Cybersecurity Morgenreport

Ausgabe: 20230712

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

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

—

Codeschmuggel möglich: Hochriskante Sicherheitslücken in ArubaOS-Firmware
Die HPE-Tochter Aruba hat Aktualisierungen für die ArubaOS-Firmware veröffentlicht. Sie schließen hochriskante Sicherheitslücken, die Codeschmuggel erlauben.
- Link

—

ARM-Grafikeinheit: Warnung vor Angriffen auf Sicherheitslücke in Treibern
Cyberkriminelle missbrauchen eine Sicherheitslücke in Treibern für ARMs Mali-Grafikeinheiten, um ihre Rechte auszuweiten oder Informationen abzugreifen.
- Link

—

Linux: Sicherheitslücke erlaubt Rechteausweitung, Exploit angekündigt
Im Linux-Kernel schlummert eine Sicherheitslücke, durch die Nutzer ihre Rechte im System ausweiten können. Der Entdecker kündigt Exploit-Code für Ende Juli an.
- Link

—

Fediverse: Kritische Sicherheitslücken in Mastodon-Software abgedichtet
Betreiber von Mastodon-Instanzen müssen die Server aktualisieren. Ältere Versionen bringen kritische Sicherheitslücken mit, die etwa Codeschmuggel erlauben.
- Link

—

Cisco Nexus 9000: Angreifer können Verschlüsselung brechen – kein Update
In den Geräten der Nexus-9000-Baureihe von Cisco können Angreifer verschlüsselten Verkehr lesen und verändern. Es gibt weder Software-Update noch Workaround.
- Link

—

Patchday: Vielfältige Attacken auf Android 11, 12 und 13 möglich
Es gibt wichtige Sicherheitsupdates für verschiedene Android-Versionen. Im schlimmsten Fall könnte Schadcode auf Geräte gelangen.
- 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	0.987670000	Link
CVE-2023-33246	0.954530000	0.990580000	Link
CVE-2023-27372	0.970730000	0.996390000	Link
CVE-2023-27350	0.971180000	0.996630000	Link
CVE-2023-25717	0.955670000	0.990990000	Link
CVE-2023-21839	0.950530000	0.989630000	Link
CVE-2023-0669	0.964550000	0.993510000	Link

BSI - Warn- und Informationsdienst (WID)

Tue, 11 Jul 2023
Linux Kernel: Mehrere Schwachstellen ermöglichen Privilegieneskalation [hoch]
Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.
- Link

—

Tue, 11 Jul 2023
SAP Patchday Juli 2023 [hoch]
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in SAP Software ausnutzen, um beliebigen Code oder Betriebssystembefehle auszuführen, Sicherheitsmechanismen zu umgehen, einen Denial of Service-Zustand auszulösen oder Informationen offenzulegen.
- Link

—

Tue, 11 Jul 2023
Red Hat OpenShift: Mehrere Schwachstellen [hoch]
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat OpenShift ausnutzen, um einen Denial of Service Angriff durchzuführen, einen nicht näher spezifizierten Angriff durchzuführen, vertrauliche Informationen offenzulegen und Daten zu manipulieren.
- Link

—

Tue, 11 Jul 2023
VMware Aria Operations for Logs: Mehrere Schwachstellen ermöglichen Ausführen von beliebigem Programmcode mit Administratorrechten [kritisch]
Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in VMware Aria Operations for Logs ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen.
- Link

—

Tue, 11 Jul 2023

Red Hat OpenShift Container Platform: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen [hoch]

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

- Link

—

Tue, 11 Jul 2023

Red Hat OpenShift: Mehrere Schwachstellen [hoch]

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

—

Tue, 11 Jul 2023

Aruba ArubaOS: Mehrere Schwachstellen [hoch]

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Aruba ArubaOS ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen, Daten zu manipulieren und Sicherheitsvorkehrungen zu umgehen.

- Link

—

Tue, 11 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

—

Mon, 10 Jul 2023

MediaWiki: Mehrere Schwachstellen [hoch]

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in MediaWiki ausnutzen, um Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen, einen Cross-Site-Scripting-Angriff durchzuführen und Angriffe mit unspezifischen Auswirkungen auszuführen.

- Link

—

Mon, 10 Jul 2023

Intel Prozessoren: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen [hoch]

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Intel Prozessoren ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- Link

—

Mon, 10 Jul 2023

Intel Prozessoren: Mehrere Schwachstellen [hoch]

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in Intel Prozessoren ausnutzen, um seine Privilegien zu erhöhen, einen Denial of Service Angriff durchzuführen oder vertrauliche Daten einzusehen.

- Link

—

Mon, 10 Jul 2023

QEMU und libvirt: Mehrere Schwachstellen [hoch]

Ein lokaler Angreifer kann mehrere Schwachstellen in QEMU und libvirt ausnutzen, um Informationen offenzulegen und um Sicherheitsmechanismen zu umgehen.

- Link

—

Mon, 10 Jul 2023

libvirt: Schwachstelle ermöglicht Denial of Service [hoch]

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

- Link

—

Mon, 10 Jul 2023
Python: Schwachstelle ermöglicht Codeausführung [hoch]
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Python ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—
Mon, 10 Jul 2023
libxml2: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff [hoch]
Ein Angreifer kann mehrere Schwachstellen in libxml2 ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.
- Link
—
Mon, 10 Jul 2023
Python: Schwachstelle ermöglicht Denial of Service [hoch]
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Python ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link
—
Mon, 10 Jul 2023
Ruby: Schwachstelle ermöglicht Manipulation von Dateien [hoch]
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Ruby ausnutzen, um Dateien zu manipulieren.
- Link
—
Mon, 10 Jul 2023
TPM 2.0 Referenzimplementierung: Mehrere Schwachstellen [hoch]
Ein lokaler Angreifer kann mehrere Schwachstellen in der TPM 2.0 Referenzimplementierung ausnutzen, um beliebigen Programmcode auszuführen, einen Denial of Service Zustand herbeizuführen und um Informationen aus dem TPM offenzulegen.
- Link
—
Mon, 10 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
—
Mon, 10 Jul 2023
Ubiquiti UniFi: Schwachstelle ermöglicht Cross-Site Scripting [hoch]
Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in der Ubiquiti UniFi Network Application ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen und dadurch seine Privilegien zu erweitern.
- Link
—

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
7/11/2023	[ARM Mali GPU Kernel Driver < r24p0 / < r30p0 Use After Free (CVE-2022-28349)]	critical
7/11/2023	[ARM Mali GPU Kernel Driver < r37p0 Use After Free (CVE-2022-28350)]	critical
7/11/2023	[Fortinet Fortigate - Existing websocket connection persists after deleting API admin (FG-IR-23-028)]	critical
7/11/2023	[Mozilla Firefox < 115.0.2]	critical
7/11/2023	[Mozilla Firefox ESR < 115.0.2]	critical
7/11/2023	[Mozilla Firefox ESR < 115.0.2]	critical
7/11/2023	[Mozilla Firefox < 115.0.2]	critical

Datum	Schwachstelle	Bewertung
7/11/2023	[Fortinet Fortigate - Proxy mode with deep inspection - Stack-based buffer overflow (FG-IR-23-183)]	critical
7/11/2023	[KB5028168: Windows 10 version 1809 / Windows Server 2019 Security Update (July 2023)]	critical
7/11/2023	[KB5028186: Windows 10 LTS 1507 Security Update (July 2023)]	critical
7/11/2023	[KB5028169: Windows 10 Version 1607 and Windows Server 2016 Security Update (July 2023)]	critical
7/11/2023	[KB5028185: Windows 11 version 22H2 Security Update (July 2023)]	critical
7/11/2023	[KB5028171: Windows 2022 / Azure Stack HCI 22H2 Security Update (July 2023)]	critical
7/11/2023	[KB5028223: Windows Server 2012 R2 Security Update (July 2023)]	critical
7/11/2023	[KB5028233: Windows Server 2012 Security Update (July 2023)]	critical
7/11/2023	[KB5028166: Windows 10 Version 20H2 / Windows 10 Version 21H2 / Windows 10 Version 22H2 Security Update (July 2023)]	critical
7/11/2023	[Security Updates for Microsoft SharePoint Server 2016 (July 2023)]	critical
7/11/2023	[Security Updates for Microsoft Word Products (July 2023)]	critical
7/11/2023	[KB5028226: Windows Server 2008 Security Update (July 2023)]	critical
7/11/2023	[KB5028182: Windows 11 version 21H2 Security Update (July 2023)]	critical
7/11/2023	[Security Updates for Microsoft SharePoint Server 2019 (July 2023)]	critical
7/11/2023	[KB5028224: Windows 2007 / Windows Server 2008 R2 Security Update (July 2023)]	critical
7/11/2023	[Security Updates for Microsoft SharePoint Server Subscription Edition (July 2023)]	critical
7/11/2023	[Debian DLA-3491-1 : erlang - LTS security update]	critical
7/11/2023	[ARM Mali GPU Kernel Driver < r38p2 / < r40p0 Use After Free (CVE-2022-38181)]	high
7/11/2023	[ARM Mali GPU Kernel Driver < r32p0 / < r35p0 Improper Memory Access (CVE-2021-44828)]	high
7/11/2023	[ARM Mali GPU Kernel Driver < r30p0 / < r31p0 Use After Free (CVE-2021-29256)]	high
7/11/2023	[ARM Mali GPU Kernel Driver < r29p0 / < r31p0 Use After Free (CVE-2021-28663)]	high
7/11/2023	[ARM Mali GPU Kernel Driver < r42p0 Use After Free (CVE-2022-46394)]	high
7/11/2023	[ARM Mali GPU Kernel Driver < r32p0 / < r36p0 Improper Memory Access (CVE-2022-22706)]	high
7/11/2023	[ARM Mali GPU Kernel Driver < r38p2 / < r40p0 Improper Memory Access (CVE-2022-41757)]	high
7/11/2023	[ARM Mali GPU Kernel Driver < r30p0 / < r31p0 Improper Memory Access (CVE-2021-28664)]	high
7/11/2023	[ARM Mali GPU Kernel Driver < r41p0 Use After Free (CVE-2022-46891)]	high
7/11/2023	[ARM Mali GPU Kernel Driver < r42p0 Use After Free (CVE-2022-46395)]	high
7/11/2023	[Debian DLA-3490-1 : thunderbird - LTS security update]	high
7/11/2023	[Security Updates for Microsoft Visual Studio Products (July 2023)]	high
7/11/2023	[Security Update for Microsoft Visual Studio Code GitHub Pull Requests and Isssues Extension (July 2023)]	high
7/11/2023	[Security Updates for Outlook (July 2023)]	high
7/11/2023	[Security Updates for Microsoft Office Products (July 2023)]	high

Datum	Schwachstelle	Bewertung
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
2023-07-11	ZooTampa	[USA]	Link
2023-07-09	Ville de Hayward	[USA]	Link
2023-07-08	Ventia	[AUS]	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-Grupppe	Webseite
2023-07-11	[CONSOLENERGY.COM]	clop	Link
2023-07-11	[KALEAERO.COM]	clop	Link
2023-07-11	[AGILYSYS.COM]	clop	Link
2023-07-11	[SCCU.COM]	clop	Link
2023-07-11	[ARVATO.COM]	clop	Link
2023-07-11	[RITEAID.COM]	clop	Link
2023-07-11	[PIONEERELECTRONICS.COM]	clop	Link
2023-07-11	[BAM.COM.GT]	clop	Link
2023-07-11	[TOMTOM.COM]	clop	Link
2023-07-11	[EMERSON.COM]	clop	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	[mamboafricaadventure]	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 Steuerber-atungsgesellschaft mbH]	8base	Link
2023-07-11	[gis4.addison-il]	cuba	Link
2023-07-08	[Weitkamp · Hirsch & Kollegen Steuerber-atungsgesellschaft 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]	clop	Link
2023-07-10	[SMA.DE]	clop	Link
2023-07-10	[VRM.DE]	clop	Link
2023-07-10	[UMASSMED.EDU]	clop	Link
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	[RADISSONHOTELSAMERICAS.COM]	clop	Link
2023-07-10	[Hamre Schumann Mueller & Larson HSML]	akira	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
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	[L8SOLUTIONS.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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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]	clop	Link
2023-07-05	[QUORUMFCU.ORG]	clop	Link
2023-07-05	[MERATIVE.COM]	clop	Link
2023-07-05	[NORGREN.COM]	clop	Link
2023-07-05	[CIENA.COM]	clop	Link
2023-07-05	[KYBURZDRUCK.CH]	clop	Link
2023-07-05	[UNITEDREGIONAL.ORG]	clop	Link
2023-07-05	[TDECU.ORG]	clop	Link
2023-07-05	[BRADYID.COM]	clop	Link
2023-07-05	[BARRICK.COM]	clop	Link
2023-07-05	[DURR.COM]	clop	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	[oneexchangecorp.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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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.