Cybersecurity Morgenreport

Ausgabe: 20230815

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

Schadcode-Attacken via WLAN auf einige Automodelle von Ford möglich
Eine Schwachstelle im Infotainmentsystem gefährdet bestimmte Modellserien von Ford und Lincoln. Die Fahrsicherheit soll davon aber nicht beeinträchtigt sein.
- Link

—

Schwerwiegende Sicherheitslücken bedrohen hierzulande kritische Infrastrukturen
Aufgrund von mehreren Schwachstellen in einem SDK, das im Industriebereich zum Einsatz kommt, sind Attacken auf kritische Infrastrukturen möglich.
- Link

—

Statischer Schlüssel in Dell Compellent leakt Zugangsdaten für VMware vCenter
Aufgrund einer Schwachstelle in Dells Compellent Integration Tools for VMware (CITV) können Angreifer Log-in-Daten entschlüsseln.
- Link

—

Sicherheitsupdates für Nextcloud: Angreifer können Daten löschen
Die Cloud-Computing-Software Nextcloud ist verwundbar. Sicherheitsupdates sind verfügbar.
- Link

—

Videomeeting-Anwendungen: Zoom rüstet Produkte gegen mögliche Attacken
Wichtige Sicherheitsupdates, für unter anderem den Windows-Client von Zoom, schließen mehrere Lücken.
- Link

—

Patchday: Kritische Schadcode-Lücken bedrohen Android 11, 12 und 13
Google und weitere Hersteller von Android-Geräten haben ihren monatlichen Sammel-Sicherheitsupdates veröffentlicht.
- Link

—

Patchday: Angreifer können Zugangsbeschränkungen von SAP PowerDesigner umgehen
Attacken vorbeugen: Firmen-Admins sollten ihre SAP-Anwendungen auf den aktuellen Stand bringen.
- Link

—

Patchday: Anwendungen von Adobe können Schadcode auf PCs lassen
Es sind wichtige Sicherheitsupdates für Adobe Commerce, Dimension, Reader und XMP Toolkit SDK erschienen.
- Link

—

Patchday: Angreifer umgehen Schutzmechanismus von Windows
Microsoft schließt unter anderem in Message Queuing, Outlook und Teams gefährliche Schadcodelücken.
- Link

—

Druck-Management-Lösung: Sicherheitslücken gefährden Papercut-Server
Im schlimmsten Fall können Angreifer Schadcode auf Papercut-Servern ausführen. Nicht alle Systeme sind standardmäßig gefährdet.
- 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-2023-3519	0.911990000	0.984640000	Link
CVE-2023-35078	0.965240000	0.994080000	Link
CVE-2023-34362	0.940540000	0.988060000	Link
CVE-2023-33246	0.963860000	0.993530000	Link
CVE-2023-28771	0.918810000	0.985250000	Link
CVE-2023-28121	0.937820000	0.987610000	Link
CVE-2023-27372	0.971220000	0.996770000	Link
CVE-2023-27350	0.971160000	0.996750000	Link
CVE-2023-25717	0.966450000	0.994610000	Link
CVE-2023-25194	0.918160000	0.985190000	Link
CVE-2023-21839	0.961530000	0.992810000	Link
CVE-2023-21554	0.902620000	0.983820000	Link
CVE-2023-20887	0.960660000	0.992560000	Link
CVE-2023-0669	0.967490000	0.995060000	Link

BSI - Warn- und Informationsdienst (WID)

Mon, 14 Aug 2023
[UPDATE] [hoch] AMD Prozessoren: Mehrere Schwachstellen
Ein lokaler Angreifer kann mehrere Schwachstellen in AMD Prozessoren ausnutzen, um beliebigen Programmcode auszuführen oder Informationen offenzulegen.
- Link

—

Mon, 14 Aug 2023
[NEU] [hoch] Red Hat OpenShift Service Mesh und Service Mesh Containers: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat OpenShift Service Mesh und Service Mesh Containers, sowie Red Hat Enterprise Linux ausnutzen, um einen Denial of Service Zustand herbeizuführen, Dateien zu manipulieren, Sicherheitsvorkehrungen zu umgehen oder Informationen offenzulegen.
- Link

—

Mon, 14 Aug 2023
[NEU] [UNGEPATCHT] [hoch] ESET Server Security: Schwachstelle ermöglicht Privilegieneskalation
Ein lokaler Angreifer kann eine Schwachstelle in ESET Server Security, ESET NOD32 Antivirus und ESET

Endpoint Security ausnutzen, um seine Privilegien zu erhöhen.
- Link

—

Mon, 14 Aug 2023
[NEU] [UNGEPATCHT] [hoch] poppler: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in poppler ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link

—

Mon, 14 Aug 2023
[UPDATE] [hoch] Apache HTTP Server: Mehrere Schwachstellen
Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen im Apache HTTP Server ausnutzen, um seine Rechte zu erweitern, Sicherheitsrestriktionen zu umgehen oder um einen Denial of Service Angriff durchzuführen.
- Link

—

Mon, 14 Aug 2023
[UPDATE] [hoch] Net-SNMP: Mehrere Schwachstellen ermöglichen Privilegieneskalation
Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Net-SNMP ausnutzen, um seine Privilegien zu erhöhen.
- Link

—

Mon, 14 Aug 2023
[UPDATE] [hoch] Apache HTTP Server: Mehrere Schwachstellen
Ein entfernter Angreifer kann mehrere Schwachstellen in Apache HTTP Server ausnutzen, um Sicherheitsvorkehrungen zu umgehen, vertrauliche Informationen offenzulegen und einen Denial of Service Zustand herzustellen.
- Link

—

Mon, 14 Aug 2023
[UPDATE] [kritisch] GNU libc: Mehrere Schwachstellen ermöglichen Codeausführung und Denial of Service
Ein Angreifer kann mehrere Schwachstellen in GNU libc ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service zu verursachen.
- Link

—

Mon, 14 Aug 2023
[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht nicht spezifizierten Angriff
Ein Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.
- Link

—

Mon, 14 Aug 2023
[UPDATE] [hoch] expat: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen
Ein Angreifer kann mehrere Schwachstellen in expat ausnutzen, um Sicherheitsvorkehrungen zu umgehen.
- Link

—

Mon, 14 Aug 2023
[UPDATE] [hoch] PostgreSQL: Schwachstelle ermöglicht Erlangen von Administratorrechten
Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in PostgreSQL ausnutzen, um Administratorrechte zu erlangen.
- Link

—

Mon, 14 Aug 2023
[UPDATE] [hoch] Rsync: Schwachstelle ermöglicht Manipulation von Dateien
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Rsync ausnutzen, um Dateien zu manipulieren.
- Link

—

Mon, 14 Aug 2023
[UPDATE] [hoch] Linux Kernel (ksmbd): Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um einen Denial of Service-Zustand herbeizuführen, Informationen offenzulegen, Sicherheitsvorkehrungen zu umgehen, Privilegien zu erweitern und beliebigen Code auszuführen.
- Link

—

Mon, 14 Aug 2023
[UPDATE] [hoch] LibreOffice: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in LibreOffice ausnutzen, um beliebigen Programmcode auszuführen und Sicherheitsmaßnahmen zu umgehen.
- Link

—

Mon, 14 Aug 2023
[UPDATE] [hoch] Ubuntu Linux: Mehrere Schwachstellen
Ein lokaler Angreifer kann mehrere Schwachstellen im Ubuntu Linux Kernel ausnutzen, um Sicherheitsvorkehrungen zu umgehen und seine Rechte zu erhöhen.
- Link

—

Mon, 14 Aug 2023
[UPDATE] [hoch] Microsoft Developer Tools: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft .NET Framework, Microsoft ASP.NET, Microsoft Azure DevOps Server und Microsoft Visual Studio ausnutzen, um beliebigen Programmcode auszuführen, seine Privilegien zu erweitern, Dateien zu manipulieren, einen Denial of Service Zustand herbeizuführen oder Informationen offenzulegen.
- Link

—

Fri, 11 Aug 2023
[UPDATE] [hoch] Lexmark Drucker: Mehrere Schwachstellen
Ein entfernter, anonymer oder authentifizierter Angreifer kann mehrere Schwachstellen in Lexmark Druckern ausnutzen, um beliebigen Programmcode auszuführen oder seine Rechte zu erweitern
- Link

—

Fri, 11 Aug 2023
[UPDATE] [hoch] Microsoft Exchange Server: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft Exchange Server 2016 und Microsoft Exchange Server 2019 ausnutzen, um seine Privilegien zu erhöhen, beliebigen Programmcode auszuführen oder Dateien zu manipulieren.
- Link

—

Fri, 11 Aug 2023
[NEU] [hoch] Veritas NetBackup Snapshot Manager: Schwachstelle ermöglicht Denial of Service
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Veritas NetBackup Snapshot Manager ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link

—

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

—

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
8/14/2023	[Amazon Linux 2 : openssh (ALAS-2023-2176)]	critical
8/14/2023	[Amazon Linux 2 : ca-certificates (ALAS-2023-2203)]	critical
8/14/2023	[Amazon Linux 2023 : ca-certificates (ALAS2023-2023-281)]	critical
8/14/2023	[Amazon Linux AMI : ca-certificates (ALAS-2023-1795)]	critical

Datum	Schwachstelle	Bewertung
8/14/2023	[Amazon Linux AMI : python-ecdsa (ALAS-2023-1800)]	critical
8/14/2023	[Amazon Linux 2 : ruby (ALAS-2023-2201)]	critical
8/14/2023	[Amazon Linux 2 : containerd (ALASNITRO-ENCLAVES-2023-026)]	critical
8/14/2023	[Amazon Linux 2 : avahi (ALAS-2023-2175)]	high
8/14/2023	[Amazon Linux 2 : nghttp2 (ALAS-2023-2180)]	high
8/14/2023	[Amazon Linux AMI : GraphicsMagick (ALAS-2023-1799)]	high
8/14/2023	[Amazon Linux 2 : aspell (ALAS-2023-2199)]	high
8/14/2023	[Amazon Linux 2 : kernel (ALASKERNEL-5.4-2023-050)]	high
8/14/2023	[Amazon Linux 2023 : python3-mako (ALAS2023-2023-288)]	high
8/14/2023	[Amazon Linux 2023 : avahi, avahi-autoipd, avahi-compat-howl (ALAS2023-2023-272)]	high
8/14/2023	[Amazon Linux 2023 : redis6, redis6-devel (ALAS2023-2023-291)]	high
8/14/2023	[Amazon Linux AMI : kernel (ALAS-2023-1792)]	high
8/14/2023	[Amazon Linux 2023 : libnghttp2, libnghttp2-devel, nghttp2 (ALAS2023-2023-278)]	high
8/14/2023	[Amazon Linux AMI : openssh (ALAS-2023-1794)]	high
8/14/2023	[Amazon Linux AMI : avahi (ALAS-2023-1790)]	high
8/14/2023	[Amazon Linux 2 : kernel (ALASKERNEL-5.15-2023-025)]	high
8/14/2023	[Amazon Linux AMI : nghttp2 (ALAS-2023-1793)]	high
8/14/2023	[Amazon Linux AMI : java-1.8.0-openjdk (ALAS-2023-1798)]	high
8/14/2023	[Amazon Linux 2023 : pcre2, pcre2-devel, pcre2-static (ALAS2023-2023-286)]	high
8/14/2023	[Amazon Linux 2023 : ghostscript, ghostscript-gtk, ghostscript-tools-dvipdf (ALAS2023-2023-276)]	high
8/14/2023	[Amazon Linux 2 : openssh (ALAS-2023-2202)]	high
8/14/2023	[RHEL 8 : .NET 6.0 (RHSA-2023:4640)]	high
8/14/2023	[RHEL 9 : rust (RHSA-2023:4634)]	high
8/14/2023	[RHEL 9 : .NET 7.0 (RHSA-2023:4642)]	high
8/14/2023	[RHEL 7 : rh-dotnet60-dotnet (RHSA-2023:4641)]	high
8/14/2023	[RHEL 9 : .NET 6.0 (RHSA-2023:4639)]	high
8/14/2023	[RHEL 8 : .NET 6.0 (RHSA-2023:4645)]	high
8/14/2023	[RHEL 8 : .NET 7.0 (RHSA-2023:4643)]	high
8/14/2023	[RHEL 9 : .NET 6.0 (RHSA-2023:4644)]	high
8/14/2023	[RHEL 8 : rust-toolset:rhel8 (RHSA-2023:4635)]	high

Die Hacks der Woche

mit Martin Haunschmid

Wasser predigen und Wein trinken? Ivanti, als Security Hersteller DARF so etwas nicht passieren!

Zum Youtube Video

Cyberangriffe: (Aug)

Datum	Opfer	Land	Information

Ransomware-Erpressungen: (Aug)

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-08-15	[Keystone Insurance Services]	8base	Link
2023-08-15	[ANS]	8base	Link
2023-08-15	[Aspect Structural Engineers]	8base	Link
2023-08-08	[Fondation De Verdeil]	noescape	Link
2023-08-14	[Freeport-McMoran - NYSE: FCX]	alphv	Link
2023-08-14	[jhillburn.com]	lockbit3	Link
2023-08-14	[qbcqatar.com.qa]	lockbit3	Link
2023-08-07	[John L Lowery & Associates]	noescape	Link
2023-08-07	[Federal Bar Association]	noescape	Link
2023-08-14	[leecorpinc.com]	lockbit3	Link
2023-08-14	[econsult.com]	lockbit3	Link
2023-08-14	[Saint Xavier University]	alphv	Link
2023-08-14	[Agriloja.pt]	everest	Link
2023-08-14	[CB Energy Australlia]	medusa	Link
2023-08-14	[Borets (Levare.com)]	medusa	Link
2023-08-13	[majan.com]	lockbit3	Link
2023-08-13	[luterkort.se]	lockbit3	Link
2023-08-13	[difccourts.ae]	lockbit3	Link
2023-08-13	[zaun.co.uk]	lockbit3	Link
2023-08-13	[roxcel.com.tr]	lockbit3	Link
2023-08-13	[meaf.com]	lockbit3	Link
2023-08-13	[stmarysschool.co.za]	lockbit3	Link
2023-08-13	[rappenglitz.de]	lockbit3	Link
2023-08-13	[siampremier.co.th]	lockbit3	Link
2023-08-12	[National Institute of Social Services for Retirees and Pensioners]	rhysida	Link
2023-08-12	[Armortex]	bianlian	Link
2023-08-12	[arganoInterRel]	alphv	Link
2023-08-11	[Rite Technology]	akira	Link
2023-08-11	[zain.com]	lockbit3	Link
2023-08-10	[Top Light]	play	Link
2023-08-10	[Algorry Zappia & Associates]	play	Link
2023-08-10	[EAI]	play	Link
2023-08-10	[The Belt Railway Company of Chicago]	akira	Link
2023-08-10	[Optimum Technology]	akira	Link
2023-08-10	[Boson]	akira	Link
2023-08-10	[Stockdale Podiatry]	8base	Link
2023-08-09	[oneatlas.com]	lockbit3	Link
2023-08-05	[Lower Yukon School District]	noescape	Link
2023-08-06	[Thermenhotel Stoiser]	incransom	Link
2023-08-09	[el-cerrito.org]	lockbit3	Link
2023-08-09	[fashions-uk.com]	lockbit3	Link
2023-08-09	[cbcstjohns.co.za]	lockbit3	Link
2023-08-09	[octoso.de]	lockbit3	Link
2023-08-09	[ricks-motorcycles.com]	lockbit3	Link
2023-08-09	[janus-engineering.com]	lockbit3	Link
2023-08-09	[csem.qc.ca]	lockbit3	Link
2023-08-09	[asfcustomers.com]	lockbit3	Link
2023-08-09	[sekuro.com.tr]	lockbit3	Link
2023-08-09	[TIMECO]	akira	Link
2023-08-09	[chula.ac.th]	lockbit3	Link
2023-08-09	[etisaleg.com]	lockbit3	Link
2023-08-09	[2plan.com]	lockbit3	Link
2023-08-08	[Sabalan Azmayesh]	arvinclub	Link
2023-08-09	[Optimum Health Solutions]	rhysida	Link
2023-08-09	[unitycouncil.org]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-08-09	[independenceia.org]	lockbit3	Link
2023-08-09	[www.finitia.net]	abyss	Link
2023-08-09	[Ramtha]	rhysida	Link
2023-08-08	[Batesville didn't react on appeal and allows Full Leak]	ragnarlocker	Link
2023-08-08	[ZESA Holdings]	everest	Link
2023-08-08	[Magic Micro Computers]	alphv	Link
2023-08-08	[Emerson School District]	medusa	Link
2023-08-08	[CH informatica]	8base	Link
2023-08-07	[Thonburi Energy Storage Systems (TESM)]	qilin	Link
2023-08-07	[Räddningstjänsten Västra Blekinge]	akira	Link
2023-08-07	[Papel Prensa SA]	akira	Link
2023-08-01	[Kreacta]	noescape	Link
2023-08-07	[Parsian Bitumen]	arvinclub	Link
2023-08-07	[varian.com]	lockbit3	Link
2023-08-06	[Delaney Browne Recruitment]	8base	Link
2023-08-06	[IBL]	alphv	Link
2023-08-05	[Draje food industrial group]	arvinclub	Link
2023-08-06	[Oregon Sports Medicine]	8base	Link
2023-08-06	[premierbpo.com]	alphv	Link
2023-08-06	[SatCom Marketing]	8base	Link
2023-08-05	[Rayden Solicitors]	alphv	Link
2023-08-05	[haynesintl.com]	lockbit3	Link
2023-08-05	[Kovair Software Data Leak]	everest	Link
2023-08-05	[Henlaw]	alphv	Link
2023-08-04	[mipe.com]	lockbit3	Link
2023-08-04	[armortex.com]	lockbit3	Link
2023-08-04	[iqcontrols.com]	lockbit3	Link
2023-08-04	[scottevest.com]	lockbit3	Link
2023-08-04	[atser.com]	lockbit3	Link
2023-08-04	[Galicia en Goles]	alphv	Link
2023-08-04	[tetco.com]	lockbit3	Link
2023-08-04	[SBS Construction]	alphv	Link
2023-08-04	[Koury Engineering]	akira	Link
2023-08-04	[Pharmatech Repblica Dominicana was hacked. All sensitive company and customer information]	alphv	Link
2023-08-04	[Grupo Garza Ponce was hacked! Due to a massive company vulnerability, more than 2 TB of se]	alphv	Link
2023-08-04	[seaside-kish co]	arvinclub	Link
2023-08-04	[Studio Domaine LLC]	nokoyawa	Link
2023-08-04	[THECHANGE]	alphv	Link
2023-08-04	[Ofimedic]	alphv	Link
2023-08-04	[Abatti Companies - Press Release]	monti	Link
2023-08-03	[Spokane Spinal Sports Care Clinic]	bianlian	Link
2023-08-03	[pointpleasant.k12.nj.us]	lockbit3	Link
2023-08-03	[Roman Catholic Diocese of Albany]	nokoyawa	Link
2023-08-03	[Venture General Agency]	akira	Link
2023-08-03	[Datawatch Systems]	akira	Link
2023-08-03	[admsc.com]	lockbit3	Link
2023-08-03	[United Tractors]	rhysida	Link
2023-08-03	[RevZero, Inc]	8base	Link
2023-08-03	[Rossman Realty Group, inc.]	8base	Link
2023-08-03	[riggsabney]	alphv	Link
2023-08-02	[fec-corp.com]	lockbit3	Link
2023-08-02	[bestmotel.de]	lockbit3	Link
2023-08-02	[Tempur Sealy International]	alphv	Link
2023-08-02	[constructioncrd.com]	lockbit3	Link
2023-08-02	[Helen F. Dalton Lawyers]	alphv	Link
2023-08-02	[TGRWA]	akira	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-08-02	[Guido]	akira	Link
2023-08-02	[Bickel & Brewer - Press Release]	monti	Link
2023-08-02	[SHERMAN.EDU]	clop	Link
2023-08-02	[COSI]	karakurt	Link
2023-08-02	[unicorpusa.com]	lockbit3	Link
2023-08-01	[Garage Living, The Dispenser USA]	play	Link
2023-08-01	[Aapd]	play	Link
2023-08-01	[Birch, Horton, Bittner & Cherot]	play	Link
2023-08-01	[DAL-TECH Engineering]	play	Link
2023-08-01	[Coral Resort]	play	Link
2023-08-01	[Professionnel France]	play	Link
2023-08-01	[ACTIVA Group]	play	Link
2023-08-01	[Aquatlantis]	play	Link
2023-08-01	[Kogetsu]	mallox	Link
2023-08-01	[Parathon by JDA eHealth Systems]	akira	Link
2023-08-01	[KIMCO Staffing Service]	alphv	Link
2023-08-01	[Pea River Electric Cooperative]	nokoyawa	Link
2023-08-01	[MBS Equipment TTI]	8base	Link
2023-08-01	[gerb.bg]	lockbit3	Link
2023-08-01	[persingerlaw.com]	lockbit3	Link
2023-08-01	[Jacklett Construction LLC]	8base	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/
7) Die Hacks der Woche - https://martinhaunschmid.com/videos

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.