

Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20250409



Inhaltsverzeichnis

1 Editorial	2
2 Security-News	3
2.1 Heise - Security-Alert	3
3 Sicherheitslücken	3
3.1 EPSS	3
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit	3
3.2 BSI - Warn- und Informationsdienst (WID)	7
3.3 Sicherheitslücken Meldungen von Tenable	11
4 Die Hacks der Woche	12
4.0.1 Information Stealer. Wie funktionieren sie?	13
5 Cyberangriffe: (Apr)	14
6 Ransomware-Erpressungen: (Apr)	14
7 Quellen	20
7.1 Quellenverzeichnis	20
8 Impressum	21

1 Editorial

Guten Morgen,

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

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

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

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

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

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

Ihr Cyberwald-Team

2 Security-News

2.1 Heise - Security-Alert

3 Sicherheitslücken

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

3.1 EPSS

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

3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2025-24813	0.935470000	0.998270000	Link
CVE-2025-0282	0.908700000	0.996180000	Link
CVE-2025-0108	0.937040000	0.998450000	Link
CVE-2024-9935	0.905290000	0.995970000	Link
CVE-2024-9474	0.941770000	0.999090000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-9465	0.937890000	0.998560000	Link
CVE-2024-9463	0.921530000	0.997030000	Link
CVE-2024-8963	0.941140000	0.999010000	Link
CVE-2024-8517	0.905300000	0.995970000	Link
CVE-2024-8504	0.922610000	0.997120000	Link
CVE-2024-8503	0.924070000	0.997260000	Link
CVE-2024-8190	0.915170000	0.996560000	Link
CVE-2024-7954	0.934920000	0.998200000	Link
CVE-2024-7593	0.940210000	0.998860000	Link
CVE-2024-6782	0.929590000	0.997720000	Link
CVE-2024-6670	0.943090000	0.999390000	Link
CVE-2024-5932	0.937400000	0.998500000	Link
CVE-2024-5806	0.929880000	0.997760000	Link
CVE-2024-57727	0.934540000	0.998170000	Link
CVE-2024-55956	0.908330000	0.996160000	Link
CVE-2024-53704	0.914910000	0.996550000	Link
CVE-2024-5217	0.936890000	0.998430000	Link
CVE-2024-51567	0.939660000	0.998780000	Link
CVE-2024-51378	0.933790000	0.998110000	Link
CVE-2024-50623	0.939920000	0.998820000	Link
CVE-2024-50603	0.936470000	0.998380000	Link
CVE-2024-4956	0.938210000	0.998600000	Link
CVE-2024-4885	0.936750000	0.998410000	Link
CVE-2024-4879	0.941130000	0.999000000	Link
CVE-2024-48248	0.910140000	0.996250000	Link
CVE-2024-47575	0.912870000	0.996410000	Link
CVE-2024-4577	0.943760000	0.999610000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-45519	0.933670000	0.998100000	Link
CVE-2024-45241	0.907990000	0.996130000	Link
CVE-2024-45216	0.922130000	0.997070000	Link
CVE-2024-45195	0.940290000	0.998870000	Link
CVE-2024-4443	0.928800000	0.997640000	Link
CVE-2024-4358	0.940510000	0.998920000	Link
CVE-2024-4257	0.919600000	0.996910000	Link
CVE-2024-41713	0.936460000	0.998380000	Link
CVE-2024-4040	0.942740000	0.999300000	Link
CVE-2024-40348	0.922050000	0.997060000	Link
CVE-2024-39914	0.917400000	0.996710000	Link
CVE-2024-38856	0.941840000	0.999110000	Link
CVE-2024-37032	0.919050000	0.996860000	Link
CVE-2024-36412	0.923410000	0.997210000	Link
CVE-2024-36401	0.943720000	0.999590000	Link
CVE-2024-36104	0.930810000	0.997840000	Link
CVE-2024-3552	0.912890000	0.996430000	Link
CVE-2024-3495	0.916030000	0.996620000	Link
CVE-2024-34470	0.917610000	0.996720000	Link
CVE-2024-34102	0.943470000	0.999510000	Link
CVE-2024-3400	0.942860000	0.999320000	Link
CVE-2024-3273	0.942130000	0.999170000	Link
CVE-2024-3272	0.930690000	0.997830000	Link
CVE-2024-32709	0.901110000	0.995740000	Link
CVE-2024-32113	0.940470000	0.998900000	Link
CVE-2024-31982	0.934840000	0.998200000	Link
CVE-2024-31851	0.923600000	0.997230000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-31850	0.925310000	0.997360000	Link
CVE-2024-31849	0.917880000	0.996750000	Link
CVE-2024-31848	0.917880000	0.996750000	Link
CVE-2024-3094	0.913330000	0.996450000	Link
CVE-2024-29973	0.934290000	0.998160000	Link
CVE-2024-29972	0.908270000	0.996150000	Link
CVE-2024-29895	0.936520000	0.998390000	Link
CVE-2024-29824	0.936130000	0.998340000	Link
CVE-2024-2961	0.934720000	0.998180000	Link
CVE-2024-29269	0.918300000	0.996800000	Link
CVE-2024-29059	0.916430000	0.996640000	Link
CVE-2024-28995	0.942870000	0.999330000	Link
CVE-2024-28987	0.939530000	0.998750000	Link
CVE-2024-2879	0.931170000	0.997870000	Link
CVE-2024-28255	0.917650000	0.996730000	Link
CVE-2024-27956	0.919980000	0.996930000	Link
CVE-2024-27954	0.920390000	0.996970000	Link
CVE-2024-27348	0.938630000	0.998650000	Link
CVE-2024-27292	0.900780000	0.995710000	Link
CVE-2024-27199	0.944960000	1.000000000	Link
CVE-2024-27198	0.945820000	1.000000000	Link
CVE-2024-25852	0.927360000	0.997510000	Link
CVE-2024-25600	0.922190000	0.997070000	Link
CVE-2024-24919	0.942890000	0.999330000	Link
CVE-2024-23917	0.943050000	0.999380000	Link
CVE-2024-23897	0.943510000	0.999530000	Link
CVE-2024-2389	0.943810000	0.999630000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-23692	0.942820000	0.999310000	Link
CVE-2024-2330	0.922980000	0.997150000	Link
CVE-2024-22120	0.924530000	0.997300000	Link
CVE-2024-22024	0.933070000	0.998050000	Link
CVE-2024-21893	0.943200000	0.999440000	Link
CVE-2024-21887	0.944160000	0.999780000	Link
CVE-2024-21762	0.907240000	0.996080000	Link
CVE-2024-21683	0.922010000	0.997060000	Link
CVE-2024-21650	0.920760000	0.996980000	Link
CVE-2024-21413	0.925630000	0.997370000	Link
CVE-2024-20767	0.938210000	0.998600000	Link
CVE-2024-1709	0.939550000	0.998760000	Link
CVE-2024-1698	0.925630000	0.997360000	Link
CVE-2024-1512	0.923180000	0.997170000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Tue, 01 Apr 2025

[NEU] [hoch] Zabbix: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Zabbix ausnutzen, um beliebigen Code auszuführen, Cross-Site-Scripting-Angriffe durchzuführen, vertrauliche Informationen preiszugeben und einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

—

Tue, 01 Apr 2025

[UPDATE] [hoch] Red Hat Enterprise Linux (Quarkus): Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Quarkus auf Red Hat Enterprise Linux ausnutzen, um Informationen offenzulegen, oder einen Denial of Service auszulösen.

- [Link](#)

—
Tue, 01 Apr 2025

[UPDATE] [hoch] FreeType: Schwachstelle ermöglicht Codeausführung

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

- [Link](#)

—

Tue, 01 Apr 2025

[NEU] [hoch] Microsoft Azure: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Microsoft Azure ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Tue, 01 Apr 2025

[NEU] [hoch] Apple macOS: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apple macOS ausnutzen, um erhöhte Rechte - sogar Root-Rechte - zu erlangen, um vertrauliche Informationen offenzulegen, um beliebigen Code auszuführen, um Daten zu manipulieren, um Sicherheitsmaßnahmen - sogar Sandbox-Einschränkungen - zu umgehen oder um einen Denial-of-Service-Zustand auszulösen.

- [Link](#)

—

Tue, 01 Apr 2025

[NEU] [hoch] Apple Safari: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apple Safari ausnutzen, um vertrauliche Informationen preiszugeben, Spoofing- und Cross-Site-Scripting-Angriffe durchzuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu verursachen, beliebigen Code auszuführen und Daten zu manipulieren.

- [Link](#)

—

Tue, 01 Apr 2025

[NEU] [hoch] Rancher: Schwachstelle ermöglicht Privilegieneskalation

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

- [Link](#)

—

Tue, 01 Apr 2025

[NEU] [hoch] Apple iOS und iPadOS: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apple iOS und Apple iPadOS

ausnutzen, um vertrauliche Informationen preiszugeben, beliebigen Code auszuführen, einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, erhöhte Rechte zu erlangen oder Daten zu manipulieren.

- [Link](#)

—

Tue, 01 Apr 2025

[UPDATE] [hoch] IBM App Connect Enterprise: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in IBM App Connect Enterprise ausnutzen, um beliebigen Code auszuführen und Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

—

Tue, 01 Apr 2025

[UPDATE] [hoch] vim: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in vim ausnutzen, um einen Denial-of-Service-Zustand zu verursachen und beliebigen Code auszuführen.

- [Link](#)

—

Tue, 01 Apr 2025

[UPDATE] [hoch] X.Org X11: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein lokaler oder entfernter, authentisierter Angreifer kann mehrere Schwachstellen in X.Org X11 ausnutzen, um seine Privilegien zu erhöhen und Code auszuführen.

- [Link](#)

—

Tue, 01 Apr 2025

[UPDATE] [hoch] X.Org X11: Schwachstelle ermöglicht Privilegieneskalation oder Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle in X.Org X11 ausnutzen, um seine Privilegien zu erhöhen und beliebigen Code auszuführen.

- [Link](#)

—

Tue, 01 Apr 2025

[UPDATE] [hoch] X.Org X11: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in X.Org X11 ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

—

Tue, 01 Apr 2025

[UPDATE] [hoch] docker: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in docker ausnutzen, um seine

Privilegien zu erhöhen.

- [Link](#)

—

Tue, 01 Apr 2025

[UPDATE] [hoch] X.Org X11 und Xming: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in X.Org X11 und Xming ausnutzen, um seine Privilegien zu erhöhen, einen Denial-of-Service-Zustand zu erzeugen oder beliebigen Code auszuführen.

- [Link](#)

—

Tue, 01 Apr 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](#)

—

Tue, 01 Apr 2025

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um erhöhte Privilegien zu erlangen oder einen Denial of Service auszulösen.

- [Link](#)

—

Tue, 01 Apr 2025

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um Dateien zu manipulieren oder seine Rechte zu erweitern.

- [Link](#)

—

Tue, 01 Apr 2025

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglichen nicht spezifizierten Angriff

Ein lokaler Angreifer kann eine Schwachstelle im Linux-Kernel ausnutzen, um einen nicht näher spezifizierten Angriff zu starten.

- [Link](#)

—

Tue, 01 Apr 2025

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

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

- [Link](#)

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
4/1/2025	[Debian dla-4103 : suricata - security update]	high
4/1/2025	[Debian dla-4102 : linux-config-6.1 - security update]	high
4/1/2025	[Debian dla-4104 : freetype2-demos - security update]	high
4/1/2025	[EulerOS 2.0 SP13 : ruby (EulerOS-SA-2025-1343)]	high
4/1/2025	[EulerOS 2.0 SP13 : rsync (EulerOS-SA-2025-1325)]	high
4/1/2025	[EulerOS 2.0 SP13 : rsync (EulerOS-SA-2025-1342)]	high
4/1/2025	[EulerOS 2.0 SP13 : bind (EulerOS-SA-2025-1328)]	high
4/1/2025	[EulerOS 2.0 SP13 : proftpd (EulerOS-SA-2025-1322)]	high
4/1/2025	[EulerOS 2.0 SP13 : kernel (EulerOS-SA-2025-1334)]	high
4/1/2025	[EulerOS 2.0 SP13 : ruby (EulerOS-SA-2025-1326)]	high
4/1/2025	[EulerOS 2.0 SP13 : proftpd (EulerOS-SA-2025-1339)]	high
4/1/2025	[EulerOS 2.0 SP13 : bind (EulerOS-SA-2025-1311)]	high
4/1/2025	[EulerOS 2.0 SP13 : kernel (EulerOS-SA-2025-1317)]	high
4/1/2025	[EulerOS 2.0 SP13 : curl (EulerOS-SA-2025-1313)]	high
4/1/2025	[EulerOS 2.0 SP13 : dhcp (EulerOS-SA-2025-1331)]	high
4/1/2025	[EulerOS 2.0 SP13 : curl (EulerOS-SA-2025-1330)]	high
4/1/2025	[EulerOS 2.0 SP13 : dhcp (EulerOS-SA-2025-1314)]	high
4/1/2025	[Fedora 41 : mingw-libxslt (2025-fd62ac3fb1)]	high
4/1/2025	[Fedora 40 : mingw-libxslt (2025-f7a12118f3)]	high

Datum	Schwachstelle	Bewertung
3/31/2025	[Amazon Linux 2023 : xorg-x11-server-common, xorg-x11-server-devel, xorg-x11-server-source (ALAS2023-2025-892)]	high
3/31/2025	[Amazon Linux 2023 : xorg-x11-server-Xwayland, xorg-x11-server-Xwayland-devel (ALAS2023-2025-891)]	high
3/31/2025	[Amazon Linux 2023 : xorg-x11-server-Xwayland, xorg-x11-server-Xwayland-devel (ALAS2023-2025-895)]	high

4 Die Hacks der Woche

mit Martin Haunschmid

4.0.1 Information Stealer. Wie funktionieren sie?



[Zum Youtube Video](#)

5 Cyberangriffe: (Apr)

Datum	Opfer	Land	Information
2025-04-06	Toppan Next Tech (TNT)	[SGP]	Link
2025-04-05	Optimax Technology	[TWN]	Link

6 Ransomware-Erpressungen: (Apr)

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-08	[physiciansmedicalbilling.net]	lockbit3	Link
2025-04-08	[gramoll.com]	lynx	Link
2025-04-08	[Taxplan]	crypto24	Link
2025-04-08	[Mochtar Karuwin Komar: Indonesian law firm - MKK]	crypto24	Link
2025-04-08	[technoforte software pvt ltd]	crypto24	Link
2025-04-08	[International Busines Service]	crypto24	Link
2025-04-08	[Iris Neofinanciera]	crypto24	Link
2025-04-08	[RFMS, Inc.]	kairos	Link
2025-04-08	[www.gchd.org]	qilin	Link
2025-04-08	[averasia]	qilin	Link
2025-04-08	[Third Avenue Management]	metaencryptor	Link
2025-04-08	[crystal-d.com]	lockbit3	Link
2025-04-08	[Bauer-Walser AG]	akira	Link
2025-04-08	[Gruppo C.R S.p.a]	sarcoma	Link
2025-04-08	[FKS Group]	sarcoma	Link
2025-04-08	[Coop57]	incransom	Link
2025-04-08	[The Fullerton Hotelsand Resorts]	akira	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-08	[Thiekon Constructie]	incransom	Link
2025-04-07	[Doman Building Materials Group]	interlock	Link
2025-04-07	[Andretti Indoor Karting & Games]	interlock	Link
2025-04-07	[galesburg.org]	kairos	Link
2025-04-07	[Cambridge Fluid Systems]	qilin	Link
2025-04-07	[The Komec]	qilin	Link
2025-04-07	[Spring Creek Golf & Country Club]	qilin	Link
2025-04-07	[JKC Australia LNG]	qilin	Link
2025-04-07	[American Air Conditioning & Heating]	qilin	Link
2025-04-07	[Dhoot Transmission]	qilin	Link
2025-04-07	[Privat-Spitex Schweiz GmbH]	qilin	Link
2025-04-07	[CVTE]	hellcat	Link
2025-04-01	[Telecontrol]	ransomhouse	Link
2025-04-04	[Metal Sales Manufacturing Corporation]	morpheus	Link
2025-04-06	[asiapacificex.com]	lockbit3	Link
2025-04-07	[TIME Group]	akira	Link
2025-04-07	[ASOLO DOLCE SAS]	akira	Link
2025-04-07	[SMYK]	akira	Link
2025-04-07	[sunbayhotel.com]	qilin	Link
2025-04-07	[Flo Components]	qilin	Link
2025-04-06	[Dubai Company]	devman	Link
2025-04-06	[Texas Construction Firm]	devman	Link
2025-04-06	[Optimax Technology]	devman	Link
2025-04-01	[National Electronic Transit (N.E.T)]	dragonforce	Link
2025-04-01	[Altara]	dragonforce	Link
2025-04-04	[IACC Holdings]	dragonforce	Link
2025-04-04	[Texla Energy Management]	dragonforce	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-01	[Krypton Solutions]	medusa	Link
2025-04-01	[FS Tool Corporation]	medusa	Link
2025-04-06	[Groupe Delcourt]	hunters	Link
2025-04-06	[Hofmann Fördertechnik GmbH]	hunters	Link
2025-04-06	[IDS Infotech]	hunters	Link
2025-04-06	[grupotersa.com.mx]	lockbit3	Link
2025-04-06	[graphiquedefrance.com]	lockbit3	Link
2025-04-06	[Swiss Capitals Group]	rhysida	Link
2025-04-04	[National Ticket Company]	bert	Link
2025-04-05	[Eagle Distilleries]	cicada3301	Link
2025-04-05	[caschile.cl]	VanHelsing	Link
2025-04-05	[Optimax Technology]	qilin	Link
2025-04-05	[ABITL Finishing]	play	Link
2025-04-05	[Baltimore Steel Erectors]	play	Link
2025-04-05	[Hawk Technology]	play	Link
2025-04-05	[Csm Engineering]	play	Link
2025-04-03	[L&S Mechanical (Reuploaded)]	spacebears	Link
2025-04-05	[Racami]	hellcat	Link
2025-04-05	[Asseco]	hellcat	Link
2025-04-05	[LeoVegas AB]	hellcat	Link
2025-04-05	[Nexia Poyiadjis IT]	hunters	Link
2025-04-05	[TEDOM]	hunters	Link
2025-04-05	[Blackmon Mooring]	hunters	Link
2025-04-05	[Apex Logistics International]	sarcoma	Link
2025-04-05	[FUJIFILM]	sarcoma	Link
2025-04-03	[Latronica Law Firm, P.C]	morpheus	Link
2025-04-04	[Royal Glass]	play	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-04	[Fraser Trebilcock]	play	Link
2025-04-04	[Drive Products]	interlock	Link
2025-04-04	[Doman]	interlock	Link
2025-04-04	[Sinari's software POC]	qilin	Link
2025-04-04	[DELOPT]	akira	Link
2025-04-04	[Source Photonics]	frag	Link
2025-04-04	[AWM Alliance Real Estate Group Ltd.]	akira	Link
2025-04-04	[RORZE Technology Inc.]	akira	Link
2025-04-04	[Sansone Group]	hunters	Link
2025-04-04	[Parker Fabrication, Inc]	akira	Link
2025-04-04	[Henna Chevrolet]	akira	Link
2025-04-04	[National Sign corp]	hunters	Link
2025-04-04	[raymurray.com]	qilin	Link
2025-04-04	[dgr.at]	qilin	Link
2025-04-04	[yumaspazio.com]	qilin	Link
2025-04-04	[The ToolShed]	sarcoma	Link
2025-04-04	[turkish defense military]	babuk2	Link
2025-04-04	[rheinmetall.com (Rheinmetall Defence)]	babuk2	Link
2025-04-04	[Woodmen Valley Chapel]	sarcoma	Link
2025-04-04	[Cherokee County School District]	interlock	Link
2025-04-03	[gangotreehomes.com (RealEstate)]	babuk2	Link
2025-04-03	[Secret plans of Indian army]	babuk2	Link
2025-04-03	[Bangladesh Armed Forces (BangLadesh Army)]	babuk2	Link
2025-04-03	[Saudi Arabian military and government internal center]	babuk2	Link
2025-04-03	[Hellenic Airforce]	babuk2	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-03	[Gem-Dandy Accessories]	akira	Link
2025-04-03	[Fuller Metric Parts]	akira	Link
2025-04-03	[ezbuy.sg (Singapore Shopping)]	babuk2	Link
2025-04-03	[Iran gas service system]	babuk2	Link
2025-04-03	[kfar hatta medical center - Lebanon]	babuk2	Link
2025-04-03	[Polizia italia mail access]	babuk2	Link
2025-04-03	[zalora.sg (Singapore Shopping)]	babuk2	Link
2025-04-02	[Hop Industries]	play	Link
2025-04-02	[Lifebreath]	play	Link
2025-04-02	[Parvin-Clauss Sign Company]	play	Link
2025-04-02	[OTA Management]	play	Link
2025-04-02	[Fulfillment Plus]	play	Link
2025-04-02	[Regionale Verkehrsbetriebe]	play	Link
2025-04-02	[aosense.com - AO Sense INC.]	babuk2	Link
2025-04-02	[Alton Steel]	lynx	Link
2025-04-02	[navy-mil-bd]	babuk2	Link
2025-04-02	[Taking stock of March 2025]	akira	Link
2025-04-02	[Socarpor]	akira	Link
2025-04-02	[Naza TTDI Sdn Bhd]	akira	Link
2025-04-02	[Mikado Publicis]	akira	Link
2025-04-02	[Entech Sales & Service, LLC]	akira	Link
2025-04-02	[Prima Power]	akira	Link
2025-04-02	[Clarity Ventures]	rhysida	Link
2025-04-02	[crownlaboratories.com]	abyss	Link
2025-04-02	[caliendoarchitects.com]	qilin	Link
2025-04-02	[Brügger Architekten AG]	killsec	Link
2025-04-02	[Royal Saudi Air Force]	killsec	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-02	[Collective Architecture]	killsec	Link
2025-04-02	[IMA Global]	killsec	Link
2025-04-02	[US BioTek Laboratories]	killsec	Link
2025-04-02	[drdo.gov.in]	babuk2	Link
2025-04-01	[uniproof.com.br]	babuk2	Link
2025-04-01	[DG2 Design]	anubis	Link
2025-04-01	[The Loretto Hospital]	incransom	Link
2025-04-01	[(UPDATE) - whitecapcanada.com]	babuk2	Link
2025-04-01	[Bamar Plastics, Inc.]	akira	Link
2025-04-01	[Mercury Integrated Manufacturing]	akira	Link
2025-04-01	[Alora Pharmaceuticals, LLC]	morpheus	Link
2025-04-01	[747 Studios]	killsec	Link
2025-04-01	[BenefitElect]	killsec	Link
2025-04-01	[Ocuco]	killsec	Link
2025-04-01	[Workers Informática Ltda]	killsec	Link
2025-04-01	[Testima Engineering]	killsec	Link
2025-04-01	[Brella]	killsec	Link
2025-04-01	[Fancy Films]	killsec	Link
2025-04-01	[Lendco]	killsec	Link
2025-04-01	[Nydegger + Finger AG]	killsec	Link
2025-04-01	[Dorel Home]	killsec	Link
2025-04-01	[Hexicor]	killsec	Link
2025-04-01	[AAPG]	killsec	Link
2025-04-01	[Hanna Global Solutions]	killsec	Link
2025-04-01	[Flagship Press Flagship Press]	killsec	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.