Feb-06-23

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

February 6, 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

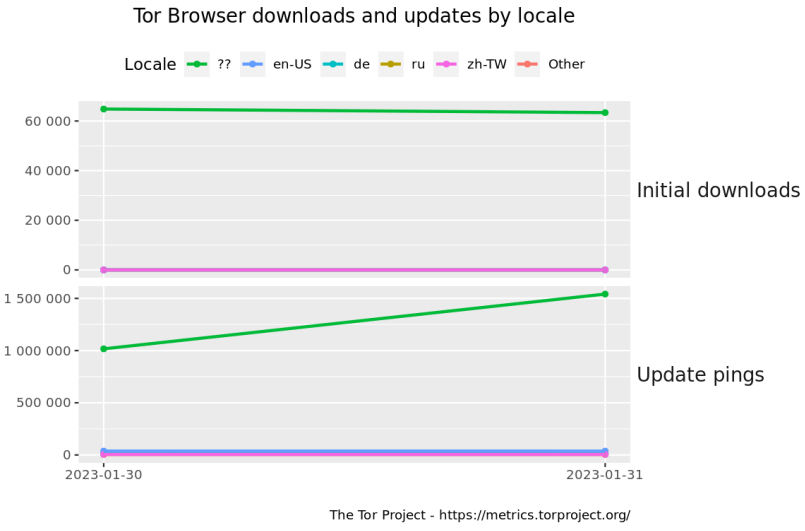
Internet Storm Center Infocon Status

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

* Dutch Police Read Messages Of Encrypted Messenger Exclu
* School Laptop Auction Devolves Into Extortion Allegation
* Iran Crew Stole Charlie Hebdo Database, Says Microsoft
* No Evidence Global Ransomware Hack Was By State Entity, Italy Says
* Former Ubiquiti Dev Pleads Guilty In Data Theft And Extortion Case
* Passion Botnet Cyberattacks Hit Healthcare
* HeadCrab Malware Compromised 1,200 Redis Servers
* Hate It When That Happens: China Says It's Checking If It Accidentally Sent A Spy Balloon To Montana
* Ransomware Attack On Data Firm ION Could Take Days To Fix
* Enter The Hunter Satellites Preparing For Space War
* Up To 29,000 Unpatched QNAP Storage Devices Are Sitting Ducks To Ransomware
* Google Boosts Bounties For Open Source Flaws Found Via Fuzzing
* HPE, NetApp Warn Of Critical Open Source Bug
* North Korea Led Biggest Year Ever Of Crypto Hacks
* DarkTrace's Shares Dive As Short Sellers Circle
* Netflix's New Password Sharing Restrictions Are Confusing
* SBF Barred From Contacting FTX Employees Via Signal
* Apple's Focus On Secrecy Violated Employee Rights
* Attackers Abuse Microsoft's Verified Publisher Status To Steal Data
* South Korea Makes Crypto Crackdown A National Justice Priority
* Bill Targets Suicide Hotline Vulnerabilities After Cyberattack On Intrado
* Chromebook SH1MMER Exploit Promises Admin Jailbreak
* KeePass Disputes Report Of Flaw That Could Exfiltrate A Database
* U.S. Stops Granting Export Licenses For China's Huawei
* GitHub Says Hackers Cloned Code-Signing Certificates In Breached Repository

Krebs on Security

* Finland's Most-Wanted Hacker Nabbed in France
* Experian Glitch Exposing Credit Files Lasted 47 Days
* Administrator of RSOCKS Proxy Botnet Pleads Guilty
* New T-Mobile Breach Affects 37 Million Accounts
* Thinking of Hiring or Running a Booter Service? Think Again.
* Microsoft Patch Tuesday, January 2023 Edition
* Identity Thieves Bypassed Experian Security to View Credit Reports
* Happy 13th Birthday, KrebsOnSecurity!
* The Equifax Breach Settlement Offer is Real, For Now
* Hacked Ring Cams Used to Record Swatting Victims

Dark Reading

* Consumer Watchdog Reports: CA Privacy Board OKs Landmark Personal Data Regulations, Some Key Protecti
* Crypto Drainers Are Ready to Ransack Investor Wallets
* Global Ransomware Attack on VMware EXSi Hypervisors Continues to Spread
* Cadien Cyber Response Launches to Deliver Incident Response & Complex Digital Forensics Services
* Cybercrime Shows No Signs of Slowing Down
* Patching & Passwords Lead the Problem Pack for Cyber-Teams
* How Cybercriminals Are Operationalizing Money Laundering and What to Do About It
* Name That Edge Toon: For the Birds
* What CISOs Can Do About Brand Impersonation Scam Sites
* Iran-Backed Actor Behind 'Holy Souls' Cyberattack on Charlie Hebdo, Microsoft Says
* Scores of Redis Servers Infested by Sophisticated Custom-Built Malware
* How the Cloud Is Shifting CISO Priorities
* MITRE Releases Tool to Design Cyber-Resilient Systems
* Hornetsecurity Combats QR Code Phishing With Launch of New Technology
* Korelock Launches IOT Smart Lock Technology Company
* Cyberattack on Fintech Firm Disrupts Derivatives Trading Globally
* 6 Examples of the Evolution of a Scam Site
* Rising 'Firebrick Ostrich' BEC Group Launches Industrial-Scale Cyberattacks
* Patch Critical Bug Now: QNAP NAS Devices Ripe for the Slaughter
* Managing the Governance Model for Software Development in a No-Code Ecosystem

The Hacker News

* GuLoader Malware Using Malicious NSIS Executables to Target E-Commerce Industry
* Microsoft: Iranian Nation-State Group Sanctioned by U.S. Behind Charlie Hebdo Hack
* SaaS in the Real World: Who's Responsible to Secure this Data?
* OpenSSH Releases Patch for New Pre-Auth Double Free Vulnerability
* FormBook Malware Spreads via Malvertising Using MalVirt Loader to Evade Detection
* PixPirate: New Android Banking Trojan Targeting Brazilian Financial Institutions
* New Wave of Ransomware Attacks Exploiting VMware Bug to Target ESXi Servers
* Warning: Hackers Actively Exploiting Zero-Day in Fortra's GoAnywhere MFT
* Is Your EV Charging Station Safe? New Security Vulnerabilities Uncovered
* Post-Macro World Sees Rise in Microsoft OneNote Documents Delivering Malware
* Iranian OilRig Hackers Using New Backdoor to Exfiltrate Data from Govt. Organizations
* The Pivot: How MSPs Can Turn a Challenge Into a Once-in-a-Decade Opportunity
* Atlassian's Jira Service Management Found Vulnerable to Critical Vulnerability
* New High-Severity Vulnerabilities Discovered in Cisco IOx and F5 BIG-IP Products
* CISA Alert: Oracle E-Business Suite and SugarCRM Vulnerabilities Under Attack

Security Week

* Comcast Wants a Slice of the Enterprise Cybersecurity Business
* Critical Baicells Device Vulnerability Can Expose Telecoms Networks to Snooping
* New York Attorney General Fines Vendor for Illegally Promoting Spyware
* SecurityWeek Analysis: Over 450 Cybersecurity M&A Deals Announced in 2022
* 20 Million Users Impacted by Data Breach at Instant Checkmate, TruthFinder
* Cyber Insights 2023 | The Coming of Web3
* Cyber Insights 2023 | Zero Trust and Identity and Access Management
* European Police Arrest 42 After Cracking Covert App
* Florida Hospital Cancels Procedures, Diverts Patients Following Cyberattack
* VMware ESXi Servers Targeted in Ransomware Attack via Old Vulnerability

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* A Close Call - PayPal Scam Warning
* Students Phished with Bogus Job Offers
* Your KnowBe4 Fresh Content Updates from January 2023
* Yahoo Suddenly Rises in Popularity in Q4 to Become the Most Impersonated Brand in Phishing Attacks
* Initial Access Brokers Leverage Legitimate Google Ads to Gain Malicious Access
* BEC Group Launches Hundreds of Campaigns
* KnowBe4 Wins Winter 2023 "Best of" Awards From TrustRadius in Multiple Categories
* Artificial Intelligence, ChatGPT and Cybersecurity: A Match Made in Heaven or a Hack Waiting to Happe
* Scammers Impersonate Financial Advisors Through Social Media Platforms
* Travel-Themed Phishing Attacks Lure Victims with Promises of Free Tickets, Points, and Exclusive Deal

ISC2.org Blog

* LATEST CYBERTHREATS AND ADVISORIES - FEBRUARY 3, 2023
* Essential Team Building for Strong Cloud Security
* Cybersecurity Industry News Review - 31 January 2023
* Royal Mail "cyber incident" is an ongoing cyberattack CEO admits to MPs
* How are you marking data privacy day?

HackRead

* Major Cybercrime Crackdown: Encrypted Messenger Exclu Seized
* Mortgage Broker 8Twelve Exposes Data of Canadian Residents
* Anonymous Leaks 128 GB of Data from Russian ISP Convex
* Dark Web Hitman Paid with BTC to Murder Teen Victim
* Instant Checkmate, TruthFinder Data Breach: 20M Accounts Leaked
* India's Largest Truck Brokerage Company Leaking 140GB of Data
* EV Charging Stations at Risk of DoS Attacks

Koddos

* Major Cybercrime Crackdown: Encrypted Messenger Exclu Seized
* Mortgage Broker 8Twelve Exposes Data of Canadian Residents
* Anonymous Leaks 128 GB of Data from Russian ISP Convex
* Dark Web Hitman Paid with BTC to Murder Teen Victim
* Instant Checkmate, TruthFinder Data Breach: 20M Accounts Leaked
* India's Largest Truck Brokerage Company Leaking 140GB of Data
* EV Charging Stations at Risk of DoS Attacks

Naked Security

* Tracers in the Dark: The Global Hunt for the Crime Lords of Crypto
* Finnish psychotherapy extortion suspect arrested in France
* OpenSSH fixes double-free memory bug that's pokable over the network
* S3 Ep120: When dud crypto simply won't let go [Audio + Text]
* Password-stealing "vulnerability" reported in KeePass - bug or feature?
* GitHub code-signing certificates stolen (but will be revoked this week)
* Serious Security: The Samba logon bug caused by outdated crypto
* Hive ransomware servers shut down at last, says FBI
* Dutch suspect locked up for alleged personal data megathefts
* S3 Ep119: Breaches, patches, leaks and tweaks! [Audio + Text]

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

* Why Crowdsourced Security is Devastating to Threat Actors
* Bridging the 3.4 Million Workforce Gap in Cybersecurity
* The Evolution of Antivirus Software to Face Modern Threats
* How Do Threat Hunters Keep Organizations Safe?
* Contain Breaches and Gain Visibility With Microsegmentation
* CEO, CIO or CFO: Who Should Your CISO Report To?
* How the Silk Road Affair Changed Law Enforcement
* Data Privacy: How the Growing Field of Regulations Impacts Businesses
* Why Zero Trust Works When Everything Else Doesn't
* 5 Golden Rules of Threat Hunting

InfoWorld

* Where the tech jobs are
* Oracle per-employee Java licensing could benefit rivals
* Why observability in dataops?
* The tech leader's guide to 2023
* Visual Studio Code 1.75 brings configuration profiles
* How multicloud changes devops
* Images considered harmful (sometimes)
* What is garbage collection? Automated memory management for your programs
* Go 1.20 previews profile-guided optimization
* 5 key new features in SingleStoreDB 8.0

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

* 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
* The Fascinating Ineptitude Of Russian Military Communications
* Cyberwar In The Ukraine Conflict
* Our New Approach To Conference Listings
* Marketing Cybersecurity In 2023
* Cybersecurity Employment Market

Google Zero Day Project

* Exploiting null-dereferences in the Linux kernel
* DER Entitlements: The (Brief) Return of the Psychic Paper

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.

* SECCON CTF 2022 Domestic Finals
* SECCON CTF 2022 International Finals
* LA CTF 2023
* HackTM CTF Quals 2023
* pbctf 2023
* CTF After Dark - Winter 2023
* KalmarCTF 2023
* hxp CTF 2022
* DaVinciCTF 2023
* HackDay Qualifications 2023

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

* GNUnet P2P Framework 0.19.3
* Zeek 5.0.6
* OpenSSH 9.2p1
* Suricata IDPE 6.0.10
* Proxmark3 4.16191 Custom Firmware
* OpenStego Free Steganography Solution 0.8.6
* Logwatch 7.8
* TOR Virtual Network Tunneling Tool 0.4.7.13
* Wireshark Analyzer 4.0.3
* MIMEDefang Email Scanner 3.3

Kali Linux Tutorials

* ExchangeFinder : Find Microsoft Exchange Instance For A Given Domain And Identify The Exact Version
* Villain : Windows And Linux Backdoor Generator And Multi-Session Handler
* PXEThief : Extract Passwords From The Operating System Deployment Functionality
* Cypherhound : Terminal Application That Contains 260+ Neo4j Cyphers For BloodHound Data Sets
* Subparse : Modular Malware Analysis Artifact Collection And Correlation Framework
* Should South East Asian Tech Startups Consider Outsourcing Support?
* AzureHound : Azure Data Exporter For BloodHound
* Xerror - An Automated Penetration Testing Tool With GUI
* Mongoaudit - An Audit and Pentesting Tool for MongoDB Databases
* ADFSRelay : Proof Of Concept Utilities Developed To Research NTLM Relaying Attacks Targeting ADFS

GBHackers Analysis

* High-Severity RCE Bug in F5 Products Let Attackers Hack the Complete Systems
* Samsung Galaxy Store Flaw Allows Remote Attacker to Run Code on Affected Phones
* Hackers Actively Exploiting Cisco AnyConnect Secure Flaw to Perform DLL Hijacking
* 22-Yrs-Old SQLite Bug Let Hackers Perform Code Execution & DOS Attack On Control Programs
* Apache Commons "Text4Shell" Flaw Could Trigger Code Execution With Malicious Input

Weekly Cyber Security Video and Podcasts

SANS DFIR

* SANS Threat Analysis Rundown
* The Truth about Ransomware: Its not Complicated!
* Think DFIRently: What is Digital Forensics & Incident Response (DFIR)?
* What makes a solid DFIR professional - How to keep growing in the field and not lose your luster

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

* Staged and non-staged payloads for the USB Rubber Ducky [PAYLOAD]
* Apple ID, Now With Hardware Keys! - ThreatWire
* T-Mobile Hack Hits 37 Million - ThreatWire

The PC Security Channel [TPSC]

* Has Windows become Spyware?
* Malware in Google Ads: Fake OBS, VLC, Notepad++

Eli the Computer Guy

* FAT SHAMMING at Amusement Park - "Average" US Male waist is 40+ inches...
* MORE TECH LAYOFFS - jack dorsey screwing block employees...
* TESLA WINS - buying a car with Apple Pay
* MUSK WINS - Mustang Mach e vs Tesla Model Y

Security Now

* Data Operand Independent Timing - Old Android apps, Kevin Rose, iOS 6.3 and FIDO, Hive hacked
* Credential Reuse - iOS 16.3, ChatGPT creates malware, Bitwarden acquires Passwordless.dev

Troy Hunt

* Weekly Update 333

Intel Techniques: The Privacy, Security, & OSINT Show

* 288-Privacy, Security, & OSINT Updates
* 287-Listener Questions, UNREDACTED 5, & OSINT 10

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Apache Tomcat On Ubuntu Log Init Privilege Escalation
* Android Binder VMA Management Security Issues
* Windows Kernel Registry Virtualization Memory Corruption
* Lenovo Diagnostics Driver Memory Access
* macOS Dirty Cow Arbitrary File Write Local Privilege Escalation
* F5 Big-IP Create Administrative User
* Oracle Database 12.1.0.2 Spatial Component Privilege Escalation
* Packet Storm New Exploits For January, 2023
* io_uring Same Type Object Reuse Privilege Escalation
* vmwgfx Driver File Descriptor Handling Privilege Escalation
* eCommerce Marketplace Platform CMS 1.7 SQL Injection
* eCommerce Marketplace Platform CMS 1.7 Cross Site Scripting
* Online Eyewear Shop 1.0 SQL Injection
* Control Web Panel Unauthenticated Remote Command Execution
* PHPJabbers Business Directory Script 3.2 Cross Site Scripting
* PHPJabbers Auto Classifieds Script 3.2 Cross Site Scripting
* mRemoteNG 1.76.20 Privilege Escalation
* Broadcast Signal Intrusion - Hacking Radio Stations
* PHPJabbers Car Park Booking System 2.0 Cross Site Scripting
* Zstore 6.6.0 Cross Site Scripting
* PHPJabbers Event Ticketing System Script 1.0 Cross Site Scripting
* PHPJabbers Travel Tours Script 1.0 SQL Injection
* PHPJabbers Travel Tours Script 1.0 Cross Site Scripting
* PHPJabbers Property Listing Script 3.1 SQL Injection
* PHPJabbers Property Listing Script 3.1 Cross Site Scripting

CXSecurity

* Lenovo Diagnostics Driver Memory Access
* macOS Dirty Cow Arbitrary File Write Local Privilege Escalation
* F5 Big-IP Create Administrative User
* Apache Tomcat On Ubuntu Log Init Privilege Escalation
* io_uring Same Type Object Reuse Privilege Escalation
* NetChess 2.1 Buffer Overflow
* Ivanti Cloud Services Appliance (CSA) Command Injection

Proof of Concept (PoC) & Exploits

Exploit Database

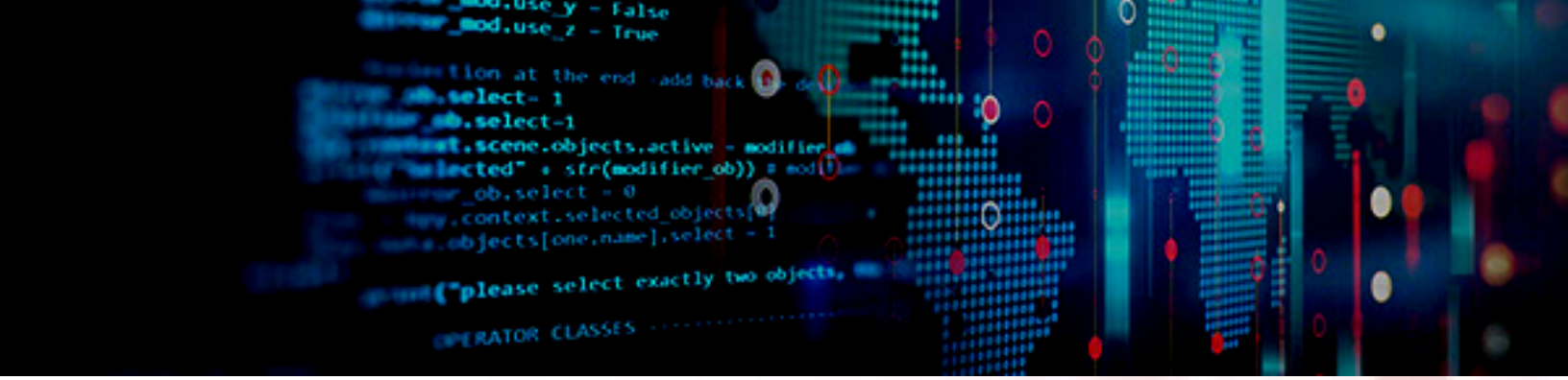
* [remote] SmartRG Router SR510n 2.6.13 - Remote Code Execution
* [webapps] CVAT 2.0 - Server Side Request Forgery
* [local] IOTransfer V4 - Unquoted Service Path
* [remote] AVEVA InTouch Access Anywhere Secure Gateway 2020 R2 - Path Traversal
* [remote] MSNSwitch Firmware MNT.2408 - Remote Code Execution
* [webapps] Open Web Analytics 1.7.3 - Remote Code Execution
* [webapps] Wordpress Plugin ImageMagick-Engine 1.7.4 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Wordpress Plugin Zephyr Project Manager 3.2.42 - Multiple SQLi
* [webapps] Testa 3.5.1 Online Test Management System - Reflected Cross-Site Scripting (XSS)
* [webapps] Aero CMS v0.0.1 - SQLi
* [webapps] Wordpress Plugin 3dady real-time web stats 1.0 - Stored Cross Site Scripting (XSS)
* [webapps] Wordpress Plugin WP-UserOnline 2.88.0 - Stored Cross Site Scripting (XSS)
* [remote] Teleport v10.1.1 - Remote Code Execution (RCE)
* [webapps] Feehi CMS 2.1.1 - Remote Code Execution (Authenticated)
* [webapps] TP-Link Tapo c200 1.1.15 - Remote Code Execution (RCE)
* [remote] WiFiMouse 1.8.3.4 - Remote Code Execution (RCE)
* [remote] Wifi HD Wireless Disk Drive 11 - Local File Inclusion
* [local] Blink1Control2 2.2.7 - Weak Password Encryption
* [webapps] Bookwyrm v0.4.3 - Authentication Bypass
* [webapps] Buffalo TeraStation Network Attached Storage (NAS) 1.66 - Authentication Bypass
* [remote] Airspan AirSpot 5410 version 0.3.4.1 - Remote Code Execution (RCE)
* [remote] Mobile Mouse 3.6.0.4 - Remote Code Execution (RCE)
* [webapps] Gitea 1.16.6 - Remote Code Execution (RCE) (Metasploit)
* [webapps] WordPress Plugin Netroics Blog Posts Grid 1.0 - Stored Cross-Site Scripting (XSS)
* [webapps] WordPress Plugin Testimonial Slider and Showcase 2.2.6 - 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*

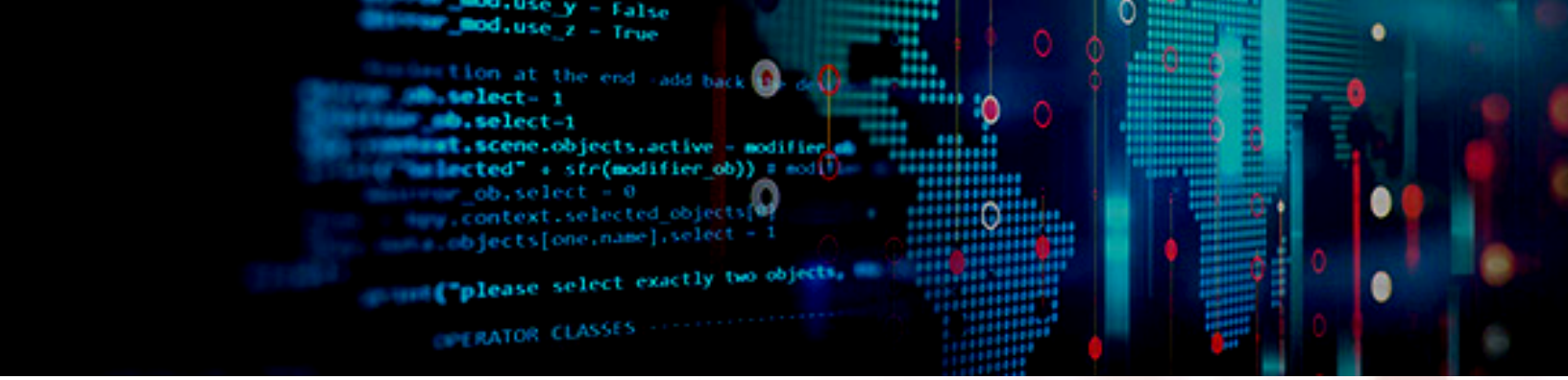
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://transparencia.cmcanaadoscarajas.pa.gov.br
https://transparencia.cmcanaadoscarajas.pa.gov.br notified by Waffen17
https://www.cmcanaadoscarajas.pa.gov.br
https://www.cmcanaadoscarajas.pa.gov.br notified by Waffen17
http://legislativo.cmc.mg.gov.br/procon/
http://legislativo.cmc.mg.gov.br/procon/ notified by Waffen17
http://www.cmc.mg.gov.br/procon/
http://www.cmc.mg.gov.br/procon/ notified by Waffen17
https://ilicinea.mg.gov.br/index.html
https://ilicinea.mg.gov.br/index.html notified by Waffen17
https://cmaltonia.pr.gov.br/index.html
https://cmaltonia.pr.gov.br/index.html notified by Waffen17
https://camaraparanapoema.pr.gov.br/index.html
https://camaraparanapoema.pr.gov.br/index.html notified by Waffen17
https://cmipueira.rn.gov.br/index.html
https://cmipueira.rn.gov.br/index.html notified by Waffen17
https://cmgrandesrios.pr.gov.br/index.html
https://cmgrandesrios.pr.gov.br/index.html notified by Waffen17
https://aguadocedonorte.es.gov.br/index.html
https://aguadocedonorte.es.gov.br/index.html notified by Waffen17
https://acaua.pi.gov.br/index.html
https://acaua.pi.gov.br/index.html notified by Waffen17
http://legado-p.mpam.mp.br
http://legado-p.mpam.mp.br notified by Waffen17
https://diario.mpam.mp.br
https://diario.mpam.mp.br notified by Waffen17
http://panaquatira.ufma.br
http://panaquatira.ufma.br notified by Waffen17
http://sistemas.unasus.ufma.br
http://sistemas.unasus.ufma.br notified by Waffen17
http://varzeagrande.mt.gov.br/storage/pwnd.htm
http://varzeagrande.mt.gov.br/storage/pwnd.htm notified by IdiotCrew
http://apmt.mt.gov.br/readme.html
http://apmt.mt.gov.br/readme.html notified by IdiotCrew

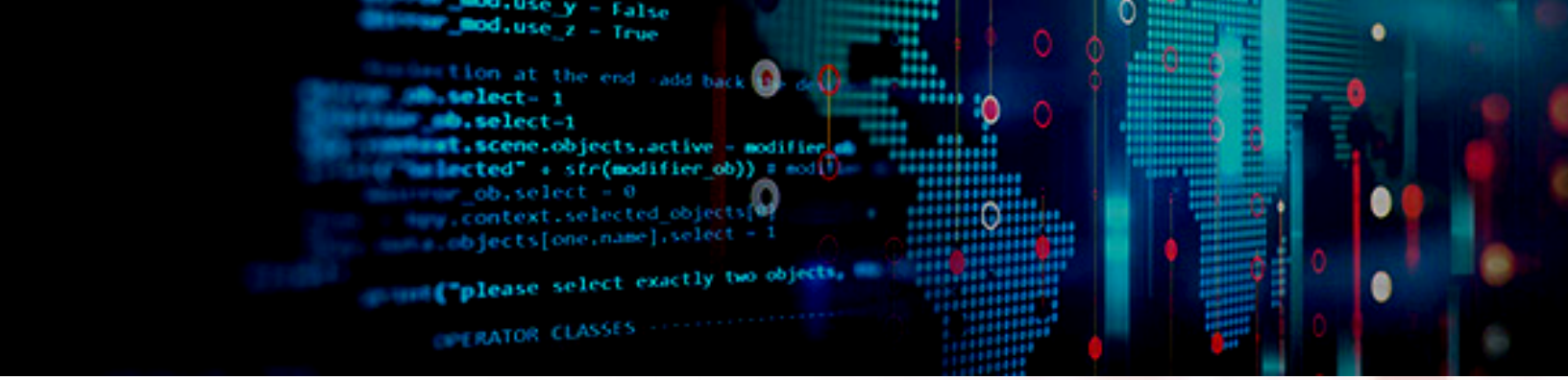


Dark Web News

Darknet Live

[Dutchman Sold Counterfeit Banknotes on the Dark Web]
[A Guide to Crypto Self-Custody]
[Austrian Resold Drugs Purchased on The Dark Web]
[Former Doctor Imprisoned for Attempting to Hire Hitmen]

Dark Web Link



Trend Micro Anti-Malware Blog

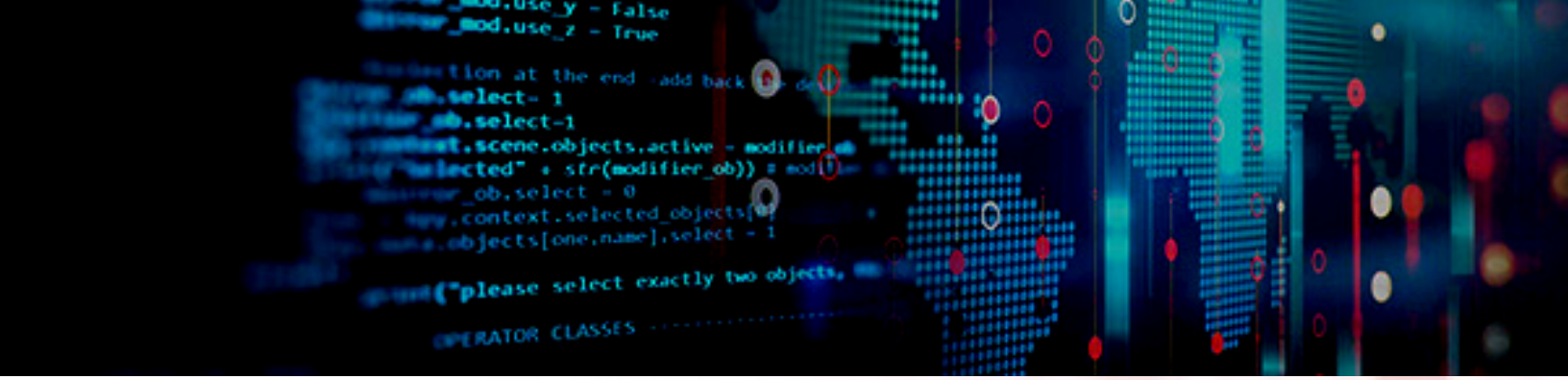
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

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

* CVE-2023-22501: Critical Broken Authentication Flaw in Jira Service Management Products
* Ransomware Campaign Compromising VMware ESXi Servers
* Metasploit Weekly Wrap-Up
* Exploitation of GoAnywhere MFT zero-day vulnerability
* Troubleshooting InsightAppSec Authentication Issues
* XDR, the Beatles, and Blunt Instruments
* CVE-2023-22374: F5 BIG-IP Format String Vulnerability
* A Customer Success Manager's Journey to Cybersecurity
* Rapid7 Observes Use of Microsoft OneNote to Spread Redline Infostealer Malware
* Year in Review: Rapid7 Threat Intelligence



Advisories

US-Cert Alerts & bulletins

* CISA Releases Six Industrial Control Systems Advisories
* CISA Adds Two Known Exploited Vulnerabilities to Catalog
* Cisco Releases Security Advisories for Multiple Products
* Drupal Releases Security Update to Address a Vulnerability in Apigee Edge
* VMware Releases Security Update for VMware vRealize Operations
* CISA Releases One Industrial Control Systems Advisory
* ISC Releases Security Advisories for Multiple Versions of BIND 9
* JCDC Announces 2023 Planning Agenda
* AA23-025A: Protecting Against Malicious Use of Remote Monitoring and Management Software
* AA22-335A: #StopRansomware: Cuba Ransomware
* Vulnerability Summary for the Week of January 23, 2023
* Vulnerability Summary for the Week of January 16, 2023

Zero Day Initiative Advisories

ZDI-CAN-20317: 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: 2023-01-26, 11 days ago. The vendor is given until 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-20324: 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: 2023-01-26, 11 days ago. The vendor is given until 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-20323: 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: 2023-01-26, 11 days ago. The vendor is given until 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-20316: 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: 2023-01-26, 11 days ago. The vendor is given until 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-20322: 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: 2023-01-26, 11 days ago. The vendor

is given until 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-20319: 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: 2023-01-26, 11 days ago. The vendor is given until 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-20314: 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: 2023-01-26, 11 days ago. The vendor is given until 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-20313: 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: 2023-01-26, 11 days ago. The vendor is given until 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-20312: 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: 2023-01-26, 11 days ago. The vendor is given until 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-20309: 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: 2023-01-26, 11 days ago. The vendor is given until 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-20321: 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: 2023-01-26, 11 days ago. The vendor is given until 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-20320: 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: 2023-01-26, 11 days ago. The vendor is given until 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-20315: 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: 2023-01-26, 11 days ago. The vendor is given until 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-20326: 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: 2023-01-26, 11 days ago. The vendor is given until 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-19905: TP-Link

A CVSS score 6.8 (AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Pumpkin,

working with DEVCORE Internship Program' was reported to the affected vendor on: 2023-01-26, 11 days ago. The vendor is given until 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-19895: Moxa

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 'Simon Janz (@esj4y)' was reported to the affected vendor on: 2023-01-26, 11 days ago. The vendor is given until 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-19981: NETGEAR

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 'Zach Hanley (@hacks_zach) of Horizon3 A.I.' was reported to the affected vendor on: 2023-01-26, 11 days ago. The vendor is given until 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-19901: HP

A CVSS score 8.8 (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Angelboy (@scwuaptx) from DEVCORE Research Team' was reported to the affected vendor on: 2023-01-26, 11 days ago. The vendor is given until 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-20086: D-Link

A CVSS score 8.8 (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Dmitry "InfoSecDJ" Janushkevich of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-01-26, 11 days ago. The vendor is given until 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-20278: 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 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2023-01-26, 11 days ago. The vendor is given until 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-20276: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-01-26, 11 days ago. The vendor is given until 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-19900: HP

A CVSS score 8.8 (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Angelboy (@scwuaptx) from DEVCORE Research Team' was reported to the affected vendor on: 2023-01-26, 11 days ago. The vendor is given until 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-20285: 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: 2023-01-26, 11 days ago. The vendor is given until 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-20275: 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 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2023-01-26, 11 days ago. The vendor is given until 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-5842-1

Ubuntu Security Notice 5842-1 - Mark Esler and David Fernandez Gonzalez discovered that EditorConfig Core C incorrectly handled memory when handling certain inputs. An attacker could possibly use this issue to cause applications using EditorConfig Core C to crash, resulting in a denial of service, or possibly execute arbitrary code.

Ubuntu Security Notice USN-5824-1

Ubuntu Security Notice 5824-1 - Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, bypass security restrictions, cross-site tracing, or execute arbitrary code.

Ubuntu Security Notice USN-5825-2

Ubuntu Security Notice 5825-2 - USN-5825-1 fixed vulnerabilities in PAM. Unfortunately that update was incomplete and could introduce a regression. This update fixes the problem. It was discovered that PAM did not correctly restrict login from an IP address that is not resolvable via DNS. An attacker could possibly use this issue to bypass authentication.

Ubuntu Security Notice USN-5816-2

Ubuntu Security Notice 5816-2 - USN-5816-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem. Niklas Baumstark discovered that a compromised web child process of Firefox could disable web security opening restrictions, leading to a new child process being spawned within the file:// context. Tom Schuster discovered that Firefox was not performing a validation check on GTK drag data. An attacker could potentially exploits this to obtain sensitive information. Various other issues were also addressed.

Ubuntu Security Notice USN-5841-1

Ubuntu Security Notice 5841-1 - It was discovered that LibTIFF incorrectly handled certain malformed images. If a user or automated system were tricked into opening a specially crafted image, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges. This issue was only fixed in Ubuntu 14.04 ESM. It was discovered that LibTIFF was incorrectly accessing a data structure when processing data with the tiffcrop tool, which could lead to a heap buffer overflow. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code.

WordPress Quick Restaurant 2.0.2 XSS / CSRF / IDOR / Missing Authorization

On January 16, 2023, the Wordfence Threat Intelligence team responsibly disclosed several vulnerabilities in Quick Restaurant Menu, a WordPress plugin that allows users to set up restaurant menus on their sites. This plugin is vulnerable to missing authorization, insecure direct object reference, cross site request forgery as well as cross site scripting in versions up to, and including, 2.0.2.

Ubuntu Security Notice USN-5840-1

Ubuntu Security Notice 5840-1 - It was discovered that Long Range ZIP incorrectly handled pointers. If a user or an automated system were tricked into opening a certain specially crafted ZIP file, an attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, Ubuntu 18.04 LTS, and Ubuntu 20.04 LTS. It was discovered that Long Range ZIP incorrectly handled pointers. If a user or an automated system were tricked into opening a certain specially crafted ZIP file, an attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 18.04 LTS and Ubuntu 20.04 LTS.

Ubuntu Security Notice USN-5839-2

Ubuntu Security Notice 5839-2 - USN-5839-1 fixed a vulnerability in Apache. This update provides the corresponding update for Ubuntu 16.04 ESM. Dimas Fariski Setyawan Putra discovered that the Apache HTTP Server mod_proxy module incorrectly truncated certain response headers. This may result in later headers not being interpreted by the client.

Debian Security Advisory 5338-1

Debian Linux Security Advisory 5338-1 - Guillaume Espanel, Pierre Libeau, Arnaud Morin and Damien Rannou discovered that missing input sanitising in the handling of VMDK images in Cinder, the OpenStack block storage system, may result in information disclosure.

Debian Security Advisory 5337-1

Debian Linux Security Advisory 5337-1 - Guillaume Espanel, Pierre Libeau, Arnaud Morin and Damien Rannou discovered that missing input sanitising in the handling of VMDK images in OpenStack Compute (codenamed Nova) may result in information disclosure.

Debian Security Advisory 5336-1

Debian Linux Security Advisory 5336-1 - Guillaume Espanel, Pierre Libeau, Arnaud Morin and Damien Rannou discovered that missing input sanitizing in the handling of VMDK images in Glance, the OpenStack image registry and delivery service, may result in information disclosure.

Debian Security Advisory 5335-1

Debian Linux Security Advisory 5335-1 - Several vulnerabilities have been discovered in the OpenJDK Java runtime, which may result in denial of service or spoofing.

Ubuntu Security Notice USN-5838-1

Ubuntu Security Notice 5838-1 - It was discovered that AdvanceCOMP did not properly manage memory while performing read operations on MNG file. If a user were tricked into opening a specially crafted MNG file, a remote attacker could possibly use this issue to cause AdvanceCOMP to crash, resulting in a denial of service. It was discovered that AdvanceCOMP did not properly manage memory while performing read operations on ZIP file. If a user were tricked into opening a specially crafted ZIP file, a remote attacker could possibly use this issue to cause AdvanceCOMP to crash, resulting in a denial of service.

Ubuntu Security Notice USN-5837-2

Ubuntu Security Notice 5837-2 - USN-5837-1 fixed a vulnerability in Django. This update provides the corresponding update for Ubuntu 16.04 ESM. Nick Pope discovered that Django incorrectly handled certain Accept-Language headers. A remote attacker could possibly use this issue to cause Django to consume memory, leading to a denial of service.

Ubuntu Security Notice USN-5839-1

Ubuntu Security Notice 5839-1 - It was discovered that the Apache HTTP Server mod_dav module incorrectly handled certain If: request headers. A remote attacker could possibly use this issue to cause the server to crash, resulting in a denial of service. ZeddYu_Lu discovered that the Apache HTTP Server mod_proxy_ajp module incorrectly interpreted certain HTTP Requests. A remote attacker could possibly use this issue to perform an HTTP Request Smuggling attack.

Ubuntu Security Notice USN-5837-1

Ubuntu Security Notice 5837-1 - Nick Pope discovered that Django incorrectly handled certain Accept-Language headers. A remote attacker could possibly use this issue to cause Django to consume memory, leading to a denial of service.

Ubuntu Security Notice USN-4781-2

Ubuntu Security Notice 4781-2 - USN-4781-1 fixed several vulnerabilities in Slurm. This update provides the corresponding updates for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. It was discovered that Slurm incorrectly handled certain messages between the daemon and the user. An attacker could possibly use this issue to assume control of an arbitrary file on the system. This issue only affected Ubuntu 16.04 ESM.

Ubuntu Security Notice USN-5836-1

Ubuntu Security Notice 5836-1 - It was discovered that Vim was not properly performing memory management operations. An attacker could possibly use this issue to cause a denial of service or execute arbitrary code.

Red Hat Security Advisory 2023-0553-01

Red Hat Security Advisory 2023-0553-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This release of Red Hat JBoss Enterprise Application Platform 7.4.9 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.4.8, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.4.9

Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include code execution, cross site scripting, denial of service, deserialization, memory exhaustion, and server-side request forgery vulnerabilities.

Red Hat Security Advisory 2023-0552-01

Red Hat Security Advisory 2023-0552-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This release of Red Hat JBoss Enterprise Application Platform 7.4.9 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.4.8, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.4.9 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include code execution, cross site scripting, denial of service, deserialization, memory exhaustion, and server-side request forgery vulnerabilities.

Red Hat Security Advisory 2023-0554-01

Red Hat Security Advisory 2023-0554-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This release of Red Hat JBoss Enterprise Application Platform 7.4.9 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.4.8, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.4.9 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include code execution, cross site scripting, denial of service, deserialization, memory exhaustion, and server-side request forgery vulnerabilities.

Hikvision Remote Code Execution / XSS / SQL Injection

Some Hikvision Hybrid SAN products were vulnerable to multiple remote code execution (command injection) vulnerabilities, including reflected cross site scripting, Ruby code injection, classic and blind SQL injection resulting in remote code execution that allows an adversary to execute arbitrary operating system commands and more. However, an adversary must be on the same network to leverage this vulnerability to execute arbitrary commands.

Red Hat Security Advisory 2023-0556-01

Red Hat Security Advisory 2023-0556-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This release of Red Hat JBoss Enterprise Application Platform 7.4.9 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.4.8, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.4.9 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include code execution, cross site scripting, denial of service, deserialization, memory exhaustion, and server-side request forgery vulnerabilities.

Ubuntu Security Notice USN-5834-1

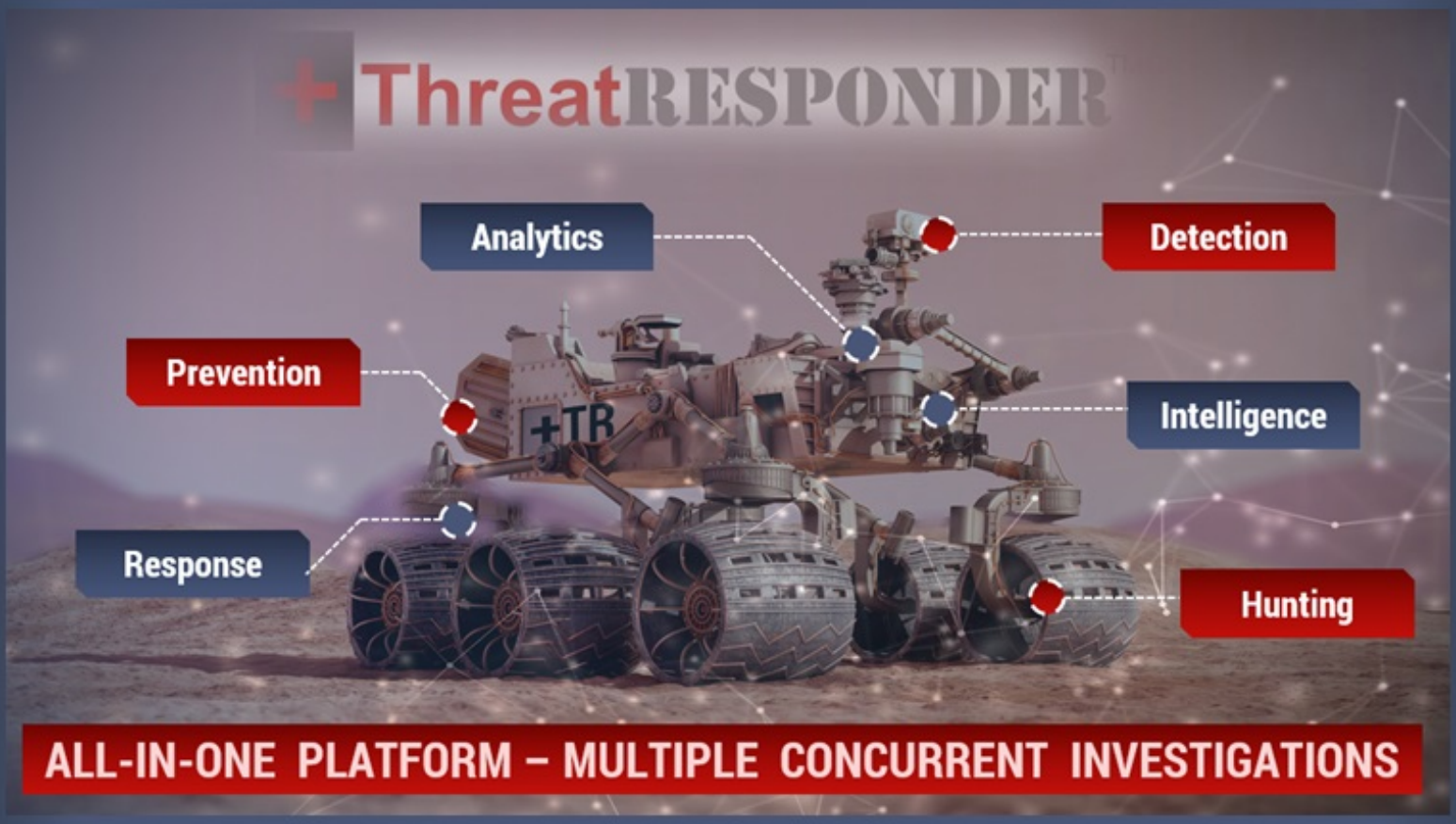
Ubuntu Security Notice 5834-1 - It was discovered that the Apache HTTP Server mod_dav module did not properly handle specially crafted request headers. A remote attacker could possibly use this issue to cause the process to crash, leading to a denial of service. It was discovered that the Apache HTTP Server mod_proxy_ajp module did not properly handle certain invalid Transfer-Encoding headers. A remote attacker could possibly use this issue to perform an HTTP Request Smuggling attack.

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



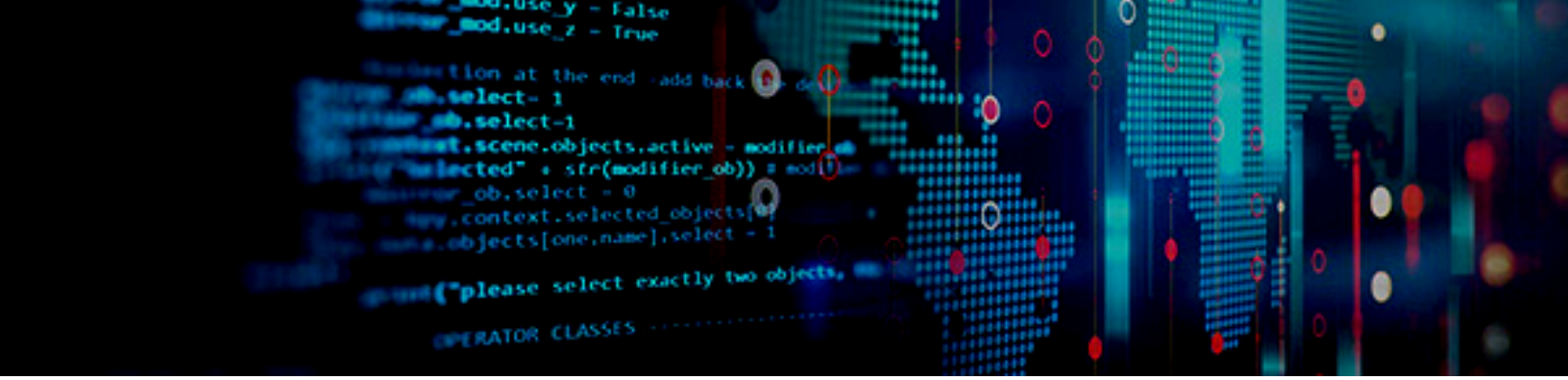
The Solution – ThreatResponder® Platform

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

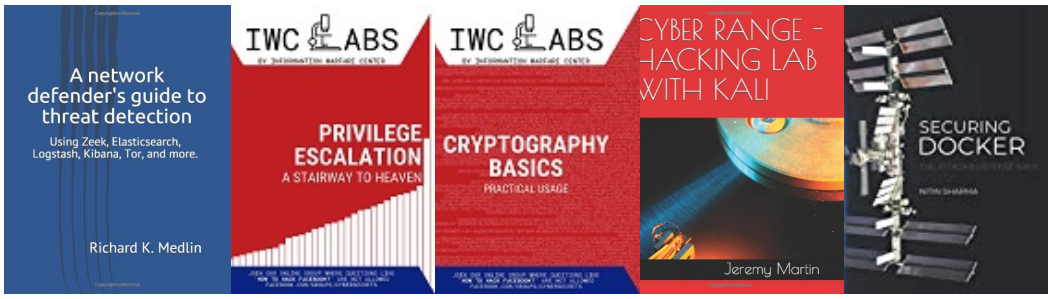


The Cyber Secrets publications on Amazon

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