Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20250213

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

Fortinet: Angriffe auf Schwachstellen laufen, Updates für diverse Produkte

Fortinet hat für zahlreiche Produkte Sicherheitsupdates veröffentlicht. Mindestens eine Lücke wird bereits attackiert.

- Link

—

Adobe-Patchday: Schadcode-Sicherheitslücken gefährden Illustrator & Co.

Angreifer können an mehreren Sicherheitslücken in Anwendungen von Adobe ansetzen, um Computer zu kompromittieren.

- Link

—

Ivanti: Kritische Codeschmuggel-Lücken in VPN und CSA

In Ivantis VPN-Software ICS, IPS und ISAC sowie in Ivanti CSA klaffen kritische Sicherheitslecks. Angreifer können Schadcode unterjubeln.

- Link

—

Microsoft-Patchday: Angreifer attackieren Windows und löschen Daten

Es sind wichtige Sicherheitsupdates für Azure, Office, Windows und Co. erschienen. Es gibt bereits Attacken. Weitere können bevorstehen.

- Link

—

Solarwinds: Update schließt teils kritische Lücken in Platform

Solarwinds hat das Update 2025.1 von Solarwinds Platform veröffentlicht. Es schließt einige teilweise kritische Sicherheitslücken.

- Link

—

Sicherheitsupdates Zimbra: Angreifer können Metadaten von E-Mails auslesen

Die Zimbra-Entwickler haben unter anderem mindestens eine kritische Lücke in der E-Mail- und Groupwarelösung geschlossen.

- Link

—

SAP-Patchday: 18 Sicherheitsmitteilungen zu teils hochriskanten Lücken

SAP veröffentlicht zum Februar-Patchday 18 Sicherheitsmitteilungen, die Sicherheitslücken behandeln, die teils als hohes Risiko eingestuft werden.

- Link

—

Anonymisierendes Linux: Tails 6.12 schließt Deanonymisierungs-Lücke

Sicherheitslücken in der anonymisierenden Linux-Distribution Tails erlauben Angreifern die Deanonymisierung von Nutzern. Tails 6.12 stoppt das.

- Link

—

Jetzt patchen! Schadcode-Attacken auf Trimble Cityworks beobachtet

Das Asset-Managementsystem Cityworks von Trimble ist verwundbar: Derzeit nutzen Angreifer eine Sicherheitslücke aus.

- Link

—

Defekter Sicherheitspatch für HCL BigFix Server Automation repariert

Angreifer können HCL BigFix SA per DoS-Attacke abschießen. Ein überarbeitetes Sicherheitsupdate soll das Problem nun lösen.

- 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	0.994140000	Link
CVE-2024-9463	0.961860000	0.996680000	Link
CVE-2024-8963	0.967240000	0.997840000	Link
CVE-2024-7593	0.971650000	0.999010000	Link
CVE-2024-6893	0.938390000	0.993680000	Link
CVE-2024-6670	0.904230000	0.991060000	Link
CVE-2024-5910	0.962890000	0.996900000	Link
CVE-2024-55956	0.967520000	0.997900000	Link
CVE-2024-5217	0.933860000	0.993210000	Link
CVE-2024-50623	0.969520000	0.998430000	Link
CVE-2024-4879	0.934670000	0.993300000	Link
CVE-2024-4577	0.958420000	0.996100000	Link
CVE-2024-4358	0.925270000	0.992490000	Link
CVE-2024-41713	0.957210000	0.995900000	Link
CVE-2024-40711	0.962170000	0.996760000	Link
CVE-2024-4040	0.969020000	0.998290000	Link
CVE-2024-38856	0.950120000	0.994910000	Link
CVE-2024-36401	0.955950000	0.995720000	Link
CVE-2024-3400	0.964000000	0.997120000	Link
CVE-2024-3273	0.937410000	0.993590000	Link
CVE-2024-32113	0.933050000	0.993150000	Link
CVE-2024-28995	0.965000000	0.997330000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-28987	0.961930000	0.996700000	Link
CVE-2024-27348	0.960260000	0.996420000	Link
CVE-2024-27198	0.968000000	0.998020000	Link
CVE-2024-24919	0.960980000	0.996530000	Link
CVE-2024-23897	0.973540000	0.999550000	Link
CVE-2024-2389	0.900180000	0.990800000	Link
CVE-2024-23692	0.964390000	0.997230000	Link
CVE-2024-21893	0.956970000	0.995840000	Link
CVE-2024-21887	0.973220000	0.999490000	Link
CVE-2024-20767	0.965330000	0.997400000	Link
CVE-2024-1709	0.957220000	0.995900000	Link
CVE-2024-1212	0.937140000	0.993560000	Link
CVE-2024-0986	0.955530000	0.995660000	Link
CVE-2024-0195	0.962680000	0.996850000	Link
CVE-2024-0012	0.969980000	0.998540000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Wed, 12 Feb 2025

[NEU] [hoch] GitLab: Mehrere Schwachstellen

Ein entfernter authentisierter Angreifer kann mehrere Schwachstellen in GitLab ausnutzen, um Cross-Site-Scripting-Angriffe durchzuführen, einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen, erhöhte Berechtigungen zu erlangen und Daten zu manipulieren.

- Link

—

Wed, 12 Feb 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

—

Wed, 12 Feb 2025

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

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

- Link

—

Wed, 12 Feb 2025

[NEU] [hoch] GNU Emacs: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Wed, 12 Feb 2025

[NEU] [hoch] Ivanti Connect Secure, Policy Secure und Secure Access Client: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Ivanti Connect Secure, Ivanti Policy Secure und Ivanti Secure Access Client ausnutzen, um seine Rechte zu erweitern, beliebigen Code auszuführen, Daten zu manipulieren und vertrauliche Informationen preiszugeben.

- Link

—

Wed, 12 Feb 2025

[NEU] [hoch] Microsoft Office: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Microsoft Excel 2016, Microsoft Office 2016, Microsoft Office Online Server, Microsoft SharePoint, Microsoft Office 2019, Microsoft SharePoint Server 2019, Microsoft 365 Apps und Microsoft Office ausnutzen, um beliebigen Code auszuführen, sich erhöhte Rechte zu verschaffen und vertrauliche Informationen preiszugeben.

- Link

—

Wed, 12 Feb 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

—

Wed, 12 Feb 2025

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

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

- Link

—

Wed, 12 Feb 2025

[UPDATE] [hoch] EDK2 NetworkPkg IP stack implementation: Mehrere Schwachstellen

Ein Angreifer aus dem angrenzenden Netzwerk oder ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in der EDK2 NetworkPkg IP stack implementation ausnutzen, um beliebigen Programmcode auszuführen, vertrauliche Informationen offenzulegen und einen Denial of Service Zustand auszulösen.

- Link

—

Wed, 12 Feb 2025

[UPDATE] [hoch] Red Hat Ansible Automation Platform: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Red Hat Ansible Automation Platform ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand erzeugen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren oder Cross-Site-Scripting (XSS)-Angriffe durchzuführen.

- Link

—

Wed, 12 Feb 2025

[UPDATE] [hoch] Django: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Django ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen oder vertrauliche Informationen offenzulegen.

- Link

—

Wed, 12 Feb 2025

[UPDATE] [hoch] Intel Firmware: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Intel Firmware ausnutzen, um seine Privilegien zu erhöhen, vertrauliche Informationen preiszugeben und einen Denial-of-Service-Zustand zu erzeugen.

- Link

—

Wed, 12 Feb 2025

[UPDATE] [hoch] Intel Prozessor (Xeon): Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Intel Prozessor ausnutzen, um einen Denial of Service Angriff durchzuführen und sich erhöhte Rechte zu verschaffen.

- Link

—

Wed, 12 Feb 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

—

Wed, 12 Feb 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

—

Wed, 12 Feb 2025

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

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

- Link

—

Wed, 12 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

—

Wed, 12 Feb 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

—

Wed, 12 Feb 2025

[UPDATE] [hoch] Cacti: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Cacti ausnutzen, um vertrauliche Informationen preiszugeben, beliebigen Code auszuführen und SQL-Abfragen zu manipulieren.

- Link

—

Wed, 12 Feb 2025

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

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

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
2/12/2025	[Oracle Linux 8 / 9 : terraform-provider-oci-fips (ELSA-2025-31356)]	critical
2/12/2025	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : MozillaThunderbird (SUSE-SU-2025:0405-1)]	critical
2/12/2025	[SUSE SLES12 Security Update : tomcat (SUSE-SU-2025:0394-1)]	critical
2/12/2025	[Debian dsa-5864 : libpam-pkcs11 - security update]	critical
2/12/2025	[SUSE SLES12 Security Update : MozillaFirefox (SUSE-SU-2025:0391-1)]	critical
2/12/2025	[Dahua Security Digital Video Recorders Permissions, Privileges, and Access Controls (CVE-2013-3614)]	critical
2/12/2025	[Dahua Security Digital Video Recorders Improper Authentication (CVE-2013-3613)]	critical

Datum	Schwachstelle	Bewertung
2/12/2025	[Dahua Security Digital Video Recorders Permissions, Privileges, and Access Controls (CVE-2013-5754)]	critical
2/12/2025	[Dahua Security Digital Video Recorders Credentials Management Errors (CVE-2013-3615)]	critical
2/12/2025	[Dahua Security Digital Video Recorders Credentials Management Errors (CVE-2013-3612)]	critical
2/12/2025	[RHEL 8 : nodejs:20 (RHSA-2025:1351)]	high
2/12/2025	[RHEL 6 : kernel (RHSA-2025:1347)]	high
2/12/2025	[GitLab 13.3 < 17.6.5 / 17.7 < 17.7.4 / 17.8 < 17.8.2 (CVE-2025-0376)]	high
2/12/2025	[Debian dsa-5865 : gir1.2-javascriptcoregtk-4.0 - security update]	high
2/12/2025	[SUSE SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2025:0428-1)]	high
2/12/2025	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : go1.24 (SUSE-SU-2025:0431-1)]	high
2/12/2025	[SUSE SLES15 Security Update : kernel (Live Patch 44 for SLE 15 SP3) (SUSE-SU-2025:0449-1)]	high
2/12/2025	[SUSE SLES15 Security Update : ovmf (SUSE-SU-2025:0407-1)]	high
2/12/2025	[SUSE SLES15 / openSUSE 15 Security Update : govulncheck-vulndb (SUSE-SU-2025:0429-1)]	high
2/12/2025	[SUSE SLED15 / SLES15 Security Update : bind (SUSE-SU-2025:0427-1)]	high
2/12/2025	[SUSE SLES15 Security Update : kernel (Live Patch 22 for SLE 15 SP4) (SUSE-SU-2025:0455-1)]	high
2/12/2025	[SUSE SLES12 Security Update : bind (SUSE-SU-2025:0389-1)]	high
2/12/2025	[Oracle Linux 9 : openssl (ELSA-2025-1330)]	high
2/12/2025	[FreeBSD : Intel CPUs – multiple vulnerabilities (d598266d-7772-4a31-9594-83b76b1fb837)]	high

Datum	Schwachstelle	Bewertung
2/12/2025	[Ubuntu 24.10 : Linux kernel (AWS) vulnerabilities (USN-7238-4)]	high
2/12/2025	[Ubuntu 20.04 LTS : Linux kernel (AWS) vulnerabilities (USN-7235-3)]	high
2/12/2025	[Ubuntu 20.04 LTS : Linux kernel (AWS) vulnerabilities (USN-7234-4)]	high
2/12/2025	[Ubuntu 22.04 LTS : Linux kernel (Azure) vulnerabilities (USN-7236-3)]	high
2/12/2025	[RHEL 9 : kpatch-patch-5_14_0-70_112_1, kpatch-patch-5_14_0-70_121_1, and kpatch-patch-5_14_0-70_85_1 (RHSA-2025:1374)]	high
2/12/2025	[Dahua Security Network Video Recorders Improper Input Validation (CVE-2024-39949)]	high
2/12/2025	[Dahua Security NVR NVR50XX, NVR52XX, NVR54XX, and NVR58XX Improper Authentication (CVE-2017-9314)]	high
2/12/2025	[Dahua Security Network Video Recorders Improper Input Validation (CVE-2024-39946)]	high
2/12/2025	[Dahua Security Network Video Recorders Improper Input Validation (CVE-2024-39948)]	high

4 Die Hacks der Woche

mit Martin Haunschmid

4.0.1 Private video

Vorschaubild Zum Youtube Video

5 Cyberangriffe: (Feb)

Datum	Opfer	Land	Information
2025-02-11	Port of Oostende	[BEL]	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
2025-02-08	FORTUNE ELECTRIC CO.,LTD	[TWN]	Link
2025-02-07	Transcend Information, Inc.	[TWN]	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-Grupppe	Webseite
2025-02-12	[Obex Medical]	killsec	Link
2025-02-12	[Cache Valley ENT]	medusa	Link
2025-02-12	[JP Express]	medusa	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2025-02-12	[Central District Health Department]	medusa	Link
2025-02-12	[morrisgroup.co]	clop	Link
2025-02-12	[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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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 MANUFACTRING]	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	[Fastighetsservice AB]	play	Link
2025-02-11	[CESI]	termite	Link
2025-02-11	[Shinn Fu Company of America]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2025-02-11	[The University of Notre Dame Australia (nd.edu.au)]	fog	Link
2025-02-11	[Prime Trust Financial]	akira	Link
2025-02-11	[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

Datum	Opfer	Ransomware-Grupppe	Webseite
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	[designdesigninc.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
2025-02-10	[dundasjafine.com]	clop	Link
2025-02-10	[drexel.ca]	clop	Link
2025-02-10	[donlen.com]	clop	Link
2025-02-10	[dlfna.com]	clop	Link
2025-02-04	[directex.net]	clop	Link
2025-02-10	[diazfoods.com]	clop	Link
2025-02-10	[detecno.com]	clop	Link
2025-02-10	[deltaenterprise.com]	clop	Link
2025-02-10	[deltachildren.com]	clop	Link
2025-02-10	[decrescente.com]	clop	Link
2025-02-10	[dbetances.com]	clop	Link
2025-02-10	[datapakservices.com]	clop	Link
2025-02-10	[coglans.com]	clop	Link
2025-02-10	[cycle.local]	clop	Link
2025-02-10	[cassinfo.com]	clop	Link
2025-02-10	[claw.local]	clop	Link
2025-02-10	[cgdc.cottong.local]	clop	Link
2025-02-10	[cps.k12.il.us]	clop	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2025-02-10	[conbraco.com]	clop	Link
2025-02-10	[clearon.com]	clop	Link
2025-02-10	[crestmills.com]	clop	Link
2025-02-10	[cranebsu.com]	clop	Link
2025-02-10	[covectra.com]	clop	Link
2025-02-10	[connexion-informatique.fr]	clop	Link
2025-02-10	[compasshealthbrands.com]	clop	Link
2025-02-10	[collectionxiix.com]	clop	Link
2025-02-10	[coghlans.com]	clop	Link
2025-02-10	[codagami.com]	clop	Link
2025-02-10	[cmcoldstores.com]	clop	Link
2025-02-10	[classicaccessories.com]	clop	Link
2025-02-10	[cinema1.ca]	clop	Link
2025-02-10	[cherokeedistributing.com]	clop	Link
2025-02-10	[chemstarcorp.com]	clop	Link
2025-02-10	[challenger.com]	clop	Link
2025-02-10	[cesarcastillo.com]	clop	Link
2025-02-10	[cedarsfoods.com]	clop	Link
2025-02-10	[cathayhome.com]	clop	Link
2025-02-10	[catchuplogistics.com]	clop	Link
2025-02-10	[castlewoodapparel.com]	clop	Link
2025-02-10	[carlsondistributing.com]	clop	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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2025-02-10	[Capital Cell Global (CCG)]	killsec	Link
2025-02-10	[ASRAM Medical College and Hospita]	killsec	Link
2025-02-10	[CAPITALFINEMEATS.COM]	clop	Link
2025-02-10	[CALIFORNIARAINLA.COM]	clop	Link
2025-02-10	[CAINEWAREHOUSING.COM]	clop	Link
2025-02-10	[BARCOMADE.COM]	clop	Link
2025-02-10	[BEINOGLOU.GR]	clop	Link
2025-02-10	[BIAGIBROS.COM]	clop	Link
2025-02-10	[BSIEDI.COM]	clop	Link
2025-02-10	[BOZICKDIST.COM]	clop	Link
2025-02-10	[BOWANDARROWPET.COM]	clop	Link
2025-02-10	[BOSSCHAIR.COM]	clop	Link
2025-02-10	[BESTBRANDSINC.COM]	clop	Link
2025-02-10	[BERKSHIREINC.COM]	clop	Link
2025-02-10	[BENSONMILLS.COM]	clop	Link
2025-02-10	[BENBECKER.EU]	clop	Link
2025-02-10	[BAYSIDENH.COM]	clop	Link
2025-02-10	[BARRETTDISTRIBUTION.COM]	clop	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2025-02-10	[BACKYARDDISCOVERY.COM]	clop	Link
2025-02-10	[ALEGACY.COM]	clop	Link
2025-02-10	[AURORAIMPORTING.COM]	clop	Link
2025-02-10	[ARLAN.NL]	clop	Link
2025-02-10	[ARKIEJIGS.COM]	clop	Link
2025-02-10	[APOLLOCORP.COM]	clop	Link
2025-02-10	[AOL.COM AJ MISSERT INC]	clop	Link
2025-02-10	[ANNABELLECANDY.COM]	clop	Link
2025-02-10	[ANDROSNA.COM]	clop	Link
2025-02-10	[ANDREWSDISTRIBUTING.COM]	clop	Link
2025-02-10	[AMSINO.COM]	clop	Link
2025-02-10	[AMERICANLIGHTING.COM]	clop	Link
2025-02-10	[ALPADVANTAGE.COM]	clop	Link
2025-02-10	[ALLTECH.COM]	clop	Link
2025-02-10	[ALLIANCEMERCANTILE.COM]	clop	Link
2025-02-10	[AIRLIQUIDE.COM]	clop	Link
2025-02-10	[AGILITYAUTOPARTS.COM]	clop	Link
2025-02-10	[AFFINITYCANADA.COM]	clop	Link
2025-02-10	[ACTIAN.COM]	clop	Link
2025-02-10	[ACPIDEAS.COM]	clop	Link
2025-02-10	[ACCEM.COM]	clop	Link
2025-02-10	[ABCOPRODUCTS.COM]	clop	Link
2025-02-10	[3PLSOFTWARE.COM]	clop	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

Datum	Opfer	Ransomware-Grupppe	Webseite
2025-02-10	[3FINITY.NET]	clop	Link
2025-02-10	[1888MILLS.COM]	clop	Link
2025-02-10	[CXTSOFTWARE.COM]	clop	Link
2025-02-10	[UNIEKINC.COM]	clop	Link
2025-02-10	[STORKCRAFT.COM]	clop	Link
2025-02-10	[COMPANY's_PART1]	clop	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
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	[Hpisd.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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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
2025-02-05	[HARADA]	qilin	Link
2025-02-06	[DIEM]	fog	Link
2025-02-06	[Top Systems]	fog	Link
2025-02-06	[eConceptions]	fog	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
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
2025-02-05	[boostheat.com]	apt73	Link
2025-02-05	[rattelacademy.com]	funksec	Link
2025-02-05	[cara.com.my]	funksec	Link
2025-02-05	[Mid-State Machine & Fabricating Corp]	play	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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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	[AIshu, 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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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

Datum	Opfer	Ransomware-Grupppe	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	[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

Datum	Opfer	Ransomware-Grupppe	Webseite
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.