

---

# Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240513



## 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 . . . . .	11
<b>4 Aktiv ausgenutzte Sicherheitslücken</b>	<b>12</b>
4.1 Exploits der letzten 5 Tage . . . . .	12
4.2 0-Days der letzten 5 Tage . . . . .	16
<b>5 Die Hacks der Woche</b>	<b>19</b>
5.0.1 2007 hat ☒ angerufen ☒, sie wollen ihre Path Traversal zurück (Und der Drop-box Sign Hack) . . . . .	19
<b>6 Cyberangriffe: (Mai)</b>	<b>20</b>
<b>7 Ransomware-Erpressungen: (Mai)</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

#### ***Juniper schließt OpenSSH-Lücken in Junos OS und Junos OS Evolved***

Junos OS und Junos OS Evolved enthalten OpenSSH. Sicherheitslücken darin schließt Juniper nun mit Betriebssystem-Updates.

- [Link](#)

—

#### ***Google Chrome: Exploit für Zero-Day-Lücke gesichtet***

In Googles Webbrowser Chrome klafft eine Sicherheitslücke, für die ein Exploit existiert. Google reagiert mit einem Notfall-Update.

- [Link](#)

—

#### ***Admins müssen selbst handeln: PuTTY-Sicherheitslücke bedroht Citrix Hypervisor***

Um XenCenter für Citrix Hypervisor abzusichern, müssen Admins händisch ein Sicherheitsupdate für das SSH-Tool PuTTY installieren.

- [Link](#)

—

#### ***Angreifer können Kontrolle über BIG-IP-Appliances von F5 erlangen***

Mehrere Sicherheitslücken gefährden BIG-IP Next Central Manager. Updates stehen zum Download bereit.

- [Link](#)

—

#### ***VMware Avi Load Balancer: Rechteauserweiterung zu root möglich***

Im Load Balancer VMware Avi können Angreifer ihre Rechte erhöhen oder unbefugt auf Informationen zugreifen. Updates korrigieren das.

- [Link](#)

—

#### ***Android-Patchday: Angreifer können Rechte im System ausweiten***

Google schließt am Android-Patchday mehrere Lücken, durch die Angreifer ihre Rechte ausweiten können.

- [Link](#)

—

#### ***Trend Micro Antivirus One: Codeschmuggel im macOS-Scanner möglich***

Trend Micros Antivirus One lässt sich durch eine Schwachstelle unter macOS beliebigen Code unterjubeln. Ein Update steht bereit.

- [Link](#)

---

***Sicherheitsupdates: Angreifer können IP-Telefone von Cisco ausspionieren***

Admins sollten zeitnah die abgesicherte Firmware für Ciscos IP-Telefone der Serien 6800, 7800 und 8800 installieren.

- [Link](#)

---

***CISA warnt: Microsoft Smartscreen- und Gitlab-Sicherheitsleck werden angegriffen***

Die US-Cybersicherheitsbehörde CISA hat Angriffe auf eine Lücke im Microsoft Smartscreen und auf eine Gitlab-Schwachstelle gesichtet.

- [Link](#)

---

***Sicherheitsupdates: Angreifer können WLAN-Gateways von Aruba kompromittieren***

Wichtige Patches schließen mehrere Schwachstellen in Mobility Conductor, Mobility Controllers, WLAN Gateways und SD-WAN Gateways von Aruba.

- [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-2023-7028	0.953820000	0.993480000	<a href="#">Link</a>
CVE-2023-6895	0.901600000	0.987730000	<a href="#">Link</a>
CVE-2023-6553	0.922860000	0.989340000	<a href="#">Link</a>
CVE-2023-5360	0.967230000	0.996510000	<a href="#">Link</a>
CVE-2023-4966	0.966680000	0.996330000	<a href="#">Link</a>
CVE-2023-48795	0.962250000	0.995090000	<a href="#">Link</a>
CVE-2023-47246	0.943770000	0.991810000	<a href="#">Link</a>
CVE-2023-46805	0.965580000	0.996070000	<a href="#">Link</a>
CVE-2023-46747	0.970410000	0.997530000	<a href="#">Link</a>
CVE-2023-46604	0.972730000	0.998490000	<a href="#">Link</a>
CVE-2023-43177	0.964020000	0.995590000	<a href="#">Link</a>
CVE-2023-42793	0.970940000	0.997740000	<a href="#">Link</a>
CVE-2023-39143	0.953670000	0.993460000	<a href="#">Link</a>
CVE-2023-38646	0.913020000	0.988540000	<a href="#">Link</a>
CVE-2023-38205	0.922000000	0.989230000	<a href="#">Link</a>
CVE-2023-38203	0.971170000	0.997860000	<a href="#">Link</a>
CVE-2023-38035	0.974190000	0.999330000	<a href="#">Link</a>
CVE-2023-36845	0.966630000	0.996320000	<a href="#">Link</a>
CVE-2023-3519	0.911860000	0.988490000	<a href="#">Link</a>
CVE-2023-35082	0.959780000	0.994590000	<a href="#">Link</a>
CVE-2023-35078	0.968160000	0.996820000	<a href="#">Link</a>
CVE-2023-34993	0.966220000	0.996200000	<a href="#">Link</a>
CVE-2023-34960	0.934040000	0.990630000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-34634	0.918830000	0.988990000	<a href="#">Link</a>
CVE-2023-34362	0.955650000	0.993810000	<a href="#">Link</a>
CVE-2023-34039	0.943170000	0.991730000	<a href="#">Link</a>
CVE-2023-3368	0.916570000	0.988780000	<a href="#">Link</a>
CVE-2023-33246	0.973220000	0.998750000	<a href="#">Link</a>
CVE-2023-32315	0.974090000	0.999260000	<a href="#">Link</a>
CVE-2023-32235	0.914550000	0.988620000	<a href="#">Link</a>
CVE-2023-30625	0.945200000	0.992110000	<a href="#">Link</a>
CVE-2023-30013	0.963050000	0.995290000	<a href="#">Link</a>
CVE-2023-29300	0.969500000	0.997210000	<a href="#">Link</a>
CVE-2023-29298	0.948030000	0.992530000	<a href="#">Link</a>
CVE-2023-28771	0.914030000	0.988600000	<a href="#">Link</a>
CVE-2023-28432	0.935270000	0.990740000	<a href="#">Link</a>
CVE-2023-28121	0.945870000	0.992190000	<a href="#">Link</a>
CVE-2023-27524	0.970430000	0.997540000	<a href="#">Link</a>
CVE-2023-27372	0.973760000	0.999030000	<a href="#">Link</a>
CVE-2023-27350	0.971240000	0.997900000	<a href="#">Link</a>
CVE-2023-26469	0.942400000	0.991600000	<a href="#">Link</a>
CVE-2023-26360	0.962720000	0.995200000	<a href="#">Link</a>
CVE-2023-26035	0.969280000	0.997150000	<a href="#">Link</a>
CVE-2023-25717	0.957880000	0.994220000	<a href="#">Link</a>
CVE-2023-25194	0.969190000	0.997120000	<a href="#">Link</a>
CVE-2023-2479	0.965320000	0.996000000	<a href="#">Link</a>
CVE-2023-24489	0.974200000	0.999340000	<a href="#">Link</a>
CVE-2023-23752	0.932080000	0.990390000	<a href="#">Link</a>
CVE-2023-23397	0.926450000	0.989870000	<a href="#">Link</a>
CVE-2023-23333	0.963260000	0.995380000	<a href="#">Link</a>

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-22527	0.974360000	0.999430000	<a href="#">Link</a>
CVE-2023-22518	0.966350000	0.996260000	<a href="#">Link</a>
CVE-2023-22515	0.972310000	0.998330000	<a href="#">Link</a>
CVE-2023-21839	0.958250000	0.994310000	<a href="#">Link</a>
CVE-2023-21554	0.959160000	0.994480000	<a href="#">Link</a>
CVE-2023-20887	0.963870000	0.995570000	<a href="#">Link</a>
CVE-2023-1671	0.968860000	0.997020000	<a href="#">Link</a>
CVE-2023-0669	0.969750000	0.997300000	<a href="#">Link</a>

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

Fri, 10 May 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](#)

—

Fri, 10 May 2024

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

Ein Angreifer kann mehrere Schwachstellen in ffmpeg ausnutzen, um beliebigen Code auszuführen oder einen 'Denial of Service'-Zustand zu verursachen.

- [Link](#)

—

Fri, 10 May 2024

**[UPDATE] [hoch] Golang Go: Mehrere Schwachstellen**

Ein entfernter anonymer Angreifer kann mehrere Schwachstellen in Golang Go ausnutzen, um beliebigen Code auszuführen oder einen 'Denial of Service'-Zustand zu verursachen.

- [Link](#)

—

Fri, 10 May 2024

**[NEU] [hoch] IBM QRadar SIEM: Mehrere Schwachstellen**



Ein Angreifer kann mehrere Schwachstellen in IBM QRadar SIEM ausnutzen, um beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand herbeizuführen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren, seine Privilegien zu erweitern, einen Cross-Site-Scripting (XSS)-Angriff durchzuführen oder einen nicht spezifizierten Angriff auszuführen.

- [Link](#)

—

Fri, 10 May 2024

**[NEU] [hoch] Juniper JUNOS: Mehrere Schwachstellen**

Ein Angreifer kann mehrere Schwachstellen in Juniper JUNOS im Zusammenhang mit OpenSSH ausnutzen, um Sicherheitsmaßnahmen zu umgehen, beliebigen Code auszuführen oder Dateien zu manipulieren.

- [Link](#)

—

Fri, 10 May 2024

**[NEU] [hoch] Google Chrome: Schwachstelle ermöglicht nicht spezifizierten Angriff**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Google Chrome ausnutzen, um beliebigen Programmcode auszuführen und weitere, nicht spezifizierte Auswirkungen zu verursachen.

- [Link](#)

—

Fri, 10 May 2024

**[NEU] [hoch] Apache OFBiz: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Apache OFBiz ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 10 May 2024

**[NEU] [hoch] Apple iTunes: Schwachstelle ermöglicht Codeausführung und Dos**

Ein entfernter anonymer Angreifer kann eine Schwachstelle in Apple iTunes ausnutzen, um beliebigen Code auszuführen oder einen Denial-of-Service-Zustand auszulösen.

- [Link](#)

—

Fri, 10 May 2024

**[UPDATE] [hoch] Node.js: Schwachstelle ermöglicht Umgehen von Sicherheitsvorkehrungen**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in Node.js ausnutzen, um Sicherheitsvorkehrungen zu umgehen.

- [Link](#)

—

Fri, 10 May 2024

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

Ein Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um beliebigen Programmcode auszuführen, einen Cross-Site-Scripting Angriff durchzuführen, einen Denial of Service Zustand herzustellen und Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

—

Fri, 10 May 2024

**[UPDATE] [hoch] Node.js: Mehrere Schwachstellen ermöglichen Manipulation von Dateien**

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um Dateien zu manipulieren.

- [Link](#)

—

Fri, 10 May 2024

**[UPDATE] [hoch] Node.js: Mehrere Schwachstellen ermöglichen "HTTP request smuggling"**

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um einen "HTTP request smuggling" Angriff durchzuführen.

- [Link](#)

—

Fri, 10 May 2024

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

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um Sicherheitsvorkehrungen zu umgehen oder Dateien zu manipulieren.

- [Link](#)

—

Fri, 10 May 2024

**[UPDATE] [hoch] Node.js: Mehrere Schwachstellen ermöglichen Codeausführung**

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um beliebigen Programmcode auszuführen, um Konfigurationen zu manipulieren und um Sicherheitsmechanismen zu umgehen.

- [Link](#)

—

Fri, 10 May 2024

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

Ein Angreifer kann mehrere Schwachstellen in Node.js ausnutzen, um Informationen offenzulegen oder Dateien zu manipulieren.

- [Link](#)

—

Fri, 10 May 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](#)

—

Fri, 10 May 2024

**[UPDATE] [hoch] IBM Java: Schwachstelle ermöglicht Codeausführung**

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in IBM Java ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Fri, 10 May 2024

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

Ein entfernter authentifizierter Angreifer kann eine Schwachstelle in WordPress ausnutzen, um Sicherheitsmaßnahmen zu umgehen oder beliebigen Code auszuführen.

- [Link](#)

—

Fri, 10 May 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](#)

—

Fri, 10 May 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](#)

—

---

### 3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
5/12/2024	[GLSA-202405-30 : Rebar3: Command Injection]	critical
5/11/2024	[RHEL 6 : poppler (Unpatched Vulnerability)]	critical
5/11/2024	[RHEL 7 : libplist (Unpatched Vulnerability)]	critical
5/11/2024	[RHEL 6 : perl-xml-libxml (Unpatched Vulnerability)]	critical
5/11/2024	[RHEL 6 : irssi (Unpatched Vulnerability)]	critical
5/11/2024	[RHEL 6 : wpa_supplicant (Unpatched Vulnerability)]	critical
5/11/2024	[RHEL 6 : rsyslog (Unpatched Vulnerability)]	critical
5/11/2024	[RHEL 8 : mozilla (Unpatched Vulnerability)]	critical
5/11/2024	[RHEL 6 : thunderbird (Unpatched Vulnerability)]	critical
5/11/2024	[RHEL 5 : squirrelmail (Unpatched Vulnerability)]	critical
5/11/2024	[RHEL 6 : mozilla (Unpatched Vulnerability)]	critical
5/11/2024	[RHEL 7 : mozilla (Unpatched Vulnerability)]	critical
5/11/2024	[RHEL 7 : ibm_jdk (Unpatched Vulnerability)]	critical
5/11/2024	[RHEL 6 : chromium-browser (Unpatched Vulnerability)]	critical
5/12/2024	[Fedora 39 : chromium (2024-1bc17d6ec7)]	high
5/12/2024	[Fedora 40 : chromium (2024-5f84678c08)]	high
5/12/2024	[GLSA-202405-31 : Kubelet: Privilege Escalation]	high
5/12/2024	[GLSA-202405-32 : Mozilla Thunderbird: Multiple Vulnerabilities]	high
5/12/2024	[GLSA-202405-33 : PoDoFo: Multiple Vulnerabilities]	high
5/12/2024	[Debian dsa-5688 : atril - security update]	high
5/12/2024	[FreeBSD : chromium – multiple security fixes (3cf8ea44-1029-11ef-9f97-a8a1599412c6)]	high
5/11/2024	[RHEL 8 : poppler (Unpatched Vulnerability)]	high
5/11/2024	[RHEL 5 : thunderbird (Unpatched Vulnerability)]	high
5/11/2024	[RHEL 8 : tpm (Unpatched Vulnerability)]	high

Datum	Schwachstelle	Bewertung
5/11/2024	[RHEL 5 : struts (Unpatched Vulnerability)]	high
5/11/2024	[RHEL 5 : nspr (Unpatched Vulnerability)]	high
5/11/2024	[RHEL 6 : python-lxml (Unpatched Vulnerability)]	high
5/11/2024	[RHEL 6 : libemf (Unpatched Vulnerability)]	high
5/11/2024	[RHEL 6 : v8 (Unpatched Vulnerability)]	high
5/11/2024	[RHEL 8 : nodejs-glob-parent (Unpatched Vulnerability)]	high
5/11/2024	[RHEL 5 : poppler (Unpatched Vulnerability)]	high
5/11/2024	[RHEL 6 : dmidecode (Unpatched Vulnerability)]	high
5/11/2024	[RHEL 6 : audiofile (Unpatched Vulnerability)]	high
5/11/2024	[RHEL 8 : git (Unpatched Vulnerability)]	high
5/11/2024	[RHEL 7 : jasperrreports (Unpatched Vulnerability)]	high
5/11/2024	[RHEL 5 : wpa_suppl (Unpatched Vulnerability)]	high
5/11/2024	[RHEL 5 : flash-plugin (Unpatched Vulnerability)]	high
5/11/2024	[RHEL 6 : xmlsec1 (Unpatched Vulnerability)]	high
5/11/2024	[AlmaLinux 9 : nodejs:18 (ALSA-2024:2779)]	high

## 4 Aktiv ausgenutzte Sicherheitslücken

### 4.1 Exploits der letzten 5 Tage

“Thu, 09 May 2024

#### **Openmediavault Remote Code Execution / Local Privilege Escalation**

Openmediavault versions prior to 7.0.32 have a vulnerability that occurs when users in the web-admin group enter commands on the crontab by selecting the root shell. As a result of exploiting the vulnerability, authenticated web-admin users can run commands with root privileges and receive reverse shell connections.

- [Link](#)

—

” “Thu, 09 May 2024

#### **RIOT 2024.01 Buffer Overflows / Lack Of Size Checks / Out-Of-Bound Access**

RIOT versions 2024.01 and below suffers from multiple buffer overflows, ineffective size checks, and out-of-bounds memory access vulnerabilities.

- [Link](#)

—

” “Thu, 09 May 2024

***Microsoft PlayReady Complete Client Identity Compromise***

The Security Explorations team has come up with two attack scenarios that make it possible to extract private ECC keys used by a PlayReady client (Windows SW DRM scenario) for the communication with a license server and identity purposes. Proof of concept included.

- [Link](#)

—

” “Thu, 09 May 2024

***Panel Amadey.d.c MVID-2024-0680 Cross Site Scripting***

Panel Amadey.d.c malware suffers from cross site scripting vulnerabilities.

- [Link](#)

—

” “Thu, 09 May 2024

***Clinic Queuing System 1.0 Remote Code Execution***

Clinic Queuing System version 1.0 suffers from a remote code execution vulnerability.

- [Link](#)

—

” “Thu, 09 May 2024

***iboss Secure Web Gateway Cross Site Scripting***

iboss Secure Web Gateway versions prior to 10.2.0 suffer from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Thu, 09 May 2024

***POMS PHP 1.0 SQL Injection / Shell Upload***

POMS PHP version 1.0 suffers from remote shell upload and remote SQL injection vulnerabilities.

- [Link](#)

—

” “Thu, 09 May 2024

***Kortex 1.0 SQL Injection***

Kortex version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Thu, 09 May 2024

**Drupal-Wiki 8.31 / 8.30 Cross Site Scripting**

Drupal-Wiki versions 8.30 and 8.31 suffer from multiple persistent cross site scripting vulnerabilities.

- [Link](#)

—

” “Mon, 06 May 2024

**Systemd Insecure PTY Handling**

Systemd-run/run0 allocates user-owned ptys and attaches the slave to high privilege programs without changing ownership or locking the pty slave.

- [Link](#)

—

” “Mon, 06 May 2024

**Microsoft PlayReady Toolkit**

The Microsoft PlayReady toolkit assists with fake client device identity generation, acquisition of license and content keys for encrypted content, and much more. It demonstrates weak content protection in the environment of CANAL+. The proof of concept exploit 3 year old vulnerabilities in CANAL+ STB devices, which make it possible to gain code execution access to target STB devices over an IP network.

- [Link](#)

—

” “Mon, 06 May 2024

**Docker Privileged Container Kernel Escape**

This Metasploit module performs a container escape onto the host as the daemon user. It takes advantage of the SYS\_MODULE capability. If that exists and the linux headers are available to compile on the target, then we can escape onto the host.

- [Link](#)

—

” “Fri, 03 May 2024

**SOPanning 1.52.00 SQL Injection**

SOPanning version 1.52.00 suffers from a remote SQL injection vulnerability in projects.php.

- [Link](#)

—

” “Fri, 03 May 2024

**SOPanning 1.52.00 Cross Site Request Forgery**

SOPanning version 1.52.00 suffers from a cross site request forgery vulnerability in xajax\_server.php.

- [Link](#)

—

” “Fri, 03 May 2024

**SOPanning 1.52.00 Cross Site Scripting**

SOPlanning version 1.52.00 suffers from a cross site scripting vulnerability in groupe\_save.php.

- [Link](#)

—

” “Thu, 02 May 2024

***htmlLawed 1.2.5 Remote Command Execution***

htmlLawed versions 1.2.5 and below proof of concept remote command execution exploit.

- [Link](#)

—

” “Wed, 01 May 2024

***Packet Storm New Exploits For April, 2024***

This archive contains all of the 132 exploits added to Packet Storm in April, 2024.

- [Link](#)

—

” “Wed, 01 May 2024

***Online Tours And Travels Management System 1.0 SQL Injection***

Online Tours and Travels Management System version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Tue, 30 Apr 2024

***Windows PspBuildCreateProcessContext Double-Fetch / Buffer Overflow***

Proof of concept code that demonstrates how the Windows kernel suffers from a privilege escalation vulnerability due to a double-fetch in PspBuildCreateProcessContext that leads to a stack buffer overflow.

- [Link](#)

—

” “Tue, 30 Apr 2024

***Windows NtQueryInformationThread Double-Fetch / Arbitrary Write***

Proof of concept code that demonstrates how the Windows kernel suffers from a privilege escalation vulnerability due to a double-fetch in NtQueryInformationThread that leads to an arbitrary write.

- [Link](#)

—

” “Tue, 30 Apr 2024

***undefinedExploiting The NT Kernel In 24H2undefined***

This is the full Windows privilege escalation exploit produced from the blog Exploiting the NT Kernel in 24H2: New Bugs in Old Code and Side Channels Against KASLR.

- [Link](#)

—



” “Tue, 30 Apr 2024

**osCommerce 4 Cross Site Scripting**

osCommerce version 4 suffers from a cross site scripting vulnerability. This finding is another vector of attack for this issue already discovered by the same researcher in November of 2023.

- [Link](#)

—

” “Mon, 29 Apr 2024

**Kemp LoadMaster Unauthenticated Command Injection**

This Metasploit module exploits an unauthenticated command injection vulnerability in Progress Kemp LoadMaster in the authorization header after version 7.2.48.1. The following versions are patched: 7.2.59.2 (GA), 7.2.54.8 (LTSF), and 7.2.48.10 (LTS).

- [Link](#)

—

” “Mon, 29 Apr 2024

**Doctor Appointment Management System 1.0 Cross Site Scripting**

Doctor Appointment Management System version 1.0 suffers from a cross site scripting vulnerability.

- [Link](#)

—

” “Mon, 29 Apr 2024

**ESET NOD32 Antivirus 17.1.11.0 Unquoted Service Path**

ESET NOD32 Antivirus version 17.1.11.0 suffers from an unquoted service path vulnerability.

- [Link](#)

—

”

## 4.2 0-Days der letzten 5 Tage

“Thu, 09 May 2024

**ZDI-24-439: Microsoft Windows Bluetooth AVDTP Protocol Integer Underflow Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 09 May 2024

**ZDI-24-438: Dassault Systèmes eDrawings Viewer DXF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 09 May 2024

**ZDI-24-437: Dassault Systèmes eDrawings Viewer DXF File Parsing Type Confusion Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 09 May 2024

**ZDI-24-436: Dassault Systèmes eDrawings Viewer DXF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 09 May 2024

**ZDI-24-435: Dassault Systèmes eDrawings Viewer DXF File Parsing Type Confusion Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 09 May 2024

**ZDI-24-434: Dassault Systèmes eDrawings Viewer SAT File Parsing Uninitialized Variable Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 09 May 2024

**ZDI-24-433: Dassault Systèmes eDrawings Viewer DXF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 09 May 2024

**ZDI-24-432: Dassault Systèmes eDrawings Viewer JT File Parsing Memory Corruption Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 09 May 2024

**ZDI-24-431: Dassault Systèmes eDrawings Viewer DXF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 09 May 2024

**ZDI-24-430: Dassault Systèmes eDrawings Viewer JT File Parsing Heap-based Buffer Overflow Remote Code Execution Vulnerability**

- [Link](#)

—

” “Thu, 09 May 2024

***ZDI-24-429: Dassault Systèmes eDrawings Viewer DXF File Parsing Out-Of-Bounds Write Remote Code Execution Vulnerability***

- [Link](#)

—

” “Thu, 09 May 2024

***ZDI-24-428: Dassault Systèmes eDrawings Viewer JT File Parsing Memory Corruption Remote Code Execution Vulnerability***

- [Link](#)

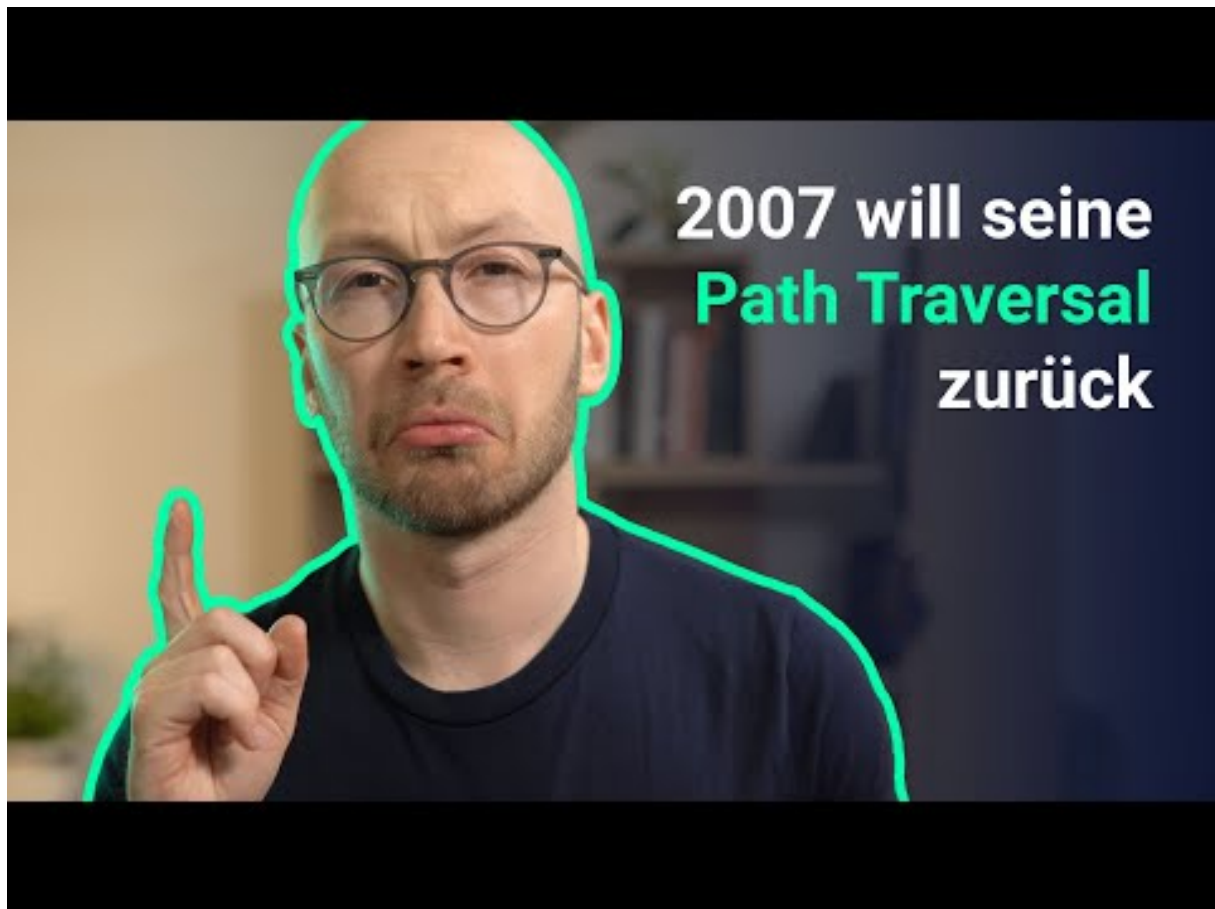
—

”

## 5 Die Hacks der Woche

mit Martin Haunschmid

### 5.0.1 2007 hat 0x00000000 angerufen 0x00000000, sie wollen ihre Path Traversal zurück (Und der Dropbox Sign Hack)



[Zum Youtube Video](#)

## 6 Cyberangriffe: (Mai)

Datum	Opfer	Land	Information
2024-05-08	Ascension Health	[USA]	<a href="#">Link</a>
2024-05-06	DocGo	[USA]	<a href="#">Link</a>
2024-05-06	Key Tronic Corporation	[USA]	<a href="#">Link</a>
2024-05-05	Wichita	[USA]	<a href="#">Link</a>
2024-05-05	Université de Sienne	[ITA]	<a href="#">Link</a>
2024-05-05	Concord Public Schools et Concord-Carlisle Regional School District	[USA]	<a href="#">Link</a>
2024-05-04	Regional Cancer Center (RCC)	[IND]	<a href="#">Link</a>
2024-05-03	Eucatex (EUCA4)	[BRA]	<a href="#">Link</a>
2024-05-03	Cégep de Lanaudière	[CAN]	<a href="#">Link</a>
2024-05-03	Coradix-Magnescan	[FRA]	<a href="#">Link</a>
2024-05-02	Umeå universitet	[SWE]	<a href="#">Link</a>
2024-05-01	Brandywine Realty Trust	[USA]	<a href="#">Link</a>

## 7 Ransomware-Erpressungen: (Mai)

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-03	[Seaman's Mechanical]	incransom	<a href="#">Link</a>
2024-05-06	[Deeside Timberframe]	incransom	<a href="#">Link</a>
2024-05-12	[McSweeney / Langevin]	qilin	<a href="#">Link</a>
2024-05-11	[NITEK International LLC]	medusa	<a href="#">Link</a>
2024-05-11	[National Metalwares, L.P]	medusa	<a href="#">Link</a>
2024-05-12	[Romeo Pitaro Injury & Litigation Lawyers]	bianlian	<a href="#">Link</a>
2024-05-11	[NHS (press update)]	incransom	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-11	[Jackson County]	blacksuit	<a href="#">Link</a>
2024-05-11	[For sale. Contact through admin.]	blacksuit	<a href="#">Link</a>
2024-05-10	[21stcenturyvitamins.com]	lockbit3	<a href="#">Link</a>
2024-05-10	[Montgomery County Board of Developmental Disabilities Services]	blacksuit	<a href="#">Link</a>
2024-05-10	[LiveHelpNow]	play	<a href="#">Link</a>
2024-05-10	[NK Parts Industries]	play	<a href="#">Link</a>
2024-05-10	[Badger Tag & Label]	play	<a href="#">Link</a>
2024-05-10	[Haumiller Engineering]	play	<a href="#">Link</a>
2024-05-10	[Barid soft]	stormous	<a href="#">Link</a>
2024-05-10	[Pella]	hunters	<a href="#">Link</a>
2024-05-10	[Reading Electric]	akira	<a href="#">Link</a>
2024-05-10	[Kuhn Rechtsanwlte GmbH]	monti	<a href="#">Link</a>
2024-05-10	[colonialsd.org]	lockbit3	<a href="#">Link</a>
2024-05-09	[wisconsinindustrialcoatings.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[amsoft.cl]	lockbit3	<a href="#">Link</a>
2024-05-09	[cultivarnet.com.br]	lockbit3	<a href="#">Link</a>
2024-05-09	[ecotruck.com.br]	lockbit3	<a href="#">Link</a>
2024-05-09	[iaconnecticut.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[incegroup.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[contest.omg]	lockbit3	<a href="#">Link</a>
2024-05-05	[Banco central argentina]	zerotolerance	<a href="#">Link</a>
2024-05-09	[Administração do Porto de São Francisco do Sul (APSFS)]	ransomhub	<a href="#">Link</a>
2024-05-09	[lavalpoincon.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[ccimp.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[ufresources.com]	lockbit3	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-09	[cloudminds.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[calvia.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[manusa.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[habeco.com.vn]	lockbit3	<a href="#">Link</a>
2024-05-09	[rehub.ie]	lockbit3	<a href="#">Link</a>
2024-05-09	[torrepacheco.es]	lockbit3	<a href="#">Link</a>
2024-05-09	[ccofva.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[dagma.com.ar]	lockbit3	<a href="#">Link</a>
2024-05-09	[Edlong]	qilin	<a href="#">Link</a>
2024-05-09	[dpkv.cz]	lockbit3	<a href="#">Link</a>
2024-05-09	[hetero.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[vikrantsprings.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[doublehorse.in]	lockbit3	<a href="#">Link</a>
2024-05-09	[iitm.ac.in]	lockbit3	<a href="#">Link</a>
2024-05-09	[cttxpress.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[garage-cretot.fr]	lockbit3	<a href="#">Link</a>
2024-05-09	[hotel-ostella.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[vm3fincas.es]	lockbit3	<a href="#">Link</a>
2024-05-09	[thaiagri.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[tegaindustries.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[kioti.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[taylorcrane.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[grc-c.co.il]	lockbit3	<a href="#">Link</a>
2024-05-09	[mogaisrael.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[ultragasmexico.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[eif.org.na]	lockbit3	<a href="#">Link</a>
2024-05-09	[auburnpikapp.org]	lockbit3	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-09	[acla-werke.com]	lockbit3	Link
2024-05-09	[college-stemarie-elven.org]	lockbit3	Link
2024-05-09	[snk.sk]	lockbit3	Link
2024-05-09	[mutualclubunion.com.ar]	lockbit3	Link
2024-05-09	[rfca.com]	lockbit3	Link
2024-05-09	[hpo.pe]	lockbit3	Link
2024-05-09	[spu.ac.th]	lockbit3	Link
2024-05-09	[livia.in]	lockbit3	Link
2024-05-09	[cinealbeniz.com]	lockbit3	Link
2024-05-09	[truehomesusa.com]	lockbit3	Link
2024-05-09	[uniter.net]	lockbit3	Link
2024-05-09	[itss.com.tr]	lockbit3	Link
2024-05-09	[elements-ing.com]	lockbit3	Link
2024-05-09	[heartlandhealthcenter.org]	lockbit3	Link
2024-05-09	[dsglobaltech.com]	lockbit3	Link
2024-05-09	[alian.mx]	lockbit3	Link
2024-05-09	[evw.k12.mn.us]	lockbit3	Link
2024-05-09	[mpeprevencion.com]	lockbit3	Link
2024-05-09	[binder.de]	lockbit3	Link
2024-05-09	[interfashion.it]	lockbit3	Link
2024-05-09	[vstar.in]	lockbit3	Link
2024-05-09	[brfibra.com]	lockbit3	Link
2024-05-09	[museu-goeldi.br]	lockbit3	Link
2024-05-09	[doxim.com]	lockbit3	Link
2024-05-09	[essinc.com]	lockbit3	Link
2024-05-09	[sislocar.com]	lockbit3	Link
2024-05-09	[depenning.com]	lockbit3	Link



Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-09	[asafoot.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[frankmiller.com]	blacksuit	<a href="#">Link</a>
2024-05-09	[vitema.vi.gov]	lockbit3	<a href="#">Link</a>
2024-05-09	[snapethorpeprimary.co.uk]	lockbit3	<a href="#">Link</a>
2024-05-09	[agencavisystems.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[salmonesaysen.cl]	lockbit3	<a href="#">Link</a>
2024-05-09	[kowessex.co.uk]	lockbit3	<a href="#">Link</a>
2024-05-09	[totto.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[randi-group.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[grupopm.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[ondozabal.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[orsiniimballaggi.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[vinatiorganics.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[peninsulacrane.com]	lockbit3	<a href="#">Link</a>
2024-05-09	[brockington.leics.sch.uk]	lockbit3	<a href="#">Link</a>
2024-05-09	[cargotrinidad.com]	lockbit3	<a href="#">Link</a>
2024-05-02	[Pinnacle Orthopaedics]	incransom	<a href="#">Link</a>
2024-05-09	[Protected: HIDE NAME]	medusalocker	<a href="#">Link</a>
2024-05-09	[Zuber Gardner CPAs]	everest	<a href="#">Link</a>
2024-05-09	[Corr & Corr]	everest	<a href="#">Link</a>
2024-05-08	[rexmoore.com]	embargo	<a href="#">Link</a>
2024-05-08	[Northeast Orthopedics and Sports Medicine]	dAn0n	<a href="#">Link</a>
2024-05-08	[Glenwood Management]	dAn0n	<a href="#">Link</a>
2024-05-08	[College Park Industries]	dAn0n	<a href="#">Link</a>
2024-05-08	[Holstein Association USA]	qilin	<a href="#">Link</a>
2024-05-08	[Unimed Vales do Taquari e Rio Pardo]	rhysida	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-08	[Electric Mirror Inc]	incransom	<a href="#">Link</a>
2024-05-08	[Richelieu Foods]	hunters	<a href="#">Link</a>
2024-05-08	[Trade-Mark Industrial]	hunters	<a href="#">Link</a>
2024-05-08	[Dragon Tax and Management INC]	bianlian	<a href="#">Link</a>
2024-05-08	[Mewborn & DeSelms]	blacksuit	<a href="#">Link</a>
2024-05-07	[Merritt Properties, LLC]	medusa	<a href="#">Link</a>
2024-05-07	[Autobell Car Wash, Inc]	medusa	<a href="#">Link</a>
2024-05-08	[fortify.pro]	apt73	<a href="#">Link</a>
2024-05-06	[Electric Mirror]	incransom	<a href="#">Link</a>
2024-05-07	[Intuitae]	qilin	<a href="#">Link</a>
2024-05-07	[Tholen Building Technology Group]	qilin	<a href="#">Link</a>
2024-05-07	[williamsrdm.com]	qilin	<a href="#">Link</a>
2024-05-07	[inforius]	qilin	<a href="#">Link</a>
2024-05-07	[Kamo Jou Trading ]	ransomhub	<a href="#">Link</a>
2024-05-07	[wichita.gov]	lockbit3	<a href="#">Link</a>
2024-05-01	[City of Buckeye (buckeyeaz.gov)]	incransom	<a href="#">Link</a>
2024-05-07	[Hibser Yamauchi Architects]	hunters	<a href="#">Link</a>
2024-05-07	[Noritsu America Corp.]	hunters	<a href="#">Link</a>
2024-05-07	[Autohaus Ebert]	metaencryptor	<a href="#">Link</a>
2024-05-07	[Elbers GmbH & Co. KG]	metaencryptor	<a href="#">Link</a>
2024-05-07	[Jetson Specialty Marketing Services, Inc.]	metaencryptor	<a href="#">Link</a>
2024-05-07	[Vega Reederei GmbH & Co. KG]	metaencryptor	<a href="#">Link</a>
2024-05-07	[Max Wild GmbH]	metaencryptor	<a href="#">Link</a>
2024-05-07	[woldae.com]	abyss	<a href="#">Link</a>
2024-05-07	[Information Integration Experts]	dAn0n	<a href="#">Link</a>
2024-05-06	[One Toyota of Oakland ]	medusa	<a href="#">Link</a>
2024-05-07	[Chemring Group ]	medusa	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-07	[lalengineering]	ransomhub	<a href="#">Link</a>
2024-05-07	[skanlog.com]	lockbit3	<a href="#">Link</a>
2024-05-07	[ctc-corp.net]	lockbit3	<a href="#">Link</a>
2024-05-07	[uslinen.com]	lockbit3	<a href="#">Link</a>
2024-05-07	[tu-ilmenau.de]	lockbit3	<a href="#">Link</a>
2024-05-07	[thede-culpepper.com]	lockbit3	<a href="#">Link</a>
2024-05-07	[kimmelcleaners.com]	lockbit3	<a href="#">Link</a>
2024-05-07	[emainc.net]	lockbit3	<a href="#">Link</a>
2024-05-07	[southernspecialtysupply.com]	lockbit3	<a href="#">Link</a>
2024-05-07	[lenmed.co.za]	lockbit3	<a href="#">Link</a>
2024-05-07	[churchill-linen.com]	lockbit3	<a href="#">Link</a>
2024-05-07	[rollingfields.com]	lockbit3	<a href="#">Link</a>
2024-05-07	[srg-plc.com]	lockbit3	<a href="#">Link</a>
2024-05-07	[gorrias-mercedes-benz.fr]	lockbit3	<a href="#">Link</a>
2024-05-05	[SBC Global, Bitfinex, Coinmama, and Rutgers University Part 2 Leak]	flocker	<a href="#">Link</a>
2024-05-07	[Central Florida Equipment]	play	<a href="#">Link</a>
2024-05-07	[High Performance Services]	play	<a href="#">Link</a>
2024-05-07	[Mauritzon]	play	<a href="#">Link</a>
2024-05-07	[Somerville]	play	<a href="#">Link</a>
2024-05-07	[Donco Air]	play	<a href="#">Link</a>
2024-05-07	[Affordable Payroll & Bookkeeping Services]	play	<a href="#">Link</a>
2024-05-07	[Utica Mack]	play	<a href="#">Link</a>
2024-05-07	[KC Scout]	play	<a href="#">Link</a>
2024-05-07	[Sentry Data Management]	play	<a href="#">Link</a>
2024-05-07	[aletech.com.br]	darkvault	<a href="#">Link</a>
2024-05-07	[Young Consulting]	blacksuit	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-06	[Thaayakam LTD ]	ransomhub	<a href="#">Link</a>
2024-05-06	[The Weinstein Firm]	qilin	<a href="#">Link</a>
2024-05-06	[Nikolaus & Hohenadel]	bianlian	<a href="#">Link</a>
2024-05-06	[NRS Healthcare ]	ransomhub	<a href="#">Link</a>
2024-05-06	[gammarenax.ch]	lockbit3	<a href="#">Link</a>
2024-05-06	[oraclinical.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[acsistemas.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[cpashin.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[epr-groupe.fr]	lockbit3	<a href="#">Link</a>
2024-05-06	[isee.biz]	lockbit3	<a href="#">Link</a>
2024-05-06	[cdev.gc.ca]	lockbit3	<a href="#">Link</a>
2024-05-06	[netspectrum.ca]	lockbit3	<a href="#">Link</a>
2024-05-06	[qstartlabs.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[syntax-architektur.at]	lockbit3	<a href="#">Link</a>
2024-05-06	[carespring.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[grand-indonesia.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[remagroup.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[telekom.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[aev-iledefrance.fr]	lockbit3	<a href="#">Link</a>
2024-05-06	[elarabygroup.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[thebiglifegroup.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[sonoco.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[ville-bouchemaine.fr]	lockbit3	<a href="#">Link</a>
2024-05-06	[eskarabajo.mx]	darkvault	<a href="#">Link</a>
2024-05-06	[Rafael Viñoly Architects]	blacksuit	<a href="#">Link</a>
2024-05-06	[TRC Talent Solutions]	blacksuit	<a href="#">Link</a>
2024-05-06	[M2E Consulting Engineers]	akira	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-06	[sunray.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[eviivo.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[kras.hr]	lockbit3	<a href="#">Link</a>
2024-05-06	[tdt.aero]	lockbit3	<a href="#">Link</a>
2024-05-06	[svenskakyrkan.se]	lockbit3	<a href="#">Link</a>
2024-05-06	[htcinc.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[irc.be]	lockbit3	<a href="#">Link</a>
2024-05-06	[geotechenv.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[ishoppes.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[parat-techology.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[getcloudapp.com]	lockbit3	<a href="#">Link</a>
2024-05-06	[yucatan.gob.mx]	lockbit3	<a href="#">Link</a>
2024-05-06	[arcus.pl]	lockbit3	<a href="#">Link</a>
2024-05-06	[Nestoil]	blacksuit	<a href="#">Link</a>
2024-05-06	[Patterson & Rothwell Ltd]	medusa	<a href="#">Link</a>
2024-05-06	[Boyden]	medusa	<a href="#">Link</a>
2024-05-06	[W.F. Whelan]	medusa	<a href="#">Link</a>
2024-05-05	[SBC Global, Bitfinex, Coinmama, and Rutgers University Part 2]	flocker	<a href="#">Link</a>
2024-05-05	[Seneca Nation Health System]	incransom	<a href="#">Link</a>
2024-05-05	[SBC Global, Bitfinex, Coinmom, and Rutgers University Part 2]	flocker	<a href="#">Link</a>
2024-05-04	[COMPEXLEGAL.COM]	clop	<a href="#">Link</a>
2024-05-04	[ikfhomefinance.com]	darkvault	<a href="#">Link</a>
2024-05-04	[The Islamic Emirat of Afghanistan National Environmental Protection Agency ]	ransomhub	<a href="#">Link</a>
2024-05-04	[Accounting Professionals LLC. Price, Breazeale & Chastang]	everest	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-04	[cmactrans.com]	blackbasta	<a href="#">Link</a>
2024-05-04	[ids-michigan.com]	blackbasta	<a href="#">Link</a>
2024-05-04	[provencherroy.ca]	blackbasta	<a href="#">Link</a>
2024-05-04	[swisspro.ch]	blackbasta	<a href="#">Link</a>
2024-05-04	[olsonsteel.com]	blackbasta	<a href="#">Link</a>
2024-05-04	[teaspa.it]	blackbasta	<a href="#">Link</a>
2024-05-04	[ayesa.com]	blackbasta	<a href="#">Link</a>
2024-05-04	[synlab.com]	blackbasta	<a href="#">Link</a>
2024-05-04	[active-pcb.com]	blackbasta	<a href="#">Link</a>
2024-05-04	[gai-it.com]	blackbasta	<a href="#">Link</a>
2024-05-04	[Macildowie Associates]	medusa	<a href="#">Link</a>
2024-05-03	[Dr Charles A Evans]	qilin	<a href="#">Link</a>
2024-05-03	[Universidad Nacional Autónoma de México ]	ransomhub	<a href="#">Link</a>
2024-05-03	[thelawrencegroup.com]	blackbasta	<a href="#">Link</a>
2024-05-02	[sharik]	stormous	<a href="#">Link</a>
2024-05-02	[tdra]	stormous	<a href="#">Link</a>
2024-05-02	[fanr.gov.ae]	stormous	<a href="#">Link</a>
2024-05-02	[Bayanat]	stormous	<a href="#">Link</a>
2024-05-02	[kidx]	stormous	<a href="#">Link</a>
2024-05-03	[MCS]	qilin	<a href="#">Link</a>
2024-05-03	[Tohlen Building Technology Group]	qilin	<a href="#">Link</a>
2024-05-03	[Stainless Foundry & Engineering]	play	<a href="#">Link</a>
2024-05-02	[Ayoub & associates CPA Firm]	everest	<a href="#">Link</a>
2024-05-02	[www.servicepower.com]	apt73	<a href="#">Link</a>
2024-05-02	[www.credio.eu]	apt73	<a href="#">Link</a>
2024-05-02	[Lopez Hnos]	rhysida	<a href="#">Link</a>
2024-05-02	[GWF Frankenwein]	raworld	<a href="#">Link</a>

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-02	[Reederei Jüngerhans]	raworld	<a href="#">Link</a>
2024-05-02	[extraco.ae]	ransomhub	<a href="#">Link</a>
2024-05-02	[watergate]	qilin	<a href="#">Link</a>
2024-05-02	[Imedi L]	akira	<a href="#">Link</a>
2024-05-01	[Azteca Tax Systems]	bianlian	<a href="#">Link</a>
2024-05-01	[Clinica de Salud del Valle de Salinas]	bianlian	<a href="#">Link</a>
2024-05-01	[cochraneglobal.com]	underground	<a href="#">Link</a>
2024-05-01	[UK government]	snatch	<a href="#">Link</a>
2024-05-01	[hookerfurniture.com]	lockbit3	<a href="#">Link</a>
2024-05-01	[alimmigration.com]	lockbit3	<a href="#">Link</a>
2024-05-01	[anatomage.com]	lockbit3	<a href="#">Link</a>
2024-05-01	[bluegrasstechnologies.net]	lockbit3	<a href="#">Link</a>
2024-05-01	[PINNACLEENGR.COM]	clop	<a href="#">Link</a>
2024-05-01	[MCKINLEYPACKAGING.COM]	clop	<a href="#">Link</a>
2024-05-01	[PILOTPEN.COM]	clop	<a href="#">Link</a>
2024-05-01	[colonial.edu]	lockbit3	<a href="#">Link</a>
2024-05-01	[cordish.com]	lockbit3	<a href="#">Link</a>
2024-05-01	[concorr.com]	lockbit3	<a href="#">Link</a>
2024-05-01	[yupousa.com]	lockbit3	<a href="#">Link</a>
2024-05-01	[peaseinc.com]	lockbit3	<a href="#">Link</a>
2024-05-01	[bdcm.com]	blackbasta	<a href="#">Link</a>
2024-05-01	[MORTON WILLIAMS]	everest	<a href="#">Link</a>
2024-05-03	[melting-mind.de]	apt73	<a href="#">Link</a>
2024-05-21	[netscout.com]	dispossessor	<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.