
Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20250421



Inhaltsverzeichnis

1 Editorial	2
2 Security-News	3
2.1 Heise - Security-Alert	3
3 Sicherheitslücken	4
3.1 EPSS	4
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit	5
3.2 BSI - Warn- und Informationsdienst (WID)	9
3.3 Sicherheitslücken Meldungen von Tenable	12
4 Die Hacks der Woche	14
4.0.1 Information Stealer. Wie funktionieren sie?	14
5 Cyberangriffe: (Apr)	15
6 Ransomware-Erpressungen: (Apr)	16
7 Quellen	28
7.1 Quellenverzeichnis	28
8 Impressum	29

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

Atlassian stopft hochriskante Lecks in Confluence, Jira & Co.

Atlassian hat Sicherheitsupdates für Bamboo, Confluence und Jira veröffentlicht. Sie dichten als hohes Risiko eingestufte Lücken.

- [Link](#)

—

Sonicwall SMA100: Angreifer missbrauchen alte Sicherheitslücke

Derzeit finden Angriffe auf alte Sicherheitslücken in Sonicwalls Firmware für Geräte der SMA100-Baureihen statt.

- [Link](#)

—

Gezielte Angriffe auf iPhones: Apple patcht Betriebssysteme außerhalb der Reihe

Die Updates sollen zwei Zero-Day-Lücken beseitigen, die offenbar für gezielte Angriffe genutzt wurden. Auch ein CarPlay-Problem geht Apple an.

- [Link](#)

—

Notfallupdate für anonymisierendes Linux Tails

Die Tails-Maintainer haben das Notfallupdate auf Version 6.14.2 veröffentlicht. Sie schließen darin Sicherheitslücken.

- [Link](#)

—

Webbrowser: Kritische Sicherheitslücke in Chrome abgedichtet

Google stopft ein als kritisches Risiko eingestuftes Sicherheitsleck im Webbrowser Chrome. Nutzer sollten zügig aktualisieren.

- [Link](#)

—

Updates von Oracle: 378 Security-Patches aber nichts zum Einbruch in die Cloud

Im Rahmen des regelmäßigen Update-Zyklus liefert Oracle Patches satt für fast die gesamte Produktpalette, die die Kunden zügig installieren sollten.

- [Link](#)

—

14.000 Fortinet-Firewalls kompromittiert: Angreifer nisten sich ein

Mehr als 14.000 Fortinet-Firewalls sind derzeit von Angreifern kompromittiert. Die verankern sich mit Symlinks im System.

- [Link](#)

100.000 Wordpress-Seiten in Gefahr: Angriffe auf SureTriggers-Plug-in laufen

Das Plug-in SureTriggers ist auf 100.000 Wordpress-Instanzen installiert. Kurze Zeit nach Bekanntwerden eines Sicherheitslecks laufen Angriffe.

- [Link](#)

Netzwerkgeräte mit Arista EOS können Verschlüsselung vergessen

Unter bestimmten Bedingungen versenden Netzwerkgeräte mit Arista EOS Daten im Klartext, die eigentlich verschlüsselt sein sollen.

- [Link](#)

***** Root-Lücken in Siemens Sentron 7KT PAC1260 Data Manager bleiben offen*****

Weil der Support für ein Siemens Mehrkanal-Strommessgerät ausgelaufen ist, gibt es keine Sicherheitsupdates mehr.

- [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-2025-29927	0.914160000	0.996250000	Link
CVE-2025-24813	0.924620000	0.997080000	Link
CVE-2025-0282	0.920990000	0.996780000	Link
CVE-2025-0108	0.937380000	0.998350000	Link
CVE-2024-9989	0.911880000	0.996070000	Link
CVE-2024-9935	0.928150000	0.997370000	Link
CVE-2024-9474	0.942830000	0.999250000	Link
CVE-2024-9465	0.942440000	0.999150000	Link
CVE-2024-9463	0.942590000	0.999200000	Link
CVE-2024-9264	0.923200000	0.996960000	Link
CVE-2024-9234	0.925020000	0.997130000	Link
CVE-2024-9047	0.914320000	0.996260000	Link
CVE-2024-9014	0.923220000	0.996970000	Link
CVE-2024-8963	0.943450000	0.999440000	Link
CVE-2024-8856	0.907730000	0.995800000	Link
CVE-2024-8517	0.910620000	0.995990000	Link
CVE-2024-8504	0.923140000	0.996950000	Link
CVE-2024-8503	0.930440000	0.997640000	Link
CVE-2024-8190	0.933930000	0.997990000	Link
CVE-2024-7954	0.939410000	0.998660000	Link
CVE-2024-7928	0.914030000	0.996230000	Link
CVE-2024-7593	0.943990000	0.999690000	Link
CVE-2024-7120	0.912160000	0.996080000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-6911	0.927560000	0.997330000	Link
CVE-2024-6782	0.937140000	0.998300000	Link
CVE-2024-6781	0.932170000	0.997820000	Link
CVE-2024-6670	0.944670000	0.999940000	Link
CVE-2024-6646	0.915540000	0.996360000	Link
CVE-2024-5932	0.941040000	0.998910000	Link
CVE-2024-5910	0.904040000	0.995550000	Link
CVE-2024-5806	0.907610000	0.995790000	Link
CVE-2024-57727	0.934600000	0.998040000	Link
CVE-2024-56145	0.918360000	0.996570000	Link
CVE-2024-55956	0.922610000	0.996900000	Link
CVE-2024-55591	0.928470000	0.997420000	Link
CVE-2024-53704	0.936090000	0.998190000	Link
CVE-2024-5217	0.941960000	0.999070000	Link
CVE-2024-51567	0.942610000	0.999200000	Link
CVE-2024-51378	0.939560000	0.998680000	Link
CVE-2024-5084	0.907680000	0.995790000	Link
CVE-2024-50623	0.939920000	0.998740000	Link
CVE-2024-50603	0.942460000	0.999150000	Link
CVE-2024-50498	0.922440000	0.996870000	Link
CVE-2024-50379	0.920560000	0.996750000	Link
CVE-2024-4956	0.939760000	0.998710000	Link
CVE-2024-48914	0.909810000	0.995940000	Link
CVE-2024-4885	0.943090000	0.999310000	Link
CVE-2024-4879	0.943360000	0.999410000	Link
CVE-2024-48307	0.909650000	0.995930000	Link
CVE-2024-48248	0.930580000	0.997670000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-47575	0.915200000	0.996320000	Link
CVE-2024-47176	0.916890000	0.996450000	Link
CVE-2024-46938	0.915900000	0.996380000	Link
CVE-2024-4577	0.943760000	0.999560000	Link
CVE-2024-45519	0.941500000	0.998980000	Link
CVE-2024-45388	0.915030000	0.996300000	Link
CVE-2024-45216	0.939010000	0.998590000	Link
CVE-2024-45195	0.941300000	0.998950000	Link
CVE-2024-4443	0.932760000	0.997880000	Link
CVE-2024-4439	0.900940000	0.995380000	Link
CVE-2024-44000	0.914660000	0.996280000	Link
CVE-2024-4358	0.942540000	0.999190000	Link
CVE-2024-43451	0.906830000	0.995740000	Link
CVE-2024-43425	0.924680000	0.997090000	Link
CVE-2024-4257	0.922930000	0.996930000	Link
CVE-2024-41713	0.939620000	0.998690000	Link
CVE-2024-41107	0.929020000	0.997480000	Link
CVE-2024-4040	0.944120000	0.999730000	Link
CVE-2024-40348	0.919180000	0.996640000	Link
CVE-2024-39914	0.926650000	0.997230000	Link
CVE-2024-38856	0.943660000	0.999520000	Link
CVE-2024-38816	0.924030000	0.997030000	Link
CVE-2024-38112	0.917790000	0.996520000	Link
CVE-2024-37032	0.917320000	0.996500000	Link
CVE-2024-36991	0.901480000	0.995420000	Link
CVE-2024-36412	0.927520000	0.997330000	Link
CVE-2024-36401	0.944180000	0.999750000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2024-36104	0.938050000	0.998470000	Link
CVE-2024-3552	0.932020000	0.997810000	Link
CVE-2024-3495	0.932990000	0.997910000	Link
CVE-2024-34470	0.932220000	0.997840000	Link
CVE-2024-34102	0.943730000	0.999550000	Link
CVE-2024-3400	0.943120000	0.999320000	Link
CVE-2024-3273	0.943830000	0.999600000	Link
CVE-2024-3272	0.938430000	0.998530000	Link
CVE-2024-32651	0.913070000	0.996140000	Link
CVE-2024-32113	0.934460000	0.998030000	Link
CVE-2024-31982	0.941010000	0.998900000	Link
CVE-2024-31851	0.914260000	0.996250000	Link
CVE-2024-31850	0.909130000	0.995890000	Link
CVE-2024-31849	0.919840000	0.996710000	Link
CVE-2024-31848	0.927370000	0.997290000	Link
CVE-2024-31750	0.926850000	0.997250000	Link
CVE-2024-3094	0.909490000	0.995910000	Link
CVE-2024-30255	0.919250000	0.996660000	Link
CVE-2024-29973	0.936960000	0.998280000	Link
CVE-2024-29972	0.915290000	0.996320000	Link
CVE-2024-29895	0.930810000	0.997690000	Link
CVE-2024-29824	0.943660000	0.999520000	Link
CVE-2024-2961	0.934720000	0.998060000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Thu, 17 Apr 2025

[UPDATE] [hoch] Google Chrome: Mehrere Schwachstellen

Ein Angreifer kann eine Schwachstelle in Google Chrome ausnutzen, um einen nicht näher spezifizierten Angriff zu starten.

- [Link](#)

—

Thu, 17 Apr 2025

[NEU] [hoch] Linux Kernel: Mehrere Schwachstellen

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

- [Link](#)

—

Thu, 17 Apr 2025

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apple iOS, Apple iPadOS und Apple macOS ausnutzen, um beliebigen Programmcode auszuführen und um Sicherheitsmechanismen zu umgehen.

- [Link](#)

—

Thu, 17 Apr 2025

[NEU] [hoch] Cisco WebEx App: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Cisco WebEx App ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Thu, 17 Apr 2025

[NEU] [hoch] PgBouncer: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen

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

- [Link](#)

—

Thu, 17 Apr 2025

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in IBM App Connect Enterprise ausnutzen, um Sicherheitsvorkehrungen zu umgehen, Informationen auszuspähen oder seine Privilegien zu eskalieren

- [Link](#)

—

Thu, 17 Apr 2025

[UPDATE] [hoch] git: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in git ausnutzen, um beliebigen Programmcode mit Benutzerrechten auszuführen oder um Daten zu manipulieren.

- [Link](#)

—

Thu, 17 Apr 2025

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erweitern, einen Denial of Service Zustand auszulösen und mehrere nicht spezifizierte Angriffe durchzuführen.

- [Link](#)

—

Thu, 17 Apr 2025

[UPDATE] [hoch] PHP: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um einen Denial of Service Angriff durchzuführen, um Sicherheitsmechanismen zu umgehen und um unbekannte Auswirkungen zu erzielen.

- [Link](#)

—

Thu, 17 Apr 2025

[UPDATE] [hoch] PHP: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um Informationen offenzulegen oder beliebigen Code auszuführen.

- [Link](#)

—

Thu, 17 Apr 2025

[UPDATE] [kritisch] PHP: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um beliebigen Programmcode auszuführen, Informationen preiszugeben und andere nicht spezifizierte Angriffe durchzuführen.

- [Link](#)

—

Thu, 17 Apr 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](#)

—

Thu, 17 Apr 2025

[UPDATE] [hoch] Apache Tomcat: Mehrere Schwachstellen

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in Apache Tomcat ausnutzen, um beliebigen Programmcode auszuführen und einen Denial-of-Service-Zustand zu erzeugen.

- [Link](#)

—

Thu, 17 Apr 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](#)

—

Thu, 17 Apr 2025

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

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

- [Link](#)

—

Thu, 17 Apr 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, 17 Apr 2025

[UPDATE] [hoch] Red Hat Enterprise Linux (Podman und Buildah): Schwachstelle ermöglicht Manipulation von Dateien

Ein lokaler Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um Dateien zu manipulieren.

- [Link](#)

—

Thu, 17 Apr 2025

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

Ein entfernter, anonymmer Angreifer kann eine Schwachstelle in PostgreSQL ausnutzen, um eine SQL

Injection durchzuführen und in der Folge beliebigen Programmcode auszuführen.

- [Link](#)

—

Thu, 17 Apr 2025

[UPDATE] [hoch] OpenSSH: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in OpenSSH ausnutzen, um kryptografische Sicherheitsvorkehrungen zu umgehen und um einen Denial of Service Zustand herbeizuführen.

- [Link](#)

—

Thu, 17 Apr 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](#)

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
4/17/2025	[Amazon Linux 2 : git (ALAS-2025-2818)]	critical
4/17/2025	[Amazon Linux 2 : goolang (ALAS-2025-2825)]	critical
4/17/2025	[Amazon Linux 2 : php (ALAS-2025-2832)]	critical
4/17/2025	[Amazon Linux 2 : ghostscript (ALAS-2025-2820)]	critical
4/17/2025	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : webkit2gtk3 (SUSE-SU-2025:1331-1)]	critical
4/17/2025	[openSUSE 15 Security Update : perl-Data-Entropy (openSUSE-SU-2025:0123-1)]	critical
4/17/2025	[Amazon Linux 2 : containerd (ALASNITRO-ENCLAVES-2025-052)]	high

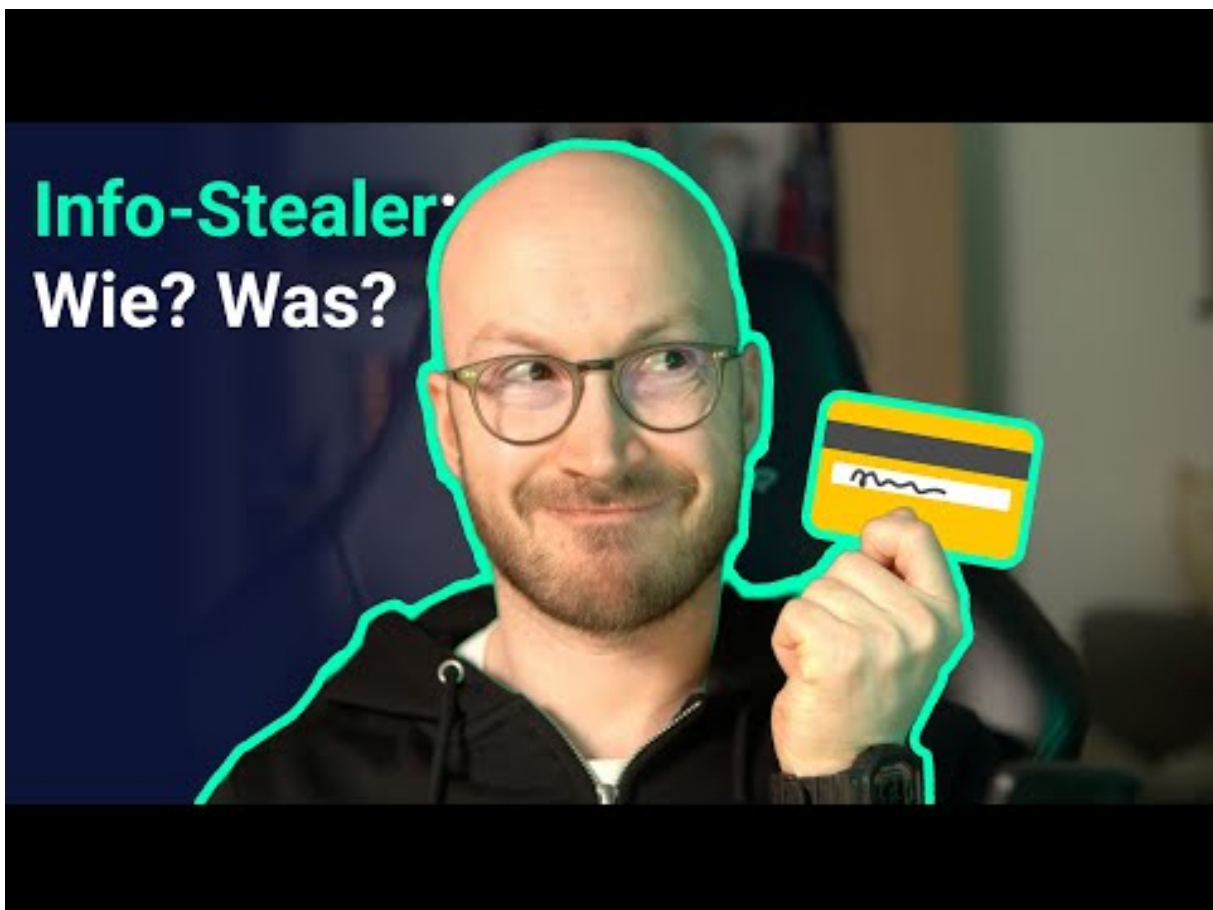
Datum	Schwachstelle	Bewertung
4/17/2025	[Amazon Linux 2023 : freetype, freetype-demos, freetype-devel (ALAS2023-2025-925)]	high
4/17/2025	[Amazon Linux 2 : kernel (ALAS-2025-2826)]	high
4/17/2025	[Amazon Linux 2 : libxslt (ALAS-2025-2823)]	high
4/17/2025	[Amazon Linux 2 : tomcat (ALAS-2025-2829)]	high
4/17/2025	[Amazon Linux 2 : docker (ALASDOCKER-2025-056)]	high
4/17/2025	[Amazon Linux 2 : nerdctl (ALAS-2025-2821)]	high
4/17/2025	[Amazon Linux 2 : containerd (ALASDOCKER-2025-055)]	high
4/17/2025	[Amazon Linux 2 : glibc (ALAS-2025-2828)]	high
4/17/2025	[Amazon Linux 2 : docker (ALASNITRO-ENCLAVES-2025-053)]	high
4/17/2025	[Amazon Linux 2 : kernel (ALASKERNEL-5.10-2025-088)]	high
4/17/2025	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : rubygem-bundler (SUSE-SU-2025:1294-1)]	high
4/17/2025	[SUSE SLED15 / SLES15 Security Update : pgadmin4 (SUSE-SU-2025:1326-1)]	high
4/17/2025	[SUSE SLES15 Security Update : apache2-mod_auth_openidc (SUSE-SU-2025:1324-1)]	high
4/17/2025	[SUSE SLES12 Security Update : expat (SUSE-SU-2025:1295-1)]	high
4/17/2025	[SUSE SLES12 Security Update : kernel (SUSE-SU-2025:1293-1)]	high
4/17/2025	[Oracle VM VirtualBox (April 2025 CPU)]	high
4/17/2025	[Oracle Application Testing Suite (April 2025 CPU)]	high
4/17/2025	[Photon OS 4.0: Erlang PHSA-2025-4.0-0782]	high
4/17/2025	[Oracle Primavera Gateway (Apr 2025 CPU)]	high
4/17/2025	[Oracle Linux 7 : libreoffice (ELSA-2025-3390)]	high
4/17/2025	[Oracle Coherence (April 2025 CPU)]	high
4/17/2025	[Oracle E-Business Suite (April 2025 CPU)]	high

Datum	Schwachstelle	Bewertung
4/17/2025	[Oracle Business Intelligence Publisher 7.6 (OAS) (April 2025 CPU)]	high
4/17/2025	[Oracle Solaris Critical Patch Update : apr2025_SRU11_4_78_189_2]	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
2025-04-18	Groupe INDIGO	[FRA]	Link
2025-04-17	William Buck	[AUS]	Link
2025-04-17	Service public de Wallonie	[BEL]	Link
2025-04-17	Limestone District School Board	[CAN]	Link
2025-04-17	Centre hospitalier de Pézenas	[FRA]	Link
2025-04-17	Tokai University	[JPN]	Link
2025-04-17	Safety21	[ITA]	Link
2025-04-15	Rhône FM	[CHE]	Link
2025-04-14	Administration communale de Jemeppe-sur-Sambre	[BEL]	Link
2025-04-12	DaVita Inc.	[USA]	Link
2025-04-12	Groupe 3R	[CHE]	Link
2025-04-10	Oregon Department of Environmental Quality (DEQ)	[USA]	Link
2025-04-09	SIAPA (Sistema Intermunicipal de los Servicios de Agua Potable y Alcantarillado)	[MEX]	Link
2025-04-09	Nippon Life India Asset Management Limited	[IND]	Link
2025-04-09	Bertie County Schools	[USA]	Link
2025-04-08	Visionary Holdings Inc.	[CAN]	Link
2025-04-07	Sensata Technologies	[USA]	Link
2025-04-06	Toppan Next Tech (TNT)	[SGP]	Link
2025-04-06	Fall River Public Schools	[USA]	Link
2025-04-05	Optimax Technology	[TWN]	Link
2025-04-03	Manchester Credit Union	[GBR]	Link

Datum	Opfer	Land	Information
2025-04-02	Bureau du défenseur public fédéral de l'Arizona	[USA]	Link

6 Ransomware-Erpressungen: (Apr)

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-15	[Accueil - Site Officiel de la commune d'Ardon]	nightspire	Link
2025-04-19	[The Michelson Organization]	qilin	Link
2025-04-20	[Premier Meats South Africa]	devman	Link
2025-04-20	[Feel Four]	devman	Link
2025-04-20	[Singapour Victim]	devman	Link
2025-04-20	[Honk Kong Victim]	devman	Link
2025-04-20	[China Harbour Engineeiring Company]	devman	Link
2025-04-16	[Iris ID]	dragonforce	Link
2025-04-16	[City of Grove]	dragonforce	Link
2025-04-16	[Lithium Americas Nevada]	medusa	Link
2025-04-19	[MRC de Maskinongé - district]	medusa	Link
2025-04-20	[FAKO-M Getränke]	sarcoma	Link
2025-04-13	[ChangShen Hospital, Taiwan]	nightspire	Link
2025-04-16	[bettininformatica - suporteon company]	ralord	Link
2025-04-18	[April, 18, 2025: Independent Title Agency, LLC ("ITA") (USA hacked. 932.4 GiB is for selli...)]	skira	Link
2025-04-18	[Independent Title Agency, LLC ("ITA") (USA)]	skira	Link
2025-04-18	[Agencia Browne y Espinoza]	akira	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-18	[Heinz Hammer Vertragswerkstatt (Mercedes-Benz car dealer)]	akira	Link
2025-04-15	[dhsmithco.com]	lynx	Link
2025-04-01	[[EVIDENCE PACK 2] Telecontrol]	ransomhouse	Link
2025-04-18	[Bosshard-farben.ch]	cloak	Link
2025-04-18	[Hubbard, McIlwain, & Brakefield, P.C.]	akira	Link
2025-04-18	[farma]	qilin	Link
2025-04-18	[www.monaghan.eu]	qilin	Link
2025-04-18	[Tänzer GmbH]	akira	Link
2025-04-18	[Toppan Next]	akira	Link
2025-04-18	[Global Media Group]	nitrogen	Link
2025-04-18	[Hayward Quartz Technology]	akira	Link
2025-04-14	[Wilmington Personal Injury Lawyer - DPLAW]	nightspire	Link
2025-04-11	[Compliance Consulting Group]	nightspire	Link
2025-04-04	[Mid-America POOL RENOVATION, Inc]	nightspire	Link
2025-04-17	[1sthealthinc.com]	qilin	Link
2025-04-17	[Sally B Gold]	lynx	Link
2025-04-17	[accesssmt.com]	qilin	Link
2025-04-17	[HOPI]	hunters	Link
2025-04-17	[Enflame Technology]	killsec	Link
2025-04-17	[yankeetrails.com]	qilin	Link
2025-04-17	[universalwindow.com]	qilin	Link
2025-04-17	[bertie.k12.nc.us]	qilin	Link
2025-04-17	[Kaye Lifestyle Homes]	sarcoma	Link
2025-04-17	[TRALFO Srl Trasporti e Spedizioni]	sarcoma	Link
2025-04-17	[Schultz Industries Inc.]	sarcoma	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-17	[Manchester Credit Union]	sarcoma	Link
2025-04-17	[Ju Percussion Group]	sarcoma	Link
2025-04-12	[VIÑUELAS ABOGADOS]	spacebears	Link
2025-04-15	[EVERTECH INSTRUMENTAL CO., LTD]	spacebears	Link
2025-04-16	[itec-gmbh.com]	safepay	Link
2025-04-16	[heinrich-steinhardt.de]	safepay	Link
2025-04-16	[hurst-schroeder.de]	safepay	Link
2025-04-16	[helixtools.co.uk]	safepay	Link
2025-04-16	[heilbronn.de]	safepay	Link
2025-04-16	[getriebetech.de]	safepay	Link
2025-04-16	[kirkel.de]	safepay	Link
2025-04-16	[extremefire.com.au]	safepay	Link
2025-04-16	[foerster-schwanau.de]	safepay	Link
2025-04-16	[eichele-bau.de]	safepay	Link
2025-04-16	[frapack.de]	safepay	Link
2025-04-16	[aqhch.com.cn]	lockbit3	Link
2025-04-16	[Koninklijke Ahold Delhaize N.V.]	incransom	Link
2025-04-07	[niemann.de]	safepay	Link
2025-04-16	[www.nelson.edu]	qilin	Link
2025-04-16	[Bio-Clima Service]	ralord	Link
2025-04-16	[Red Chamber]	play	Link
2025-04-16	[d-line-it.com]	kairos	Link
2025-04-16	[Lamberti Group]	akira	Link
2025-04-16	[Feldman & Lopez]	lynx	Link
2025-04-16	[Hyalogic]	lynx	Link
2025-04-16	[aeamg.org.br]	lockbit3	Link
2025-04-16	[ende.bo]	lockbit3	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-16	[Dale Partners Architects]	akira	Link
2025-04-16	[Anfarm Hellas]	akira	Link
2025-04-16	[D'Granel]	akira	Link
2025-04-08	[shengyusteel.com]	underground	Link
2025-04-15	[semex.com]	underground	Link
2025-04-15	[McElwee Firm]	lynx	Link
2025-04-16	[govonisabbiatrici]	qilin	Link
2025-04-14	[KraftKisarna]	dragonforce	Link
2025-04-14	[Pryor Morrow]	dragonforce	Link
2025-04-14	[Pratt Homes]	dragonforce	Link
2025-04-15	[Setpoint Systems]	dragonforce	Link
2025-04-14	[Pawnee Heights Unified School District]	medusa	Link
2025-04-16	[iblinfo.de]	incransom	Link
2025-04-15	[a-1freeman]	qilin	Link
2025-04-15	[Astra Products]	lynx	Link
2025-04-15	[Lake HVAC]	lynx	Link
2025-04-15	[ARRCO LSM]	ralord	Link
2025-04-15	[spscompanies.com]	lynx	Link
2025-04-15	[nevadareadymix.com]	lynx	Link
2025-04-15	[Heierli]	akira	Link
2025-04-15	[Bolivar Insulation]	akira	Link
2025-04-15	[King Industries Inc.]	akira	Link
2025-04-15	[PEÑA BRIONES MCDANIEL & CO.]	akira	Link
2025-04-15	[Inductors Inc.]	akira	Link
2025-04-15	[NewHotel cloud company]	ralord	Link
2025-04-15	[trocaire.edu]	incransom	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-15	[Oregon Department of Environmental Quality]	rhysida	Link
2025-04-14	[NL Olson & Associates]	qilin	Link
2025-04-14	[CDI]	qilin	Link
2025-04-14	[Waller]	play	Link
2025-04-14	[Cortez Resources]	play	Link
2025-04-14	[Comport Technology Solutions]	play	Link
2025-04-14	[Merri-Makers]	play	Link
2025-04-14	[O'Brien & Ryan]	play	Link
2025-04-14	[Voigt-Abernathy Company]	play	Link
2025-04-14	[Destination Toronto]	play	Link
2025-04-14	[James & Sons Fine Jewelers]	play	Link
2025-04-14	[Al-Hejailan Group]	ralord	Link
2025-04-14	[Caputo]	akira	Link
2025-04-14	[Agricola Da Quinta De Corona]	akira	Link
2025-04-14	[STUMPF MÜLLER Biberach]	akira	Link
2025-04-14	[Oklahoma Steel & Wire]	akira	Link
2025-04-14	[Orthopaedic Specialists of Connecticut]	incransom	Link
2025-04-14	[MENTAL HEALTH]	incransom	Link
2025-04-10	[REFFINDO-PT Pupk Indonesia]	nightspire	Link
2025-04-13	[FEELFOUR]	devman	Link
2025-04-13	[Med institute]	devman	Link
2025-04-13	[Bangkok Electronics Co., Ltd]	devman	Link
2025-04-13	[Tawasol]	devman	Link
2025-04-13	[Texas Construction Firm]	devman	Link
2025-04-13	[Optimax Technology]	devman	Link
2025-04-13	[CALTON.COM]	clon	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-01	[STORT]	nightspire	Link
2025-04-04	[Sistel Connections]	nightspire	Link
2025-04-01	[InterLOGIC Inc]	nightspire	Link
2025-04-01	[Secretaria de Educacion de Veracruz, SEV]	nightspire	Link
2025-04-06	[Nicera]	nightspire	Link
2025-04-08	[Emotrans Chile]	nightspire	Link
2025-04-08	[Zaphira Uniformes]	nightspire	Link
2025-04-03	[Audit Accounting Advisory Taxes]	nightspire	Link
2025-04-03	[Condista]	dragonforce	Link
2025-04-07	[Precision Textiles]	dragonforce	Link
2025-04-07	[Coulter & Tateoka]	dragonforce	Link
2025-04-09	[Miller & Caggiano]	dragonforce	Link
2025-04-09	[Service Trade SpA]	dragonforce	Link
2025-04-09	[Harris Steel]	dragonforce	Link
2025-04-12	[Ossman Consultants Limited]	dragonforce	Link
2025-04-08	[McFarland Commercial Insurance Services]	medusa	Link
2025-04-08	[Bridgebank Limited]	medusa	Link
2025-04-08	[Pulse Urgent Care]	medusa	Link
2025-04-08	[National Association for Stock Car Auto Racing]	medusa	Link
2025-04-12	[Fall River Public Schools]	medusa	Link
2025-04-13	[intelliloan.com]	lockbit3	Link
2025-04-13	[FEELFOUR]	qilin	Link
2025-04-12	[All4Labels -Global Packaging Group]	akira	Link
2025-04-11	[Chickenshed]	incransom	Link
2025-04-12	[visionproducts.llc]	lockbit3	Link
2025-04-12	[acimfunds.com]	lockbit3	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-12	[MS SUPPLY CHAIN SOLUTIONS (MALAYSIA) SDN. BHD]	qilin	Link
2025-04-12	[Mapaex]	qilin	Link
2025-04-12	[CMC Corperation]	crypto24	Link
2025-04-12	[Dimension Composite]	rhysida	Link
2025-04-12	[bilbie.com.au]	lynx	Link
2025-04-11	[Bjørklund]	termite	Link
2025-04-11	[C?l???t Group]	play	Link
2025-04-10	[Batesville Products,Inc.]	akira	Link
2025-04-11	[Colmar Industrial Supplies]	lynx	Link
2025-04-04	[Restaurant Associates]	lynx	Link
2025-04-11	[Imagineering Finishing Technologies]	incransom	Link
2025-04-10	[On IT]	termite	Link
2025-04-10	[Sfrent.net]	play	Link
2025-04-10	[The Study]	play	Link
2025-04-02	[Codinter]	play	Link
2025-04-10	[PAC Strapping Products]	play	Link
2025-04-10	[New York Sports Club]	play	Link
2025-04-10	[hasbco Company]	ralord	Link
2025-04-10	[ModulusGroup,Ludi-SFM]	crypto24	Link
2025-04-10	[inspec-international.com]	incransom	Link
2025-04-10	[TMA Group of Companies]	sarcoma	Link
2025-04-10	[SeproTec Multilingual Solutions]	akira	Link
2025-04-10	[Harvest]	RunSomeWares	Link
2025-04-07	[3P Corporation]	spacebears	Link
2025-04-10	[sk.com]	qilin	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2025-04-10	[Algas Engineering Pte Ltd - Algas Engineering]	qilin	Link
2025-04-09	[Správa služeb hlavního města Prahy]	cicada3301	Link
2025-04-07	[Potomac Financial Services]	hellcat	Link
2025-04-09	[Dumont Telephone]	akira	Link
2025-04-09	[Bangkok Electronics Co., Ltd]	qilin	Link
2025-04-09	[Simms Sigal Linwood Inc.]	akira	Link
2025-04-09	[Hotell Euroopa]	akira	Link
2025-04-09	[Consonic]	akira	Link
2025-04-09	[ccso2014.local(sheriffs)]	incransom	Link
2025-04-09	[Yozgat City Hospital]	bert	Link
2025-04-08	[physiciansmedicalbilling.net]	lockbit3	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	[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	[galesburg.org]	kairos	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
2025-04-06	[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
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

Datum	Opfer	Ransomware-Gruppe	Webseite
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
2025-04-03	[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	[Fraser Trebilcock]	play	Link
2025-04-04	[Drive Products]	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

Datum	Opfer	Ransomware-Gruppe	Webseite
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
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	[Parvin-Clauss Sign Company]	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

Datum	Opfer	Ransomware-Gruppe	Webseite
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	[caliendearchitects.com]	qilin	Link
2025-04-02	[Brügger Architekten AG]	killsec	Link
2025-04-02	[Royal Saudi Air Force]	killsec	Link
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

Datum	Opfer	Ransomware-Gruppe	Webseite
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.