

---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240322



## Inhaltsverzeichnis

<b>1 Editorial</b>	<b>2</b>
<b>2 Security-News</b>	<b>3</b>
2.1 Heise - Security-Alert . . . . .	3
<b>3 Sicherheitslücken</b>	<b>4</b>
3.1 EPSS . . . . .	4
3.1.1 CVEs mit hoher Exploit-Wahrscheinlichkeit . . . . .	5
3.2 BSI - Warn- und Informationsdienst (WID) . . . . .	7
3.3 Sicherheitslücken Meldungen von Tenable . . . . .	10
<b>4 Aktiv ausgenutzte Sicherheitslücken</b>	<b>13</b>
4.1 Exploits der letzten 5 Tage . . . . .	13
4.2 0-Days der letzten 5 Tage . . . . .	17
<b>5 Die Hacks der Woche</b>	<b>18</b>
5.0.1 Hättest du diese Lücke gefunden? ☒ . . . . .	18
<b>6 Cyberangriffe: (Mär)</b>	<b>19</b>
<b>7 Ransomware-Erpressungen: (Mär)</b>	<b>20</b>
<b>8 Quellen</b>	<b>31</b>
8.1 Quellenverzeichnis . . . . .	31
<b>9 Impressum</b>	<b>32</b>

## 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

#### ***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](#)

—

#### ***Webbrowser Chrome: Google dichtet mehrere Sicherheitslecks ab***

Insgesamt zwölf Schwachstellen bessert Google mit aktualisierten Versionen des Chrome-Webrowsers aus.

- [Link](#)

—

#### ***Sicherheitsupdates für Firefox und Thunderbird***

Mozilla dichtet zahlreiche Sicherheitslücken im Webbrowser Firefox und Mailer Thunderbird ab.

- [Link](#)

—

#### ***Spring Security: Zugriffskontrollmechanismen in Java-Framework kaputt***

Die auf Sicherheitsmechanismen spezialisierte Unterbibliothek des Java-Entwicklungsframeworks kommt in manchen Fällen aus dem Tritt. Updates sind verfügbar.

- [Link](#)

—

**Home- und Raspberry-Matic: Kritische Lücke erlaubt Codeschmuggel**

In HomeMatic sowie in RaspberryMatic klafft eine Codeschmuggel-Lücke. Sie gilt als kritisch. Ein Update steht bereit.

- [Link](#)

---

**Spring Framework: Updates beheben neue, alte Sicherheitslücke**

Nutzen Spring-basierte Anwendungen eine URL-Parsing-Funktion des Frameworks, öffnen sie sich für verschiedene Attacken. Nicht zum ersten Mal.

- [Link](#)

---

**HP: Viele Laptops und PCs von Codeschmuggel-Lücke betroffen**

Eine BIOS-Sicherheitsfunktion von HP-Laptops und -PCs kann von Angreifern umgangen werden. BIOS-Updates stehen bereit oder werden grad entwickelt.

- [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-2023-6895	0.901600000	0.987220000	<a href="#">Link</a>
CVE-2023-6553	0.916210000	0.988350000	<a href="#">Link</a>
CVE-2023-5360	0.967230000	0.996360000	<a href="#">Link</a>
CVE-2023-4966	0.966110000	0.996050000	<a href="#">Link</a>
CVE-2023-47246	0.943540000	0.991470000	<a href="#">Link</a>
CVE-2023-46805	0.962740000	0.994970000	<a href="#">Link</a>
CVE-2023-46747	0.972020000	0.998050000	<a href="#">Link</a>
CVE-2023-46604	0.973060000	0.998610000	<a href="#">Link</a>
CVE-2023-43177	0.927670000	0.989650000	<a href="#">Link</a>
CVE-2023-42793	0.970930000	0.997590000	<a href="#">Link</a>
CVE-2023-39143	0.933560000	0.990250000	<a href="#">Link</a>
CVE-2023-38646	0.916640000	0.988420000	<a href="#">Link</a>
CVE-2023-38205	0.934710000	0.990370000	<a href="#">Link</a>
CVE-2023-38203	0.960070000	0.994380000	<a href="#">Link</a>
CVE-2023-38035	0.972370000	0.998290000	<a href="#">Link</a>
CVE-2023-36845	0.966580000	0.996150000	<a href="#">Link</a>
CVE-2023-35813	0.905250000	0.987460000	<a href="#">Link</a>
CVE-2023-3519	0.911860000	0.988030000	<a href="#">Link</a>
CVE-2023-35082	0.935540000	0.990460000	<a href="#">Link</a>
CVE-2023-35078	0.963380000	0.995160000	<a href="#">Link</a>
CVE-2023-34960	0.935410000	0.990450000	<a href="#">Link</a>
CVE-2023-34634	0.925600000	0.989380000	<a href="#">Link</a>
CVE-2023-34362	0.960450000	0.994490000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-34039	0.901300000	0.987190000	<a href="#">Link</a>
CVE-2023-3368	0.904650000	0.987430000	<a href="#">Link</a>
CVE-2023-33246	0.973410000	0.998830000	<a href="#">Link</a>
CVE-2023-32315	0.973840000	0.999050000	<a href="#">Link</a>
CVE-2023-32235	0.905760000	0.987510000	<a href="#">Link</a>
CVE-2023-30625	0.948330000	0.992190000	<a href="#">Link</a>
CVE-2023-30013	0.945460000	0.991770000	<a href="#">Link</a>
CVE-2023-29300	0.963690000	0.995260000	<a href="#">Link</a>
CVE-2023-29298	0.921360000	0.988860000	<a href="#">Link</a>
CVE-2023-28771	0.922340000	0.988980000	<a href="#">Link</a>
CVE-2023-28432	0.941310000	0.991120000	<a href="#">Link</a>
CVE-2023-28121	0.929770000	0.989790000	<a href="#">Link</a>
CVE-2023-27524	0.972240000	0.998210000	<a href="#">Link</a>
CVE-2023-27372	0.971520000	0.997870000	<a href="#">Link</a>
CVE-2023-27350	0.972040000	0.998080000	<a href="#">Link</a>
CVE-2023-26469	0.937680000	0.990700000	<a href="#">Link</a>
CVE-2023-26360	0.962420000	0.994880000	<a href="#">Link</a>
CVE-2023-26035	0.970030000	0.997230000	<a href="#">Link</a>
CVE-2023-25717	0.957880000	0.993890000	<a href="#">Link</a>
CVE-2023-2479	0.962540000	0.994910000	<a href="#">Link</a>
CVE-2023-24489	0.973620000	0.998930000	<a href="#">Link</a>
CVE-2023-23752	0.952140000	0.992830000	<a href="#">Link</a>
CVE-2023-23397	0.923530000	0.989080000	<a href="#">Link</a>
CVE-2023-23333	0.963260000	0.995130000	<a href="#">Link</a>
CVE-2023-22527	0.965680000	0.995930000	<a href="#">Link</a>
CVE-2023-22518	0.970110000	0.997250000	<a href="#">Link</a>
CVE-2023-22515	0.971880000	0.998010000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-21839	0.960490000	0.994500000	<a href="#">Link</a>
CVE-2023-21554	0.959700000	0.994270000	<a href="#">Link</a>
CVE-2023-20887	0.964080000	0.995380000	<a href="#">Link</a>
CVE-2023-20198	0.916450000	0.988390000	<a href="#">Link</a>
CVE-2023-1671	0.961560000	0.994680000	<a href="#">Link</a>
CVE-2023-0669	0.968640000	0.996790000	<a href="#">Link</a>

### 3.2 BSI - Warn- und Informationsdienst (WID)

Thu, 21 Mar 2024

#### **[NEU] [hoch] Ruby: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Ruby ausnutzen, um Informationen offenzulegen oder Code auszuführen.

- [Link](#)

—

Thu, 21 Mar 2024

#### **[NEU] [hoch] Checkmk: Mehrere Schwachstellen**

Ein lokaler Angreifer kann mehrere Schwachstellen in Checkmk ausnutzen, um seine Privilegien zu erhöhen oder Informationen offenzulegen.

- [Link](#)

—

Thu, 21 Mar 2024

#### **[NEU] [hoch] Micro Focus ArcSight: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonym Angreifer kann eine Schwachstelle in Micro Focus ArcSight ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Thu, 21 Mar 2024

#### **[NEU] [hoch] Ivanti Sentry: Schwachstelle ermöglicht Codeausführung**

Ein benachbarter, anonym Angreifer kann eine Schwachstelle in Ivanti Sentry ausnutzen, um beliebigen Programmcode auszuführen.



- [Link](#)

—

Thu, 21 Mar 2024

***[NEU] [hoch] Microsoft GitHub Enterprise: Mehrere Schwachstellen ermöglichen Umgehen von Sicherheitsvorkehrungen***

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Microsoft GitHub Enterprise ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Thu, 21 Mar 2024

***[UPDATE] [hoch] Atlassian Jira Software: Mehrere Schwachstellen ermöglichen Codeausführung und DoS***

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in der Atlassian Jira Software ausnutzen, um beliebigen Code auszuführen oder einen Denial-of-Service-Zustand zu verursachen.

- [Link](#)

—

Thu, 21 Mar 2024

***[UPDATE] [kritisch] Apache Tomcat: Schwachstelle ermöglicht Denial of Service***

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

- [Link](#)

—

Thu, 21 Mar 2024

***[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen***

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

- [Link](#)

—

Thu, 21 Mar 2024

***[UPDATE] [hoch] Red Hat FUSE: Mehrere Schwachstellen***

Ein entfernter, anonymer, authentisierter oder lokaler Angreifer kann mehrere Schwachstellen in Red Hat FUSE ausnutzen, um vertrauliche Informationen offenzulegen, beliebigen Code auszuführen, einen Denial of Service Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, Daten und Informationen zu manipulieren und seine Privilegien zu erweitern.

- [Link](#)

—

Thu, 21 Mar 2024

***[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen***

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen, einen Denial-of-Service-Zustand zu verursachen und seine Privilegien zu erweitern.

- [Link](#)

—

Thu, 21 Mar 2024

**[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um beliebigen Programmcode mit Administratorrechten auszuführen, einen Denial-of-Service-Zustand zu verursachen und seine Privilegien zu erweitern.

- [Link](#)

—

Thu, 21 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](#)

—

Thu, 21 Mar 2024

**[UPDATE] [hoch] Linux Kernel: Mehrere Schwachstellen**

Ein lokaler Angreifer kann mehrere Schwachstellen im Linux Kernel ausnutzen, um einen Denial of Service Angriff und einen nicht spezifizierten Angriff durchzuführen.

- [Link](#)

—

Thu, 21 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](#)

—

Thu, 21 Mar 2024

**[UPDATE] [hoch] Linux Kernel: Schwachstelle ermöglicht Codeausführung**

Ein lokaler Angreifer kann eine Schwachstelle im Linux Kernel ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Thu, 21 Mar 2024

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

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

- [Link](#)

—

Thu, 21 Mar 2024

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

Ein entfernter, authentisierter oder anonymes 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](#)

—

Thu, 21 Mar 2024

**[UPDATE] [hoch] LibreOffice: Mehrere Schwachstellen**

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

- [Link](#)

—

Thu, 21 Mar 2024

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

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

- [Link](#)

—

Thu, 21 Mar 2024

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

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

- [Link](#)

—

---

### 3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
3/22/2024	[Fedora 39 : webkitgtk (2024-ee43b83290)]	critical
3/21/2024	[EulerOS Virtualization 2.9.0 : kernel (EulerOS-SA-2024-1468)]	critical
3/21/2024	[Amazon Linux 2023 : cargo, clippy, rust (ALAS2023-2024-566)]	critical
3/21/2024	[Siemens SCALANCE W1750D Buffer Overflow (CVE-2023-22785)]	critical
3/21/2024	[Siemens SCALANCE W1750D Buffer Overflow (CVE-2023-22784)]	critical
3/21/2024	[Siemens SCALANCE W1750D Buffer Overflow (CVE-2023-22783)]	critical
3/21/2024	[Siemens SCALANCE W1750D Buffer Overflow (CVE-2023-22780)]	critical
3/21/2024	[Siemens SCALANCE W1750D Buffer Overflow (CVE-2023-22782)]	critical
3/21/2024	[Siemens SCALANCE W1750D Buffer Overflow (CVE-2023-22786)]	critical
3/21/2024	[Siemens SCALANCE W1750D Buffer Overflow (CVE-2023-22781)]	critical
3/21/2024	[Siemens SCALANCE W1750D Buffer Overflow (CVE-2023-22779)]	critical
3/22/2024	[Fedora 39 : chromium (2024-ec79868e3b)]	high
3/22/2024	[Debian dsa-5644 : thunderbird - security update]	high
3/22/2024	[Oracle Linux 8 : nodejs:16 (ELSA-2024-1444)]	high
3/21/2024	[EulerOS Virtualization 2.9.0 : libXpm (EulerOS-SA-2024-1472)]	high
3/21/2024	[EulerOS Virtualization 2.9.1 : mozjs60 (EulerOS-SA-2024-1458)]	high
3/21/2024	[EulerOS Virtualization 2.9.1 : sudo (EulerOS-SA-2024-1463)]	high

Datum	Schwachstelle	Bewertung
3/21/2024	[EulerOS Virtualization 2.9.1 : kernel (EulerOS-SA-2024-1453)]	high
3/21/2024	[EulerOS Virtualization 2.9.1 : libXpm (EulerOS-SA-2024-1457)]	high
3/21/2024	[Amazon Linux 2023 : cargo, clippy, rust (ALAS2023-2024-574)]	high
3/21/2024	[Amazon Linux 2023 : wireshark-cli, wireshark-devel (ALAS2023-2024-567)]	high
3/21/2024	[Amazon Linux 2023 : nodejs, nodejs-devel, nodejs-full-i18n (ALAS2023-2024-569)]	high
3/21/2024	[Amazon Linux 2023 : libsndfile, libsndfile-devel, libsndfile-utils (ALAS2023-2024-572)]	high
3/21/2024	[Amazon Linux 2023 : aws-nitro-enclaves-cli, aws-nitro-enclaves-cli-devel, aws-nitro-enclaves-cli-integration-tests (ALAS2023-2024-575)]	high
3/21/2024	[Amazon Linux 2023 : fontforge, fontforge-devel (ALAS2023-2024-565)]	high
3/21/2024	[Siemens SCALANCE W1750D Command Injection (CVE-2023-22789)]	high
3/21/2024	[Siemens SCALANCE W1750D Improper Input Validation (CVE-2023-22787)]	high
3/21/2024	[Siemens SCALANCE W1750D Command Injection (CVE-2023-22790)]	high
3/21/2024	[Siemens SCALANCE W1750D Command Injection (CVE-2023-22788)]	high

## 4 Aktiv ausgenutzte Sicherheitslücken

### 4.1 Exploits der letzten 5 Tage

“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 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](#)

—

” “Tue, 19 Mar 2024

#### **Quick.CMS 6.7 SQL Injection**

Quick.CMS version 6.7 suffers from a remote SQL injection vulnerability that allows for authentication bypass.

- [Link](#)

—

” “Tue, 19 Mar 2024

#### **Atlassian Confluence 8.5.3 Remote Code Execution**

Atlassian Confluence versions 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x, and 8.5.0 through 8.5.3 suffer from a remote code execution vulnerability.

- [Link](#)

—

” “Tue, 19 Mar 2024

#### **Backdrop CMS 1.23.0 Cross Site Scripting**

Backdrop CMS version 1.23.0 suffers from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Tue, 19 Mar 2024

#### **ZoneMinder Snapshots Remote Code Execution**

ZoneMinder Snapshots versions prior to 1.37.33 suffer from an unauthenticated remote code execution vulnerability.

- [Link](#)

—

” “Tue, 19 Mar 2024

#### **WEBIGniter 28.7.23 Cross Site Scripting**

WEBIGniter version 28.7.23 suffers from a cross site scripting vulnerability.

- [Link](#)

—

” “Tue, 19 Mar 2024

#### **WordPress File Upload Cross Site Scripting**

WordPress File Upload plugin versions prior to 4.23.3 suffer from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Tue, 19 Mar 2024

#### **Gibbon LMS 26.0.00 PHP Deserialization / Code Execution**



Gibbon LMS version 26.0.00 suffers from a PHP deserialization vulnerability that allows for authenticated remote code execution.

- [Link](#)

—

” “Tue, 19 Mar 2024

***Fortra FileCatalyst Workflow 5.x Remote Code Execution***

This is a proof of concept exploit for CVE-2024-25153, a remote code execution vulnerability in Fortra FileCatalyst Workflow versions 5.x, before 5.1.6 Build 114.

- [Link](#)

—

” “Tue, 19 Mar 2024

***Generic And Automated Drive-By GPU Cache Attacks From The Browser***

In this paper, the authors present the first GPU cache side-channel attack from within the browser, more specifically from the restricted WebGPU environment. The foundation for our generic and automated attacks are self-configuring primitives applicable to a wide variety of devices, which they demonstrate on a set of 11 desktop GPUs from 5 different generations and 2 vendors.

- [Link](#)

—

” “Mon, 18 Mar 2024

***dav1d Integer Overflow / Out-Of-Bounds Write***

There is an integer overflow in dav1d when decoding an AV1 video with large width/height. The integer overflow may result in an out-of-bounds write.

- [Link](#)

—

” “Mon, 18 Mar 2024

***UPS Network Management Card 4 Path Traversal***

UPS Network Management Card version 4 suffers from a path traversal vulnerability.

- [Link](#)

—

” “Mon, 18 Mar 2024

***Gasmark Pro 1.0 Shell Upload***

Gasmark Pro version 1.0 suffers from a remote shell upload vulnerability.

- [Link](#)

—

” “Mon, 18 Mar 2024

***Nokia BMC Log Scanner 13 Command Injection***

Nokia BMC Log Scanner version 13 suffers from a remote command injection vulnerability.

- [Link](#)

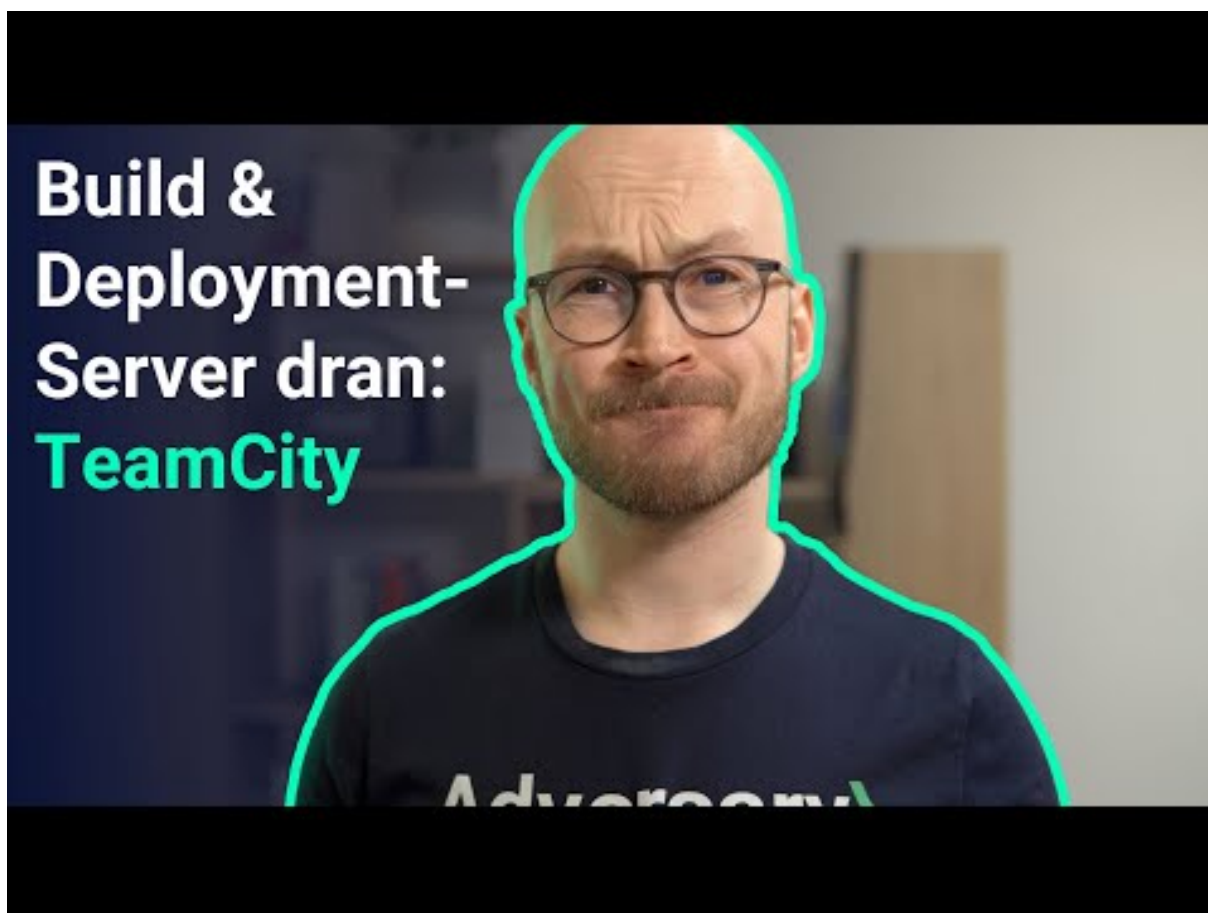
—  
”

## **4.2 0-Days der letzten 5 Tage**

## 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
2024-03-19	Goed	[BEL]	<a href="#">Link</a>
2024-03-18	Unimed Cuiabá	[BRA]	<a href="#">Link</a>
2024-03-17	Ville de Pensacola	[USA]	<a href="#">Link</a>
2024-03-17	South China Athletic Association	[HKG]	<a href="#">Link</a>
2024-03-17	Polycab	[IND]	<a href="#">Link</a>
2024-03-15	Fujitsu	[JPN]	<a href="#">Link</a>
2024-03-15	Deutsches Meeresmuseum de Stralsund	[DEU]	<a href="#">Link</a>
2024-03-15	Communauté de communes de Nuits-Saint-Georges	[FRA]	<a href="#">Link</a>
2024-03-14	NHS Dumfries and Galloway	[GBR]	<a href="#">Link</a>
2024-03-14	Scranton School District	[USA]	<a href="#">Link</a>
2024-03-14	Radiant Logistics, Inc.	[USA]	<a href="#">Link</a>
2024-03-13	Maxis	[MYS]	<a href="#">Link</a>
2024-03-12	Riverview School District	[USA]	<a href="#">Link</a>
2024-03-11	District de North Vancouver	[CAN]	<a href="#">Link</a>
2024-03-10	edpnet	[BEL]	<a href="#">Link</a>
2024-03-10	Town of Huntsville	[CAN]	<a href="#">Link</a>
2024-03-10	MarineMax	[USA]	<a href="#">Link</a>
2024-03-10	EDIS	[AUT]	<a href="#">Link</a>
2024-03-09	Leicester City Council	[GBR]	<a href="#">Link</a>
2024-03-08	Kärntner Landesversicherung (KLV)	[AUT]	<a href="#">Link</a>
2024-03-07	Administradora de Subsidios Sociales (ADESS)	[DOM]	<a href="#">Link</a>
2024-03-07	Beyers Koffie	[BEL]	<a href="#">Link</a>
2024-03-06	Brasserie Duvel Moortgat	[BEL]	<a href="#">Link</a>
2024-03-06	Nisqually Red Wind Casino	[USA]	<a href="#">Link</a>

Datum	Opfer	Land	Information
2024-03-04	FINTRAC (Financial Transactions and Reports Analysis Centre of Canada)	[CAN]	<a href="#">Link</a>
2024-03-04	South St. Paul Public Schools	[USA]	<a href="#">Link</a>
2024-03-01	Hansab	[EST]	<a href="#">Link</a>

## 7 Ransomware-Erpressungen: (Mär)

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-03-22	[Casa Santiveri]	qilin	<a href="#">Link</a>
2024-03-21	[ptsmi.co.id]	qilin	<a href="#">Link</a>
2024-03-21	[Industrial de Alimentos EYL SA]	ransomhub	<a href="#">Link</a>
2024-03-21	[politiaromana.ro]	killsec	<a href="#">Link</a>
2024-03-21	[rabitbd.com]	killsec	<a href="#">Link</a>
2024-03-21	[pbgbank.com]	killsec	<a href="#">Link</a>
2024-03-21	[excellifecoaching.com]	killsec	<a href="#">Link</a>
2024-03-21	[keralapolice.gov.in]	killsec	<a href="#">Link</a>
2024-03-21	[Henry County, Illinois]	medusa	<a href="#">Link</a>
2024-03-21	[northerncasket.com]	lockbit3	<a href="#">Link</a>
2024-03-21	[tmbs.ch]	lockbit3	<a href="#">Link</a>
2024-03-21	[pathologie-bochum.de]	lockbit3	<a href="#">Link</a>
2024-03-21	[La Pastina ]	ransomhub	<a href="#">Link</a>
2024-03-21	[Bisco Industries]	raworld	<a href="#">Link</a>
2024-03-21	[Bluelinea]	raworld	<a href="#">Link</a>
2024-03-21	[Deepnoid]	raworld	<a href="#">Link</a>
2024-03-21	[Eastern Media International Corporation]	raworld	<a href="#">Link</a>
2024-03-21	[Eyegene]	raworld	<a href="#">Link</a>

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

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

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-03-03	[highfashion.com.hk]	mallox	<a href="#">Link</a>
2024-03-14	[Ramdev Chemical Industries]	mallox	<a href="#">Link</a>
2024-03-16	[Rafum Group]	mallox	<a href="#">Link</a>
2024-03-16	[Autorità di Sistema Portuale del Mar Tirreno Settentrionale It]	medusa	<a href="#">Link</a>
2024-03-16	[Elior UK ]	medusa	<a href="#">Link</a>
2024-03-16	[Indoarsip]	trigona	<a href="#">Link</a>
2024-03-16	[Bwizer]	trigona	<a href="#">Link</a>
2024-03-16	[Topa Partners]	trigona	<a href="#">Link</a>
2024-03-16	[HUDSONBUSSALES.COM]	clop	<a href="#">Link</a>
2024-03-15	[Desco Steel]	medusa	<a href="#">Link</a>
2024-03-15	[Metzger Veterinary Services]	medusa	<a href="#">Link</a>
2024-03-16	[Consolidated Benefits Resources]	bianlian	<a href="#">Link</a>
2024-03-16	[agribank.com.na]	lockbit3	<a href="#">Link</a>
2024-03-16	[triella.com]	lockbit3	<a href="#">Link</a>
2024-03-16	[rrib.com]	lockbit3	<a href="#">Link</a>
2024-03-16	[newmans-online.co.uk]	lockbit3	<a href="#">Link</a>
2024-03-16	[hdstrading.com]	lockbit3	<a href="#">Link</a>
2024-03-16	[duttonbrock.com]	lockbit3	<a href="#">Link</a>
2024-03-16	[colefabrics.com]	lockbit3	<a href="#">Link</a>
2024-03-16	[bergmeister.eu]	lockbit3	<a href="#">Link</a>
2024-03-16	[automotionsshade.com]	lockbit3	<a href="#">Link</a>
2024-03-16	[Miki Travel]	hunters	<a href="#">Link</a>
2024-03-16	[certifiedcollection.com]	lockbit3	<a href="#">Link</a>
2024-03-16	[Acculabs Inc]	incransom	<a href="#">Link</a>
2024-03-08	[oyaksgs.com.tr]	lockbit3	<a href="#">Link</a>
2024-03-15	[elezabypharmacy.com]	lockbit3	<a href="#">Link</a>



Datum	Opfer	Ransomware-Gruppe	Webseite
2024-03-15	[South St Paul Public Schools]	blacksuit	<a href="#">Link</a>
2024-03-12	[ATL Leasing]	hunters	<a href="#">Link</a>
2024-03-14	[lostlb]	stormous	<a href="#">Link</a>
2024-03-14	[education.eeb-lost]	stormous	<a href="#">Link</a>
2024-03-14	[worthenind.com]	lockbit3	<a href="#">Link</a>
2024-03-14	[rushenergyservices.com]	lockbit3	<a href="#">Link</a>
2024-03-14	[sbmandco.com]	lockbit3	<a href="#">Link</a>
2024-03-14	[mckimcreed.com]	lockbit3	<a href="#">Link</a>
2024-03-14	[moperry.com]	lockbit3	<a href="#">Link</a>
2024-03-14	[Cosmocolor]	hunters	<a href="#">Link</a>
2024-03-14	[voidinteractive.net you are welcome in our chat]	donutleaks	<a href="#">Link</a>
2024-03-14	[journeyfreight.com]	lockbit3	<a href="#">Link</a>
2024-03-14	[dhanisisd.net]	lockbit3	<a href="#">Link</a>
2024-03-14	[mioa.gov]	stormous	<a href="#">Link</a>
2024-03-14	[gfad.de]	blackbasta	<a href="#">Link</a>
2024-03-14	[Keboda Technology Co., Ltd.]	bianlian	<a href="#">Link</a>
2024-03-14	[iamdesign.com]	abyss	<a href="#">Link</a>
2024-03-14	[yarco.com]	abyss	<a href="#">Link</a>
2024-03-13	[McKim & Creed ]	ransomhub	<a href="#">Link</a>
2024-03-13	[SBM & Co ]	ransomhub	<a href="#">Link</a>
2024-03-13	[Summit Almonds]	akira	<a href="#">Link</a>
2024-03-13	[Encina Wastewater Authority]	blackbyte	<a href="#">Link</a>
2024-03-13	[SBM & Co]	ransomhub	<a href="#">Link</a>
2024-03-13	[Felda Global Ventures Holdings Berhad]	qilin	<a href="#">Link</a>
2024-03-13	[geruestbau.com]	lockbit3	<a href="#">Link</a>
2024-03-13	[Judge Rotenberg Center]	blacksuit	<a href="#">Link</a>

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

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

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-03-09	[go4kora ]	ransomhub	<a href="#">Link</a>
2024-03-09	[H + G EDV Vertriebs]	blacksuit	<a href="#">Link</a>
2024-03-09	[Fincasrevuelta]	everest	<a href="#">Link</a>
2024-03-09	[Lindsay Municipal Hospital]	bianlian	<a href="#">Link</a>
2024-03-09	[Group Health Cooperative - Rev 500kk]	blacksuit	<a href="#">Link</a>
2024-03-09	[ACE Air Cargo]	hunters	<a href="#">Link</a>
2024-03-09	[Watsonclinic.com]	donutleaks	<a href="#">Link</a>
2024-03-06	[Continental Aerospace Technologies]	play	<a href="#">Link</a>
2024-03-08	[redwoodcoastrc.org]	lockbit3	<a href="#">Link</a>
2024-03-08	[PowerRail Distribution]	blacksuit	<a href="#">Link</a>
2024-03-08	[Denninger's ]	medusa	<a href="#">Link</a>
2024-03-08	[SIEA ]	ransomhub	<a href="#">Link</a>
2024-03-08	[Hozzify ]	ransomhub	<a href="#">Link</a>
2024-03-07	[rmhfanchise.com]	lockbit3	<a href="#">Link</a>
2024-03-07	[New York Home Healthcare]	bianlian	<a href="#">Link</a>
2024-03-07	[Palmer Construction Co., Inc]	bianlian	<a href="#">Link</a>
2024-03-07	[en-act-architecture]	qilin	<a href="#">Link</a>
2024-03-07	[Merchant ID ]	ransomhub	<a href="#">Link</a>
2024-03-07	[SP Mundi ]	ransomhub	<a href="#">Link</a>
2024-03-07	[www.duvel.com]	stormous	<a href="#">Link</a>
2024-03-06	[www.loghmanpharma.com]	stormous	<a href="#">Link</a>
2024-03-06	[MainVest]	play	<a href="#">Link</a>
2024-03-06	[C????????? A???????e T?????????]	play	<a href="#">Link</a>
2024-03-05	[Haivision MCS]	medusa	<a href="#">Link</a>
2024-03-06	[Tocci Building Corporation]	medusa	<a href="#">Link</a>
2024-03-06	[JVCKENWOOD ]	medusa	<a href="#">Link</a>
2024-03-06	[American Renal Associates ]	medusa	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-03-06	[US #1364 Federal Credit Union]	medusa	<a href="#">Link</a>
2024-03-06	[viadirectamarketing]	stormous	<a href="#">Link</a>
2024-03-06	[Liquid Environmental Solutions]	incransom	<a href="#">Link</a>
2024-03-06	[Infosoft]	akira	<a href="#">Link</a>
2024-03-06	[brightwires.com.sa]	qilin	<a href="#">Link</a>
2024-03-06	[Medical Billing Specialists]	akira	<a href="#">Link</a>
2024-03-06	[Telecentro]	akira	<a href="#">Link</a>
2024-03-06	[Steiner (Austrian furniture makers)]	akira	<a href="#">Link</a>
2024-03-06	[Biomedical Research Institute]	meow	<a href="#">Link</a>
2024-03-06	[K???o??]	play	<a href="#">Link</a>
2024-03-06	[Kudulis Reisinger Price]	8base	<a href="#">Link</a>
2024-03-06	[Global Zone]	8base	<a href="#">Link</a>
2024-03-06	[Mediplast AB]	8base	<a href="#">Link</a>
2024-03-05	[airbogo]	stormous	<a href="#">Link</a>
2024-03-05	[sunwave.com.cn]	lockbit3	<a href="#">Link</a>
2024-03-05	[SJCME.EDU]	clap	<a href="#">Link</a>
2024-03-05	[central.k12.or.us]	lockbit3	<a href="#">Link</a>
2024-03-05	[iemsc.com]	qilin	<a href="#">Link</a>
2024-03-05	[hawita-gruppe]	qilin	<a href="#">Link</a>
2024-03-05	[Future Generations Foundation]	meow	<a href="#">Link</a>
2024-03-04	[Seven Seas Group]	snatch	<a href="#">Link</a>
2024-03-04	[Paul Davis Restoration]	medusa	<a href="#">Link</a>
2024-03-04	[Veeco]	medusa	<a href="#">Link</a>
2024-03-04	[dismogas]	stormous	<a href="#">Link</a>
2024-03-04	[everplast]	stormous	<a href="#">Link</a>
2024-03-04	[DiVal Safety Equipment, Inc.]	hunters	<a href="#">Link</a>
2024-03-04	[America Chung Nam orACN]	akira	<a href="#">Link</a>

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

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

## 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](https://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](mailto:info@cyberwald.com)

Cyberwald ist ein privates, nicht-kommerzielles Projekt zur Förderung des Bewusstseins für Cybersicherheit.