

Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20250223



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) | 3 |
| 3.3 Sicherheitslücken Meldungen von Tenable | 7 |
| 4 Die Hacks der Woche | 9 |
| 4.0.1 Alte S3-Buckets ausgraben, Sachen hacken ☒ | 10 |
| 5 Cyberangriffe: (Feb) | 11 |
| 6 Ransomware-Erpressungen: (Feb) | 12 |
| 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 |
|-----|------|-----------|-----------------------|
|-----|------|-----------|-----------------------|

3.2 BSI - Warn- und Informationsdienst (WID)

Fri, 21 Feb 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 Feb 2025

[UPDATE] [hoch] Red Hat Enterprise Linux und 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](#)

—

Fri, 21 Feb 2025

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

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

- [Link](#)

—

Fri, 21 Feb 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 Feb 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](#)

—

Fri, 21 Feb 2025

[UPDATE] [hoch] Google Chrome/Microsoft Edge: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Google Chrome/Microsoft Edge ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu erzeugen und einen nicht näher spezifizierten Angriff zu starten.

- [Link](#)

—

Fri, 21 Feb 2025

[UPDATE] [hoch] Exim: Schwachstelle ermöglicht SQL-Injection

Ein Angreifer kann eine Schwachstelle in Exim ausnutzen, um einen SQL-Injection Angriff durchzuführen.

- [Link](#)

—

Fri, 21 Feb 2025

[NEU] [hoch] xwiki: Schwachstelle ermöglicht Codeausführung

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

- [Link](#)

—

Fri, 21 Feb 2025

[UPDATE] [hoch] Apache Tomcat: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache Tomcat ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsmechanismen zu umgehen oder Informationen offenzulegen.

- [Link](#)

—

Fri, 21 Feb 2025

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen

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

- [Link](#)

—

Fri, 21 Feb 2025

[UPDATE] [hoch] Ivanti Endpoint Manager: Mehrere Schwachstellen

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Ivanti Endpoint Manager ausnutzen, um seine Privilegien zu erweitern, Code auszuführen, einen Denial-of-Service-Zustand zu erzeugen und Informationen offenzulegen.

- [Link](#)

—

Fri, 21 Feb 2025

[UPDATE] [hoch] Microsoft Edge: Mehrere Schwachstellen

Ein entfernter anonymer oder lokaler Angreifer kann diese Schwachstelle ausnutzen, um beliebigen Code auszuführen, Spoofing-Angriffe durchzuführen, vertrauliche Informationen offenzulegen, Daten zu manipulieren und einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

—

Fri, 21 Feb 2025

[UPDATE] [hoch] WebKit (GTK und WPE): Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in WebKit ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen preiszugeben und einen Denial-of-Service-Zustand zu erzeugen.

- [Link](#)

—

Thu, 20 Feb 2025

[NEU] [hoch] Microsoft Power Pages: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Microsoft Power Pages ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

—

Thu, 20 Feb 2025

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

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

- [Link](#)

—

Thu, 20 Feb 2025

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

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

- [Link](#)

—

Thu, 20 Feb 2025

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

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

- [Link](#)

—

Thu, 20 Feb 2025

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

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

- [Link](#)

—

Thu, 20 Feb 2025

[UPDATE] [hoch] Moxa Router: Mehrere Schwachstellen ermöglichen Dateimanipulation und

Codeausführung

Ein entfernter anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Moxa Router ausnutzen, um Dateien zu manipulieren und beliebigen Code auszuführen.

- [Link](#)

—

Thu, 20 Feb 2025

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

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

- [Link](#)

—

3.3 Sicherheitslücken Meldungen von Tenable

| Datum | Schwachstelle | Bewertung |
|-----------|--|-----------|
| 2/22/2025 | [SUSE SLED15 / SLES15 / openSUSE 15 Security Update : brise (SUSE-SU-2025:0601-1)] | critical |
| 2/22/2025 | [SUSE SLES15 / openSUSE 15 Security Update : grafana (SUSE-SU-2025:0623-1)] | critical |
| 2/22/2025 | [SUSE SLES15 / openSUSE 15 Security Update : helm (SUSE-SU-2025:0602-1)] | critical |
| 2/21/2025 | [AlmaLinux 9 : mysql (ALSA-2025:1671)] | critical |
| 2/22/2025 | [Fedora 40 : proftpd (2025-d37ad923f5)] | high |
| 2/22/2025 | [SUSE SLES12 Security Update : postgresql15 (SUSE-SU-2025:0634-1)] | high |
| 2/22/2025 | [SUSE SLES12 Security Update : webkit2gtk3 (SUSE-SU-2025:0639-1)] | high |
| 2/22/2025 | [SUSE SLES15 Security Update : postgresql16 (SUSE-SU-2025:0636-1)] | high |
| 2/22/2025 | [Fedora 40 : chromium (2025-c0c371a0b6)] | high |

| Datum | Schwachstelle | Bewertung |
|-----------|---|-----------|
| 2/22/2025 | [Fedora 41 : proftpd (2025-835949b994)] | high |
| 2/22/2025 | [SUSE SLES12 Security Update : postgresql14 (SUSE-SU-2025:0615-1)] | high |
| 2/22/2025 | [SUSE SLED15 / SLES15 / openSUSE 15 Security Update : postgresql17 (SUSE-SU-2025:0616-1)] | high |
| 2/22/2025 | [SUSE SLES12 Security Update : postgresql16 (SUSE-SU-2025:0637-1)] | high |
| 2/22/2025 | [SUSE SLES15 Security Update : postgresql13 (SUSE-SU-2025:0619-1)] | high |
| 2/22/2025 | [SUSE SLES15 / openSUSE 15 Security Update : postgresql15 (SUSE-SU-2025:0614-1)] | high |
| 2/22/2025 | [SUSE SLES15 Security Update : postgresql14 (SUSE-SU-2025:0632-1)] | high |
| 2/22/2025 | [SUSE SLES15 / openSUSE 15 Security Update : postgresql14 (SUSE-SU-2025:0631-1)] | high |
| 2/22/2025 | [SUSE SLES15 Security Update : webkit2gtk3 (SUSE-SU-2025:0638-1)] | high |
| 2/22/2025 | [SUSE SLES15 / openSUSE 15 Security Update : ovmf (SUSE-SU-2025:0608-1)] | high |
| 2/22/2025 | [SUSE SLES15 Security Update : grub2 (SUSE-SU-2025:0607-1)] | high |
| 2/22/2025 | [openSUSE 15 Security Update : chromium (openSUSE-SU-2025:0070-1)] | high |
| 2/22/2025 | [SUSE SLED15 / SLES15 / openSUSE 15 Security Update : postgresql16 (SUSE-SU-2025:0635-1)] | high |
| 2/22/2025 | [SUSE SLES15 Security Update : ovmf (SUSE-SU-2025:0609-1)] | high |
| 2/22/2025 | [SUSE SLES12 Security Update : postgresql13 (SUSE-SU-2025:0606-1)] | high |
| 2/22/2025 | [SUSE SLES15 Security Update : postgresql17 (SUSE-SU-2025:0618-1)] | high |

| Datum | Schwachstelle | Bewertung |
|-----------|---|-----------|
| 2/22/2025 | [SUSE SLES15 / openSUSE 15 Security Update : google-osconfig-agent (SUSE-SU-2025:0611-1)] | high |
| 2/22/2025 | [SUSE SLES15 Security Update : postgresql15 (SUSE-SU-2025:0633-1)] | high |
| 2/22/2025 | [SUSE SLED15 / SLES15 / openSUSE 15 Security Update : emacs (SUSE-SU-2025:0599-1)] | high |
| 2/22/2025 | [SUSE SLES12 Security Update : grub2 (SUSE-SU-2025:0629-1)] | high |
| 2/22/2025 | [Debian dla-4064 : libxml2 - security update] | high |
| 2/22/2025 | [CBL Mariner 2.0 Security Update: nvidia-container-toolkit (CVE-2025-23359)] | high |
| 2/22/2025 | [CBL Mariner 2.0 Security Update: reaper (CVE-2024-52798)] | high |
| 2/21/2025 | [AlmaLinux 9 : libpq (ALSA-2025:1738)] | high |
| 2/21/2025 | [AlmaLinux 9 : postgresql:15 (ALSA-2025:1741)] | high |
| 2/21/2025 | [AlmaLinux 9 : bind (ALSA-2025:1681)] | high |
| 2/21/2025 | [Microsoft Edge (Chromium) < 133.0.3065.82 Multiple Vulnerabilities] | high |
| 2/21/2025 | [CBL Mariner 2.0 Security Update: emacs (CVE-2025-1244)] | high |
| 2/21/2025 | [Azure Linux 3.0 Security Update: mysql (CVE-2025-0725)] | high |
| 2/21/2025 | [Azure Linux 3.0 Security Update: postgresql (CVE-2025-1094)] | high |
| 2/21/2025 | [CBL Mariner 2.0 Security Update: postgresql (CVE-2025-1094)] | high |
| 2/21/2025 | [Azure Linux 3.0 Security Update: emacs (CVE-2025-1244)] | high |

4 Die Hacks der Woche

mit Martin Haunschmid

4.0.1 Alte S3-Buckets ausgraben, Sachen hacken ☒



[Zum Youtube Video](#)

5 Cyberangriffe: (Feb)

| Datum | Opfer | Land | Information |
|------------|---|-------|----------------------|
| 2025-02-19 | Genea | [AUS] | Link |
| 2025-02-19 | Paratus Namibia | [NAM] | Link |
| 2025-02-19 | Prefeitura de Paranhos | [BRA] | Link |
| 2025-02-18 | Raymond | [IND] | Link |
| 2025-02-18 | Cayuga Health | [USA] | Link |
| 2025-02-18 | HCRG Care Group | [GBR] | Link |
| 2025-02-17 | Appomattox County Public Schools | [USA] | Link |
| 2025-02-17 | Bibliothèque Muntpunt | [BEL] | Link |
| 2025-02-17 | Einstein-Gymnasium à Kehl | [DEU] | Link |
| 2025-02-13 | Eckert & Ziegler SE | [DEU] | Link |
| 2025-02-13 | Université de la Bundeswehr | [DEU] | Link |
| 2025-02-11 | Port of Oostende | [BEL] | Link |
| 2025-02-11 | Ville de Tulln | [AUT] | Link |
| 2025-02-11 | Alf DaFrè | [ITA] | Link |
| 2025-02-10 | LUP-Kliniken | [DEU] | Link |
| 2025-02-10 | City of Tarrant | [USA] | Link |
| 2025-02-10 | Sault Tribe, Kewadin Casinos | [USA] | Link |
| 2025-02-10 | Secrétariat de la Conférence des évêques allemands (Deutsche Bischofskonferenz) | [DEU] | Link |
| 2025-02-10 | Utsunomiya Central Clinic | [JPN] | Link |
| 2025-02-09 | Williamsburg James City County Public Schools | [USA] | Link |
| 2025-02-08 | FORTUNE ELECTRIC CO.,LTD | [TWN] | Link |
| 2025-02-07 | Transcend Information, Inc. | [TWN] | Link |
| 2025-02-07 | Rainbow District School Board | [CAN] | Link |
| 2025-02-07 | CPI UK | [GBR] | Link |

| Datum | Opfer | Land | Information |
|------------|------------------------------|-------|----------------------|
| 2025-02-05 | IMI | [GBR] | Link |
| 2025-02-05 | REMSA Health | [USA] | Link |
| 2025-02-04 | Pinehurst Radiology | [USA] | Link |
| 2025-02-04 | GFOS mbH | [DEU] | Link |
| 2025-02-03 | Lee Enterprises | [USA] | Link |
| 2025-02-02 | Top-Medien | [CHE] | Link |
| 2025-02-02 | Mayer Steel Pipe Corporation | [TWN] | Link |
| 2025-02-02 | Nan Ya PCB (KunShan) Corp. | [TWN] | Link |
| 2025-02-02 | Université des Bahamas | [BHS] | Link |
| 2025-02-01 | CESI | [FRA] | Link |

6 Ransomware-Erpressungen: (Feb)

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|-------------------------------------|-------------------|----------------------|
| 2025-02-21 | [Metropolitan Borough of Gateshead] | medusa | Link |
| 2025-02-21 | [Martin Energy Group Services] | medusa | Link |
| 2025-02-21 | [G&S Electric LLC] | medusa | Link |
| 2025-02-21 | [Benton Police Department] | medusa | Link |
| 2025-02-14 | [Al Bawani] | dragonforce | Link |
| 2025-02-21 | [Tristram European] | dragonforce | Link |
| 2025-02-22 | [SPEED Co] | hunters | Link |
| 2025-02-22 | [CCOO Servicios] | hunters | Link |
| 2025-02-22 | [Peter Glenn Ski Sport] | rhysida | Link |
| 2025-02-22 | [evergreenpnw.com] | incransom | Link |
| 2025-02-13 | [allegHENYbradford.com] | ransomhub | Link |
| 2025-02-09 | [teamsters175.org] | incransom | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|-----------------------------------|-------------------|----------------------|
| 2025-02-17 | [Vvf Illinois Services] | lynx | Link |
| 2025-02-21 | [www.electro-fusion.com] | ransomhub | Link |
| 2025-02-21 | [www.midwestvascular.net] | ransomhub | Link |
| 2025-02-15 | [www.witheyaddison.com] | ransomhub | Link |
| 2025-02-17 | [www.nola-law.com] | ransomhub | Link |
| 2025-02-21 | [planetone-asia.com] | lynx | Link |
| 2025-02-21 | [Luminus Management] | akira | Link |
| 2025-02-21 | [Siegel Group] | interlock | Link |
| 2025-02-21 | [Insyst GmbH] | akira | Link |
| 2025-02-21 | [guadeloupeformation.com] | ransomhub | Link |
| 2025-02-21 | [headcount.com] | ransomhub | Link |
| 2025-02-21 | [jindalgroup.com] | ransomhub | Link |
| 2025-02-03 | [statesideseattle.com] | incransom | Link |
| 2025-02-21 | [Paratus] | akira | Link |
| 2025-02-21 | [Barhite & Holzinger Inc.] | akira | Link |
| 2025-02-21 | [l.warsemann.fr] | qilin | Link |
| 2025-02-13 | [www.elecgalapagos.com.ec] | ransomhub | Link |
| 2025-02-21 | [www.flas-esq.com] | ransomhub | Link |
| 2025-02-06 | [www.saracenproperties.com] | ransomhub | Link |
| 2025-02-21 | [Crossroads Trading Company, Inc] | qilin | Link |
| 2025-02-15 | [(kc2) geokon.com] | lynx | Link |
| 2025-02-20 | [palauhealth] | qilin | Link |
| 2025-02-20 | [Medical File] | killsec | Link |
| 2025-02-17 | [eaglepost.com] | ransomhub | Link |
| 2025-02-18 | [gilcar.co] | ransomhub | Link |
| 2025-02-20 | [www.okddsi.net] | ransomhub | Link |
| 2025-02-20 | [newhorizonsbaking.com] | cactus | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|--------------------------------------|-------------------|----------------------|
| 2025-02-20 | [Andover Family Medicine] | qilin | Link |
| 2025-02-20 | [Waggonereng.com] | cloak | Link |
| 2025-02-20 | [Nebraska Irrigation] | akira | Link |
| 2025-02-20 | [Mac Jee] | akira | Link |
| 2025-02-20 | [www.selt-sistemi.com] | kraken | Link |
| 2025-02-20 | [Minaris Medical America] | akira | Link |
| 2025-02-20 | [Access2Jobs] | qilin | Link |
| 2025-02-20 | [Berg Engineering Consultants, Ltd.] | akira | Link |
| 2025-02-13 | [www.pransystems.com] | ransomhub | Link |
| 2025-02-10 | [www.phdental.com] | ransomhub | Link |
| 2025-02-07 | [www.riverdale.edu] | ransomhub | Link |
| 2025-02-20 | [M-1 TOOLWORKS] | apos | Link |
| 2025-02-17 | [Robinson Family Dentistry] | medusa | Link |
| 2025-02-17 | [Crager LaBorde] | medusa | Link |
| 2025-02-18 | [HCRG Care Group] | medusa | Link |
| 2025-02-20 | [ehdd.com] | incransom | Link |
| 2025-02-19 | [Ligentia] | termite | Link |
| 2025-02-19 | [rossmanmedia.ae] | funksec | Link |
| 2025-02-19 | [Ondunova] | akira | Link |
| 2025-02-10 | [ziese.net] | safepay | Link |
| 2025-02-12 | [foyerntredamedepaix.be] | safepay | Link |
| 2025-02-19 | [Südkabel GmbH] | akira | Link |
| 2025-02-19 | [VISEO] | fog | Link |
| 2025-02-19 | [Next TI] | fog | Link |
| 2025-02-19 | [Alabama Ophthalmology Associates] | bianlian | Link |
| 2025-02-19 | [DR.Claims FL LLC] | killsec | Link |
| 2025-02-19 | [EzyLegal] | killsec | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|---|-------------------|----------------------|
| 2025-02-19 | [Vector Engineering, Inc] | akira | Link |
| 2025-02-19 | [Hall Law Group LLP] | akira | Link |
| 2025-02-18 | [haleycomfort.com] | ransomhub | Link |
| 2025-02-19 | [DBK] | qilin | Link |
| 2025-02-19 | [Haggin Oaks Golf (hagginoaks.com)] | fog | Link |
| 2025-02-19 | [traffic-advertising-llc] | qilin | Link |
| 2025-02-19 | [dr-elizabeth-bjornson] | qilin | Link |
| 2025-02-12 | [Eservices.gov.zm] | flocker | Link |
| 2025-02-19 | [lake-washington-vascular] | qilin | Link |
| 2025-02-19 | [Gitlabs: Next TI, VISEO, Hochschule Trier] | fog | Link |
| 2025-02-19 | [BeniPlus] | killsec | Link |
| 2025-02-19 | [Brolly] | killsec | Link |
| 2025-02-19 | [Help Me Grow Yolo] | killsec | Link |
| 2025-02-19 | [NimuSoft] | killsec | Link |
| 2025-02-18 | [footballticketnet.com] | funksec | Link |
| 2025-02-18 | [uniekinc.com] | cactus | Link |
| 2025-02-18 | [midwayimporting.com] | cactus | Link |
| 2025-02-18 | [revitalash.com] | cactus | Link |
| 2025-02-18 | [bestbrands.com] | cactus | Link |
| 2025-02-07 | [autogedal.ro] | apt73 | Link |
| 2025-02-07 | [www.mwmechanicalinc.com] | ransomhub | Link |
| 2025-02-02 | [www.alphamedctr.com] | ransomhub | Link |
| 2025-02-02 | [www.ccttechnologies.com] | ransomhub | Link |
| 2025-02-18 | [www.macmed.com] | ransomhub | Link |
| 2025-02-18 | [Decore-Ative Specialties] | akira | Link |
| 2025-02-18 | [Daniels Homes] | akira | Link |
| 2025-02-18 | [PREMIER HOUSEWARES LIMITED] | akira | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|---|-------------------|----------------------|
| 2025-02-18 | [Ranhill Bersekutu] | lynx | Link |
| 2025-02-18 | [Buanderie Centrale de Montreal] | rhysida | Link |
| 2025-02-14 | [myhscu.com] | embargo | Link |
| 2025-02-17 | [www.macter.com] | ransomhub | Link |
| 2025-02-17 | [Cuna Supply] | play | Link |
| 2025-02-17 | [The Townsley Law Firm Information] | play | Link |
| 2025-02-17 | [Bushmans] | play | Link |
| 2025-02-17 | [Inland Empire Distribution Systems, Inc.] | play | Link |
| 2025-02-17 | [Wylie Steel Fabricators] | play | Link |
| 2025-02-17 | [Oxford Companies] | play | Link |
| 2025-02-17 | [Stage 3 Separation] | play | Link |
| 2025-02-17 | [Transkid] | play | Link |
| 2025-02-17 | [Rheinischer Sch] | play | Link |
| 2025-02-17 | [Startek Peglar & Calcagni] | play | Link |
| 2025-02-17 | [Weed Man Canada] | play | Link |
| 2025-02-17 | [Bulldog Oilfield Services] | play | Link |
| 2025-02-17 | [danecourt.kent.sch.uk] | kairos | Link |
| 2025-02-17 | [toitiusa.com] | kairos | Link |
| 2025-02-17 | [lekiaviation.com] | ransomhub | Link |
| 2025-02-17 | [bisindustries.com] | ransomhub | Link |
| 2025-02-17 | [kinseysinc.com] | cactus | Link |
| 2025-02-17 | [steelerubber.com] | cactus | Link |
| 2025-02-17 | [almostfamousclothing.com] | cactus | Link |
| 2025-02-17 | [This entry has been removed following a request from the company.] | cactus | Link |
| 2025-02-17 | [ssmcoop.com] | cactus | Link |
| 2025-02-17 | [hiway.com.br] | funksec | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|---|-------------------|----------------------|
| 2025-02-17 | [Thong Sia] | akira | Link |
| 2025-02-17 | [Swissmem] | hunters | Link |
| 2025-02-17 | [Bulverde Glass, Inc.] | qilin | Link |
| 2025-02-17 | [Hisingstads Bleck] | lynx | Link |
| 2025-02-17 | [Leadership Strategies] | lynx | Link |
| 2025-02-17 | [LINTEC & LINNHOF Holdings] | lynx | Link |
| 2025-02-17 | [HRS_IDEA_Expertises] | lynx | Link |
| 2025-02-17 | [Autoschade Pippel] | lynx | Link |
| 2025-02-17 | [Pedensia Graphics Distribution] | lynx | Link |
| 2025-02-17 | [Winbas] | lynx | Link |
| 2025-02-17 | [hamton] | lynx | Link |
| 2025-02-17 | [Greencastle-Antrim Senior High School (gcasd.org)] | fog | Link |
| 2025-02-17 | [Woman's Athletic Club of Chicago] | akira | Link |
| 2025-02-17 | [P.N. Sakkoulas] | akira | Link |
| 2025-02-17 | [Allied Tenesis] | lynx | Link |
| 2025-02-17 | [DA Capital] | akira | Link |
| 2025-02-14 | [COSMED] | akira | Link |
| 2025-02-17 | [Persante Health Care] | incransom | Link |
| 2025-02-05 | [annegrady.org] | embargo | Link |
| 2025-02-16 | [Pamrya.de] | fog | Link |
| 2025-02-16 | [QBurst] | fog | Link |
| 2025-02-16 | [Acqua development] | fog | Link |
| 2025-02-16 | [Gitlabs: Acqua development, QBurst, Pamyra.de] | fog | Link |
| 2025-02-08 | [Gpstech2007.com] | flocker | Link |
| 2025-02-08 | [Mervis.info] | flocker | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|--|-------------------|----------------------|
| 2025-02-08 | [Realtime.tw] | flocker | Link |
| 2025-02-15 | [saulttribe.com/kewadin.com] | ransomhub | Link |
| 2025-02-15 | [www.rowetactical.com] | ransomhub | Link |
| 2025-02-15 | [www.transcend-info.com] | ransomhub | Link |
| 2025-02-15 | [www.cityoftarrant.com] | ransomhub | Link |
| 2025-02-07 | [www.imgenterprises.com] | ransomhub | Link |
| 2025-02-15 | [www.solardatasystems.com] | ransomhub | Link |
| 2025-02-06 | [www.310tempering.com] | ransomhub | Link |
| 2025-02-12 | [www.colacouronnelocations.com] | ransomhub | Link |
| 2025-02-10 | [Fortune Electric Co Ltd] | lynx | Link |
| 2025-02-09 | [Northeast Delta Human Services Authority] | incransom | Link |
| 2025-02-09 | [City of McKinney] | incransom | Link |
| 2025-02-15 | [halex.com] | abyss | Link |
| 2025-02-05 | [Hydronic & Steam Equipment] | play | Link |
| 2025-02-11 | [Ratioparts] | play | Link |
| 2025-02-14 | [Heritage South Credit Union] | embargo | Link |
| 2025-02-14 | [Primaveras] | akira | Link |
| 2025-02-08 | [www.calspa.it] | ransomhub | Link |
| 2025-02-14 | [Nelson & Townsend, CPA's] | akira | Link |
| 2025-02-14 | [Castle Rock Construction Company] | akira | Link |
| 2025-02-14 | [Genus] | akira | Link |
| 2025-02-14 | [Window World of Raleigh] | akira | Link |
| 2025-02-14 | [F.TECH R&D NORTH AMERICA INC.] | qilin | Link |
| 2025-02-14 | [Go Strictly] | akira | Link |
| 2025-02-14 | [Bethany Lutheran Church] | qilin | Link |
| 2025-02-10 | [GANRO] | lynx | Link |
| 2025-02-14 | [Regency Media] | akira | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|---|-------------------|----------------------|
| 2025-02-14 | [brockbanks.co.uk] | ransomhub | Link |
| 2025-02-14 | [The Agency] | rhysida | Link |
| 2025-02-13 | [ADULLACT] | fog | Link |
| 2025-02-13 | [Ayomi] | fog | Link |
| 2025-02-13 | [Omydoo] | fog | Link |
| 2025-02-13 | [Gitlabs: Omydoo, Ayomi, ADULLACT] | fog | Link |
| 2025-02-13 | [Aspire Rural Health System] | bianlian | Link |
| 2025-02-13 | [Mozo Grau (mozo-grau.com)] | fog | Link |
| 2025-02-13 | [CoMo-Industrial Engineering] | akira | Link |
| 2025-02-13 | [enventuregt.com] | ransomhub | Link |
| 2025-02-13 | [snoqualmietribe.us] | ransomhub | Link |
| 2025-02-13 | [vadatech.com] | qilin | Link |
| 2025-02-13 | [Nippon Steel USA] | bianlian | Link |
| 2025-02-13 | [Financial Services of America, Inc.] | bianlian | Link |
| 2025-02-13 | [Layfield & Borel CPA's L.L.C] | bianlian | Link |
| 2025-02-13 | [Dain, Torpy, Le Ray, Wiest & Garner, P.C.] | bianlian | Link |
| 2025-02-13 | [Dan Eckman CPA] | akira | Link |
| 2025-02-12 | [Elite Advanced LaserCorporation] | akira | Link |
| 2025-02-12 | [Obex Medical] | killsec | Link |
| 2025-02-12 | [Cache Valley ENT] | medusa | Link |
| 2025-02-12 | [JP Express] | medusa | Link |
| 2025-02-12 | [Central District Health Department] | medusa | Link |
| 2025-02-12 | [morrisgroup.co] | clap | Link |
| 2025-02-05 | [stjerome.org] | safepay | Link |
| 2025-02-12 | [Therma Seal Insulation Systems] | ciphbit | Link |
| 2025-02-12 | [Squeezer-software] | fog | Link |
| 2025-02-12 | [Spacemanic] | fog | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|--|-------------------|----------------------|
| 2025-02-12 | [INGV] | fog | Link |
| 2025-02-12 | [Gitlabs: INGV, Spacemanic, Squeezer-software] | fog | Link |
| 2025-02-12 | [Quality Home Health Care] | qilin | Link |
| 2025-02-12 | [avtovelomoto.by] | funksec | Link |
| 2025-02-12 | [alderconstruction.com] | ransomhub | Link |
| 2025-02-12 | [steveallcorn.remax.com] | ransomhub | Link |
| 2025-02-12 | [bergconst.com] | ransomhub | Link |
| 2025-02-12 | [burdickpainting.com] | ransomhub | Link |
| 2025-02-12 | [columbiacabinets.com] | ransomhub | Link |
| 2025-02-12 | [ekvallbyrne.com] | ransomhub | Link |
| 2025-02-12 | [krmcustomhomes.com] | ransomhub | Link |
| 2025-02-12 | [laderalending.com] | ransomhub | Link |
| 2025-02-12 | [minnesotaexteriors.com] | ransomhub | Link |
| 2025-02-12 | [rogerspetro.com] | ransomhub | Link |
| 2025-02-12 | [sundanceliving.com] | ransomhub | Link |
| 2025-02-12 | [thejdkgroup.com] | ransomhub | Link |
| 2025-02-12 | [twncomm.com] | ransomhub | Link |
| 2025-02-12 | [Vicky Foods] | akira | Link |
| 2025-02-12 | [Hess (hess-gmbh.de)] | fog | Link |
| 2025-02-12 | [TJKM] | qilin | Link |
| 2025-02-03 | [askgs.ma] | ransomhub | Link |
| 2025-02-12 | [slchc.edu] | ransomhub | Link |
| 2025-02-12 | [weathersa.co.za] | ransomhub | Link |
| 2025-02-12 | [Erie Management Group, LLC] | qilin | Link |
| 2025-02-12 | [curtisint.com] | cactus | Link |
| 2025-02-12 | [britannicahome.com] | cactus | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|--|-------------------|----------------------|
| 2025-02-12 | [uniquehd.com] | cactus | Link |
| 2025-02-12 | [tomsmithindustries.com] | qilin | Link |
| 2025-02-04 | [Accelerator] | dragonforce | Link |
| 2025-02-04 | [O&S Associates] | dragonforce | Link |
| 2025-02-12 | [Leading Edge Specialized Dentistry] | rhysida | Link |
| 2025-02-12 | [Hammond Trucking & Excavation] | rhysida | Link |
| 2025-02-12 | [BH Aircraft Company, Inc.] | rhysida | Link |
| 2025-02-12 | [My New Jersey Dentist] | rhysida | Link |
| 2025-02-12 | [Town Counsel Law & Litigation] | rhysida | Link |
| 2025-02-06 | [MICRO MANUFACTURING] | medusalocker | Link |
| 2025-02-05 | [The Brown & Hurley Group] | lynx | Link |
| 2025-02-11 | [Tie Down Engineering] | play | Link |
| 2025-02-01 | [Baltimore Country Club] | play | Link |
| 2025-02-11 | [Jildor Shoes] | play | Link |
| 2025-02-11 | [Mainline Information Systems] | play | Link |
| 2025-02-11 | [CESI] | termite | Link |
| 2025-02-11 | [ROCK SOLID Stabilization & Reclamation] | play | Link |
| 2025-02-11 | [Saint George's College (saintgeorge.cl)] | fog | Link |
| 2025-02-11 | [Aurora Public Schools (aurorak12.org)] | fog | Link |
| 2025-02-11 | [Natures Organics] | medusa | Link |
| 2025-02-11 | [Paignton Zoo] | medusa | Link |
| 2025-02-11 | [SRP Companies] | medusa | Link |
| 2025-02-11 | [lacold.com] | clop | Link |
| 2025-02-11 | [The University of Notre Dame Australia (nd.edu.au)] | fog | Link |
| 2025-02-11 | [Prime Trust Financial] | akira | Link |
| 2025-02-01 | [sehma.com] | threeam | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|-----------------------------------|-------------------|----------------------|
| 2025-02-11 | [I.B.G SPA] | sarcoma | Link |
| 2025-02-11 | [ldi-trucking-inc] | sarcoma | Link |
| 2025-02-11 | [Wisper Reimer Ingenieure GmbH] | sarcoma | Link |
| 2025-02-11 | [Unimicron] | sarcoma | Link |
| 2025-02-11 | [Logix Corporate Solutions] | killsec | Link |
| 2025-02-11 | [sole technology] | monti | Link |
| 2025-02-10 | [primesourcestaffing.com] | ransomhub | Link |
| 2025-02-04 | [The Children's Center Of Hamden] | incransom | Link |
| 2025-02-10 | [komline.com] | ransomhub | Link |
| 2025-02-10 | [bazcooil.com] | ransomhub | Link |
| 2025-02-10 | [sdfab.com] | ransomhub | Link |
| 2025-02-10 | [kaplanstahler.com] | ransomhub | Link |
| 2025-02-04 | [www.jsp.com] | ransomhub | Link |
| 2025-02-10 | [ekonom.com] | cllop | Link |
| 2025-02-10 | [editel.eu] | cllop | Link |
| 2025-02-10 | [derrytransport.com] | cllop | Link |
| 2025-02-10 | [dana-co.com] | cllop | Link |
| 2025-02-10 | [designdesigninc.com] | cllop | Link |
| 2025-02-10 | [daatagroup.com] | cllop | Link |
| 2025-02-10 | [dunnriteproducts.com] | cllop | Link |
| 2025-02-10 | [d2go.io] | cllop | Link |
| 2025-02-10 | [dynastyfootwear.com] | cllop | Link |
| 2025-02-10 | [dxc.com] | cllop | Link |
| 2025-02-10 | [dundasjafine.com] | cllop | Link |
| 2025-02-10 | [drexel.ca] | cllop | Link |
| 2025-02-10 | [donlen.com] | cllop | Link |
| 2025-02-10 | [dlfna.com] | cllop | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|-----------------------------|-------------------|----------------------|
| 2025-02-04 | [directex.net] | clon | Link |
| 2025-02-10 | [diazfoods.com] | clon | Link |
| 2025-02-10 | [detecno.com] | clon | Link |
| 2025-02-10 | [deltaenterprise.com] | clon | Link |
| 2025-02-10 | [deltachildren.com] | clon | Link |
| 2025-02-10 | [decescente.com] | clon | Link |
| 2025-02-10 | [dbetances.com] | clon | Link |
| 2025-02-10 | [datapakservices.com] | clon | Link |
| 2025-02-10 | [coglans.com] | clon | Link |
| 2025-02-10 | [cycle.local] | clon | Link |
| 2025-02-10 | [cassinfo.com] | clon | Link |
| 2025-02-10 | [claw.local] | clon | Link |
| 2025-02-10 | [cgdc.cottong.local] | clon | Link |
| 2025-02-10 | [cps.k12.il.us] | clon | Link |
| 2025-02-10 | [conbraco.com] | clon | Link |
| 2025-02-10 | [clearon.com] | clon | Link |
| 2025-02-10 | [crestmills.com] | clon | Link |
| 2025-02-10 | [cranebsu.com] | clon | Link |
| 2025-02-10 | [covetra.com] | clon | Link |
| 2025-02-10 | [connexion-informatique.fr] | clon | Link |
| 2025-02-10 | [compasshealthbrands.com] | clon | Link |
| 2025-02-10 | [collectionxiix.com] | clon | Link |
| 2025-02-10 | [coghlans.com] | clon | Link |
| 2025-02-10 | [codagami.com] | clon | Link |
| 2025-02-10 | [cmcoldstores.com] | clon | Link |
| 2025-02-10 | [classicaccessories.com] | clon | Link |
| 2025-02-10 | [cinema1.ca] | clon | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|-------------------------------------|-------------------|----------------------|
| 2025-02-10 | [cherokeedistributing.com] | cllop | Link |
| 2025-02-10 | [chemstarcorp.com] | cllop | Link |
| 2025-02-10 | [challenger.com] | cllop | Link |
| 2025-02-10 | [cesarcastillo.com] | cllop | Link |
| 2025-02-10 | [cedarsfoods.com] | cllop | Link |
| 2025-02-10 | [cathayhome.com] | cllop | Link |
| 2025-02-10 | [catchuplogistics.com] | cllop | Link |
| 2025-02-10 | [castlewoodapparel.com] | cllop | Link |
| 2025-02-10 | [carlsondistributing.com] | cllop | Link |
| 2025-02-10 | [Enfin] | killsec | Link |
| 2025-02-10 | [Recievership Specialists] | bianlian | Link |
| 2025-02-10 | [abcapital.com.ph] | lockbit3 | Link |
| 2025-02-10 | [Allen & Pinnix] | akira | Link |
| 2025-02-10 | [The Pawn] | akira | Link |
| 2025-02-10 | [Polstermöbel Oelsa GmbH] | sarcoma | Link |
| 2025-02-03 | [Grail Springs Retreat] | medusa | Link |
| 2025-02-05 | [Rural Health Services] | medusa | Link |
| 2025-02-07 | [Adler Shine LLP] | medusa | Link |
| 2025-02-07 | [SimonMed Imaging] | medusa | Link |
| 2025-02-08 | [PAD Aviation Technics GmbH] | medusa | Link |
| 2025-02-10 | [Serenity Salon & Spa] | medusa | Link |
| 2025-02-10 | [Michael's Hair Body Mind] | medusa | Link |
| 2025-02-10 | [Greenwich Medical Spa] | medusa | Link |
| 2025-02-10 | [Capital Cell Global (CCG)] | killsec | Link |
| 2025-02-10 | [ASRAM Medical College and Hospita] | killsec | Link |
| 2025-02-10 | [CAPITALFINEMEATS.COM] | cllop | Link |
| 2025-02-10 | [CALIFORNIARAINLA.COM] | cllop | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|---------------------------|-------------------|----------------------|
| 2025-02-10 | [CAINEWAREHOUSING.COM] | cllop | Link |
| 2025-02-10 | [BARCOMADE.COM] | cllop | Link |
| 2025-02-10 | [BEINOGLOU.GR] | cllop | Link |
| 2025-02-10 | [BIAGIBROS.COM] | cllop | Link |
| 2025-02-10 | [BSIEDI.COM] | cllop | Link |
| 2025-02-10 | [BOZICKDIST.COM] | cllop | Link |
| 2025-02-10 | [BOWANDARROWPET.COM] | cllop | Link |
| 2025-02-10 | [BOSSCHAIR.COM] | cllop | Link |
| 2025-02-10 | [BESTBRANDSINC.COM] | cllop | Link |
| 2025-02-10 | [BERKSHIREINC.COM] | cllop | Link |
| 2025-02-10 | [BENSONMILLS.COM] | cllop | Link |
| 2025-02-10 | [BENBECKER.EU] | cllop | Link |
| 2025-02-10 | [BAYSIDENH.COM] | cllop | Link |
| 2025-02-10 | [BARRETTDISTRIBUTION.COM] | cllop | Link |
| 2025-02-10 | [BACKYARDDISCOVERY.COM] | cllop | Link |
| 2025-02-10 | [ALEGACY.COM] | cllop | Link |
| 2025-02-10 | [AURORAIMPORTING.COM] | cllop | Link |
| 2025-02-10 | [ARLAN.NL] | cllop | Link |
| 2025-02-10 | [ARKIEJIGS.COM] | cllop | Link |
| 2025-02-10 | [APOLLOCORP.COM] | cllop | Link |
| 2025-02-10 | [AOL.COM AJ MISSERT INC] | cllop | Link |
| 2025-02-10 | [ANNABELLECANDY.COM] | cllop | Link |
| 2025-02-10 | [ANDROSNA.COM] | cllop | Link |
| 2025-02-10 | [ANDREWSDISTRIBUTING.COM] | cllop | Link |
| 2025-02-10 | [AMSINO.COM] | cllop | Link |
| 2025-02-10 | [AMERICANLIGHTING.COM] | cllop | Link |
| 2025-02-10 | [ALPADVANTAGE.COM] | cllop | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|-----------------------------|-------------------|----------------------|
| 2025-02-10 | [ALLTECH.COM] | clop | Link |
| 2025-02-10 | [ALLIANCEMERCANTILE.COM] | clop | Link |
| 2025-02-10 | [AIRLIQUIDE.COM] | clop | Link |
| 2025-02-10 | [AGILITYAUTOPARTS.COM] | clop | Link |
| 2025-02-10 | [AFFINITYCANADA.COM] | clop | Link |
| 2025-02-10 | [ACTIAN.COM] | clop | Link |
| 2025-02-10 | [ACPIDEAS.COM] | clop | Link |
| 2025-02-10 | [ACCEM.COM] | clop | Link |
| 2025-02-10 | [ABCOPRODUCTS.COM] | clop | Link |
| 2025-02-10 | [3PLSOFTWARE.COM] | clop | Link |
| 2025-02-10 | [Brockway Hair Design] | medusa | Link |
| 2025-02-10 | [True World Foods] | medusa | Link |
| 2025-02-10 | [MEDES College] | medusa | Link |
| 2025-02-03 | [Glow Medi Spa] | medusa | Link |
| 2025-02-10 | [3FINITY.NET] | clop | Link |
| 2025-02-10 | [1888MILLS.COM] | clop | Link |
| 2025-02-10 | [CXTSOFTWARE.COM] | clop | Link |
| 2025-02-10 | [UNIEKINC.COM] | clop | Link |
| 2025-02-10 | [STORKCRAFT.COM] | clop | Link |
| 2025-02-10 | [COMPANY's_PART1] | clop | Link |
| 2025-02-10 | [Old National Events Plaza] | akira | Link |
| 2025-02-09 | [Marshall Motor Holdings] | lynx | Link |
| 2025-02-10 | [Albright Institute] | killsec | Link |
| 2025-02-10 | [WhoHire] | killsec | Link |
| 2025-02-10 | [Upstate Glass Tempering] | sarcoma | Link |
| 2025-02-10 | [Saied Music] | sarcoma | Link |
| 2025-02-09 | [Kitty cookies] | kraken | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|---|-------------------|----------------------|
| 2025-02-09 | [www.cdprojekt.com] | kraken | Link |
| 2025-02-09 | [www.mgl.law] | kraken | Link |
| 2025-02-09 | [www.fudpucker.com] | kraken | Link |
| 2025-02-09 | [ctntelco.com] | kraken | Link |
| 2025-02-09 | [iRidge Inc.] | fog | Link |
| 2025-02-09 | [Maxvy Technologies Pvt] | fog | Link |
| 2025-02-09 | [Universitatea Politehnica din Bucuresti] | fog | Link |
| 2025-02-09 | [Hpisd.org] | ransomhub | Link |
| 2025-02-09 | [wwcsd.net] | ransomhub | Link |
| 2025-02-09 | [Israel Police] | handala | Link |
| 2025-02-09 | [Gitlabs: Universitatea Politehnica din Bucuresti, Maxvy Technologies Pvt, iRidge Inc.] | fog | Link |
| 2025-02-08 | [Substitute Teacher Service] | cicada3301 | Link |
| 2025-02-08 | [SAKAI SOUKEN Co.] | hunters | Link |
| 2025-02-08 | [cmr24] | stormous | Link |
| 2025-02-08 | [phidac.be] | funksec | Link |
| 2025-02-07 | [3SS] | fog | Link |
| 2025-02-07 | [Fligno] | fog | Link |
| 2025-02-07 | [Chalmers tekniska högskola] | fog | Link |
| 2025-02-07 | [herbalcanadaonline.com] | funksec | Link |
| 2025-02-07 | [Gitlabs: Chalmers tekniska högskola, Fligno, 3SS] | fog | Link |
| 2025-02-06 | [teamues.com] | ransomhub | Link |
| 2025-02-07 | [iaaglobal.org] | funksec | Link |
| 2025-02-07 | [Tropical Foods Company Inc] | akira | Link |
| 2025-02-07 | [sautech.edu] | ransomhub | Link |
| 2025-02-07 | [autogedal.ro] | funksec | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|--|-------------------|----------------------|
| 2025-02-07 | [nldappraisals.com] | qilin | Link |
| 2025-02-07 | [renmarkfinancial.com] | qilin | Link |
| 2025-02-06 | [northernresponse.com] | cactus | Link |
| 2025-02-06 | [savoiesfoods.com] | cactus | Link |
| 2025-02-06 | [zsattorneys.com] | ransomhub | Link |
| 2025-02-06 | [Presence From Innovation (PFI)] | akira | Link |
| 2025-02-06 | [Robertshaw] | hunters | Link |
| 2025-02-04 | [HARADA] | qilin | Link |
| 2025-02-06 | [DIEM] | fog | Link |
| 2025-02-06 | [Top Systems] | fog | Link |
| 2025-02-06 | [eConceptions] | fog | Link |
| 2025-02-06 | [Gitlabs: eConceptions, Top Systems, DIEM] | fog | Link |
| 2025-02-05 | [McCORMICK TAYLOR] | qilin | Link |
| 2025-02-05 | [corehandf.com] | threeam | Link |
| 2025-02-05 | [Dash Business] | bianlian | Link |
| 2025-02-05 | [Hall Chadwick] | bianlian | Link |
| 2025-02-05 | [NESCTC Security Services] | bianlian | Link |
| 2025-02-05 | [Shinsung Delta Tech] | lynx | Link |
| 2025-02-05 | [Banfi Vintners] | lynx | Link |
| 2025-02-05 | [annegrady.org] | ransomhub | Link |
| 2025-02-05 | [rablighting.com] | qilin | Link |
| 2025-02-05 | [boostheat.com] | apt73 | Link |
| 2025-02-05 | [rattelacademy.com] | funksec | Link |
| 2025-02-05 | [cara.com.my] | funksec | Link |
| 2025-02-04 | [casperstruck.com] | kairos | Link |
| 2025-02-04 | [medicalreportsltd.com] | kairos | Link |
| 2025-02-01 | [LUA Coffee] | fog | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|--|-------------------|----------------------|
| 2025-02-01 | [GFZ Helmholtz Centre for Geosciences] | fog | Link |
| 2025-02-01 | [PT. ITPRENEUR INDONESIA TECHNOLOGY] | fog | Link |
| 2025-02-04 | [Devlion] | fog | Link |
| 2025-02-04 | [SOLEIL] | fog | Link |
| 2025-02-04 | [hemio.de] | fog | Link |
| 2025-02-03 | [Madia] | fog | Link |
| 2025-02-03 | [X-lab group] | fog | Link |
| 2025-02-03 | [Bolin Centre for Climate Research] | fog | Link |
| 2025-02-04 | [Gitlabs: hemio.de, SOLEIL, Devlion] | fog | Link |
| 2025-02-04 | [mielectric.com.br] | akira | Link |
| 2025-02-04 | [engineeredequip.com] | akira | Link |
| 2025-02-04 | [emin.cl] | akira | Link |
| 2025-02-04 | [alphascriptrx.com] | akira | Link |
| 2025-02-04 | [premierop.com] | akira | Link |
| 2025-02-04 | [acesaz.com] | akira | Link |
| 2025-02-04 | [mipa.com.br] | akira | Link |
| 2025-02-04 | [usm-americas.com] | akira | Link |
| 2025-02-04 | [feheq.com] | akira | Link |
| 2025-02-04 | [stewartautosales.com] | akira | Link |
| 2025-02-04 | [milleraa.com] | akira | Link |
| 2025-02-04 | [jsfrental.com] | akira | Link |
| 2025-02-04 | [summitmovinghouston.com] | akira | Link |
| 2025-02-04 | [dwgp.com] | akira | Link |
| 2025-02-04 | [easycom.com] | akira | Link |
| 2025-02-04 | [alfa.com.co] | akira | Link |
| 2025-02-04 | [westernwoodsinc.com] | akira | Link |
| 2025-02-04 | [viscira.com] | akira | Link |

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

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|--|-------------------|----------------------|
| 2025-02-04 | [gaheritagefcu.org] | ransomhub | Link |
| 2025-02-04 | [SSMC] | cicada3301 | Link |
| 2025-02-04 | [Rivers Casino and Rush Street Gaming] | cicada3301 | Link |
| 2025-02-04 | [Asterra Properties] | cicada3301 | Link |
| 2025-02-04 | [Caliente Construction] | cicada3301 | Link |
| 2025-02-04 | [C2S Technologies Inc.] | everest | Link |
| 2025-02-04 | [ITSS] | everest | Link |
| 2025-02-03 | [brewsterfiredepartment.org] | safepay | Link |
| 2025-02-03 | [Dickerson & Nieman Realtors] | play | Link |
| 2025-02-03 | [Gitlabs: Bolin Centre for Climate Research, X-lab group, Madia] | fog | Link |
| 2025-02-03 | [gruppozaccaria.it] | lockbit3 | Link |
| 2025-02-03 | [Karadeniz Holding (karadenizholding.com)] | fog | Link |
| 2025-02-03 | [www.wongfleming.com] | ransomhub | Link |
| 2025-02-03 | [smithmidland.com] | ransomhub | Link |
| 2025-02-03 | [www.origene.com] | ransomhub | Link |
| 2025-02-03 | [Denton Regional Suicide Prevention Coalition] | qilin | Link |
| 2025-02-03 | [fasttrackcargo.com] | funksec | Link |
| 2025-02-03 | [Ponte16 Hotel & Casino] | killsec | Link |
| 2025-02-03 | [Elslaw.com (EARLY , LUCARELLI , SWEENEY & MEISENKOTHEN LAW)] | qilin | Link |
| 2025-02-03 | [DRI Title & Escrow] | qilin | Link |
| 2025-02-03 | [DPA Auctions] | qilin | Link |
| 2025-02-03 | [Altair Travel] | qilin | Link |
| 2025-02-03 | [Civil Design, Inc] | qilin | Link |
| 2025-02-03 | [The Gatesworth Senior Living St. Louis] | qilin | Link |
| 2025-02-03 | [GOVirtual-it.com (VIRTUAL IT)] | qilin | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|---|-------------------|----------------------|
| 2025-02-03 | [coel.com.mx] | apt73 | Link |
| 2025-02-03 | [Alford Walden Law] | qilin | Link |
| 2025-02-03 | [Pasco Systems] | qilin | Link |
| 2025-02-03 | [MPP Group of Companies] | qilin | Link |
| 2025-02-03 | [Pineland community service board] | spacebears | Link |
| 2025-02-02 | [usuhs.edu] | lockbit3 | Link |
| 2025-02-02 | [Four Eye Clinics] | abyss | Link |
| 2025-02-02 | [jpcgroupinc.com] | abyss | Link |
| 2025-02-02 | [hreu.eu] | funksec | Link |
| 2025-02-02 | [Tosaf] | handala | Link |
| 2025-02-02 | [turbomp] | stormous | Link |
| 2025-02-02 | [Cyrious Software] | bianlian | Link |
| 2025-02-02 | [Medical Associates of Brevard] | bianlian | Link |
| 2025-02-02 | [Civic Committee] | bianlian | Link |
| 2025-02-02 | [Ayres Law Firm] | bianlian | Link |
| 2025-02-02 | [Growth Acceleration Partners] | bianlian | Link |
| 2025-02-01 | [fiberskynet.net] | funksec | Link |
| 2025-02-01 | [tirtaraharja.co.id] | funksec | Link |
| 2025-02-01 | [Gitlabs: PT. ITPRENEUR INDONESIA TECHNOLOGY, GFZ Helmholtz Centre for Geosciences, LUA Cof...] | fog | Link |
| 2025-02-01 | [myisp.live] | funksec | Link |
| 2025-02-01 | [DATACONSULTANTS.COM] | clop | Link |
| 2025-02-01 | [CHAMPIONHOMES.COM] | clop | Link |
| 2025-02-01 | [CIERANT.COM] | clop | Link |
| 2025-02-01 | [DATATRAC.COM] | clop | Link |
| 2025-02-01 | [Nano Health] | killsec | Link |

| Datum | Opfer | Ransomware-Gruppe | Webseite |
|------------|---------------------------------------|-------------------|----------------------|
| 2025-02-01 | [St. Nicholas School] | 8base | Link |
| 2025-02-01 | [Héron] | 8base | Link |
| 2025-02-01 | [Tan Teck Seng Electric (Co) Pte Ltd] | 8base | Link |
| 2025-02-01 | [High Learn Ltd] | 8base | Link |
| 2025-02-01 | [CAMRIDGEPORT] | spacebears | Link |
| 2025-02-01 | [Falcon Gaming] | arcusmedia | Link |
| 2025-02-01 | [Eascon] | arcusmedia | Link |
| 2025-02-01 | [Utilissimo Transportes] | arcusmedia | Link |
| 2025-02-01 | [GATTELLI SpA] | arcusmedia | Link |
| 2025-02-01 | [Technico] | arcusmedia | Link |
| 2025-02-01 | [Wireless Solutions (Morris.Domain)] | lynx | Link |

7 Quellen

7.1 Quellenverzeichnis

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

8 Impressum



Herausgeber:

Marlon Hübner
Brückenstraße 3
57629 Höchstenbach

E-Mail

info@cyberwald.com

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