



Ausgabe: 20230715

# 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

### ***PoC-Exploit verfügbar: Adobe legt Patch für Coldfusion nach***

Kurz nach dem Juli-Patchday legt Adobe weitere Updates nach, um eine kritische Schwachstelle in Coldfusion abzudichten. PoC-Exploitcode wurde entdeckt.

- [Link](#)

---

### ***Cisco schließt kritische Lücke in SD-WAN vManage***

Cisco warnt vor einer kritischen Schwachstelle in SD-WAN vManage, die Angreifern aus dem Netz die Übernahme verwundbarer Systeme ermöglicht.

- [Link](#)

---

### ***Groupware Zimbra: Zero-Day-Lücke macht manuelles Patchen nötig***

Zimbra hat einen manuell anzuwendenden Patch veröffentlicht, der eine Zero-Day-Sicherheitslücke in der Groupware schließt.

- [Link](#)

---

### ***Codeschmuggel-Lücke in Ghostscript betrifft LibreOffice und mehr***

Eine Lücke in Ghostscript, die Einschmuggeln von Schadcode erlaubt, betrifft Linux-Systeme und Software wie LibreOffice oder Inkscape – auch unter Windows.

- [Link](#)

---

### ***Webkonferenzen: Zoom schließt mehrere Sicherheitslücken***

Vor allem in Zoom Rooms und im Zoom Desktop-Client für Windows schlummern hochriskante Sicherheitslücken. Updates stehen bereit.

- [Link](#)

---

### ***Update gegen kritische Lücke in FortiOS/FortiProxy***

Fortinet verteilt Sicherheitsupdates für FortiOS/FortiProxy. Sie schließen eine kritische Sicherheitslücke.

- [Link](#)

---

### ***Teils kritische Sicherheitslücken in Citrix' Secure Access Clients***

Citrix hat Aktualisierungen für die Secure Access Clients veröffentlicht, die teils kritische Schwachstellen ausbessern.

- [Link](#)

---

### ***Patchday: Kritische Schwachstellen in Adobe Indesign und Coldfusion abgedichtet***

Der Juli-Patchday von Adobe bringt Sicherheitsupdates für Indesign und Coldfusion. Sie schließen Lücken, die der Hersteller als kritisches Risiko einstuft.

- [Link](#)

---

### ***Patchday: Microsoft meldet fünf Zero-Days, teils ohne Update***

Der Juli-Patchday von Microsoft liefert viele Updates: 130 Lücken behandelt das Unternehmen. Darunter fünf Zero-Days. Eine Sicherheitslücke bleibt aber offen.

- [Link](#)

---

### ***Webbrowser: Firefox und Firefox ESR 115.0.2 schließen Sicherheitslücke***

Die Mozilla-Entwickler haben Firefox und Firefox ESR in Version 115.0.2 veröffentlicht. Darin dichten sie ein Sicherheitsleck ab und korrigieren einige Fehler.

- [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	0.987710000	<a href="#">Link</a>
CVE-2023-33246	0.955810000	0.991030000	<a href="#">Link</a>
CVE-2023-27372	0.970730000	0.996410000	<a href="#">Link</a>
CVE-2023-27350	0.971180000	0.996660000	<a href="#">Link</a>
CVE-2023-25717	0.955670000	0.990990000	<a href="#">Link</a>
CVE-2023-21839	0.950530000	0.989680000	<a href="#">Link</a>
CVE-2023-0669	0.963970000	0.993340000	<a href="#">Link</a>

## BSI - Warn- und Informationsdienst (WID)

Fri, 14 Jul 2023

**vm2: Schwachstelle ermöglicht Codeausführung** [hoch]

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

- [Link](#)

Fri, 14 Jul 2023

**Linux Kernel: Schwachstelle ermöglicht Privilegieneskalation** [hoch]

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

Fri, 14 Jul 2023

**Linux Kernel: Schwachstelle ermöglicht Privilegieneskalation** [hoch]

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

Fri, 14 Jul 2023

**Linux Kernel: Mehrere Schwachstellen** [hoch]

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen und vertrauliche Informationen offenzulegen.

- [Link](#)

Fri, 14 Jul 2023

**Linux Kernel: Schwachstelle ermöglicht Privilegieneskalation** [hoch]

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

---

Fri, 14 Jul 2023

***Linux Kernel: Schwachstelle ermöglicht Privilegieneskalation*** [hoch]

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

---

Fri, 14 Jul 2023

***Linux Kernel: Schwachstelle ermöglicht Privilegieneskalation*** [hoch]

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

---

Fri, 14 Jul 2023

***Microsoft Developer Tools: Mehrere Schwachstellen*** [hoch]

Ein entfernter, authentisierter oder anonym Angreifer kann mehrere Schwachstellen in Microsoft Visual Studio 2022, Microsoft Visual Studio Code und Microsoft .NET Framework ausnutzen, um seine Privilegien zu erweitern, beliebigen Programmcode auszuführen, Sicherheitsvorkehrungen zu umgehen oder Dateien zu manipulieren.

- [Link](#)

---

Fri, 14 Jul 2023

***IEEE 802.11 (WLAN): Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen*** [hoch]

Ein entfernter, anonym oder authentisierter Angreifer kann mehrere Schwachstellen in der IEEE 802.11 Spezifikation und zahlreichen Implementierungen ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

---

Fri, 14 Jul 2023

***Android Patchday Juli 2023*** [hoch]

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Google Android ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen, seine Privilegien zu erweitern, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

---

Thu, 13 Jul 2023

***Zabbix: Mehrere Schwachstellen*** [hoch]

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Zabbix ausnutzen, um einen Denial of Service Angriff durchzuführen und um Informationen offenzulegen.

- [Link](#)

---

Thu, 13 Jul 2023

***Jenkins Plugins: Mehrere Schwachstellen*** [hoch]

Ein entfernter, anonym oder authentisierter Angreifer kann mehrere Schwachstellen in Jenkins Plugins ausnutzen, um Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen und Daten zu manipulieren.

- [Link](#)

---

Thu, 13 Jul 2023

***OpenBSD: Mehrere Schwachstellen*** [hoch]

Ein Angreifer kann mehrere Schwachstellen in OpenBSD ausnutzen, um einen Denial of Service Angriff durchzuführen, Sicherheitsmaßnahmen zu umgehen und nicht näher spezifizierte Auswirkungen zu verursachen.

- [Link](#)

---

Thu, 13 Jul 2023

***Apple Produkte: Schwachstelle ermöglicht Codeausführung*** [hoch]

Ein entfernter, anonym Angreifer kann eine Schwachstelle in Apple Safari, Apple iOS, Apple iPadOS und Apple macOS ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

---

Thu, 13 Jul 2023

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

Ein entfernter, anonymen Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um einen Denial of Service Angriff durchzuführen oder beliebigen Programmcode auszuführen.

- [Link](#)

Thu, 13 Jul 2023

### ***Juniper Patchday Juli 2023*** [hoch]

Ein Angreifer aus dem angrenzenden Netzwerk oder ein entfernter anonymen oder lokaler Angreifer kann mehrere Schwachstellen in verschiedenen Juniper Produkten ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand auszulösen und seine Privilegien zu erweitern.

- [Link](#)

Thu, 13 Jul 2023

### ***SonicWall GMS und SonicWall Analytics: Mehrere Schwachstellen*** [hoch]

Ein entfernter, anonymen oder authentisierter Angreifer kann mehrere Schwachstellen in SonicWall GMS und SonicWall Analytics ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, seine Privilegien zu erweitern und Daten zu manipulieren.

- [Link](#)

Thu, 13 Jul 2023

### ***Extreme Networks IQ Engine: Schwachstelle ermöglicht Codeausführung*** [hoch]

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in Extreme Networks IQ Engine ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

Thu, 13 Jul 2023

### ***Cisco SD-WAN vManage: Schwachstelle ermöglicht Manipulation und Offenlegung von Informationen*** [hoch]

Ein entfernter, anonymen Angreifer kann eine Schwachstelle in Cisco SD-WAN vManage ausnutzen, um Informationen offenzulegen oder zu manipulieren.

- [Link](#)

Thu, 13 Jul 2023

### ***Linux Kernel: Schwachstelle ermöglicht Privilegieneskalation*** [hoch]

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erweitern oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

---

## Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
7/15/2023	[openSUSE 15 Security Update : python-Django (SUSE-SU-2023:2839-1)]	critical
7/14/2023	[Amazon Linux 2 : ecs-service-connect-agent (ALASECS-2023-003)]	critical
7/14/2023	[Debian DLA-3496-1 : lemonldap-ng - LTS security update]	critical
7/13/2023	[SUSE SLES12 Security Update : sysstat (SUSE-SU-2020:0026-2)]	critical
7/15/2023	[Debian DSA-5452-1 : gpac - security update]	high
7/15/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : ghostscript (SUSE-SU-2023:2829-1)]	high
7/15/2023	[SUSE SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2023:2830-1)]	high
7/15/2023	[SUSE SLED12 / SLES12 Security Update : kernel (SUSE-SU-2023:2822-1)]	high

Datum	Schwachstelle	Bewertung
7/15/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : bind (SUSE-SU-2023:2836-1)]	high
7/15/2023	[openSUSE 15 Security Update : poppler (SUSE-SU-2023:2838-1)]	high
7/15/2023	[SUSE SLES15 / openSUSE 15 Security Update : mariadb (SUSE-SU-2023:2835-1)]	high
7/15/2023	[SUSE SLES15 Security Update : kernel (SUSE-SU-2023:2834-1)]	high
7/15/2023	[SUSE SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2023:2831-1)]	high
7/14/2023	[Amazon Linux 2 : containerd (ALASECS-2023-002)]	high
7/14/2023	[Amazon Linux 2 : runc (ALASECS-2023-004)]	high
7/14/2023	[Fedora 37 : cups (2023-9dbd5b28d4)]	high
7/14/2023	[Dell Display Manager 2.1.1.17 Privilege Escalation]	high
7/14/2023	[FreeBSD : electron22 – multiple vulnerabilities (3446e45d-a51b-486f-9b0e-e4402d91fed6)]	high
7/14/2023	[AlmaLinux 8 : .NET 7.0 (ALSA-2023:4058)]	high
7/14/2023	[AlmaLinux 8 : .NET 6.0 (ALSA-2023:4059)]	high
7/14/2023	[AlmaLinux 9 : .NET 7.0 (ALSA-2023:4057)]	high
7/14/2023	[Security Update for .NET Core SDK (July 2023)]	high
7/14/2023	[Security Updates for Microsoft Office Products (May 2023) (macOS)]	high
7/14/2023	[Amazon Linux 2 : ecs-init, docker, containerd, runc (ALASECS-2022-001)]	high
7/14/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2023:2820-1)]	high
7/14/2023	[SUSE SLES12 Security Update : libqt5-qtbase (SUSE-SU-2023:2816-1)]	high
7/14/2023	[AlmaLinux 9 : firefox (ALSA-2023:4071)]	high
7/14/2023	[AlmaLinux 8 : thunderbird (ALSA-2023:4063)]	high
7/14/2023	[AlmaLinux 8 : firefox (ALSA-2023:4076)]	high
7/14/2023	[AlmaLinux 9 : thunderbird (ALSA-2023:4064)]	high
7/13/2023	[RHEL 8 : firefox (RHSA-2023:4069)]	high
7/13/2023	[RHEL 9 : thunderbird (RHSA-2023:4066)]	high
7/13/2023	[Office and Windows HTML Remote Code Execution Vulnerability (CVE-2023-36884) Mitigation]	high
7/13/2023	[SUSE SLES15 Security Update : netcdf (SUSE-SU-2021:3805-1)]	high
7/13/2023	[SUSE SLES15 Security Update : kernel (SUSE-SU-2021:3807-1)]	high
7/13/2023	[SUSE SLES15 Security Update : netcdf (SUSE-SU-2021:3804-1)]	high
7/13/2023	[SUSE SLES15 Security Update : kernel (SUSE-SU-2021:3806-1)]	high
7/13/2023	[Ubuntu 16.04 ESM : PostgreSQL vulnerability (USN-6230-1)]	high
7/13/2023	[AlmaLinux 9 : .NET 6.0 (ALSA-2023:4060)]	high

## Cyberangriffe: (Jul)

Datum	Opfer	Land	Information
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>
2023-07-02	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
2023-07-14	[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>
2023-07-12	[Ministry of Energy and Mines (Cuba) " STORMOUS + GhostSec "]	stormous	<a href="#">Link</a>
2023-07-12	[GRIPA.ORG]	clp	<a href="#">Link</a>
2023-07-12	[SLB.COM]	clp	<a href="#">Link</a>
2023-07-12	[AMCTHEATRES.COM]	clp	<a href="#">Link</a>
2023-07-12	[AINT.COM]	clp	<a href="#">Link</a>
2023-07-12	[JACKENTERTAINMENT.COM]	clp	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
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	[CLEARRESULT.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>
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	[mamboafricaadventure]	stormous	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
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	[RADISSONHOTELSAMERICAS.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>
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)]	rancouz	<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>

Datum	Opfer	Ransomware-Gruppe	Webseite
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	[LSOLUTIONS.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>
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>

Datum	Opfer	Ransomware-Gruppe	Webseite
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.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/>

# 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.