
Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20250323



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	13
4.0.1 Information Stealer. Wie funktionieren sie?	14
5 Cyberangriffe: (Mär)	15
6 Ransomware-Erpressungen: (Mär)	16
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

3 Sicherheitslücken

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

3.1 EPSS

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

3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2025-0108	0.924750000	0.997420000	Link
CVE-2024-9474	0.939550000	0.998800000	Link
CVE-2024-9465	0.937890000	0.998640000	Link
CVE-2024-9463	0.919600000	0.997020000	Link
CVE-2024-8963	0.941140000	0.999010000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-8517	0.905300000	0.996170000	Link
CVE-2024-8504	0.916220000	0.996770000	Link
CVE-2024-8503	0.920200000	0.997070000	Link
CVE-2024-8190	0.915170000	0.996720000	Link
CVE-2024-7954	0.934920000	0.998290000	Link
CVE-2024-7593	0.939590000	0.998810000	Link
CVE-2024-6782	0.929590000	0.997820000	Link
CVE-2024-6670	0.943090000	0.999380000	Link
CVE-2024-5932	0.937400000	0.998590000	Link
CVE-2024-5806	0.929880000	0.997830000	Link
CVE-2024-57727	0.934200000	0.998250000	Link
CVE-2024-55956	0.908330000	0.996300000	Link
CVE-2024-55591	0.906810000	0.996240000	Link
CVE-2024-53704	0.910910000	0.996430000	Link
CVE-2024-5217	0.936890000	0.998520000	Link
CVE-2024-51567	0.939930000	0.998860000	Link
CVE-2024-51378	0.932710000	0.998110000	Link
CVE-2024-50623	0.940480000	0.998930000	Link
CVE-2024-50603	0.933410000	0.998180000	Link
CVE-2024-4956	0.936560000	0.998490000	Link
CVE-2024-4885	0.936750000	0.998510000	Link
CVE-2024-4879	0.941130000	0.999000000	Link
CVE-2024-47575	0.912870000	0.996560000	Link
CVE-2024-4577	0.943760000	0.999630000	Link
CVE-2024-45519	0.933670000	0.998210000	Link
CVE-2024-45216	0.920980000	0.997140000	Link
CVE-2024-45195	0.940290000	0.998900000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-4443	0.928800000	0.997720000	Link
CVE-2024-4358	0.940870000	0.998970000	Link
CVE-2024-41713	0.930790000	0.997900000	Link
CVE-2024-4040	0.942450000	0.999230000	Link
CVE-2024-40348	0.922050000	0.997190000	Link
CVE-2024-39914	0.914110000	0.996630000	Link
CVE-2024-38856	0.941840000	0.999110000	Link
CVE-2024-36401	0.943720000	0.999600000	Link
CVE-2024-36104	0.930810000	0.997910000	Link
CVE-2024-3552	0.912890000	0.996570000	Link
CVE-2024-3495	0.916030000	0.996760000	Link
CVE-2024-34470	0.922580000	0.997230000	Link
CVE-2024-34102	0.943470000	0.999520000	Link
CVE-2024-3400	0.943400000	0.999480000	Link
CVE-2024-3273	0.942130000	0.999150000	Link
CVE-2024-3272	0.930690000	0.997900000	Link
CVE-2024-32709	0.902690000	0.996020000	Link
CVE-2024-32113	0.939340000	0.998780000	Link
CVE-2024-31982	0.934840000	0.998290000	Link
CVE-2024-31851	0.923600000	0.997360000	Link
CVE-2024-31850	0.923600000	0.997360000	Link
CVE-2024-31849	0.915310000	0.996730000	Link
CVE-2024-31848	0.915310000	0.996730000	Link
CVE-2024-3094	0.909890000	0.996350000	Link
CVE-2024-29973	0.934290000	0.998250000	Link
CVE-2024-29972	0.908270000	0.996290000	Link
CVE-2024-29895	0.936520000	0.998480000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-29824	0.936130000	0.998430000	Link
CVE-2024-2961	0.929030000	0.997740000	Link
CVE-2024-29269	0.918300000	0.996900000	Link
CVE-2024-29059	0.916430000	0.996790000	Link
CVE-2024-28995	0.942870000	0.999320000	Link
CVE-2024-28987	0.939530000	0.998800000	Link
CVE-2024-2879	0.931170000	0.997940000	Link
CVE-2024-28255	0.913600000	0.996590000	Link
CVE-2024-27956	0.919980000	0.997050000	Link
CVE-2024-27954	0.919300000	0.996990000	Link
CVE-2024-27348	0.938630000	0.998700000	Link
CVE-2024-27292	0.900780000	0.995920000	Link
CVE-2024-27199	0.944440000	0.999900000	Link
CVE-2024-27198	0.945820000	1.000000000	Link
CVE-2024-25852	0.927360000	0.997590000	Link
CVE-2024-25600	0.922190000	0.997200000	Link
CVE-2024-24919	0.942890000	0.999320000	Link
CVE-2024-23917	0.942750000	0.999290000	Link
CVE-2024-23897	0.943510000	0.999530000	Link
CVE-2024-2389	0.943810000	0.999640000	Link
CVE-2024-23692	0.943360000	0.999470000	Link
CVE-2024-2330	0.916970000	0.996820000	Link
CVE-2024-22120	0.924530000	0.997410000	Link
CVE-2024-22024	0.936170000	0.998430000	Link
CVE-2024-21893	0.943200000	0.999420000	Link
CVE-2024-21887	0.943920000	0.999700000	Link
CVE-2024-21762	0.907240000	0.996250000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-21683	0.922010000	0.997190000	Link
CVE-2024-21650	0.920760000	0.997120000	Link
CVE-2024-21413	0.925630000	0.997480000	Link
CVE-2024-20767	0.938210000	0.998680000	Link
CVE-2024-1709	0.940610000	0.998940000	Link
CVE-2024-1698	0.925630000	0.997470000	Link
CVE-2024-1561	0.901790000	0.995970000	Link
CVE-2024-1512	0.923180000	0.997320000	Link
CVE-2024-13160	0.916310000	0.996780000	Link
CVE-2024-13159	0.925980000	0.997520000	Link
CVE-2024-12356	0.921460000	0.997160000	Link
CVE-2024-1212	0.929150000	0.997760000	Link
CVE-2024-11680	0.931700000	0.998010000	Link
CVE-2024-10924	0.925170000	0.997450000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 21 Mar 2025

[UPDATE] [hoch] Google Chrome: Schwachstelle ermöglicht Codeausführung

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

- [Link](#)

—

Fri, 21 Mar 2025

[UPDATE] [hoch] libxml2: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in libxml2 ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

—

Fri, 21 Mar 2025

[UPDATE] [hoch] libxml2: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in libxml2 ausnutzen, um einen Denial of Service Angriff durchzuführen oder vertrauliche Daten einsehen.

- [Link](#)

—

Fri, 21 Mar 2025

[UPDATE] [hoch] AMD Prozessoren: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in AMD Prozessoren ausnutzen, um beliebigen Programmcode auszuführen oder Informationen offenzulegen.

- [Link](#)

—

Fri, 21 Mar 2025

[UPDATE] [hoch] Apache Camel und mehrere Red Hat Produkte: Mehrere Schwachstellen

Ein entfernter anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Apache Camel und in mehreren Red Hat-Produkten ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen preiszugeben und beliebigen Code auszuführen.

- [Link](#)

—

Fri, 21 Mar 2025

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um einen Denial of Service Zustand herbeizuführen oderum einen nicht näher spezifizierten Angriff durchzuführen.

- [Link](#)

—

Fri, 21 Mar 2025

[UPDATE] [hoch] libxml2: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in libxml2 ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen oder einen nicht näher spezifizierten Angriff zu starten.

- [Link](#)

—

Fri, 21 Mar 2025

[NEU] [hoch] Synology Replication Service: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Synology Replication Service ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 21 Mar 2025

[UPDATE] [hoch] Gitea: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Gitea ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Fri, 21 Mar 2025

[UPDATE] [hoch] PostgreSQL: Schwachstelle ermöglicht SQL Injection und Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in PostgreSQL ausnutzen, um eine SQL Injection durchzuführen und in der Folge beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 21 Mar 2025

[UPDATE] [kritisch] Webkit/Apple : Schwachstelle ermöglicht Umgehung von Sicherheitsmechanismen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Webkit und in Apple iOS, Apple iPadOS, Apple macOS und Apple Safari ausnutzen, um Sicherheitsmechanismen zu umgehen.

- [Link](#)

—

Thu, 20 Mar 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](#)

—

Thu, 20 Mar 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](#)

—

Thu, 20 Mar 2025

[UPDATE] [hoch] Microsoft Windows/Windows Server: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft Windows Server, Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2, Microsoft Windows 10, Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows, Microsoft Windows Server

2022 und Microsoft Windows 11 ausnutzen, um beliebigen Programmcode auszuführen, seine Rechte zu erweitern, zu spoofen, Sicherheitsmaßnahmen zu umgehen, Informationen offenzulegen oder einen Denial of Service auszulösen .

- [Link](#)

—

Thu, 20 Mar 2025

[NEU] [hoch] Veeam Backup & Replication: Schwachstelle ermöglicht Codeausführung

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Veeam Backup & Replication ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Thu, 20 Mar 2025

[NEU] [hoch] ESRI ArcGIS Portal: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in ESRI ArcGIS Portal ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Thu, 20 Mar 2025

[NEU] [hoch] IBM InfoSphere Information Server: Schwachstelle ermöglicht Privilegieneskalation

Ein lokaler Angreifer kann eine Schwachstelle in IBM InfoSphere Information Server ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Thu, 20 Mar 2025

[UPDATE] [hoch] SAP: Mehrere Schwachstellen

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in verschiedenen SAP Produkten ausnutzen, um dadurch die Vertraulichkeit, Verfügbarkeit und die Integrität der Anwendung zu gefährden.

- [Link](#)

—

Thu, 20 Mar 2025

[UPDATE] [hoch] ffmpeg: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in ffmpeg ausnutzen, um einen Denial of Service Angriff durchzuführen, vertrauliche Informationen offenzulegen oder beliebigen Code auszuführen.

- [Link](#)

—

Thu, 20 Mar 2025

[UPDATE] [hoch] docker: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Docker ausnutzen, um seine Privilegien zu erhöhen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen oder Dateien zu manipulieren.

- [Link](#)

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
3/22/2025	[RHEL 8 : firefox update (Important) (RHSA-2024:6850)]	critical
3/22/2025	[RHEL 9 : firefox update (Important) (RHSA-2024:6782)]	critical
3/22/2025	[RHEL 8 : php:7.4 (RHSA-2025:3076)]	critical
3/22/2025	[RHEL 9 : firefox update (Important) (RHSA-2024:6786)]	critical
3/22/2025	[RHEL 8 : php:7.4 (RHSA-2025:3016)]	critical
3/22/2025	[RHEL 8 : firefox update (Important) (RHSA-2024:6839)]	critical
3/22/2025	[RHEL 8 : mysql:8.0 (RHSA-2025:2883)]	high
3/22/2025	[RHEL 8 : webkit2gtk3 (RHSA-2025:3005)]	high
3/22/2025	[RHEL 9 : thunderbird (RHSA-2025:2957)]	high
3/22/2025	[RHEL 9 : webkit2gtk3 (RHSA-2025:3001)]	high
3/22/2025	[RHEL 8 : tigervnc (RHSA-2025:2880)]	high
3/22/2025	[RHEL 9 : thunderbird (RHSA-2025:2899)]	high
3/22/2025	[RHEL 8 : webkit2gtk3 (RHSA-2025:2863)]	high
3/22/2025	[RHEL 8 : kpatch-patch-4_18_0-553, kpatch-patch-4_18_0-553_16_1, kpatch-patch-4_18_0-553_30_1, and kpatch-patch-4_18_0-553_40_1 (RHSA-2025:3049)]	high
3/22/2025	[RHEL 8 : postgresql:12 (RHSA-2025:3050)]	high

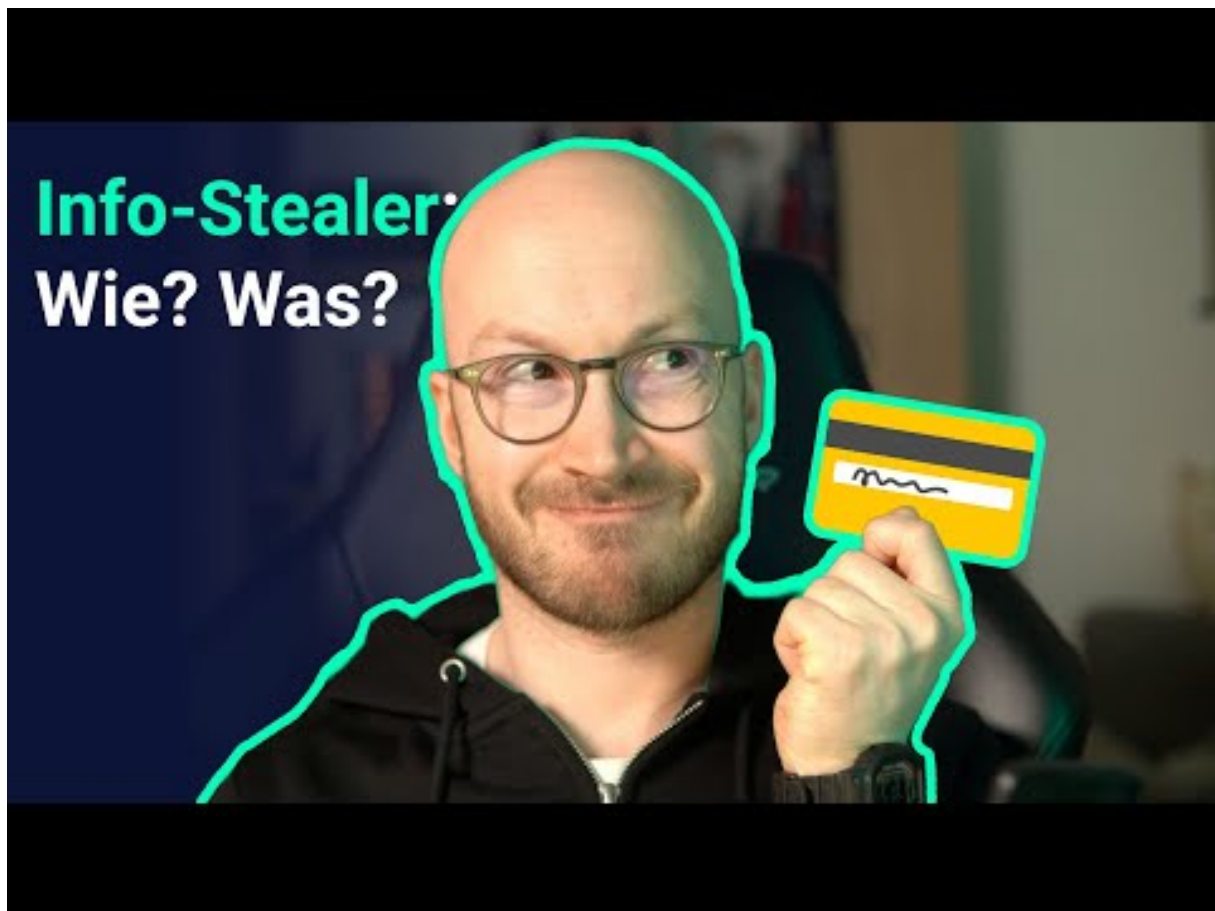
Datum	Schwachstelle	Bewertung
3/22/2025	[RHEL 9 : kpatch-patch-5_14_0-427_13_1, kpatch-patch-5_14_0-427_31_1, kpatch-patch-5_14_0-427_44_1, and kpatch-patch-5_14_0-427_55_1 (RHSA-2025:3097)]	high
3/22/2025	[RHEL 9 : tigervnc (RHSA-2025:2873)]	high
3/22/2025	[RHEL 8 : thunderbird (RHSA-2025:2900)]	high
3/22/2025	[RHEL 8 : webkit2gtk3 (RHSA-2025:2998)]	high
3/22/2025	[RHEL 8 : kernel (RHSA-2025:3026)]	high
3/22/2025	[RHEL 8 : postgresql:12 (RHSA-2025:3063)]	high
3/22/2025	[RHEL 9 : thunderbird (RHSA-2025:3013)]	high
3/22/2025	[RHEL 9 : grub2 (RHSA-2025:2869)]	high
3/22/2025	[RHEL 8 / 9 : OpenShift Container Platform 4.14.49 (RHSA-2025:2712)]	high
3/22/2025	[RHEL 8 : tigervnc (RHSA-2025:2865)]	high
3/22/2025	[RHEL 8 : thunderbird (RHSA-2025:3009)]	high
3/22/2025	[RHEL 8 : postgresql:12 (RHSA-2025:3082)]	high
3/22/2025	[RHEL 8 : pcs (RHSA-2025:2956)]	high
3/22/2025	[RHEL 9 : kpatch-patch-5_14_0-284_104_1, kpatch-patch-5_14_0-284_52_1, kpatch-patch-5_14_0-284_79_1, and kpatch-patch-5_14_0-284_92_1 (RHSA-2025:3096)]	high
3/22/2025	[RHEL 8 : mysql:8.0 (RHSA-2025:2882)]	high
3/22/2025	[RHEL 9 : webkit2gtk3 (RHSA-2025:3000)]	high
3/22/2025	[RHEL 8 / 9 : OpenShift Container Platform 4.13.56 (RHSA-2025:2703)]	high
3/22/2025	[RHEL 8 : kernel-rt (RHSA-2025:3027)]	high
3/22/2025	[RHEL 7 : tigervnc (RHSA-2025:2861)]	high

Datum	Schwachstelle	Bewertung
3/22/2025	[RHEL 8 : kpatch-patch-4_18_0-477_43_1, kpatch-patch-4_18_0-477_67_1, kpatch-patch-4_18_0-477_81_1, and kpatch-patch-4_18_0-477_89_1 (RHSA-2025:3094)]	high
3/22/2025	[RHEL 8 : thunderbird (RHSA-2025:3036)]	high
3/22/2025	[RHEL 8 : postgresql:12 (RHSA-2025:3062)]	high
3/22/2025	[RHEL 9 : thunderbird (RHSA-2025:2959)]	high
3/22/2025	[RHEL 8 : tigervnc (RHSA-2025:2862)]	high
3/22/2025	[RHEL 9 : tigervnc (RHSA-2025:2875)]	high
3/22/2025	[RHEL 7 : xorg-x11-server (RHSA-2025:2879)]	high
3/22/2025	[RHEL 8 : pcs (RHSA-2025:2955)]	high
3/22/2025	[RHEL 8 : postgresql:12 (RHSA-2025:3064)]	high
3/22/2025	[RHEL 8 : webkit2gtk3 (RHSA-2025:3034)]	high
3/22/2025	[RHEL 8 : thunderbird (RHSA-2025:2958)]	high
3/22/2025	[RHEL 9 : kpatch-patch-5_14_0-503_15_1 and kpatch-patch-5_14_0-503_26_1 (RHSA-2025:3048)]	high
3/22/2025	[RHEL 8 : pcs (RHSA-2025:2872)]	high
3/22/2025	[RHEL 8 : tigervnc (RHSA-2025:2866)]	high

4 Die Hacks der Woche

mit Martin Haunschmid

4.0.1 Information Stealer. Wie funktionieren sie?



[Zum Youtube Video](#)

5 Cyberangriffe: (Mär)

Datum	Opfer	Land	Information
2025-03-20	DHR Health	[USA]	Link
2025-03-20	Water and Sewerage Corporation	[BHS]	Link
2025-03-19	North Shore Health Network	[CAN]	Link
2025-03-17	Keding Enterprises Co., Ltd.	[TWN]	Link
2025-03-17	Sozialholding der Stadt Mönchengladbach	[DEU]	Link
2025-03-17	Virgin Islands Lottery (VIL)	[VIR]	Link
2025-03-16	Mairie de Kirkel	[DEU]	Link
2025-03-16	Atchison County	[USA]	Link
2025-03-16	Ascom	[CHE]	Link
2025-03-16	James Pascoe	[NZL]	Link
2025-03-15	Strafford County	[USA]	Link
2025-03-15	Cerballiance	[FRA]	Link
2025-03-14	Spar Gruppe Schweiz	[CHE]	Link
2025-03-13	Mairie de Murça	[PRT]	Link
2025-03-13	Pelham School District	[USA]	Link
2025-03-12	Edesur Dominicana	[DOM]	Link
2025-03-12	Prefeitura Municipal de Palmeira	[BRA]	Link
2025-03-11	YAP Health Services	[FSM]	Link
2025-03-11	Derby Police Department	[USA]	Link
2025-03-09	Aerticket	[DEU]	Link
2025-03-07	Crystal D	[USA]	Link
2025-03-06	Bikur Rofeh	[ISR]	Link
2025-03-05	Ålands Centralandelslag (ÅCA)	[FIN]	Link
2025-03-05	Endless Mountains Health Systems (EMHS)	[USA]	Link
2025-03-05	Fachhochschule Nordwestschweiz	[CHE]	Link
2025-03-05	St Albert the Great College	[MLT]	Link

Datum	Opfer	Land	Information
2025-03-04	Unikorn Semiconductor Corp.	[TWN]	Link
2025-03-04	Stadtwerke Schwerte	[DEU]	Link
2025-03-04	Adina Hotels	[AUS]	Link
2025-03-03	Whitman Hospital and Medical Clinics	[USA]	Link
2025-03-03	Mission, Texas	[USA]	Link
2025-03-03	Brucha	[AUT]	Link
2025-03-03	Vranken-Pommery Monopole	[FRA]	Link
2025-03-02	HomeTeamNS	[SGP]	Link
2025-03-02	POLSA (Polish Space Agency)	[POL]	Link
2025-03-02	Adval Tech Group	[CHE]	Link
2025-03-02	Penn-Harris-Madison school district	[USA]	Link
2025-03-02	Ivinhema	[BRA]	Link
2025-03-02	Berkeley Research Group (BRG)	[USA]	Link
2025-03-01	National Presto Industries, Inc.	[USA]	Link
2025-03-01	TFE Hotels	[AUS]	Link

6 Ransomware-Erpressungen: (Mär)

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-22	[Doumen]	lynx	Link
2025-03-22	[MinebeaMitsumi Inc]	cicada3301	Link
2025-03-22	[Goshen Medical Center]	bianlian	Link
2025-03-22	[REOC San Antonio]	play	Link
2025-03-22	[Zaveta Custom Homes]	play	Link
2025-03-17	[Yadea Group Holdings Ltd]	dragonforce	Link
2025-03-20	[Colemanmaterials]	dragonforce	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-21	[Advance Tapes International]	medusa	Link
2025-03-22	[SPARSH Hospital]	killsec	Link
2025-03-22	[Innovative Surfaces]	killsec	Link
2025-03-22	[Synesis Surveillance System]	babuk2	Link
2025-03-22	[inmarsat.com]	babuk2	Link
2025-03-22	[jp-property.com]	babuk2	Link
2025-03-22	[Aztec Municipal School District]	interlock	Link
2025-03-22	[compassionhealthcare.org]	safepay	Link
2025-03-20	[gbsn.com.br]	ransomhub	Link
2025-03-21	[armetal.com]	babuk2	Link
2025-03-21	[www.scpautomation.com]	ransomhub	Link
2025-03-21	[www.gestionquintessence.com]	ransomhub	Link
2025-03-21	[www.engines.man.eu]	ransomhub	Link
2025-03-21	[www.abmenviro.ca]	ransomhub	Link
2025-03-21	[www.ahmadiyya.ca]	ransomhub	Link
2025-03-21	[www.elizajennings.org]	ransomhub	Link
2025-03-21	[www.sinkdirect.com]	ransomhub	Link
2025-03-06	[www.broadmoormethodist.org]	ransomhub	Link
2025-03-13	[www.parklandmanufacturing.com]	ransomhub	Link
2025-03-15	[www.solinst.com]	ransomhub	Link
2025-03-21	[www.allstarhealthcaresolutions.com]	ransomhub	Link
2025-03-07	[www.njcalwe.com]	ransomhub	Link
2025-03-09	[www.gcsnet.com]	ransomhub	Link
2025-03-21	[www.core-1.com]	ransomhub	Link
2025-03-06	[www.esquirebrands.com]	ransomhub	Link
2025-03-21	[www.avalonapparel.com]	ransomhub	Link
2025-03-10	[www.oneupinnovations.com]	ransomhub	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-21	[Cayman National Bank]	killsec	Link
2025-03-21	[bellendorf.de]	incransom	Link
2025-03-21	[Officio Medical]	killsec	Link
2025-03-21	[CS Plastics]	akira	Link
2025-03-21	[Subsurfco LLC]	qilin	Link
2025-03-21	[The Ticktin Law Group]	babuk2	Link
2025-03-21	[Mpaj.gov.my]	babuk2	Link
2025-03-21	[exostar.com TOP Defense AS]	babuk2	Link
2025-03-21	[Standard Capital Securities (Pvt) Backoffice - Pakistan Stock Market Data Vault]	babuk2	Link
2025-03-17	[www.mslglobalexp.com]	ransomhub	Link
2025-03-20	[mohrss.gov.cn (Ministry of Human Resources and Social Security)]	babuk2	Link
2025-03-20	[amazon.com]	babuk2	Link
2025-03-18	[L&S Mechanical]	spacebears	Link
2025-03-02	[Whittaker & Company]	spacebears	Link
2025-03-20	[www.janvier-labs.com]	ransomhub	Link
2025-03-17	[National Safety Council]	medusa	Link
2025-03-17	[Augusta Industrial Services, Inc.]	medusa	Link
2025-03-19	[Champions Group]	medusa	Link
2025-03-19	[J McCann & Co Ltd]	medusa	Link
2025-03-19	[Big Horn County School District #4]	medusa	Link
2025-03-20	[Obra Play]	killsec	Link
2025-03-20	[interiseworld.com]	killsec	Link
2025-03-20	[Instituto de Ojos]	killsec	Link
2025-03-20	[Oag.state.va.us]	cloak	Link
2025-03-20	[Wr-recht.de]	cloak	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-20	[Baltimorecityschools]	cloak	Link
2025-03-20	[Land Planners]	akira	Link
2025-03-20	[Auren]	akira	Link
2025-03-20	[Newtown Friends School (newtownfriends.org)]	fog	Link
2025-03-20	[fr.sodexo.com]	babuk2	Link
2025-03-20	[Corporate access, up to Shipping Apps in QATAR]	babuk2	Link
2025-03-20	[woqod.com]	babuk2	Link
2025-03-20	[mof.go.th - Ministry of Finance (Thailand)]	babuk2	Link
2025-03-20	[ZB ZIMMERMANN UND BECKER GmbH]	akira	Link
2025-03-20	[Cargills Bank]	hunters	Link
2025-03-20	[Luff Industries]	qilin	Link
2025-03-20	[Megacentro]	hunters	Link
2025-03-20	[smic.mi.th (Thailand Intelligence Agency)]	babuk2	Link
2025-03-20	[www.kvhealth.net]	kraken	Link
2025-03-19	[www.gob.ve]	babuk2	Link
2025-03-19	[Access Panel Financial Technology Company (Thailand)]	babuk2	Link
2025-03-19	[United States County Palm Beach Government]	babuk2	Link
2025-03-19	[Municipal taxation Secretariat Access - Brazil Government]	babuk2	Link
2025-03-19	[Intelligence Bureau of the Joint Staff Department of the Central Military Commission...]	babuk2	Link
2025-03-19	[rac.gov.my]	babuk2	Link
2025-03-19	[nimapinfotech.com]	babuk2	Link
2025-03-17	[controlledair.com]	ransomhub	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-19	[Q railing]	play	Link
2025-03-19	[www.medsrx.com]	VanHelsing	Link
2025-03-07	[Los Madroños Hospital]	qilin	Link
2025-03-19	[The Ely Company, Inc.]	akira	Link
2025-03-19	[Machu Picchu Foods]	akira	Link
2025-03-19	[LINC Systems]	akira	Link
2025-03-19	[VEST LLC]	akira	Link
2025-03-19	[Palomino Petroleum]	lynx	Link
2025-03-18	[warmsworth.doncaster.sch.uk]	incransom	Link
2025-03-19	[CD]	monti	Link
2025-03-19	[Gloria Cales]	monti	Link
2025-03-18	[newhollandwood.com]	incransom	Link
2025-03-18	[Coopertruni]	arcusmedia	Link
2025-03-18	[THX Transport]	arcusmedia	Link
2025-03-18	[Kiribati Government]	arcusmedia	Link
2025-03-18	[Atos-racks.com]	VanHelsing	Link
2025-03-18	[AMICIO]	lynx	Link
2025-03-18	[Ted Hosmer Enterprises]	rhysida	Link
2025-03-18	[51talk.com]	lockbit3	Link
2025-03-18	[esaote.com]	babuk2	Link
2025-03-18	[nstda.or.th]	babuk2	Link
2025-03-18	[pajak.go.id]	babuk2	Link
2025-03-18	[dukcapil.kemendagri.go.id (SIK DUKCAPIL MINISTRY OF HOME AFFAIRS OF INDONESIA)]	babuk2	Link
2025-03-18	[semaphore.asso.fr]	funksec	Link
2025-03-13	[PTS Group]	qilin	Link
2025-03-18	[whitecapcanada.com]	babuk2	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-18	[JAMEL CONTAINERS LLC]	akira	Link
2025-03-18	[Cleveland Municipal Court]	qilin	Link
2025-03-18	[hcahealthcare.com INC.]	babuk2	Link
2025-03-18	[SAGETRA INC.]	akira	Link
2025-03-18	[gaertnerhof-jeutter.de]	incransom	Link
2025-03-18	[sp.tnitelecom.com]	babuk2	Link
2025-03-18	[Otelier.io]	babuk2	Link
2025-03-18	[expertdata.com.au]	incransom	Link
2025-03-18	[airtelligence.com]	incransom	Link
2025-03-18	[highwirepress.com]	babuk2	Link
2025-03-18	[Harcourts Prime Properties]	killsec	Link
2025-03-07	[Far East Consortium]	nightspire	Link
2025-03-16	[Bridgewater Retirement Community]	nightspire	Link
2025-03-17	[Electronics For Imaging]	hellcat	Link
2025-03-17	[www.baxterlaboratories.com]	ransomhub	Link
2025-03-17	[ccktech.com]	ransomhub	Link
2025-03-17	[Lepant Law Office]	qilin	Link
2025-03-17	[Worldlawn Power Equipment]	qilin	Link
2025-03-17	[Diode Technologies]	qilin	Link
2025-03-17	[terrell.k12.ga.us]	safepay	Link
2025-03-03	[oneill.com]	ransomhub	Link
2025-03-17	[www.jhayber.com]	ransomhub	Link
2025-03-17	[RAE (Real Academia Española) (rae.es)]	fog	Link
2025-03-17	[Solist]	akira	Link
2025-03-17	[CableVision]	hunters	Link
2025-03-12	[www.cityofbellville.com]	VanHelsing	Link
2025-03-17	[assaabloy.com]	cactus	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-17	[kyb.com]	cactus	Link
2025-03-17	[PIBOR ISO SA]	akira	Link
2025-03-17	[SMC Corporation]	qilin	Link
2025-03-17	[KIU System Solutions]	apos	Link
2025-03-17	[taobao.com]	babuk2	Link
2025-03-17	[This entry has been removed following a request from the company]	babuk2	Link
2025-03-17	[March, 6, 2025: City government office in Van (Turkey) van.bel.tr hacked. 7.4 TiB is for s...]	skira	Link
2025-03-17	[icmr.gov.in]	babuk2	Link
2025-03-16	[Ministry Of Defense of the Republic Of Korea]	babuk2	Link
2025-03-16	[JD.com Inc (Chinese)]	babuk2	Link
2025-03-16	[KD Panels]	crazyhunter	Link
2025-03-16	[Kairav Chemofarbe Industries]	trinity	Link
2025-03-16	[consultoria-consultores.es]	trinity	Link
2025-03-16	[ROBONG-WINMINI]	trinity	Link
2025-03-16	[Lake Psychological Services]	trinity	Link
2025-03-16	[CANAM Realty Group]	trinity	Link
2025-03-16	[CNS]	trinity	Link
2025-03-16	[la-z-boy]	trinity	Link
2025-03-15	[sitro.com.au]	incransom	Link
2025-03-15	[www.ameda.com]	ransomhub	Link
2025-03-16	[SRP Companies (Second lock! + Company scam!)]	medusa	Link
2025-03-16	[Coldwell Banker D'Ann Harper, REALTORS]	medusa	Link
2025-03-15	[Kleen-Pak Products]	dragonforce	Link
2025-03-15	[Moncaro]	dragonforce	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-16	[DTS -services]	dragonforce	Link
2025-03-16	[Florida Department of Transportation (FDOT)]	babuk2	Link
2025-03-16	[Orange.com]	babuk2	Link
2025-03-16	[Courageous Home Care]	hunters	Link
2025-03-10	[Tanaka Electronics Taiwan Co.,LTD]	nightspire	Link
2025-03-05	[Waihong Environmental Services Limited]	nightspire	Link
2025-03-12	[Wilson Re Limited]	nightspire	Link
2025-03-16	[MESS sales srl]	sarcoma	Link
2025-03-15	[Ascom Holding AG]	hellcat	Link
2025-03-15	[Ricardo Rodriguez]	qilin	Link
2025-03-15	[Belarus E-commerce & Energy Data]	babuk2	Link
2025-03-15	[nrru.ac.th - University]	babuk2	Link
2025-03-14	[yeanshalle.de]	incransom	Link
2025-03-14	[Perrigo Company]	termite	Link
2025-03-14	[Fulcrum Lifting]	lynx	Link
2025-03-14	[argusdatainsights.de]	safepay	Link
2025-03-14	[idcconstruction.com]	ransomhub	Link
2025-03-14	[Domina Entrega Total]	akira	Link
2025-03-14	[jennyoo.com]	ransomhub	Link
2025-03-14	[Unicorr Packaging Group]	akira	Link
2025-03-14	[iaai.com - Washington DC DMV]	babuk2	Link
2025-03-14	[Indiv Usa]	lynx	Link
2025-03-14	[Tryon]	lynx	Link
2025-03-14	[The Ministry of National Defense - mod.gov.vn (NavyVietnam)]	babuk2	Link
2025-03-14	[movistar.com.pe]	babuk2	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-14	[JAGGEDPEAK.COM]	clon	Link
2025-03-14	[RACKSPACE.COM]	clon	Link
2025-03-14	[LIPPERTENT.COM]	clon	Link
2025-03-14	[GARANIMALS.COM]	clon	Link
2025-03-13	[Portland Street Honda]	medusa	Link
2025-03-13	[Karen S Pouliot]	medusa	Link
2025-03-14	[mdm-insurance.com]	abyss	Link
2025-03-14	[Cothron's Security Professionals]	rhysida	Link
2025-03-13	[www.raymond.in]	ransomhub	Link
2025-03-13	[dtrglaw.com]	ransomhub	Link
2025-03-12	[rixos.com]	embargo	Link
2025-03-13	[Taiwan - Mackay Hospital]	babuk2	Link
2025-03-13	[cch.org.tw - Changhua Christian Hospital]	babuk2	Link
2025-03-13	[nuclep.gov.br. Nuclep Brazil]	babuk2	Link
2025-03-14	[parliament.iq]	babuk2	Link
2025-03-14	[web.asia.edu.tw - Taiwan (Asia University)]	babuk2	Link
2025-03-14	[Intelligence Bureau of the Joint Staff Department of the Central Military Commission China]	babuk2	Link
2025-03-14	[Indian military and government defense 20TB]	babuk2	Link
2025-03-13	[fstlogistics.com]	lynx	Link
2025-03-13	[Harrells.com]	lynx	Link
2025-03-13	[SL Tennessee Information]	play	Link
2025-03-13	[Backes]	play	Link
2025-03-13	[Best Cheer Stone]	play	Link
2025-03-14	[Terralogic]	secp0	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-13	[University Diagnostic Medical Imaging, PC (udmi.net)]	fog	Link
2025-03-12	[El Camino Real Academy (elcaminorealacademy)]	fog	Link
2025-03-13	[Iraqi Ministry of Finance]	babuk2	Link
2025-03-13	[Iraqi Council of Ministers]	babuk2	Link
2025-03-12	[Ascoma Group]	akira	Link
2025-03-03	[Raja Ferry Port Public Company Limited]	nightspire	Link
2025-03-08	[Far East Consortium International Limited]	nightspire	Link
2025-03-03	[Business Ledger Limited]	nightspire	Link
2025-03-01	[Tohpe Corporation]	nightspire	Link
2025-03-12	[Hydro-Vacuum S.A.]	nightspire	Link
2025-03-12	[marinabaysands.com - Singapore Hotel (Internal Server)]	babuk2	Link
2025-03-12	[Yushin America, Inc]	qilin	Link
2025-03-12	[PACOMARTINEZ]	akira	Link
2025-03-12	[SMG Bahamas]	akira	Link
2025-03-12	[extremepperformance.com]	funksec	Link
2025-03-12	[hitekgroup.in india Finance]	babuk2	Link
2025-03-12	[Industrial Acceptance Corporation]	akira	Link
2025-03-12	[baillie.com]	cactus	Link
2025-03-12	[CAHOKIA CUSD 187 SCHOOL DISTRICT]	qilin	Link
2025-03-12	[India's telecommunication network]	babuk2	Link
2025-03-12	[Best Telecom Laos]	akira	Link
2025-03-12	[CNQC]	akira	Link
2025-03-12	[Peerless Food Equipment]	akira	Link
2025-03-12	[Helmut Hölbling Spedition GmbH]	akira	Link
2025-03-12	[www.visualisation.one]	ransomhub	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-12	[HYPONAMIRU]	arcusmedia	Link
2025-03-12	[HYPERNOVA TELECOM]	arcusmedia	Link
2025-03-12	[unimore.it]	funksec	Link
2025-03-12	[Baykar Turkish defense company C4I and artificial intelligence]	babuk2	Link
2025-03-11	[tradingacademy.com]	safepay	Link
2025-03-11	[ultimateclasslimo.com]	safepay	Link
2025-03-11	[havenresorts.com]	safepay	Link
2025-03-11	[lgipr.com]	safepay	Link
2025-03-11	[jockeysalud.com.pe]	safepay	Link
2025-03-11	[motomecanica.com]	safepay	Link
2025-03-11	[cali.losolivos.co]	safepay	Link
2025-03-11	[Skyward Specialty Insurance]	killsec	Link
2025-03-11	[Trymata]	killsec	Link
2025-03-03	[Gaines County, Texas]	qilin	Link
2025-03-11	[Springfield Water and Sewer Commission]	lynx	Link
2025-03-11	[Suder&Suder]	qilin	Link
2025-03-11	[Longue Vue Club]	lynx	Link
2025-03-11	[Taking stock of February 2025]	akira	Link
2025-03-11	[WAUGH & GOODWIN, LLP]	akira	Link
2025-03-11	[airexplore.aero Company]	babuk2	Link
2025-03-11	[Veristat]	akira	Link
2025-03-11	[Edesur Dominicana]	hunters	Link
2025-03-11	[All4Labels - Global Packaging Group]	akira	Link
2025-03-11	[Essex County OB/GYN Associates]	incransom	Link
2025-03-11	[Princeton Hydro]	akira	Link
2025-03-11	[isee-eg.com]	funksec	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-11	[fnnde.gov.br brazilian government]	babuk2	Link
2025-03-11	[wapda.gov.pk]	babuk2	Link
2025-03-11	[lexmark.com Company]	babuk2	Link
2025-03-10	[Wilkinson Rogers (wilkinsonrogers.com)]	fog	Link
2025-03-11	[forvismazars.com.fr (mazars.fr)]	babuk2	Link
2025-03-10	[Magnolia Manor (magnoliamanor.com)]	fog	Link
2025-03-10	[petstop.com Company]	babuk2	Link
2025-03-10	[misaludhealth.com]	babuk2	Link
2025-03-10	[bank.pingan.com (CN)]	babuk2	Link
2025-03-10	[Access to Indian Ministry of Defence and Military Secret (DRDO) documents By Babuk Locker ...]	babuk2	Link
2025-03-10	[fredsalvuccicorp.com]	kairos	Link
2025-03-10	[Mandarin.com.br]	babuk2	Link
2025-03-10	[Callico Distributors, Inc.]	akira	Link
2025-03-10	[Pacific Honda Company]	akira	Link
2025-03-10	[Arcusin]	akira	Link
2025-03-10	[www.hexosys.com]	ransomhub	Link
2025-03-10	[Safe-Strap Company, LLC]	akira	Link
2025-03-10	[Fickling & Company]	akira	Link
2025-03-07	[GPS 909]	akira	Link
2025-03-10	[mazars.fr]	babuk2	Link
2025-03-10	[Dacas Argentina]	qilin	Link
2025-03-05	[Cotswold Fayre]	dragonforce	Link
2025-03-05	[Vercoe Insurance Brokers]	dragonforce	Link
2025-03-05	[Steel Dynamics UK]	dragonforce	Link
2025-03-05	[E Leet Woodworking]	dragonforce	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-04	[Customer Management Systems]	medusa	Link
2025-03-06	[CPI Books]	medusa	Link
2025-03-09	[ACTi Corporation]	lynx	Link
2025-03-09	[BerksBar.org]	incransom	Link
2025-03-09	[klabs.it]	funksec	Link
2025-03-03	[Salemerode.com]	flocker	Link
2025-03-09	[State Bar of Texas (www.texasbar.com)]	incransom	Link
2025-03-09	[Greenwood Village South GVS]	incransom	Link
2025-03-07	[prelco.ca]	qilin	Link
2025-03-09	[Jerue Companies]	play	Link
2025-03-09	[Syma-System]	play	Link
2025-03-09	[Compound Solutions]	play	Link
2025-03-09	[T J Machine & Tool]	play	Link
2025-03-09	[Gevril]	play	Link
2025-03-09	[Peak Season]	play	Link
2025-03-09	[Yorke & Curtis]	play	Link
2025-03-09	[Buckley BalaWilson Mew]	play	Link
2025-03-09	[Holiday Comfort]	play	Link
2025-03-09	[Clawson Honda]	play	Link
2025-03-09	[Dectron]	play	Link
2025-03-09	[Nor Arc]	play	Link
2025-03-09	[British virgin islands London Office]	rhapsida	Link
2025-03-05	[Changhua Christian Hospital]	crazyhunter	Link
2025-03-05	[Huacheng Electric]	crazyhunter	Link
2025-03-05	[Mackay Hospital]	crazyhunter	Link
2025-03-05	[Asia University Hospital]	crazyhunter	Link
2025-03-05	[Asia University]	crazyhunter	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-06	[mitchellmcnutt.com]	ransomhub	Link
2025-03-08	[univ-rennes.fr]	funksec	Link
2025-03-05	[Tech NH]	lynx	Link
2025-03-07	[Allworx]	bianlian	Link
2025-03-07	[Minnesota Orthodontics]	bianlian	Link
2025-03-07	[REYCOTEL]	arcusmedia	Link
2025-03-07	[total-ps.com]	ransomhub	Link
2025-03-07	[Hancock Public School]	interlock	Link
2025-03-07	[lofotenseafood.com]	lynx	Link
2025-03-07	[ADDA (adda.io)]	ransomexx	Link
2025-03-07	[Swift Haulage Berhad]	akira	Link
2025-03-07	[Aj Taylor Electrical Contractors Ltd]	sarcoma	Link
2025-03-07	[Sittab INC]	akira	Link
2025-03-07	[wheats.com]	ransomhub	Link
2025-03-07	[srmg.com.au]	ransomhub	Link
2025-03-07	[sorbonne-universite.fr]	funksec	Link
2025-03-06	[RFA Decor]	akira	Link
2025-03-05	[www.portlandschools.org]	ransomhub	Link
2025-03-05	[www.hinton.ca]	ransomhub	Link
2025-03-05	[www.convention.qc.ca]	ransomhub	Link
2025-03-06	[hickorylaw.com]	ransomhub	Link
2025-03-06	[lovesac.com]	ransomhub	Link
2025-03-06	[agi.net]	monti	Link
2025-03-06	[Adval Tech]	lynx	Link
2025-03-06	[WJCC Public Schools (wjccschools.org)]	fog	Link
2025-03-06	[Connekted, Inc.]	qilin	Link
2025-03-06	[Naples Heritage Golf & Country Club]	incransom	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-06	[Ministry of Foreign Affairs of Ukraine]	qilin	Link
2025-03-06	[Oberlin Cable Co-op (oberlin.net)]	fog	Link
2025-03-06	[Elite Advanced Laser Corporation]	akira	Link
2025-03-05	[1X Internet]	fog	Link
2025-03-05	[Bizcode]	fog	Link
2025-03-05	[Manning Publications Co.]	fog	Link
2025-03-05	[Engikam]	fog	Link
2025-03-05	[FHNW]	fog	Link
2025-03-05	[Aeonsparx]	fog	Link
2025-03-05	[Flightsim studio]	fog	Link
2025-03-05	[Neopoly]	fog	Link
2025-03-05	[Kr3m]	fog	Link
2025-03-05	[InfoReach]	fog	Link
2025-03-05	[Euranova]	fog	Link
2025-03-05	[Inelmatic]	fog	Link
2025-03-05	[Kotliva]	fog	Link
2025-03-05	[Blue Planet]	fog	Link
2025-03-05	[Eumetsat]	fog	Link
2025-03-05	[Melexis]	fog	Link
2025-03-06	[City government office in Van (Turkey) - van.bel.tr]	skira	Link
2025-03-06	[Law Diary (USA)]	skira	Link
2025-03-06	[Carruth Compliance Consulting]	skira	Link
2025-03-06	[CCL Products India]	skira	Link
2025-03-06	[Krisala Developer (India)]	skira	Link
2025-03-05	[The 19 biggest gitlabs]	fog	Link
2025-03-05	[willms-fleisch.de]	safepay	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-05	[Pervedant]	lynx	Link
2025-03-05	[SCOLARO FETTER GRIZANTI & McGOUGH, P.C. (scolaro.com)]	fog	Link
2025-03-05	[Adrenalina]	akira	Link
2025-03-05	[Cyncly Company]	akira	Link
2025-03-05	[City Plumbing & Electric Supply Co]	akira	Link
2025-03-04	[www.sunsweet.com]	ransomhub	Link
2025-03-05	[Best Collateral, Inc.]	rhysida	Link
2025-03-04	[Chicago Doorways, LLC]	qilin	Link
2025-03-05	[Schmiedetechnik Plettenberg GmbH & Co KG]	lynx	Link
2025-03-04	[365labs - Security Corp]	monti	Link
2025-03-04	[PFS Grupo - Plan de igualdad, Sostenibilidad]	qilin	Link
2025-03-04	[Pampili (pampili.com.br)]	fog	Link
2025-03-04	[Keystone Pacific Property Management LLC]	bianlian	Link
2025-03-04	[Mosley Glick O'Brien, Inc.]	bianlian	Link
2025-03-04	[FANTIN group]	akira	Link
2025-03-04	[Grupo Baston Aerosol (baston.com.br)]	fog	Link
2025-03-04	[Ray Fogg Corporate Properties]	akira	Link
2025-03-04	[goencon.com]	ransomhub	Link
2025-03-04	[Seabank Group]	lynx	Link
2025-03-04	[Tata Technologies]	hunters	Link
2025-03-04	[Wendy Wu Tours]	killsec	Link
2025-03-04	[rockhillwc.com]	qilin	Link
2025-03-04	[bpmmicro.com]	qilin	Link
2025-03-04	[peruzzi.com]	qilin	Link
2025-03-04	[IOVATE.COM]	clop	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-04	[Legal Aid Society of Salt Lake]	bianlian	Link
2025-03-04	[Ewald Consulting]	bianlian	Link
2025-03-04	[Netcom-World]	apos	Link
2025-03-04	[InternetWay]	apos	Link
2025-03-04	[cimenyan.desa.id]	funksec	Link
2025-03-03	[familychc.com]	ransomhub	Link
2025-03-03	[andreyevengineering.com]	ransomhub	Link
2025-03-03	[drvitenas.com]	kairos	Link
2025-03-03	[usarice.com]	kairos	Link
2025-03-03	[Sunnking SustainableSolutions]	akira	Link
2025-03-03	[LINKGROUP]	arcusmedia	Link
2025-03-03	[Openreso]	arcusmedia	Link
2025-03-03	[Itapeseg]	arcusmedia	Link
2025-03-03	[logic insectes]	arcusmedia	Link
2025-03-03	[RJ IT Solutions]	arcusmedia	Link
2025-03-03	[Grafitec]	arcusmedia	Link
2025-03-03	[synaptic.co.tz]	arcusmedia	Link
2025-03-03	[quigleyeye.com]	cactus	Link
2025-03-03	[La Unión]	lynx	Link
2025-03-03	[Central McGowan (centralmcgowan.com)]	fog	Link
2025-03-03	[Klesk Metal Stamping Co (kleskmetalstamping.com)]	fog	Link
2025-03-03	[Forstenlechner Installationstechnik]	akira	Link
2025-03-03	[ceratec.com]	abyss	Link
2025-03-02	[Pre Con Industries]	play	Link
2025-03-02	[IT-IQ Botswana]	play	Link
2025-03-02	[North American Fire Hose]	play	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-03-02	[Couri Insurance Agency]	play	Link
2025-03-02	[Optometrics]	play	Link
2025-03-02	[International Process Plants]	play	Link
2025-03-02	[Ganong Bros]	play	Link
2025-03-02	[FM.GOB.AR]	monti	Link
2025-03-02	[Bell Ambulance]	medusa	Link
2025-03-02	[Workforce Group]	killsec	Link
2025-03-01	[germancentre.sg]	incransom	Link
2025-03-01	[JEFFREYCOURT.COM]	clop	Link
2025-03-01	[APTEAN.COM]	clop	Link
2025-03-01	[Wayne County, Michigan]	interlock	Link
2025-03-01	[The Smeg Group]	interlock	Link
2025-03-01	[Newton & Associates, Inc]	rhysida	Link

7 Quellen

7.1 Quellenverzeichnis

- 1) Cyberwatch - <https://github.com/Casualtek/Cyberwatch>
- 2) Ransomware.live - <https://data.ransomware.live>
- 3) Heise Security Alerts! - <https://www.heise.de/security/alerts/>
- 4) First EPSS - <https://www.first.org/epss/>
- 5) BSI WID - <https://wid.cert-bund.de/>
- 6) Tenable Plugins - <https://www.tenable.com/plugins/>
- 7) Exploit - packetstormsecurity.com
- 8) 0-Day - <https://www.zerodayinitiative.com/rss/published/>
- 9) Die Hacks der Woche - <https://martinhaunschmid.com/videos>

8 Impressum



Herausgeber:

Marlon Hübner
Brückenstraße 3
57629 Höchstenbach

E-Mail

info@cyberwald.com

Cyberwald ist ein privates, nicht-kommerzielles Projekt zur Förderung des Bewusstseins für Cybersicherheit.