Cybersecurity Morgenreport

von Cyberwald

Marlon Hübner

20240514

Inhaltsverzeichnis

1 Editorial

Guten Morgen,

willkommen zum Cybersecurity Morgenreport von Cyberwald, Ihrem täglichen Begleiter in der Welt der IT-Sicherheit. Als nicht-kommerzielles Projekt ist es unser Anliegen, Awareness und Wissen rund um das Thema Cybersecurity kostenlos zu vermitteln. In der heutigen digitalen Welt ist es für Unternehmen von entscheidender Bedeutung, sich über aktuelle Sicherheitsrisiken zeitnah zu informieren. Cyberbedrohungen entwickeln sich ständig weiter und können erhebliche Schäden verursachen, wenn sie nicht rechtzeitig erkannt und abgewehrt werden. Durch die Nutzung aktueller Informationen können Unternehmen ihre IT-Sicherheitsmaßnahmen stärken und sich effektiv gegen diese Bedrohungen schützen.

Unser Ziel ist es, Ihnen, den IT-Verantwortlichen, einen kompakten und leicht verständlichen Überblick über aktuelle Sicherheitsrisiken zu geben. Wir präsentieren Ihnen täglich Sicherheitsmeldungen und Berichte über neue Sicherheitslücken, die Ihre Systeme und Daten bedrohen könnten.

Darüber hinaus listen wir aktuelle Cyberangriffe und Ransomware-Vorfälle auf. Dies ist von besonderer Bedeutung, da es Unternehmen ermöglicht, sich auf mögliche Supply-Chain- und Phishing-Angriffe vorzubereiten. Durch das Verständnis der Methoden und Taktiken, die von Cyberkriminellen verwendet werden, können Unternehmen ihre Verteidigungsmaßnahmen entsprechend anpassen und stärken.

Für den Cybersecurity Morgenreport greifen wir automatisiert auf öffentliche Informationsquellen zu, filtern und sortieren diese Informationen, um sie Ihnen in einer übersichtlichen Form zur Verfügung zu stellen. Wir bemühen uns, die Inhalte so verständlich wie möglich zu gestalten und vorzugsweise vollständig in deutscher Sprache wiederzugeben. Bei Bedarf übersetzen wir die öffentlichen Informationen und fassen sie durch eine KI zusammen.

Der Cybersecurity Morgenreport ist ein dynamisches Projekt. Wir passen und erweitern unsere Inhalte ständig, um Ihnen die relevantesten und aktuellsten Informationen zu liefern. Derzeit befinden wir uns im Alpha-Stadium des Projekts und freuen uns über Ihr Feedback und Ihre Anregungen.

Wir hoffen, dass der Cybersecurity Morgenreport Ihnen hilft, Ihre IT-Sicherheitsmaßnahmen zu verbessern und Ihre Systeme vor den ständig wechselnden Bedrohungen zu schützen. Bleiben Sie sicher und informiert mit dem Cybersecurity Morgenreport von Cyberwald.

Ihr Cyberwald-Team

2 Security-News

2.1 Heise - Security-Alert

Jetzt updaten! Erneut Zeroday-Lücke in Google Chrome, Exploit verfügbar

Google veröffentlicht erneut ein Notfall-Update für den Webbrowser Chrome. Es gibt schon einen Exploit für die Zero-Day-Lücke.

- Link

—

IBM Security Guardium: Lücken erlauben Codeschmuggel und Rechtausweitung

IBM hat für seine Cloud-Sicherheitssoftware Security Guardium Updates bereitgestellt. Sie schließen teils kritische Sicherheitslücken.

- Link

—

Backup-Managementtool: Schadcode-Lücke bedroht Veeam Service Provider

Um eine kritische Schwachstelle zu schließen, sollten Admins Veeam Service Provider zeitnah auf den aktuellen Stand bringen.

- Link

—

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: Rechteausweitung 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

—

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	0.993490000	Link
CVE-2023-6895	0.901600000	0.987740000	Link
CVE-2023-6553	0.922860000	0.989340000	Link
CVE-2023-5360	0.967230000	0.996520000	Link
CVE-2023-4966	0.966680000	0.996340000	Link
CVE-2023-48795	0.962250000	0.995100000	Link
CVE-2023-47246	0.943770000	0.991830000	Link
CVE-2023-46805	0.965580000	0.996070000	Link
CVE-2023-46747	0.970410000	0.997540000	Link
CVE-2023-46604	0.972730000	0.998490000	Link
CVE-2023-43177	0.964020000	0.995600000	Link
CVE-2023-42793	0.970940000	0.997740000	Link
CVE-2023-39143	0.953670000	0.993470000	Link
CVE-2023-38646	0.913020000	0.988550000	Link
CVE-2023-38205	0.922000000	0.989230000	Link
CVE-2023-38203	0.971170000	0.997860000	Link
CVE-2023-38035	0.974190000	0.999330000	Link
CVE-2023-36845	0.966630000	0.996320000	Link
CVE-2023-3519	0.911860000	0.988490000	Link
CVE-2023-35082	0.959780000	0.994600000	Link
CVE-2023-35078	0.968160000	0.996820000	Link
CVE-2023-34993	0.966220000	0.996210000	Link
CVE-2023-34960	0.934040000	0.990640000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-34634	0.918830000	0.988990000	Link
CVE-2023-34362	0.955650000	0.993820000	Link
CVE-2023-34039	0.943170000	0.991750000	Link
CVE-2023-3368	0.916570000	0.988780000	Link
CVE-2023-33246	0.973220000	0.998760000	Link
CVE-2023-32315	0.974090000	0.999260000	Link
CVE-2023-32235	0.914550000	0.988630000	Link
CVE-2023-30625	0.945200000	0.992110000	Link
CVE-2023-30013	0.963050000	0.995310000	Link
CVE-2023-29300	0.969500000	0.997210000	Link
CVE-2023-29298	0.948030000	0.992530000	Link
CVE-2023-28771	0.914030000	0.988600000	Link
CVE-2023-28432	0.935270000	0.990750000	Link
CVE-2023-28121	0.945870000	0.992190000	Link
CVE-2023-27524	0.970950000	0.997740000	Link
CVE-2023-27372	0.973760000	0.999030000	Link
CVE-2023-27350	0.971240000	0.997900000	Link
CVE-2023-26469	0.942400000	0.991620000	Link
CVE-2023-26360	0.962720000	0.995220000	Link
CVE-2023-26035	0.969280000	0.997150000	Link
CVE-2023-25717	0.957880000	0.994220000	Link
CVE-2023-25194	0.969190000	0.997120000	Link
CVE-2023-2479	0.965320000	0.996000000	Link
CVE-2023-24489	0.974200000	0.999330000	Link
CVE-2023-23752	0.932080000	0.990390000	Link
CVE-2023-23397	0.926450000	0.989870000	Link
CVE-2023-23333	0.963260000	0.995390000	Link

CVE	EPSS	Perzentil	weitere Informationen
CVE-2023-22527	0.974360000	0.999440000	Link
CVE-2023-22518	0.966350000	0.996260000	Link
CVE-2023-22515	0.972310000	0.998340000	Link
CVE-2023-21839	0.958250000	0.994310000	Link
CVE-2023-21554	0.959390000	0.994540000	Link
CVE-2023-20887	0.963870000	0.995580000	Link
CVE-2023-1671	0.968860000	0.997020000	Link
CVE-2023-0669	0.969690000	0.997260000	Link

3.2 BSI - Warn- und Informationsdienst (WID)

Mon, 13 May 2024

[NEU] [hoch] Moodle: Mehrere Schwachstellen

Ein entfernter Angreifer kann mehrere Schwachstellen in Moodle ausnutzen, um beliebigen Code auszuführen, ReCAPTCHA zu umgehen, vertrauliche Informationen offenzulegen oder einen Cross-Site Scripting (XSS)-Angriff durchzuführen.

- Link

—

Mon, 13 May 2024

[NEU] [hoch] Cacti: Mehrere Schwachstellen

Ein entfernter, authentisierter Angreifer kann mehrere Schwachstellen in Cacti ausnutzen, um Sicherheitsvorkehrungen zu umgehen, Code auszuführen oder und SQL-Injection oder Cross-Site-Scripting Angriffe durchzuführen.

- Link

—

Mon, 13 May 2024

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

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

- Link

—

Mon, 13 May 2024

[NEU] [hoch] IBM Security Guardium: Mehrere Schwachstellen

Ein Angreifer kann mehrere Schwachstellen in IBM Security Guardium ausnutzen, um seine Privilegien zu erhöhen, beliebigen Code auszuführen, Sicherheitsmaßnahmen zu umgehen, einen Denial-of-Service-Zustand zu verursachen oder vertrauliche Informationen offenzulegen.

- Link

—

Mon, 13 May 2024

[UPDATE] [hoch] Red Hat Enterprise Linux (python-pillow): Mehrere Schwachstellen

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Red Hat Enterprise Linux in python-pillow ausnutzen, um einen Denial of Service Angriff durchzuführen und vertrauliche Informationen offenzulegen.

- Link

—

Mon, 13 May 2024

[UPDATE] [hoch] Apache Portable Runtime (APR): Mehrere Schwachstellen

Ein lokaler Angreifer kann mehrere Schwachstellen in Apache Portable Runtime (APR) ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial of Service Zustand herbeizuführen.

- Link

—

Mon, 13 May 2024

[UPDATE] [hoch] LibreOffice: Mehrere Schwachstellen

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

- Link

—

Mon, 13 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

—

Mon, 13 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

—

Mon, 13 May 2024

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

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

- Link

—

Mon, 13 May 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Mozilla Firefox, Mozilla Firefox ESR und Mozilla Thunderbird ausnutzen, um beliebigen Code auszuführen, vertrauliche Informationen offenzulegen, Sicherheitsmaßnahmen zu umgehen oder einen nicht spezifizierten Angriff durchzuführen.

- Link

—

Mon, 13 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

—

Mon, 13 May 2024

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

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

- Link

—

Mon, 13 May 2024

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

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

- Link

—

Mon, 13 May 2024

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

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Chrome / Microsoft Edge ausnutzen, um beliebigen Programmcode auszuführen und weitere, nicht spezifizierte Auswirkungen zu verursachen.

- Link

—

Mon, 13 May 2024

[UPDATE] [hoch] ffmpeg: Schwachstelle ermöglicht Codeausführung und DoS

Ein lokaler Angreifer kann eine Schwachstelle in ffmpeg ausnutzen, um beliebigen Programmcode auszuführen oder einen Denial-of-Service-Zustand zu verursachen.

- Link

—

Mon, 13 May 2024

[UPDATE] [hoch] less: Schwachstelle ermöglicht Codeausführung

Ein lokaler Angreifer kann eine Schwachstelle in less ausnutzen, um beliebigen Programmcode auszuführen.

- Link

—

Mon, 13 May 2024

[UPDATE] [hoch] FreeRDP: Mehrere Schwachstellen ermöglichen nicht spezifizierten Angriff

Ein Angreifer kann mehrere Schwachstellen in FreeRDP ausnutzen, um einen nicht näher spezifizierten Angriff durchzuführen.

- Link

—

Mon, 13 May 2024

[UPDATE] [hoch] ffmpeg: Mehrere Schwachstellen ermöglichen Denial of Service

Ein Angreifer kann mehrere Schwachstellen in ffmpeg ausnutzen, um einen Denial of Service Angriff durchzuführen.

- Link

—

Mon, 13 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

—

3.3 Sicherheitslücken Meldungen von Tenable

Datum	Schwachstelle	Bewertung
5/12/2024	[GLSA-202405-30 : Rebar3: Command Injection]	critical
5/11/2024	[RHEL 6 : chromium-browser (Unpatched Vulnerability)]	critical
5/13/2024	[RHEL 8 : squid:4 (RHSA-2024:2822)]	high
5/13/2024	[RHEL 9 : varnish (RHSA-2024:2820)]	high
5/13/2024	[RHEL 8 : bind and dhcp (RHSA-2024:2821)]	high
5/13/2024	[Ubuntu 22.04 LTS / 23.10 / 24.04 LTS : SQL parse vulnerability (USN-6771-1)]	high
5/13/2024	[Oracle Linux 7 : Unbreakable Enterprise kernel (ELSA-2024-12378)]	high
5/13/2024	[Google Chrome < 124.0.6367.207 Vulnerability]	high
5/13/2024	[macOS 12.x < 12.7.5 Multiple Vulnerabilities (HT214105)]	high
5/13/2024	[Apple iOS < 16.7.8 Multiple Vulnerabilities (HT214100)]	high
5/13/2024	[Amazon Linux AMI : kernel (ALAS-2024-1937)]	high
5/13/2024	[Amazon Linux 2023 : python3, python3-devel, python3-idle (ALAS2023-2024-616)]	high
5/13/2024	[Amazon Linux 2023 : flatpak, flatpak-devel, flatpak-libs (ALAS2023-2024-611)]	high
5/13/2024	[Amazon Linux 2023 : bpftool, kernel, kernel-devel (ALAS2023-2024-613)]	high
5/13/2024	[Amazon Linux 2023 : ecs-init (ALAS2023-2024-620)]	high
5/13/2024	[Amazon Linux 2023 : clamav, clamav-data, clamav-devel (ALAS2023-2024-615)]	high
5/13/2024	[Amazon Linux 2023 : python3.11, python3.11-devel, python3.11-idle (ALAS2023-2024-617)]	high
5/13/2024	[Amazon Linux 2023 : git, git-all, git-core (ALAS2023-2024-609)]	high

Datum	Schwachstelle	Bewertung
5/13/2024	[Amazon Linux AMI : golang (ALAS-2024-1938)]	high
5/13/2024	[Amazon Linux AMI : python38 (ALAS-2024-1936)]	high
5/13/2024	[macOS 13.x < 13.6.7 Multiple Vulnerabilities (HT214107)]	high
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 5 : wpa_supplicant (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

“Mon, 13 May 2024

Kemp LoadMaster Local sudo Privilege Escalation

This Metasploit module abuses a feature of the sudo command on Progress Kemp LoadMaster. Certain binary files are allowed to automatically elevate with the sudo command. This is based off of the file name. Some files have this permission are not write-protected from the default bal user. As such, if the file is overwritten with an arbitrary file, it will still auto-elevate. This module overwrites the /bin/loadkeys file with another executable.

- Link

—

” “Mon, 13 May 2024

Panel.SmokeLoader MVID-2024-0682 Cross Site Request Forgery / Cross Site Scripting

Panel.SmokeLoader malware suffers from cross site request forgery, and cross site scripting vulnerabilities.

- Link

—

” “Mon, 13 May 2024

Panel.SmokeLoader MVID-2024-0681 Cross Site Scripting

Panel.SmokeLoader malware suffers from a cross site scripting vulnerability.

- Link

—

” “Mon, 13 May 2024

Esteghlal F.C. Cross Site Scripting

Esteghlal F.C.’s site suffers from a cross site scripting vulnerability.

- Link

—

” “Mon, 13 May 2024

Arm Mali 5th Gen Dangling ATE

In mmu_insert_pages_no_flush(), when a HUGE_HEAD page is mapped to a 2M aligned GPU address, this is done by creating an Address Translation Entry (ATE) at MIDGARD_MMU_LEVEL(2) (in other words, an ATE covering 2M of memory is created). This is wrong because it assumes that at least 2M of memory should be mapped. mmu_insert_pages_no_flush() can be called in cases where less than that should be mapped, for example when creating a short alias of a big native allocation. Later, when kbase_mmu_teardown_pgd_pages() tries to tear down this region, it will detect that unmapping a subsection of a 2M ATE is not possible and write a log message complaining about this, but then proceed as if everything was fine while leaving the ATE intact. This means the higher-level code will proceed to free the referenced physical memory while the ATE still points to it.

- Link

—

” “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

SOPlanning 1.52.00 SQL Injection

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

- Link

—

” “Fri, 03 May 2024

SOPlanning 1.52.00 Cross Site Request Forgery

SOPlanning version 1.52.00 suffers from a cross site request forgery vulnerability in xajax_server.php.

- Link

—

” “Fri, 03 May 2024

SOPlanning 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

—

”

4.2 0-Days der letzten 5 Tage

“Mon, 13 May 2024

ZDI-24-441: Delta Electronics CNCSoft-B DOPSoft Uncontrolled Search Path Remote Code Execution Vulnerability

- Link

—

” “Mon, 13 May 2024

ZDI-24-440: Delta Electronics InfraSuite Device Master ActiveMQ Deserialization of Untrusted Data Remote Code Execution Vulnerability

- Link

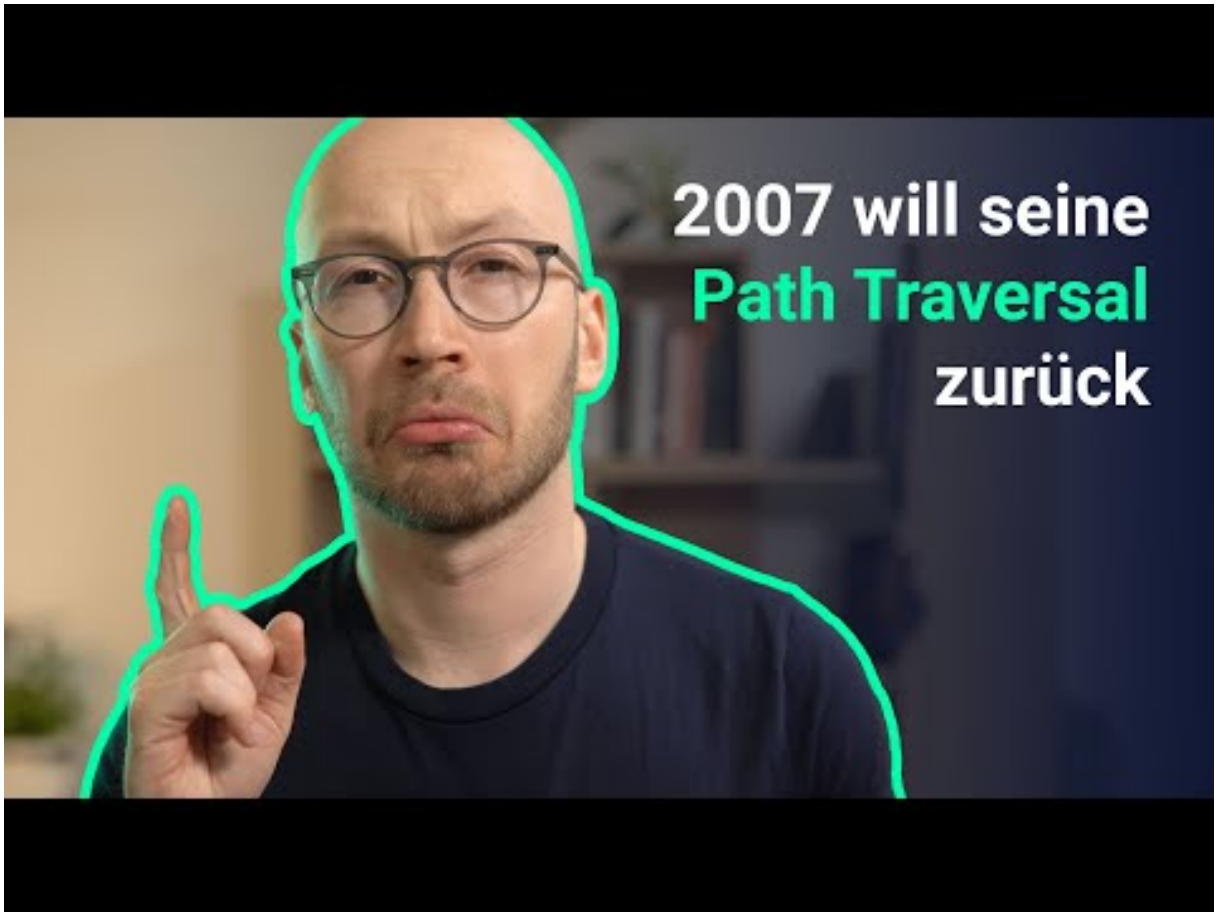
—

”

5 Die Hacks der Woche

mit Martin Haunschmid

5.0.1 2007 hat angerufen , 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]	Link
2024-05-06	DocGo	[USA]	Link
2024-05-06	Key Tronic Corporation	[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
2024-05-04	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
2024-05-01	Brandywine Realty Trust	[USA]	Link

7 Ransomware-Erpressungen: (Mai)

Datum	Opfer	Ransomware-Grupppe	Webseite
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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-05-13	[Eden Project Ltd]	incransom	Link
2024-05-13	[Helapet Ltd]	incransom	Link
2024-05-13	[oseranhahn.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
2024-05-12	[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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-05-11	[NHS (press update)]	incransom	Link
2024-05-11	[Jackson County]	blacksuit	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-05-09	[ufresources.com]	lockbit3	Link
2024-05-09	[cloudminds.com]	lockbit3	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-05-09	[auburnpikapp.org]	lockbit3	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-05-09	[depenning.com]	lockbit3	Link
2024-05-09	[asafoot.com]	lockbit3	Link
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	[ondozabal.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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-05-08	[Unimed Vales do Taquari e Rio Pardo]	rhysida	Link
2024-05-08	[Electric Mirror Inc]	incransom	Link
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	[Tholen Building Technology Group]	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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-05-07	[Chemring Group]	medusa	Link
2024-05-07	[lalengineering]	ransomhub	Link
2024-05-07	[skanlog.com]	lockbit3	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-05-07	[Young Consulting]	blacksuit	Link
2024-05-06	[Thaayakam LTD]	ransomhub	Link
2024-05-06	[The Weinstein Firm]	qilin	Link
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

Datum	Opfer	Ransomware-Grupppe	Webseite
2024-05-06	[M2E Consulting Engineers]	akira	Link
2024-05-06	[sunray.com]	lockbit3	Link
2024-05-06	[eviivo.com]	lockbit3	Link
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]	clop	Link
2024-05-04	[ikfhomefinance.com]	darkvault	Link
2024-05-04	[The Islamic Emirat of Afghanistan National Environmental Protection Agency]	ransomhub	Link

Datum	Opfer	Ransomware-Grupppe	Webseite
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
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	[MCS]	qilin	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

Datum	Opfer	Ransomware-Grupppe	Webseite
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	[watergate]	qilin	Link
2024-05-02	[Imedi L]	akira	Link
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.