Cybersecurity Morgenreport

Ausgabe: 20230808

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

Druck-Management-Lösung: Sicherheitslücken gefährden Papercut-Server
Im schlimmsten Fall können Angreifer Schadcode auf Papercut-Servern ausführen. Nicht alle Systeme sind standardmäßig gefährdet.
- Link

—

Sicherheitsupdates: Angreifer können Drucker von HP und Samsung attackieren
Einige Drucker-Modelle von HP und Samsung sind verwundbar. Sicherheitsupdates lösen das Problem.
- Link

—

Sicherheitsupdates F5 BIG-IP: Angreifer können Passwörter erraten
Es sind wichtige Sicherheitspatches für mehrere BIG-IP-Produkte von F5 erschienen. Admins sollten zeitnah handeln.
- Link

—

Sicherheitsupdates: Angreifer können Aruba-Switches kompromittieren
Bestimmte Switch-Modelle von Aruba sind verwundbar. Die Entwickler haben eine Sicherheitslücke geschlossen.
- Link

—

Upgrade nötig: Kritische Lücke bedroht ältere MobileIron-Ausgaben von Ivanti
Angreifer können an einer kritischen Schwachstelle in der nicht mehr im Support befindlichen Mobile-Device-Management-Lösung Ivanti MobileIron ansetzen.
- Link

—

Firefox, Thunderbird und Tor Browser bekommen Sicherheitsupdates
Angreifer könnten aus der Firefox-Sandbox ausbrechen. Die Entwickler haben noch weitere Lücken geschlossen.
- Link

—

Angreifer kapern Minecraft-Server über BleedingPipe-Exploit
Mehrere Mincecraft-Modifikationen weisen eine Schwachstelle auf, die Angreifer derzeit aktiv ausnutzen. Davon sollen neben Servern auch Clients betroffen sein.
- Link

—

Sicherheitsupdate: WordPress-Websites mit Plug-in Ninja Forms attackierbar
Angreifer könnten über eine Sicherheitslücke im Ninja-Forms-Plug-in auf eigentlich geschützte WordPress-Daten zugreifen.
- Link

—

Jetzt patchen! Ivanti schließt erneut Zero-Day-Lücke in EPMM
Derzeit nehmen Angreifer Ivanti Endpoint Manager Mobile (EPMM) ins Visier. Nun gibt es einen Patch gegen eine weitere Schwachstelle.
- Link

—

Angreifer können NAS- und IP-Videoüberwachungssysteme von Qnap lahmlegen
Mehrere Netzwerkprodukte von Qnap sind für eine DoS-Attacken anfällig. Dagegen abgesicherte Software schafft Abhilfe.
- 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	0.984500000	Link
CVE-2023-35078	0.955330000	0.991110000	Link
CVE-2023-34362	0.940540000	0.987960000	Link
CVE-2023-33246	0.963860000	0.993480000	Link
CVE-2023-28771	0.918810000	0.985130000	Link
CVE-2023-28121	0.937820000	0.987540000	Link
CVE-2023-27372	0.970090000	0.996170000	Link
CVE-2023-27350	0.971160000	0.996740000	Link
CVE-2023-25717	0.960700000	0.992550000	Link
CVE-2023-25194	0.918160000	0.985080000	Link
CVE-2023-21839	0.953670000	0.990650000	Link
CVE-2023-20887	0.960590000	0.992520000	Link
CVE-2023-0669	0.965030000	0.993910000	Link

BSI - Warn- und Informationsdienst (WID)

Mon, 07 Aug 2023
[UPDATE] [UNGEPATCHT] [hoch] ffmpeg wrapper for Java: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle im ffmpeg wrapper for Java ausnutzen, um beliebigen Programmcode auszuführen.
- Link

—

Mon, 07 Aug 2023
[UPDATE] [hoch] Mozilla Firefox und Mozilla Thunderbird: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Programmcode auszuführen, seine Privilegien zu erweitern, Informationen offenzulegen, Dateien zu manipulieren, einen Denial of Service Zustand herbeizuführen oder Sicherheitsvorkehrungen zu umgehen.
- Link

—

Mon, 07 Aug 2023
[NEU] [hoch] PHP: Mehrere Schwachstellen
Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in PHP ausnutzen, um Informationen offenzulegen oder beliebigen Code auszuführen.

- Link

—

Mon, 07 Aug 2023

[NEU] [hoch] HPE Fabric OS: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in HPE Fabric OS für HPE Fibre Channel und SAN Switches ausnutzen, um seine Privilegien zu erhöhen, Informationen offenzulegen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Mon, 07 Aug 2023

[UPDATE] [hoch] Google Chrome: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsmaßnahmen zu umgehen und vertrauliche Informationen offenzulegen.

- Link

—

Mon, 07 Aug 2023

[UPDATE] [hoch] Apple macOS: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apple macOS ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen, beliebigen Programmcode auszuführen, Informationen offenzulegen, seine Privilegien zu erweitern, Dateien zu manipulieren, einen Denial of Service Zustand herbeizuführen, Sicherheitsvorkehrungen zu umgehen oder sonstige Auswirkungen zu verursachen.

- Link

—

Mon, 07 Aug 2023

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

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

- Link

—

Mon, 07 Aug 2023

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

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

- Link

—

Fri, 04 Aug 2023

[NEU] [hoch] Ivanti Endpoint Manager Mobile.: Schwachstelle ermöglicht Manipulation von Dateien

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Ivanti Endpoint Manager Mobile. ausnutzen, um Dateien zu manipulieren.

- Link

—

Fri, 04 Aug 2023

[UPDATE] [hoch] Google Chrome und Microsoft Edge: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um vertrauliche Informationen offenzulegen, Sicherheitsmechanismen zu umgehen, den Benutzer zu täuschen und nicht näher beschriebene Auswirkungen zu erzielen.

- Link

—

Fri, 04 Aug 2023

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

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

- Link

—

Fri, 04 Aug 2023

[UPDATE] [hoch] OpenSSH: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in OpenSSH ausnutzen, um beliebigen Programm-

code auszuführen.
- Link
—
Fri, 04 Aug 2023
[NEU] [hoch] Veritas NetBackup: Mehrere Schwachstellen
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Veritas NetBackup ausnutzen, um beliebigen Programmcode auszuführen und nicht spezifizierte Auswirkungen zu verursachen.
- Link
—
Thu, 03 Aug 2023
[UPDATE] [hoch] vim: Mehrere Schwachstellen ermöglichen Codeausführung
Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in vim ausnutzen, um beliebigen Code auszuführen, Speicher zu modifizieren und einen Denial of Service Zustand zu verursachen.
- Link
—
Thu, 03 Aug 2023
[UPDATE] [hoch] vim: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in vim ausnutzen, um beliebigen Programmcode auszuführen, einen Denial of Service Zustand herbeizuführen oder Dateien zu manipulieren.
- Link
—
Thu, 03 Aug 2023
[UPDATE] [hoch] vim: Mehrere Schwachstellen
Ein entfernter, anonymer oder lokaler Angreifer kann mehrere Schwachstellen in vim ausnutzen, um einen Denial of Service Angriff durchzuführen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen und den Speicher zu manipulieren.
- Link
—
Thu, 03 Aug 2023
[UPDATE] [hoch] vim: Schwachstelle ermöglicht Codeausführung
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in vim ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen und vertrauliche Informationen offenzulegen
- Link
—
Thu, 03 Aug 2023
[UPDATE] [hoch] Python: Schwachstelle ermöglicht Denial of Service
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Python ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link
—
Thu, 03 Aug 2023
[UPDATE] [hoch] Microsoft Developer Tools: Mehrere Schwachstellen
Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Microsoft .NET Framework, Microsoft Azure DevOps Server, Microsoft NuGet, Microsoft Visual Studio und Microsoft Visual Studio Code ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, einen Denial-of-Service-Zustand herbeizuführen, seine Rechte zu erweitern und Daten zu manipulieren.
- Link
—
Thu, 03 Aug 2023
[UPDATE] [hoch] Microsoft Developer Tools: Mehrere Schwachstellen
Ein entfernter, authentisierter oder anonymer 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
—

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
8/7/2023	[RHEL 8 : thunderbird (RHSA-2023:4492)]	critical
8/7/2023	[Debian DSA-5469-1 : thunderbird - security update]	critical
8/7/2023	[RHEL 7 : thunderbird (RHSA-2023:4495)]	critical
8/7/2023	[RHEL 8 : thunderbird (RHSA-2023:4497)]	critical
8/7/2023	[RHEL 8 : thunderbird (RHSA-2023:4500)]	critical
8/7/2023	[RHEL 9 : thunderbird (RHSA-2023:4499)]	critical
8/7/2023	[RHEL 9 : thunderbird (RHSA-2023:4494)]	critical
8/7/2023	[RHEL 8 : thunderbird (RHSA-2023:4496)]	critical
8/7/2023	[RHEL 8 : thunderbird (RHSA-2023:4493)]	critical
8/7/2023	[Ubuntu 16.04 ESM : unixODBC vulnerability (USN-6276-1)]	critical
8/7/2023	[Mitsubishi MELSEC-F Series Authentication Bypass by Capture-replay (CVE-2023-2846)]	critical
8/6/2023	[Debian DLA-3517-1 : pdfcrack - LTS security update]	critical
8/4/2023	[Oracle Linux 8 : firefox (ELSA-2023-4468)]	critical
8/7/2023	[Fedora 38 : llhttp / python-aiohttp (2023-f75af676f2)]	high
8/7/2023	[openSUSE 15 Security Update : virtualbox (openSUSE-SU-2023:0213-1)]	high
8/7/2023	[Debian DSA-5468-1 : webkit2gtk - security update]	high
8/7/2023	[FreeBSD : electron{23,24,25} – multiple vulnerabilities (f3a35fb8-2d70-47c9-a516-6aad7eb222b1)]	high
8/7/2023	[Zyxel USG < 5.37 / ATP < 5.37 / VPN < 5.37 Multiple Vulnerabilities]	high
8/7/2023	[Microsoft Edge (Chromium) < 114.0.1823.106 / 115.0.1901.200 Multiple Vulnerabilities]	high
8/7/2023	[RHEL 7 : Red Hat JBoss Enterprise Application Platform (RHSA-2023:4505)]	high
8/7/2023	[RHEL 9 : Red Hat JBoss Enterprise Application Platform (RHSA-2023:4507)]	high
8/7/2023	[RHEL 8 : Red Hat JBoss Enterprise Application Platform (RHSA-2023:4506)]	high
8/7/2023	[AlmaLinux 8 : ruby:2.7 (ALSA-2021:2584)]	high
8/7/2023	[AlmaLinux 8 : ruby:2.6 (ALSA-2021:2588)]	high
8/7/2023	[AlmaLinux 8 : kernel-rt (ALSA-2023:1584)]	high
8/7/2023	[AlmaLinux 8 : kernel (ALSA-2022:0825)]	high
8/7/2023	[AlmaLinux 8 : java-17-openjdk (ALSA-2022:1445)]	high
8/5/2023	[openSUSE 15 Security Update : amanda (openSUSE-SU-2023:0205-1)]	high
8/5/2023	[openSUSE 15 Security Update : amanda (openSUSE-SU-2023:0206-1)]	high
8/5/2023	[Fedora 38 : seamonkey (2023-e7f8101829)]	high
8/5/2023	[Fedora 38 : amanda (2023-4db1d56125)]	high
8/5/2023	[Fedora 37 : libopenmpt (2023-d43fda08d6)]	high
8/5/2023	[Fedora 37 : amanda (2023-566e354e4a)]	high
8/5/2023	[Debian DSA-5467-1 : chromium - security update]	high
8/5/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : xtrans (SUSE-SU-2023:3190-1)]	high
8/5/2023	[SUSE SLES12 Security Update : javapackages-tools, javassist, mysql-connector-java, protobuf, python-python-gflags (SUSE-SU-2023:3187-1)]	high
8/5/2023	[SUSE SLES12 Security Update : xtrans (SUSE-SU-2023:3189-1)]	high
8/5/2023	[Debian DLA-3516-1 : burp - LTS security update]	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
2023-08-07	[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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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.