May-22-23

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 22, 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

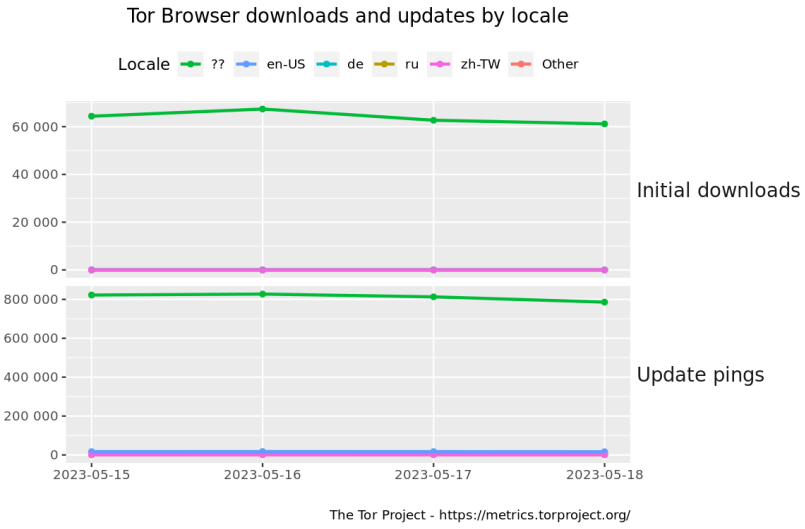
Internet Storm Center Infocon Status

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

Current News
* Packet Storm Security
* Krebs on Security
* Dark Reading
* The Hacker News
* Security Week
* Infosecurity Magazine
* KnowBe4 Security Awareness Training Blog
* ISC2.org Blog
* HackRead
* Koddos
* Naked Security
* Threat Post
* Null-Byte
* IBM Security Intelligence
* Threat Post
* C4ISRNET - Media for the Intelligence Age Military

The Hacker Corner:
* Security Conferences
* Google Zero Day Project

Cyber Range Content
* CTF Times Capture the Flag Event List
* Vulnhub

Tools & Techniques
* Packet Storm Security Latest Published Tools
* Kali Linux Tutorials
* GBHackers Analysis

InfoSec Media for the Week
* Black Hat Conference Videos
* Defcon Conference Videos
* Hak5 Videos
* Eli the Computer Guy Videos
* Security Now Videos
* Troy Hunt Weekly
* Intel Techniques: The Privacy, Security, & OSINT Show

Exploits and Proof of Concepts
* Packet Storm Security Latest Published Exploits
* CXSecurity Latest Published Exploits
* Exploit Database Releases

Cyber Crime & Malware Files/Links Latest Identified
* CyberCrime-Tracker

Advisories
* Hacked Websites
* Dark Web News
* US-Cert (Current Activity-Alerts-Bulletins)
* Zero Day Initiative Advisories
* Packet Storm Security's Latest List

Information Warfare Center Products
* CSI Linux
* Cyber Secrets Videos & Resoures
* Information Warfare Center Print & eBook Publications

Packet Storm Security

* FTC To Crack Down On Biometric, Health Privacy Violations
* Cisco Squashes Critical Bugs In Small Biz Switches
* Millions Of Android TVs And Phones Come With Malware
* US Supreme Court Leaves Protections For Internet Companies Unscathed
* Threat Actor Bypasses Detection, Protections In Microsoft Azure Serial Console
* Six Million Patients' Data Feared Stolen From PharMerica
* Polish News Websites Hit By DDoS Attacks
* DOJ Links Iran, China, And Russia To Five IP-Theft Related Cases
* Twitter Sued Over Saudi Spying That Landed User In Prison
* Upstart Encryption App Walks Back Privacy Claims, Pulls From Stores After Probe
* Malware Turns Home Routers Into Proxies For Chinese Hackers
* Ex-Apple Engineer Accused Of Stealing Self-Driving Car Secrets
* Oil And Gas Sectors Lag Behind Other Industries In Gathering Intel
* US Charges, Sanctions Russian Ransomware Operator Who Leaked Stolen DC Police Data
* Microsoft Is Scanning The Inside Of Password Protected Zip Files For Malware
* Twitter Criticized For Blocking Tweets In Turkey
* OpenAI Chief Concerned About AI Used To Compromise Elections
* Lawmakers Want To Train Rural Hospital Workforce In Infosec
* Ruling Makes Exchanges Liable For Customer Losses In EU
* Intel Says Friday's Mystery Security Update Microcode Isn't Really A Security Update
* Not-Too-Safe Boot: Remotely Bypassing Endpoint Security Solutions And Anti-Tampering Mechanisms
* North Korean Hackers Stole $721 Million In Cryptocurrency From Japan
* Pakistan Shut Down The Internet - But That Didn't Stop Protests
* Passkeys May Not Be For You, But They Are Safe And Easy - Here's Why
* Toyota Bungling Customer Privacy Is Becoming A Pattern

Krebs on Security

* Russian Hacker "Wazawaka" Indicted for Ransomware
* Re-Victimization from Police-Auctioned Cell Phones
* Microsoft Patch Tuesday, May 2023 Edition
* Feds Take Down 13 More DDoS-for-Hire Services
* $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?

Dark Reading

* CommonMagic APT Campaign Broadens Target Scope to Central and Western Ukraine
* Apple Patches 3 Zero-Days Possibly Already Exploited
* Data Siloes: Overcoming the Greatest Challenge in SecOps
* 3 Common Initial Attack Vectors Account for Most Ransomware Campaigns
* Keep Your Friends Close and Your Identity Closer
* Google Debuts Quality Ratings for Security Bug Disclosures
* AppSec Teams Stuck in Catch-Up Cycle Due to Massive Cloud-Native Enablement Gap
* Enterprises Rely on Multicloud Security to Protect Cloud Workloads
* KeePass Vulnerability Imperils Master Passwords
* Trojan-Rigged Phishing Attacks Pepper China-Taiwan Conflict
* 10 Types of AI Attacks CISOs Should Track
* Microsoft Azure VMs Hijacked in Cloud Cyberattack
* Embedding Security by Design: A Shared Responsibility
* OX Security Launches OX-GPT, AppSec's First ChatGPT Integration
* Satori Augments Its Data Security Platform With Posture Management and Data Store Discovery Capabilit
* Once Again, Malware Discovered Hidden in npm
* LexisNexis Risk Solutions Cybercrime Report Reveals 20% Annual Increase in Global Digital Attack Rate
* WithSecure Launches New Range of Incident Response and Readiness Services
* 3 Ways Hackers Use ChatGPT to Cause Security Headaches
* ActZero Teams Up With UScellular to Secure Mobile Devices From Ransomware Attacks

The Hacker News

* U.K. Fraudster Behind iSpoof Scam Receives 13-Year Jail Term for Cyber Crimes
* KeePass Exploit Allows Attackers to Recover Master Passwords from Memory
* PyPI Repository Under Attack: User Sign-Ups and Package Uploads Temporarily Halted
* Meet 'Jack' from Romania! Mastermind Behind Golden Chickens Malware
* Notorious Cyber Gang FIN7 Returns With Cl0p Ransomware in New Wave of Attacks
* Warning: Samsung Devices Under Attack! New Security Flaw Exposed
* Privacy Sandbox Initiative: Google to Phase Out Third-Party Cookies Starting 2024
* Dr. Active Directory vs. Mr. Exposed Attack Surface: Who'll Win This Fight?
* Developer Alert: NPM Packages for Node.js Hiding Dangerous TurkoRat Malware
* Searching for AI Tools? Watch Out for Rogue Sites Distributing RedLine Malware
* WebKit Under Attack: Apple Issues Emergency Patches for 3 New Zero-Day Vulnerabilities
* This Cybercrime Syndicate Pre-Infected Over 8.9 Million Android Phones Worldwide
* Zero Trust + Deception: Join This Webinar to Learn How to Outsmart Attackers!
* How to Reduce Exposure on the Manufacturing Attack Surface
* Escalating China-Taiwan Tensions Fuel Alarming Surge in Cyber Attacks

Security Week

* US Teenager Indicted for Credential Stuffing Attack on Fantasy Sports Website
* Pimcore Platform Flaws Exposed Users to Code Execution
* Researchers Identify Second Developer of 'Golden Chickens' Malware
* Cloudflare Unveils New Secrets Management Solution
* Apple Patches 3 Exploited WebKit Zero-Day Vulnerabilities
* Investors Make $6M Bet on Manifest for SBOM Management Technology
* Industrial Secure Remote Access Is Essential, but Firms Concerned About Risks
* Triple Threat: Insecure Economy, Cybercrime Recruitment and Insider Threats
* Quantum Decryption Brought Closer by Topological Qubits
* New SBOM Hub Helps All Stakeholders in Software Distribution Chain

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* Phishing Tops the List Globally as Both Initial Attack Vector and as part of Cyberattacks
* New "Greatness" Phishing-as-a-Service Tool Aids in Attacks Against Microsoft 365 Customers
* Large-Scale "Catphishing" that Targets Victims Looking for Love
* KnowBe4 Celebrates Success of 60,000-Customer Milestone
* The Number of Phishing Attacks Continues to Grow at a Rate of 150% Per Year
* CyberheistNews Vol 13 #20 [Foot in the Door] The Q1 2023's Top-Clicked Phishing Scams | INFOGRAPHIC
* The Face Off: AI Deepfakes and the Threat to the 2024 Election
* The State of Organizational Cyber Defenses Impacts Cyber Insurance Availability, Cost, and Terms
* FTC Warns of MetaMask and PayPal Phishing Campaigns
* 78% of Ransomware Victim Organizations Encounter Additional Threats-Turned-Extortions

ISC2.org Blog

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

HackRead

* OpenAI Launches ChatGPT App for iOS, Bolstering Accessibility and Safety
* Teen Charged in DraftKings Data Breach
* FBI, GCHQ Unite To Foil Russian Malware Hacking Tool
* Guide to Choosing the Best Family Cell Phone Plan
* Is it Getting Harder to Pigeonhole Games into Specific Genres?
* Debt Collection Firm Credit Control Corporation Hit by Major Data Breach
* Facebook glitch sent unintended friend requests to users

Koddos

* OpenAI Launches ChatGPT App for iOS, Bolstering Accessibility and Safety
* Teen Charged in DraftKings Data Breach
* FBI, GCHQ Unite To Foil Russian Malware Hacking Tool
* Guide to Choosing the Best Family Cell Phone Plan
* Is it Getting Harder to Pigeonhole Games into Specific Genres?
* Debt Collection Firm Credit Control Corporation Hit by Major Data Breach
* Facebook glitch sent unintended friend requests to users

Naked Security

* Apple's secret is out: 3 zero-days fixed, so be sure to patch now!
* S3 Ep135: Sysadmin by day, extortionist by night
* US offers $10m bounty for Russian ransomware suspect outed in indictment
* Belkin Wemo Smart Plug V2 - the buffer overflow that won't be patched
* Zut alors! Raclage crapuleux! Clearview AI in 20% more trouble in France
* Whodunnit? Cybercrook gets 6 years for ransoming his own employer
* S3 Ep134: It's a PRIVATE key - the hint is in the name!
* Bootkit zero-day fix - is this Microsoft's most cautious patch ever?
* Low-level motherboard security keys leaked in MSI breach, claim researchers
* PHP Packagist supply chain poisoned by hacker "looking for a job"

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

* Educating Your Board of Directors on Cybersecurity
* HEAT and EASM: What to Know About the Top Acronyms at RSA
* Is Patching the Holy Grail of Cybersecurity?
* IBM Security Guardium Ranked as a Leader in the Data Security Platforms Market
* Are Ransomware Attacks Declining, or Has Reporting Worsened?
* Do You Really Need a CISO?
* Can Large Language Models Boost Your Security Posture?
* Today's Biggest Threats Against the Energy Grid
* SaaS vs. On-Prem Data Security: Which is Right for You?
* How I Got Started: Offensive Security

InfoWorld

* JetBrains adds iOS support to cross-platform UI framework
* TypeScript 5.1 release candidate arrives
* Visual Studio updates shine on C++, Git, Wasm, and DX
* Are multiyear cloud agreements a good idea?
* Smart packaging with IoT goes beyond better tracking
* What is deep tech? Life after consumer apps
* Azul Systems boosts Java startups with CRaC
* How to use the rate limiting algorithms in ASP.NET Core
* Ruby previews pure Ruby JIT compiler
* InfoWorld Technology of the Year Awards 2023 Nominations Now Open

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.

* Hackathon Nordic IT Security
* Security Fest 2023
* Hack a Bit (Final)
* TJCTF 2023
* BSidesTLV 2023 CTF
* ESAIP CTF 2023
* DEF CON CTF Qualifier 2023
* BxMCTF 2023
* DanteCTF 2023
* CyberSci Nationals 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

* AIDE 0.18.3
* Simple Universal Fortigate Fuzzer
* Samhain File Integrity Checker 4.4.10
* Suricata IDPE 6.0.12
* 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

Kali Linux Tutorials

* WindowSpy : A Cobalt Strike Beacon Object File Meant For Targetted User Surveillance
* SilentMoonwalk - PoC Implementation Of A Fully Dynamic Call Stack Spoofer
* Unlock Your Employees' Potential: How UEM Can Help Achieve Employee Experience
* Mimicry : Security Tool For Active Deception In Exploitation And Post-Exploitation
* How to Use the Snort IDS/IPS Complete Practical Guide
* 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
* Power of Ecommerce Fraud Prevention Tools
* Shoggoth - Asmjit Based Polymorphic Encryptor

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

* Stay Ahead of Ransomware Livestream Series - Episode 2
* Memory Forensics Acquisition Cloud
* SANS Threat Analysis Rundown | Katie Nickels
* FOR498 - New Course Name, New Content & A Whole Lot of Actionable Intelligence in 90 min or less

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

* Critical Flaw in Ruckus WiFi APs - Update Firmware ASAP - ThreatWire
* Google Adds Passkey Support - Upgrade Now! - ThreatWire
* Google To Add E2EE To 2FA Authenticator Cloud Backups - ThreatWire

The PC Security Channel [TPSC]

* Windows XP Horror vs Windows 11
* Royal Ransomware: Inside a targeted attack

Eli the Computer Guy

* SQL INTRO with MySQL and Python - Hands on Class
* Anthroware CEO Jon Jones - Fire Side Chat in Asheville NC
* Eli the Computer Guy is going live!
* OpenAI Dall-E API Image Creation and Manipulation with Python - Hands on Class

Security Now

* Location Tracker Behavior - Diving deep into Google and Apple's tracker spec, SpinRite update
* Detecting Unwanted Location Trackers - Google Passkeys, Chrome lock icon, AI news sites, Vint Cerf

Troy Hunt

* Weekly Update 348

Intel Techniques: The Privacy, Security, & OSINT Show

* 297-KYC, 2FA, macOS, & OSINT Updates
* 296-The Argument for a Stock Browser

Proof of Concept (PoC) & Exploits

Packet Storm Security

* CiviCRM 5.59.alpha1 Cross Site Scripting
* ChurchCRM 4.5.4 Cross Site Scripting
* MobileTrans 4.0.11 Weak Service Permissions
* Filmora 12 Build 1.0.0.7 Unquoted Service Path
* Bludit CMS 3.14.1 Cross Site Scripting
* IBM AIX 7.2 inscout Privilege Escalation
* WordPress Core 6.2 XSS / CSRF / Directory Traversal
* SEO Friendly Blog CMS 1.0 Cross Site Scripting
* Ivanti Avalanche FileStoreConfig Shell Upload
* Kiddoware Kids Place Parental Control Android App 3.8.49 XSS / CSRF / File Upload
* Telegram On macOS TCC Bypass
* VideoStream Local Privilege Escalation
* GaanaGawaana Music Platform PHP Script 1.0 Cross Site Scripting / SQL Injection
* Screen SFT DAB 600/C Unauthenticated Information Disclosure
* Screen SFT DAB 600/C Authentication Bypass / Reset Board Config
* Screen SFT DAB 600/C Authentication Bypass / Admin Password Change
* Screen SFT DAB 600/C Authentication Bypass / Erase Account
* Screen SFT DAB 600/C Authentication Bypass / Password Change
* Screen SFT DAB 600/C Authentication Bypass / Account Creation
* RockMongo 1.1.7 Cross Site Scripting
* TinyWebGallery 2.5 Cross Site Scripting
* Epson Stylus SX510W Denial Of Service
* Siemens SIMATIC S7-1200 Cross Site Request Forgery
* Online Clinic Management System 2.2 Cross Site Scripting
* FLEX Denial Of Service

CXSecurity

* FLEX Denial Of Service
* IBM AIX 7.2 inscout Privilege Escalation
* Millhouse-Project 1.414 Shell Upload
* Millhouse-Project 1.414 Cross Site Scripting
* Pentaho Business Server Authentication Bypass / SSTI / Code Execution
* Zyxel Chained Remote Code Execution
* HammerSpace GDE / GFS 4.6.6-324 Authentication Bypass

Proof of Concept (PoC) & Exploits

Exploit Database

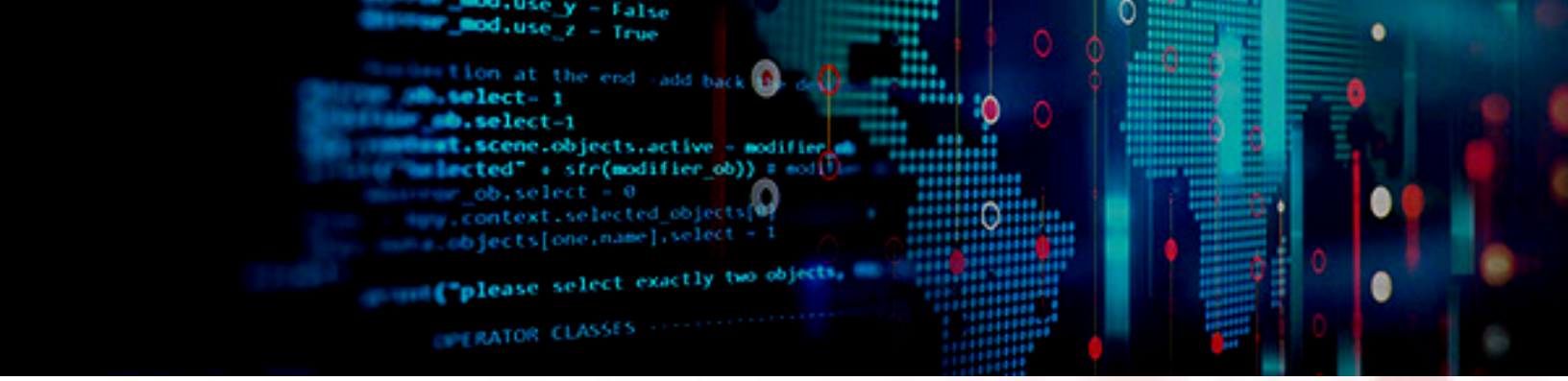
* [webapps] TinyWebGallery v2.5 - Stored Cross-Site Scripting (XSS)
* [remote] Epson Stylus SX510W Printer Remote Power Off - Denial of Service
* [webapps] Job Portal 1.0 - File Upload Restriction Bypass
* [webapps] Online Clinic Management System 2.2 - Multiple Stored Cross-Site Scripting (XSS)
* [dos] FLEX 1080
* [webapps] RockMongo 1.1.7 - Stored Cross-Site Scripting (XSS)
* [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)

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*

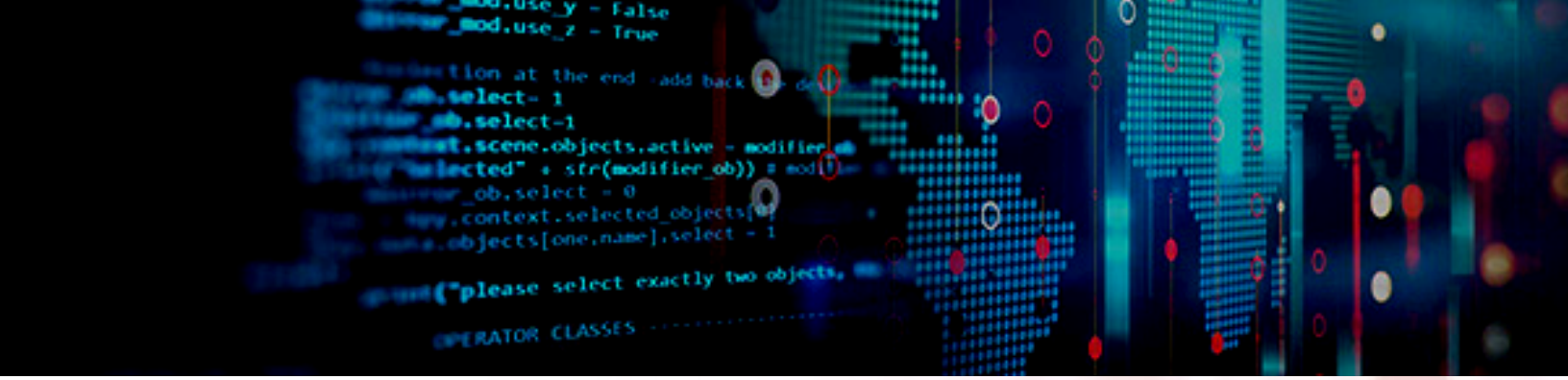
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://www.juchitlan.gob.mx/o.htm
http://www.juchitlan.gob.mx/o.htm notified by chinafans
http://camoluk.bel.tr/z.html
http://camoluk.bel.tr/z.html notified by Zer0FauLT
http://fevivienda.gov.co/Loser.html
http://fevivienda.gov.co/Loser.html notified by Boss Ranzen
https://dif.poncitlan.gob.mx/join.txt
https://dif.poncitlan.gob.mx/join.txt notified by mr.anderson
https://directorio.poncitlan.gob.mx/join.txt
https://directorio.poncitlan.gob.mx/join.txt notified by mr.anderson
http://srikandi.sukabumikota.go.id/z.php
http://srikandi.sukabumikota.go.id/z.php notified by GayAnon
https://radionigeriaabuja.gov.ng/vz.txt
https://radionigeriaabuja.gov.ng/vz.txt notified by aDriv4
http://mytv.crirs.cr.gov.ng
http://mytv.crirs.cr.gov.ng notified by Sh434t
http://reverse.crirs.cr.gov.ng
http://reverse.crirs.cr.gov.ng notified by Sh434t
http://tv.crirs.cr.gov.ng
http://tv.crirs.cr.gov.ng notified by Sh434t
https://api.crirs.cr.gov.ng
https://api.crirs.cr.gov.ng notified by Sh434t
https://basic.crirs.cr.gov.ng
https://basic.crirs.cr.gov.ng notified by Sh434t
https://goverment.crirs.cr.gov.ng
https://goverment.crirs.cr.gov.ng notified by Sh434t
https://eagrimet.cilss.int/1915.php
https://eagrimet.cilss.int/1915.php notified by D4LGH4CK_TM
https://forum2is.cilss.int/1915.php
https://forum2is.cilss.int/1915.php notified by D4LGH4CK_TM
https://pariis-bibliotheque.cilss.int/turk.php
https://pariis-bibliotheque.cilss.int/turk.php notified by D4LGH4CK_TM
https://caraga.bfar.da.gov.ph/xx.html
https://caraga.bfar.da.gov.ph/xx.html notified by xstro0

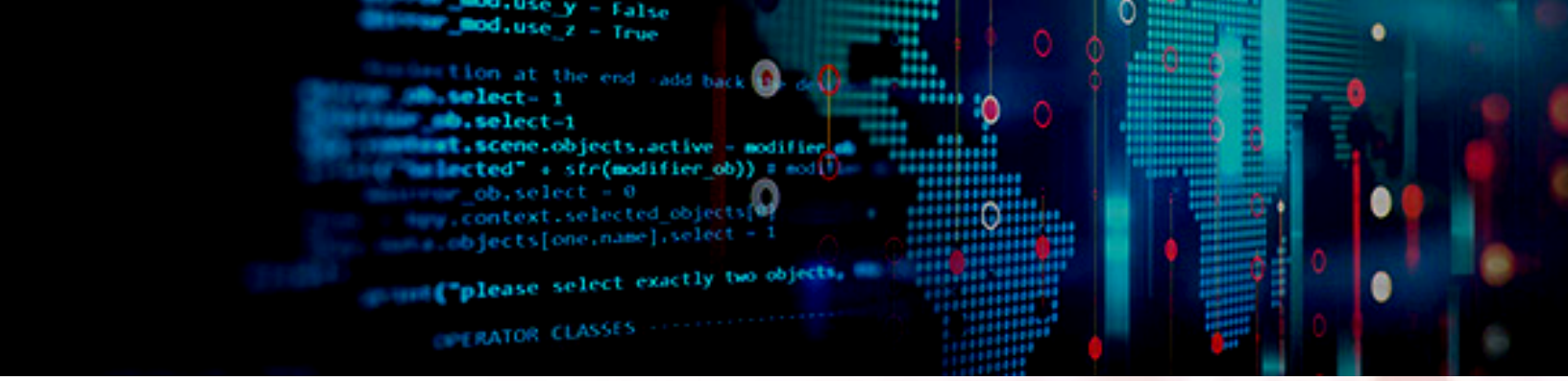


Dark Web News

Darknet Live

[Skynet Market Admin Pleads Guilty]
[The Hitchhiker's Guide to VPNs]
[Silk Road Vendor and Murder-for-Hire Orchestrator Charged]
[UK Trio Manufactured and Sold Counterfeit Xanax Pills]

Dark Web Link



Trend Micro Anti-Malware Blog

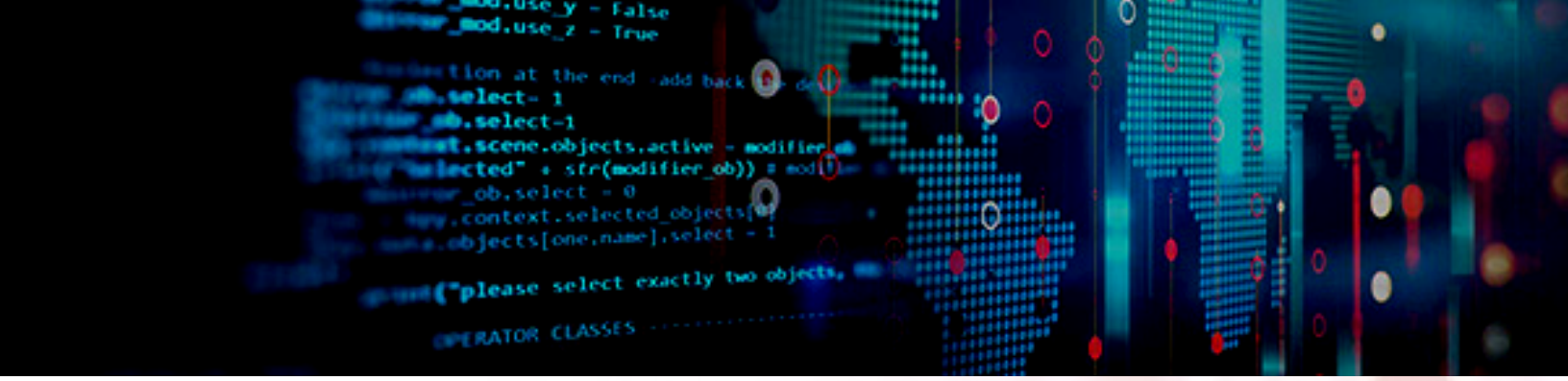
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

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
* Introducing: 'Saved Filters' in InsightCloudSec
* Rapid7 Recognized as a Strong Performer in The Forrester Waveâ„¢ for MDR, Q2 2023
* CVE-2023-27350: Ongoing Exploitation of PaperCut Remote Code Execution Vulnerability
* Metasploit Wrap-up
* [The Lost Bots] S03E03. The Rise of The Machines
* The Velociraptor 2023 Annual Community Survey
* Patch Tuesday - May 2023
* Metasploit Weekly Wrap-Up
* AppDomain Manager Injection: New Techniques For Red Teams



Advisories

US-Cert Alerts & bulletins

* CISA Adds Three Known Exploited Vulnerabilities to Catalog
* Cisco Releases Security Advisory for Small Business Series Switches
* CISA Releases Five Industrial Control Systems Advisories
* CISA and Partners Release BianLian Ransomware Cybersecurity Advisory
* CISA Releases Three Industrial Control Systems Advisories
* CISA Adds Seven Known Exploited Vulnerabilities to Catalog
* CISA and FBI Release Joint Advisory in Response to Active Exploitation of PaperCut Vulnerability
* CISA Releases Fifteen Industrial Control Systems Advisories
* #StopRansomware: BianLian Ransomware Group
* Malicious Actors Exploit CVE-2023-27350 in PaperCut MF and NG
* Vulnerability Summary for the Week of May 8, 2023
* Vulnerability Summary for the Week of May 1, 2023

Zero Day Initiative Advisories

ZDI-CAN-20604: Kofax
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 'rgod' was reported to the affected vendor on: 2023-05-19, 3 days ago. The vendor is given until 2023-09-16 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-20605: Kofax
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 'rgod' was reported to the affected vendor on: 2023-05-19, 3 days ago. The vendor is given until 2023-09-16 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-21202: Linux
A CVSS score 4.0 (AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-05-19, 3 days ago. The vendor is given until 2023-09-16 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-20601: Kofax
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 'rgod' was reported to the affected vendor on: 2023-05-19, 3 days ago. The vendor is given until 2023-09-16 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-20940: Linux
A CVSS score 7.5 (AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-05-19, 3 days ago. The vendor is given until 2023-09-16 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-21201: Microsoft

A CVSS score 7.5 (AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Li Jiantao (@CurseRed), Ngo Wei Lin (@Creastery), Pan Zhenpeng (@Peterpan980927), Poh Jia Hao (@Chocologicall) of STAR Labs SG Pte. Ltd.' was reported to the affected vendor on: 2023-05-19, 3 days ago. The vendor is given until 2023-09-16 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-21200: Microsoft

A CVSS score 5.6 (AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Li Jiantao (@CurseRed), Ngo Wei Lin (@Creastery), Pan Zhenpeng (@Peterpan980927), Poh Jia Hao (@Chocologicall) of STAR Labs SG Pte. Ltd.' was reported to the affected vendor on: 2023-05-19, 3 days ago. The vendor is given until 2023-09-16 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-21106: 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 'Simon Janz (@esj4y)' was reported to the affected vendor on: 2023-05-19, 3 days ago. The vendor is given until 2023-09-16 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-21132: 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 'Simon Janz (@esj4y)' was reported to the affected vendor on: 2023-05-19, 3 days ago. The vendor is given until 2023-09-16 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-20812: Microsoft

A CVSS score 7.1 (AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:N) severity vulnerability discovered by 'Li Jiantao (@CurseRed), Ngo Wei Lin (@Creastery), Pan Zhenpeng (@Peterpan980927), Poh Jia Hao (@Chocologicall) of STAR Labs SG Pte. Ltd.' was reported to the affected vendor on: 2023-05-19, 3 days ago. The vendor is given until 2023-09-16 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-20851: Schneider Electric

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 'Sina Kheirkhah (@SinSinology) of Summoning Team (@SummoningTeam)' was reported to the affected vendor on: 2023-05-19, 3 days ago. The vendor is given until 2023-09-16 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-20982: Microsoft

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: 2023-05-19, 3 days ago. The vendor is given until 2023-09-16 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-21183: Google

A CVSS score 4.3 (AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Hossein Lotfi of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-05-19, 3 days ago. The vendor is given until 2023-09-16 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-21025: Foxit

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: 2023-05-17, 5 days ago. The vendor is given until 2023-09-14 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-21019: Foxit

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: 2023-05-17, 5 days ago. The vendor is given until 2023-09-14 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-21020: Foxit

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: 2023-05-17, 5 days ago. The vendor is given until 2023-09-14 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-21062: Foxit

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: 2023-05-17, 5 days ago. The vendor is given until 2023-09-14 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-21085: Foxit

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: 2023-05-17, 5 days ago. The vendor is given until 2023-09-14 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-21083: Foxit

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: 2023-05-17, 5 days ago. The vendor is given until 2023-09-14 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-21022: Foxit

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: 2023-05-17, 5 days ago. The vendor is given until 2023-09-14 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-21100: 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 'Nicholas Zubrisky' was reported to the affected vendor on: 2023-05-17, 5 days ago. The vendor is given until 2023-09-14 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-20971: oFono

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 'Mitch Zakocs @ ASU SEFCOM Lab' was reported to the affected vendor on: 2023-05-17, 5 days ago. The vendor is given until 2023-09-14 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-20768: Famatech

A CVSS score 7.3 (AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Xavier DANEST' was reported to the affected vendor on: 2023-05-12, 10 days ago. The vendor is given until 2023-09-09 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-21086: Sante

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: 2023-05-11, 11 days ago. The vendor

is given until 2023-09-08 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

Red Hat Security Advisory 2023-3167-01

Red Hat Security Advisory 2023-3167-01 - New Red Hat build of Cryostat 2.3.0 on RHEL 8 container images have been released, adding a variety of features and bug fixes. Issues addressed include a denial of service vulnerability.

Ubuntu Security Notice USN-6091-1

Ubuntu Security Notice 6091-1 - It was discovered that some AMD x86-64 processors with SMT enabled could speculatively execute instructions using a return address from a sibling thread. A local attacker could possibly use this to expose sensitive information. Ziming Zhang discovered that the VMware Virtual GPU DRM driver in the Linux kernel contained an out-of-bounds write vulnerability. A local attacker could use this to cause a denial of service.

Red Hat Security Advisory 2023-3229-01

Red Hat Security Advisory 2023-3229-01 - An update for openshift-gitops-kam is now available for Red Hat OpenShift GitOps 1.8. Red Hat Product Security has rated this update as having a security impact of Important. Issues addressed include a bypass vulnerability.

Ubuntu Security Notice USN-6090-1

Ubuntu Security Notice 6090-1 - It was discovered that some AMD x86-64 processors with SMT enabled could speculatively execute instructions using a return address from a sibling thread. A local attacker could possibly use this to expose sensitive information. Zheng Wang discovered that the Intel i915 graphics driver in the Linux kernel did not properly handle certain error conditions, leading to a double-free. A local attacker could possibly use this to cause a denial of service.

Ubuntu Security Notice USN-6089-1

Ubuntu Security Notice 6089-1 - It was discovered that the Intel i915 graphics driver in the Linux kernel did not perform a GPU TLB flush in some situations. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Red Hat Security Advisory 2023-0584-01

Red Hat Security Advisory 2023-0584-01 - Secondary Scheduler Operator for Red Hat OpenShift 1.1.1. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2023-3195-01

Red Hat Security Advisory 2023-3195-01 - Jenkins is a continuous integration server that monitors executions of repeated jobs, such as building a software project or jobs run by cron. Issues addressed include bypass, cross site scripting, information leakage, and insecure permissions vulnerabilities.

WordPress Elementor Lite 5.7.1 Arbitrary Password Reset

On May 11 2023, Essential Addons for Elementor, a WordPress plugin with over one million active installations, released a patch for a critical vulnerability that made it possible for any unauthenticated user to reset arbitrary user passwords, including user accounts with administrative-level access. Versions 5.7.1 and below are affected.

Debian Security Advisory 5405-1

Debian Linux Security Advisory 5405-1 - It was discovered that missing input sanitizing in the implementation of the OIDCStripCookie option in mod_auth_openidc could result in denial of service.

Red Hat Security Advisory 2023-3221-01

Red Hat Security Advisory 2023-3221-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 102.11.0. Issues addressed include a bypass vulnerability.

Red Hat Security Advisory 2023-3220-01

Red Hat Security Advisory 2023-3220-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 102.11.0 ESR. Issues addressed include a bypass vulnerability.

Red Hat Security Advisory 2023-3223-01

Red Hat Security Advisory 2023-3223-01 - Red Hat AMQ Streams, based on the Apache Kafka project, offers

a distributed backbone that allows microservices and other applications to share data with extremely high throughput and extremely low latency. This release of Red Hat AMQ Streams 2.4.0 serves as a replacement for Red Hat AMQ Streams 2.3.0, and includes security and bug fixes, and enhancements. Issues addressed include denial of service, deserialization, information leakage, memory exhaustion, and resource exhaustion vulnerabilities.

Ubuntu Security Notice USN-6087-1

Ubuntu Security Notice 6087-1 - 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 only affected Ubuntu 16.04 ESM.

Ubuntu Security Notice USN-6088-1

Ubuntu Security Notice 6088-1 - It was discovered that runC incorrectly made /sys/fs/cgroup writable when in rootless mode. An attacker could possibly use this issue to escalate privileges. It was discovered that runC incorrectly performed access control when mounting /proc to non-directories. An attacker could possibly use this issue to escalate privileges. It was discovered that runC incorrectly handled /proc and /sys mounts inside a container. An attacker could possibly use this issue to bypass AppArmor, and potentially SELinux.

Ubuntu Security Notice USN-6086-1

Ubuntu Security Notice 6086-1 - It was discovered that minimatch incorrectly handled certain inputs. If a user or an automated system were tricked into opening a specially crafted input file, a remote attacker could possibly use this issue to cause a denial of service.

Red Hat Security Advisory 2023-1329-01

Red Hat Security Advisory 2023-1329-01 - Red Hat build of MicroShift is Red Hat's light-weight Kubernetes orchestration solution designed for edge device deployments and is built from the edge capabilities of Red Hat OpenShift. MicroShift is an application that is deployed on top of Red Hat Enterprise Linux devices at the edge, providing an efficient way to operate single-node clusters in these low-resource environments. This advisory contains the RPM packages for Red Hat build of MicroShift 4.13.0. Issues addressed include a man-in-the-middle vulnerability.

Red Hat Security Advisory 2023-2138-01

Red Hat Security Advisory 2023-2138-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the extra low-latency container images for Red Hat OpenShift Container Platform 4.13. Issues addressed include a bypass vulnerability.

Red Hat Security Advisory 2023-3205-01

Red Hat Security Advisory 2023-3205-01 - OpenShift Virtualization is Red Hat's virtualization solution designed for Red Hat OpenShift Container Platform. This advisory contains OpenShift Virtualization 4.13.0 images. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2023-1325-01

Red Hat Security Advisory 2023-1325-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.13.0. Issues addressed include bypass, denial of service, and information leakage vulnerabilities.

Red Hat Security Advisory 2023-1328-01

Red Hat Security Advisory 2023-1328-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. Issues addressed include denial of service and out of bounds read vulnerabilities.

Red Hat Security Advisory 2023-3204-01

Red Hat Security Advisory 2023-3204-01 - OpenShift Virtualization is Red Hat's virtualization solution designed for Red Hat OpenShift Container Platform. This advisory contains OpenShift Virtualization 4.13.0 RPMs. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2023-2695-01

Red Hat Security Advisory 2023-2695-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.11.40.

Red Hat Security Advisory 2023-3198-01

Red Hat Security Advisory 2023-3198-01 - Jenkins is a continuous integration server that monitors executions of repeated jobs, such as building a software project or jobs run by cron. Issues addressed include bypass, code execution, cross site request forgery, cross site scripting, denial of service, deserialization, information leakage, and insecure permissions vulnerabilities.

Red Hat Security Advisory 2023-1326-01

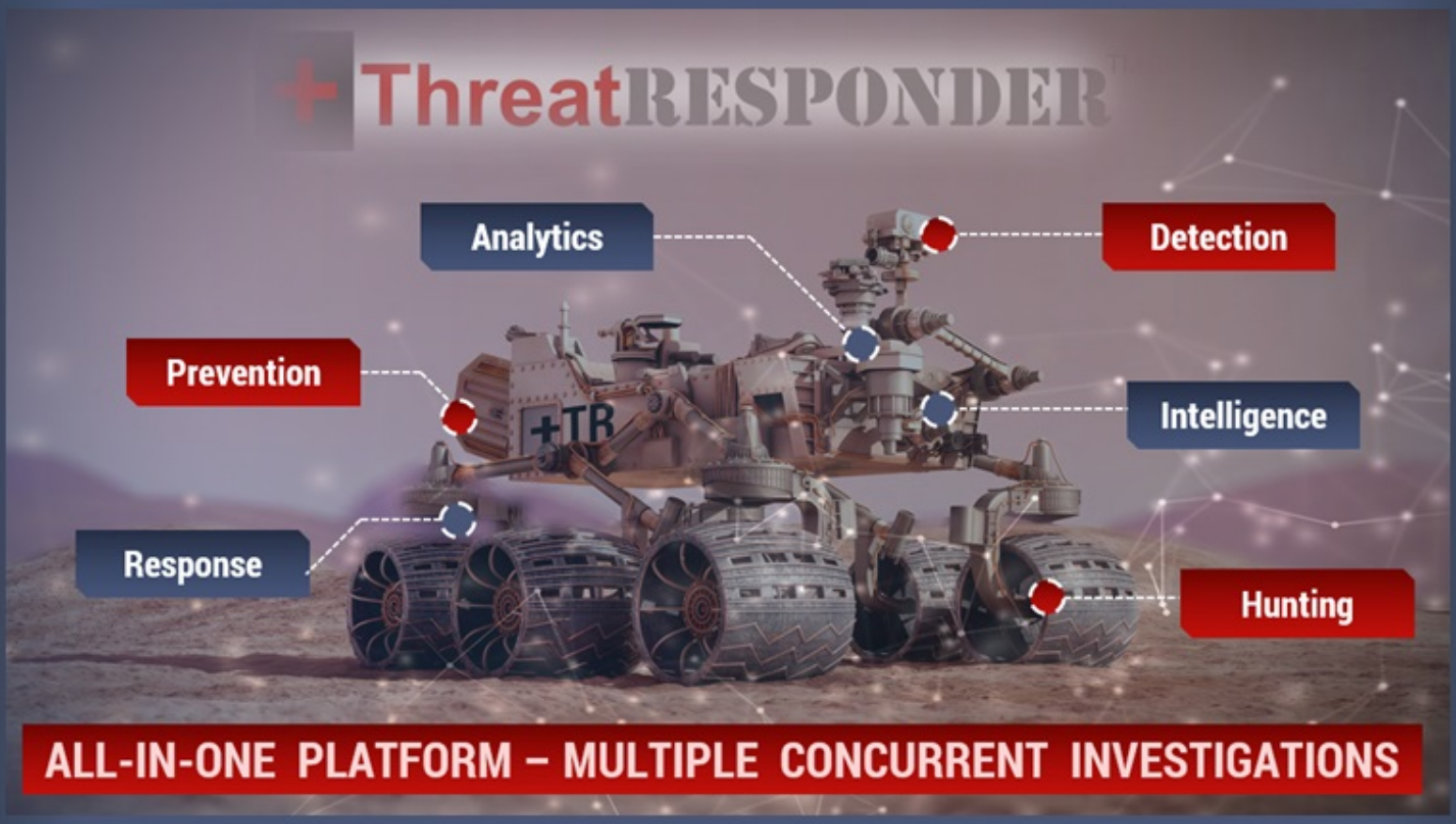
Red Hat Security Advisory 2023-1326-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the container images for Red Hat OpenShift Container Platform 4.13.0. Issues addressed include bypass, denial of service, information leakage, out of bounds read, and remote SQL injection vulnerabilities.

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



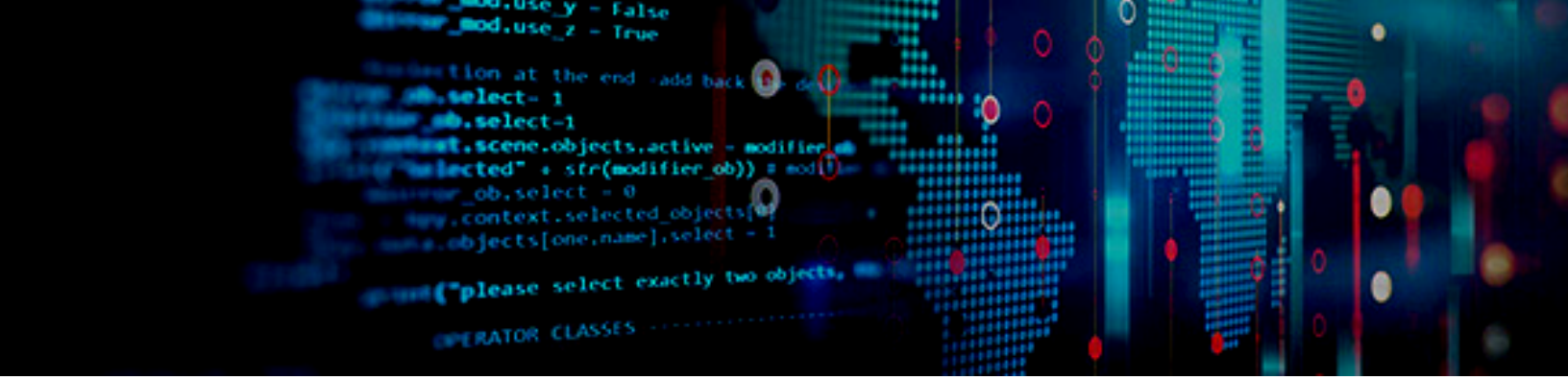
The Solution – ThreatResponder® Platform

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

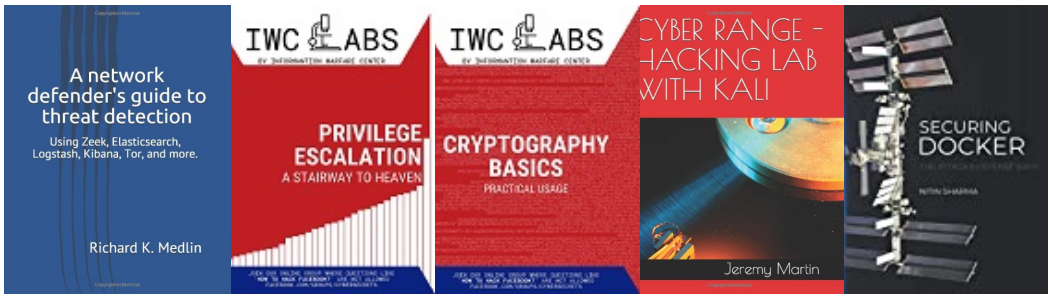


The Cyber Secrets publications on Amazon

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