Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240220

Inhaltsverzeichnis

1 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

2 Security-News

2.1 Heise - Security-Alert

Solarwinds: Codeschmuggel möglich, Updates verfügbar

Solarwinds schließt Sicherheitslücken in Access Rights Manager und Platform (Orion). Angreifer können Schadcode einschleusen.

- Link

—

Eset: Schwachstelle in Hintergrundscanner löscht beliebige Dateien

Der Hintergrundwächter der Eset-Virenscanner enthält eine Schwachstelle, durch die bösartige Akteure Dateien mit Systemrechten löschen können.

- Link

—

Node.js: Sicherheitsupdates beheben Codeschmuggel und Serverabstürze

Neben Problemen im Kern des Projekts aktualisiert das Node-Projekt auch einige externe Bibliotheken.

- Link

—

Jetzt patchen! Angreifer nutzen kritische Lücke in Microsoft Exchange Server aus

Derzeit verschaffen sich Angreifer Zugriffe auf Exchange Server, um diese zu kompromittieren. Schutzlösungen sind verfügbar.

- Link

—

AMD meldet zahlreiche Sicherheitslücken in Prozessoren

AMD hat Sicherheitsmitteilungen zu Schwachstellen in diversen Prozessoren veröffentlicht. Firmwareupdates sollen sie ausbessern.

- Link

—

Webkonferenz-Tool Zoom: Rechteausweitung durch kritische Schwachstelle

Zoom warnt vor mehreren Schwachstellen in den Produkten des Unternehmens. Eine gilt als kritisches Sicherheitsrisiko.

- Link

—

Patchday: Adobe schließt Schadcode-Lücken in Acrobat & Co.

Für mehrere Adobe-Produkte sind wichtige Sicherheitsupdates erschienen. Damit haben die Entwickler unter anderem kritische Schwachstellen geschlossen.

- Link

—

Sicherheitslücke in Webmailer Roundcube wird angegriffen

Angreifer attackieren eine Sicherheitslücke in dem Webmail-Programm Roundcube. Ein Update steht bereits länger bereit.

- Link

—

Patchday: Attacken auf Windows - Sicherheitsfunktion SmartScreen umgangen

Aufgrund von laufenden Attacken sollten Windows-Admins die aktuellen Sicherheitsupdates zügig installieren.

- Link

—

DNS-Server: Bind, dnsmasq und Unbound stolpern über Sicherheitslücke "KeyTrap"

Mit einer präparierten DNS-Anfrage können Angreifer eine hohe Prozessorlast verursachen und den Dienst für legitime Nutzer so blockieren. Patches stehen bereit.

- Link

—

3 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.

3.1 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.

3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-6553	0.916210000	0.988150000	Link
CVE-2023-5360	0.967230000	0.996290000	Link
CVE-2023-4966	0.963970000	0.995180000	Link
CVE-2023-47246	0.943540000	0.991260000	Link
CVE-2023-46805	0.962740000	0.994800000	Link
CVE-2023-46747	0.971390000	0.997730000	Link
CVE-2023-46604	0.972850000	0.998420000	Link
CVE-2023-43177	0.932620000	0.989930000	Link
CVE-2023-42793	0.973130000	0.998590000	Link
CVE-2023-41265	0.915100000	0.988010000	Link
CVE-2023-39143	0.925430000	0.989140000	Link
CVE-2023-38646	0.903940000	0.987070000	Link
CVE-2023-38205	0.932790000	0.989970000	Link
CVE-2023-38035	0.974110000	0.999230000	Link
CVE-2023-36845	0.964780000	0.995410000	Link
CVE-2023-3519	0.912410000	0.987820000	Link
CVE-2023-35082	0.962080000	0.994630000	Link
CVE-2023-35078	0.949930000	0.992230000	Link
CVE-2023-34960	0.931300000	0.989760000	Link
CVE-2023-34634	0.919000000	0.988450000	Link
CVE-2023-34362	0.961230000	0.994430000	Link
CVE-2023-3368	0.928930000	0.989460000	Link
CVE-2023-33246	0.973410000	0.998760000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-32315	0.973860000	0.999030000	Link
CVE-2023-32235	0.902020000	0.986970000	Link
CVE-2023-30625	0.951530000	0.992490000	Link
CVE-2023-30013	0.936180000	0.990260000	Link
CVE-2023-29300	0.959640000	0.994080000	Link
CVE-2023-28771	0.923800000	0.988980000	Link
CVE-2023-28121	0.933120000	0.989990000	Link
CVE-2023-27524	0.972330000	0.998190000	Link
CVE-2023-27372	0.970420000	0.997320000	Link
CVE-2023-27350	0.972270000	0.998160000	Link
CVE-2023-26469	0.936750000	0.990360000	Link
CVE-2023-26360	0.957020000	0.993550000	Link
CVE-2023-26035	0.968710000	0.996740000	Link
CVE-2023-25717	0.962730000	0.994790000	Link
CVE-2023-2479	0.964780000	0.995400000	Link
CVE-2023-24489	0.973500000	0.998820000	Link
CVE-2023-23752	0.949820000	0.992200000	Link
CVE-2023-23397	0.904540000	0.987100000	Link
CVE-2023-22527	0.964800000	0.995420000	Link
CVE-2023-22518	0.969180000	0.996880000	Link
CVE-2023-22515	0.973330000	0.998720000	Link
CVE-2023-21839	0.962110000	0.994630000	Link
CVE-2023-21554	0.961220000	0.994420000	Link
CVE-2023-20887	0.965640000	0.995780000	Link
CVE-2023-20198	0.919220000	0.988470000	Link
CVE-2023-1671	0.964220000	0.995250000	Link
CVE-2023-0669	0.968020000	0.996540000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Mon, 19 Feb 2024

[UPDATE] [hoch] Red Hat Enterprise Linux: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Red Hat Enterprise Linux ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Mon, 19 Feb 2024

[UPDATE] [hoch] JFrog Artifactory: Schwachstelle ermöglicht SQL-Injection

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in JFrog Artifactory ausnutzen, um eine SQL-Injection durchzuführen.

- Link

—

Mon, 19 Feb 2024

[NEU] [hoch] Icinga: Schwachstelle ermöglicht Cross-Site Scripting

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Icinga ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen.

- Link

—

Mon, 19 Feb 2024

[UPDATE] [hoch] Apache log4j: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Apache log4j ausnutzen, um beliebigen Programmcode auszuführen oder einen SQL-Injection durchzuführen.

- Link

—

Mon, 19 Feb 2024

[UPDATE] [hoch] CUPS: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in CUPS, Debian Linux und SUSE Linux ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Mon, 19 Feb 2024

[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 Privi-

legien zu erweitern, Informationen offenzulegen, Dateien zu manipulieren, einen Denial of Service Zustand herbeizuführen oder Sicherheitsvorkehrungen zu umgehen.

- Link

—

Mon, 19 Feb 2024

[UPDATE] [hoch] Mozilla Firefox und Thunderbird: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen und vertrauliche Informationen offenzulegen.

- Link

—

Mon, 19 Feb 2024

[UPDATE] [hoch] CUPS: Schwachstelle ermöglicht Codeausführung

Ein entfernter Angreifer kann eine Schwachstelle in CUPS ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Mon, 19 Feb 2024

[UPDATE] [kritisch] Exim: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Exim ausnutzen, um beliebigen Programmcode auszuführen oder Informationen offenzulegen.

- Link

—

Mon, 19 Feb 2024

[UPDATE] [hoch] Mozilla Firefox und Thunderbird: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu verursachen oder vertrauliche Informationen offenzulegen. Zur erfolgreichen Ausnutzung ist eine Benutzeraktion erforderlich.

- Link

—

Mon, 19 Feb 2024

[UPDATE] [hoch] Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, vertrauliche Informationen offenzulegen oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Mon, 19 Feb 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- Link

—

Mon, 19 Feb 2024

[UPDATE] [hoch] Google Chrome: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Google Chrome ausnutzen, um beliebigen Programmcode auszuführen oder um einen Denial of Service Zustand herbeizuführen.

- Link

—

Mon, 19 Feb 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Mon, 19 Feb 2024

[UPDATE] [hoch] Google Chrome und Microsoft Edge: Schwachstelle ermöglicht Codeausführung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Mon, 19 Feb 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome und Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Mon, 19 Feb 2024

[UPDATE] [hoch] Google Chrome: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- Link

—

Mon, 19 Feb 2024

[UPDATE] [hoch] Mozilla Firefox: Mehrere Schwachstellen

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen, seine Rechte zu erweitern oder einen Phishing-Angriff durchzuführen.

- Link

—

Mon, 19 Feb 2024

[UPDATE] [hoch] Microsoft Edge: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft Edge ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, Informationen falsch darzustellen und nicht spezifizierte Auswirkungen zu verursachen.

- Link

—

Mon, 19 Feb 2024

[UPDATE] [hoch] docker: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Docker ausnutzen, um seine Privilegien zu erhöhen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen oder Dateien zu manipulieren.

- Link

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
2/19/2024	[Amazon Linux 2 : gstreamer1-plugins-bad-free (ALAS-2024-2454)]	critical
2/19/2024	[Amazon Linux 2 : amazon-ssm-agent (ALAS-2024-2458)]	critical
2/19/2024	[Amazon Linux 2 : xorg-x11-server (ALAS-2024-2455)]	critical

Datum	Schwachstelle	Bewertung
2/19/2024	[Amazon Linux AMI : amazon-ssm-agent (ALAS-2024-1920)]	critical
2/19/2024	[Amazon Linux 2 : ghostscript (ALAS-2024-2469)]	critical
2/19/2024	[Amazon Linux 2 : webkitgtk4 (ALAS-2024-2459)]	critical
2/19/2024	[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : NPM IP vulnerability (USN-6643-1)]	critical
2/18/2024	[GLSA-202402-21 : QtNetwork: Multiple Vulnerabilities]	critical
2/19/2024	[Nginx 1.25.x < 1.25.4 Multiple Vulnerabilities]	high
2/19/2024	[Fedora 39 : caddy (2024-22b915e51a)]	high
2/19/2024	[Fedora 39 : bind / bind-dyndb-ldap (2024-21310568fa)]	high
2/19/2024	[Fedora 39 : dnsmasq (2024-e24211eff0)]	high
2/19/2024	[QNAP QTS / QuTS hero Multiple Vulnerabilities in QTS, QuTS hero (QSA-23-38)]	high
2/19/2024	[nginx 1.25.x < 1.25.4 DoS]	high
2/19/2024	[Oracle Linux 7 : python-pillow (ELSA-2024-0857)]	high
2/19/2024	[Debian dla-3735 : golang-github-opencontainers-runc-dev - security update]	high
2/19/2024	[Amazon Linux 2 : woodstox-core (ALAS-2024-2463)]	high
2/19/2024	[Amazon Linux 2 : xstream (ALAS-2024-2464)]	high
2/19/2024	[Amazon Linux 2 : nss-util (ALAS-2024-2470)]	high
2/19/2024	[Amazon Linux 2 : postgresql (ALAS-2024-2462)]	high
2/19/2024	[Amazon Linux 2 : kernel (ALAS-2024-2453)]	high
2/19/2024	[Amazon Linux 2 : edk2 (ALAS-2024-2465)]	high
2/19/2024	[Amazon Linux 2 : unbound (ALAS-2024-2467)]	high
2/19/2024	[Amazon Linux AMI : kernel (ALAS-2024-1919)]	high
2/19/2024	[Amazon Linux 2 : ipa (ALAS-2024-2457)]	high
2/19/2024	[Amazon Linux AMI : php72 (ALAS-2024-1921)]	high
2/19/2024	[Amazon Linux 2 : jtidy (ALAS-2024-2461)]	high
2/19/2024	[Amazon Linux 2 : liblouis (ALAS-2024-2471)]	high

Datum	Schwachstelle	Bewertung
2/19/2024	[Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS / 23.10 : LibTIFF vulnerabilities (USN-6644-1)]	high
2/19/2024	[Ubuntu 20.04 LTS : Bind vulnerabilities (USN-6642-1)]	high
2/19/2024	[RHEL 8 : gimp:2.8 (RHSA-2024:0861)]	high
2/19/2024	[RHEL 8 : gimp:2.8 (RHSA-2024:0863)]	high
2/19/2024	[RHEL 8 : gimp:2.8 (RHSA-2024:0862)]	high
2/18/2024	[Debian dsa-5626 : pdns-recursor - security update]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Mon, 19 Feb 2024

Microsoft Windows Defender / Backdoor_JS.Relvelshe.A Detection / Mitigation Bypass

Back in 2022, the researcher released a proof of concept to bypass the Backdoor:JS/Relvelshe.A detection in Windows Defender but it no longer works as it was mitigated. However, adding a simple javascript try catch error statement and eval’ing the hex string, it executes as of the time of this post.

- Link

—

” “Mon, 19 Feb 2024

Microsoft Windows Defender / Trojan.Win32/Powessere.G VBScript Detection Bypass

This is additional research regarding a mitigation bypass in Windows Defender. Back in 2022, the researcher disclosed how it could be easily bypassed by passing an extra path traversal when referencing mshtml but that issue has since been mitigated. However, the researcher discovered using multiple commas can also be used to achieve the bypass. This issue was addressed. The fix was short lived as the researcher found yet another third trivial bypass. Previously, the researcher disclosed 3 bypasses using rundll32 javascript, but this example leverages the VBSCRIPT and ActiveX engines.

- Link

—

” “Mon, 19 Feb 2024

InstantCMS 2.16.1 Cross Site Scripting

InstantCMS version 2.16.1 suffers from a persistent cross site scripting vulnerability that appears to require administrative access.

- Link

—

” “Mon, 19 Feb 2024

SureMDM On-Premise CAPTCHA Bypass / User Enumeration

SureMDM On-Premise versions prior to 6.31 suffer from CAPTCHA bypass and user enumeration vulnerabilities.

- Link

—

” “Mon, 19 Feb 2024

Online Library Management System 3 Password Reset

Online Library Management System version 3 suffers from a password reset vulnerability due to a logic flaw of allowing the same email address to be set for multiple users.

- Link

—

” “Mon, 19 Feb 2024

Employee Management System 1.0 SQL Injection

Employee Management System version 1.0 suffers from a remote SQL injection vulnerability. Original discovery of this finding is attributed to Ozlem Balci in January of 2024.

- Link

—

” “Mon, 19 Feb 2024

Chrome chrome.pageCapture.saveAsMHTML() Extension API Blocked Origin Bypass

Chrome has an issue where the chrome.pageCapture.saveAsMHTML() extension API can be used on blocked origins due to a racy access check.

- Link

—

” “Mon, 19 Feb 2024

WonderCMS 4.3.2 Cross Site Scripting / Remote Code Execution

WonderCMS version 4.3.2 remote exploit that leverages cross site scripting to achieve remote code execution.

- Link

—

” “Mon, 19 Feb 2024

User Registration And Login And User Management System 3.1 SQL Injection

User Registration and Login and User Management System version 3.1 suffers from a remote SQL injection vulnerability.

- Link

—

” “Mon, 19 Feb 2024

Microsoft Windows Defender / Detection Bypass Part 3

This is additional research regarding a mitigation bypass in Windows Defender. Back in 2022, the researcher disclosed how it could be easily bypassed by passing an extra path traversal when referencing mshtml but that issue has since been mitigated. However, the researcher discovered using multiple commas can also be used to achieve the bypass. This issue was addressed. The fix was short lived as the researcher has found yet another third trivial bypass.

- Link

—

” “Mon, 19 Feb 2024

JFrog Artifactory SQL Injection

JFrog Artifactory versions prior to 7.25.4 suffer from a remote blind SQL injection vulnerability.

- Link

—

” “Thu, 15 Feb 2024

Metabase 0.46.6 Remote Code Execution

Metabase version 0.46.6 pre-authentication remote code execution exploit.

- Link

—

” “Thu, 15 Feb 2024

DS Wireless Communication Code Execution

Proof of concept code for a flaw in DS Wireless Communication (DWC) with DWC_VERSION_3 and DWC_VERSION_11 that allows remote attackers to execute arbitrary code on a game-playing client’s machine via a modified GPCM message.

- Link

—

” “Wed, 14 Feb 2024

Statamic CMS Cross Site Scripting

Statamic CMS versions prior to 4.46.0 and 3.4.17 suffer from multiple persistent cross site scripting vulnerabilities.

- Link

—

” “Wed, 14 Feb 2024

Adapt CMS 3.0.3 Cross Site Scripting / Shell Upload

Adapt CMS version 3.0.3 suffers from persistent cross site scripting and remote shell upload vulnerabilities.

- Link

—

” “Tue, 13 Feb 2024

XoopsCore25 2.5.11 Cross Site Scripting

XoopsCore25 version 2.5.11 suffers from a cross site scripting vulnerability.

- Link

—

” “Tue, 13 Feb 2024

ManageEngine ADManager Plus Recovery Password Disclosure

ManageEngine ADManager Plus versions prior to build 7183 suffers from a recovery password disclosure vulnerability.

- Link

—

” “Tue, 13 Feb 2024

Splunk 9.0.4 Information Disclosure

Splunk version 9.0.4 suffers from an information disclosure vulnerability.

- Link

—

” “Mon, 12 Feb 2024

LaborOfficeFree 19.10 MySQL Root Password Calculator

LaborOfficeFree installs a MySQL instance that runs as SYSTEM and calculates the MySQL root password based on two constants. Each time the program needs to connect to MySQL as root, it employs the reverse algorithm to calculate the root password. This issue has been tested on version 19.10 exclusively, but allegedly, versions prior to 19.10 are also vulnerable.

- Link

—

” “Mon, 12 Feb 2024

Windows Defender Detection Mitigation Bypass

This is additional research regarding a mitigation bypass in Windows Defender. Back in 2022, the researcher disclosed how it could be easily bypassed by passing an extra path traversal when referencing mshtml but that issue has since been mitigated. However, the researcher discovered using multiple commas can also be used to achieve the bypass.

- Link

—

” “Mon, 12 Feb 2024

WyreStorm Apollo VX20 Incorrect Access Control

An issue was discovered on WyreStorm Apollo VX20 versions prior to 1.3.58. Remote attackers can restart the device via a /device/reboot HTTP GET request.

- Link

—

” “Mon, 12 Feb 2024

WyreStorm Apollo VX20 Credential Disclosure

WyreStorm Apollo VX20 versions prior to 1.3.58 suffer from a cleartext credential disclosure vulnerability when accessing /device/config with an HTTP GET.

- Link

—

” “Mon, 12 Feb 2024

WyreStorm Apollo VX20 Account Enumeration

An issue was discovered on WyreStorm Apollo VX20 devices prior to version 1.3.58. The TELNET service prompts for a password only after a valid username is entered. Attackers who can reach the Apollo VX20 Telnet service can determine valid accounts allowing for account discovery.

- Link

—

” “Mon, 12 Feb 2024

Enpass Desktop Application 6.9.2 HTML Injection

Enpass Desktop Application version 6.9.2 suffers from an html injection vulnerability.

- Link

—

” “Mon, 12 Feb 2024

Complaint Management System 2.0 SQL Injection

Complaint Management System version 2.0 suffers from multiple remote SQL injection vulnerabilities.

- Link

—

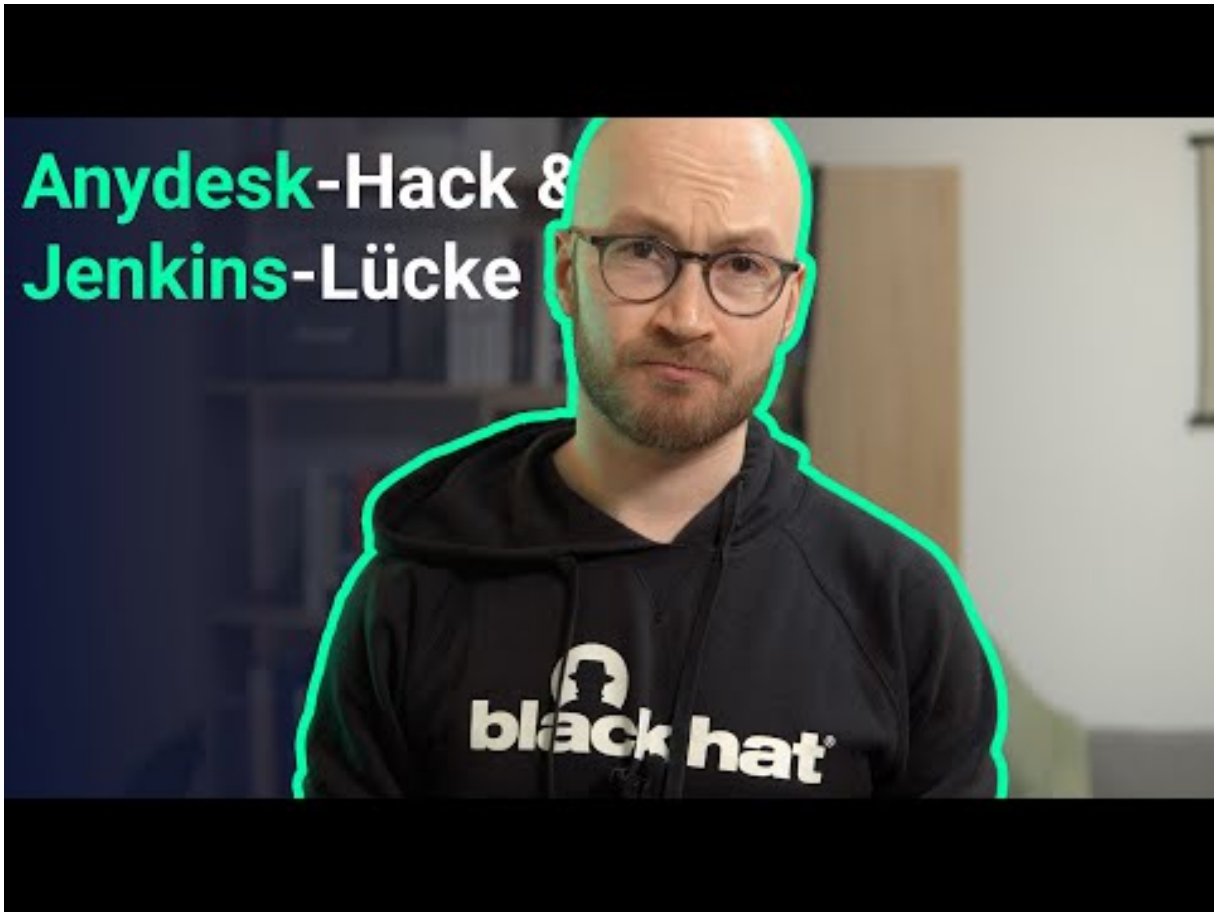
”

4.2 0-Days der letzten 5 Tage

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 AnyDesk-Hack und Jenkins-Lücke



Zum Youtube Video

6 Cyberangriffe: (Feb)

Datum	Opfer	Land	Information
2024-02-18	Evangelische Landeskirche Hannovers	[DEU]	Link
2024-02-15	PSI	[DEU]	Link
2024-02-14	JCT600	[GBR]	Link
2024-02-13	Aztech Global	[SGP]	Link
2024-02-13	Varta	[DEU]	Link
2024-02-13	Coeur d'Alene	[USA]	Link
2024-02-13	Act21	[FRA]	Link
2024-02-13	School District 67	[CAN]	Link
2024-02-12	MSH International	[CAN]	Link
2024-02-11	Centre hospitalier d'Armentières	[FRA]	Link
2024-02-11	Hipocrate Information System (HIS)	[ROU]	Link
2024-02-11	Clinique privée La Colline (groupe Hirslanden)	[CHE]	Link
2024-02-11	Consulting Radiologists Ltd.	[USA]	Link
2024-02-09	Office of Colorado State Public Defender	[USA]	Link
2024-02-07	Université de Central Missouri	[USA]	Link
2024-02-07	SouthState Bank	[USA]	Link
2024-02-07	Commune de Petersberg	[DEU]	Link
2024-02-07	Krankenhaus Lindenbrunn	[DEU]	Link
2024-02-06	Commune de Kalmar	[SWE]	Link
2024-02-06	Advania	[SWE]	Link
2024-02-06	Onclusive	[GBR]	Link
2024-02-06	Kind	[DEU]	Link
2024-02-05	Prudential Financial, Inc.	[USA]	Link
2024-02-05	Central Arkansas Library System (CALS)	[USA]	Link
2024-02-04	Northern Light Health	[USA]	Link

Datum	Opfer	Land	Information
2024-02-04	Middletown Area School District	[USA]	Link
2024-02-02	Germantown	[USA]	Link
2024-02-02	Université de Reykjavík	[ISL]	Link
2024-02-02	Hôpital de la Trinité à Lippstadt, ainsi que les cliniques associées à Erwitte et Geseke.	[DEU]	Link
2024-02-02	Mairie de Korneuburg	[AUT]	Link
2024-02-02	Welch's	[USA]	Link
2024-02-01	Landkreis Kelheim	[DEU]	Link
2024-02-01	Groton Public Schools	[USA]	Link
2024-02-01	Diagnostic Medical Systems Group (DMS Group)	[FRA]	Link
2024-02-01	Ajuntament de Sant Antoni de Portmany	[ESP]	Link
2024-02-01	Minnesota State University-Moorhead (MSUM)	[USA]	Link

7 Ransomware-Erpressungen: (Feb)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-02-19	[loransrl]	qilin	Link
2024-02-19	[soco.be]	lockbit3	Link
2024-02-19	[se.com]	cactus	Link
2024-02-19	[First Professional Services]	bianlian	Link
2024-02-19	[aivi.it]	trisec	Link
2024-02-19	[ki.se]	trisec	Link
2024-02-18	[Compression Leasing Services]	dragonforce	Link
2024-02-18	[Westward 360]	dragonforce	Link
2024-02-08	[aeromechinc.com]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-02-18	[carlfischer.com]	lockbit3	Link
2024-02-17	[Bimbo Bakeries]	medusa	Link
2024-02-07	[bucher-strauss.ch]	lockbit3	Link
2024-02-16	[delia.pl]	stormous	Link
2024-02-14	[bombaygrills.com]	stormous	Link
2024-02-14	[calcomp.co.th]	stormous	Link
2024-02-02	[Abelsantosyasoc.com.ar]	stormous	Link
2024-02-18	[VSP Dental]	alphv	Link
2024-02-17	[Greater Napanee]	hunters	Link
2024-02-17	[Tiete Automobile]	hunters	Link
2024-02-17	[Voice Technologies]	hunters	Link
2024-02-17	[Aftrp]	hunters	Link
2024-02-17	[Chicago Zoological Society]	hunters	Link
2024-02-17	[BS&B Safety Systems L.L.C]	hunters	Link
2024-02-17	[Wapiti Energy]	hunters	Link
2024-02-17	[PSI]	hunters	Link
2024-02-17	[CP Communications]	hunters	Link
2024-02-16	[Prudential Financial]	alphv	Link
2024-02-16	[LoanDepot]	alphv	Link
2024-02-16	[www.cogans.ie]	trisec	Link
2024-02-16	[The Chas. E. Phipps]	medusa	Link
2024-02-16	[BRONSTEIN-CARMONA.COM]	clop	Link
2024-02-14	[davidsbridal.com]	werewolves	Link
2024-02-16	[Réseau Ribé]	hunters	Link
2024-02-16	[BRAM Auto Group]	akira	Link
2024-02-16	[etisalat.ae]	lockbit3	Link
2024-02-16	[theclosingagent.com]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-02-16	[spaldingssd.com]	lockbit3	Link
2024-02-16	[tormetal.cl]	lockbit3	Link
2024-02-16	[Concello de Teo]	hunters	Link
2024-02-16	[pacifica.co.uk]	blackbasta	Link
2024-02-16	[Ribe-Groupe]	hunters	Link
2024-02-16	[Griffin Dewatering]	hunters	Link
2024-02-15	[Dobrowski Stafford & Pierce]	bianlian	Link
2024-02-15	[LD Davis]	play	Link
2024-02-15	[von Hagen]	play	Link
2024-02-15	[Norman, Fox]	play	Link
2024-02-15	[HR Ewell & Hy-tec]	play	Link
2024-02-15	[Mechanical Reps]	play	Link
2024-02-15	[Onclusive]	play	Link
2024-02-15	[MeerServices]	play	Link
2024-02-15	[DuBose Strapping]	play	Link
2024-02-15	[SilverLining]	play	Link
2024-02-15	[Schuster Trucking Company]	hunters	Link
2024-02-15	[Asam]	akira	Link
2024-02-15	[Advantage Orthopedic & Sports Medicine Clinic]	bianlian	Link
2024-02-12	[Rush Energy Services Inc [Time’s up]]	alphv	Link
2024-02-13	[Hawbaker Engineering]	snatch	Link
2024-02-15	[ASP BasilicataASM MateraIRCCS CROB]	rhysida	Link
2024-02-15	[champion.com.co]	lockbit3	Link
2024-02-15	[coreengg.com]	lockbit3	Link
2024-02-15	[sitrack.com]	lockbit3	Link
2024-02-15	[hatsinteriors.com]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-02-15	[pradiergranulats.fr]	lockbit3	Link
2024-02-15	[centralepaysanne.lu]	lockbit3	Link
2024-02-15	[ASA Electronics [2.7 TB]]	alphv	Link
2024-02-14	[studiogalbusera.com]	lockbit3	Link
2024-02-14	[Nekoosa School District]	akira	Link
2024-02-14	[BM Catalysts bmcatalysts.co.uk]	mydata	Link
2024-02-14	[vanwingerden.com]	abyss	Link
2024-02-14	[KALEEDS]	qilin	Link
2024-02-14	[conseguros]	qilin	Link
2024-02-14	[kabat.pl]	lockbit3	Link
2024-02-13	[Sindicato de Enfermería (SATSE)]	hunters	Link
2024-02-13	[wsnelson.com]	lockbit3	Link
2024-02-13	[fultoncountyga.gov]	lockbit3	Link
2024-02-14	[UNIFER]	8base	Link
2024-02-14	[Institutional Casework, Inc]	8base	Link
2024-02-14	[ATB SA Ingénieurs-conseils SIA]	8base	Link
2024-02-14	[mmiculinary.com]	lockbit3	Link
2024-02-12	[adioscancer.com]	lockbit3	Link
2024-02-14	[giraud]	qilin	Link
2024-02-13	[rajawali.com]	lockbit3	Link
2024-02-13	[motilaloswal.com]	lockbit3	Link
2024-02-13	[barberemerson.com]	blackbasta	Link
2024-02-13	[ffppkg.co.uk]	blackbasta	Link
2024-02-13	[patriziapepe.com]	blackbasta	Link
2024-02-13	[btl.info]	blackbasta	Link
2024-02-13	[globalrescue.com]	blackbasta	Link
2024-02-13	[ssmnlaw.com]	blackbasta	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-02-13	[leonardssyrups.com]	blackbasta	Link
2024-02-13	[ROOSENS BÉTONS]	qilin	Link
2024-02-13	[universalservicesms.com]	lockbit3	Link
2024-02-13	[Communication Federal Credit Union]	hunters	Link
2024-02-13	[doprastav.sk]	lockbit3	Link
2024-02-13	[The Source]	alphv	Link
2024-02-13	[ArcisGolf]	alphv	Link
2024-02-13	[Trans-Northern Pipelines]	alphv	Link
2024-02-13	[Herrs]	alphv	Link
2024-02-13	[Procopio]	alphv	Link
2024-02-13	[New Indy Containerboard]	alphv	Link
2024-02-13	[auruminstitute.org]	lockbit3	Link
2024-02-10	[SOPEM]	hunters	Link
2024-02-13	[Satse]	hunters	Link
2024-02-13	[Sanok Rubber CompanySpólka Akcyjna]	akira	Link
2024-02-12	[garonproducts.com]	threeam	Link
2024-02-07	[tecasrl.it]	lockbit3	Link
2024-02-12	[Antunovich Associates]	blacksuit	Link
2024-02-12	[DHX–Dependable Hawaiian Express]	knight	Link
2024-02-12	[Forgepresion.com]	cloak	Link
2024-02-12	[Rush Energy Services Inc [You have 48 hours]]	alphv	Link
2024-02-12	[SERCIDE]	alphv	Link
2024-02-12	[Lower Valley Energy, Inc]	alphv	Link
2024-02-12	[Modern Kitchens]	medusa	Link
2024-02-12	[vhprimary.com]	lockbit3	Link
2024-02-12	[germaintoiture.fr]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-02-12	[Disaronno International]	meow	Link
2024-02-12	[Allmetal Inc.]	meow	Link
2024-02-12	[Freedom Munitions]	meow	Link
2024-02-12	[Arlington Perinatal Associates]	meow	Link
2024-02-12	[jacksonvillebeach.org]	lockbit3	Link
2024-02-12	[robs.org]	lockbit3	Link
2024-02-12	[parkhomeassist.co.uk]	lockbit3	Link
2024-02-12	[grotonschools.org]	lockbit3	Link
2024-02-12	[isspol.gov]	lockbit3	Link
2024-02-12	[lyon.co.uk]	lockbit3	Link
2024-02-12	[dienerprecisionpumps.com]	lockbit3	Link
2024-02-12	[envie.org]	lockbit3	Link
2024-02-12	[sealco-leb.com]	lockbit3	Link
2024-02-12	[camarotto.it]	lockbit3	Link
2024-02-12	[paltertonprimary.co.uk]	lockbit3	Link
2024-02-12	[fidcornelis.be]	lockbit3	Link
2024-02-12	[plexustelerad.com]	lockbit3	Link
2024-02-12	[cabc.com.ar]	lockbit3	Link
2024-02-12	[textiles.org.tw]	lockbit3	Link
2024-02-12	[silverairways.com]	lockbit3	Link
2024-02-12	[Kreyenhop & Kluge]	hunters	Link
2024-02-12	[Kadac Australia]	medusa	Link
2024-02-11	[Amoskeag Network Consulting Group LLC]	medusa	Link
2024-02-11	[lacolline-skincare.com]	lockbit3	Link
2024-02-10	[Upper Merion Township]	qilin	Link
2024-02-10	[YKP LTDA]	ransomhub	Link
2024-02-10	[Village of Skokie]	hunters	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-02-10	[Lancaster County Sheriff's Office]	hunters	Link
2024-02-10	[Nastech]	hunters	Link
2024-02-10	[Benchmark Management Group]	hunters	Link
2024-02-10	[SOPEM Tunisie]	hunters	Link
2024-02-10	[Impact Energy Services]	hunters	Link
2024-02-10	[Groupe Goyette]	hunters	Link
2024-02-10	[Dalmahoy Hotel & Country Club]	hunters	Link
2024-02-10	[Carespring Health Care]	hunters	Link
2024-02-10	[Avianor Aircraft]	hunters	Link
2024-02-10	[mranet.org]	abyss	Link
2024-02-10	[aisg-online.com]	lockbit3	Link
2024-02-10	[maddockhenson]	alphv	Link
2024-02-10	[verdimed.es]	lockbit3	Link
2024-02-10	[Pacific American Fish Company Inc.]	incransom	Link
2024-02-09	[water.cc]	lockbit3	Link
2024-02-09	[CTSI]	bianlian	Link
2024-02-09	[J.P. Original]	bianlian	Link
2024-02-09	[TechNet Kronoberg AB]	bianlian	Link
2024-02-09	[Capozzi Adler, P.C.]	bianlian	Link
2024-02-09	[Drost Kivlahan McMahon & O'Connor LLC]	bianlian	Link
2024-02-09	[Grace Lutheran Foundation]	alphv	Link
2024-02-09	[ZGEO]	qilin	Link
2024-02-09	[alfiras.com]	lockbit3	Link
2024-02-09	[wannago.cloud]	qilin	Link
2024-02-09	[grupomoraval.com]	lockbit3	Link
2024-02-09	[cdtmedicus.pl]	lockbit3	Link
2024-02-09	[soken-ce.co.jp]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-02-09	[maximumresearch.com]	lockbit3	Link
2024-02-09	[indoramaventures.com]	lockbit3	Link
2024-02-09	[willislease.com]	blackbasta	Link
2024-02-09	[northseayachtsupport.nl]	lockbit3	Link
2024-02-09	[seymourct.org]	lockbit3	Link
2024-02-09	[bsaarchitects.com]	lockbit3	Link
2024-02-09	[moneyadvicetrust.org]	lockbit3	Link
2024-02-09	[posen.com]	abyss	Link
2024-02-09	[macqueeneq.com]	lockbit3	Link
2024-02-09	[parksite.com]	cactus	Link
2024-02-07	[galbusera.it]	lockbit3	Link
2024-02-08	[Ducont]	hunters	Link
2024-02-08	[perkinsmfg.com]	lockbit3	Link
2024-02-08	[originalfootwear.com]	lockbit3	Link
2024-02-08	[Jewish Home Lifecare]	alphv	Link
2024-02-08	[Distecna]	akira	Link
2024-02-07	[Western Municipal Construction]	blacksuit	Link
2024-02-07	[Southwest Binding & Laminating]	blacksuit	Link
2024-02-07	[TeraGo]	akira	Link
2024-02-07	[transaxle.com]	abyss	Link
2024-02-07	[Anderco PTE LTD]	8base	Link
2024-02-07	[Tetrosyl Group Limited]	8base	Link
2024-02-07	[Therme Laa Hotel and Silent Spa]	8base	Link
2024-02-07	[Karl Rieker GmbH and Co. KG]	8base	Link
2024-02-07	[YRW Limited - Chartered Accountants]	8base	Link
2024-02-06	[axsbolivia.com]	lockbit3	Link
2024-02-06	[vimarequipment.com]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-02-06	[deltron.com]	abyss	Link
2024-02-06	[B&B Electric Inc]	bianlian	Link
2024-02-06	[AVer Information]	akira	Link
2024-02-06	[Celeste]	akira	Link
2024-02-06	[ArpuPlus]	medusa	Link
2024-02-06	[gocco.com]	cactus	Link
2024-02-06	[spbglobal.com]	cactus	Link
2024-02-05	[Modern Kitchens]	play	Link
2024-02-05	[Greenwich Leisure]	play	Link
2024-02-05	[Ready Mixed Concrete]	play	Link
2024-02-05	[Northeastern Sheet Metal]	play	Link
2024-02-05	[Hannon Transport]	play	Link
2024-02-05	[McMillan Pazdan Smith]	play	Link
2024-02-05	[Mason Construction]	play	Link
2024-02-05	[Albert Bartlett]	play	Link
2024-02-05	[Perry-McCall Construction]	play	Link
2024-02-05	[Virgin Islands Lottery]	play	Link
2024-02-05	[Premier Facility Management]	play	Link
2024-02-05	[Douglas County Libraries]	play	Link
2024-02-05	[Leaders Staffing]	play	Link
2024-02-06	[asecos.com]	blackbasta	Link
2024-02-05	[GRUPO SCA Release of all data)]	knight	Link
2024-02-05	[themisbourne.co.uk]	lockbit3	Link
2024-02-05	[Vail-Summit Orthopaedics & Neurosurgery (VSON)]	alphv	Link
2024-02-05	[hutchpaving.com]	lockbit3	Link
2024-02-05	[davis-french-associates.co.uk]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-02-05	[Campaign for Tobacco-Free Kids]	blacksuit	Link
2024-02-05	[VCS Observation]	akira	Link
2024-02-05	[noe.wifi.at]	lockbit3	Link
2024-02-05	[ksa-architecture.com]	lockbit3	Link
2024-02-05	[GRTC Transit System]	bianlian	Link
2024-02-05	[semesco.com]	lockbit3	Link
2024-02-05	[ultraflexx.com]	lockbit3	Link
2024-02-05	[tgestiona.br]	lockbit3	Link
2024-02-05	[philogen.com]	lockbit3	Link
2024-02-05	[prima.com]	lockbit3	Link
2024-02-05	[logtainer.com]	lockbit3	Link
2024-02-05	[portline.pt]	lockbit3	Link
2024-02-04	[DOD contractors you are welcome in our chat.]	donutleaks	Link
2024-02-04	[cxm.com]	lockbit3	Link
2024-02-04	[Cole, Cole, Easley & Sciba]	bianlian	Link
2024-02-04	[Commonwealth Sign]	qilin	Link
2024-02-04	[FEPCO Zona Franca SAS]	knight	Link
2024-02-03	[pbwtulsa.com]	lockbit3	Link
2024-02-02	[Digitel Venezuela]	medusa	Link
2024-02-02	[Chaney, Couch, Callaway, Carter & Associates Family Dentistry.]	bianlian	Link
2024-02-02	[manitou-group.com]	lockbit3	Link
2024-02-02	[AbelSantosyAsociados]	knight	Link
2024-02-02	[lexcaribbean.com]	lockbit3	Link
2024-02-02	[Law Office of Michael H Joseph]	bianlian	Link
2024-02-02	[Tandem]	bianlian	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-02-02	[Innovex Downhole Solutions]	play	Link
2024-02-01	[CityDfDefiance(Disclosure of all)]	knight	Link
2024-02-01	[DIROX LTDA (Vietnã)]	knight	Link
2024-02-01	[etsolutions.com.mx]	threeam	Link
2024-02-01	[gatesshields.com]	lockbit3	Link
2024-02-01	[manchesterfertility.com]	lockbit3	Link
2024-02-01	[stemcor.com]	lockbit3	Link
2024-02-01	[Borah Goldstein Altschuler Nahins & Goidel]	akira	Link
2024-02-01	[dms-imaging]	cuba	Link
2024-02-01	[bandcllp.com]	lockbit3	Link
2024-02-01	[taloninternational.com]	lockbit3	Link
2024-02-01	[Southwark Council]	meow	Link
2024-02-01	[Robert D. Clements Jr Law Group, LLLP]	bianlian	Link
2024-02-01	[CNPC Peru S.A.]	rhysida	Link
2024-02-01	[Primeimaging database for sale]	everest	Link

8 Quellen

8.1 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) Exploit - packetstormsecurity.com
8) 0-Day - https://www.zerodayinitiative.com/rss/published/
9) Die Hacks der Woche - https://martinhaunschmid.com/videos

9 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.