



Ausgabe: 20230713

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

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](#)

Patchday: SAP warnt vor 16 Sicherheitslücken in der Business-Software

Am Juli-Patchday hat SAP 16 Sicherheitsmeldungen zur Geschäfts-Software aus dem Unternehmen veröffentlicht. Updates dichten auch eine kritische Lücke ab.

- [Link](#)

Exploit für Root-Lücke in VMware Aria Operations for Logs aufgetaucht

Teils kritische Sicherheitslücken in VMware Aria Operations for Logs stopfen Updates aus dem April. Jetzt ist Exploit-Code aufgetaucht, der eine Lücke angreift.

- [Link](#)

Zero-Day für Safari geschlossen – Update: Zurückgezogen

Apple hat Montagabend eine schnelle Aktualisierung für seinen Browser ausgespielt. Betroffen von der offenbar bereits ausgenutzten Lücke: Macs und Mobilgeräte.

- [Link](#)

Minecraft: Virtuelle Computer reißen Sicherheitslücken auf

In zwei Minecraft-Mods, die tatsächlich programmierbare Computer oder Roboter für das Spiel bereitstellen, klaffen kritische Sicherheitslücken.

- [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	0.987680000	Link
CVE-2023-33246	0.954530000	0.990580000	Link
CVE-2023-27372	0.970730000	0.996400000	Link
CVE-2023-27350	0.971180000	0.996640000	Link
CVE-2023-25717	0.955670000	0.990980000	Link
CVE-2023-21839	0.950530000	0.989650000	Link
CVE-2023-0669	0.963970000	0.993310000	Link

BSI - Warn- und Informationsdienst (WID)

Wed, 12 Jul 2023

Microsoft Windows: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode mit Administratorrechten [hoch]

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in verschiedenen Versionen von Microsoft Windows und Microsoft Windows Server ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen.

- [Link](#)

Wed, 12 Jul 2023

Microsoft Office: Mehrere Schwachstellen [hoch]

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in verschiedenen Microsoft Office Produkten ausnutzen, um seine Privilegien zu erweitern, beliebigen Programmcode auszuführen, Informationen offenzulegen, Sicherheitsvorkehrungen zu umgehen oder Dateien zu manipulieren.

- [Link](#)

Wed, 12 Jul 2023

Microsoft Windows: Mehrere Schwachstellen [kritisch]

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in verschiedenen Versionen von Microsoft Windows und Microsoft Windows Server ausnutzen, um seine Privilegien zu erweitern, beliebigen Programmcode auszuführen, Informationen offenzulegen, Dateien zu manipulieren, Sicherheitsvorkehrungen zu umgehen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

Wed, 12 Jul 2023

Apache HttpComponents: Schwachstelle ermöglicht Täuschung des Nutzers [hoch]

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Apache HttpComponents ausnutzen, um den Nutzer zu täuschen.

- [Link](#)

Wed, 12 Jul 2023

Apple Produkte: Schwachstelle ermöglicht Codeausführung [hoch]

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

- [Link](#)

Wed, 12 Jul 2023

Grafana: Schwachstelle ermöglicht Übernahme von Benutzerkonto [hoch]

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Grafana ausnutzen, um ein Benutzerkonto zu übernehmen.

- [Link](#)

Wed, 12 Jul 2023

Autodesk AutoCAD: Mehrere Schwachstellen [hoch]

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

- [Link](#)

Wed, 12 Jul 2023

Citrix Systems Secure Access client: Mehrere Schwachstellen ermöglichen Privilegieneskalation [hoch]

Ein lokaler Angreifer kann mehrere Schwachstellen in Citrix Systems Secure Access client ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

Wed, 12 Jul 2023

Red Hat OpenShift Container Platform: Schwachstelle ermöglicht Privilegieneskalation [hoch]

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

- [Link](#)

Wed, 12 Jul 2023

Linux Kernel: Schwachstelle ermöglicht Erlangen von Administratorrechten [hoch]

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um Administratorrechte zu erlangen.

- [Link](#)

Wed, 12 Jul 2023

Linux Kernel: Mehrere Schwachstellen [hoch]

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand zu verursachen und seine Privilegien zu erweitern.

- [Link](#)

Wed, 12 Jul 2023

Nvidia Treiber: Mehrere Schwachstellen [hoch]

Ein lokaler Angreifer kann mehrere Schwachstellen im Nvidia Treiber ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand auszulösen, seine Privilegien zu erweitern und Daten zu manipulieren.

- [Link](#)

Wed, 12 Jul 2023

Linux Kernel: Mehrere Schwachstellen [hoch]

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um einen Denial of Service Angriff und einen nicht spezifizierten Angriff durchzuführen.

- [Link](#)

Wed, 12 Jul 2023

Linux Kernel: Schwachstelle ermöglicht Privilegieneskalation [hoch]

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

- [Link](#)

Wed, 12 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](#)

Wed, 12 Jul 2023

Linux Kernel: Schwachstelle ermöglicht Ausführen von beliebigem Programmcode mit Administratorrechten [hoch]

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen.

- [Link](#)

Wed, 12 Jul 2023

Intel i915 Graphics Driver für Linux: Schwachstelle ermöglicht Privilegieneskalation [hoch]

Ein lokaler Angreifer kann eine Schwachstelle im Intel i915 Graphics Driver für Linux ausnutzen, um seine Privilegien zu erhöhen.

- [Link](#)

Wed, 12 Jul 2023

Linux Kernel (vmwgfx): Mehrere Schwachstellen [hoch]

Ein lokaler Angreifer kann mehrere Schwachstellen in Linux Kernel ausnutzen, um Informationen offenzulegen und um seine Privilegien zu erweitern.

- [Link](#)

Wed, 12 Jul 2023

Citrix Systems ShareFile StorageZones Controller: Schwachstelle ermöglicht Übernahme der Kontrolle [kritisch]

Ein entfernter, anonym Angreifer kann eine Schwachstelle in Citrix Systems ShareFile StorageZones Controller ausnutzen, um den Controller zu kompromittieren.

- [Link](#)

Wed, 12 Jul 2023

Nvidia Treiber: Mehrere Schwachstellen [hoch]

Ein Angreifer kann mehrere Schwachstellen in Nvidia Treibern ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand zu verursachen, seine Privilegien zu erweitern und Daten zu manipulieren.

- [Link](#)

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
7/12/2023	[SUSE SLES12 Security Update : kernel (SUSE-SU-2023:2805-1)]	critical
7/12/2023	[RHEL 9 : grafana (RHSA-2023:4030)]	critical
7/12/2023	[Cisco SD-WAN vManage Unauthenticated REST API Access (cisco-sa-vmanage-unauthapi-sphCLYPA)]	critical
7/12/2023	[AlmaLinux 9 : grafana (ALSA-2023:4030)]	critical
7/12/2023	[Security Updates for Microsoft Office Products C2R (July 2023)]	critical
7/12/2023	[Ubuntu 20.04 LTS / 22.04 LTS / 22.10 / 23.04 : Thunderbird vulnerabilities (USN-6214-1)]	critical

Datum	Schwachstelle	Bewertung
7/11/2023	[Debian DLA-3491-1 : erlang - LTS security update]	critical
7/12/2023	[Debian DLA-3493-1 : symfony - LTS security update]	high
7/12/2023	[openSUSE 15 Security Update : python-Django (openSUSE-SU-2023:0174-1)]	high
7/12/2023	[Fedora 37 : kernel (2023-2932e6c7d8)]	high
7/12/2023	[Fedora 38 : cutter-re / rizin (2023-3dc1f9ba12)]	high
7/12/2023	[Fedora 37 : yt-dlp (2023-79e2b35ba6)]	high
7/12/2023	[SUSE SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2023:2809-1)]	high
7/12/2023	[SUSE SLES12 Security Update : kernel (SUSE-SU-2023:2808-1)]	high
7/12/2023	[Security Updates for Microsoft Office Products (July 2023) (macOS)]	high
7/12/2023	[Security Updates for Microsoft Dynamics 365 (on-premises) (July 2023)]	high
7/12/2023	[Juniper Junos OS Vulnerability (JSA71642)]	high
7/12/2023	[Adobe InDesign < 17.4.2 / 18.0 < 18.4 Multiple Vulnerabilities (APSB23-38) (macOS)]	high
7/12/2023	[Adobe InDesign < 17.4.2 / 18.0 < 18.4 Multiple Vulnerabilities (APSB23-38)]	high
7/12/2023	[Juniper Junos OS Multiple Vulnerabilities (JSA71655)]	high
7/12/2023	[Security Update for Microsoft .NET Core (July 2023)]	high
7/12/2023	[CentOS 8 : nodejs:18 (CESA-2023:4035)]	high
7/12/2023	[Wireshark 3.6.x < 3.6.15 A Vulnerability]	high
7/12/2023	[Wireshark 3.6.x < 3.6.15 A Vulnerability (macOS)]	high
7/12/2023	[Wireshark 4.0.x < 4.0.7 Multiple Vulnerabilities]	high
7/12/2023	[Wireshark 4.0.x < 4.0.7 Multiple Vulnerabilities (macOS)]	high
7/12/2023	[Security Updates for Outlook C2R Multiple Vulnerabilities (July 2023)]	high
7/12/2023	[Security Updates for Microsoft Excel Products C2R (July 2023)]	high
7/12/2023	[Security Updates for Microsoft ASP.NET Core (July 2023)]	high
7/12/2023	[Ubuntu 22.04 LTS / 22.10 / 23.04 : .NET vulnerability (USN-6217-1)]	high
7/12/2023	[Ubuntu 20.04 LTS : lib3mf vulnerability (USN-6216-1)]	high
7/12/2023	[Ubuntu 18.04 ESM / 20.04 LTS : dwarves vulnerabilities (USN-6215-1)]	high
7/12/2023	[AlmaLinux 8 : nodejs:18 (ALSA-2023:4035)]	high
7/12/2023	[Nutanix AOS : Multiple Vulnerabilities (NXSA-AOS-6.6.2.7)]	high
7/12/2023	[Nutanix AOS : Multiple Vulnerabilities (NXSA-AOS-6.6.2.6)]	high
7/12/2023	[Rockwell Automation ControlLogix Communications Modules Denial of Service (CVE-2023-3596)]	high
7/11/2023	[Debian DLA-3492-1 : yajl - LTS security update]	high
7/11/2023	[Wago (CVE-2023-1150)]	high

Cyberangriffe: (Jul)

Datum	Opfer	Land	Information
2023-07-12	Comune di Ferrara	[ITA]	Link
2023-07-11	ZooTampa	[USA]	Link
2023-07-09	Ville de Hayward	[USA]	Link
2023-07-08	Ventia	[AUS]	Link
2023-07-08	Comté de Kent	[USA]	Link
2023-07-07	Université de l'Ouest de l'Écosse (UWS)	[GBR]	Link
2023-07-07	Bureau du Procureur Général et le Ministère des Affaires Juridiques de Trinité-et-Tobago (AGLA)	[TTO]	Link
2023-07-07	Jackson Township	[USA]	Link
2023-07-07	Maison Mercier	[FRA]	Link
2023-07-07	Diputación Provincial de Zaragoza	[ESP]	Link
2023-07-06	Commission électorale du Pakistan (ECP)	[PAK]	Link
2023-07-05	Hôpital universitaire Luigi Vanvitelli de Naples	[ITA]	Link
2023-07-04	Nagoya Port Transport Association	[JPN]	Link
2023-07-04	Roys of Wroxham	[GBR]	Link
2023-07-04	ibis acam	[AUT]	Link
2023-07-02	Aéroport de Montpellier	[FRA]	Link
2023-07-02	Ville d'Agen	[FRA]	Link

Ransomware-Erpressungen: (Jul)

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-07-13	[Telepizza]	8base	Link
2023-07-13	[The Traffic Tech]	8base	Link
2023-07-13	[Quikcard Solutions Inc.]	8base	Link
2023-07-13	[Jadranka Group]	8base	Link
2023-07-13	[Dental One Craigieburn]	8base	Link
2023-07-13	[ANL Packaging]	8base	Link
2023-07-13	[BTU]	8base	Link
2023-07-12	[Ministerio de Cultura de la Republica de Cuba " STORMOUS + GhostSec "]	stormous	Link
2023-07-12	[Ministry of Foreign Trade " STORMOUS + GhostSec "]	stormous	Link
2023-07-12	[Ministry of Energy and Mines (Cuba) " STORMOUS + GhostSec "]	stormous	Link
2023-07-12	[GRIPA.ORG]	clop	Link
2023-07-12	[SLB.COM]	clop	Link
2023-07-12	[AMCTHEATRES.COM]	clop	Link
2023-07-12	[AINT.COM]	clop	Link
2023-07-12	[JACKENTERTAINMENT.COM]	clop	Link
2023-07-12	[NASCO.COM]	clop	Link
2023-07-12	[TGIDIRECT.COM]	clop	Link
2023-07-12	[HONEYWELL.COM]	clop	Link
2023-07-12	[CLEARERESULT.COM]	clop	Link
2023-07-12	[RADIUSGS.COM]	clop	Link
2023-07-09	[Bitimen exchange]	arvinclub	Link
2023-07-12	[affinityhealthservices.ne]	lockbit3	Link
2023-07-12	[ATS Infrastructure]	bianlian	Link
2023-07-12	[Henock Construction]	bianlian	Link
2023-07-12	[Lyon & Healy]	bianlian	Link
2023-07-12	[Mission Parks]	bianlian	Link
2023-07-07	[Innodis Group]	noescape	Link
2023-07-12	[Divgi-TTS was hacked. Due to the extreme low level of security, a huge amount of confident]	alphv	Link
2023-07-12	[Eastin Hotel Makkasan Bangkok was hacked. Customers' financial and personal information ha]	alphv	Link
2023-07-12	[SMS-SME was hacked. A huge amount of confidential information was stolen, information of c]	alphv	Link
2023-07-12	[Algeiba.com has a critical level of security on its network. Customer and partner data is]	alphv	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-07-12	[Amber Court 2020 was hacking. A lot of customers' personal information was stolen.]	alphv	Link
2023-07-12	[Maruchan Inc]	alphv	Link
2023-07-12	[Schmidt Salzman & Moran, Ltd]	akira	Link
2023-07-12	[Wright Moore DeHart Dupuis & Hutchinson]	alphv	Link
2023-07-12	[Better System Co.,Ltd]	qilin	Link
2023-07-08	[Protactics]	noescape	Link
2023-07-11	[CONSOLEENERGY.COM]	clon	Link
2023-07-11	[KALEAERO.COM]	clon	Link
2023-07-11	[AGILYSYS.COM]	clon	Link
2023-07-11	[SCCU.COM]	clon	Link
2023-07-11	[ARVATO.COM]	clon	Link
2023-07-11	[RITEAID.COM]	clon	Link
2023-07-11	[PIONEERELECTRONICS16.COM]	clon	Link
2023-07-11	[BAM.COM.GT]	clon	Link
2023-07-11	[TOMTOM.COM]	clon	Link
2023-07-11	[EMERSON.COM]	clon	Link
2023-07-11	[berjaya]	stormous	Link
2023-07-11	[Ingersoll Rand]	stormous	Link
2023-07-11	[Arrowall]	stormous	Link
2023-07-11	[OKS]	stormous	Link
2023-07-11	[Matrix]	stormous	Link
2023-07-11	[treenovum.es]	stormous	Link
2023-07-11	[archiplusinter.com]	stormous	Link
2023-07-11	[marehotels]	stormous	Link
2023-07-11	[mamboafrikaadventure]	stormous	Link
2023-07-11	[Nipun Consultancy]	stormous	Link
2023-07-11	[Murfreesboro Medical Clinic]	bianlian	Link
2023-07-11	[A123 Systems]	akira	Link
2023-07-11	[MicroPort Scientific / LivaNova]	qilin	Link
2023-07-11	[panoramaeyecare.com]	lockbit3	Link
2023-07-11	[Pesquera Diamante S.A.]	8base	Link
2023-07-11	[Weitkamp · Hirsch and Kollegen Steuerberatungsgesellschaft mbH]	8base	Link
2023-07-11	[gis4.addison-il]	cuba	Link
2023-07-08	[Weitkamp · Hirsch & Kollegen Steuerberatungsgesellschaft mbH]	8base	Link
2023-07-08	[Kansas medical center LLC]	8base	Link
2023-07-08	[Danbury Public Schools]	8base	Link
2023-07-08	[Advanced Fiberglass Industries]	8base	Link
2023-07-08	[Citelis Mobility]	8base	Link
2023-07-08	[Motor Components, LLC]	8base	Link
2023-07-10	[RICOHACUMEN.COM]	clon	Link
2023-07-10	[SMA.DE]	clon	Link
2023-07-10	[VRM.DE]	clon	Link
2023-07-10	[UMASSMED.EDU]	clon	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-07-10	[VISIONWARE.CA]	clop	Link
2023-07-10	[JHU.EDU]	clop	Link
2023-07-10	[FMFCU.ORG]	clop	Link
2023-07-10	[JPRMP.COM]	clop	Link
2023-07-10	[WESTAT.COM]	clop	Link
2023-07-10	[RADISSONHOTELSAMERICA.COM]	clop	Link
2023-07-10	[Hamre Schumann Mueller & Larson HSML]	akira	Link
2023-07-10	[Belize Electricity Limited - Leaked]	ragnarlocker	Link
2023-07-10	[Green Diamond]	akira	Link
2023-07-10	[Citta Nuova]	rhysida	Link
2023-07-09	[leeindustries.com]	lockbit3	Link
2023-07-09	[Garuda Indonesia]	mallox	Link
2023-07-09	[roys.co.uk]	lockbit3	Link
2023-07-09	[Evergreen Seamless Pipes & Tubes]	bianlian	Link
2023-07-03	[Peroni Pompe]	donutleaks	Link
2023-07-08	[Cabra Consulting Ltd]	8base	Link
2023-07-07	[Tracker de Colombia SAS]	medusa	Link
2023-07-07	[Lane Valente Industries]	play	Link
2023-07-07	[New Century Advisors, LLC]	8base	Link
2023-07-07	[ROBERT L BAYLESS PRODUCER LLC]	8base	Link
2023-07-07	[Industrial Heat Transfer (iht-inc.com)]	rancoz	Link
2023-07-07	[CROWE.COM]	clop	Link
2023-07-07	[AUTOZONE.COM]	clop	Link
2023-07-07	[BCDTRAVEL.COM]	clop	Link
2023-07-07	[AMERICANNATIONAL.COM]	clop	Link
2023-07-07	[USG.EDU]	clop	Link
2023-07-07	[CYTOMX.COM]	clop	Link
2023-07-07	[MARYKAY.COM]	clop	Link
2023-07-07	[FISCDP.COM]	clop	Link
2023-07-07	[KERNAGENCY.COM]	clop	Link
2023-07-07	[UOFLHEALTH.ORG]	clop	Link
2023-07-07	[LSOLUTIONS.CO.UK]	clop	Link
2023-07-07	[TDAMERITRADE.COM]	clop	Link
2023-07-07	[Kenya Bureau Of Standards]	rhysida	Link
2023-07-07	[Lazer Tow]	play	Link
2023-07-07	[Star Island Resort]	play	Link
2023-07-07	[Indiana Dimension]	play	Link
2023-07-07	[Lawer SpA]	play	Link
2023-07-06	[DELARUE.COM]	clop	Link
2023-07-06	[ENERGYTRANSFER.COM]	clop	Link
2023-07-06	[PAYCOR.COM]	clop	Link
2023-07-06	[NETSCOUT.COM]	clop	Link
2023-07-06	[WOLTERSKLUWER.COM]	clop	Link
2023-07-06	[CADENCEBANK.COM]	clop	Link
2023-07-06	[BANKWITHUNITED.COM]	clop	Link
2023-07-06	[NEWERATECH.COM]	clop	Link
2023-07-06	[NST Attorneys at Law]	play	Link
2023-07-06	[Uniquify]	play	Link
2023-07-06	[Geneva Software]	play	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-07-06	[MUJI Europe Holdings Limited]	play	Link
2023-07-06	[Betty Lou's]	play	Link
2023-07-06	[Capacity LLC]	play	Link
2023-07-06	[Safety Network]	play	Link
2023-07-06	[Carvin Software]	bianlian	Link
2023-07-06	[Ella Insurance Brokerage]	bianlian	Link
2023-07-06	[betalandservices.com]	lockbit3	Link
2023-07-06	[chasc.org]	lockbit3	Link
2023-07-06	[cls-group.com]	lockbit3	Link
2023-07-06	[gacegypt.net]	lockbit3	Link
2023-07-06	[siegfried.com.mx]	lockbit3	Link
2023-07-06	[Pinnergy]	akira	Link
2023-07-06	[Bangladesh Krishi Bank]	alphv	Link
2023-07-06	[ASIC Soluciones]	qilin	Link
2023-07-06	[KIRWIN FRYDAY MEDCALF Lawyers LLP]	8base	Link
2023-07-05	[TRANSPERFECT.COM]	clon	Link
2023-07-05	[QUORUMFCU.ORG]	clon	Link
2023-07-05	[MERATIVE.COM]	clon	Link
2023-07-05	[NORGREN.COM]	clon	Link
2023-07-05	[CIENA.COM]	clon	Link
2023-07-05	[KYBURZDRUCK.CH]	clon	Link
2023-07-05	[UNITEDREGIONAL.ORG]	clon	Link
2023-07-05	[TDECU.ORG]	clon	Link
2023-07-05	[BRADYID.COM]	clon	Link
2023-07-05	[BARRICK.COM]	clon	Link
2023-07-05	[DURR.COM]	clon	Link
2023-07-05	[ZooTampa at Lowry Park]	blacksuit	Link
2023-07-05	[Avalign Technologies]	blackbyte	Link
2023-07-05	[Portugal Scotturb Data Leaked]	ragnarlocker	Link
2023-07-03	[guestgroup.com.au]	lockbit3	Link
2023-07-05	[Murphy]	akira	Link
2023-07-05	[eurosupport.com]	lockbit3	Link
2023-07-05	[recamlaser.com]	lockbit3	Link
2023-07-05	[mitr.com]	lockbit3	Link
2023-07-04	[Hoosier Equipment company]	medusalocker	Link
2023-07-04	[Yunus Emre Institute Turkey]	medusa	Link
2023-07-04	[Polanglo]	8base	Link
2023-07-03	[Jefferson County Health Center]	karakurt	Link
2023-07-03	[snjb.net]	lockbit3	Link
2023-07-03	[oneexchange.com]	lockbit3	Link
2023-07-03	[Townsquare Media Inc]	alphv	Link
2023-07-03	[Ayuntamiento de Arganda City Council]	rhysida	Link
2023-07-03	[Duncan Disability Law]	alphv	Link
2023-07-03	[Hollywood Forever]	rhysida	Link
2023-07-03	[Mutuelle LMP]	medusa	Link
2023-07-03	[Luna Hotels & Resorts]	medusa	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2023-07-03	[BM GROUP POLYTEC S.p.A.]	rhysida	Link
2023-07-03	[Brett Martin]	blackbyte	Link
2023-07-02	[blowtherm.it]	lockbit3	Link
2023-07-02	[Ucamco Belgium]	medusalocker	Link
2023-07-01	[Ashley HomeStore]	mallox	Link
2023-07-01	[Blount Fine Foods]	blackbasta	Link
2023-07-01	[Blount]	blackbasta	Link
2023-07-01	[DVA - DVision Architecture]	ransomexx	Link
2023-07-01	[Kondratoff Persick LLP]	bianlian	Link
2023-07-01	[Undisclosed Staffing Company]	bianlian	Link

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

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