
Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240531



Inhaltsverzeichnis

1 Editorial	2
2 Security-News	3
2.1 Heise - Security-Alert	3
3 Sicherheitslücken	4
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
4 Aktiv ausgenutzte Sicherheitslücken	13
4.1 Exploits der letzten 5 Tage	13
4.2 0-Days der letzten 5 Tage	17
5 Die Hacks der Woche	20
5.0.1 FCK Stalkerware.	20
6 Cyberangriffe: (Mai)	21
7 Ransomware-Erpressungen: (Mai)	22
8 Quellen	42
8.1 Quellenverzeichnis	42
9 Impressum	44

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

IT-Monitoring: Checkmk schließt Lücke, die Änderung von Dateien ermöglicht

Eine Sicherheitslücke in der Monitoring-Software Checkmk ermöglicht Angreifern, unbefugt lokale Dateien auf dem Checkmk-Server zu lesen und zu schreiben.

- [Link](#)

—

Notfallpatch: Angreifer attackieren VPN-Verbindungen von Checkpoint Gateways

Checkpoint hat ein Notfall-Sicherheitsupdate veröffentlicht. Derzeit haben Angreifer Network Security Gateways wie Quantum Maestro im Visier.

- [Link](#)

—

Foxit PDF Reader: Halbherzige Zertifikatprüfung ermöglicht Rechteausweitung

Die Update-Routinen vom Foxit PDF Reader prüfen Zertifikate nicht richtig. Angreifer können dadurch ihre Rechte ausweiten.

- [Link](#)

—

Proof-of-Concept-Exploits für kritische FortiSIEM-Lücken: Jetzt patchen!

IT-Sicherheitsforscher haben für kritische Sicherheitslücken in FortiSIEM Proof-of-Concept-Exploits veröffentlicht. Höchste Zeit, die Updates zu installieren.

- [Link](#)

—

Supportende: Rechte-Sicherheitslücke gefährdet Ivanti Endpoint Manager 2021

Angreifer können Schadcode mit erhöhten Rechten ausführen. Admins müssen Ivanti EPM auf eine noch unterstützte Version upgraden.

- [Link](#)

—

Kritische Sicherheitslücke gewährt Angreifern Zugriff auf TP-Link-Router C5400X

Der TP-Link-WLAN-Router C5400X ist verwundbar. Ein Sicherheitspatch schließt eine kritische Schwachstelle.

- [Link](#)

—

Windows Server 2019: Aktualisiertes Sicherheitsupdate behebt Installationsfehler

Das Sicherheitsupdate für Windows Server 2019 schlug mit den Fehlernummern 0x800f0982 und 0x80004005 fehl. Ein aktualisiertes Update ist verfügbar.

- [Link](#)

GitLab: Accountübernahme nach 1-Klick-Attacke möglich

Mehrere Sicherheitslücken in GitLab gefährden Systeme. Gegen mögliche Attacken gerüstete Versionen stehen zum Download bereit.

- [Link](#)

Google Chrome: Vierte bereits missbrauchte Zero-Day-Lücke in zwei Wochen

Google schließt eine Zero-Day-Lücke im Chrome-Webbrowser, die bereits angegriffen wird. Die vierte in zwei Wochen.

- [Link](#)

Workaround vonnöten: Kritische Lücken bedrohen Ivanti Endpoint Manager

Gegen mögliche Schadcode-Attacken gerüstete Ivanti-EPM-Versionen lassen noch auf sich warten. Bislang gibt es nur einen Hot Patch für eine Version.

- [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	0.959520000	0.994650000	Link
CVE-2023-6553	0.923550000	0.989570000	Link
CVE-2023-5360	0.965120000	0.995960000	Link
CVE-2023-4966	0.969890000	0.997380000	Link
CVE-2023-48795	0.959010000	0.994530000	Link
CVE-2023-47246	0.935450000	0.990920000	Link
CVE-2023-46805	0.965580000	0.996130000	Link
CVE-2023-46747	0.971160000	0.997910000	Link
CVE-2023-46604	0.922790000	0.989470000	Link
CVE-2023-4542	0.922430000	0.989420000	Link
CVE-2023-43208	0.963060000	0.995410000	Link
CVE-2023-43177	0.964020000	0.995690000	Link
CVE-2023-42793	0.970940000	0.997790000	Link
CVE-2023-41265	0.914120000	0.988780000	Link
CVE-2023-39143	0.948440000	0.992790000	Link
CVE-2023-38646	0.908390000	0.988330000	Link
CVE-2023-38205	0.928030000	0.990120000	Link
CVE-2023-38203	0.970370000	0.997560000	Link
CVE-2023-38146	0.905210000	0.988090000	Link
CVE-2023-38035	0.975060000	0.999830000	Link
CVE-2023-36845	0.966630000	0.996350000	Link
CVE-2023-3519	0.911860000	0.988620000	Link
CVE-2023-35082	0.968540000	0.996980000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-35078	0.968250000	0.996890000	Link
CVE-2023-34993	0.967190000	0.996520000	Link
CVE-2023-34960	0.933660000	0.990740000	Link
CVE-2023-34634	0.923550000	0.989580000	Link
CVE-2023-34362	0.961530000	0.995040000	Link
CVE-2023-34039	0.935790000	0.990960000	Link
CVE-2023-3368	0.932830000	0.990650000	Link
CVE-2023-33246	0.972320000	0.998390000	Link
CVE-2023-32315	0.974090000	0.999270000	Link
CVE-2023-32235	0.914550000	0.988800000	Link
CVE-2023-30625	0.950680000	0.993120000	Link
CVE-2023-30013	0.963050000	0.995410000	Link
CVE-2023-29300	0.969500000	0.997250000	Link
CVE-2023-29298	0.948030000	0.992700000	Link
CVE-2023-28771	0.918640000	0.989150000	Link
CVE-2023-28432	0.938730000	0.991310000	Link
CVE-2023-28121	0.932700000	0.990640000	Link
CVE-2023-27524	0.971240000	0.997960000	Link
CVE-2023-27372	0.973760000	0.999050000	Link
CVE-2023-27350	0.971070000	0.997850000	Link
CVE-2023-26469	0.942400000	0.991740000	Link
CVE-2023-26360	0.962980000	0.995390000	Link
CVE-2023-26035	0.969280000	0.997190000	Link
CVE-2023-25717	0.956860000	0.994170000	Link
CVE-2023-25194	0.968000000	0.996830000	Link
CVE-2023-2479	0.965320000	0.996050000	Link
CVE-2023-24489	0.973760000	0.999050000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-23752	0.932080000	0.990540000	Link
CVE-2023-23397	0.922480000	0.989430000	Link
CVE-2023-23333	0.963260000	0.995470000	Link
CVE-2023-22527	0.974590000	0.999560000	Link
CVE-2023-22518	0.962670000	0.995290000	Link
CVE-2023-22515	0.973130000	0.998750000	Link
CVE-2023-21839	0.959090000	0.994560000	Link
CVE-2023-21554	0.955760000	0.993990000	Link
CVE-2023-20887	0.963500000	0.995530000	Link
CVE-2023-1698	0.907920000	0.988320000	Link
CVE-2023-1671	0.969090000	0.997130000	Link
CVE-2023-0669	0.969690000	0.997310000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Wed, 29 May 2024

[NEU] [hoch] OpenSSL: Schwachstelle ermöglicht Codeausführung, Datenmanipulation, Offenlegung von Informationen und Dos

Ein entfernter anonymer Angreifer kann eine Schwachstelle in OpenSSL ausnutzen, um beliebigen Code auszuführen, einen Denial-of-Service-Zustand zu verursachen, vertrauliche Informationen offenzulegen und Daten zu manipulieren.

- [Link](#)

—

Wed, 29 May 2024

[UPDATE] [hoch] git: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer oder ein lokaler authentifizierter Angreifer kann mehrere Schwachstellen in git ausnutzen, um beliebigen Programmcode auszuführen und die Sicherheitsmaßnahmen zu umgehen.

- [Link](#)

—

Wed, 29 May 2024

[NEU] [hoch] Xerox FreeFlow Print Server: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Xerox FreeFlow Print Server ausnutzen, um die Vertraulichkeit, Verfügbarkeit und Integrität des Systems zu gefährden

- [Link](#)

—

Wed, 29 May 2024

[NEU] [hoch] TIBCO Managed File Transfer: Schwachstelle ermöglicht Umgehen von Authentifizierung

Ein entfernter, anonymer Angreifer kann eine Schwachstelle in TIBCO Managed File Transfer ausnutzen, um die Authentifizierung zu umgehen.

- [Link](#)

—

Wed, 29 May 2024

[NEU] [hoch] ILIAS: Mehrere Schwachstellen ermöglichen Codeausführung

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

- [Link](#)

—

Wed, 29 May 2024

[UPDATE] [hoch] GNU libc: Schwachstelle ermöglicht Codeausführung

Ein Angreifer kann eine Schwachstelle in GNU libc ausnutzen, um einen Denial-of-Service-Zustand zu verursachen, Code auszuführen oder seine Privilegien zu erweitern.

- [Link](#)

—

Wed, 29 May 2024

[UPDATE] [hoch] Oracle MySQL: Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Oracle MySQL ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- [Link](#)

—

Wed, 29 May 2024

[UPDATE] [hoch] Intel PROSet Wireless WiFi Software: Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Intel PROSet Wireless WiFi Software ausnutzen, um seine Privilegien zu erhöhen oder einen Denial of Service Zustand herbeizuführen.

- [Link](#)

—

Wed, 29 May 2024

[UPDATE] [hoch] Python: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Python ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, Dateien zu manipulieren oder vertrauliche Informationen offenzulegen.

- [Link](#)

—

Wed, 29 May 2024

[UPDATE] [hoch] Splunk Splunk Enterprise: Mehrere Schwachstellen

Ein entfernter, authentifizierter Angreifer kann mehrere Schwachstellen in Splunk Splunk Enterprise ausnutzen, um beliebigen Code auszuführen, einen 'Denial of Service'-Zustand zu verursachen, seine Privilegien zu erweitern und weitere, nicht spezifizierte Auswirkungen zu verursachen.

- [Link](#)

—

Wed, 29 May 2024

[UPDATE] [hoch] Red Hat Ansible Automation Platform: Mehrere Schwachstellen

Ein entfernter, anonym Angreifer kann mehrere Schwachstellen in Red Hat Ansible Automation Platform ausnutzen, um beliebigen Code auszuführen oder falsche Informationen zu präsentieren.

- [Link](#)

—

Wed, 29 May 2024

[UPDATE] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um einen Denial-of-Service-Zustand herbeizuführen, Sicherheitsmaßnahmen zu umgehen, seine Privilegien zu erweitern, vertrauliche Informationen offenzulegen oder beliebigen Code auszuführen.

- [Link](#)

—

Wed, 29 May 2024

[UPDATE] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um vertrauliche Informationen offenzulegen oder einen nicht näher spezifizierten Angriff zu starten.

- [Link](#)

—

Wed, 29 May 2024

[UPDATE] [hoch] Splunk Enterprise: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Splunk Splunk Enterprise ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen, um Code auszuführen und um nicht näher spezifizierte Auswirkungen zu erzielen.

- [Link](#)

—

Wed, 29 May 2024

[UPDATE] [hoch] Perl: Mehrere Schwachstellen ermöglichen Codeausführung

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in Perl ausnutzen, um beliebigen Programmcode auszuführen.

- [Link](#)

—

Wed, 29 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](#)

—

Wed, 29 May 2024

[UPDATE] [hoch] docker: Mehrere Schwachstellen

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

- [Link](#)

—

Wed, 29 May 2024

[UPDATE] [kritisch] Fortinet FortiSIEM: Mehrere Schwachstellen ermöglichen Codeausführung mit "root" Rechten

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in Fortinet FortiSIEM ausnutzen, um beliebigen Programmcode mit "root" Rechten auszuführen.

- [Link](#)

—

Wed, 29 May 2024

[UPDATE] [hoch] Oracle Java SE: Mehrere Schwachstellen

Ein entfernter, anonymmer Angreifer kann mehrere Schwachstellen in Oracle Java SE ausnutzen, um die Vertraulichkeit, Integrität und Verfügbarkeit zu gefährden.

- [Link](#)

—

Wed, 29 May 2024

[UPDATE] [hoch] Red Hat Enterprise Linux: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux ausnutzen, um einen Denial-of-Service-Zustand zu erzeugen, vertrauliche Informationen offenzulegen, Dateien zu manipulieren oder seine Privilegien zu erweitern.

- [Link](#)

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
5/30/2024	[SUSE SLES12 Security Update : kernel (SUSE-SU-2024:1834-1)]	critical
5/30/2024	[SUSE SLED15 / SLES15 / openSUSE 15 Security Update : git (SUSE-SU-2024:1807-1)]	critical
5/30/2024	[SUSE SLED12 / SLES12 Security Update : freerdp (SUSE-SU-2024:1835-1)]	critical
5/30/2024	[Ubuntu 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : PyMySQL vulnerability (USN-6801-1)]	critical
5/30/2024	[Google Chrome < 125.0.6422.141 Multiple Vulnerabilities]	critical
5/30/2024	[Google Chrome < 125.0.6422.141 Multiple Vulnerabilities]	critical
5/30/2024	[Oracle Linux 9 : glibc (ELSA-2024-3339)]	high
5/30/2024	[Oracle Linux 8 : gdk-pixbuf2 (ELSA-2024-3341)]	high
5/30/2024	[Oracle Linux 8 : xorg-x11-server-Xwayland (ELSA-2024-3343)]	high
5/30/2024	[SUSE SLES15 / openSUSE 15 Security Update : kernel (SUSE-SU-2024:1813-1)]	high
5/30/2024	[SUSE SLES12 Security Update : libfastjson (SUSE-SU-2024:1846-1)]	high
5/30/2024	[SUSE SLES15 Security Update : gdk-pixbuf (SUSE-SU-2024:1842-1)]	high
5/30/2024	[SUSE SLES12 Security Update : xdg-desktop-portal (SUSE-SU-2024:1832-1)]	high

Datum	Schwachstelle	Bewertung
5/30/2024	[SUSE SLES15 Security Update : xdg-desktop-portal (SUSE-SU-2024:1831-1)]	high
5/30/2024	[SUSE SLES15 / openSUSE 15 Security Update : warewulf4 (SUSE-SU-2024:1838-1)]	high
5/30/2024	[SUSE SLES15 / openSUSE 15 Security Update : libxml2 (SUSE-SU-2024:0461-2)]	high
5/30/2024	[SUSE SLES15 Security Update : xdg-desktop-portal (SUSE-SU-2024:1806-1)]	high
5/30/2024	[Qlik Sense Enterprise Privilage Escalation (CVE-2024-36077)]	high
5/30/2024	[Cisco IOS XE Software Internet Key Exchange Version 1 Fragmentation DoS (cisco-sa-ikev1-NO2ccFWz)]	high
5/30/2024	[Cisco IOS Software Internet Key Exchange Version 1 Fragmentation DoS (cisco-sa-ikev1-NO2ccFWz)]	high
5/30/2024	[Check Point Quantum Gateway Directory Traversal (Direct Check)]	high
5/30/2024	[Oracle Linux 8 : python3 (ELSA-2024-3347)]	high
5/30/2024	[Oracle Linux 8 : glibc (ELSA-2024-3269)]	high
5/30/2024	[Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 / 24.04 LTS : FFmpeg vulnerabilities (USN-6803-1)]	high
5/30/2024	[Ubuntu 18.04 LTS / 20.04 LTS / 22.04 LTS / 23.10 : browserify-sign vulnerability (USN-6800-1)]	high
5/30/2024	[RHEL 8 : ruby:3.0 (RHSA-2024:3500)]	high
5/30/2024	[RHEL 9 : less (RHSA-2024:3513)]	high
5/30/2024	[RHEL 8 : edk2 (RHSA-2024:3497)]	high
5/30/2024	[Veritas System Recovery Arbitrary File Creation (VTS24-005)]	high
5/30/2024	[Debian dla-3824 : gir1.2-gst-plugins-base-1.0 - security update]	high
5/30/2024	[AlmaLinux 9 : less (ALSA-2024:3513)]	high

Datum	Schwachstelle	Bewertung
5/30/2024	[Oracle Linux 9 : less (ELSA-2024-3513)]	high

4 Aktiv ausgenutzte Sicherheitslücken

4.1 Exploits der letzten 5 Tage

“Thu, 30 May 2024

Aquatronica Control System 5.1.6 Password Disclosure

Aquatronica Control System version 5.1.6 has a tcp.php endpoint on the controller that is exposed to unauthenticated attackers over the network. This vulnerability allows remote attackers to send a POST request which can reveal sensitive configuration information, including plaintext passwords. This can lead to unauthorized access and control over the aquarium controller, compromising its security and potentially allowing attackers to manipulate its settings.

- [Link](#)

—

” “Thu, 30 May 2024

Progress Flowmon 12.3.5 Local sudo Privilege Escalation

This Metasploit module abuses a feature of the sudo command on Progress Flowmon. Certain binary files are allowed to automatically elevate with the sudo command. This is based off of the file name. This includes executing a PHP command with a specific file name. If the file is overwritten with PHP code it can be used to elevate privileges to root. Progress Flowmon up to at least version 12.3.5 is vulnerable.

- [Link](#)

—

” “Thu, 30 May 2024

Akaunting 3.1.8 Client-Side Template Injection

Akaunting version 3.1.8 suffers from a client-side template injection vulnerability.

- [Link](#)

—

” “Thu, 30 May 2024

Akaunting 3.1.8 Server-Side Template Injection

Akaunting version 3.1.8 suffers from a server-side template injection vulnerability.

- [Link](#)

—

” “Thu, 30 May 2024

ORing IAP-420 2.01e Cross Site Scripting / Command Injection

ORing IAP-420 version 2.01e suffers from remote command injection and persistent cross site scripting vulnerabilities.

- [Link](#)

—

” “Wed, 29 May 2024

Flowmon Unauthenticated Command Injection

This Metasploit module exploits an unauthenticated command injection vulnerability in Progress Flowmon versions before v12.03.02.

- [Link](#)

—

” “Tue, 28 May 2024

Eclipse ThreadX Buffer Overflows

Eclipse ThreadX versions prior to 6.4.0 suffers from a missing array size check causing a memory overwrite, missing parameter checks leading to integer wraparound, under allocations, heap buffer overflows, and more.

- [Link](#)

—

” “Tue, 28 May 2024

HAWKI 1.0.0-beta.1 XSS / File Overwrite / Session Fixation

HAWKI version 1.0.0-beta.1 before commit 146967f suffers from cross site scripting, arbitrary file overwrite, and session fixation vulnerabilities.

- [Link](#)

—

” “Tue, 28 May 2024

Siemens CP-XXXX Series Exposed Serial Shell

Siemens CP-XXXX Series (CP-2014, CP-2016, CP-2017, CP-2019, CP-5014) expose serial shells on multiple PLCs. A serial interface can be accessed with physical access to the PCB. After connecting to the interface, access to a shell with various debug functions as well as a login prompt is possible. The hardware is no longer produced nor offered to the market.

- [Link](#)

—

” “Mon, 27 May 2024

ElkArte Forum 1.1.9 Remote Code Execution

ElkArte Forum version 1.1.9 suffers from a remote code execution vulnerability.

- [Link](#)

—

” “Fri, 24 May 2024

Jcow Social Network Cross Site Scripting

Jcow Social Networking versions 14.2 up to 16.2.1 suffer from a persistent cross site scripting vulnerability.

- [Link](#)

—

” “Fri, 24 May 2024

4BRO Insecure Direct Object Reference / API Information Exposure

4BRO versions prior to 2024-04-17 suffer from insecure direct object reference and API information disclosure vulnerabilities.

- [Link](#)

—

” “Fri, 24 May 2024

Debezium UI 2.5 Credential Disclosure

Debezium UI version 2.5 suffers from a credential disclosure vulnerability.

- [Link](#)

—

” “Thu, 23 May 2024

FleetCart 4.1.1 Information Disclosure

FleetCart version 4.1.1 suffers from an information leakage vulnerability.

- [Link](#)

—

” “Wed, 22 May 2024

NorthStar C2 Cross Site Scripting / Code Execution

NorthStar C2, prior to commit 7674a44 on March 11 2024, contains a vulnerability where the logs page is vulnerable to a stored cross site scripting issue. An unauthenticated user can simulate an agent registration to cause the cross site scripting attack and take over a users session. With this access, it is then possible to run a new payload on all of the NorthStar C2 compromised hosts (agents), and kill the original agent. Successfully tested against NorthStar C2 commit e7fdce148b6a81516e8aa5e5e037acd082611f73 running on Ubuntu 22.04. The agent was running on Windows 10 19045.

- [Link](#)

—

” “Wed, 22 May 2024

AVideo WWBNIndex Plugin Unauthenticated Remote Code Execution

This Metasploit module exploits an unauthenticated remote code execution vulnerability in the WWBNIndex plugin of the AVideo platform. The vulnerability exists within the submitIndex.php file, where user-supplied input is passed directly to the require() function without proper sanitization. By

exploiting this, an attacker can leverage the PHP filter chaining technique to execute arbitrary PHP code on the server. This allows for the execution of commands and control over the affected system. The exploit is particularly dangerous because it does not require authentication, making it possible for any remote attacker to exploit this vulnerability.

- [Link](#)

—

” “Wed, 22 May 2024

Chat Bot 1.0 SQL Injection

Chat Bot version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Tue, 21 May 2024

CHAOS 5.0.8 Cross Site Scripting / Remote Command Execution

CHAOS version 5.0.8 is a free and open-source Remote Administration Tool that allows generated binaries to control remote operating systems. The web application contains a remote command execution vulnerability which can be triggered by an authenticated user when generating a new executable. The web application also contains a cross site scripting vulnerability within the view of a returned command being executed on an agent.

- [Link](#)

—

” “Tue, 21 May 2024

Joomla 4.2.8 Information Disclosure

Joomla versions 4.2.8 and below remote unauthenticated information disclosure exploit.

- [Link](#)

—

” “Tue, 21 May 2024

Nethserver 7 / 8 Cross Site Scripting

The NethServer module installed as WebTop, produced by Sonicle, is affected by a stored cross site scripting vulnerability due to insufficient input sanitization and output escaping which allows an attacker to store a malicious payload as to execute arbitrary web scripts or HTML. Versions 7 and 8 are affected.

- [Link](#)

—

” “Tue, 21 May 2024

PowerVR DevmemIntChangeSparse2() Dangling Page Table Entry

PowerVR suffers from a wrong order of operations in DevmemIntChangeSparse2() that leads to a temporarily dangling page table entry.

- [Link](#)

—

” “Tue, 21 May 2024

*****PowerVR _UnrefAndMaybeDestroy() Use-After-Free*****

PowerVR suffers from a use-after-free vulnerability in _UnrefAndMaybeDestroy().

- [Link](#)

—

” “Tue, 21 May 2024

Arm Mali r45p0 Broken State Use-After-Free

Arm Mali versions since r45p0 suffer from a broken KBASE_USER_BUF_STATE_* state machine for userspace mappings that can lead to a use-after-free condition.

- [Link](#)

—

” “Mon, 20 May 2024

Tenant Limited 1.0 SQL Injection

Tenant Limited version 1.0 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

” “Mon, 20 May 2024

WordPress XStore Theme 9.3.8 SQL Injection

WordPress XStore theme version 9.3.8 suffers from a remote SQL injection vulnerability.

- [Link](#)

—

”

4.2 0-Days der letzten 5 Tage

“Thu, 30 May 2024

ZDI-24-526: (Pwn2Own) VMware Workstation VBluetoothHCI_PacketOut Use-After-Free Privilege Escalation Vulnerability

- [Link](#)

—

” “Wed, 29 May 2024

ZDI-24-525: A10 Thunder ADC Incorrect Permission Assignment Local Privilege Escalation Vulnerability

- [Link](#)

—

” “Wed, 29 May 2024

ZDI-24-524: A10 Thunder ADC CsrRequestView Command Injection Remote Code Execution Vul-

nerability

- [Link](#)

—

” “Wed, 29 May 2024

ZDI-24-523: Phoenix Contact CHARX SEC-3100 Link Following Local Privilege Escalation Vulnerability

- [Link](#)

—

” “Wed, 29 May 2024

ZDI-24-522: (Pwn2Own) Phoenix Contact CHARX SEC-3100 Filename Command Injection Remote Code Execution Vulnerability

- [Link](#)

—

” “Wed, 29 May 2024

ZDI-24-521: (Pwn2Own) Phoenix Contact CHARX SEC-3100 OCPP charx_pack_logs Command Injection Remote Code Execution Vulnerability

- [Link](#)

—

” “Wed, 29 May 2024

ZDI-24-520: (Pwn2Own) Phoenix Contact CHARX SEC-3100 Missing Encryption Authentication Bypass Vulnerability

- [Link](#)

—

” “Wed, 29 May 2024

ZDI-24-519: (Pwn2Own) Phoenix Contact CHARX SEC-3100 Untrusted Search Path Local Privilege Escalation Vulnerability

- [Link](#)

—

” “Wed, 29 May 2024

ZDI-24-518: Progress Software Telerik Reporting ValidateMetadaUri XML External Entity Processing Information Disclosure Vulnerability

- [Link](#)

—

” “Wed, 29 May 2024

ZDI-24-517: Progress Software WhatsUp Gold FaviconController Server-Side Request Forgery Information Disclosure Vulnerability

- [Link](#)

—

” “Tue, 28 May 2024

ZDI-24-516: Progress Software WhatsUp Gold HttpContentActiveController Server-Side Request Forgery Information Disclosure Vulnerability

- [Link](#)

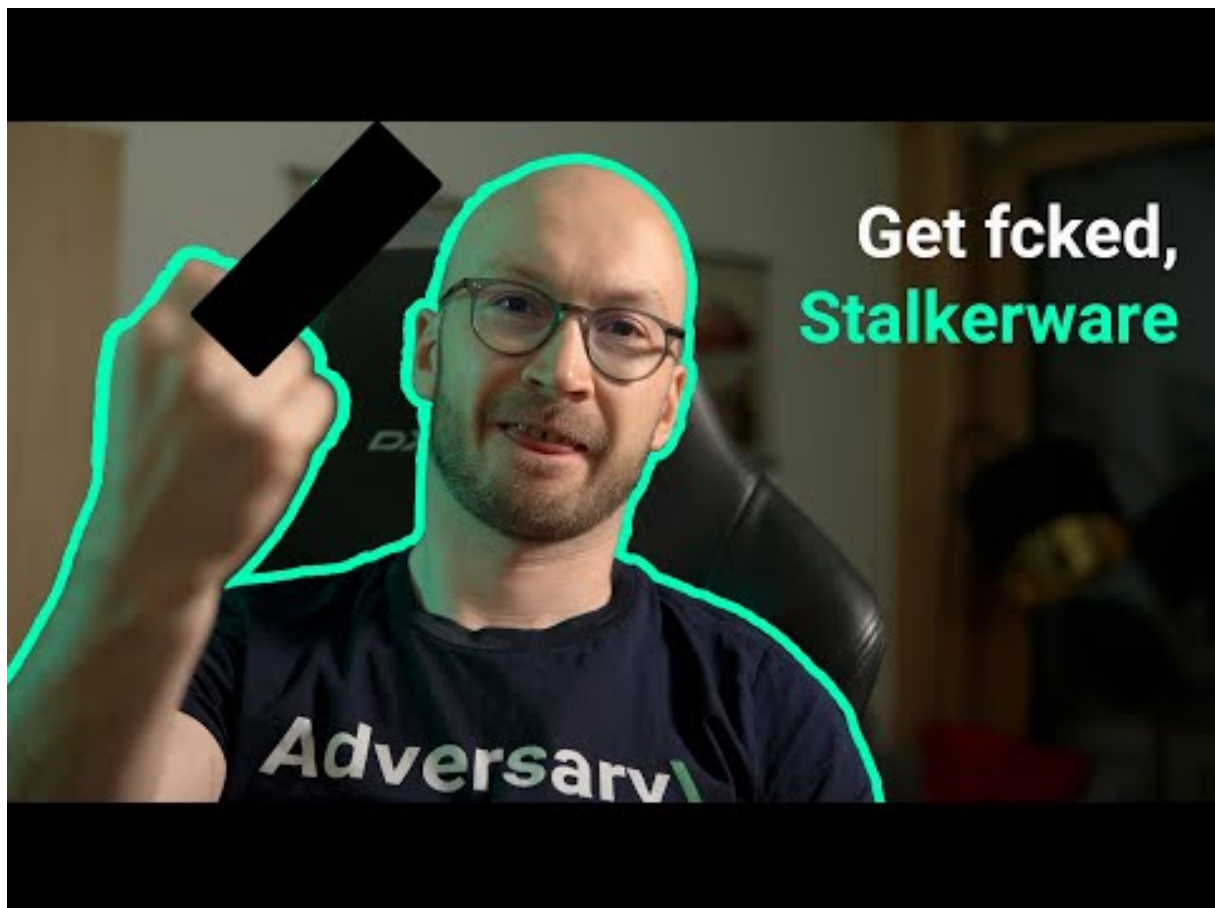
—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 FCK Stalkerware.



[Zum Youtube Video](#)

6 Cyberangriffe: (Mai)

Datum	Opfer	Land	Information
2024-05-28	Uniprévoyance	[FRA]	Link
2024-05-28	Kantonsschule Frauenfeld	[CHE]	Link
2024-05-28	Smith & Caughey's	[NZL]	Link
2024-05-28	Guardian Childcare	[AUS]	Link
2024-05-26	La ville de Dammartin-en-Goële	[FRA]	Link
2024-05-26	Center Line Public Schools	[USA]	Link
2024-05-25	Seattle Public Library	[USA]	Link
2024-05-24	Comté d'Albany	[USA]	Link
2024-05-24	Islamabad Safe City Authority	[PAK]	Link
2024-05-24	Mobitwin	[BEL]	Link
2024-05-23	Le département de la Justice et du Développement constitutionnel (DJ&CD)	[ZAF]	Link
2024-05-22	Jumbo Group	[SGP]	Link
2024-05-21	Le Cup (Centre Unique de Programmation)	[ITA]	Link
2024-05-21	Top-Medien	[CHE]	Link
2024-05-20	Hong Kong Institute of Contemporary Culture Lee Shau Kee School of Creativity	[HKG]	Link
2024-05-19	Malheur County	[USA]	Link
2024-05-17	AddComm	[NLD]	Link
2024-05-16	American Radio Relay League (ARRL)	[USA]	Link
2024-05-15	MediSecure	[AUS]	Link
2024-05-15	Rockford Public Schools	[USA]	Link
2024-05-15	Ranzijn	[NLD]	Link
2024-05-15	Le Collège Ahuntsic	[CAN]	Link
2024-05-15	Central Contra Costa Transit Authority (County Connection)	[USA]	Link

Datum	Opfer	Land	Information
2024-05-13	Universidad Complutense de Madrid	[ESP]	Link
2024-05-13	L'aéroport et l'école de commerce de Pau	[FRA]	Link
2024-05-13	First Nations Health Authority (FNHA)	[CAN]	Link
2024-05-12	Christie's	[CHE]	Link
2024-05-12	Travelite Holdings Ltd.	[SGP]	Link
2024-05-12	Union Township School District	[USA]	Link
2024-05-11	Wehrle-Werk AG	[DEU]	Link
2024-05-08	Ascension Health	[USA]	Link
2024-05-07	Mālama I Ke Ola Health Center	[USA]	Link
2024-05-06	DocGo	[USA]	Link
2024-05-06	Key Tronic Corporation	[USA]	Link
2024-05-06	Trego County Lemke Memorial Hospital	[USA]	Link
2024-05-05	Wichita	[USA]	Link
2024-05-05	Université de Sienne	[ITA]	Link
2024-05-05	Concord Public Schools et Concord-Carlisle Regional School District	[USA]	Link
2024-05-05	Palomar Health	[USA]	Link
2024-05-04	Regional Cancer Center (RCC)	[IND]	Link
2024-05-03	Eucatex (EUCA4)	[BRA]	Link
2024-05-03	Cégep de Lanaudière	[CAN]	Link
2024-05-03	Coradix-Magnescan	[FRA]	Link
2024-05-02	Umeå universitet	[SWE]	Link
2024-05-02	Ewing Marion Kauffman School	[USA]	Link
2024-05-01	Brandywine Realty Trust	[USA]	Link

7 Ransomware-Erpressungen: (Mai)

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-30	[aytosanlorenzo.es]	lockbit3	Link
2024-05-30	[www.indigoent.ca]	qiulong	Link
2024-05-30	[strikeusa.com]	lockbit3	Link
2024-05-30	[Rob's Whole Health Pharmacy]	rhysida	Link
2024-05-30	[Faultless Brands]	akira	Link
2024-05-30	[DreamWall]	akira	Link
2024-05-30	[Excel Security Corp.]	akira	Link
2024-05-30	[UNICRED.COM.AR]	cllop	Link
2024-05-27	[Wichita County Mounted Patrol]	medusa	Link
2024-05-27	[Brownell Boat Stands & Equipment Company]	medusa	Link
2024-05-30	[MagicLand]	akira	Link
2024-05-30	[Elmhurst Group]	play	Link
2024-05-30	[WALSER AUTOMOTIVE GROUP]	play	Link
2024-05-30	[FPL Food]	play	Link
2024-05-30	[Ntv]	play	Link
2024-05-29	[Credit Central]	play	Link
2024-05-29	[heras.co.uk]	lockbit3	Link
2024-05-29	[Western Dovetail]	akira	Link
2024-05-29	[I.L.A. Local 1964]	dragonforce	Link
2024-05-29	[mcmtelecom.com]	blackout	Link
2024-05-28	[Aircod.com]	redransomware	Link
2024-05-28	[Bjurholms kommun]	ransomhub	Link
2024-05-07	[iiexperts.com]	dAn0n	Link
2024-05-08	[neosmteam.com]	dAn0n	Link
2024-05-08	[glenwoodnyc.com]	dAn0n	Link
2024-05-23	[s-f-concrete.com]	dAn0n	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-08	[college-park.com]	dAn0n	Link
2024-05-28	[Manuchar]	hunters	Link
2024-05-28	[Arrabawn Co-op]	hunters	Link
2024-05-28	[Avelina]	akira	Link
2024-05-28	[Brett Slater Solicitors]	akira	Link
2024-05-28	[OTR]	akira	Link
2024-05-28	[PSG BANATSKI DVOR D.O.O. NOVI SAD (SERBIA)]	ransomhub	Link
2024-05-28	[American Clinical Solutions(acslabtest.com)auctioning]	ransomhub	Link
2024-05-27	[SIAED.it - HOSTER/DEV FOR ITALY BIGGEST BANKS]	ransomhub	Link
2024-05-27	[Christies Auction House - christies.com]	ransomhub	Link
2024-05-27	[S L B TRANSIT INC]	8base	Link
2024-05-27	[Information Technology]	handala	Link
2024-05-27	[Natsume Tax Accountant Corporation]	8base	Link
2024-05-27	[The Kelly Group]	8base	Link
2024-05-27	[Osaka Motorcycle Business Cooperative]	8base	Link
2024-05-27	[Matusima]	8base	Link
2024-05-27	[Shirasaki]	8base	Link
2024-05-27	[Architecture LEJEUNE GIOVANELLI]	8base	Link
2024-05-25	[Hytera US Inc]	spacebears	Link
2024-05-27	[alliedtelesis.com]	lockbit3	Link
2024-05-23	[Datanet]	qilin	Link
2024-05-26	[CNPC Sport]	monti	Link
2024-05-26	[Esc Pau Etudes-Conseils]	monti	Link
2024-05-26	[Aéroport de Pau]	monti	Link
2024-05-02	[High Group]	handala	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-16	[Amigour Company]	handala	Link
2024-05-22	[Harmony Pharm]	handala	Link
2024-05-25	[Ramat Gan Academic College]	handala	Link
2024-05-26	[National Publisher Services LLC]	bianlian	Link
2024-05-26	[Payne & Jones]	bianlian	Link
2024-05-26	[Wind Composite Services Group, LLC]	bianlian	Link
2024-05-23	[Assist Informatica]	mallox	Link
2024-05-25	[multigroup.info]	lockbit3	Link
2024-05-25	[pressurejet.com]	lockbit3	Link
2024-05-25	[mgops.sedziszow-mlp.pl]	lockbit3	Link
2024-05-25	[kharafiglobal.com]	lockbit3	Link
2024-05-25	[sunpetro.com]	lockbit3	Link
2024-05-25	[cafesnovell.com]	lockbit3	Link
2024-05-25	[highwaystrust.com]	lockbit3	Link
2024-05-25	[sysroad.com]	lockbit3	Link
2024-05-25	[longviewoms.com]	lockbit3	Link
2024-05-18	[Access Sports Medicine & Orthopaedics]	incransom	Link
2024-05-20	[Crandall ISD (CISD.crandallisd.org)]	incransom	Link
2024-05-23	[S&F Concrete Contractors]	dAn0n	Link
2024-05-25	[\$150.000]	blacksuit	Link
2024-05-24	[bnsgroup.co.uk]	lockbit3	Link
2024-05-24	[Ipsotek LTD]	blacksuit	Link
2024-05-24	[Vanguard Utility Partners]	akira	Link
2024-05-24	[workscapes.com]	lockbit3	Link
2024-05-24	[EMPIRECOMFORT.COM]	clop	Link
2024-05-24	[kns.com]	lockbit3	Link
2024-05-24	[colfax.k12.wi.us - \$150.000]	blacksuit	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-24	[Sichuan Dowell Science and Technology Company Inc]	blacksuit	Link
2024-05-24	[hiawathahomes]	blacksuit	Link
2024-05-23	[valleylandtitleco.com]	lockbit3	Link
2024-05-22	[umbrellaproperties.com PART2]	dispossessor	Link
2024-05-23	[brightwayconsultants.co.uk]	apt73	Link
2024-05-23	[Nutec Group]	bianlian	Link
2024-05-04	[United Urology Group]	ransomhouse	Link
2024-05-23	[Hands TheFamilyHelpNetwork.ca]	incransom	Link
2024-05-23	[iseta.fr (institut des Sciences de l'Environnement et des Territoires d'Annecy)]	ransomhub	Link
2024-05-22	[ICC]	rhysida	Link
2024-05-22	[Newman Ferrara]	akira	Link
2024-05-22	[IZOMAT Praha]	akira	Link
2024-05-22	[GRANVILLE FOOD CARE LIMITED]	akira	Link
2024-05-22	[Richland City Hall]	incransom	Link
2024-05-22	[Midwest Covenant Home]	incransom	Link
2024-05-22	[First Nations Health Authority (fnha.local)]	incransom	Link
2024-05-21	[Golden Acre]	qilin	Link
2024-05-22	[Ryder Scott Co.]	play	Link
2024-05-22	[Tri-state General Contractors]	play	Link
2024-05-22	[Starostwo Powiatowe w Świebodzinie]	play	Link
2024-05-22	[Aspire Tax]	play	Link
2024-05-22	[The Louis G Freeman]	play	Link
2024-05-22	[Experis Technology Group]	play	Link
2024-05-22	[Anchorage Daily News]	play	Link
2024-05-22	[RDI-USA]	play	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-22	[Ardenbrook]	play	Link
2024-05-22	[Visa Lighting]	play	Link
2024-05-22	[Semicore Equipment]	play	Link
2024-05-22	[Levin Porter Associates]	play	Link
2024-05-22	[Critchfield & Johnston]	bianlian	Link
2024-05-21	[shamrocktradingcorp.com]	embargo	Link
2024-05-21	[londondrugs.com]	lockbit3	Link
2024-05-21	[schmittyandsons.com]	lockbit3	Link
2024-05-21	[ThrottleUp]	ransomhub	Link
2024-05-21	[ramfoam.com]	lockbit3	Link
2024-05-21	[ALO diamonds]	8base	Link
2024-05-21	[Brittany Horne]	ransomhub	Link
2024-05-20	[Aztec Services Group]	medusa	Link
2024-05-20	[International Modern Hospital]	medusa	Link
2024-05-20	[Heras]	medusa	Link
2024-05-21	[levian.com]	blackbasta	Link
2024-05-21	[lactanet.ca]	blackbasta	Link
2024-05-21	[mfgroup.it]	blackbasta	Link
2024-05-21	[grupocadarso.com]	blackbasta	Link
2024-05-21	[atlasoil.com]	blackbasta	Link
2024-05-21	[trugreen.com]	blackbasta	Link
2024-05-20	[Matadero de Gijón - Biogas energy plant - mataderodegijon.es]	ransomhub	Link
2024-05-20	[American Clinical Solutions(acslabtest.com)]	ransomhub	Link
2024-05-20	[ORIUX: Experts in Mobility]	ransomhub	Link
2024-05-20	[Jess-link Products]	hunters	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-20	[MAH Machine]	bianlian	Link
2024-05-20	[Margin]	akira	Link
2024-05-20	[GE Aerospace]	meow	Link
2024-05-20	[Crooker]	8base	Link
2024-05-20	[Embellir]	8base	Link
2024-05-20	[LEMKEN]	8base	Link
2024-05-20	[California Highway Patrol (SVEL237.org)]	incransom	Link
2024-05-20	[qualityplumbingassociates.com]	lockbit3	Link
2024-05-18	[Regional Obstetrical Consultants]	incransom	Link
2024-05-20	[Specialty Market Managers]	incransom	Link
2024-05-20	[Sterling Transportation Services (sts.local)]	incransom	Link
2024-05-20	[Continuing Healthcare Solutions (chs.local)]	incransom	Link
2024-05-20	[schuettmetals.com]	cactus	Link
2024-05-07	[allied-mechanical-services-inc]	incransom	Link
2024-05-16	[Patriot Machine, Updated data leak.]	donutleaks	Link
2024-05-18	[carcajou.fr]	lockbit3	Link
2024-05-18	[equinoxinc.org]	lockbit3	Link
2024-05-18	[unisi.it]	lockbit3	Link
2024-05-18	[Widdop & Co.]	rhysida	Link
2024-05-18	[Colégio Nova Dimensão]	arcusmedia	Link
2024-05-18	[catiglass.com \$100.000]	blacksuit	Link
2024-05-18	[Bluebonnet Nutrition]	bianlian	Link
2024-05-18	[Center for Digestive Health]	bianlian	Link
2024-05-18	[drmsusa.com]	incransom	Link
2024-05-17	[WEICON]	medusa	Link
2024-05-17	[County Connection]	medusa	Link
2024-05-17	[Elm Grove]	medusa	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-17	[Comwave]	medusa	Link
2024-05-17	[Mesopolys]	spacebears	Link
2024-05-14	[Pittsburgh's Trusted Orthopaedic Surgeons]	donutleaks	Link
2024-05-17	[Sullairargentina.com]	redransomware	Link
2024-05-15	[www.belcherpharma.com]	underground	Link
2024-05-17	[orga-soft.de]	embargo	Link
2024-05-17	[Houston Waste Solutions]	ransomhub	Link
2024-05-17	[Shyang Shin Bao Ind. Co., Ltd. (hereinafter referred to as "SSB")]	qilin	Link
2024-05-17	[Vision Mechanical]	blacksuit	Link
2024-05-08	[aharvey.nf.ca]	incransom	Link
2024-05-17	[PRIMARYSYS.COM]	clop	Link
2024-05-17	[Formosa Plastics USA]	hunters	Link
2024-05-16	[Dean Lumber & Supply]	dragonforce	Link
2024-05-16	[WindCom]	dragonforce	Link
2024-05-17	[For sale. Contact through admin. \$100.000]	blacksuit	Link
2024-05-17	[agranibank.org]	killsec	Link
2024-05-17	[laxmicapital.com.np]	killsec	Link
2024-05-16	[pricemodern.com]	lockbit3	Link
2024-05-16	[OKUANT - okuant.com]	ransomhub	Link
2024-05-16	[valleyjoist.com]	lockbit3	Link
2024-05-16	[fulcrum.pro]	cactus	Link
2024-05-16	[Insurance Agency Marketing Services]	moneymessage	Link
2024-05-15	[Neovia]	snatch	Link
2024-05-16	[Baeckerei-raddatz.de]	cloak	Link
2024-05-14	[Colonial Surety Company]	medusa	Link
2024-05-16	[kauffmanschool.org]	lockbit3	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-16	[ema-eda.com]	lockbit3	Link
2024-05-16	[twpunionschools.org]	lockbit3	Link
2024-05-16	[Chuo System Service Co.,Ltd]	ransomhub	Link
2024-05-16	[East Shore Sound]	ransomhub	Link
2024-05-16	[thermalsolutionsllc.com]	threeam	Link
2024-05-16	[escriba.com.br]	threeam	Link
2024-05-16	[RIO TECHNOLOGY]	arcusmedia	Link
2024-05-16	[Egyptian Sudanese]	arcusmedia	Link
2024-05-15	[Consulting Radiologists]	qilin	Link
2024-05-03	[FIAB SpA]	qilin	Link
2024-05-15	[project sold]	monti	Link
2024-05-14	[Malone]	dragonforce	Link
2024-05-14	[Hardings Transport]	dragonforce	Link
2024-05-14	[Connelly Security Systems]	dragonforce	Link
2024-05-14	[Motor Munich]	dragonforce	Link
2024-05-15	[epsd.org]	lockbit3	Link
2024-05-15	[district70.org]	lockbit3	Link
2024-05-15	[keuka.edu]	lockbit3	Link
2024-05-15	[allcare-med.com]	lockbit3	Link
2024-05-15	[Coplosa]	8base	Link
2024-05-15	[Surrey Place Healthcare & Rehabilitation]	rhysida	Link
2024-05-15	[daubertchemical.com]	lockbit3	Link
2024-05-08	[BRAZIL GOV]	arcusmedia	Link
2024-05-11	[Braz Assessoria Contábil]	arcusmedia	Link
2024-05-11	[Thibabem Atacadista]	arcusmedia	Link
2024-05-11	[FILSCAP]	arcusmedia	Link
2024-05-11	[Cusat]	arcusmedia	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-11	[Frigrífico Boa Carne]	arcusmedia	Link
2024-05-11	[GOLD RH S.A.S]	arcusmedia	Link
2024-05-11	[Grupo SASMET]	arcusmedia	Link
2024-05-15	[City of Neodesha]	ransomhub	Link
2024-05-08	[gravetye-manoir]	incransom	Link
2024-05-15	[Wealth Depot LLC]	everest	Link
2024-05-14	[morrisgroupint.com]	lockbit3	Link
2024-05-14	[pierfoundry.com]	blacksuit	Link
2024-05-14	[Fiskars Group]	akira	Link
2024-05-14	[Bruno generators (Italian manufacturing)]	akira	Link
2024-05-14	[GMJ & Co, Chartered Accountants]	bianlian	Link
2024-05-14	[Rocky Mountain Sales]	ransomhub	Link
2024-05-14	[Talley Group]	incransom	Link
2024-05-14	[acla.de]	lockbit3	Link
2024-05-14	[Watt Carmichael]	dragonforce	Link
2024-05-14	[500gb/www.confins.com.br/10kk/BR/Come to chat or we will attack you again.]	ransomhub	Link
2024-05-14	[eucatex.com.br]	ransomhub	Link
2024-05-14	[LPDB KUMKM LPDB.ID/LPDB.GO.ID]	ransomhub	Link
2024-05-13	[Accurate Lock and Hardware]	dragonforce	Link
2024-05-13	[Monocon International Refractory]	dragonforce	Link
2024-05-13	[Persyn]	dragonforce	Link
2024-05-13	[Aero Tec Laboratories]	hunters	Link
2024-05-13	[Altipal]	dragonforce	Link
2024-05-13	[Municipalité La Guadeloupe]	qilin	Link
2024-05-13	[Eden Project Ltd]	incransom	Link
2024-05-13	[Helapet Ltd]	incransom	Link

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-13	[oseranbahn.com]	lockbit3	Link
2024-05-13	[jmjcorporation.com]	lockbit3	Link
2024-05-13	[countyins.com]	lockbit3	Link
2024-05-13	[utc-silverstone.co.uk]	lockbit3	Link
2024-05-13	[hesperiausd.org]	lockbit3	Link
2024-05-13	[Eden Project]	incransom	Link
2024-05-13	[umbrellaproperties.com]	dispossessor	Link
2024-05-13	[Treasury of Cote d'Ivoire]	hunters	Link
2024-05-13	[scanda.com.mx]	cactus	Link
2024-05-13	[acfin.cl]	cactus	Link
2024-05-13	[New Boston Dental Care]	8base	Link
2024-05-13	[Service public de Wallonie]	8base	Link
2024-05-13	[Cushman Contracting Corporation]	8base	Link
2024-05-13	[Costa Edutainment SpA]	8base	Link
2024-05-13	[Sigmund Espeland AS]	8base	Link
2024-05-13	[Brovedani Group]	8base	Link
2024-05-13	[Fic Expertise]	8base	Link
2024-05-13	[W.I.S. Sicherheit]	8base	Link
2024-05-12	[Brick Court Chambers]	medusa	Link
2024-05-03	[Seaman's Mechanical]	incransom	Link
2024-05-06	[Deeside Timberframe]	incransom	Link
2024-05-09	[McSweeney / Langevin]	qilin	Link
2024-05-11	[NITEK International LLC]	medusa	Link
2024-05-11	[National Metalwares, L.P]	medusa	Link
2024-05-12	[Romeo Pitaro Injury & Litigation Lawyers]	bianlian	Link
2024-05-11	[NHS (press update)]	incransom	Link
2024-05-11	[Jackson County]	blacksuit	Link

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

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

Datum	Opfer	Ransomware-Gruppe	Webseite
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
2024-05-09	[asafoot.com]	lockbit3	Link

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

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

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-07	[ctc-corp.net]	lockbit3	Link
2024-05-07	[uslinen.com]	lockbit3	Link
2024-05-07	[tu-ilmenau.de]	lockbit3	Link
2024-05-07	[thede-culpepper.com]	lockbit3	Link
2024-05-07	[kimmelcleaners.com]	lockbit3	Link
2024-05-07	[emainc.net]	lockbit3	Link
2024-05-07	[southernspecialtysupply.com]	lockbit3	Link
2024-05-07	[lenmed.co.za]	lockbit3	Link
2024-05-07	[churchill-linen.com]	lockbit3	Link
2024-05-07	[rollingfields.com]	lockbit3	Link
2024-05-07	[srg-plc.com]	lockbit3	Link
2024-05-07	[gorrias-mercedes-benz.fr]	lockbit3	Link
2024-05-05	[SBC Global, Bitfinex, Coinmama, and Rutgers University Part 2 Leak]	flocker	Link
2024-05-07	[Central Florida Equipment]	play	Link
2024-05-07	[High Performance Services]	play	Link
2024-05-07	[Mauritzon]	play	Link
2024-05-07	[Somerville]	play	Link
2024-05-07	[Donco Air]	play	Link
2024-05-07	[Affordable Payroll & Bookkeeping Services]	play	Link
2024-05-07	[Utica Mack]	play	Link
2024-05-07	[KC Scout]	play	Link
2024-05-07	[Sentry Data Management]	play	Link
2024-05-07	[aletech.com.br]	darkvault	Link
2024-05-07	[Young Consulting]	blacksuit	Link
2024-05-06	[Thaayakam LTD]	ransomhub	Link
2024-05-06	[The Weinstein Firm]	qilin	Link

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

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

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

Datum	Opfer	Ransomware-Gruppe	Webseite
2024-05-01	[Azteca Tax Systems]	bianlian	Link
2024-05-01	[Clinica de Salud del Valle de Salinas]	bianlian	Link
2024-05-01	[cochraneglobal.com]	underground	Link
2024-05-01	[UK government]	snatch	Link
2024-05-01	[hookerfurniture.com]	lockbit3	Link
2024-05-01	[alimmigration.com]	lockbit3	Link
2024-05-01	[anatomage.com]	lockbit3	Link
2024-05-01	[bluegrasstechnologies.net]	lockbit3	Link
2024-05-01	[PINNACLEENGR.COM]	clop	Link
2024-05-01	[MCKINLEYPACKAGING.COM]	clop	Link
2024-05-01	[PILOTPEN.COM]	clop	Link
2024-05-01	[colonial.edu]	lockbit3	Link
2024-05-01	[cordish.com]	lockbit3	Link
2024-05-01	[concorr.com]	lockbit3	Link
2024-05-01	[yupousa.com]	lockbit3	Link
2024-05-01	[peaseinc.com]	lockbit3	Link
2024-05-01	[bdcm.com]	blackbasta	Link
2024-05-01	[MORTON WILLIAMS]	everest	Link
2024-05-03	[melting-mind.de]	apt73	Link
2024-05-21	[netscout.com]	dispossessor	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.