



Ausgabe: 20230725

# 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

# Security-News

## Heise - Security-Alert

### ***Lücken gestopft: Apple bringt iOS 16.6, macOS 13.5, watchOS 9.6 und tvOS 16.6***

Fehlerbehebungen und vor allem sicherheitsrelevante Fixes liefern frische Apple-Updates vom Montagabend. Es gab auch Zero-Day-Löcher.

- [Link](#)

---

### ***Ivanti schließt Zero-Day-Lücke in MobileIron***

Ein Update soll Angriffe auf das Mobile Device Management mit MobileIron verhindern.

- [Link](#)

---

### ***OpenSSH 9.3p2 dichtet hochriskantes Sicherheitsleck ab***

Die OpenSSH-Entwickler haben Version 9.3p2 veröffentlicht. Sie schließt eine Sicherheitslücke, die als hochriskant gilt.

- [Link](#)

---

### ***VMware Tanzu Spring: Updates gegen teils kritische Sicherheitslücken***

Aktualisierte Versionen von VMware Tanzu Spring schließen Sicherheitslücken. Eine davon gilt als kritisch.

- [Link](#)

---

### ***Neue Notfall-Updates für Adobe Coldfusion***

Wenige Tage nach dem jüngsten außertourlichen Update kommen schon die nächsten. Eine von drei Zero-Day-Lücken wird bereits aktiv für Angriffe genutzt.

- [Link](#)

---

### ***Patchday: Oracle liefert mehr als 500 Sicherheitsupdates für über 130 Produkte***

Oracle bedenkt 508 Sicherheitslücken mit aktualisierter Software zum Juli-Patchday. Sie betreffen mehr als 130 Produkte des Unternehmens.

- [Link](#)

---

### ***Webbrowser: Google stopft 20 Sicherheitslecks in Chrome 115***

Google hat den Webbrowser Chrome in Version 115 vorgelegt. Darin bessern die Entwickler 20 Schwachstellen aus.

- [Link](#)

---

### ***Citrix: Updates schließen kritische Zero-Day-Lücke in Netscaler ADC und Gateway***

IT-Verantwortliche sollten zügig aktualisieren: Citrix hat Updates für bereits angegriffene Lücken in Netscaler ADC und Gateway veröffentlicht.

- [Link](#)

---

### ***JavaScript-Sandbox vm2: Neue kritische Schwachstelle, kein Update mehr***

Für die jüngste kritische Sicherheitslücke im Open-Source-Projekt vm2 gibt es keinen Bugfix, sondern der Betreiber rät zum Umstieg auf isolated-vm.

- [Link](#)

---

### ***Wordpress: Angriffswelle auf Woocommerce Payments läuft derzeit***

Die IT-Forscher von Wordfence beobachten eine Angriffswelle auf das Woocommerce Payments-Plug-in. Es ist auf mehr als 600.000 Websites installiert.

- [Link](#)

---

## 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.

## 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.

### CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-34362	0.940540000	0.987860000	<a href="#">Link</a>
CVE-2023-33246	0.955810000	0.991090000	<a href="#">Link</a>
CVE-2023-28121	0.937820000	0.987430000	<a href="#">Link</a>
CVE-2023-27372	0.970730000	0.996460000	<a href="#">Link</a>
CVE-2023-27350	0.971180000	0.996710000	<a href="#">Link</a>
CVE-2023-25717	0.955670000	0.991060000	<a href="#">Link</a>
CVE-2023-25194	0.918160000	0.984960000	<a href="#">Link</a>
CVE-2023-21839	0.950530000	0.989700000	<a href="#">Link</a>
CVE-2023-0669	0.965030000	0.993800000	<a href="#">Link</a>

## BSI - Warn- und Informationsdienst (WID)

Mon, 24 Jul 2023

**[NEU] [hoch] Gitea: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonym Angreifer kann eine Schwachstelle in Gitea ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Mon, 24 Jul 2023

**[NEU] [UNGEPATCHT] [kritisch] vm2: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonym Angreifer kann eine Schwachstelle in vm2 ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Mon, 24 Jul 2023

**[NEU] [hoch] Ivanti Endpoint Manager: Schwachstelle ermöglicht Denial of Service**

Ein entfernter, anonym Angreifer kann eine Schwachstelle in Ivanti Endpoint Manager ausnutzen, um einen Denial of Service Angriff durchzuführen.

- [Link](#)

Mon, 24 Jul 2023

**[NEU] [hoch] Lenovo Computer Hyperscale: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen oder Codeausführung**

Ein Angreifer aus dem angrenzenden Netzwerk oder ein lokaler Angreifer kann mehrere Schwachstellen in Lenovo Computer Hyperscale ausnutzen, um Sicherheitsvorkehrungen zu umgehen oder beliebigen Code

auszuführen.

- [Link](#)

---

Mon, 24 Jul 2023

**[UPDATE] [hoch] RPM: Schwachstelle ermöglicht Manipulation von Dateien**

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in RPM ausnutzen, um Dateien zu manipulieren.

- [Link](#)

---

Mon, 24 Jul 2023

**[UPDATE] [hoch] dbus: Mehrere Schwachstellen**

Ein lokaler Angreifer kann mehrere Schwachstellen in dbus ausnutzen, um einen Denial of Service Angriff durchzuführen, Informationen offenzulegen oder beliebigen Programmcode mit Administratorrechten auszuführen.

- [Link](#)

---

Mon, 24 Jul 2023

**[UPDATE] [hoch] git: Mehrere Schwachstellen**

Ein entfernter, anonymen Angreifer kann mehrere Schwachstellen in git ausnutzen, um Sicherheitsvorkehrungen zu umgehen und beliebigen Code auszuführen.

- [Link](#)

---

Mon, 24 Jul 2023

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

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

- [Link](#)

---

Fri, 21 Jul 2023

**[UPDATE] [hoch] poppler: Schwachstelle ermöglicht nicht spezifizierten Angriff**

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in poppler ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- [Link](#)

---

Fri, 21 Jul 2023

**[UPDATE] [kritisch] tcpdump: Mehrere Schwachstellen ermöglichen Codeausführung**

Ein entfernter, anonymen Angreifer kann mehrere Schwachstellen in tcpdump ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

---

Fri, 21 Jul 2023

**[UPDATE] [hoch] Red Hat OpenShift Container Platform: Mehrere Schwachstellen**

Ein lokaler oder entfernter, anonymen Angreifer kann mehrere Schwachstellen in Red Hat OpenShift Container Platform ausnutzen, um seine Privilegien zu erhöhen, Code zur Ausführung zu bringen oder Dateien zu manipulieren

- [Link](#)

---

Fri, 21 Jul 2023

**[UPDATE] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen**

Ein entfernter, anonymen Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um beliebigen Programmcode auszuführen, Dateien zu manipulieren, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

---

Fri, 21 Jul 2023

**[UPDATE] [hoch] Red Hat OpenStack Platform : Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in der Red Hat OpenStack Platform ausnutzen, um seine Privilegien zu erhöhen, einen Denial of Service zu verursachen oder Informationen offenzulegen.

- [Link](#)

---

Fri, 21 Jul 2023

**[UPDATE] [hoch] Red Hat OpenShift Container Platform: Mehrere Schwachstellen ermöglichen**

### ***Umgehen von Sicherheitsvorkehrungen***

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in der Red Hat OpenShift Container Platform ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

---

Fri, 21 Jul 2023

#### ***[UPDATE] [hoch] Red Hat OpenShift: Mehrere Schwachstellen***

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um einen Denial of Service Zustand herbeizuführen, Informationen offenzulegen, Dateien zu manipulieren oder Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

---

Fri, 21 Jul 2023

#### ***[UPDATE] [hoch] Red Hat OpenShift Container Platform: Schwachstelle ermöglicht Privilegien- eskalation***

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Red Hat OpenShift Container Platform ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

---

Fri, 21 Jul 2023

#### ***[UPDATE] [hoch] Oracle Communications: Mehrere Schwachstellen***

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

- [Link](#)

---

Fri, 21 Jul 2023

#### ***[UPDATE] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen ermöglichen Codeaus- führung***

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

---

Fri, 21 Jul 2023

#### ***[NEU] [hoch] HP LaserJet Pro: Schwachstelle ermöglicht Privilegieneskalation oder Offenlegung von Informationen***

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in HP LaserJet Pro ausnutzen, um seine Privilegien zu erhöhen oder Informationen offenzulegen.

- [Link](#)

---

Fri, 21 Jul 2023

#### ***[NEU] [hoch] GStreamer: Schwachstelle ermöglicht Denial of Service oder Codeausführung***

Ein entfernter, anonymer Angreifer kann eine Schwachstellen in GStreamer ausnutzen, um einen Denial of Service Zustand zu verursachen oder beliebigen Code auszuführen.

- [Link](#)

---

---

## **Sicherheitslücken Meldungen von Tenable**

Datum	Schwachstelle	Bewertung
7/24/2023	[CyberPower PowerPanel Business Management Use of Default Password (CVE-2023-25131)]	critical
7/24/2023	[Ubuntu 20.04 LTS / 22.04 LTS / 23.04 : OpenSSH vulnerability (USN-6242-1)]	critical
7/23/2023	[Fedora 38 : openssh (2023-878e04f4ae)]	critical
7/21/2023	[Oracle Application Testing Suite (Jul 2023 CPU)]	critical
7/21/2023	[Oracle Business Intelligence Enterprise Edition (OAS) (July 2023 CPU)]	critical

Datum	Schwachstelle	Bewertung
7/21/2023	[Oracle Business Intelligence Enterprise Edition (July 2023 CPU)]	critical
7/21/2023	[Oracle Business Intelligence Publisher (OBIEE) (July 2023 CPU)]	critical
7/21/2023	[FreeBSD : OpenSSH – remote code execution via a forwarded agent socket (887eb570-27d3-11ee-adba-c80aa9043978)]	critical
7/21/2023	[Netwrix Auditor < 10.5 Insecure Object Deserialization]	critical
7/21/2023	[Oracle MySQL Enterprise Monitor (Jul 2023 CPU)]	critical
7/24/2023	[Ubuntu 23.04 : FRR vulnerability (USN-6240-1)]	high
7/24/2023	[macOS 12.x < 12.6.8 Multiple Vulnerabilities (HT213844)]	high
7/24/2023	[macOS 13.x < 13.5 Multiple Vulnerabilities (HT213843)]	high
7/24/2023	[macOS 11.x < 11.7.9 Multiple Vulnerabilities (HT213845)]	high
7/23/2023	[Fedora 37 : kernel / kernel-headers / kernel-tools (2023-3661f028b8)]	high
7/23/2023	[Fedora 38 : kernel / kernel-headers / kernel-tools (2023-e4e985b5dd)]	high
7/23/2023	[Fedora 37 : ghostscript (2023-83c805b441)]	high
7/23/2023	[Debian DSA-5457-1 : webkit2gtk - security update]	high
7/23/2023	[FreeBSD : gitea – Disallow dangerous URL schemes (ab0bab3c-2927-11ee-8608-07b8d3947721)]	high
7/22/2023	[Fedora 37 : dotnet7.0 (2023-18264c31f6)]	high
7/22/2023	[Fedora 38 : dotnet7.0 (2023-d25e798d6c)]	high
7/22/2023	[Fedora 38 : dotnet6.0 (2023-feda45bc39)]	high
7/22/2023	[Fedora 38 : libopenmpt (2023-5f840297cb)]	high
7/22/2023	[Fedora 37 : dotnet6.0 (2023-4a48637c3f)]	high
7/21/2023	[Oracle Linux 8 : kernel (ELSA-2023-3847)]	high
7/21/2023	[Oracle Identity Manager (Jul 2023 CPU)]	high
7/21/2023	[Oracle Linux 7 : firefox (ELSA-2023-4079)]	high
7/21/2023	[Veritas InfoScale Operations Manager prior to 8.0.0.410 Insecure File Upload (VTS23-009)]	high

## Die Hacks der Woche

mit Martin Haunschmid

Ein gefundenes Fressen für Cloud Gegner? Microsoft GEHACKT!



[Zum Youtube Video](#)



## Cyberangriffe: (Jul)

Datum	Opfer	Land	Information
2023-07-20	ITL Industries Ltd	[IND]	<a href="#">Link</a>
2023-07-18	Ortivus	[SWE]	<a href="#">Link</a>
2023-07-16	TOMRA	[NOR]	<a href="#">Link</a>
2023-07-16	Helix	[RUS]	<a href="#">Link</a>
2023-07-16	George County	[USA]	<a href="#">Link</a>
2023-07-13	Morehead State University	[USA]	<a href="#">Link</a>
2023-07-12	Comune di Ferrara	[ITA]	<a href="#">Link</a>
2023-07-11	ZooTampa	[USA]	<a href="#">Link</a>
2023-07-11	Ville de Cornelius	[USA]	<a href="#">Link</a>
2023-07-11	Tribunal de Contas do Estado do Rio de Janeiro (TCE-RJ)	[BRA]	<a href="#">Link</a>
2023-07-11	La Province de Namur	[BEL]	<a href="#">Link</a>
2023-07-09	Ville de Hayward	[USA]	<a href="#">Link</a>
2023-07-08	Ventia	[AUS]	<a href="#">Link</a>
2023-07-08	Comté de Kent	[USA]	<a href="#">Link</a>
2023-07-07	Université de l'Ouest de l'Écosse (UWS)	[GBR]	<a href="#">Link</a>
2023-07-07	Bureau du Procureur Général et le Ministère des Affaires Juridiques de Trinité-et-Tobago (AGLA)	[TTO]	<a href="#">Link</a>
2023-07-07	Jackson Township	[USA]	<a href="#">Link</a>
2023-07-07	Maison Mercier	[FRA]	<a href="#">Link</a>
2023-07-07	Diputación Provincial de Zaragoza	[ESP]	<a href="#">Link</a>
2023-07-06	Commission électorale du Pakistan (ECP)	[PAK]	<a href="#">Link</a>
2023-07-05	Hôpital universitaire Luigi Vanvitelli de Naples	[ITA]	<a href="#">Link</a>
2023-07-04	Nagoya Port Transport Association	[JPN]	<a href="#">Link</a>
2023-07-04	Roys of Wroxham	[GBR]	<a href="#">Link</a>
2023-07-04	ibis acam	[AUT]	<a href="#">Link</a>
2023-07-04	Meteolux.lu	[LUX]	<a href="#">Link</a>
2023-07-02	Aéroport de Montpellier	[FRA]	<a href="#">Link</a>
2023-07-02	Ville d'Agen	[FRA]	<a href="#">Link</a>

## Ransomware-Erpressungen: (Jul)

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-07-25	[Republic.bz]	alphv	<a href="#">Link</a>
2023-07-25	[NEBRASKALAND]	alphv	<a href="#">Link</a>
2023-07-24	[IT Luggage]	blacksuit	<a href="#">Link</a>
2023-07-24	[John Mulder Heating & Air Conditioning]	play	<a href="#">Link</a>
2023-07-24	[Scharco Elektronik]	play	<a href="#">Link</a>
2023-07-24	[Primoteq]	play	<a href="#">Link</a>
2023-07-24	[Grupo MH]	play	<a href="#">Link</a>
2023-07-24	[FERRE BARNIEDO]	play	<a href="#">Link</a>
2023-07-24	[BION_2]	blackbasta	<a href="#">Link</a>
2023-07-24	[El Milagro]	akira	<a href="#">Link</a>
2023-07-24	[SBM]	akira	<a href="#">Link</a>
2023-07-24	[dynamite]	stormous	<a href="#">Link</a>
2023-07-24	[Charles & Colvard Ltd.]	akira	<a href="#">Link</a>
2023-07-24	[ebpsupply.com]	lockbit3	<a href="#">Link</a>
2023-07-24	[Collins Aerospace (An RTX Business)]	bianlian	<a href="#">Link</a>
2023-07-24	[EJM Engineered Systems]	8base	<a href="#">Link</a>
2023-07-23	[Franklins european bathrooms]	mallox	<a href="#">Link</a>
2023-07-23	[Exbon Development, Inc]	8base	<a href="#">Link</a>
2023-07-23	[Jackson Township Police Department and Administration.]	donutleaks	<a href="#">Link</a>
2023-07-23	[championgse.com]	lockbit3	<a href="#">Link</a>
2023-07-23	[THE COLLINS LAW FIRM]	alphv	<a href="#">Link</a>
2023-07-20	[Pechexport]	cyclops	<a href="#">Link</a>
2023-07-20	[Cvlan]	cyclops	<a href="#">Link</a>
2023-07-23	[Sun Pain Management]	medusa	<a href="#">Link</a>
2023-07-23	[Cafe Britt]	medusa	<a href="#">Link</a>
2023-07-22	[Chan and Associates]	8base	<a href="#">Link</a>
2023-07-22	[Siden & Associates Press Release]	monti	<a href="#">Link</a>
2023-07-22	[Hungarian Investment Promotion Agency Press Release]	monti	<a href="#">Link</a>
2023-07-22	[Samson Electric]	play	<a href="#">Link</a>
2023-07-22	[Axiety]	rhysida	<a href="#">Link</a>
2023-07-22	[Bartlett]	blackbasta	<a href="#">Link</a>
2023-07-21	[Azimut.it]	alphv	<a href="#">Link</a>
2023-07-21	[Yamaha Canada Music Ltd]	akira	<a href="#">Link</a>
2023-07-21	[Hirsch Bedner Associates]	alphv	<a href="#">Link</a>
2023-07-21	[CORDELL]	alphv	<a href="#">Link</a>
2023-07-21	[plbint.com]	abyss	<a href="#">Link</a>
2023-07-20	[Bright Future Electric, LLC ]	akira	<a href="#">Link</a>
2023-07-20	[Corinium Carpets]	noescape	<a href="#">Link</a>
2023-07-20	[Tampa General Hospital]	nokoyawa	<a href="#">Link</a>
2023-07-20	[CANAROPA Inc]	nokoyawa	<a href="#">Link</a>
2023-07-20	[Campbell Killin Brittan & Ray LLC]	alphv	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-07-20	[Entegra]	alphv	<a href="#">Link</a>
2023-07-20	[Alberto Couto Alves]	cactus	<a href="#">Link</a>
2023-07-20	[Agoravita]	cactus	<a href="#">Link</a>
2023-07-20	[American Meteorological Society]	cactus	<a href="#">Link</a>
2023-07-20	[Biocair International]	cactus	<a href="#">Link</a>
2023-07-20	[Confartigianato Federimpresa FC]	cactus	<a href="#">Link</a>
2023-07-20	[ScanSource]	cactus	<a href="#">Link</a>
2023-07-20	[CWS]	cactus	<a href="#">Link</a>
2023-07-20	[Hawa Sliding Solutions]	cactus	<a href="#">Link</a>
2023-07-20	[Imagination]	cactus	<a href="#">Link</a>
2023-07-20	[Italkraft]	cactus	<a href="#">Link</a>
2023-07-20	[Michigan Production Machining]	cactus	<a href="#">Link</a>
2023-07-20	[Novobit]	cactus	<a href="#">Link</a>
2023-07-20	[Artemide]	cactus	<a href="#">Link</a>
2023-07-20	[Reyes Automotive Group]	cactus	<a href="#">Link</a>
2023-07-20	[Rotomail Italia SpA]	cactus	<a href="#">Link</a>
2023-07-20	[Phoenix Taxis]	cactus	<a href="#">Link</a>
2023-07-20	[Wasserstrom]	cactus	<a href="#">Link</a>
2023-07-20	[Americold]	cactus	<a href="#">Link</a>
2023-07-20	[cityserve-mech.co.uk]	lockbit3	<a href="#">Link</a>
2023-07-20	[Hightway Care]	bianlian	<a href="#">Link</a>
2023-07-20	[Magnolia Steel]	bianlian	<a href="#">Link</a>
2023-07-20	[New Braunfels Cardiology]	bianlian	<a href="#">Link</a>
2023-07-19	[Anesco Ltd]	8base	<a href="#">Link</a>
2023-07-19	[Kensington Publishing]	play	<a href="#">Link</a>
2023-07-19	[Fernmoor Homes]	play	<a href="#">Link</a>
2023-07-19	[ECS Technology Group]	play	<a href="#">Link</a>
2023-07-19	[Woodbine Hospitality]	play	<a href="#">Link</a>
2023-07-19	[Sea Force IX]	play	<a href="#">Link</a>
2023-07-19	[Centennial Management]	play	<a href="#">Link</a>
2023-07-19	[Undisclosed Aerospace Company]	bianlian	<a href="#">Link</a>
2023-07-19	[Cumberland Pharmaceuticals Inc.]	bianlian	<a href="#">Link</a>
2023-07-19	[Braintree Public Schools]	royal	<a href="#">Link</a>
2023-07-19	[obeidpartners.com]	lockbit3	<a href="#">Link</a>
2023-07-19	[Lumberton Independent School District]	rhysida	<a href="#">Link</a>
2023-07-19	[PWCCLINETSANDDOCUMENTS.COM]	clp	<a href="#">Link</a>
2023-07-19	[DMA.US]	clp	<a href="#">Link</a>
2023-07-19	[VENTIVTECH.COM]	clp	<a href="#">Link</a>
2023-07-19	[BLUEFIN.COM]	clp	<a href="#">Link</a>
2023-07-19	[ESTEELAUDER.COM]	clp	<a href="#">Link</a>
2023-07-19	[OFCOM.ORG.UK]	clp	<a href="#">Link</a>
2023-07-19	[ALLEGIANTAIR.COM]	clp	<a href="#">Link</a>
2023-07-19	[ITT.COM]	clp	<a href="#">Link</a>
2023-07-19	[SMC3.COM]	clp	<a href="#">Link</a>
2023-07-19	[COMREG.IE]	clp	<a href="#">Link</a>
2023-07-19	[JONASFITNESS.COM]	clp	<a href="#">Link</a>
2023-07-19	[AA.COM]	clp	<a href="#">Link</a>
2023-07-18	[EA SMITH]	alphv	<a href="#">Link</a>
2023-07-19	[VOG]	alphv	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-07-18	[The Estée Lauder Companies]	alphv	<a href="#">Link</a>
2023-07-18	[DTD Express ]	medusa	<a href="#">Link</a>
2023-07-18	[KUITs]	alphv	<a href="#">Link</a>
2023-07-18	[Tampa general hospital]	snatch	<a href="#">Link</a>
2023-07-18	[Acomen]	noescape	<a href="#">Link</a>
2023-07-18	[Girardini Holding Srl]	noescape	<a href="#">Link</a>
2023-07-18	[Health Springs Medical Center ]	medusa	<a href="#">Link</a>
2023-07-18	[Nini Collection Ltd (Nini's Jewels)]	medusa	<a href="#">Link</a>
2023-07-18	[lfcaire.org]	lockbit3	<a href="#">Link</a>
2023-07-18	[suninsurance.com.fj]	lockbit3	<a href="#">Link</a>
2023-07-18	[berg-life.com]	lockbit3	<a href="#">Link</a>
2023-07-18	[cotrelec.com]	lockbit3	<a href="#">Link</a>
2023-07-18	[ope.com.na]	lockbit3	<a href="#">Link</a>
2023-07-18	[dixiesfed.com]	lockbit3	<a href="#">Link</a>
2023-07-18	[flexity.com]	lockbit3	<a href="#">Link</a>
2023-07-18	[www.brockhouse.co.uk]	abyss	<a href="#">Link</a>
2023-07-18	[academia21.com]	lockbit3	<a href="#">Link</a>
2023-07-18	[CashCall, Inc.]	8base	<a href="#">Link</a>
2023-07-18	[Seasia Infotech]	snatch	<a href="#">Link</a>
2023-07-18	[Ningbo Joyson Electronic Corp.]	snatch	<a href="#">Link</a>
2023-07-18	[Wasserstrom]	snatch	<a href="#">Link</a>
2023-07-17	[Protected: Hidden name]	medusalocker	<a href="#">Link</a>
2023-07-17	[Senior]	stormous	<a href="#">Link</a>
2023-07-17	[hopetech.com]	lockbit3	<a href="#">Link</a>
2023-07-17	[johnreilly.co.uk]	lockbit3	<a href="#">Link</a>
2023-07-17	[Cavanaugh, Biggs & Lemon P.A., Attorneys at Law]	alphv	<a href="#">Link</a>
2023-07-17	[www.tractrad.com]	abyss	<a href="#">Link</a>
2023-07-17	[RCI.COM]	clon	<a href="#">Link</a>
2023-07-17	[SIERRAWIRELESS.COM]	clon	<a href="#">Link</a>
2023-07-17	[COMPUCOM.COM]	clon	<a href="#">Link</a>
2023-07-17	[CFINS.COM]	clon	<a href="#">Link</a>
2023-07-17	[DESMI.COM]	clon	<a href="#">Link</a>
2023-07-17	[FMGL.COM.AU]	clon	<a href="#">Link</a>
2023-07-17	[VALMET.COM]	clon	<a href="#">Link</a>
2023-07-17	[VITESCO-TECHNOLOGIES.COM]	clon	<a href="#">Link</a>
2023-07-17	[TJX.COM]	clon	<a href="#">Link</a>
2023-07-17	[Stephen F. Austin State University]	rhysida	<a href="#">Link</a>
2023-07-17	[IRIS Informatique]	rhysida	<a href="#">Link</a>
2023-07-17	[ICT-College]	rhysida	<a href="#">Link</a>
2023-07-15	[Venture Drilling Supply]	8base	<a href="#">Link</a>
2023-07-16	[test.com]	lockbit3	<a href="#">Link</a>
2023-07-11	[selmi.com.br]	lockbit3	<a href="#">Link</a>
2023-07-16	[www.stri.se]	abyss	<a href="#">Link</a>
2023-07-16	[Baumschlager Hutter Partners - Business Information]	alphv	<a href="#">Link</a>
2023-07-16	[www.arb.ch]	abyss	<a href="#">Link</a>
2023-07-11	[Propper International]	moneymessage	<a href="#">Link</a>
2023-07-14	[Meteksan Defence Industry]	moneymessage	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-07-15	[equmedia.es]	lockbit3	<a href="#">Link</a>
2023-07-15	[jasperpictures]	stormous	<a href="#">Link</a>
2023-07-15	[magnumphotos.com]	lockbit3	<a href="#">Link</a>
2023-07-15	[konrad-mr.de]	lockbit3	<a href="#">Link</a>
2023-07-15	[greatlakesmbpm.com]	lockbit3	<a href="#">Link</a>
2023-07-15	[hgc.com.hk]	lockbit3	<a href="#">Link</a>
2023-07-15	[province.namur.be]	lockbit3	<a href="#">Link</a>
2023-07-15	[energym.co.il]	lockbit3	<a href="#">Link</a>
2023-07-15	[co.langlade.wi.us]	lockbit3	<a href="#">Link</a>
2023-07-15	[Highland Health Systems]	alphv	<a href="#">Link</a>
2023-07-14	[Chin Hin Group]	alphv	<a href="#">Link</a>
2023-07-14	[Caterham High School]	rhysida	<a href="#">Link</a>
2023-07-08	[Superloop ISP]	cyclops	<a href="#">Link</a>
2023-07-14	[NOTABLEFRONTIER.COM]	clp	<a href="#">Link</a>
2023-07-14	[GRACE.COM]	clp	<a href="#">Link</a>
2023-07-14	[PRGX.COM]	clp	<a href="#">Link</a>
2023-07-14	[HESS.COM]	clp	<a href="#">Link</a>
2023-07-14	[MYCWT.COM]	clp	<a href="#">Link</a>
2023-07-14	[SCHNABEL-ENG.COM]	clp	<a href="#">Link</a>
2023-07-14	[ARIETISHEALTH.COM]	clp	<a href="#">Link</a>
2023-07-14	[PINNACLETPA.COM]	clp	<a href="#">Link</a>
2023-07-14	[REPSOLSINOPECUK.COM]	clp	<a href="#">Link</a>
2023-07-11	[Jordan Airmotive Ltd]	noescape	<a href="#">Link</a>
2023-07-11	[Burton & South Derbyshire College]	noescape	<a href="#">Link</a>
2023-07-14	[JTI.COM]	clp	<a href="#">Link</a>
2023-07-14	[VOSS.NET]	clp	<a href="#">Link</a>
2023-07-14	[UFCU.ORG]	clp	<a href="#">Link</a>
2023-07-14	[YAKULT.COM.PH]	clp	<a href="#">Link</a>
2023-07-14	[ROCHESTER.EDU]	clp	<a href="#">Link</a>
2023-07-14	[eyedoc.com.na]	lockbit3	<a href="#">Link</a>
2023-07-14	[CPA Advisors Group]	8base	<a href="#">Link</a>
2023-07-14	[Info Salons]	8base	<a href="#">Link</a>
2023-07-14	[The Big Life group]	rhysida	<a href="#">Link</a>
2023-07-13	[Gerber ChildrenswearLLC]	akira	<a href="#">Link</a>
2023-07-13	[Blackjewel L.L.C.]	lockbit3	<a href="#">Link</a>
2023-07-13	[SHUTTERFLY.COM]	clp	<a href="#">Link</a>
2023-07-13	[DISCOVERY.COM]	clp	<a href="#">Link</a>
2023-07-13	[ASPENTECH.COM]	clp	<a href="#">Link</a>
2023-07-13	[MOTHERSON.COM]	clp	<a href="#">Link</a>
2023-07-13	[PAYCOM.COM]	clp	<a href="#">Link</a>
2023-07-13	[Telepizza]	8base	<a href="#">Link</a>
2023-07-13	[The Traffic Tech]	8base	<a href="#">Link</a>
2023-07-13	[Quikcard Solutions Inc.]	8base	<a href="#">Link</a>
2023-07-13	[Jadranka Group]	8base	<a href="#">Link</a>
2023-07-13	[Dental One Craigieburn]	8base	<a href="#">Link</a>
2023-07-13	[ANL Packaging]	8base	<a href="#">Link</a>
2023-07-13	[BTU]	8base	<a href="#">Link</a>
2023-07-12	[Ministerio de Cultura de la Republica de Cuba "STORMOUS + GhostSec "]	stormous	<a href="#">Link</a>
2023-07-12	[Ministry of Foreign Trade "STORMOUS + GhostSec "]	stormous	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-07-12	[Ministry of Energy and Mines (Cuba) ” STORMOUS + GhostSec ”]	stormous	<a href="#">Link</a>
2023-07-12	[GRIPA.ORG]	clop	<a href="#">Link</a>
2023-07-12	[SLB.COM]	clop	<a href="#">Link</a>
2023-07-12	[AMCTHEATRES.COM]	clop	<a href="#">Link</a>
2023-07-12	[AINT.COM]	clop	<a href="#">Link</a>
2023-07-12	[JACKENTERTAINMENT.COM]	clop	<a href="#">Link</a>
2023-07-12	[NASCO.COM]	clop	<a href="#">Link</a>
2023-07-12	[TGIDIRECT.COM]	clop	<a href="#">Link</a>
2023-07-12	[HONEYWELL.COM]	clop	<a href="#">Link</a>
2023-07-12	[CLEARERESULT.COM]	clop	<a href="#">Link</a>
2023-07-12	[RADIUSGS.COM]	clop	<a href="#">Link</a>
2023-07-09	[Bitimen exchange]	arvinclub	<a href="#">Link</a>
2023-07-12	[affinityhealthservices.ne]	lockbit3	<a href="#">Link</a>
2023-07-12	[ATS Infrastructure]	bianlian	<a href="#">Link</a>
2023-07-12	[Henock Construction]	bianlian	<a href="#">Link</a>
2023-07-12	[Lyon & Healy]	bianlian	<a href="#">Link</a>
2023-07-12	[Mission Parks]	bianlian	<a href="#">Link</a>
2023-07-07	[Innodis Group]	noescape	<a href="#">Link</a>
2023-07-12	[Divgi-TTS was hacked. Due to the extreme low level of security, a huge amount of confident]	alphv	<a href="#">Link</a>
2023-07-12	[Eastin Hotel Makkasan Bangkok was hacked. Customers’ financial and personal information ha]	alphv	<a href="#">Link</a>
2023-07-12	[SMS-SME was hacked. A huge amount of confidential information was stolen, information of c]	alphv	<a href="#">Link</a>
2023-07-12	[Algeiba.com has a critical level of security on its network. Customer and partner data is ]	alphv	<a href="#">Link</a>
2023-07-12	[Amber Court 2020 was hacking. A lot of customers’ personal information was stolen.]	alphv	<a href="#">Link</a>
2023-07-12	[Maruchan Inc]	alphv	<a href="#">Link</a>
2023-07-12	[Schmidt Salzman & Moran, Ltd]	akira	<a href="#">Link</a>
2023-07-12	[Wright Moore DeHart Dupuis & Hutchinson]	alphv	<a href="#">Link</a>
2023-07-12	[Better System Co.,Ltd]	qilin	<a href="#">Link</a>
2023-07-08	[Protactics]	noescape	<a href="#">Link</a>
2023-07-11	[CONSOLEENERGY.COM]	clop	<a href="#">Link</a>
2023-07-11	[KALEAERO.COM]	clop	<a href="#">Link</a>
2023-07-11	[AGILYSYS.COM]	clop	<a href="#">Link</a>
2023-07-11	[SCCU.COM]	clop	<a href="#">Link</a>
2023-07-11	[ARVATO.COM]	clop	<a href="#">Link</a>
2023-07-11	[RITEAID.COM]	clop	<a href="#">Link</a>
2023-07-11	[PIONEERELECTRONICS.COM]	clop	<a href="#">Link</a>
2023-07-11	[BAM.COM.GT]	clop	<a href="#">Link</a>
2023-07-11	[TOMTOM.COM]	clop	<a href="#">Link</a>
2023-07-11	[EMERSON.COM]	clop	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-07-11	[berjaya]	stormous	<a href="#">Link</a>
2023-07-11	[Ingersoll Rand]	stormous	<a href="#">Link</a>
2023-07-11	[Arrowall]	stormous	<a href="#">Link</a>
2023-07-11	[OKS]	stormous	<a href="#">Link</a>
2023-07-11	[Matrix]	stormous	<a href="#">Link</a>
2023-07-11	[treenovum.es]	stormous	<a href="#">Link</a>
2023-07-11	[archiplusinter.com]	stormous	<a href="#">Link</a>
2023-07-11	[marehotels]	stormous	<a href="#">Link</a>
2023-07-11	[mamboafrikaadventure]	stormous	<a href="#">Link</a>
2023-07-11	[Nipun Consultancy]	stormous	<a href="#">Link</a>
2023-07-11	[Murfreesboro Medical Clinic]	bianlian	<a href="#">Link</a>
2023-07-11	[A123 Systems]	akira	<a href="#">Link</a>
2023-07-11	[MicroPort Scientific / LivaNova]	qilin	<a href="#">Link</a>
2023-07-11	[panoramaeyecare.com]	lockbit3	<a href="#">Link</a>
2023-07-11	[Pesquera Diamante S.A.]	8base	<a href="#">Link</a>
2023-07-11	[Weitkamp · Hirsch and Kollegen Steuerberatungsgesellschaft mbH]	8base	<a href="#">Link</a>
2023-07-11	[gis4.addison-il]	cuba	<a href="#">Link</a>
2023-07-08	[Weitkamp · Hirsch & Kollegen Steuerberatungsgesellschaft mbH]	8base	<a href="#">Link</a>
2023-07-08	[Kansas medical center LLC]	8base	<a href="#">Link</a>
2023-07-08	[Danbury Public Schools]	8base	<a href="#">Link</a>
2023-07-08	[Advanced Fiberglass Industries]	8base	<a href="#">Link</a>
2023-07-08	[Citelis Mobility]	8base	<a href="#">Link</a>
2023-07-08	[Motor Components, LLC]	8base	<a href="#">Link</a>
2023-07-10	[RICOHACUMEN.COM]	clop	<a href="#">Link</a>
2023-07-10	[SMA.DE]	clop	<a href="#">Link</a>
2023-07-10	[VRM.DE]	clop	<a href="#">Link</a>
2023-07-10	[UMASSMED.EDU]	clop	<a href="#">Link</a>
2023-07-10	[VISIONWARE.CA]	clop	<a href="#">Link</a>
2023-07-10	[JHU.EDU]	clop	<a href="#">Link</a>
2023-07-10	[FMFCU.ORG]	clop	<a href="#">Link</a>
2023-07-10	[JPRMP.COM]	clop	<a href="#">Link</a>
2023-07-10	[WESTAT.COM]	clop	<a href="#">Link</a>
2023-07-10	[RADISSONHOTELSAMERICA.COM]	clop	<a href="#">Link</a>
2023-07-10	[Hamre Schumann Mueller & Larson HSML]	akira	<a href="#">Link</a>
2023-07-10	[Belize Electricity Limited - Leaked]	ragnarlocker	<a href="#">Link</a>
2023-07-10	[Green Diamond]	akira	<a href="#">Link</a>
2023-07-10	[Citta Nuova]	rhysida	<a href="#">Link</a>
2023-07-09	[leeindustries.com]	lockbit3	<a href="#">Link</a>
2023-07-09	[Garuda Indonesia]	mallox	<a href="#">Link</a>
2023-07-09	[roys.co.uk]	lockbit3	<a href="#">Link</a>
2023-07-09	[Evergreen Seamless Pipes & Tubes]	bianlian	<a href="#">Link</a>
2023-07-03	[Peroni Pompe]	donutleaks	<a href="#">Link</a>
2023-07-08	[Cabra Consulting Ltd]	8base	<a href="#">Link</a>
2023-07-07	[Tracker de Colombia SAS]	medusa	<a href="#">Link</a>
2023-07-07	[Lane Valente Industries]	play	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-07-07	[New Century Advisors, LLC]	8base	<a href="#">Link</a>
2023-07-07	[ROBERT L BAYLESS PRODUCER LLC]	8base	<a href="#">Link</a>
2023-07-07	[Industrial Heat Transfer (iht-inc.com)]	rancoz	<a href="#">Link</a>
2023-07-07	[CROWE.COM]	clop	<a href="#">Link</a>
2023-07-07	[AUTOZONE.COM]	clop	<a href="#">Link</a>
2023-07-07	[BCDTRAVEL.COM]	clop	<a href="#">Link</a>
2023-07-07	[AMERICANNATIONAL.COM]	clop	<a href="#">Link</a>
2023-07-07	[USG.EDU]	clop	<a href="#">Link</a>
2023-07-07	[CYTOMX.COM]	clop	<a href="#">Link</a>
2023-07-07	[MARYKAY.COM]	clop	<a href="#">Link</a>
2023-07-07	[FISCDP.COM]	clop	<a href="#">Link</a>
2023-07-07	[KERNAGENCY.COM]	clop	<a href="#">Link</a>
2023-07-07	[UOFLHEALTH.ORG]	clop	<a href="#">Link</a>
2023-07-07	[L8SOLUTIONS.CO.UK]	clop	<a href="#">Link</a>
2023-07-07	[TDAMERITRADE.COM]	clop	<a href="#">Link</a>
2023-07-07	[Kenya Bureau Of Standards]	rhysida	<a href="#">Link</a>
2023-07-07	[Lazer Tow]	play	<a href="#">Link</a>
2023-07-07	[Star Island Resort]	play	<a href="#">Link</a>
2023-07-07	[Indiana Dimension]	play	<a href="#">Link</a>
2023-07-07	[Lawer SpA]	play	<a href="#">Link</a>
2023-07-06	[DELARUE.COM]	clop	<a href="#">Link</a>
2023-07-06	[ENERGYTRANSFER.COM]	clop	<a href="#">Link</a>
2023-07-06	[PAYCOR.COM]	clop	<a href="#">Link</a>
2023-07-06	[NETSCOUT.COM]	clop	<a href="#">Link</a>
2023-07-06	[WOLTERSKLUWER.COM]	clop	<a href="#">Link</a>
2023-07-06	[CADENCEBANK.COM]	clop	<a href="#">Link</a>
2023-07-06	[BANKWITHUNITED.COM]	clop	<a href="#">Link</a>
2023-07-06	[NEWERATECH.COM]	clop	<a href="#">Link</a>
2023-07-06	[NST Attorneys at Law]	play	<a href="#">Link</a>
2023-07-06	[Uniquify]	play	<a href="#">Link</a>
2023-07-06	[Geneva Software]	play	<a href="#">Link</a>
2023-07-06	[MUJI Europe Holdings Limited]	play	<a href="#">Link</a>
2023-07-06	[Betty Lou's]	play	<a href="#">Link</a>
2023-07-06	[Capacity LLC]	play	<a href="#">Link</a>
2023-07-06	[Safety Network]	play	<a href="#">Link</a>
2023-07-06	[Carvin Software]	bianlian	<a href="#">Link</a>
2023-07-06	[Ella Insurance Brokerage]	bianlian	<a href="#">Link</a>
2023-07-06	[betalandservices.com]	lockbit3	<a href="#">Link</a>
2023-07-06	[chasc.org]	lockbit3	<a href="#">Link</a>
2023-07-06	[cls-group.com]	lockbit3	<a href="#">Link</a>
2023-07-06	[gacegypt.net]	lockbit3	<a href="#">Link</a>
2023-07-06	[siegfried.com.mx]	lockbit3	<a href="#">Link</a>
2023-07-06	[Pinnergy]	akira	<a href="#">Link</a>
2023-07-06	[Bangladesh Krishi Bank]	alphv	<a href="#">Link</a>
2023-07-06	[ASIC Soluciones]	qilin	<a href="#">Link</a>
2023-07-06	[KIRWIN FRYDAY MEDCALF Lawyers LLP]	8base	<a href="#">Link</a>
2023-07-05	[TRANSPERFECT.COM]	clop	<a href="#">Link</a>
2023-07-05	[QUORUMFCU.ORG]	clop	<a href="#">Link</a>
2023-07-05	[MERATIVE.COM]	clop	<a href="#">Link</a>
2023-07-05	[NORGREN.COM]	clop	<a href="#">Link</a>
2023-07-05	[CIENA.COM]	clop	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2023-07-05	[KYBURZDRUCK.CH]	clop	<a href="#">Link</a>
2023-07-05	[UNITEDREGIONAL.ORG]	clop	<a href="#">Link</a>
2023-07-05	[TDECU.ORG]	clop	<a href="#">Link</a>
2023-07-05	[BRADYID.COM]	clop	<a href="#">Link</a>
2023-07-05	[BARRICK.COM]	clop	<a href="#">Link</a>
2023-07-05	[DURR.COM]	clop	<a href="#">Link</a>
2023-07-05	[ZooTampa at Lowry Park]	blacksuit	<a href="#">Link</a>
2023-07-05	[Avalign Technologies]	blackbyte	<a href="#">Link</a>
2023-07-05	[Portugal Scotturb Data Leaked]	ragnarlocker	<a href="#">Link</a>
2023-07-03	[guestgroup.com.au]	lockbit3	<a href="#">Link</a>
2023-07-05	[Murphy]	akira	<a href="#">Link</a>
2023-07-05	[eurosupport.com]	lockbit3	<a href="#">Link</a>
2023-07-05	[recamlaser.com]	lockbit3	<a href="#">Link</a>
2023-07-05	[mitr.com]	lockbit3	<a href="#">Link</a>
2023-07-04	[Hoosier Equipment company]	medusalocker	<a href="#">Link</a>
2023-07-04	[Yunus Emre Institute Turkey]	medusa	<a href="#">Link</a>
2023-07-04	[Polanglo]	8base	<a href="#">Link</a>
2023-07-03	[Jefferson County Health Center]	karakurt	<a href="#">Link</a>
2023-07-03	[snjb.net]	lockbit3	<a href="#">Link</a>
2023-07-03	[oneexchange corp.com]	lockbit3	<a href="#">Link</a>
2023-07-03	[Townsquare Media Inc]	alphv	<a href="#">Link</a>
2023-07-03	[Ayuntamiento de Arganda City Council]	rhysida	<a href="#">Link</a>
2023-07-03	[Duncan Disability Law]	alphv	<a href="#">Link</a>
2023-07-03	[Hollywood Forever]	rhysida	<a href="#">Link</a>
2023-07-03	[Mutuelle LMP]	medusa	<a href="#">Link</a>
2023-07-03	[Luna Hotels & Resorts ]	medusa	<a href="#">Link</a>
2023-07-03	[BM GROUP POLYTEC S.p.A.]	rhysida	<a href="#">Link</a>
2023-07-03	[Brett Martin]	blackbyte	<a href="#">Link</a>
2023-07-02	[blowtherm.it]	lockbit3	<a href="#">Link</a>
2023-07-02	[Ucamco Belgium]	medusalocker	<a href="#">Link</a>
2023-07-01	[Ashley HomeStore]	mallox	<a href="#">Link</a>
2023-07-01	[Blount Fine Foods]	blackbasta	<a href="#">Link</a>
2023-07-01	[Blount]	blackbasta	<a href="#">Link</a>
2023-07-01	[DVA - DVision Architecture]	ransomexx	<a href="#">Link</a>
2023-07-01	[Kondratoff Persick LLP]	bianlian	<a href="#">Link</a>
2023-07-01	[Undisclosed Staffing Company]	bianlian	<a href="#">Link</a>

# Quellen

## 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) Die Hacks der Woche - <https://martinhaunschmid.com/videos>

# Impressum



***Herausgeber:***

Marlon Hübner  
Brückenstraße 3  
57629 Höchstenbach

***E-Mail***

[info@cyberwald.com](mailto:info@cyberwald.com)

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