechanicalinc.com]	ransomhub	Link
2025-02-18	[www.alphamedctr.com]	ransomhub	Link
2025-02-18	[www.ccttechnologies.com]	ransomhub	Link
2025-02-18	[www.copleystoughton.com]	ransomhub	Link
2025-02-18	[www.macmed.com]	ransomhub	Link
2025-02-18	[Decore-Ative Specialties]	akira	Link
2025-02-18	[Daniels Homes]	akira	Link
2025-02-18	[PREMIER HOUSEWARES LIMITED]	akira	Link
2025-02-18	[ranhillbersekutu.com.my]	lynx	Link
2025-02-18	[lavi.co.il]	incransom	Link
2025-02-18	[pyasolutions.com]	incransom	Link
2025-02-18	[Buanderie Centrale de Montreal]	rhysida	Link
2025-02-14	[myhscu.com]	embargo	Link
2025-02-17	[www.macter.com]	ransomhub	Link
2025-02-17	[Cuna Supply]	play	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-17	[The Townsley Law Firm Information]	play	Link
2025-02-17	[Bushmans]	play	Link
2025-02-17	[Inland Empire Distribution Systems, Inc.]	play	Link
2025-02-17	[Wylie Steel Fabricators]	play	Link
2025-02-17	[Oxford Companies]	play	Link
2025-02-17	[Stage 3 Separation]	play	Link
2025-02-17	[Transkid]	play	Link
2025-02-17	[Rheinischer Sch]	play	Link
2025-02-17	[Startek Peglar & Calcagni]	play	Link
2025-02-17	[Weed Man Canada]	play	Link
2025-02-17	[Bulldog Oilfield Services]	play	Link
2025-02-17	[danecourt.kent.sch.uk]	kairos	Link
2025-02-17	[toitiusa.com]	kairos	Link
2025-02-17	[lekiaviation.com]	ransomhub	Link
2025-02-17	[bisindustries.com]	ransomhub	Link
2025-02-17	[kinseysinc.com]	cactus	Link
2025-02-17	[steelerubber.com]	cactus	Link
2025-02-17	[almostfamousclothing.com]	cactus	Link
2025-02-17	[teamwass.com]	cactus	Link
2025-02-17	[ssmcoop.com]	cactus	Link
2025-02-17	[hiway.com.br]	funksec	Link
2025-02-17	[Thong Sia]	akira	Link
2025-02-17	[Swissmem]	hunters	Link
2025-02-17	[Bulverde Glass, Inc.]	qilin	Link
2025-02-17	[Hisingstads Bleck]	lynx	Link
2025-02-17	[Leadership Strategies]	lynx	Link
2025-02-17	[LINTEC & LINNHOF Holdings]	lynx	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-17	[HRS_IDEA_Expertises]	lynx	Link
2025-02-17	[Autoschade Pippel]	lynx	Link
2025-02-17	[Pedensia Graphics Distribution]	lynx	Link
2025-02-17	[Winbas]	lynx	Link
2025-02-17	[hamton]	lynx	Link
2025-02-17	[Greencastle-Antrim Senior High School (gcsd.org)]	fog	Link
2025-02-17	[Woman's Athletic Club of Chicago]	akira	Link
2025-02-17	[P.N. Sakkoulas]	akira	Link
2025-02-17	[Allied Tenesis]	lynx	Link
2025-02-17	[DA Capital]	akira	Link
2025-02-14	[COSMED]	akira	Link
2025-02-17	[Persante Health Care]	incransom	Link
2025-02-05	[annegrady.org]	embargo	Link
2025-02-16	[Pamrya.de]	fog	Link
2025-02-16	[QBurst]	fog	Link
2025-02-16	[Acqua development]	fog	Link
2025-02-16	[Gitlabs: Acqua development, QBurst, Pamyra.de]	fog	Link
2025-02-08	[Gpstech2007.com]	flocker	Link
2025-02-08	[Mervis.info]	flocker	Link
2025-02-08	[Realtime.tw]	flocker	Link
2025-02-15	[saulttribe.com/kewadin.com]	ransomhub	Link
2025-02-15	[www.rowetactical.com]	ransomhub	Link
2025-02-15	[www.transcend-info.com]	ransomhub	Link
2025-02-15	[www.naga.ae]	ransomhub	Link
2025-02-15	[www.cityoftarrant.com]	ransomhub	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-15	[www.imgenterprises.com]	ransomhub	Link
2025-02-15	[www.solardatasystems.com]	ransomhub	Link
2025-02-15	[www.310tempering.com]	ransomhub	Link
2025-02-15	[www.colacouronnelocations.com]	ransomhub	Link
2025-02-10	[Fortune Electric Co Ltd]	lynx	Link
2025-02-09	[Northeast Delta Human Services Authority]	incransom	Link
2025-02-09	[City of McKinney]	incransom	Link
2025-02-15	[halex.com]	abyss	Link
2025-02-11	[Hydronic & Steam Equipment]	play	Link
2025-02-11	[Ratioparts]	play	Link
2025-02-14	[Heritage South Credit Union]	embargo	Link
2025-02-14	[Primaveras]	akira	Link
2025-02-08	[www.calspa.it]	ransomhub	Link
2025-02-14	[Nelson & Townsend, CPA's]	akira	Link
2025-02-14	[Castle Rock Construction Company]	akira	Link
2025-02-14	[Genus]	akira	Link
2025-02-14	[Window World of Raleigh]	akira	Link
2025-02-14	[F.TECH R&D NORTH AMERICA INC.]	qilin	Link
2025-02-14	[Go Strictly]	akira	Link
2025-02-14	[Bethany Lutheran Church]	qilin	Link
2025-02-10	[GANRO]	lynx	Link
2025-02-14	[Regency Media]	akira	Link
2025-02-14	[brockbanks.co.uk]	ransomhub	Link
2025-02-14	[The Agency]	rhysida	Link
2025-02-13	[Shields Facilities Maintenance]	play	Link
2025-02-13	[ADULLACT]	fog	Link
2025-02-13	[Ayomi]	fog	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-13	[Omydoo]	fog	Link
2025-02-13	[Gitlabs: Omydoo, Ayomi, ADULLACT]	fog	Link
2025-02-13	[Aspire Rural Health System]	bianlian	Link
2025-02-13	[Mozo Grau (mozo-grau.com)]	fog	Link
2025-02-13	[CoMo-Industrial Engineering]	akira	Link
2025-02-13	[enventuregt.com]	ransomhub	Link
2025-02-13	[snoqualmietribe.us]	ransomhub	Link
2025-02-13	[vadatech.com]	qilin	Link
2025-02-13	[Nippon Steel USA]	bianlian	Link
2025-02-13	[Financial Services of America, Inc.]	bianlian	Link
2025-02-13	[Layfield & Borel CPA's L.L.C]	bianlian	Link
2025-02-13	[Dain, Torpy, Le Ray, Wiest & Garner, P.C.]	bianlian	Link
2025-02-13	[Dan Eckman CPA]	akira	Link
2025-02-12	[Elite Advanced LaserCorporation]	akira	Link
2025-02-12	[Obex Medical]	killsec	Link
2025-02-12	[Cache Valley ENT]	medusa	Link
2025-02-12	[JP Express]	medusa	Link
2025-02-12	[Central District Health Department]	medusa	Link
2025-02-12	[morrisgroup.co]	clop	Link
2025-02-05	[stjerome.org]	safepay	Link
2025-02-12	[Therma Seal Insulation Systems]	ciphbit	Link
2025-02-12	[Squeezer-software]	fog	Link
2025-02-12	[Spacemanic]	fog	Link
2025-02-12	[INGV]	fog	Link
2025-02-12	[Gitlabs: INGV, Spacemanic, Squeezer-software]	fog	Link
2025-02-12	[Quality Home Health Care]	qilin	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-12	[avtovelomoto.by]	funksec	Link
2025-02-12	[alderconstruction.com]	ransomhub	Link
2025-02-12	[steveallcorn.remax.com]	ransomhub	Link
2025-02-12	[bergconst.com]	ransomhub	Link
2025-02-12	[burdickpainting.com]	ransomhub	Link
2025-02-12	[columbiacabinets.com]	ransomhub	Link
2025-02-12	[ekvallbyrne.com]	ransomhub	Link
2025-02-12	[krmcustomhomes.com]	ransomhub	Link
2025-02-12	[laderalending.com]	ransomhub	Link
2025-02-12	[minnesotaexteriors.com]	ransomhub	Link
2025-02-12	[rogerspetro.com]	ransomhub	Link
2025-02-12	[sundanceliving.com]	ransomhub	Link
2025-02-12	[thejdkgroup.com]	ransomhub	Link
2025-02-12	[twncomm.com]	ransomhub	Link
2025-02-12	[Vicky Foods]	akira	Link
2025-02-12	[Hess (hess-gmbh.de)]	fog	Link
2025-02-12	[TJKM]	qilin	Link
2025-02-03	[askgs.ma]	ransomhub	Link
2025-02-12	[slchc.edu]	ransomhub	Link
2025-02-12	[weathersa.co.za]	ransomhub	Link
2025-02-12	[Erie Management Group, LLC]	qilin	Link
2025-02-12	[curtisint.com]	cactus	Link
2025-02-12	[britannicahome.com]	cactus	Link
2025-02-12	[uniquehd.com]	cactus	Link
2025-02-12	[tomsmithindustries.com]	qilin	Link
2025-02-04	[Accelerator]	dragonforce	Link
2025-02-04	[O&S Associates]	dragonforce	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-12	[Leading Edge Specialized Dentistry]	rhysida	Link
2025-02-12	[Hammond Trucking & Excavation]	rhysida	Link
2025-02-12	[BH Aircraft Company, Inc.]	rhysida	Link
2025-02-12	[My New Jersey Dentist]	rhysida	Link
2025-02-12	[Town Counsel Law & Litigation]	rhysida	Link
2025-02-06	[MICRO MANUFACTURING]	medusalocker	Link
2025-02-05	[The Brown & Hurley Group]	lynx	Link
2025-02-11	[Tie Down Engineering]	play	Link
2025-02-11	[Monroe Transportation Services Inc]	play	Link
2025-02-11	[Kensington Glass Arts]	play	Link
2025-02-11	[EAC Consulting]	play	Link
2025-02-11	[Baltimore Country Club]	play	Link
2025-02-11	[Jildor Shoes]	play	Link
2025-02-11	[Mainline Information Systems]	play	Link
2025-02-11	[Fastighetservice AB]	play	Link
2025-02-11	[CESI]	termite	Link
2025-02-11	[Shinn Fu Company of America]	play	Link
2025-02-11	[ROCK SOLID Stabilization & Reclamation]	play	Link
2025-02-11	[Cold Storage Manufacturing]	play	Link
2025-02-11	[Neaton Auto Products Manufacturing]	play	Link
2025-02-11	[Saint George's College (saintgeorge.cl)]	fog	Link
2025-02-11	[Aurora Public Schools (aurorak12.org)]	fog	Link
2025-02-11	[Natures Organics]	medusa	Link
2025-02-11	[Paignton Zoo]	medusa	Link
2025-02-11	[SRP Companies]	medusa	Link
2025-02-11	[lacold.com]	clop	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-11	[The University of Notre Dame Australia (nd.edu.au)]	fog	Link
2025-02-11	[Prime Trust Financial]	akira	Link
2025-02-01	[sehma.com]	threeam	Link
2025-02-11	[I.B.G SPA]	sarcoma	Link
2025-02-11	[ldi-trucking-inc]	sarcoma	Link
2025-02-11	[Wisper Reimer Ingenieure GmbH]	sarcoma	Link
2025-02-11	[Unimicron]	sarcoma	Link
2025-02-11	[Logix Corporate Solutions]	killsec	Link
2025-02-11	[sole technology]	monti	Link
2025-02-10	[primesourcestaffing.com]	ransomhub	Link
2025-02-04	[The Children's Center Of Hamden]	incransom	Link
2025-02-10	[komline.com]	ransomhub	Link
2025-02-10	[bazcooil.com]	ransomhub	Link
2025-02-10	[sdfab.com]	ransomhub	Link
2025-02-10	[kaplanstahler.com]	ransomhub	Link
2025-02-04	[www.jsp.com]	ransomhub	Link
2025-02-10	[ekonom.com]	clop	Link
2025-02-10	[editel.eu]	clop	Link
2025-02-10	[derrytransport.com]	clop	Link
2025-02-10	[dana-co.com]	clop	Link
2025-02-10	[designndesigninc.com]	clop	Link
2025-02-10	[daatagroup.com]	clop	Link
2025-02-10	[dunnriteproducts.com]	clop	Link
2025-02-10	[d2go.io]	clop	Link
2025-02-10	[dynastyfootwear.com]	clop	Link
2025-02-10	[dxc.com]	clop	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-10	[dundasjafine.com]	clon	Link
2025-02-10	[drexel.ca]	clon	Link
2025-02-10	[donlen.com]	clon	Link
2025-02-10	[dlfna.com]	clon	Link
2025-02-04	[directex.net]	clon	Link
2025-02-10	[diazfoods.com]	clon	Link
2025-02-10	[detecno.com]	clon	Link
2025-02-10	[deltaenterprise.com]	clon	Link
2025-02-10	[deltachildren.com]	clon	Link
2025-02-10	[decescente.com]	clon	Link
2025-02-10	[dbetances.com]	clon	Link
2025-02-10	[datapakservices.com]	clon	Link
2025-02-10	[coglans.com]	clon	Link
2025-02-10	[cycle.local]	clon	Link
2025-02-10	[cassinfo.com]	clon	Link
2025-02-10	[claw.local]	clon	Link
2025-02-10	[cgdc.cottong.local]	clon	Link
2025-02-10	[cps.k12.il.us]	clon	Link
2025-02-10	[conbraco.com]	clon	Link
2025-02-10	[clearon.com]	clon	Link
2025-02-10	[crestmills.com]	clon	Link
2025-02-10	[cranebsu.com]	clon	Link
2025-02-10	[covetra.com]	clon	Link
2025-02-10	[connexion-informatique.fr]	clon	Link
2025-02-10	[compasshealthbrands.com]	clon	Link
2025-02-10	[collectionxiix.com]	clon	Link
2025-02-10	[coghlans.com]	clon	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-10	[codagami.com]	cllop	Link
2025-02-10	[cmcoldstores.com]	cllop	Link
2025-02-10	[classicaccessories.com]	cllop	Link
2025-02-10	[cinema1.ca]	cllop	Link
2025-02-10	[cherokeedistributing.com]	cllop	Link
2025-02-10	[chemstarcorp.com]	cllop	Link
2025-02-10	[challenger.com]	cllop	Link
2025-02-10	[cesarcastillo.com]	cllop	Link
2025-02-10	[cedarsfoods.com]	cllop	Link
2025-02-10	[cathayhome.com]	cllop	Link
2025-02-10	[catchuplogistics.com]	cllop	Link
2025-02-10	[castlewoodapparel.com]	cllop	Link
2025-02-10	[carlsondistributing.com]	cllop	Link
2025-02-10	[Enfin]	killsec	Link
2025-02-10	[Recievership Specialists]	bianlian	Link
2025-02-10	[abcapital.com.ph]	lockbit3	Link
2025-02-10	[Allen & Pinnix]	akira	Link
2025-02-10	[The Pawn]	akira	Link
2025-02-10	[Polstermöbel Oelsa GmbH]	sarcoma	Link
2025-02-03	[Grail Springs Retreat]	medusa	Link
2025-02-05	[Rural Health Services]	medusa	Link
2025-02-07	[Adler Shine LLP]	medusa	Link
2025-02-07	[SimonMed Imaging]	medusa	Link
2025-02-08	[PAD Aviation Technics GmbH]	medusa	Link
2025-02-10	[Serenity Salon & Spa]	medusa	Link
2025-02-10	[Michael's Hair Body Mind]	medusa	Link
2025-02-10	[Greenwich Medical Spa]	medusa	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-10	[Capital Cell Global (CCG)]	killsec	Link
2025-02-10	[ASRAM Medical College and Hospita]	killsec	Link
2025-02-10	[CAPITALFINEMEATS.COM]	cllop	Link
2025-02-10	[CALIFORNIARAINLA.COM]	cllop	Link
2025-02-10	[CAINEWAREHOUSING.COM]	cllop	Link
2025-02-10	[BARCOMADE.COM]	cllop	Link
2025-02-10	[BEINOGLOU.GR]	cllop	Link
2025-02-10	[BIAGIBROS.COM]	cllop	Link
2025-02-10	[BSIEDI.COM]	cllop	Link
2025-02-10	[BOZICKDIST.COM]	cllop	Link
2025-02-10	[BOWANDARROWPET.COM]	cllop	Link
2025-02-10	[BOSSCHAIR.COM]	cllop	Link
2025-02-10	[BESTBRANDSINC.COM]	cllop	Link
2025-02-10	[BERKSHIREINC.COM]	cllop	Link
2025-02-10	[BENSONMILLS.COM]	cllop	Link
2025-02-10	[BENBECKER.EU]	cllop	Link
2025-02-10	[BAYSIDENH.COM]	cllop	Link
2025-02-10	[BARRETTDISTRIBUTION.COM]	cllop	Link
2025-02-10	[BACKYARDDISCOVERY.COM]	cllop	Link
2025-02-10	[ALEGACY.COM]	cllop	Link
2025-02-10	[AURORAIMPORTING.COM]	cllop	Link
2025-02-10	[ARLAN.NL]	cllop	Link
2025-02-10	[ARKIEJIGS.COM]	cllop	Link
2025-02-10	[APOLLOCORP.COM]	cllop	Link
2025-02-10	[AOL.COM AJ MISSERT INC]	cllop	Link
2025-02-10	[ANNABELLECANDY.COM]	cllop	Link
2025-02-10	[ANDROSNA.COM]	cllop	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-10	[ANDREWSDISTRIBUTING.COM]	clon	Link
2025-02-10	[AMSINO.COM]	clon	Link
2025-02-10	[AMERICANLIGHTING.COM]	clon	Link
2025-02-10	[ALPADVANTAGE.COM]	clon	Link
2025-02-10	[ALLTECH.COM]	clon	Link
2025-02-10	[ALLIANCEMERCANTILE.COM]	clon	Link
2025-02-10	[AIRLIQUIDE.COM]	clon	Link
2025-02-10	[AGILITYAUTOPARTS.COM]	clon	Link
2025-02-10	[AFFINITYCANADA.COM]	clon	Link
2025-02-10	[ACTIAN.COM]	clon	Link
2025-02-10	[ACPIDEAS.COM]	clon	Link
2025-02-10	[ACCEM.COM]	clon	Link
2025-02-10	[ABCOPRODUCTS.COM]	clon	Link
2025-02-10	[3PLSOFTWARE.COM]	clon	Link
2025-02-10	[Brockway Hair Design]	medusa	Link
2025-02-10	[True World Foods]	medusa	Link
2025-02-10	[MEDES College]	medusa	Link
2025-02-03	[Glow Medi Spa]	medusa	Link
2025-02-10	[3FINITY.NET]	clon	Link
2025-02-10	[1888MILLS.COM]	clon	Link
2025-02-10	[CXTSOFTWARE.COM]	clon	Link
2025-02-10	[UNIEKINC.COM]	clon	Link
2025-02-10	[STORKCRAFT.COM]	clon	Link
2025-02-10	[COMPANY's_PART1]	clon	Link
2025-02-10	[Old National Events Plaza]	akira	Link
2025-02-09	[Marshall Motor Holdings]	lynx	Link
2025-02-10	[Albright Institute]	killsec	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-10	[WhoHire]	killsec	Link
2025-02-10	[Upstate Glass Tempering]	sarcoma	Link
2025-02-10	[Saied Music]	sarcoma	Link
2025-02-09	[Kitty cookies]	kraken	Link
2025-02-09	[www.cdprojekt.com]	kraken	Link
2025-02-09	[www.mgl.law]	kraken	Link
2025-02-09	[www.fudpucker.com]	kraken	Link
2025-02-09	[ctntelco.com]	kraken	Link
2025-02-09	[iRidge Inc.]	fog	Link
2025-02-09	[Maxvy Technologies Pvt]	fog	Link
2025-02-09	[Universitatea Politehnica din Bucuresti]	fog	Link
2025-02-09	[Hpsid.org]	ransomhub	Link
2025-02-09	[wwcsd.net]	ransomhub	Link
2025-02-09	[Israel Police]	handala	Link
2025-02-09	[Gitlabs: Universitatea Politehnica din Bucuresti, Maxvy Technologies Pvt, iRidge Inc.]	fog	Link
2025-02-08	[Substitute Teacher Service]	cicada3301	Link
2025-02-08	[SAKAI SOUKEN Co.]	hunters	Link
2025-02-08	[cmr24]	stormous	Link
2025-02-08	[phidac.be]	funksec	Link
2025-02-07	[3SS]	fog	Link
2025-02-07	[Fligno]	fog	Link
2025-02-07	[Chalmers tekniska högskola]	fog	Link
2025-02-07	[herbalcanadaonline.com]	funksec	Link
2025-02-07	[Gitlabs: Chalmers tekniska högskola, Fligno, 3SS]	fog	Link
2025-02-06	[teamues.com]	ransomhub	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-07	[iaaglobal.org]	funksec	Link
2025-02-07	[Tropical Foods Company Inc]	akira	Link
2025-02-07	[sautech.edu]	ransomhub	Link
2025-02-07	[autogedal.ro]	funksec	Link
2025-02-07	[nldappraisals.com]	qilin	Link
2025-02-07	[renmarkfinancial.com]	qilin	Link
2025-02-06	[lowernazareth.com]	safepay	Link
2025-02-06	[northernresponse.com]	cactus	Link
2025-02-06	[savoiesfoods.com]	cactus	Link
2025-02-06	[zsattorneys.com]	ransomhub	Link
2025-02-06	[NG-BLU Networks]	akira	Link
2025-02-06	[Presence From Innovation (PFI)]	akira	Link
2025-02-06	[Robertshaw]	hunters	Link
2025-02-04	[HARADA]	qilin	Link
2025-02-06	[DIEM]	fog	Link
2025-02-06	[Top Systems]	fog	Link
2025-02-06	[eConceptions]	fog	Link
2025-02-06	[Gitlabs: eConceptions, Top Systems, DIEM]	fog	Link
2025-02-05	[McCORMICK TAYLOR]	qilin	Link
2025-02-05	[corehandf.com]	threeam	Link
2025-02-05	[Dash Business]	bianlian	Link
2025-02-05	[Hall Chadwick]	bianlian	Link
2025-02-05	[NESCTC Security Services]	bianlian	Link
2025-02-05	[Shinsung Delta Tech]	lynx	Link
2025-02-05	[Banfi Vintners]	lynx	Link
2025-02-05	[annegrady.org]	ransomhub	Link
2025-02-05	[rablighting.com]	qilin	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-05	[boostheat.com]	apt73	Link
2025-02-05	[rattelacademy.com]	funksec	Link
2025-02-05	[cara.com.my]	funksec	Link
2025-02-04	[casperstruck.com]	kairos	Link
2025-02-04	[medicalreportsltd.com]	kairos	Link
2025-02-01	[LUA Coffee]	fog	Link
2025-02-01	[GFZ Helmholtz Centre for Geosciences]	fog	Link
2025-02-01	[PT. ITPRENEUR INDONESIA TECHNOLOGY]	fog	Link
2025-02-04	[Devlion]	fog	Link
2025-02-04	[SOLEIL]	fog	Link
2025-02-04	[hemio.de]	fog	Link
2025-02-03	[Madia]	fog	Link
2025-02-03	[X-lab group]	fog	Link
2025-02-03	[Bolin Centre for Climate Research]	fog	Link
2025-02-04	[Gitlabs: hemio.de, SOLEIL, Devlion]	fog	Link
2025-02-04	[mielectric.com.br]	akira	Link
2025-02-04	[engineeredequip.com]	akira	Link
2025-02-04	[emin.cl]	akira	Link
2025-02-04	[alphascriptrx.com]	akira	Link
2025-02-04	[premierop.com]	akira	Link
2025-02-04	[acesaz.com]	akira	Link
2025-02-04	[mipa.com.br]	akira	Link
2025-02-04	[usm-americas.com]	akira	Link
2025-02-04	[feheq.com]	akira	Link
2025-02-04	[stewartautosales.com]	akira	Link
2025-02-04	[milleraa.com]	akira	Link
2025-02-04	[jsfrental.com]	akira	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-04	[summitmovinghouston.com]	akira	Link
2025-02-04	[dwgp.com]	akira	Link
2025-02-04	[easycom.com]	akira	Link
2025-02-04	[alfa.com.co]	akira	Link
2025-02-04	[westernwoodsinc.com]	akira	Link
2025-02-04	[viscira.com]	akira	Link
2025-02-04	[elitt-sas.fr]	akira	Link
2025-02-04	[cfctech.com]	akira	Link
2025-02-04	[armellini.com]	akira	Link
2025-02-04	[mbacomputer.com]	akira	Link
2025-02-04	[directex.net]	akira	Link
2025-02-04	[360energy.com.ar]	akira	Link
2025-02-04	[saludsa.com.ec]	akira	Link
2025-02-04	[intercomp.com.mt]	akira	Link
2025-02-04	[C & R Molds Inc]	bianlian	Link
2025-02-04	[Commercial Solutions]	bianlian	Link
2025-02-04	[www.aymcdonald.com]	ransomhub	Link
2025-02-04	[capstoneins.ca]	ransomhub	Link
2025-02-04	[clarkfreightways.com]	ransomhub	Link
2025-02-04	[mistralsolutions.com]	apt73	Link
2025-02-04	[India car owners]	apt73	Link
2025-02-04	[Alshu, Eshoo]	ransomhouse	Link
2025-02-04	[kksp.com]	qilin	Link
2025-02-04	[brainsystem.eu]	funksec	Link
2025-02-04	[Taking stock of 2024]	Part 2]	akira
2025-02-04	[esle.eu]	funksec	Link
2025-02-04	[forum-rainbow-rp.forumotion.eu]	funksec	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-04	[mgainnovation.com]	cactus	Link
2025-02-04	[cornwelltools.com]	cactus	Link
2025-02-04	[rashtiandrashti.com]	cactus	Link
2025-02-04	[alojaimi.com]	ransomhub	Link
2025-02-04	[www.aswgr.com]	ransomhub	Link
2025-02-04	[heartlandrvs.com]	ransomhub	Link
2025-02-04	[gaheritagefcu.org]	ransomhub	Link
2025-02-04	[SSMC]	cicada3301	Link
2025-02-04	[Rivers Casino and Rush Street Gaming]	cicada3301	Link
2025-02-04	[Asterra Properties]	cicada3301	Link
2025-02-04	[Caliente Construction]	cicada3301	Link
2025-02-04	[C2S Technologies Inc.]	everest	Link
2025-02-04	[ITSS]	everest	Link
2025-02-03	[brewsterfiredepartment.org]	safepay	Link
2025-02-03	[Dickerson & Nieman Realtors]	play	Link
2025-02-03	[Sheridan Nurseries]	play	Link
2025-02-03	[The Hill Brush]	play	Link
2025-02-03	[DPC Development]	play	Link
2025-02-03	[Woodway USA]	play	Link
2025-02-03	[Daniel Island Club]	play	Link
2025-02-03	[QGS Development]	play	Link
2025-02-03	[Gitlabs: Bolin Centre for Climate Research, X-lab group, Madia]	fog	Link
2025-02-03	[gruppozaccaria.it]	lockbit3	Link
2025-02-03	[Karadeniz Holding (karadenizholding.com)]	fog	Link
2025-02-03	[www.wongfleming.com]	ransomhub	Link
2025-02-03	[smithmidland.com]	ransomhub	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-02-03	[www.origene.com]	ransomhub	Link
2025-02-03	[Denton Regional Suicide Prevention Coalition]	qilin	Link
2025-02-03	[fasttrackcargo.com]	funksec	Link
2025-02-03	[Ponte16 Hotel & Casino]	killsec	Link
2025-02-03	[Elslaw.com (EARLY , LUCARELLI , SWEENEY & MEISENKOTHEN LAW)]	qilin	Link
2025-02-03	[DRI Title & Escrow]	qilin	Link
2025-02-03	[DPA Auctions]	qilin	Link
2025-02-03	[Altair Travel]	qilin	Link
2025-02-03	[Civil Design, Inc]	qilin	Link
2025-02-03	[The Gatesworth Senior Living St. Louis]	qilin	Link
2025-02-03	[GOVirtual-it.com (VIRTUAL IT)]	qilin	Link
2025-02-03	[coel.com.mx]	apt73	Link
2025-02-03	[Alford Walden Law]	qilin	Link
2025-02-03	[Pasco Systems]	qilin	Link
2025-02-03	[MPP Group of Companies]	qilin	Link
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

Datum	Opfer	Ransomware-Gruppe	Webseite
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	[DATACONSULTANTS.COM]	clop	Link
2025-02-01	[CHAMPIONHOMES.COM]	clop	Link
2025-02-01	[CIERANT.COM]	clop	Link
2025-02-01	[DATATRAC.COM]	clop	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.