May-08-23

CYBER WEEKLY AWARENESS REPORT

JOIN OUR ONLINE GROUP WHERE QUESTIONS LIKE "**HOW TO HACK FACEBOOK?**" ARE NOT ALLOWED
FACEBOOK.COM/GROUPS/CYBERSECRETS

ARGOS
APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity

May 8, 2023

The Cyber WAR (Weekly Awareness Report) is an Open Source Intelligence AKA OSINT resource focusing on advanced persistent threats and other digital dangers received by over ten thousand individuals. APTs fit into a cybercrime category directed at both business and political targets. Attack vectors include system compromise, social engineering, and even traditional espionage. Included are clickable links to news stories, vulnerabilities, exploits, & other industry risk.

Summary

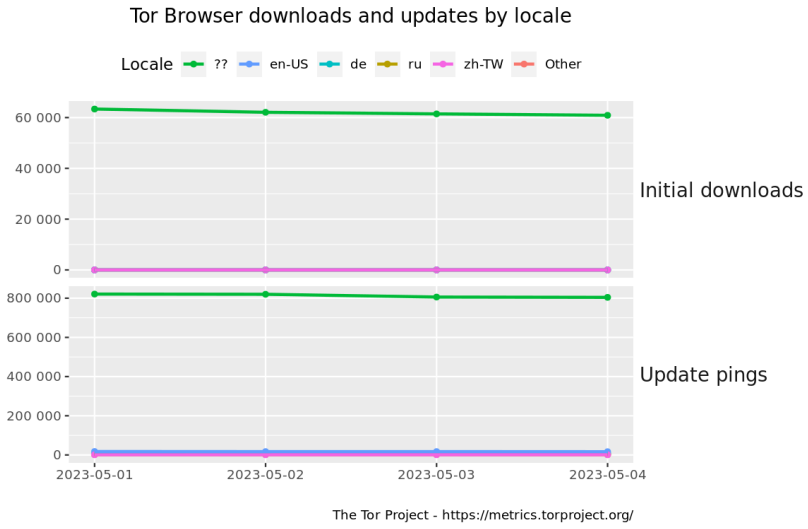
Internet Storm Center Infocon Status

The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

Other IWC Publications

Cyber Secrets books and ebook series can be found on Amazon.com at. amzn.to/2UuIG9B

Cyber Secrets was originally a video series and is on both YouTube.



Interesting News

* Free Cyberforensics Training - CSI Linux Basics

Download the distro and take the course to learn what CSI Linux can add to your arsenal. This include a case management solution, document templates (reports and legal docs), and more GUI options for gathering digital evidence while storing it to the ongoing case.
https://training.csilinux.com/course/view.php?id=5

* * Our active Facebook group discusses the gambit of cyber security issues. Join the Cyber Secrets Facebook group here.

Index of Sections

Packet Storm Security

* Ransomware Watchers Are Finding Creative Ways To Track Attacks
* Banks Warn Of Big Increase In Online Scams
* DEF CON To Set Thousands Of Hackers Loose On LLMs
* Twitter Admits To Security Incident Involving Circles Tweets
* Capita Admits Some Pension Data Likely Accessed In March Breach
* Cisco Warns RCE Bug In EOL IP Phone Adapters Won't Get Patched
* China Labels USA Empire Of Hacking Based On Old Wikileaks Dump
* Tennessee Health System Stops All Operations Amid Cyberattack Recovery
* Senator Asks Big Banks How They're Going To Stop AI Cloned Voices From Breaking Into Banks
* Ex-Uber CSO Gets Probation For Covering Up Theft Of Data On Millions Of People
* TikTok Spied On Me. Why?
* Google Will Retire Chrome's HTTPS Padlock Icon Because No One Knows What It Means
* Operation SpecTor Smashes Global Dark Web Drug Empire
* FTC Says Facebook Broke Terms Of $5B Data Privacy Settlement
* Facebook Cracks Down On Malware Actors Targeting Biz Accounts
* Go Ahead, Forget That Password. Use A Passkey Instead, Says Google
* Mirai Botnet Loves Exploiting Your Unpatched TP-Link Routers
* Microsoft Warns Iran Increasing Its Cyber Influence Operations
* Tor Project, LGBTQ Groups, And CDT Sound Alarm Over Efforts To Weaken Encryption
* Meta Says ChatGPT-Related Malware Is On The Rise
* Apple Uses Rapid Security Response Feature For The First Time
* T-Mobile Promises Better Security After Year's Second Breach
* White House To Study Employer Tools That Monitor Workers
* AI Godfather Geoffrey Hinton Warns Of Dangers As He Quits Google
* Russia's APT28 Targets Ukraine With Bogus Windows Updates

Krebs on Security

* $10M Is Yours If You Can Get This Guy to Leave Russia
* Promising Jobs at the U.S. Postal Service, 'US Job Services' Leaks Customer Data
* Many Public Salesforce Sites are Leaking Private Data
* 3CX Breach Was a Double Supply Chain Compromise
* Giving a Face to the Malware Proxy Service 'Faceless'
* Why is 'Juice Jacking' Suddenly Back in the News?
* Microsoft (& Apple) Patch Tuesday, April 2023 Edition
* FBI Seizes Bot Shop 'Genesis Market' Amid Arrests Targeting Operators, Suppliers
* A Serial Tech Investment Scammer Takes Up Coding?
* German Police Raid DDoS-Friendly Host 'FlyHosting'

Dark Reading

* Whiteford Taylor & Preston LLP Issues Notice of Data Incident
* Government, Industry Efforts to Thwart Ransomware Slowly Start to Pay Off
* 1M NextGen Patient Records Compromised in Data Breach
* Western Digital Confirms Customer Data Stolen in Ransomware Attack
* Why the 'Why' of a Data Breach Matters
* Why the FTX Collapse Was an Identity Problem
* North Korean APT Uses Malicious Microsoft OneDrive Links to Spread New Malware
* KnowBe4 Launches Password Kit to Celebrate World Password Day
* Satori Unveils Universal Data Permissions Scanner, a Free Open Source Tool that Sheds Light on Data A
* Browser Isolation Adapts to Remote Work, Greater Cloud Usage
* Judge Spares Former Uber CISO Jail Time Over 2016 Data Breach Charges
* Apple Patches Bluetooth Flaw in AirPods, Beats
* Attackers Route Malware Activity Over Popular CDNs
* New White House AI Initiatives Include AI Software-Vetting Event at DEF CON
* 2 Years After Colonial Pipeline, US Critical Infrastructure Still Not Ready for Ransomware
* The (Security) Cost of Too Much Data Privacy
* Unifying XDR and SIEM Capabilities in 1 Platform
* Google Expands Passkey Support With Passwordless Authentication
* Identifying Compromised Data Can Be a Logistical Nightmare
* Autocrypt Releases Comprehensive Key Management Solution for Automotive Manufacturing

The Hacker News

* Join Our Webinar: Learn How to Defeat Ransomware with Identity-Focused Protection
* MSI Data Breach: Private Code Signing Keys Leaked on the Dark Web
* Western Digital Confirms Customer Data Stolen by Hackers in March Breach
* SideCopy Using Action RAT and AllaKore RAT to infiltrate Indian Organizations
* How to Set Up a Threat Hunting and Threat Intelligence Program
* CERT-UA Warns of SmokeLoader and RoarBAT Malware Attacks Against Ukraine
* Dragon Breath APT Group Using Double-Clean-App Technique to Target Gambling Industry
* New Vulnerability in Popular WordPress Plugin Exposes Over 2 Million Sites to Cyberattacks
* New Android Malware 'FluHorse' Targeting East Asian Markets with Deceptive Tactics
* Hackers Targeting Italian Corporate Banking Clients with New Web-Inject Toolkit DrIBAN
* N. Korean Kimsuky Hackers Using New Recon Tool ReconShark in Latest Cyberattacks
* Lack of Visibility: The Challenge of Protecting Websites from Third-Party Scripts
* Packagist Repository Hacked: Over a Dozen PHP Packages with 500 Million Installs Compromised
* Fleckpe Android Malware Sneaks onto Google Play Store with Over 620,000 Downloads
* Cisco Warns of Vulnerability in Popular Phone Adapter, Urges Migration to Newer Model

Security Week

* Google Releases Open Source Bazel Plugin for Container Image Security
* Ransomware Group Claims Attack on Constellation Software
* Vulnerability in Field Builder Plugin Exposes Over 2M WordPress Sites to Attacks
* Private Tweets Exposed Due to Twitter Circle Security Bug
* 1 Million Impacted by Data Breach at NextGen Healthcare
* $1.1M Paid to Resolve Ransomware Attack on California County
* Western Digital Confirms Ransomware Group Stole Customer Information
* Pro-Russian Hackers Claim Downing of French Senate Website
* New Android Trojans Infected Many Devices in Asia via Google Play, Phishing
* Google Launches New Cybersecurity Analyst Training Program

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* Comprehensive Anti-Phishing Mitigations: A Quick Overview
* Blocking Social Engineering by Foreign Bad Actors: The Role of the New Foreign Malign Influence Cente
* [Eye Opener] HTML Phishing Attacks Surge by 100% in 12 Months
* A Master Class on IT Security: Roger Grimes Teaches You Phishing Mitigation
* [New Feature] Show Your C-Suite the ROI of Security Awareness Training with KnowBe4 Executive Reports
* CNBC: Why Nearly 80% of Leaders are Increasing Cybersecurity Spend
* Response-Based Business Email Compromise Contributes to 97% of Attacks
* Global Cyber Attacks Continue to Rise as Q1 Sees a 7% Increase
* Ransomware Attacks Surge 91% in a Single Month to Reach an All-Time High
* Walmart Jumps to Top of the List of the Worlds Most Impersonated Brands Used in Phishing Attacks

ISC2.org Blog

Unfortunately, at the time of this report, the ISC2 Blog resource was not availible.

HackRead

* Cyberpress Launches Cybersecurity Press Release Distribution Platform
* Transferring WhatsApp Data Between Android and iPhone [2023]
* Cyberpress Launches Cybersecurity Press Release Distribution Platform
* Seized: 9 Crypto Laundering Sites Used by Ransomware Gangs
* What are Residential proxies and what is their use?
* Card Skimmers and ATMs Used to Drain EBT Accounts in SoCal
* Mullvad VPN's Office Raided By Police for User Data

Koddos

* Cyberpress Launches Cybersecurity Press Release Distribution Platform
* Transferring WhatsApp Data Between Android and iPhone [2023]
* Cyberpress Launches Cybersecurity Press Release Distribution Platform
* Seized: 9 Crypto Laundering Sites Used by Ransomware Gangs
* What are Residential proxies and what is their use?
* Card Skimmers and ATMs Used to Drain EBT Accounts in SoCal
* Mullvad VPN's Office Raided By Police for User Data

Naked Security

* PHP Packagist supply chain poisoned by hacker "looking for a job"
* S3 Ep133: Apple takes "tight-lipped" to a whole new level
* World Password Day: 2 + 2 = 4
* Tracked by hidden tags? Apple and Google unite to propose safety and security standards…
* Apple delivers first-ever Rapid Security Response "cyberattack" patch - leaves some users confused
* Mac malware-for-hire steals passwords and cryptocoins, sends "crime logs" via Telegram
* Google wins court order to force ISPs to filter botnet traffic
* S3 Ep132: Proof-of-concept lets anyone hack at will
* Google leaking 2FA secrets - researchers advise against new "account sync" feature for now
* PaperCut security vulnerabilities under active attack - vendor urges customers to patch

Threat Post

* Student Loan Breach Exposes 2.5M Records
* Watering Hole Attacks Push ScanBox Keylogger
* Tentacles of '0ktapus' Threat Group Victimize 130 Firms
* Ransomware Attacks are on the Rise
* Cybercriminals Are Selling Access to Chinese Surveillance Cameras
* Twitter Whistleblower Complaint: The TL;DR Version
* Firewall Bug Under Active Attack Triggers CISA Warning
* Fake Reservation Links Prey on Weary Travelers
* iPhone Users Urged to Update to Patch 2 Zero-Days
* Google Patches Chrome's Fifth Zero-Day of the Year

Null-Byte

* These High-Quality Courses Are Only $49.99
* How to Perform Advanced Man-in-the-Middle Attacks with Xerosploit
* The Best-Selling VPN Is Now on Sale
* Unlock Facial Detection & Recognition on the Inexpensive ESP32-Based Wi-Fi Spy Camera
* Learn C# & Start Designing Games & Apps
* How to Set Up a Wi-Fi Spy Camera with an ESP32-CAM
* Get a Jump Start into Cybersecurity with This Bundle
* Hack Networks & Devices Right from Your Wrist with the Wi-Fi Deauther Watch
* This Top-Rated Course Will Make You a Linux Master
* Fingerprint Web Apps & Servers for Better Recon & More Successful Hacks

IBM Security Intelligence

* How the ZeuS Trojan Info Stealer Changed Cybersecurity
* Why Robot Vacuums Have Cameras (and What to Know About Them)
* What "Beginner" Skills do Security Leaders Need to Refresh?
* 79% of Cyber Pros Make Decisions Without Threat Intelligence
* Is Your Critical SaaS Data Secure?
* Rationalizing Your Hybrid Cloud Security Tools
* ChatGPT Confirms Data Breach, Raising Security Concerns
* Expert Insights on the X-Force Threat Intelligence Index
* How Morris Worm Command and Control Changed Cybersecurity
* Why People Skills Matter as Much as Industry Experience

InfoWorld

* Somehow OpenSearch has succeeded
* Kubernetes cost management for the real world
* Visual Studio Code 1.78 debuts profile templates for Python, Java, Angular
* Configure finops processes with the right metrics
* Databricks doubles down in India with staff hires, new R&D hub
* JDK 21: The new features in Java 21
* DataStax's new LunaML to support Kaskada deployment
* ServiceNow, Hugging Face's free StarCoder LLM takes on Copilot, CodeWhisperer
* R tutorials: Learn R programming for data science
* Databricks acquires AI-centric Okera to aid data governance in LLMs

C4ISRNET - Media for the Intelligence Age Military

* Unmanned program could suffer if Congress blocks F-22 retirements, Hunter says
* UK to test Sierra Nevada's high-flying spy balloons
* Babcock inks deals to pitch Israeli tech for British radar, air defense programs
* This infantry squad vehicle is getting a laser to destroy drones
* As Ukraine highlights value of killer drones, Marine Corps wants more
* Army Space, Cyber and Special Operations commands form 'triad' to strike anywhere, anytime
* Shell companies purchase radioactive materials, prompting push for nuclear licensing reform
* Marine regiment shows off capabilities at RIMPAC ahead of fall experimentation blitz
* Maxar to aid L3Harris in tracking missiles from space
* US Army's 'Lethality Task Force' looks to save lives with AI

The Hacker Corner

Conferences

* 5 Things That Make The DEF CON Experience Special
* The 5 Most Controversial DEF CON Talks Of All Time
* 6 Notable DEF CON Moments
* Best AI Conferences To Attend in 2023
* How To Organize A Conference? Here's How To Get It Right!
* Virtual Conferences Marketing & Technology
* How To Plan an Event Marketing Strategy
* Zero Trust Cybersecurity Companies
* Types of Major Cybersecurity Threats In 2022
* The Five Biggest Trends In Cybersecurity In 2022

Google Zero Day Project

* Release of a Technical Report into Intel Trust Domain Extensions
* Multiple Internet to Baseband Remote Code Execution Vulnerabilities in Exynos Modems

Capture the Flag (CTF)

CTF Time has links to a lot of current Capture the Flag competitions and information on past events. Below is a list if CTFs they have on thier calendar.

* m0leCon CTF 2023 Teaser
* HackDay Final 2023
* HackTM CTF Finals 2023
* HeroCTF v5
* Crypt_Find
* p4ctf 2023 teaser
* Challenge the Cyber - Aquatic Adventure
* VolgaCTF 2023 Qualifier
* DeadSec CTF 2023
* Grey Cat The Flag 2023 Qualifiers

VulnHub Downloadable CTFs for your Cyber Range (Most use VirtualBox)

* Matrix-Breakout: 2 Morpheus
* Web Machine: (N7)
* The Planets: Earth
* Jangow: 1.0.1
* Red: 1

Tools & Techniques

Packet Storm Security Tools Links

* Clam AntiVirus Toolkit 1.1.0
* MIMEDefang Email Scanner 3.4.1
* MIMEDefang Email Scanner 3.4
* FortiGate Brute Forcer
* American Fuzzy Lop plus plus 4.06c
* I2P 2.2.1
* Suricata IDPE 6.0.11
* Wireshark Analyzer 4.0.5
* Faraday 4.3.5
* Zeek 5.0.8

Kali Linux Tutorials

* Wifi_Db : Script To Parse Aircrack-ng Captures To A SQLite Database
* Seekr : A Multi-Purpose OSINT Toolkit With A Neat Web-Interface
* Grepmarx : A Source Code Static Analysis Platform For AppSec Enthusiasts
* Shoggoth - Asmjit Based Polymorphic Encryptor
* CMLoot : Find Interesting Files Stored On (System Center) Configuration Manager (SCCM/CM) SMB Shares
* RedditC2 : Abusing Reddit API To Host The C2 Traffic
* Noseyparker : Find Secrets And Sensitive Information In Textual Data And Git History
* MSI Dump : A Tool That Analyzes Malicious MSI Installation
* How to Use Social Engineering Toolkit(SET) - A Complete Guide
* Fingerprintx : Standalone Utility For Service Discovery On Open Ports!

GBHackers Analysis

* Microsoft Changed the Method of Naming the Hacker Groups
* Accidental 'write' Permissions In Alibaba PostgreSQL Let Attackers Access Sensitive Data
* Ex-Conti and FIN7 Hackers Team Up To Develop Domino Backdoor Malware
* ChatGPT Account Takeover Bug Allows Hackers To Gain User's Online Account
* Used Routers Fully Loaded With Corporate Secrets for Just $100

Weekly Cyber Security Video and Podcasts

SANS DFIR

* SANS Threat Analysis Rundown | Katie Nickels
* FOR498 - New Course Name, New Content & A Whole Lot of Actionable Intelligence in 90 min or less
* Cloud-Powered DFIR: Harnessing the cloud to improve investigator efficiency
* Breaking the Ransomware Tool Set: When a Threat Actor Opsec

Defcon Conference

* DEF CON 30 - Cesare Pizzi - Old Malware, New tools: Ghidra and Commodore 64
* DEF CON 30 BiC Village - Segun Olaniyan- Growth Systems for Cybersecurity Enthusiasts
* DEF CON 30 - Silk - DEF CON Memorial Interview
* DEF CON 30 Car Hacking Village - Evadsnibor - Getting Naughty on CAN bus with CHV Badge

Hak5

* Malicious OAuth Apps Hide Themselves In Plain Sight - ThreatWire
* The RESTRICT Act: TLDR? Watch This - ThreatWire
* Should AI Training Be Paused? - ThreatWire

The PC Security Channel [TPSC]

* Network Security Tools to stop hackers
* 3CX: How this malware almost hacked every business

Eli the Computer Guy

* OpenAI Dall-E API Image Creation and Manipulation with Python - Hands on Class
* STARTUP MEETUP in ASHEVILLE NC - Fireside Chats with Founders
* CHATGPT API and PYTHON - Hands on Class
* TKINTER INTRO - GUI APPS IN PYTHON - Hands on Class

Security Now

* OSB OMG and Other News! - Age verification, Google Authenticator E2EE, VirusTotal AI, cURL
* An End-to-End Encryption Proposal - Wipe those routers, Lockdown Mode, ChatGPT black market

Troy Hunt

* Weekly Update 346

Intel Techniques: The Privacy, Security, & OSINT Show

* 295-Breach Data Collection Revisited
* 294-Preparing for Home Disaster

Proof of Concept (PoC) & Exploits

Packet Storm Security

* FICO Origination Manager Decision Module 4.8.1 XSS / Session Hijacking
* BlogMagz CMS 1.0 Cross Site Scripting
* Found Information System 1.0 SQL Injection
* Rollout::UI 0.5 Cross Site Scripting
* Oracle RMAN Missing Auditing
* Online Pizza Ordering System 1.0 Shell Upload
* Codigo Markdown Editor 1.0.1 Code Execution
* Shannon Baseband Integer Overflow
* UliCMS 2023-1 Sniffing-Vicuna Shell Upload
* UliCMS 2023-1 Sniffing-Vicuna Cross Site Scripting
* File Thingie 2.5.7 Shell Upload
* Wolf CMS 0.8.3.1 Shell Upload
* Pluck CMS 4.7.18 Cross Site Scripting
* EasyPHP Webserver 14.1 Path Traversal / Remote Code Execution
* Jedox 2022.4.2 Database Credential Disclosure
* Jedox 2020.2.5 Database Credential Disclosure
* Jedox 2020.2.5 Groovy-Scripts Remote Code Execution
* Jedox 2020.2.5 Configurable Storage Path Remote Code Execution
* Jedox 2020.2.5 Cross Site Scripting
* Jedox 2022.4.2 Directory Traversal / Remote Code Execution
* Jedox 2022.4.2 RPC Interface Remote Code Execution
* Shannon Baseband fmtp SDP Attribute Memory Corruption
* Companymaps 8.0 SQL Injection
* Companymaps 8.0 Cross Site Scripting
* Shannon Baseband acfg / pcfg SDP Attribute Memory Corruption

CXSecurity

* File Thingie 2.5.7 Shell Upload
* Adobe ColdFusion Unauthenticated Remote Code Execution
* Fortigate 7.0.1 Stack Overflow
* Sielco PolyEco Digital FM Transmitter 2.0.6 Authentication Bypass Exploit
* Lilac-Reloaded For Nagios 2.0.8 Remote Code Execution
* Chitor-CMS 1.1.2 SQL Injection
* Mware Workspace ONE Remote Code Execution

Proof of Concept (PoC) & Exploits

Exploit Database

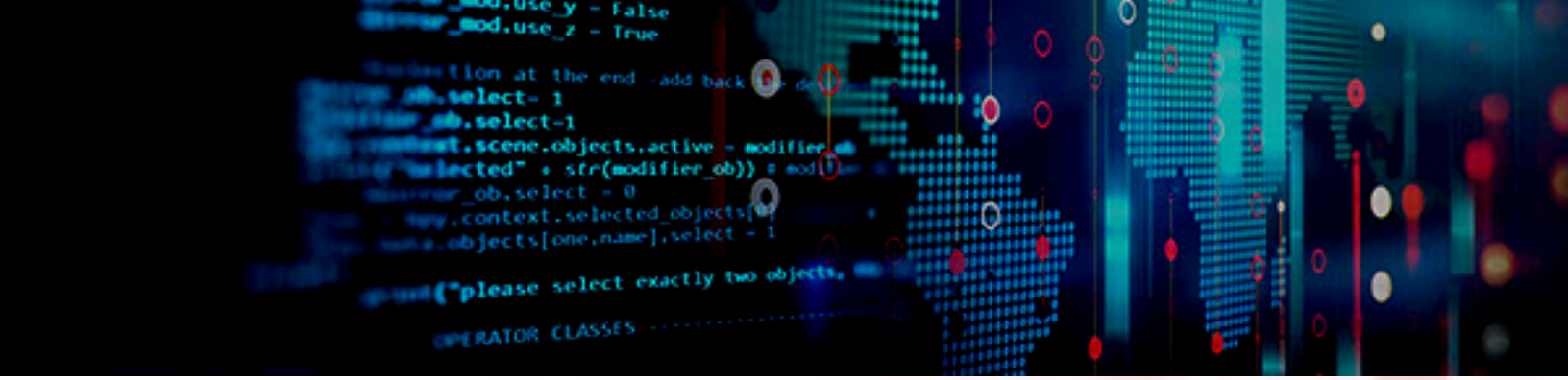
* [webapps] File Thingie 2.5.7 - Remote Code Execution (RCE)
* [webapps] Ulicms-2023.1 sniffing-vicuna - Stored Cross-Site Scripting (XSS)
* [webapps] Ulicms-2023.1 sniffing-vicuna - Remote Code Execution (RCE)
* [local] Codigo Markdown Editor v1.0.1 (Electron) - Remote Code Execution
* [webapps] Online Pizza Ordering System v1.0 - Unauthenticated File Upload
* [webapps] EasyPHP Webserver 14.1 - Multiple Vulnerabilities (RCE and Path Traversal)
* [webapps] Jedox 2022.4.2 - Disclosure of Database Credentials via Connection Checks
* [webapps] Jedox 2020.2.5 - Disclosure of Database Credentials via Improper Access Controls
* [webapps] Jedox 2020.2.5 - Remote Code Execution via Executable Groovy-Scripts
* [webapps] Jedox 2020.2.5 - Remote Code Execution via Configurable Storage Path
* [webapps] Jedox 2020.2.5 - Stored Cross-Site Scripting in Log-Module
* [webapps] Jedox 2022.4.2 - Remote Code Execution via Directory Traversal
* [webapps] Jedox 2022.4.2 - Code Execution via RPC Interfaces
* [webapps] Cmaps v8.0 - SQL injection
* [webapps] Wolf CMS 0.8.3.1 - Remote Code Execution (RCE)
* [webapps] pluck v4.7.18 - Stored Cross-Site Scripting (XSS)
* [webapps] KodExplorer v4.51.03 - Pwned-Admin File-Inclusion - Remote Code Execution (RCE)
* [webapps] GLPI 9.5.7 - Username Enumeration
* [webapps] Companymaps v8.0 - Stored Cross Site Scripting (XSS)
* [webapps] PHPJabbers Simple CMS 5.0 - SQL Injection
* [webapps] PHPJabbers Simple CMS V5.0 - Stored Cross-Site Scripting (XSS)
* [local] FS-S3900-24T4S - Privilege Escalation
* [webapps] OpenEMR v7.0.1 - Authentication credentials brute force
* [local] Advanced Host Monitor v12.56 - Unquoted Service Path
* [webapps] PHPFusion 9.10.30 - Stored Cross-Site Scripting (XSS)

Exploit Database for offline use

Kali has the Exploit-DB preinstalled and updates the database on a monthly basis. The tool that they have added is called "SearchSploit". This can be installed on Linux, Mac, and Windows. Using the tool is also quite simple. In the command line, type:

user@yourlinux:~$ *searchsploit keyword1 keyword2*

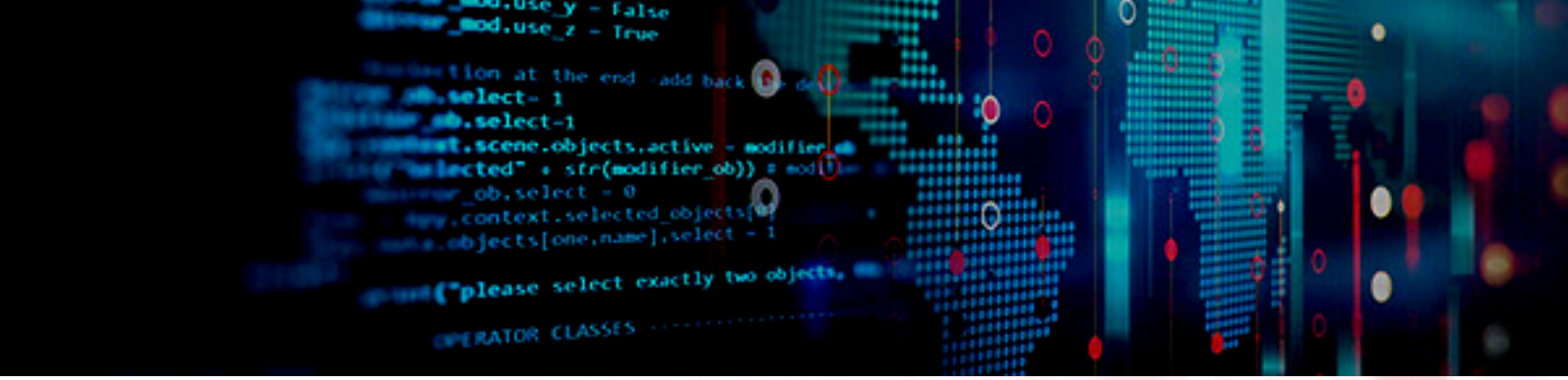
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://ejournal.perpusnas.go.id/public/site/images/admin4/mwhehe.gif
https://ejournal.perpusnas.go.id/public/site/images/admin4/mwhehe.gif notified by Simsimi
https://jurnal.kebumenkab.go.id//public/site/images/admin/mwhehe.gif
https://jurnal.kebumenkab.go.id//public/site/images/admin/mwhehe.gif notified by Simsimi
https://simpeg.kalbarprov.go.id/fotosimpeg/195907011986111003/mwhehe.gif
https://simpeg.kalbarprov.go.id/fotosimpeg/195907011986111003/mwhehe.gif notified by Simsimi
https://suporteti.defensoria.pr.def.br/zct.txt
https://suporteti.defensoria.pr.def.br/zct.txt notified by CyberTeam
http://pnsa.gov.ps
http://pnsa.gov.ps notified by SOK
https://ditjenpkp2trans.kemendesa.go.id/el.htm
https://ditjenpkp2trans.kemendesa.go.id/el.htm notified by ./An9el4-137
https://blm-banjarmasin.kemendesa.go.id/el.htm
https://blm-banjarmasin.kemendesa.go.id/el.htm notified by ./An9el4-137
https://blm-makassar.kemendesa.go.id/el.htm
https://blm-makassar.kemendesa.go.id/el.htm notified by ./An9el4-137
https://ditjenpdtu.kemendesa.go.id/el.htm
https://ditjenpdtu.kemendesa.go.id/el.htm notified by ./An9el4-137
https://blm-jayapura.kemendesa.go.id/el.htm
https://blm-jayapura.kemendesa.go.id/el.htm notified by ./An9el4-137
https://itjen.kemendesa.go.id/el.htm
https://itjen.kemendesa.go.id/el.htm notified by ./An9el4-137
https://blm-ambon.kemendesa.go.id/el.htm
https://blm-ambon.kemendesa.go.id/el.htm notified by ./An9el4-137
https://bblm-yogyakarta.kemendesa.go.id/el.htm
https://bblm-yogyakarta.kemendesa.go.id/el.htm notified by ./An9el4-137
https://bbplm-jakarta.kemendesa.go.id/el.htm
https://bbplm-jakarta.kemendesa.go.id/el.htm notified by ./An9el4-137
https://sircov.gouv.cg/el.htm
https://sircov.gouv.cg/el.htm notified by ./An9el4-137
https://workflow.mwri.gov.eg/el.htm
https://workflow.mwri.gov.eg/el.htm notified by ./An9el4-137
https://mpp.sulselprov.go.id/galau.html
https://mpp.sulselprov.go.id/galau.html notified by ./Fell Ganns

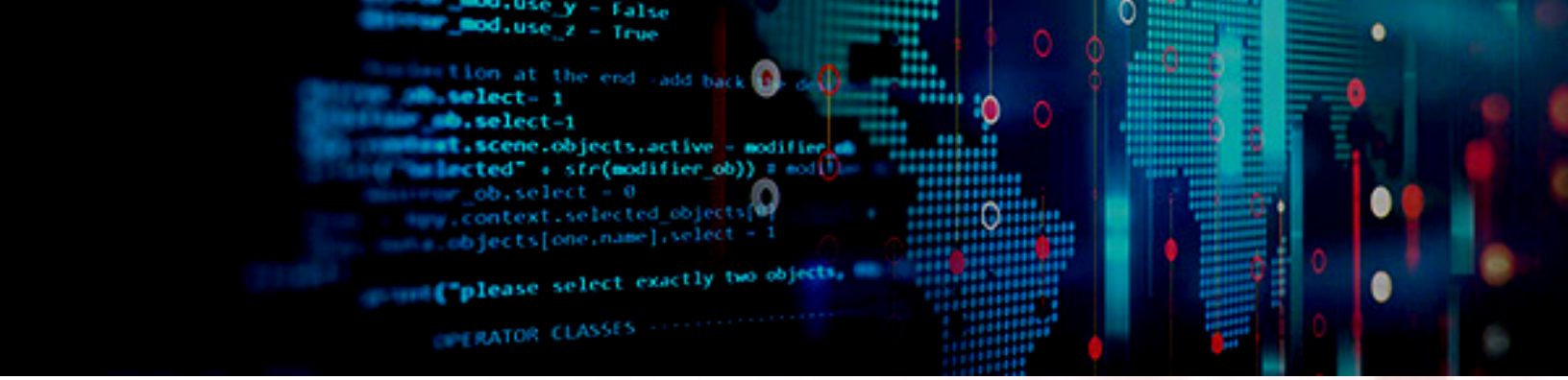


Dark Web News

Darknet Live

[Operation SpecTor: Hundreds of Vendors Arrested]
[Ohio Man Imprisoned for Stealing Seized Bitcoin]
[Australian Cannabis Vendor Busted]
[Washington Fraudster Sentenced to Prison]

Dark Web Link



Trend Micro Anti-Malware Blog

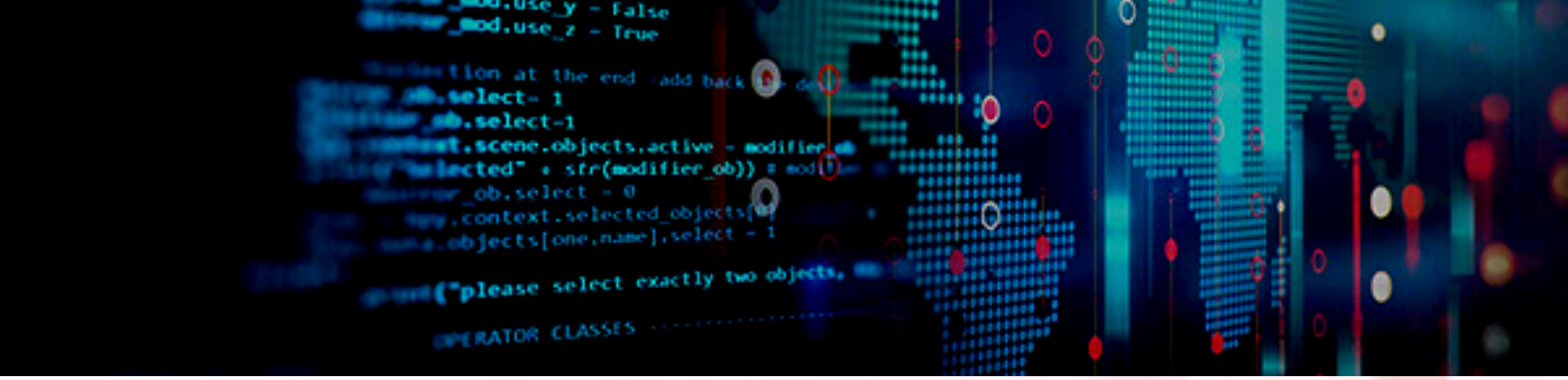
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

* Skimming for Sale: Commodity Skimming and Magecart Trends in Q1 2022
* RiskIQ Threat Intelligence Roundup: Phishing, Botnets, and Hijacked Infrastructure
* RiskIQ Threat Intelligence Roundup: Trickbot, Magecart, and More Fake Sites Targeting Ukraine
* RiskIQ Threat Intelligence Roundup: Campaigns Targeting Ukraine and Global Malware Infrastructure
* RiskIQ Threat Intelligence Supercharges Microsoft Threat Detection and Response
* RiskIQ Intelligence Roundup: Spoofed Sites and Surprising Infrastructure Connections
* RiskIQ Threat Intelligence Roundup: QBot, Magecart, Agent Tesla Headline Hijacked Infrastructure
* RiskIQ Threat Intelligence Roundup: C2 and Nation-State Threat Infrastructure
* Jupyter Notebooks Make RiskIQ Data a Digital 'Mech Suit' for Threat Intelligence Analysts
* "Offshore" Shinjiru Provides Bulletproof Services to Cyberattackers

FireEye

* Metasploit Weekly Wrap-Up
* AppDomain Manager Injection: New Techniques For Red Teams
* Cloud Security Strategies for Manufacturing
* Three Takeaways from the GartnerÂ® Market Guide for Managed Detection and Response Services
* Metasploit Weekly Wrap-Up
* New InsightCloudSec Compliance Pack: Implementing and Enforcing ISO 27001:2022
* Using Rapid7 Insight Agent and InsightVM Scan Assistant in Tandem
* Starting a Career in Tech? Learn How Rapid7's Emerging Talent Programmes Foster Long-Term Success
* 4 Takeaways from the 2023 GartnerÂ® Market Guide for CNAPP
* Metasploit Weekly Wrap-Up



Advisories

US-Cert Alerts & bulletins

* CISA Releases One Industrial Control Systems Advisory
* CISA Releases One Industrial Control Systems Advisory
* CISA Urges Organizations to Incorporate the FCC Covered List Into Risk Management Plans
* CISA Adds Three Known Exploited Vulnerabilities to Catalog
* CISA Requests for Comment on Secure Software Self-Attestation Form
* CISA Releases One Industrial Control Systems Medical Advisory
* CISA Releases Two Industrial Control Systems Advisories
* Abuse of the Service Location Protocol May Lead to DoS Attacks
* APT28 Exploits Known Vulnerability to Carry Out Reconnaissance and Deploy Malware on Cisco Routers
* #StopRansomware: LockBit 3.0
* Vulnerability Summary for the Week of January 31, 2011
* Summary of Security Items from February 2 through February 8, 2006

Zero Day Initiative Advisories

ZDI-CAN-20818: Siemens
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-05-08, 0 days ago. The vendor is given until 2023-09-05 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-20840: Siemens
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-05-08, 0 days ago. The vendor is given until 2023-09-05 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-20825: Siemens
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-05-08, 0 days ago. The vendor is given until 2023-09-05 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-20826: Siemens
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-05-08, 0 days ago. The vendor is given until 2023-09-05 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-20942: JRuby
A CVSS score 8.1 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Pratik Shetty' was reported to the affected vendor on: 2023-05-08, 0 days ago. The vendor is given until 2023-09-05 to

publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20525: Adtran

A CVSS score 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'ther3d0ne - https://thered0ne.com' was reported to the affected vendor on: 2023-05-05, 3 days ago. The vendor is given until 2023-09-02 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21068: Microsoft

A CVSS score 5.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-05-05, 3 days ago. The vendor is given until 2023-09-02 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21072: Microsoft

A CVSS score 5.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-05-05, 3 days ago. The vendor is given until 2023-09-02 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21077: Adtran

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'ther3d0ne - https://thered0ne.com' was reported to the affected vendor on: 2023-05-05, 3 days ago. The vendor is given until 2023-09-02 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20695: Microsoft

A CVSS score 7.0 (AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mikhail Shcherbakov (@yu5k3)' was reported to the affected vendor on: 2023-05-05, 3 days ago. The vendor is given until 2023-09-02 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21071: Microsoft

A CVSS score 5.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-05-05, 3 days ago. The vendor is given until 2023-09-02 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21070: Microsoft

A CVSS score 5.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-05-05, 3 days ago. The vendor is given until 2023-09-02 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21069: Microsoft

A CVSS score 5.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-05-05, 3 days ago. The vendor is given until 2023-09-02 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21073: Microsoft

A CVSS score 5.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-05-05, 3 days ago. The vendor is given until 2023-09-02 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20842: Siemens

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous'

was reported to the affected vendor on: 2023-05-05, 3 days ago. The vendor is given until 2023-09-02 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21078: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-05-04, 4 days ago. The vendor is given until 2023-09-01 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20970: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-05-03, 5 days ago. The vendor is given until 2023-08-31 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21001: Cacti

A CVSS score 6.6 (AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-05-03, 5 days ago. The vendor is given until 2023-08-31 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20606: Delta Electronics

A CVSS score 6.5 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-05-03, 5 days ago. The vendor is given until 2023-08-31 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20531: Triangle MicroWorks

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Li Jiantao, Ngo Wei Lin, Pan Zhenpeng of STAR Labs SG Pte. Ltd.' was reported to the affected vendor on: 2023-05-03, 5 days ago. The vendor is given until 2023-08-31 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20995: SolarWinds

A CVSS score 7.2 (AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Piotr Bazydlo (@chudypb) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-05-03, 5 days ago. The vendor is given until 2023-08-31 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20767: Cacti

A CVSS score 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-05-03, 5 days ago. The vendor is given until 2023-08-31 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20913: Canonical

A CVSS score 7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Stonejiajia' was reported to the affected vendor on: 2023-05-03, 5 days ago. The vendor is given until 2023-08-31 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20793: Schneider Electric

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Sina Kheirkhah (@SinSinology) of Summoning Team (@SummoningTeam) ' was reported to the affected vendor on: 2023-05-03, 5 days ago. The vendor is given until 2023-08-31 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Ubuntu Security Notice USN-6060-1

Ubuntu Security Notice 6060-1 - Multiple security issues were discovered in MySQL and this update includes new upstream MySQL versions to fix these issues. MySQL has been updated to 8.0.33 in Ubuntu 20.04 LTS, Ubuntu 22.04 LTS, Ubuntu 22.10, and Ubuntu 23.04. Ubuntu 18.04 LTS has been updated to MySQL 5.7.42. In addition to security fixes, the updated packages contain bug fixes, new features, and possibly incompatible changes.

Ubuntu Security Notice USN-6059-1

Ubuntu Security Notice 6059-1 - It was discovered that Erlang did not properly implement TLS client certificate validation during the TLS handshake. A remote attacker could use this issue to bypass client authentication.

Ubuntu Security Notice USN-6055-2

Ubuntu Security Notice 6055-2 - USN-6055-1 fixed a vulnerability in Ruby. Unfortunately it introduced a regression. This update reverts the patches applied to CVE-2023-28755 in order to fix the regression pending further investigation. It was discovered that Ruby incorrectly handled certain regular expressions. An attacker could possibly use this issue to cause a denial of service.

Debian Security Advisory 5399-1

Debian Linux Security Advisory 5399-1 - Several vulnerabilities were discovered in odoo, a suite of web based open source business apps.

Ubuntu Security Notice USN-6058-1

Ubuntu Security Notice 6058-1 - It was discovered that the Traffic-Control Index implementation in the Linux kernel did not properly perform filter deactivation in some situations. A local attacker could possibly use this to gain elevated privileges.

Debian Security Advisory 5398-1

Debian Linux Security Advisory 5398-1 - Multiple security issues were discovered in Chromium, which could result in the execution of arbitrary code, denial of service or information disclosure.

wfc-pkt-router Incorrect Bind

wfc-pkt-router suffers from a vulnerability where it can wrongly bind to an external network interface instead of the VPN tunnel.

Ubuntu Security Notice USN-6057-1

Ubuntu Security Notice 6057-1 - It was discovered that the Traffic-Control Index implementation in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. It was discovered that the OverlayFS implementation in the Linux kernel did not properly handle copy up operation in some conditions. A local attacker could possibly use this to gain elevated privileges.

Red Hat Security Advisory 2023-2137-01

Red Hat Security Advisory 2023-2137-01 - Samba is an open-source implementation of the Server Message Block protocol and the related Common Internet File System protocol, which allow PC-compatible machines to share files, printers, and various information.

Red Hat Security Advisory 2023-2136-01

Red Hat Security Advisory 2023-2136-01 - Samba is an open-source implementation of the Server Message Block protocol and the related Common Internet File System protocol, which allow PC-compatible machines to share files, printers, and various information.

Debian Security Advisory 5396-2

Debian Linux Security Advisory 5396-2 - The webkit2gtk update released as 5396-1 introduced a compatibility problem that caused Evolution to display e-mail incorrectly. Evolution has been updated to solve this issue.

Ubuntu Security Notice USN-6056-1

Ubuntu Security Notice 6056-1 - It was discovered that a race condition existed in the Xen transport layer implementation for the 9P file system protocol in the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or expose sensitive information.

Red Hat Security Advisory 2023-2126-01

Red Hat Security Advisory 2023-2126-01 - Libreswan is an implementation of IPsec and IKE for Linux. IPsec is the Internet Protocol Security and uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks such as virtual private network.

Apple Security Advisory 2023-05-03-1

Apple Security Advisory 2023-05-03-1 - AirPods Firmware Update 5E133 and Beats Firmware Update 5B66 address bluetooth authentication vulnerabilities.

Red Hat Security Advisory 2023-2124-01

Red Hat Security Advisory 2023-2124-01 - Libreswan is an implementation of IPsec and IKE for Linux. IPsec is the Internet Protocol Security and uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks such as virtual private network.

Red Hat Security Advisory 2023-2121-01

Red Hat Security Advisory 2023-2121-01 - Libreswan is an implementation of IPsec and IKE for Linux. IPsec is the Internet Protocol Security and uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks such as virtual private network.

Red Hat Security Advisory 2023-2122-01

Red Hat Security Advisory 2023-2122-01 - Libreswan is an implementation of IPsec and IKE for Linux. IPsec is the Internet Protocol Security and uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks such as virtual private network.

Red Hat Security Advisory 2023-2120-01

Red Hat Security Advisory 2023-2120-01 - Libreswan is an implementation of IPsec and IKE for Linux. IPsec is the Internet Protocol Security and uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks such as virtual private network.

Red Hat Security Advisory 2023-2125-01

Red Hat Security Advisory 2023-2125-01 - Libreswan is an implementation of IPsec and IKE for Linux. IPsec is the Internet Protocol Security and uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks such as virtual private network.

Red Hat Security Advisory 2023-2123-01

Red Hat Security Advisory 2023-2123-01 - Libreswan is an implementation of IPsec and IKE for Linux. IPsec is the Internet Protocol Security and uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks such as virtual private network.

Red Hat Security Advisory 2023-2127-01

Red Hat Security Advisory 2023-2127-01 - Samba is an open-source implementation of the Server Message Block protocol and the related Common Internet File System protocol, which allow PC-compatible machines to share files, printers, and various information.

Ubuntu Security Notice USN-6055-1

Ubuntu Security Notice 6055-1 - It was discovered that Ruby incorrectly handled certain regular expressions. An attacker could possibly use this issue to cause a denial of service. It was discovered that Ruby incorrectly handled certain regular expressions. An attacker could possibly use this issue to cause a denial of service. This issue is being addressed only for Ubuntu 18.04 LTS and Ubuntu 20.04 LTS.

Red Hat Security Advisory 2023-2107-01

Red Hat Security Advisory 2023-2107-01 - The Migration Toolkit for Containers (MTC) 1.7.9 is now available.

Red Hat Product Security has rated this update as having a security impact of Moderate. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2023-2104-01

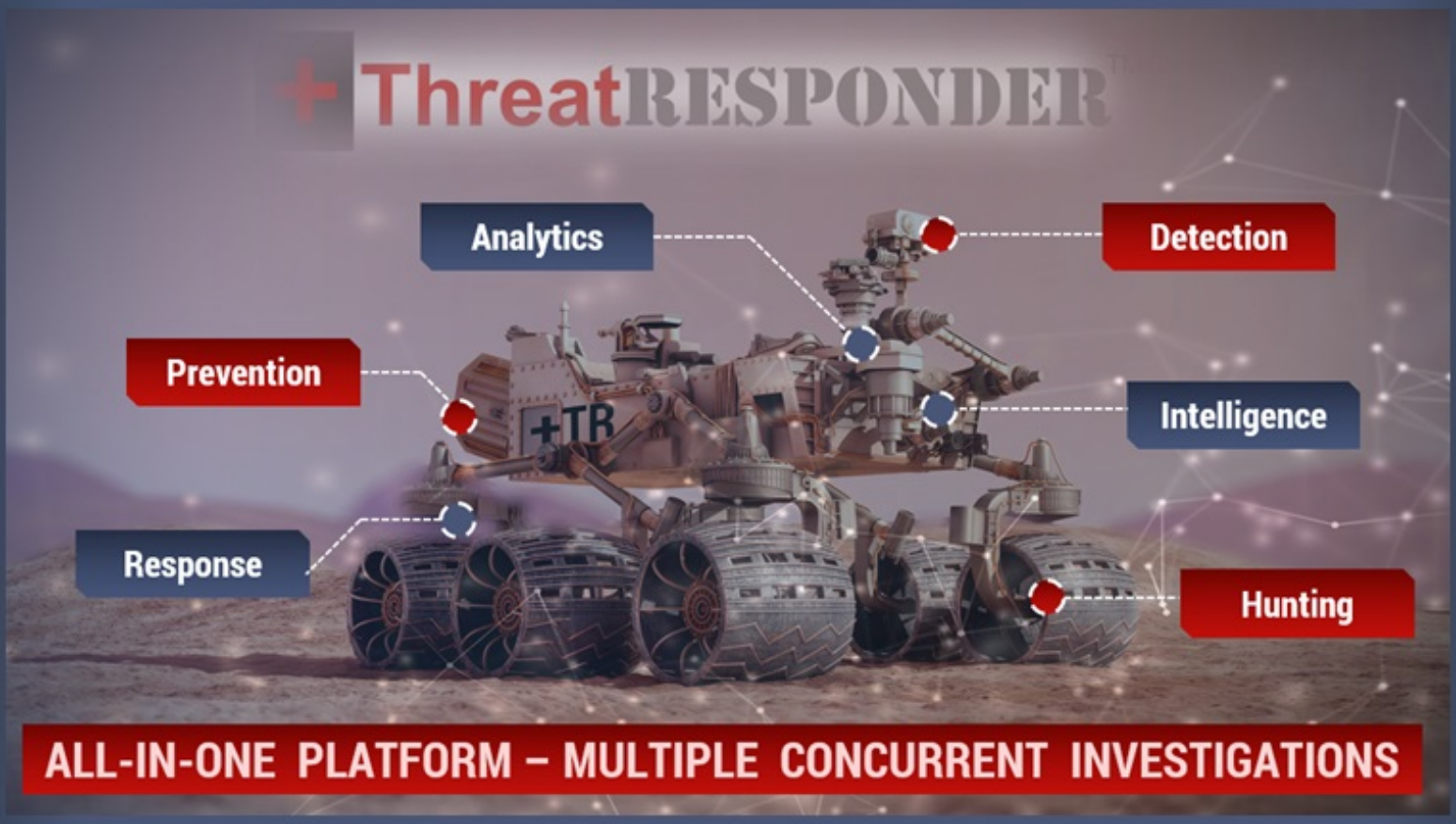
Red Hat Security Advisory 2023-2104-01 - Red Hat Advanced Cluster Management for Kubernetes 2.5.8 images Red Hat Advanced Cluster Management for Kubernetes provides the capabilities to address common challenges that administrators and site reliability engineers face as they work across a range of public and private cloud environments. Clusters and applications are all visible and managed from a single console—with security policy built in. This advisory contains the container images for Red Hat Advanced Cluster Management for Kubernetes, which fix several bugs. Issues addressed include a denial of service vulnerability.

Are You...

- Spending several hours, days, or weeks conducting forensic investigations?
- Using different and unnecessary tools that pose correlation challenges?
- Wasting money on needless travels?
- Overworked, understaffed, and facing a backlog of cases?
- Uploading potentially sensitive files to VirusTotal or third-party sites?

Do DFIR Investigations Better

- Conduct DFIR investigations on any remote endpoint regardless of its geolocation – all on a single-pane of glass
- Perform in-depth forensics investigation dating back to the first day the target endpoint was installed
- Conduct full dynamic and static malware analyses with just a click of a mouse
- Conduct legally-defensible multiple DFIR cases simultaneously



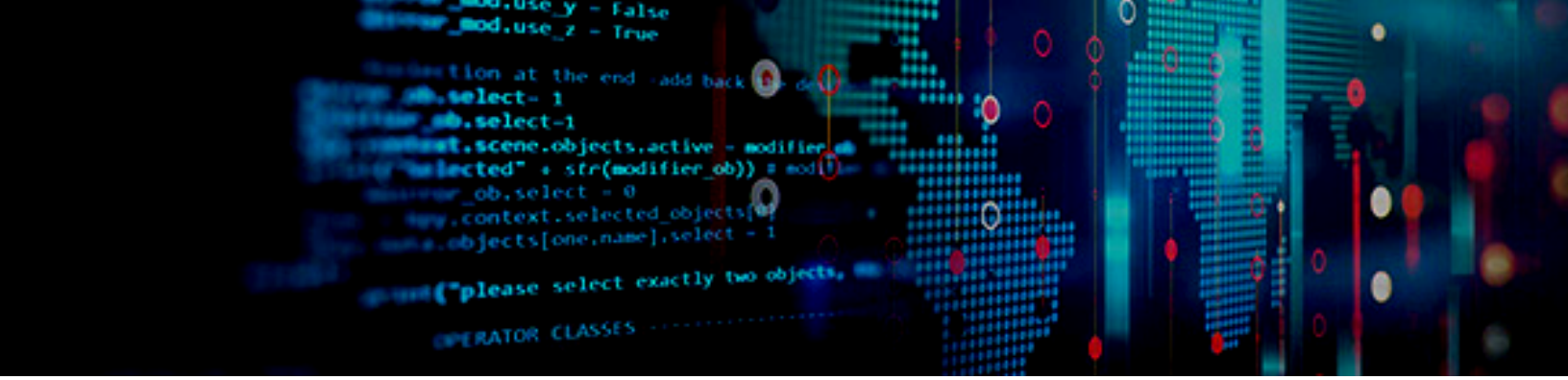
The Solution – ThreatResponder® Platform

ThreatResponder® Platform is an all-in-one cloud-native endpoint threat **detection**, **prevention**, **response**, **analytics**, **intelligence**, **investigation**, and **hunting** product

Get a Trial Copy

Mention **CODE: CIR-0119**

https://netsecurity.com

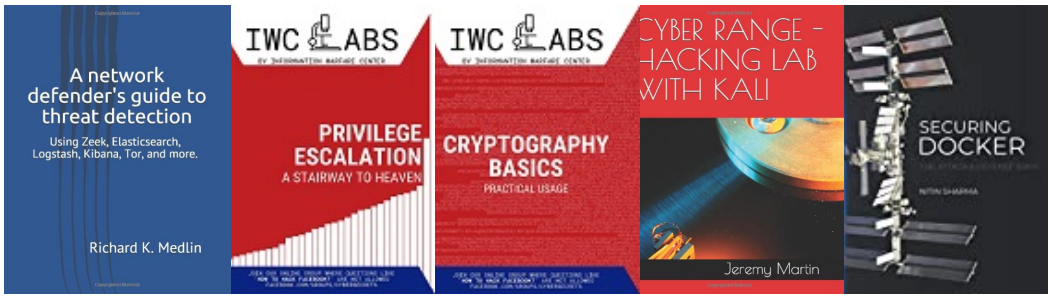


The Cyber Secrets publications on Amazon

The Cyber Weekl Awareness Report (WAR) is an Open Source Intelligence (AKA OSINT) resource centering around an array of subjects ranging from Exploits, Advanced Persistent Threat, National Infrastructure, Dark Web, Digital Forensics & Incident Response (DIFR), and the gambit of digital dangers.

Items that focus on cyber defense and DFIR usually spotlight capabilities in the CSI Linux environment. If interested in helping evolve, please let us know. The Cyber Secrets publications rotates between odd quarters issues focusing on Blue Team and the even issues on Red Team.

Other Publications from Information Warfare Center



CYBER WEEKLY AWARENESS REPORT

VISIT US AT **INFORMATIONWARFARECENTER.COM**

THE IWC ACADEMY
ACADEMY.INFORMATIONWARFARECENTER.COM

FACEBOOK GROUP
FACEBOOK.COM/GROUPS/CYBERSECRETS

CSI LINUX
CSILINUX.COM

CYBERSECURITY TV
CYBERSEC.TV

ARGOS
APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity

ThreatRESPONDER

Accredited Training Center
EC-Council

CYBERQ GROUP