Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240328

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

Google Chrome: Kritische Schwachstelle bedroht Browser-Nutzer

In Chrome haben Googles Entwickler sieben Sicherheitslücken abgedichtet. Mindestens eine davon stellt ein kritisches Risiko dar.

- Link

—

Loadbalancer: Sicherheitslücken in Loadmaster von Progress/Kemp

In der Loadbalancer-Software Loadmaster von Progress/Kemp klaffen Sicherheitslücken, durch die Angreifer etwa Befehle einschleusen können.

- Link

—

Sicherheitslücken in Microsofts WiX-Installer-Toolset gestopft

Das quelloffene WiX-Installer-Toolset von Microsoft hat zwei Sicherheitslücken. Die dichten aktualisierte Versionen ab.

- Link

—

Firefox: Notfall-Update schließt kritische Sicherheitslücken

Die Mozilla-Entwickler haben zwei kritische Sicherheitslücken mit dem Update auf Firefox 124.0.1 und Firefox ESR 115.9.1 geschlossen.

- Link

—

Kritische Sicherheitslücke in FortiClientEMS wird angegriffen

Eine kritische Schwachstelle in FortiClientEMS wird inzwischen aktiv angegriffen. Zudem ist ein Proof-of-Concept-Exploit öffentlich geworden.

- Link

—

Microsoft schließt Sicherheitslücke in Xbox-Gaming-Dienst – nach Hickhack

Microsoft hat ein Sicherheitsleck im Xbox Gaming Service abgedichtet. Dem ging jedoch eine Diskussion voraus.

- Link

—

IBM-Software: Angreifer können Systeme mit Schadcode kompromittieren

Es sind wichtige Sicherheitsupdates für IBM App Connect Enterprise und InfoSphere Information Server erschienen.

- Link

—

Lücken in Ruby-Gems ermöglichen Codeschmuggel und Datenleck

Angreifer könnten eigenen Code im Kontext eines Ruby-Programms ausführen. Nutzer der RDoc- und StringIO-Gems sollten aktualisierte Versionen einspielen.

- Link

—

Attacken auf Ivanti Standalone Sentry und Neurons möglich

Angreifer können an kritische Sicherheitslücken in Ivanti-Software ansetzen. Sicherheitsupdates sind verfügbar.

- Link

—

Sicherheitsupdates für Atlassian Bamboo, Bitbucket, Confluence und Jira

Atlassian behandelt 25 Sicherheitslücken in Bamboo, Bitbucket, Confluence und Jira. Eine davon gilt als kritisch.

- 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-2023-39143	0.939910000	0.990970000	Link
CVE-2023-38646	0.916640000	0.988470000	Link
CVE-2023-38035	0.972370000	0.998290000	Link
CVE-2023-36845	0.966640000	0.996190000	Link
CVE-2023-35082	0.932380000	0.990180000	Link
CVE-2023-30625	0.948330000	0.992260000	Link
CVE-2023-26469	0.943740000	0.991530000	Link
CVE-2023-25194	0.968970000	0.996900000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Wed, 27 Mar 2024

[UPDATE] [hoch] http/2 Implementierungen: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in verschiedenen http/2 Implementierungen ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Wed, 27 Mar 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

—

Wed, 27 Mar 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, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen oder einen nicht spezifizierten Angriff durchzuführen.

- Link

—

Wed, 27 Mar 2024

[UPDATE] [hoch] Mozilla Firefox, Firefox ESR 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 herbeizuführen, vertrauliche Informationen offenzulegen, seine Privilegien zu erweitern oder einen nicht spezifizierten Angriff durchzuführen.

- Link

—

Wed, 27 Mar 2024

[UPDATE] [hoch] Mozilla Firefox und Firefox ESR: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox und Mozilla Firefox ESR ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 27 Mar 2024

[NEU] [hoch] Python: Schwachstelle ermöglicht Codeausführung

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

- Link

—

Wed, 27 Mar 2024

[NEU] [hoch] Hitachi Energy RTU500: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Hitachi Energy RTU500 ausnutzen, um einen Denial of Service Angriff durchzuführen oder vertrauliche Informationen offenlegen.

- Link

—

Wed, 27 Mar 2024

[UPDATE] [hoch] Ruby: Schwachstelle ermöglicht Manipulation von Dateien

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Ruby ausnutzen, um Dateien zu manipulieren.

- Link

—

Wed, 27 Mar 2024

[UPDATE] [hoch] Node.js: Mehrere Schwachstellen

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

—

Wed, 27 Mar 2024

[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Privilegieneskalation

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Wed, 27 Mar 2024

[UPDATE] [kritisch] Node.js: Mehrere Schwachstellen

Ein entfernter, authentisierter oder anonymer Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um beliebigen Programmcode auszuführen, Informationen offenzulegen, einen Denial of Service Zustand herbeizuführen oder Sicherheitsvorkehrungen zu umgehen.

- Link

—

Wed, 27 Mar 2024

[UPDATE] [hoch] LibreOffice: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in LibreOffice ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Wed, 27 Mar 2024

[UPDATE] [hoch] Node.js: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren oder seine Privilegien zu erweitern.

- Link

—

Wed, 27 Mar 2024

[UPDATE] [hoch] PostgreSQL JDBC Driver: Schwachstelle ermöglicht SQL-Injection

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in PostgreSQL JDBC Driver ausnutzen, um eine SQL-Injection durchzuführen.

- Link

—

Wed, 27 Mar 2024

[UPDATE] [hoch] Squid: Schwachstelle ermöglicht Denial of Service

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Squid ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Wed, 27 Mar 2024

[UPDATE] [hoch] Microsoft Visual Studio 2022: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Microsoft Visual Studio 2022, Microsoft Visual Studio Code und Microsoft .NET Framework ausnutzen, um einen Denial of Service Angriff durchzuführen oder seine Privilegien zu erweitern.

- Link

—

Wed, 27 Mar 2024

[NEU] [hoch] Google Chrome: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

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

- Link

—

Wed, 27 Mar 2024

[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen ermöglichen Privilegieneskalation

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Tue, 26 Mar 2024

[NEU] [hoch] Ubiquiti UniFi: Schwachstelle ermöglicht Privilegieneskalation

Ein entfernter, authentisierter Angreifer kann eine Schwachstelle in Ubiquiti UniFi ausnutzen, um seine Privilegien zu erhöhen.

- Link

—

Tue, 26 Mar 2024

[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

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
3/27/2024	[FreeBSD : emacs – multiple vulnerabilities (f661184a-eb90-11ee-92fc-1c697a616631)]	critical
3/27/2024	[Rocky Linux 8 : postgresql-jdbc (RLSA-2024:1435)]	critical
3/27/2024	[FreeBSD : phpmyfaq – multiple vulnerabilities (8b3be705-eba7-11ee-99b3-589cfc0f81b0)]	high
3/27/2024	[Debian dla-3776 : libnode-dev - security update]	high
3/27/2024	[Oracle Linux 8 : thunderbird (ELSA-2024-1494)]	high
3/27/2024	[Oracle Linux 9 : expat (ELSA-2024-1530)]	high
3/27/2024	[RHEL 9 : kernel-rt (RHSA-2024:1533)]	high
3/27/2024	[RHEL 9 : kernel (RHSA-2024:1532)]	high
3/27/2024	[Rocky Linux 8 : .NET 8.0 (RLSA-2024:1311)]	high
3/27/2024	[Rocky Linux 8 : nodejs:16 (RLSA-2024:1444)]	high
3/27/2024	[Rocky Linux 9 : nodejs:18 (RLSA-2024:1503)]	high
3/27/2024	[Rocky Linux 8 : libreoffice (RLSA-2024:1514)]	high
3/27/2024	[Rocky Linux 8 : go-toolset:rhel8 (RLSA-2024:1472)]	high
3/27/2024	[Rocky Linux 8 : thunderbird (RLSA-2024:1494)]	high
3/27/2024	[Rocky Linux 8 : firefox (RLSA-2024:1484)]	high

Datum	Schwachstelle	Bewertung
3/27/2024	[Rocky Linux 8 : dnsmasq (RLSA-2024:1335)]	high
3/27/2024	[Rocky Linux 8 : .NET 7.0 (RLSA-2024:1308)]	high
3/27/2024	[Rocky Linux 8 : ruby:3.1 (RLSA-2024:1431)]	high
3/27/2024	[Rocky Linux 8 : nodejs:18 (RLSA-2024:1510)]	high
3/27/2024	[Oracle Linux 8 : nodejs:18 (ELSA-2024-1510)]	high
3/27/2024	[Debian dla-3777 : composer - security update]	high
3/27/2024	[Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : curl vulnerabilities (USN-6718-1)]	high
3/27/2024	[Cisco IOS XE Software SD Access Fabric Edge Node DoS (cisco-sa-ios-xe-sda-edge-dos-qZWuWXWG)]	high
3/27/2024	[Splunk Enterprise 9.0.0 < 9.0.9, 9.1.0 < 9.1.4, 9.2.0 < 9.2.1 (SVD-2024-0302)]	high
3/27/2024	[RHEL 8 : dnsmasq (RHSA-2024:1545)]	high
3/27/2024	[RHEL 8 : dnsmasq (RHSA-2024:1544)]	high
3/27/2024	[GitLab 0.0 < 16.8.5 / 16.9 < 16.9.3 / 16.10 < 16.10.1 (CVE-2023-6371)]	high
3/27/2024	[Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : util-linux vulnerability (USN-6719-1)]	high
3/27/2024	[Ubuntu 16.04 LTS / 18.04 LTS : curl vulnerability (USN-6718-2)]	high
3/27/2024	[RHEL 9 : dnsmasq (RHSA-2024:1543)]	high
3/27/2024	[Slackware Linux 15.0 / current curl Multiple Vulnerabilities (SSA:2024-087-01)]	high
3/27/2024	[Splunk Enterprise 9.0.0 < 9.0.9, 9.1.0 < 9.1.4, 9.2.0 < 9.2.1 (SVD-2024-0301)]	high
3/27/2024	[Microsoft Edge (Chromium) < 122.0.2365.113 / 123.0.2420.65 Multiple Vulnerabilities]	high
3/27/2024	[Wireshark 4.2.x < 4.2.4 A Vulnerability (macOS)]	high
3/27/2024	[Wireshark 4.2.x < 4.2.4 A Vulnerability]	high

Datum	Schwachstelle	Bewertung
3/27/2024	[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : unixODBC vulnerability (USN-6715-1)]	high
3/27/2024	[Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel (Intel IoTG) vulnerabilities (USN-6686-5)]	high
3/27/2024	[Fedora 38 : thunderbird (2024-5d080305ab)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Wed, 27 Mar 2024

Sharepoint Dynamic Proxy Generator Remote Command Execution

This Metasploit module exploits two vulnerabilities in Sharepoint 2019 - an authentication bypass as noted in CVE-2023-29357 which was patched in June of 2023 and CVE-2023-24955 which was a remote command execution vulnerability patched in May of 2023. The authentication bypass allows attackers to impersonate the Sharepoint Admin user. This vulnerability stems from the signature validation check used to verify JSON Web Tokens (JWTs) used for OAuth authentication. If the signing algorithm of the user-provided JWT is set to none, SharePoint skips the signature validation step due to a logic flaw in the ReadTokenCore() method. After impersonating the administrator user, the attacker has access to the Sharepoint API and is able to exploit CVE-2023-24955. This authenticated remote command execution vulnerability leverages the impersonated privileged account to replace the /BusinessDataMetadataCatalog/BDCMetadata.bdcm file in the webroot directory with a payload. The payload is then compiled and executed by Sharepoint allowing attackers to remotely execute commands via the API.

- Link

—

” “Wed, 27 Mar 2024

WordPress Bricks Builder Theme 1.9.6 Remote Code Execution

This Metasploit module exploits an unauthenticated remote code execution vulnerability in the Bricks Builder Theme versions 1.9.6 and below for WordPress. The vulnerability allows attackers to execute arbitrary PHP code by leveraging a nonce leakage to bypass authentication and exploit the eval() function usage within the theme. Successful exploitation allows for full control of the affected WordPress site. It is recommended to upgrade to version 1.9.6.1 or higher.

- Link

—

” “Wed, 27 Mar 2024

Artica Proxy Unauthenticated PHP Deserialization

A command injection vulnerability in Artica Proxy appliance versions 4.50 and 4.40 allows remote attackers to run arbitrary commands via an unauthenticated HTTP request. The Artica Proxy administrative web application will deserialize arbitrary PHP objects supplied by unauthenticated users and subsequently enable code execution as the www-data user.

- Link

—

” “Tue, 26 Mar 2024

Bludit 3.13.0 Cross Site Scripting

Bludit version 3.13.0 suffers from a cross site scripting vulnerability.

- Link

—

” “Tue, 26 Mar 2024

Insurance Management System PHP And MySQL 1.0 Cross Site Scripting

Insurance Management System PHP and MySQL version 1.0 suffers from multiple persistent cross site scripting vulnerabilities.

- Link

—

” “Tue, 26 Mar 2024

Craft CMS 4.4.14 Remote Code Execution

Craft CMS version 4.4.14 suffers from an unauthenticated remote code execution vulnerability.

- Link

—

” “Tue, 26 Mar 2024

LimeSurvey Community 5.3.32 Cross Site Scripting

LimeSurvey Community version 5.3.32 suffers from a persistent cross site scripting vulnerability.

- Link

—

” “Tue, 26 Mar 2024

Orange Station 1.0 Shell Upload

Orange Station version 1.0 suffers from a remote shell upload vulnerability.

- Link

—

” “Tue, 26 Mar 2024

Nagios XI 2024R1.01 SQL Injection

Nagios XI versions 2024R1.01 suffers from a remote SQL injection vulnerability.

- Link

—

” “Tue, 26 Mar 2024

MobileShop Master 1.0 SQL Injection

MobileShop Master version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Tue, 26 Mar 2024

LBT-T300-mini1 Buffer Overflow

LBT-T300-mini1 suffers from a remote buffer overflow vulnerability.

- Link

—

” “Fri, 22 Mar 2024

Win32.STOP.Ransomware (Smokeloader) MVID-2024-0676 Remote Code Execution

Win32.STOP.Ransomware (smokeloader) malware suffers from both local and remote code execution vulnerabilities. The remote code execution can be achieved by leveraging a man-in-the-middle attack.

- Link

—

” “Fri, 22 Mar 2024

Task Management System 1.0 SQL Injection

Task Management System version 1.0 suffers from multiple remote SQL injection vulnerabilities.

- Link

—

” “Thu, 21 Mar 2024

OpenNMS Horizon 31.0.7 Remote Command Execution

This Metasploit module exploits built-in functionality in OpenNMS Horizon in order to execute arbitrary commands as the opennms user. For versions 32.0.2 and higher, this module requires valid credentials for a user with ROLE_FILESYSTEM_EDITOR privileges and either ROLE_ADMIN or ROLE_REST. For versions 32.0.1 and lower, credentials are required for a user with ROLE_FILESYSTEM_EDITOR, ROLE_REST, and/or ROLE_ADMIN privileges. In that case, the module will automatically escalate privileges via CVE-2023-40315 or CVE-2023-0872 if necessary. This module has been successfully tested against OpenNMS version 31.0.7.

- Link

—

” “Thu, 21 Mar 2024

Xbox GamingService Arbitrary Folder Move

Proof of concept exploit for an arbitrary folder move issue in the GamingService component of Xbox.

- Link

—

” “Wed, 20 Mar 2024

Lektor Static CMS 3.3.10 Arbitrary File Upload / Remote Code Execution

Lektor Static CMS version 3.3.10 suffers from an arbitrary file upload vulnerability that can be leveraged to achieve remote code execution.

- Link

—

” “Wed, 20 Mar 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

—

” “Wed, 20 Mar 2024

Blood Bank 1.0 SQL Injection

Blood Bank version 1.0 suffers from suffers from a remote SQL injection vulnerability. Original discovery of SQL injection in this version is attributed to Nitin Sharma in October of 2021.

- Link

—

” “Wed, 20 Mar 2024

Simple Task List 1.0 SQL Injection

Simple Task List version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Wed, 20 Mar 2024

Teacher Subject Allocation Management System 1.0 SQL Injection

Teacher Subject Allocation Management System version 1.0 suffers from a remote SQL injection vulnerability.

- Link

—

” “Wed, 20 Mar 2024

Hitachi NAS SMU 14.8.7825 Information Disclosure

Hitachi NAS (HNAS) System Management Unit (SMU) version 14.8.7825 suffers from an information disclosure vulnerability.

- Link

—

” “Tue, 19 Mar 2024

Tramyardg Autoexpress 1.3.0 Cross Site Scripting

Tramyardg Autoexpress version 1.3.0 suffers from a persistent cross site scripting vulnerability.
- Link
—
” “Tue, 19 Mar 2024
Tramyardg Autoexpress 1.3.0 Authentication Bypass
Tramyardg Autoexpress version 1.3.0 allows for authentication bypass via unauthenticated API access to admin functionality. This could allow a remote anonymous attacker to delete or update vehicles as well as upload images for vehicles.
- Link
—
” “Tue, 19 Mar 2024
Tramyardg Autoexpress 1.3.0 SQL Injection
Tramyardg Autoexpress version 1.3.0 suffers from a remote SQL injection vulnerability.
- Link
—
” “Tue, 19 Mar 2024
SurveyJS Survey Creator 1.9.132 Cross Site Scripting
SurveyJS Survey Creator versions 1.9.132 and below suffer from both reflective and persistent cross site scripting vulnerabilities.
- Link
—
”

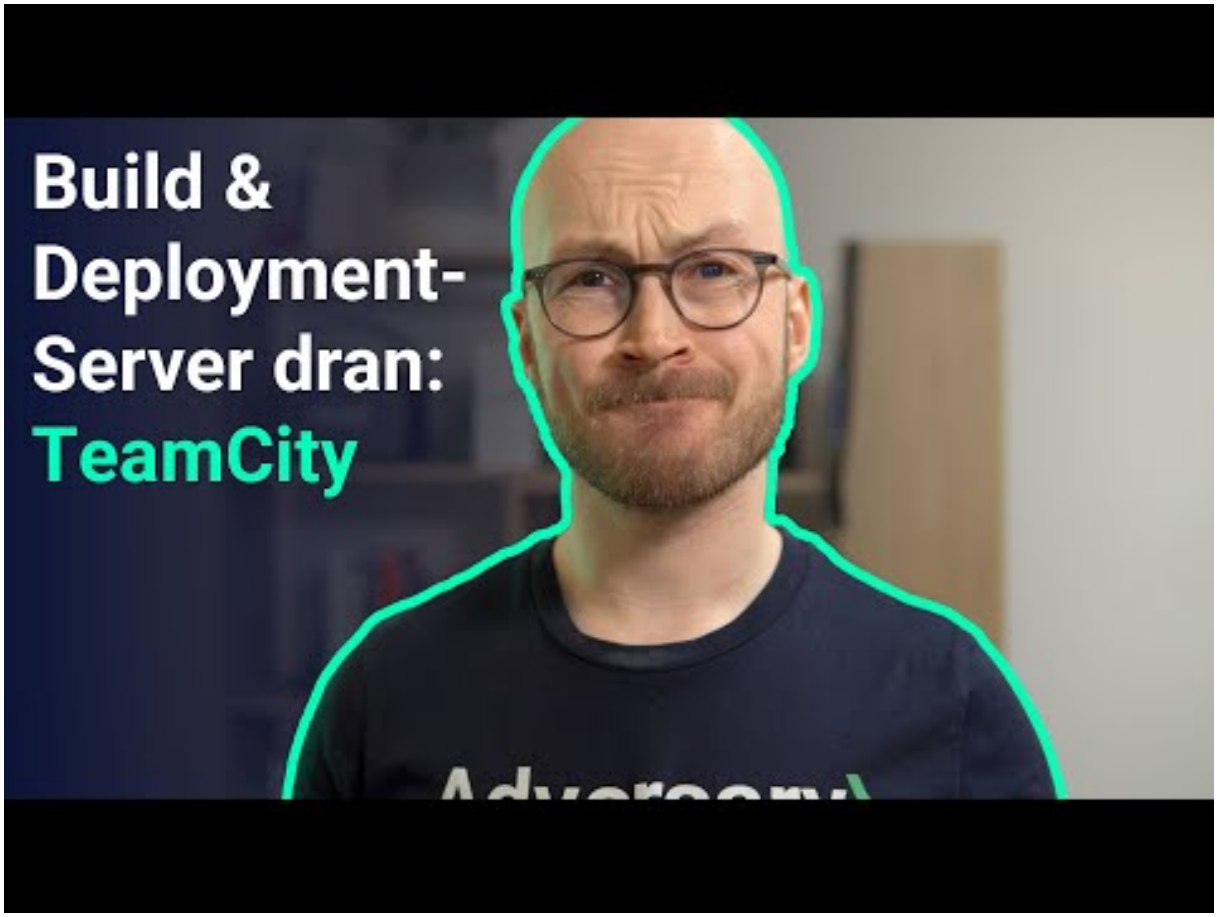
4.2 0-Days der letzten 5 Tage

“Wed, 27 Mar 2024
ZDI-24-296: Autodesk DWG TrueView DWG File Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability
- Link
—
” “Wed, 27 Mar 2024
ZDI-24-295: Autodesk FBX Review ABC File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability
- Link
—
”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 Hättest du diese Lücke gefunden?



Zum Youtube Video

6 Cyberangriffe: (Mär)

Datum	Opfer	Land	Information
2024-03-26	Gilmer County	[USA]	Link
2024-03-26	Unimed VTRP	[BRA]	Link
2024-03-25	City of St. Cloud	[USA]	Link
2024-03-24	Ariza Credit Union	[GRD]	Link
2024-03-24	VNDirect	[VNM]	Link
2024-03-24	Intermarché by Mestdagh	[BEL]	Link
2024-03-21	Tarrant Appraisal District	[USA]	Link
2024-03-20	Nampak	[ZAF]	Link
2024-03-19	Goed	[BEL]	Link
2024-03-18	Unimed Cuiabá	[BRA]	Link
2024-03-18	Comté de Henry, Illinois	[USA]	Link
2024-03-17	Ville de Pensacola	[USA]	Link
2024-03-17	South China Athletic Association	[HKG]	Link
2024-03-17	Polycab	[IND]	Link
2024-03-15	Fujitsu	[JPN]	Link
2024-03-15	Deutsches Meeresmuseum de Stralsund	[DEU]	Link
2024-03-15	Communauté de communes de Nuits-Saint-Georges	[FRA]	Link
2024-03-15	Trifyl	[FRA]	Link
2024-03-14	NHS Dumfries and Galloway	[GBR]	Link
2024-03-14	Scranton School District	[USA]	Link
2024-03-14	Radiant Logistics, Inc.	[USA]	Link
2024-03-13	Maxis	[MYS]	Link
2024-03-12	Riverview School District	[USA]	Link
2024-03-11	District de North Vancouver	[CAN]	Link
2024-03-11	Scullion Law	[GBR]	Link

Datum	Opfer	Land	Information
2024-03-10	edpnet	[BEL]	Link
2024-03-10	Town of Huntsville	[CAN]	Link
2024-03-10	MarineMax	[USA]	Link
2024-03-10	EDIS	[AUT]	Link
2024-03-09	Leicester City Council	[GBR]	Link
2024-03-08	Kärntner Landesversicherung (KLV)	[AUT]	Link
2024-03-07	Administradora de Subsidios Sociales (ADESS)	[DOM]	Link
2024-03-07	Beyers Koffie	[BEL]	Link
2024-03-06	Brasserie Duvel Moortgat	[BEL]	Link
2024-03-06	Nisqually Red Wind Casino	[USA]	Link
2024-03-04	FINTRAC (Financial Transactions and Reports Analysis Centre of Canada)	[CAN]	Link
2024-03-04	South St. Paul Public Schools	[USA]	Link
2024-03-01	Hansab	[EST]	Link

7 Ransomware-Erpressungen: (Mär)

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-28	[Primeimaging Data Leak]	everest	Link
2024-03-27	[Otolaryngology Associates]	incransom	Link
2024-03-27	[anovahealth.com]	lockbit3	Link
2024-03-27	[PT Bank Pembangunan Daerah Banten Tbk]	medusa	Link
2024-03-27	[vilis.com]	blackbasta	Link
2024-03-27	[pstrans.com]	blackbasta	Link
2024-03-27	[fpdcompany.com]	blackbasta	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-27	[northamericansigns.com]	blackbasta	Link
2024-03-27	[otrwheel.com]	blackbasta	Link
2024-03-27	[prodrive.com]	blackbasta	Link
2024-03-27	[dgse.com]	blackbasta	Link
2024-03-27	[Summer Fresh]	qilin	Link
2024-03-27	[Pavilion Construction]	play	Link
2024-03-27	[Boingo Graphics]	play	Link
2024-03-27	[bulwarkpestcontrol.com]	blackbasta	Link
2024-03-27	[lagunitas.com]	blackbasta	Link
2024-03-27	[carolinafoodsinc.com]	blackbasta	Link
2024-03-27	[ero-etikett.com]	blackbasta	Link
2024-03-27	[amerlux.com]	blackbasta	Link
2024-03-27	[organizedliving.com]	blackbasta	Link
2024-03-27	[mjcelco.com]	blackbasta	Link
2024-03-27	[kmbdg.com]	blackbasta	Link
2024-03-27	[pctinternational.com]	blackbasta	Link
2024-03-27	[theshootingwarehouse.com]	blackbasta	Link
2024-03-27	[Mermet]	akira	Link
2024-03-27	[Tbr Kowalczyk]	play	Link
2024-03-27	[JM Thompson]	play	Link
2024-03-27	[Weld Plus]	play	Link
2024-03-27	[qosina.com]	cactus	Link
2024-03-27	[Festspielhaus Baden-Baden]	play	Link
2024-03-27	[West Monroe]	play	Link
2024-03-27	[Frawner]	play	Link
2024-03-27	[Alber Law Group]	play	Link
2024-03-27	[Hartz]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-27	[Quality Enclosures]	play	Link
2024-03-27	[Lawrence Semiconductor Research Laboratory]	play	Link
2024-03-27	[Lambda Energy Resources]	play	Link
2024-03-27	[dkpvlaw.com]	lockbit3	Link
2024-03-27	[lifelinedatacenters.com]	lockbit3	Link
2024-03-27	[countryvillahealthservices.com]	lockbit3	Link
2024-03-27	[lindquistinsurance.com]	abyss	Link
2024-03-27	[pcscivilinc.com]	lockbit3	Link
2024-03-27	[krueth.de]	lockbit3	Link
2024-03-26	[NHS Scotland]	incransom	Link
2024-03-27	[tmt-mc.jp]	lockbit3	Link
2024-03-27	[contenderboats.com]	cactus	Link
2024-03-27	[HC Querétaro]	8base	Link
2024-03-27	[UNDP]	8base	Link
2024-03-27	[Lindos Group Of Companies]	8base	Link
2024-03-27	[isophon glas GmbH]	8base	Link
2024-03-26	[Miki Travel Limited]	snatch	Link
2024-03-26	[nampak.com]	lockbit3	Link
2024-03-26	[El Debate]	rhysida	Link
2024-03-26	[SummerFresh]	qilin	Link
2024-03-26	[polycab.com]	lockbit3	Link
2024-03-26	[Barrie and Community Family Health Team]	incransom	Link
2024-03-26	[Lieberman LLP]	bianlian	Link
2024-03-26	[Affiliated Dermatologists and Dermatologic Surgeons]	bianlian	Link
2024-03-26	[Koi Design]	akira	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-26	[Tanis Brush]	akira	Link
2024-03-26	[Crimsgroup]	everest	Link
2024-03-26	[Woodsboro ISD]	ransomhub	Link
2024-03-25	[regencymedia.com.au]	lockbit3	Link
2024-03-25	[wblight.com]	lockbit3	Link
2024-03-25	[CLARK Material Handling Company]	hunters	Link
2024-03-25	[Dunbier Boat Trailers]	dragonforce	Link
2024-03-25	[Big Issue Group]	qilin	Link
2024-03-25	[Greenline Service]	dragonforce	Link
2024-03-25	[Teton Orthopaedics]	dragonforce	Link
2024-03-25	[Calida]	akira	Link
2024-03-25	[Vita IT]	akira	Link
2024-03-25	[European Centre for Compensation]	akira	Link
2024-03-25	[Burnham Wood Charter Schools]	qilin	Link
2024-03-25	[kh.org]	threeam	Link
2024-03-25	[Ejército del Per]	incransom	Link
2024-03-25	[Law Offices of John V. Orrick, P.L.]	incransom	Link
2024-03-25	[Pantana CPA]	incransom	Link
2024-03-19	[Hallesche Kraftverkehrs & Speditions GmbH]	hunters	Link
2024-03-24	[Vhs-vaterstetten.de]	cloak	Link
2024-03-24	[Gascontec.com]	cloak	Link
2024-03-24	[Equatorial Energia]	cloak	Link
2024-03-23	[SchwarzGrantz]	raworld	Link
2024-03-23	[Title Management Inc]	raworld	Link
2024-03-23	[Pascoe International]	raworld	Link
2024-03-23	[Regina Dental Group]	medusa	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-23	[Impac Mortgage Holdings]	medusa	Link
2024-03-22	[Power Generation Engineering and Services Company (PGESCo) - pgesco.com]	ransomhub	Link
2024-03-22	[Bira 91]	bianlian	Link
2024-03-22	[Chambers Construction Co.]	bianlian	Link
2024-03-22	[newagesys.com]	cactus	Link
2024-03-22	[kelson.on.ca]	cactus	Link
2024-03-22	[flynncompanies.com]	blackbasta	Link
2024-03-22	[Casa Santiveri]	qilin	Link
2024-03-21	[ptsmi.co.id]	qilin	Link
2024-03-21	[Industrial de Alimentos EYL SA]	ransomhub	Link
2024-03-21	[politiaromana.ro]	killsec	Link
2024-03-21	[rabitbd.com]	killsec	Link
2024-03-21	[pbgbank.com]	killsec	Link
2024-03-21	[excellifecoaching.com]	killsec	Link
2024-03-21	[keralapolice.gov.in]	killsec	Link
2024-03-21	[Henry County, Illinois]	medusa	Link
2024-03-21	[northerncasket.com]	lockbit3	Link
2024-03-21	[tmbs.ch]	lockbit3	Link
2024-03-21	[pathologie-bochum.de]	lockbit3	Link
2024-03-21	[La Pastina]	ransomhub	Link
2024-03-21	[Bisco Industries]	raworld	Link
2024-03-21	[Bluelinea]	raworld	Link
2024-03-21	[Deepnoid]	raworld	Link
2024-03-21	[Eastern Media International Corporation]	raworld	Link
2024-03-21	[Eyegene]	raworld	Link
2024-03-21	[Insurance Providers Group]	raworld	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-21	[Thaire]	raworld	Link
2024-03-21	[Decimal Point Analytics Pvt]	raworld	Link
2024-03-21	[Wealth Enhancement Group]	raworld	Link
2024-03-21	[Zurvita]	raworld	Link
2024-03-21	[Piex Group]	raworld	Link
2024-03-21	[Yuxin Automobile Co.Ltd]	raworld	Link
2024-03-21	[24/7 Express Logistics]	raworld	Link
2024-03-21	[Aceromex]	raworld	Link
2024-03-21	[Chung Hwa Chemical Industrial Works]	raworld	Link
2024-03-21	[SUMMIT VETERINARY PHARMACEUTICALS LIMITED]	raworld	Link
2024-03-21	[Informist Media]	raworld	Link
2024-03-21	[ALAB laboratoria]	raworld	Link
2024-03-21	[Di Martino Group]	raworld	Link
2024-03-21	[Rockford Gastroenterology Associates]	raworld	Link
2024-03-21	[HALLIDAYS GROUP LIMITED]	raworld	Link
2024-03-21	[Die Unfallkasse Thüringen]	raworld	Link
2024-03-21	[NIDEC GPM GmbH]	raworld	Link
2024-03-21	[Wurzbacher]	raworld	Link
2024-03-21	[Ranzijn]	raworld	Link
2024-03-21	[SHORTERM GROUP]	raworld	Link
2024-03-20	[MarineMax]	rhysida	Link
2024-03-20	[Suburban Surgical Care Specialists]	medusa	Link
2024-03-20	[igf-inc.com]	blackbasta	Link
2024-03-20	[logistasolutions.com]	blackbasta	Link
2024-03-20	[oceaneering.com]	blackbasta	Link
2024-03-20	[interluxury.com]	blackbasta	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-20	[Kolbe Striping]	rhysida	Link
2024-03-20	[Springfield Sign]	8base	Link
2024-03-20	[ÖSTENSSONS LIVS AB]	8base	Link
2024-03-20	[Filexis AG Treuhand und Immobilien]	8base	Link
2024-03-20	[South Star Electronics]	trigona	Link
2024-03-19	[Accipiter Capital Management, LLC]	medusa	Link
2024-03-19	[Urban Strategies]	medusa	Link
2024-03-19	[Sting AD]	hunters	Link
2024-03-19	[Jasper-Dubois County Public Library]	dragonforce	Link
2024-03-19	[Therapeutic Health Services]	hunters	Link
2024-03-19	[Panzeri Cattaneo]	hunters	Link
2024-03-19	[Retirement Line]	snatch	Link
2024-03-19	[Delta Pipeline]	bianlian	Link
2024-03-19	[Mayer Antonellis Jachowicz & Haranas, LLP]	bianlian	Link
2024-03-19	[P&B Capital Group]	bianlian	Link
2024-03-17	[Butler, Lavanceau & Sober]	snatch	Link
2024-03-18	[Dr. Leeman ENT]	bianlian	Link
2024-03-18	[HSI]	hunters	Link
2024-03-18	[AGL]	hunters	Link
2024-03-18	[Sun Holdings]	hunters	Link
2024-03-17	[paginesi]	stormous	Link
2024-03-18	[eclinicalsol.com]	cactus	Link
2024-03-18	[grupatopex.com]	cactus	Link
2024-03-18	[activeconceptsllc.com]	blackbasta	Link
2024-03-17	[Romark Laboratories]	medusa	Link
2024-03-18	[crinetics.com]	lockbit3	Link
2024-03-03	[highfashion.com.hk]	mallox	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-14	[Ramdev Chemical Industries]	mallox	Link
2024-03-16	[Rafum Group]	mallox	Link
2024-03-16	[Autorità di Sistema Portuale del Mar Tirreno Settentrionale It]	medusa	Link
2024-03-16	[Elior UK]	medusa	Link
2024-03-16	[Indoarsip]	trigona	Link
2024-03-16	[Bwizer]	trigona	Link
2024-03-16	[Topa Partners]	trigona	Link
2024-03-16	[HUDSONBUSSALES.COM]	clop	Link
2024-03-15	[Desco Steel]	medusa	Link
2024-03-15	[Metzger Veterinary Services]	medusa	Link
2024-03-16	[Consolidated Benefits Resources]	bianlian	Link
2024-03-16	[agribank.com.na]	lockbit3	Link
2024-03-16	[triella.com]	lockbit3	Link
2024-03-16	[rrib.com]	lockbit3	Link
2024-03-16	[newmans-online.co.uk]	lockbit3	Link
2024-03-16	[hdstrading.com]	lockbit3	Link
2024-03-16	[duttonbrock.com]	lockbit3	Link
2024-03-16	[colefabrics.com]	lockbit3	Link
2024-03-16	[bergmeister.eu]	lockbit3	Link
2024-03-16	[automotionshade.com]	lockbit3	Link
2024-03-16	[Miki Travel]	hunters	Link
2024-03-16	[certifiedcollection.com]	lockbit3	Link
2024-03-16	[Acculabs Inc]	incransom	Link
2024-03-08	[oyaksgs.com.tr]	lockbit3	Link
2024-03-15	[elezabypharmacy.com]	lockbit3	Link
2024-03-15	[South St Paul Public Schools]	blacksuit	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-12	[ATL Leasing]	hunters	Link
2024-03-14	[lostlb]	stormous	Link
2024-03-14	[education.eeb-lost]	stormous	Link
2024-03-14	[worthenind.com]	lockbit3	Link
2024-03-14	[rushenergyservices.com]	lockbit3	Link
2024-03-14	[sbmandco.com]	lockbit3	Link
2024-03-14	[mckimcreed.com]	lockbit3	Link
2024-03-14	[moperry.com]	lockbit3	Link
2024-03-14	[Cosmocolor]	hunters	Link
2024-03-14	[voidinteractive.net you are welcome in our chat]	donutleaks	Link
2024-03-14	[journeyfreight.com]	lockbit3	Link
2024-03-14	[dhanisisd.net]	lockbit3	Link
2024-03-14	[mioa.gov]	stormous	Link
2024-03-14	[gfad.de]	blackbasta	Link
2024-03-14	[Keboda Technology Co., Ltd.]	bianlian	Link
2024-03-14	[iamdesign.com]	abyss	Link
2024-03-14	[yarco.com]	abyss	Link
2024-03-13	[McKim & Creed]	ransomhub	Link
2024-03-13	[SBM & Co]	ransomhub	Link
2024-03-13	[Summit Almonds]	akira	Link
2024-03-13	[Encina Wastewater Authority]	blackbyte	Link
2024-03-13	[SBM & Co]	ransomhub	Link
2024-03-13	[Felda Global Ventures Holdings Berhad]	qilin	Link
2024-03-13	[geruestbau.com]	lockbit3	Link
2024-03-13	[Judge Rotenberg Center]	blacksuit	Link
2024-03-12	[Dörr Group]	snatch	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-13	[Kovra]	ransomhub	Link
2024-03-13	[Brewer Davidson]	8base	Link
2024-03-13	[Forstinger Österreich GmbH]	8base	Link
2024-03-04	[vsexshop.ru]	werewolves	Link
2024-03-11	[QEO Group]	play	Link
2024-03-12	[ATL]	hunters	Link
2024-03-12	[duvel.com	boulevard.com]	blackbasta
2024-03-11	[Kenneth Young Center]	medusa	Link
2024-03-12	[sunholdings.net]	lockbit3	Link
2024-03-12	[xcelbrands.com]	blackbasta	Link
2024-03-12	[cpacsystems.se]	blackbasta	Link
2024-03-12	[elmatic.de]	blackbasta	Link
2024-03-12	[keystonetech.com]	blackbasta	Link
2024-03-12	[dutyfreeamericas.com]	blackbasta	Link
2024-03-12	[sierralobo.com]	blackbasta	Link
2024-03-12	[contechs.co.uk]	blackbasta	Link
2024-03-12	[creativeenvironments.com]	blackbasta	Link
2024-03-12	[linksunlimited.com]	blackbasta	Link
2024-03-12	[imperialtrading.com]	blackbasta	Link
2024-03-12	[Brooks Tropicals]	rhysida	Link
2024-03-12	[Withall]	blacksuit	Link
2024-03-12	[WALKERSANDFORD]	blacksuit	Link
2024-03-12	[Kaplan]	hunters	Link
2024-03-06	[Sprimoglass]	8base	Link
2024-03-11	[Schokinag]	play	Link
2024-03-11	[Zips Car Wash]	play	Link
2024-03-11	[Bechtold]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-11	[Canada Revenue Agency]	play	Link
2024-03-11	[White Oak Partners]	play	Link
2024-03-11	[Ruda Auto]	play	Link
2024-03-11	[Image Pointe]	play	Link
2024-03-11	[Grassmid Transport]	play	Link
2024-03-11	[Fashion UK]	play	Link
2024-03-11	[QI Group]	play	Link
2024-03-11	[BiTec]	play	Link
2024-03-11	[Bridger Insurance]	play	Link
2024-03-11	[SREE Hotels]	play	Link
2024-03-11	[Q?? ??o??]	play	Link
2024-03-11	[Premier Technology]	play	Link
2024-03-11	[londonvisionclinic.com]	lockbit3	Link
2024-03-11	[lec-london.uk]	lockbit3	Link
2024-03-11	[Computan]	ransomhub	Link
2024-03-11	[plymouth.com]	cactus	Link
2024-03-11	[neigc.com]	abyss	Link
2024-03-11	[gpaa.gov.za]	lockbit3	Link
2024-03-11	[NetVigour]	hunters	Link
2024-03-11	[cleshar.co.uk]	cactus	Link
2024-03-11	[ammega.com]	cactus	Link
2024-03-11	[renypicot.es]	cactus	Link
2024-03-11	[Scadea Solutions]	ransomhub	Link
2024-03-09	[https://www.consorzioinnova.it]	alphalocker	Link
2024-03-09	[DVT]	ransomhub	Link
2024-03-09	[Rekamy]	ransomhub	Link
2024-03-09	[go4kora]	ransomhub	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-09	[H + G EDV Vertriebs]	blacksuit	Link
2024-03-09	[Fincasrevuelta]	everest	Link
2024-03-09	[Lindsay Municipal Hospital]	bianlian	Link
2024-03-09	[Group Health Cooperative - Rev 500kk]	blacksuit	Link
2024-03-09	[ACE Air Cargo]	hunters	Link
2024-03-09	[Watsonclinic.com]	donutleaks	Link
2024-03-06	[Continental Aerospace Technologies]	play	Link
2024-03-08	[redwoodcoastrc.org]	lockbit3	Link
2024-03-08	[PowerRail Distribution]	blacksuit	Link
2024-03-08	[Denninger’s]	medusa	Link
2024-03-08	[SIEA]	ransomhub	Link
2024-03-08	[Hozzify]	ransomhub	Link
2024-03-07	[rmhfranchise.com]	lockbit3	Link
2024-03-07	[New York Home Healthcare]	bianlian	Link
2024-03-07	[Palmer Construction Co., Inc]	bianlian	Link
2024-03-07	[en-act-architecture]	qilin	Link
2024-03-07	[Merchant ID]	ransomhub	Link
2024-03-07	[SP Mundi]	ransomhub	Link
2024-03-07	[www.duvel.com]	stormous	Link
2024-03-06	[www.loghmanpharma.com]	stormous	Link
2024-03-06	[MainVest]	play	Link
2024-03-06	[C?????????? A???????e T???????????]	play	Link
2024-03-05	[Haivision MCS]	medusa	Link
2024-03-06	[Tocci Building Corporation]	medusa	Link
2024-03-06	[JVCKENWOOD]	medusa	Link
2024-03-06	[American Renal Associates]	medusa	Link
2024-03-06	[US #1364 Federal Credit Union]	medusa	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-06	[viadirectamarketing]	stormous	Link
2024-03-06	[Liquid Environmental Solutions]	incransom	Link
2024-03-06	[Infosoft]	akira	Link
2024-03-06	[brightwires.com.sa]	qilin	Link
2024-03-06	[Medical Billing Specialists]	akira	Link
2024-03-06	[Telecentro]	akira	Link
2024-03-06	[Steiner (Austrian furniture makers)]	akira	Link
2024-03-06	[Biomedical Research Institute]	meow	Link
2024-03-06	[K???o???]	play	Link
2024-03-06	[Kudulis Reisinger Price]	8base	Link
2024-03-06	[Global Zone]	8base	Link
2024-03-06	[Mediplast AB]	8base	Link
2024-03-05	[airbogo]	stormous	Link
2024-03-05	[sunwave.com.cn]	lockbit3	Link
2024-03-05	[SJCME.EDU]	clop	Link
2024-03-05	[central.k12.or.us]	lockbit3	Link
2024-03-05	[iemsc.com]	qilin	Link
2024-03-05	[hawita-gruppe]	qilin	Link
2024-03-05	[Future Generations Foundation]	meow	Link
2024-03-04	[Seven Seas Group]	snatch	Link
2024-03-04	[Paul Davis Restoration]	medusa	Link
2024-03-04	[Veeco]	medusa	Link
2024-03-04	[dismogas]	stormous	Link
2024-03-04	[everplast]	stormous	Link
2024-03-04	[DiVal Safety Equipment, Inc.]	hunters	Link
2024-03-04	[America Chung Nam orACN]	akira	Link
2024-03-03	[jovani.com]	lockbit3	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-03	[valoremreply.com]	lockbit3	Link
2024-03-04	[Martin’s, Inc.]	bianlian	Link
2024-03-03	[Prompt Financial Solutions]	medusa	Link
2024-03-03	[Sophiahemmet University]	medusa	Link
2024-03-03	[Centennial Law Group LLP]	medusa	Link
2024-03-03	[Eastern Rio Blanco Metropolitan]	medusa	Link
2024-03-03	[Chris Argiropoulos Professional]	medusa	Link
2024-03-03	[THAISUMMIT.US]	clop	Link
2024-03-03	[THESAFIRCHOICE.COM]	clop	Link
2024-03-03	[ipmaltamira]	alphv	Link
2024-03-03	[earnesthealth.com]	lockbit3	Link
2024-03-03	[Ward Transport & Logistics]	dragonforce	Link
2024-03-03	[Ponoka.ca]	cloak	Link
2024-03-03	[stockdevelopment.com]	lockbit3	Link
2024-03-03	[Ewig Usa]	alphv	Link
2024-03-02	[aerospace.com]	lockbit3	Link
2024-03-02	[starkpower.de]	lockbit3	Link
2024-03-02	[roehr-stolberg.de]	lockbit3	Link
2024-03-02	[schuett-grundei.de]	lockbit3	Link
2024-03-02	[unitednotions.com]	lockbit3	Link
2024-03-02	[smuldes.com]	lockbit3	Link
2024-03-02	[esser-ps.de]	lockbit3	Link
2024-03-01	[SBM & Co [You have 48 hours. Check your e-mail]]	alphv	Link
2024-03-01	[Skyland Grain]	play	Link
2024-03-01	[American Nuts]	play	Link
2024-03-01	[A&A Wireless]	play	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-03-01	[Powill Manufacturing & Engineering]	play	Link
2024-03-01	[Trans+Plus Systems]	play	Link
2024-03-01	[Hedlunds]	play	Link
2024-03-01	[Red River Title]	play	Link
2024-03-01	[Compact Mould]	play	Link
2024-03-01	[Winona Pattern & Mold]	play	Link
2024-03-01	[Marketon]	play	Link
2024-03-01	[Stack Infrastructure]	play	Link
2024-03-01	[Coastal Car]	play	Link
2024-03-01	[New Bedford Welding Supply]	play	Link
2024-03-01	[Influence Communication]	play	Link
2024-03-01	[Kool-air]	play	Link
2024-03-01	[FBi Construction]	play	Link
2024-03-01	[SBM & Co]	alphv	Link
2024-03-01	[Shooting House]	ransomhub	Link
2024-03-01	[Crystal Window & Door Systems]	dragonforce	Link
2024-03-01	[Gilmore Construction]	blacksuit	Link
2024-03-01	[Petrus Resources Ltd]	alphv	Link
2024-03-01	[CoreData]	akira	Link
2024-03-01	[Gansevoort Hotel Group]	akira	Link
2024-03-01	[DJI Company]	mogilevich	Link
2024-03-01	[Kick]	mogilevich	Link
2024-03-01	[Shein]	mogilevich	Link
2024-03-01	[Kumagai Gumi Group]	alphv	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.