Cybersecurity Morgenreport

Ausgabe: 20230719

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

Webbrowser: Google stopft 20 Sicherheitslecks in Chrome 115
Google hat den Webbrowser Chrome in Version 115 vorgelegt. Darin bessern die Entwickler 20 Schwachstellen aus.
- Link

Citrix: Updates schließen kritische Zero-Day-Lücke in Netscaler ADC und Gateway
IT-Verantwortliche sollten zügig aktualisieren: Citrix hat Updates für bereits angegriffene Lücken in Netscaler ADC und Gateway veröffentlicht.
- Link

JavaScript-Sandbox vm2: Neue kritische Schwachstelle, kein Update mehr
Für die jüngste kritische Sicherheitslücke im Open-Source-Projekt vm2 gibt es keinen Bugfix, sondern der Betreiber rät zum Umstieg auf isolated-vm.
- Link

Wordpress: Angriffswelle auf Woocommerce Payments läuft derzeit
Die IT-Forscher von Wordfence beobachten eine Angriffswelle auf das Woocommerce Payments-Plug-in. Es ist auf mehr als 600.000 Websites installiert.
- Link

Zyxel dichtet hochriskante Sicherheitslücken in Firewalls ab
Zyxel warnt vor mehreren, teils hochriskanten Schwachstellen in den Firewalls und WLAN-Controllern. Aktualisierte Firmware bessert sie aus.
- Link

Mehrere kritische Lücken in Sonicwalls GMS-Firewall-Management geschlossen
In Sonicwalls GMS-Firewall-Management sowie Analytics-Management klaffen unter anderem kritische Sicherherheitslücken. Updates dichten sie ab.
- Link

Juniper dichtet teils kritische Sicherheitslücken ab
Der Netzwerkausrüster Juniper hat 17 Sicherheitsmeldungen zu teils kritischen Lücken veröffentlicht. Updates zum Schließen stehen bereit.
- Link

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

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	0.987730000	Link
CVE-2023-33246	0.955810000	0.991040000	Link
CVE-2023-27372	0.970730000	0.996430000	Link
CVE-2023-27350	0.971180000	0.996670000	Link
CVE-2023-25717	0.955670000	0.991010000	Link
CVE-2023-21839	0.950530000	0.989680000	Link
CVE-2023-0669	0.963970000	0.993360000	Link

BSI - Warn- und Informationsdienst (WID)

Tue, 18 Jul 2023
[UPDATE] [hoch] 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

—

Tue, 18 Jul 2023
[UPDATE] [hoch] cURL: Mehrere Schwachstellen [hoch]
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in cURL ausnutzen, um einen Denial of Service zu verursachen, Informationen offenzulegen oder weitere, nicht näher spezifizierte Angriffe durchzuführen.
- Link

—

Tue, 18 Jul 2023
[UPDATE] [hoch] 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

—

Tue, 18 Jul 2023
[UPDATE] [hoch] Adobe ColdFusion: Mehrere Schwachstellen [hoch]
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Adobe ColdFusion ausnutzen, um Sicherheitsvorkehrungen zu umgehen oder beliebigen Programmcode auszuführen.
- Link

—

Tue, 18 Jul 2023
[NEU] [hoch] Mattermost: Mehrere Schwachstellen [hoch]
Ein entfernter, anonymer Angreifer kann diese Schwachstellen in Mattermost ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen und Sicherheitsmaßnahmen zu umgehen.
- Link
—
Tue, 18 Jul 2023
[NEU] [hoch] VMware Tanzu Spring Security: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen [hoch]
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in VMware Tanzu Spring Security ausnutzen, um Sicherheitsvorkehrungen zu umgehen.
- Link
—
Tue, 18 Jul 2023
[NEU] [hoch] Zyxel Firewall: Mehrere Schwachstellen [hoch]
Ein Angreifer aus dem angrenzenden Netz kann mehrere Schwachstellen in Zyxel Firewall ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.
- Link
—
Tue, 18 Jul 2023
[UPDATE] [hoch] Grafana: Schwachstelle ermöglicht Übernahme von Benutzerkonto [hoch]
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Grafana ausnutzen, um ein Benutzerkonto zu übernehmen.
- Link
—
Tue, 18 Jul 2023
[UPDATE] [hoch] OpenSSL: Mehrere Schwachstellen ermöglichen Denial of Service [hoch]
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in OpenSSL ausnutzen, um einen Denial of Service Angriff durchzuführen oder Informationen offenzulegen.
- Link
—
Tue, 18 Jul 2023
[UPDATE] [hoch] OpenSSL: Schwachstelle ermöglicht Offenlegung von Informationen [hoch]
Ein Angreifer kann eine Schwachstelle in OpenSSL ausnutzen, um Informationen offenzulegen.
- Link
—
Tue, 18 Jul 2023
[UPDATE] [hoch] Red Hat Enterprise Linux (OpenvSwitch): Mehrere Schwachstellen [hoch]
Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux bezüglich des OpenvSwitch Pakets ausnutzen, um einen Denial of Service Angriff durchzuführen oder weitere, nicht spezifizierte Auswirkungen zu verursachen.
- Link
—
Tue, 18 Jul 2023
[UPDATE] [hoch] 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, 18 Jul 2023
[UPDATE] [hoch] Node.js: Mehrere Schwachstellen [hoch]
Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um seine Privilegien zu erweitern, Dateien zu manipulieren, einen Denial of Service Zustand herbeizuführen, Informationen offenzulegen oder Sicherheitsvorkehrungen zu umgehen.
- Link
—
Tue, 18 Jul 2023
[UPDATE] [hoch] 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, 18 Jul 2023
[UPDATE] [hoch] Microsoft Developer Tools: Mehrere Schwachstellen [hoch]
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
—
Mon, 17 Jul 2023
[UPDATE] [hoch] 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
—
Mon, 17 Jul 2023
[UPDATE] [hoch] poppler: Schwachstelle ermöglicht nicht spezifizierten Angriff [hoch]
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in poppler ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.
- Link
—
Mon, 17 Jul 2023
[NEU] [hoch] Adobe ColdFusion: Schwachstelle ermöglicht Codeausführung [hoch]
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Adobe ColdFusion ausnutzen, um beliebigen Programmcode auszuführen.
- Link
—
Mon, 17 Jul 2023
[NEU] [hoch] Bitdefender Engine: Schwachstelle ermöglicht Denial of Service [hoch]
Ein entfernter, anonymer Angreifer kann eine Schwachstelle in verschiedenen Bitdefender Engines ausnutzen, um einen Denial of Service Angriff durchzuführen.
- Link
—
Mon, 17 Jul 2023
[NEU] [hoch] IBM InfoSphere Information Server: Mehrere Schwachstellen [hoch]
Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in IBM InfoSphere Information Server ausnutzen, um beliebigen Programmcode auszuführen, Sicherheitsvorkehrungen zu umgehen oder einen Denial of Service Zustand herbeizuführen.
- Link
—

Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
7/18/2023	[openSUSE 15 Security Update : openvswitch (SUSE-SU-2023:2250-2)]	critical
7/18/2023	[Adobe ColdFusion < 2018.x < 2018u18 / 2021.x < 2021u8 / 2023.x < 2023u2 Code Execution (APSB23-41)]	critical
7/18/2023	[RHEL 9 : curl (RHSA-2023:4139)]	critical
7/18/2023	[Microsoft 365 (Office) App Code Execution (December 2021)]	critical
7/18/2023	[Citrix ADC and Citrix Gateway Multiple Vulnerabilities (CTX561482)]	critical
7/18/2023	[Google Chrome < 115.0.5790.98 Multiple Vulnerabilities]	critical
7/18/2023	[Google Chrome < 115.0.5790.98 Multiple Vulnerabilities]	critical

Datum	Schwachstelle	Bewertung
7/18/2023	[Amazon Corretto Java 8.x < 8.382.05.1 Multiple Vulnerabilities]	critical
7/18/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : go1.20 (SUSE-SU-2023:2846-1)]	high
7/18/2023	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : go1.19 (SUSE-SU-2023:2845-1)]	high
7/18/2023	[SUSE SLES12 Security Update : MozillaFirefox, MozillaFirefox-branding-SLE (SUSE-SU-2023:2850-1)]	high
7/18/2023	[SUSE SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2023:2859-1)]	high
7/18/2023	[SUSE SLES15 Security Update : libqt5-qtbase (SUSE-SU-2023:2860-1)]	high
7/18/2023	[SUSE SLES12 Security Update : ghostscript (SUSE-SU-2023:2844-1)]	high
7/18/2023	[SUSE SLES15 Security Update : nodejs16 (SUSE-SU-2023:2861-1)]	high
7/18/2023	[SUSE SLES15 Security Update : MozillaFirefox, MozillaFirefox-branding-SLE (SUSE-SU-2023:2849-1)]	high
7/18/2023	[SUSE SLES12 Security Update : java-1_8_0-ibm (SUSE-SU-2023:2863-1)]	high
7/18/2023	[Cisco ACI Multi-Site CloudSec Encryption Information Disclosure (cisco-sa-aci-cloudsec-enc-Vs5Wn2sX)]	high
7/18/2023	[AlmaLinux 8 : bind9.16 (ALSA-2023:4100)]	high
7/18/2023	[AlmaLinux 8 : bind (ALSA-2023:4102)]	high
7/18/2023	[AlmaLinux 9 : bind (ALSA-2023:4099)]	high
7/18/2023	[RHEL 8 : edk2 (RHSA-2023:4124)]	high
7/18/2023	[RHEL 8 : kernel-rt (RHSA-2023:4126)]	high
7/18/2023	[RHEL 9 : kernel (RHSA-2023:4137)]	high
7/18/2023	[RHEL 7 : bind (RHSA-2023:4152)]	high
7/18/2023	[RHEL 8 : kpatch-patch (RHSA-2023:4146)]	high
7/18/2023	[RHEL 8 : bind (RHSA-2023:4153)]	high
7/18/2023	[RHEL 8 : kernel (RHSA-2023:4125)]	high
7/18/2023	[RHEL 7 : kernel (RHSA-2023:4151)]	high
7/18/2023	[RHEL 8 : edk2 (RHSA-2023:4128)]	high
7/18/2023	[RHEL 8 : kernel (RHSA-2023:4130)]	high
7/18/2023	[RHEL 8 : bind (RHSA-2023:4154)]	high
7/18/2023	[RHEL 8 : kpatch-patch (RHSA-2023:4145)]	high
7/18/2023	[RHEL 7 : kernel-rt (RHSA-2023:4150)]	high
7/18/2023	[RHEL 9 : kernel-rt (RHSA-2023:4138)]	high
7/18/2023	[Autodesk Maya USD Plugin < 0.23.0 Multiple Vulnerabilities (ADSK-SA-2023-0003)]	high
7/18/2023	[RHEL 9 : webkit2gtk3 (RHSA-2023:4201)]	high
7/18/2023	[RHEL 9 : python3.9 (RHSA-2023:4203)]	high
7/18/2023	[RHEL 8 : webkit2gtk3 (RHSA-2023:4202)]	high
7/18/2023	[Ubuntu 16.04 ESM / 18.04 ESM : YAJL vulnerabilities (USN-6233-1)]	high
7/18/2023	[Ubuntu 16.04 ESM : libwebp vulnerability (USN-6078-2)]	high
7/18/2023	[Ubuntu 16.04 ESM / 18.04 ESM : Bind vulnerability (USN-6183-2)]	high
7/18/2023	[Amazon Corretto Java 17.x < 17.0.8.7.1 Multiple Vulnerabilities]	high
7/18/2023	[Amazon Corretto Java 11.x < 11.0.20.8.1 Multiple Vulnerabilities]	high
7/18/2023	[AlmaLinux 9 : webkit2gtk3 (ALSA-2023:4201)]	high

Die Hacks der Woche

mit Martin Haunschmid

Ein gefundenes Fressen für Cloud Gegner? Microsoft GEHACKT!

Zum Youtube Video

Cyberangriffe: (Jul)

Datum	Opfer	Land	Information
2023-07-16	TOMRA	[NOR]	Link
2023-07-13	Morehead State University	[USA]	Link
2023-07-12	Comune di Ferrara	[ITA]	Link
2023-07-11	ZooTampa	[USA]	Link
2023-07-11	Ville de Cornelius	[USA]	Link
2023-07-11	Tribunal de Contas do Estado do Rio de Janeiro (TCE-RJ)	[BRA]	Link
2023-07-11	La Province de Namur	[BEL]	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-Grupppe	Webseite
2023-07-19	[PWCCLINETSANDDOCUMENTS.COM]	clop	Link
2023-07-19	[DMA.US]	clop	Link
2023-07-19	[VENTIVTECH.COM]	clop	Link
2023-07-19	[BLUEFIN.COM]	clop	Link
2023-07-19	[ESTEELAUDER.COM]	clop	Link
2023-07-19	[OFCOM.ORG.UK]	clop	Link
2023-07-19	[ALLEGIANTAIR.COM]	clop	Link
2023-07-19	[ITT.COM]	clop	Link
2023-07-19	[SMC3.COM]	clop	Link
2023-07-19	[COMREG.IE]	clop	Link
2023-07-19	[JONASFITNESS.COM]	clop	Link
2023-07-19	[AA.COM]	clop	Link
2023-07-18	[EA SMITH]	alphv	Link
2023-07-19	[VOG]	alphv	Link
2023-07-18	[The Estée Lauder Companies]	alphv	Link
2023-07-18	[DTD Express]	medusa	Link
2023-07-18	[KUITS]	alphv	Link
2023-07-18	[Tampa general hospital]	snatch	Link
2023-07-18	[Acomen]	noescape	Link
2023-07-18	[Girardini Holding Srl]	noescape	Link
2023-07-18	[Health Springs Medical Center]	medusa	Link
2023-07-18	[Nini Collection Ltd (Nini's Jewels)]	medusa	Link
2023-07-18	[lfcaire.org]	lockbit3	Link
2023-07-18	[suninsurance.com.fj]	lockbit3	Link
2023-07-18	[berg-life.com]	lockbit3	Link
2023-07-18	[cotrelec.com]	lockbit3	Link
2023-07-18	[ope.com.na]	lockbit3	Link
2023-07-18	[dixiesfed.com]	lockbit3	Link
2023-07-18	[flexity.com]	lockbit3	Link
2023-07-18	[www.brockhouse.co.uk]	abyss	Link
2023-07-18	[academia21.com]	lockbit3	Link
2023-07-18	[CashCall, Inc.]	8base	Link
2023-07-18	[Seasia Infotech]	snatch	Link
2023-07-18	[Ningbo Joyson Electronic Corp.]	snatch	Link
2023-07-18	[Wasserstrom]	snatch	Link
2023-07-17	[Protected: Hidden name]	medusalocker	Link
2023-07-17	[Senior]	stormous	Link
2023-07-17	[hopetech.com]	lockbit3	Link
2023-07-17	[johnreilly.co.uk]	lockbit3	Link
2023-07-17	[Cavanaugh, Biggs & Lemon P.A., Attorneys at Law]	alphv	Link
2023-07-17	[www.tractrad.com]	abyss	Link
2023-07-17	[RCI.COM]	clop	Link
2023-07-17	[SIERRAWIRELESS.COM]	clop	Link
2023-07-17	[COMPUCOM.COM]	clop	Link
2023-07-17	[CFINS.COM]	clop	Link
2023-07-17	[DESMI.COM]	clop	Link
2023-07-17	[FMGL.COM.AU]	clop	Link
2023-07-17	[VALMET.COM]	clop	Link
2023-07-17	[VITESCO-TECHNOLOGIES.COM]	clop	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-07-17	[TJX.COM]	clop	Link
2023-07-17	[Stephen F. Austin State University]	rhysida	Link
2023-07-17	[IRIS Informatique]	rhysida	Link
2023-07-17	[ICT-College]	rhysida	Link
2023-07-15	[Venture Drilling Supply]	8base	Link
2023-07-16	[test.com]	lockbit3	Link
2023-07-11	[selmi.com.br]	lockbit3	Link
2023-07-16	[www.stri.se]	abyss	Link
2023-07-16	[Baumschlager Hutter Partners - Business Information]	alphv	Link
2023-07-16	[www.arb.ch]	abyss	Link
2023-07-11	[Propper International]	moneymessage	Link
2023-07-14	[Meteksan Defence Industry]	moneymessage	Link
2023-07-15	[equmedia.es]	lockbit3	Link
2023-07-15	[jasperpictures]	stormous	Link
2023-07-15	[magnumphotos.com]	lockbit3	Link
2023-07-15	[konrad-mr.de]	lockbit3	Link
2023-07-15	[greatlakesmbpm.com]	lockbit3	Link
2023-07-15	[hgc.com.hk]	lockbit3	Link
2023-07-15	[province.namur.be]	lockbit3	Link
2023-07-15	[energym.co.il]	lockbit3	Link
2023-07-15	[co.langlade.wi.us]	lockbit3	Link
2023-07-15	[Highland Health Systems]	alphv	Link
2023-07-14	[Chin Hin Group]	alphv	Link
2023-07-14	[Caterham High School]	rhysida	Link
2023-07-08	[Superloop ISP]	cyclops	Link
2023-07-14	[NOTABLEFRONTIER.COM]	clop	Link
2023-07-14	[GRACE.COM]	clop	Link
2023-07-14	[PRGX.COM]	clop	Link
2023-07-14	[HESS.COM]	clop	Link
2023-07-14	[MYCWT.COM]	clop	Link
2023-07-14	[SCHNABEL-ENG.COM]	clop	Link
2023-07-14	[ARIETISHEALTH.COM]	clop	Link
2023-07-14	[PINNACLETPA.COM]	clop	Link
2023-07-14	[REPSOLSINOPECUK.COM]	clop	Link
2023-07-11	[Jordan Airmotive Ltd]	noescape	Link
2023-07-11	[Burton & South Derbyshire College]	noescape	Link
2023-07-14	[JTI.COM]	clop	Link
2023-07-14	[VOSS.NET]	clop	Link
2023-07-14	[UFCU.ORG]	clop	Link
2023-07-14	[YAKULT.COM.PH]	clop	Link
2023-07-14	[ROCHESTER.EDU]	clop	Link
2023-07-14	[eyedoc.com.na]	lockbit3	Link
2023-07-14	[CPA Advisors Group]	8base	Link
2023-07-14	[Info Salons]	8base	Link
2023-07-14	[The Big Life group]	rhysida	Link
2023-07-13	[Gerber ChildrenswearLLC]	akira	Link
2023-07-13	[Blackjewel L.L.C.]	lockbit3	Link
2023-07-13	[SHUTTERFLY.COM]	clop	Link
2023-07-13	[DISCOVERY.COM]	clop	Link
2023-07-13	[ASPENTECH.COM]	clop	Link
2023-07-13	[MOTHERSON.COM]	clop	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2023-07-13	[PAYCOM.COM]	clop	Link
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	[CLEARESULT.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
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

Datum	Opfer	Ransomware-Grupppe	Webseite
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	[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

Datum	Opfer	Ransomware-Grupppe	Webseite
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	[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

Datum	Opfer	Ransomware-Grupppe	Webseite
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]	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
2023-07-01	[Kondratoff Persick LLP]	bianlian	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
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/
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.