May-29-23

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 29, 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

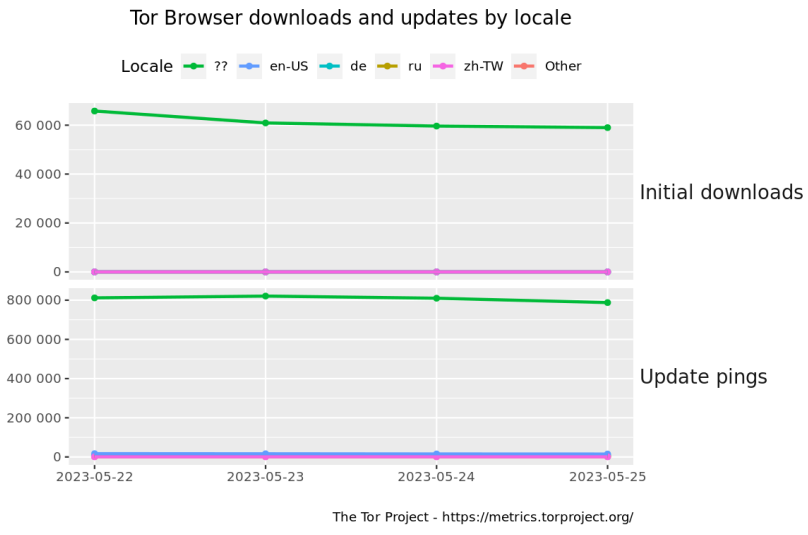
Internet Storm Center Infocon Status

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

* Senator Wyden Seems Surprised By US Govt Spyware Stance
* AI Opinion: I Do Not Think Ethical Surveillance Can Exist
* OneMain Pays $4.5M After Ignored Security Flaws Caused Data Breaches
* Is Cybersecurity An Unsolvable Problem?
* Google Cloud Patches Vulnerability In CloudSQL Service
* CosmicEnergy Malware Poses Plausible Threat To Electric Grids
* BlackByte Ransomware Crew Claims City Of Augusta, Georgia
* Dutch Watchdog Looking Into Alleged Tesla Data Breach
* Reflections On Ten Years Past The Snowden Revelations
* Legion Malware Expands Scope To Target AWS CloudWatch Monitoring Tool
* UN Official And Others In Armenia Hacked By NSO Group Spyware
* API Bug In OAuth Dev Tool Opened Apps To Account Hijacking
* Why Are 1.8M Apria Patients Just Now Being Notified Of A 2021 Breach?
* Chinese Hackers That Triggered US Alarm Hit Defense Targets
* Facial Recognition System Used By Met Police Shows Racial Bias At Low Thresholds
* Infecting SSH Public Keys With Backdoors
* Netflix Puts U.S. Password Sharing Customers On Notice
* BlackCat Ransomware Takes Control With New Kernel Driver
* Widespread FBI Abuse Of Foreign Spy Law Sets Off Alarm Bells
* OpenAI Leaders Call For Regulation To Prevent AI Destroying Humanity
* Quantum Attack Would Trigger Great Depression, Think Tank Warns
* KeePass Bug Lets Attackers Extract The Master Password From Memory
* Ads For Lucrative Jobs In Asia Fail To Mention Chance Of Slavery As Crypto-Scammer
* Uncle Sam Strangles Criminals' Cash Flow By Reining In Money Mules
* China Hasn't Told Micron Why It Failed Security Review, Or What Its Ban Means

Krebs on Security

* Phishing Domains Tanked After Meta Sued Freenom
* Interview With a Crypto Scam Investment Spammer
* 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

Dark Reading

* Top Cyberattacks Revealed in New Threat Intelligence Report
* 2 Lenses for Examining the Safety of Open Source Software
* 130K+ Patients' Social Security Numbers Leaked in UHS of Delaware Data Breach
* Tesla Whistleblower Leaks 100GB of Data, Revealing Safety Complaints
* Travel-Themed Phishing, BEC Campaigns Get Smarter as Summer Season Arrives
* How Safe Is Your Wearable Device?
* Russia's War in Ukraine Shows Cyberattacks Can Be War Crimes
* 'Volt Typhoon' Breaks Fresh Ground for China-Backed Cyber Campaigns
* Red Hat Tackles Software Supply Chain Security
* CosmicEnergy Malware Emerges, Capable of Electric Grid Shutdown
* Lazarus Group Striking Vulnerable Windows IIS Web Servers
* Netflix's Password-Sharing Ban Offers Security Upsides
* Perception Point Report Finds That Advanced Phishing Attacks Grew by 356% in 2022
* Memcyco Delivers Real-Time Brandjacking Detection and Protection Solution
* Bank of Ghana Opens SOC to Enable Threat Intelligence Sharing
* 'Operation Magalenha' Attacks Give a Window Into Brazil's Cybercrime Ecosystem
* Google Cloud Bug Allows Server Takeover From CloudSQL Service
* Dangerous Regions: Isolating Branch Offices in High-Risk Countries
* CISO Criminalization, Vague Cyber Disclosure Rules Create Angst for Security Teams
* 'Volt Typhoon' China-Backed APT Infiltrates US Critical Infrastructure Orgs

The Hacker News

* New BrutePrint Attack Lets Attackers Unlock Smartphones with Fingerprint Brute-Force
* AceCryptor: Cybercriminals' Powerful Weapon, Detected in 240K+ Attacks
* 3 Challenges in Building a Continuous Threat Exposure Management (CTEM) Program and How to Beat Them
* New GobRAT Remote Access Trojan Targeting Linux Routers in Japan
* Don't Click That ZIP File! Phishers Weaponizing .ZIP Domains to Trick Victims
* PyPI Implements Mandatory Two-Factor Authentication for Project Owners
* New Stealthy Bandit Stealer Targeting Web Browsers and Cryptocurrency Wallets
* Critical OAuth Vulnerability in Expo Framework Allows Account Hijacking
* Severe Flaw in Google Cloud's Cloud SQL Service Exposed Confidential Data
* Predator Android Spyware: Researchers Uncover New Data Theft Capabilities
* 5 Must-Know Facts about 5G Network Security and Its Cloud Benefits
* New COSMICENERGY Malware Exploits ICS Protocol to Sabotage Power Grids
* Barracuda Warns of Zero-Day Exploited to Breach Email Security Gateway Appliances
* Dark Frost Botnet Launches Devastating DDoS Attacks on Gaming Industry
* Zyxel Issues Critical Security Patches for Firewall and VPN Products

Security Week

* Industrial Giant ABB Confirms Ransomware Attack, Data Theft
* Organizations Worldwide Targeted in Rapidly Evolving Buhti Ransomware Operation
* Google Cloud Users Can Now Automate TLS Certificate Lifecycle
* Zyxel Firewalls Hacked by Mirai Botnet
* Watch Now: Threat Detection and Incident Response Virtual Summit
* NCC Group Releases Open Source Tools for Developers, Pentesters
* Memcyco Raises $10 Million in Seed Funding to Prevent Website Impersonation
* New Russia-Linked CosmicEnergy ICS Malware Could Disrupt Electric Grids
* Security Pros: Before You Do Anything, Understand Your Threat Landscape
* Major Massachusetts Health Insurer Hit by Ransomware Attack, Member Data May Be Compromised

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* [Mastering Minds] China's Cognitive Warfare Ambitions Are Social Engineering At Scale
* Your KnowBe4 Fresh Content Updates from May 2023
* Verizon Sends New Smishing Warning
* [SEG Headache] More Than Half of Cybersecurity Leaders Say That Too Many Phishing Attacks Get Through
* Financial Fraud Phishing Attacks Increase 72% In One Year; Financial Industry Takes the Brunt
* BatLoader Malware is Now Distributed in Drive-By Attacks
* More Than Half of all Email-Based Cyberattacks Bypass Legacy Security Filters
* [Hands-On Defense] Unpatched Software Causes 33% of Successful Attacks
* CyberheistNews Vol 13 #21 [Double Trouble] 78% of Ransomware Victims Face Multiple Extortions in Scar
* [Microsoft Warning] A 38% Spike In Business Email Compromise with new Cybercrime-as-a-Service

ISC2.org Blog

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

HackRead

* Data Breach at MCNA Dental Insurer Impacts 9 Million Users
* Jimbos Protocol Hack: $7.5 Million Lost in Latest DeFi Attack
* Stealing From Wallets to Browsers: Bandit Stealer Hits Windows Devices
* Gaming Firms and Community Members Hit by Dark Frost Botnet
* Mirai Malware Hits Zyxel Devices After Command Injection Bug
* Operation Magalenha: Brazilian Hackers Hit Portuguese Banks in Malware Attack
* Netflix's Password Sharing Crackdown Goes Global: 103 Countries Affected

Koddos

* Data Breach at MCNA Dental Insurer Impacts 9 Million Users
* Jimbos Protocol Hack: $7.5 Million Lost in Latest DeFi Attack
* Stealing From Wallets to Browsers: Bandit Stealer Hits Windows Devices
* Gaming Firms and Community Members Hit by Dark Frost Botnet
* Mirai Malware Hits Zyxel Devices After Command Injection Bug
* Operation Magalenha: Brazilian Hackers Hit Portuguese Banks in Malware Attack
* Netflix's Password Sharing Crackdown Goes Global: 103 Countries Affected

Naked Security

* S3 Ep136: Navigating a manic malware maelstrom
* Ransomware tales: The MitM attack that really had a Man in the Middle
* PyPI open-source code repository deals with manic malware maelstrom
* Phone scamming kingpin gets 13 years for running "iSpoof" service
* 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

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

* Despite Tech Layoffs, Cybersecurity Positions are Hiring
* How I Got Started: White Hat Hacker
* Heads Up CEO! Cyber Risk Influences Company Credit Ratings
* CISA, NSA Issue New IAM Best Practice Guidelines
* 6 Ways to Mitigate Risk While Expanding Access
* Hypervisors and Ransomware: Defending Attractive Targets
* NIST Launches Cybersecurity Initiative for Small Businesses
* 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?

InfoWorld

* When the rubber duck talks back
* 5 best practices for software development partnerships
* Latest Deno release supports NPM packages
* Amazing federated multicloud apps
* PostgreSQL 16 advances query parallelism
* Microsoft Dev Box due this summer
* Angular users want better server-side rendering
* Microsoft .NET 8 boosts Blazor, WebAssembly
* How to use factory-based middleware activation in ASP.NET Core
* Snowflake acquires Neeva to add generative AI-based search to Data Cloud

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.

* BxMCTF 2023
* DanteCTF 2023
* CyberSci Nationals 2023
* Break the Syntax CTF 2023
* justCTF 2023
* PwnMe Finals : "8 bits"
* HSCTF 10
* Ugra CTF Open 2023
* Season III: US Cyber Open CTF
* GPN CTF 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

* Wireshark Analyzer 4.0.6
* tc Tor Chat Client
* Stegano 0.11.2
* Zeek 5.0.9
* Nmap Port Scanner 7.94
* 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

Kali Linux Tutorials

* Reportly : An AzureAD User Activity Report Tool
* From Endpoint Management to Experience Management - UEM Does It The Best!
* How to Use Ettercap to Intercept and Sniff Passwords
* 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

GBHackers Analysis

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

Weekly Cyber Security Video and Podcasts

SANS DFIR

* SANS Threat Analysis Rundown | Katie Nickels
* SANS Threat Analysis Rundown | Katie Nickels
* Stay Ahead of Ransomware Livestream Series - Episode 2
* Memory Forensics Acquisition Cloud

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

* KeePass Master Passwords Could Be Stolen - ThreatWire
* Critical Flaw in Ruckus WiFi APs - Update Firmware ASAP - ThreatWire
* Google Adds Passkey Support - Upgrade Now! - ThreatWire

The PC Security Channel [TPSC]

* How to use Windows Firewall to block Hackers and Malware
* Windows XP Horror vs Windows 11

Eli the Computer Guy

* SILICON DOJO - In Person Tech Education in Asheville NC
* SQL INTRO with MySQL and Python - Hands on Class
* Anthroware CEO Jon Jones - Fire Side Chat in Asheville NC
* OpenAI Dall-E API Image Creation and Manipulation with Python - Hands on Class

Security Now

* VCaaS - Voice Cloning as a Service - HP printer update, KeePass vulnerability, SpinRite bug
* Location Tracker Behavior - Diving deep into Google and Apple's tracker spec, SpinRite update

Troy Hunt

* Weekly Update 349

Intel Techniques: The Privacy, Security, & OSINT Show

* 298-OSINT Maintenance
* 297-KYC, 2FA, macOS, & OSINT Updates

Proof of Concept (PoC) & Exploits

Packet Storm Security

* New MVC Shop 1.0 SQL Injection / Missing Attributes
* Simple Customer Relationship Management CRM 2023 1.0 SQL Injection
* e-Biz Technocrats Pvt.Ltd SQL Injection
* Jobs Portal 3.6 Insecure Settings
* Camaleon CMS 2.7.0 Server-Side Template Injection
* Seagate Central Storage 2015.0916 User Creation / Command Execution
* SCM Manager 1.60 Cross Site Scripting
* Ulicms 2023.1 Create Administrator
* Zenphoto 1.6 Cross Site Scripting
* WBCE CMS 1.6.1 Cross Site Scripting
* WordPress Beautiful Cookie Consent Banner 2.10.1 Cross Site Scripting
* 2023 Online Course Registration 1.0 SQL Injection
* WFTPD 3.25 Credential Disclosure
* Service Provider Management System 1.0 SQL Injection
* FusionInvoice 2023-1.0 Cross Site Scripting
* GetSimple CMS 3.3.16 Shell Upload
* thrsrossi Millhouse-Project 1.414 Shell Upload
* Roxy WI 6.1.0.0 Remote Command Execution
* eScan Management Console 14.0.1400.2281 SQL Injection
* Webkul Qloapps 1.5.2 Cross Site Scripting
* eScan Management Console 14.0.1400.2281 Cross Site Scripting
* Quicklancer 1.0 SQL Injection
* Smart School 1.0 SQL Injection
* LeadPro CRM 1.0 SQL Injection
* Yank Note 3.52.1 Arbitrary Code Execution

CXSecurity

* SCM Manager 1.60 Cross Site Scripting
* Screen SFT DAB 600/C Authentication Bypass Admin Password Change
* Laravel 10.11 Database Disclosure / Information Disclosure
* Screen SFT DAB 600/C Authentication Bypass Reset Board Config
* thrsrossi Millhouse-Project 1.414 Remote Code Execution
* PaperCut NG/MG 22.0.4 Remote Code Execution (RCE)
* FLEX Denial Of Service

Proof of Concept (PoC) & Exploits

Exploit Database

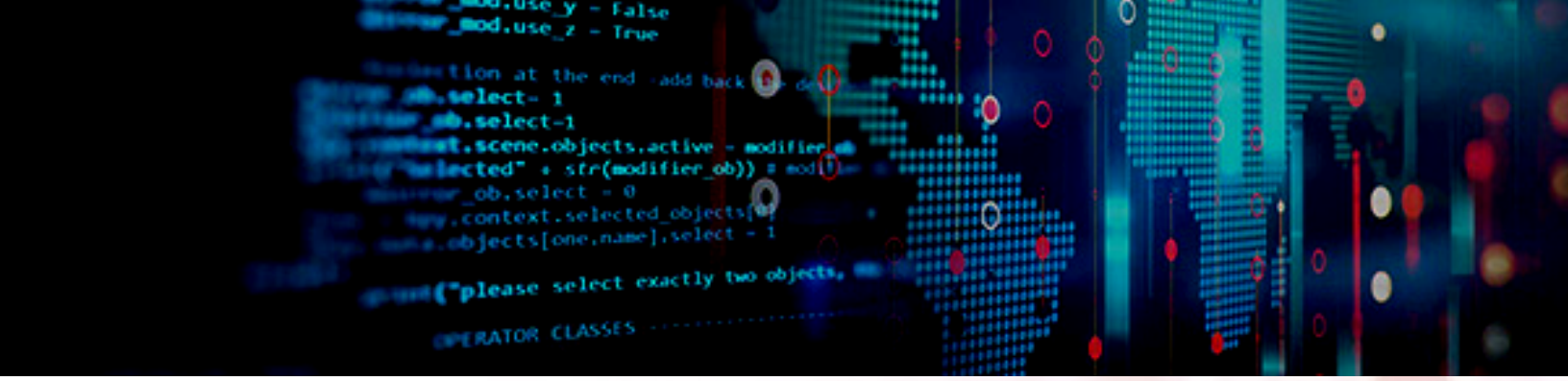
* [webapps] Camaleon CMS v2.7.0 - Server-Side Template Injection (SSTI)
* [webapps] SCM Manager 1.60 - Cross-Site Scripting Stored (Authenticated)
* [remote] Seagate Central Storage 2015.0916 - Unauthenticated Remote Command Execution (Metasploit)
* [webapps] Ulicms 2023.1 - create admin user via mass assignment
* [webapps] Zenphoto 1.6 - Multiple stored XSS
* [webapps] WBCE CMS 1.6.1 - Multiple Stored Cross-Site Scripting (XSS)
* [local] Filmora 12 version (Build 1.0.0.7) - Unquoted Service Paths Privilege Escalation
* [webapps] Service Provider Management System v1.0 - SQL Injection
* [webapps] Roxy WI v6.1.0.0 - Unauthenticated Remote Code Execution (RCE) via subprocess_execute
* [webapps] FusionInvoice 2023-1.0 - Stored XSS (Cross-Site Scripting)
* [local] MobileTrans 4.0.11 - Weak Service Privilege Escalation
* [webapps] CiviCRM 5.59.alpha1 - Stored XSS (Cross-Site Scripting)
* [webapps] ChurchCRM v4.5.4 - Reflected XSS via Image (Authenticated)
* [webapps] Bludit CMS v3.14.1 - Stored Cross-Site Scripting (XSS) (Authenticated)
* [webapps] GetSimple CMS v3.3.16 - Remote Code Execution (RCE)
* [webapps] Quicklancer v1.0 - SQL Injection
* [webapps] Stackposts Social Marketing Tool v1.0 - SQL Injection
* [webapps] Smart School v1.0 - SQL Injection
* [webapps] LeadPro CRM v1.0 - SQL Injection
* [local] Yank Note v3.52.1 (Electron) - Arbitrary Code Execution
* [local] Gin Markdown Editor v0.7.4 (Electron) - Arbitrary Code Execution
* [webapps] Affiliate Me Version 5.0.1 - SQL Injection
* [webapps] eScan Management Console 14.0.1400.2281 - Cross Site Scripting
* [webapps] eScan Management Console 14.0.1400.2281 - SQL Injection (Authenticated)
* [webapps] Webkul Qloapps 1.5.2 - 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*

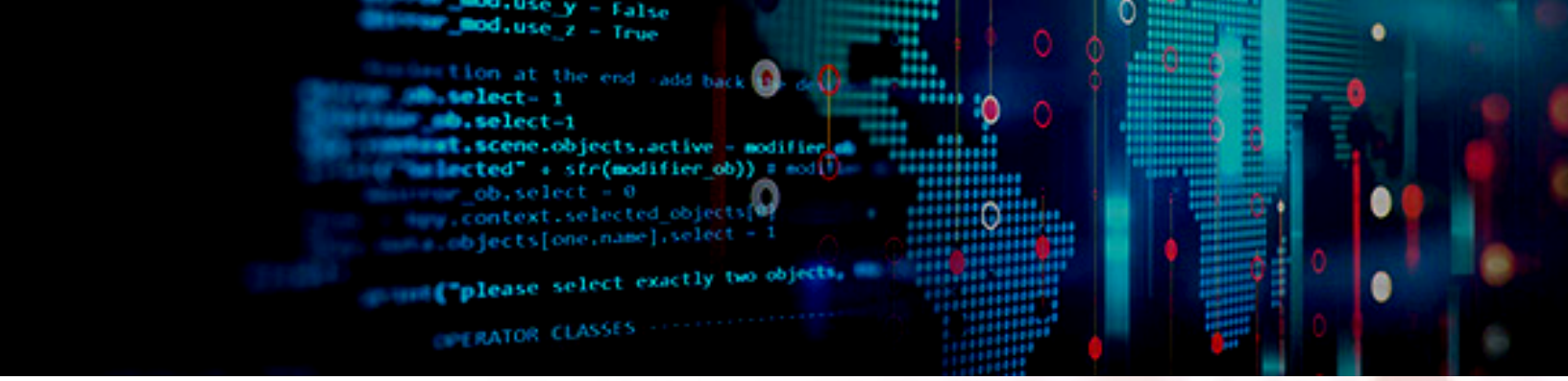
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://ati.prefeitura.sp.gov.br
http://ati.prefeitura.sp.gov.br notified by nel00d
https://xpat-egov-mv.com
https://xpat-egov-mv.com notified by nel00d
http://metadata42.defensoria-nsjp.gob.mx
http://metadata42.defensoria-nsjp.gob.mx notified by Simsimi
http://metadata41.defensoria-nsjp.gob.mx
http://metadata41.defensoria-nsjp.gob.mx notified by Simsimi
http://metadata40.defensoria-nsjp.gob.mx
http://metadata40.defensoria-nsjp.gob.mx notified by Simsimi
http://metadata39.defensoria-nsjp.gob.mx
http://metadata39.defensoria-nsjp.gob.mx notified by Simsimi
http://metadata38.defensoria-nsjp.gob.mx
http://metadata38.defensoria-nsjp.gob.mx notified by Simsimi
http://metadata37.defensoria-nsjp.gob.mx
http://metadata37.defensoria-nsjp.gob.mx notified by Simsimi
http://metadata36.defensoria-nsjp.gob.mx
http://metadata36.defensoria-nsjp.gob.mx notified by Simsimi
http://metadata35.defensoria-nsjp.gob.mx
http://metadata35.defensoria-nsjp.gob.mx notified by Simsimi
http://metadata34.defensoria-nsjp.gob.mx
http://metadata34.defensoria-nsjp.gob.mx notified by Simsimi
http://metadata33.defensoria-nsjp.gob.mx
http://metadata33.defensoria-nsjp.gob.mx notified by Simsimi
http://metadata33.eastus.cloudapp.azure.com
http://metadata33.eastus.cloudapp.azure.com notified by Simsimi
http://www.machadinho.ro.gov.br/vz.txt
http://www.machadinho.ro.gov.br/vz.txt notified by aDriv4
http://www.coronavirus.apodaca.gob.mx/vz.txt
http://www.coronavirus.apodaca.gob.mx/vz.txt notified by aDriv4
http://tramites.apodaca.gob.mx/vz.txt
http://tramites.apodaca.gob.mx/vz.txt notified by aDriv4
http://tys.apodaca.gob.mx/vz.txt
http://tys.apodaca.gob.mx/vz.txt notified by aDriv4

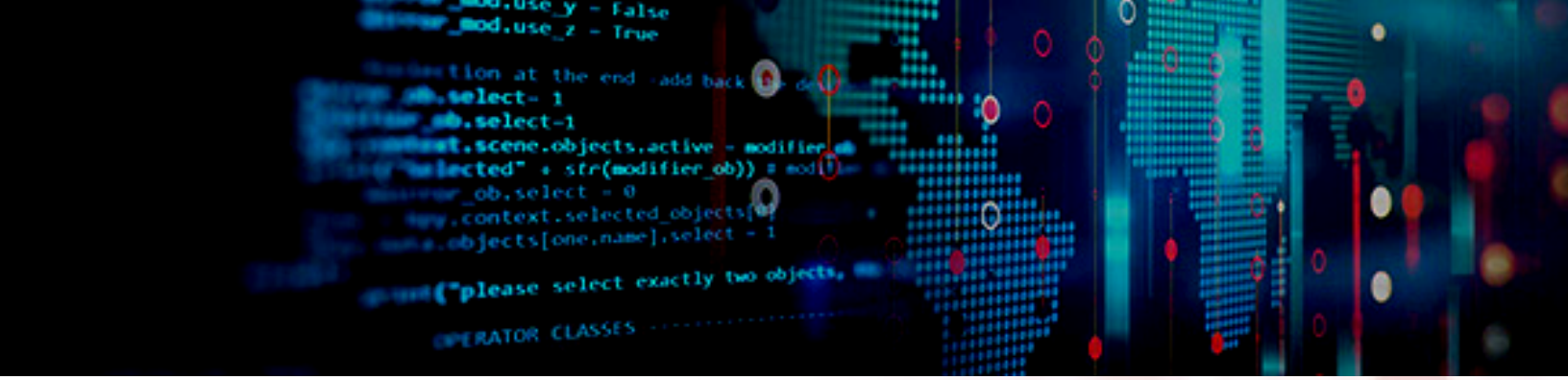


Dark Web News

Darknet Live

[Florida Man Imprisoned for Reselling Fentanyl]
[Investigating the Selective Scamming Behavior of Non-KYC Exchange FixedFloat]
[Australian Drugs Vendor AusCokeKing Busted]
[Skynet Market Admin Pleads Guilty]

Dark Web Link



Trend Micro Anti-Malware Blog

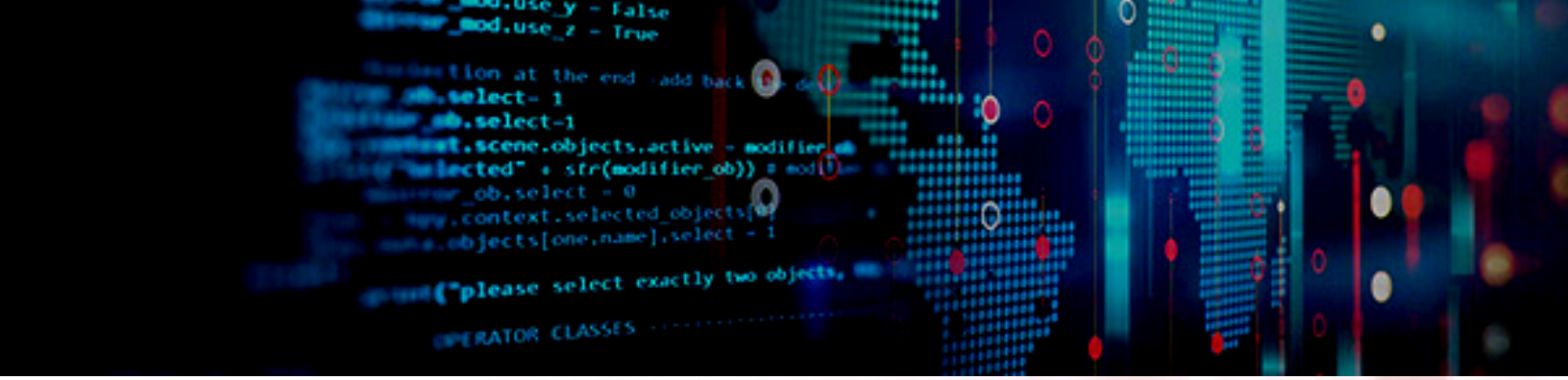
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

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

* Fetch Payloads: A Shorter Path from Command Injection to Metasploit Session
* Healthcare Orgs: Do You Need an Outsourced SOC?
* VeloCON 2023: Submissions Wanted!
* Casting a Light on Shadow IT in Cloud Environments
* 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



Advisories

US-Cert Alerts & bulletins

* CISA Adds One Known Exploited Vulnerability to Catalog
* CISA Warns of Hurricane/Typhoon-Related Scams
* CISA Releases One Industrial Control Systems Advisory
* CISA and Partners Release Cybersecurity Advisory Guidance detailing PRC state-sponsored actors evadin
* CISA and Partners Update the #StopRansomware Guide, Developed through the Joint Ransomware Task Force
* CISA Releases Four Industrial Control Systems Advisories
* CISA Adds Three Known Exploited Vulnerabilities to Catalog
* CISA Adds Three Known Exploited Vulnerabilities to Catalog
* People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection
* #StopRansomware: BianLian Ransomware Group
* Vulnerability Summary for the Week of May 15, 2023
* Vulnerability Summary for the Week of May 8, 2023

Zero Day Initiative Advisories

ZDI-CAN-21246: 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: 2023-05-26, 3 days ago. The vendor is given until 2023-09-23 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-21244: 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: 2023-05-26, 3 days ago. The vendor is given until 2023-09-23 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-21241: Adobe
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-05-26, 3 days ago. The vendor is given until 2023-09-23 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-21243: 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: 2023-05-26, 3 days ago. The vendor is given until 2023-09-23 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-21242: 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: 2023-05-26, 3 days ago. The vendor is given until 2023-09-23 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-21245: 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: 2023-05-26, 3 days ago. The vendor is given until 2023-09-23 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-21240: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-05-26, 3 days ago. The vendor is given until 2023-09-23 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-21256: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-05-26, 3 days ago. The vendor is given until 2023-09-23 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-21118: 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 'Mark Vincent Yason (@MarkYason)' was reported to the affected vendor on: 2023-05-24, 5 days ago. The vendor is given until 2023-09-21 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-21122: 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 'Mark Vincent Yason (@MarkYason)' was reported to the affected vendor on: 2023-05-24, 5 days ago. The vendor is given until 2023-09-21 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-21063: 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 'Anonymous' was reported to the affected vendor on: 2023-05-24, 5 days ago. The vendor is given until 2023-09-21 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-21103: 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 'Mark Vincent Yason (@MarkYason)' was reported to the affected vendor on: 2023-05-24, 5 days ago. The vendor is given until 2023-09-21 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-20977: Microsoft

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-05-23, 6 days ago. The vendor is given until 2023-09-20 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-21023: 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: 2023-05-23, 6 days ago. The vendor is given until 2023-09-20 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-20989: Microsoft

A CVSS score 6.4 (AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:N/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-05-23, 6 days ago. The vendor is given until 2023-09-20 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-21166: PDF-XChange

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: 2023-05-23, 6 days ago. The vendor is given until 2023-09-20 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-21060: 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: 2023-05-23, 6 days ago. The vendor is given until 2023-09-20 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-21051: Siemens

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-05-23, 6 days ago. The vendor is given until 2023-09-20 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-21225: Softing

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 'Pan ZhenPeng (@Peterpan0927) & Li JianTao (@CurseRed) of STAR Labs SG Pte. Ltd. (@starlabs_sg)' was reported to the affected vendor on: 2023-05-23, 6 days ago. The vendor is given until 2023-09-20 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-21167: Apple

A CVSS score 8.8 (AV:N/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: 2023-05-23, 6 days ago. The vendor is given until 2023-09-20 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-21121: Fuji Electric

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2023-05-23, 6 days ago. The vendor is given until 2023-09-20 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-21041: Siemens

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-05-23, 6 days ago. The vendor is given until 2023-09-20 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-21054: Siemens

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-05-23, 6 days ago. The vendor is given until 2023-09-20 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-20573: 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: 2023-05-23, 6 days ago. The vendor is given until 2023-09-20 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-6110-1

Ubuntu Security Notice 6110-1 - It was discovered that Jhead did not properly handle certain crafted Canon images when processing them. An attacker could possibly use this issue to crash Jhead, resulting in a denial of service. It was discovered that Jhead did not properly handle certain crafted images when printing Canon-specific information. An attacker could possibly use this issue to crash Jhead, resulting in a denial of service. It was discovered that Jhead did not properly handle certain crafted images when removing unknown sections. An attacker could possibly use this issue to crash Jhead, resulting in a denial of service.

Ubuntu Security Notice USN-6097-1

Ubuntu Security Notice 6097-1 - It was discovered that Linux PTP did not properly perform a length check when forwarding a PTP message between ports. A remote attacker could possibly use this issue to access sensitive information, execute arbitrary code, or cause a denial of service.

Debian Security Advisory 5415-1

Debian Linux Security Advisory 5415-1 - Two security issues were discovered in LibreOffice, which could potentially result in the execution of arbitrary code when loading a malformed spreadsheet document or unacknowledged loading of linked documents within a floating frame.

Debian Security Advisory 5412-1

Debian Linux Security Advisory 5412-1 - Several vulnerabilities were discovered in libraw, a library for reading RAW files obtained from digital photo cameras, which may result in denial of service or the execution of arbitrary code if specially crafted files are processed.

Debian Security Advisory 5414-1

Debian Linux Security Advisory 5414-1 - Jose Gomez discovered that the Catalog API endpoint in the Docker registry implementation did not sufficiently enforce limits, which could result in denial of service.

Debian Security Advisory 5411-1

Debian Linux Security Advisory 5411-1 - Multiple issues were found in GPAC multimedia framework, which could result in denial of service or potentially the execution of arbitrary code.

Ubuntu Security Notice USN-6109-1

Ubuntu Security Notice 6109-1 - 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. Jordy Zomer and Alexandra Sandulescu discovered that the Linux kernel did not properly implement speculative execution barriers in usercopy functions in certain situations. A local attacker could use this to expose sensitive information.

Debian Security Advisory 5413-1

Debian Linux Security Advisory 5413-1 - An issue has been found in sniproxy, a transparent TLS and HTTP layer 4 proxy with SNI support. Due to bad handling of wildcard backend hosts, a crafted HTTP or TLS packet might lead to remote arbitrary code execution.

Red Hat Security Advisory 2023-3326-01

Red Hat Security Advisory 2023-3326-01 - Red Hat Advanced Cluster Management for Kubernetes 2.6.6 images. This advisory contains the container images for Red Hat Advanced Cluster Management for Kubernetes, which fix several bugs.

Red Hat Security Advisory 2023-3325-01

Red Hat Security Advisory 2023-3325-01 - Multicluster Engine for Kubernetes 2.1.7 images Multicluster engine for Kubernetes provides the foundational components that are necessary for the centralized management of multiple Kubernetes-based clusters across data centers, public clouds, and private clouds. You can use the engine to create new Red Hat OpenShift Container Platform clusters or to bring existing Kubernetes-based clusters under management by importing them. After the clusters are managed, you can use the APIs that are provided by the engine to distribute configuration based on placement policy.

Red Hat Security Advisory 2023-3323-01

Red Hat Security Advisory 2023-3323-01 - Go Toolset provides the Go programming language tools and

libraries. Go is alternatively known as golang.

Ubuntu Security Notice USN-6054-2

Ubuntu Security Notice 6054-2 - USN-6054-1 fixed a vulnerability in Django. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. Moataz Al-Sharida and nawaik discovered that Django incorrectly handled uploading multiple files using one form field. A remote attacker could possibly use this issue to bypass certain validations.

Red Hat Security Advisory 2023-3319-01

Red Hat Security Advisory 2023-3319-01 - Go Toolset provides the Go programming language tools and libraries. Go is alternatively known as golang.

Ubuntu Security Notice USN-6108-1

Ubuntu Security Notice 6108-1 - It was discovered that Jhead did not properly handle certain crafted images while rotating them. An attacker could possibly use this issue to crash Jhead, resulting in a denial of service. Kyle Brown discovered that Jhead did not properly handle certain crafted images while regenerating the Exif thumbnail. An attacker could possibly use this issue to execute arbitrary commands.

Ubuntu Security Notice USN-6106-1

Ubuntu Security Notice 6106-1 - It was discovered that calamares-settings-ubuntu allowed creating the first user with a blank password, contrary to expectations.

Red Hat Security Advisory 2023-3299-01

Red Hat Security Advisory 2023-3299-01 - 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, denial of service, deserialization, improper authorization, and information leakage vulnerabilities.

Ubuntu Security Notice USN-6105-1

Ubuntu Security Notice 6105-1 - The ca-certificates package contained outdated CA certificates. This update refreshes the included certificates to those contained in the 2.60 version of the Mozilla certificate authority bundle.

Ubuntu Security Notice USN-6105-2

Ubuntu Security Notice 6105-2 - USN-6105-1 updated ca-certificates. This provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. The ca-certificates package contained outdated CA certificates. This update refreshes the included certificates to those contained in the 2.60 version of the Mozilla certificate authority bundle.

Red Hat Security Advisory 2023-3318-01

Red Hat Security Advisory 2023-3318-01 - Go Toolset provides the Go programming language tools and libraries. Go is alternatively known as golang. The golang packages provide the Go programming language compiler.

Ubuntu Security Notice USN-6100-1

Ubuntu Security Notice 6100-1 - It was discovered that HTML::StripScripts does not properly parse HTML content with certain style attributes. A remote attacker could use this issue to cause a regular expression denial of service.

Red Hat Security Advisory 2023-3296-01

Red Hat Security Advisory 2023-3296-01 - Multicluster Engine for Kubernetes 2.2.4 images Multicluster engine for Kubernetes provides the foundational components that are necessary for the centralized management of multiple Kubernetes-based clusters across data centers, public clouds, and private clouds. You can use the engine to create new Red Hat OpenShift Container Platform clusters or to bring existing Kubernetes-based clusters under management by importing them. After the clusters are managed, you can use the APIs that are provided by the engine to distribute configuration based on placement policy.

Red Hat Security Advisory 2023-3297-01

Red Hat Security Advisory 2023-3297-01 - Red Hat Advanced Cluster Management for Kubernetes 2.7.4 images Red Hat Advanced Cluster Management for Kubernetes provides the capabilities to address common

challenges that administrators and site reliability engineers face as they work across a range of public and private cloud environments. Clusters and applications are all visible and managed from a single console—with security policy built in. This advisory contains the container images for Red Hat Advanced Cluster Management for Kubernetes, which fix several bugs.

Red Hat Security Advisory 2023-3291-01

Red Hat Security Advisory 2023-3291-01 - Ruby is an extensible, interpreted, object-oriented, scripting language. It has features to process text files and to perform system management tasks. Issues addressed include HTTP response splitting and denial of service vulnerabilities.

Ubuntu Security Notice USN-6104-1

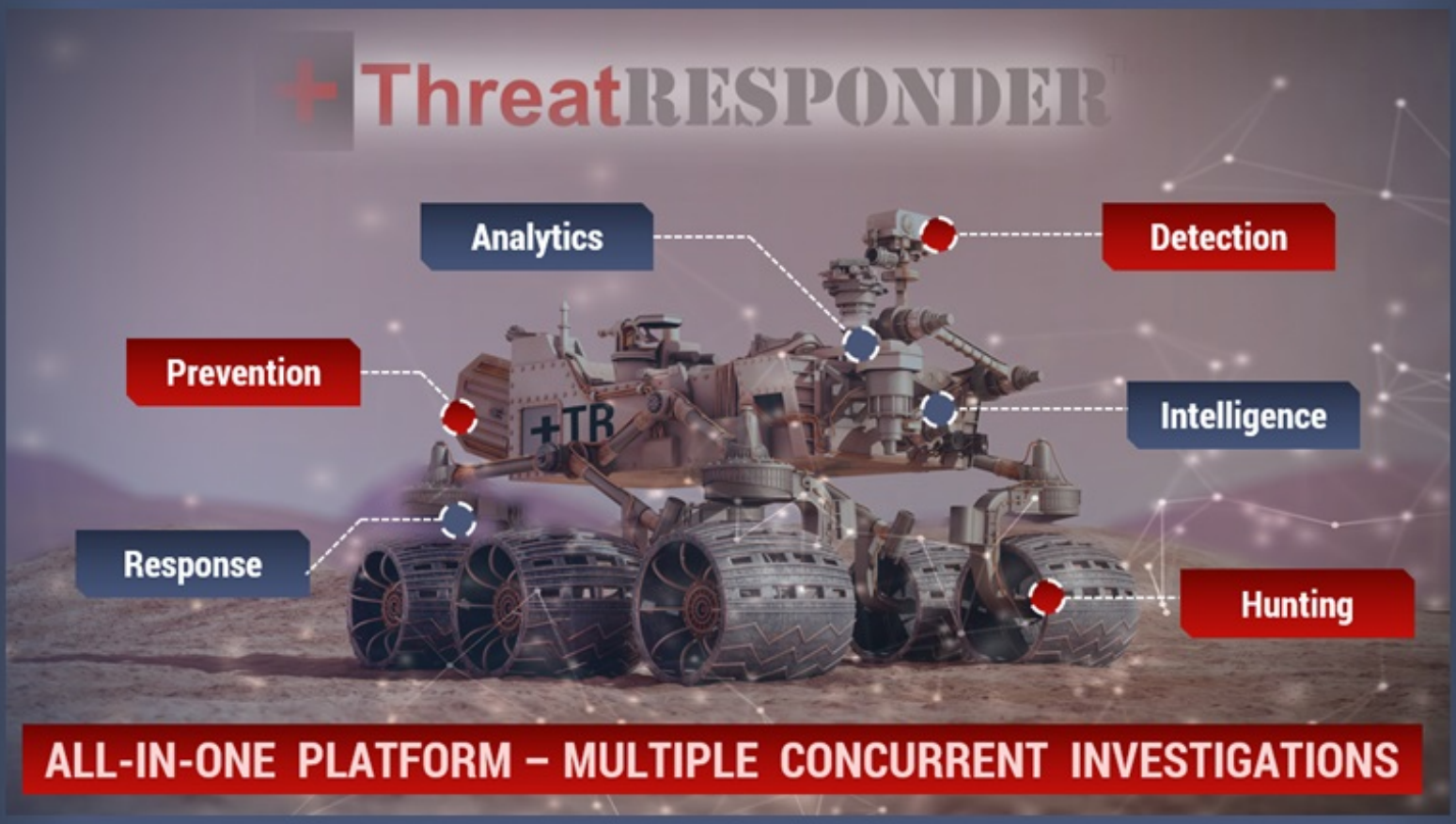
Ubuntu Security Notice 6104-1 - Alexander Lakhin discovered that PostgreSQL incorrectly handled certain CREATE privileges. An authenticated user could possibly use this issue to execute arbitrary code as the bootstrap supervisor. Wolfgang Walther discovered that PostgreSQL incorrectly handled certain row security policies. An authenticated user could possibly use this issue to complete otherwise forbidden reads and modifications.

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



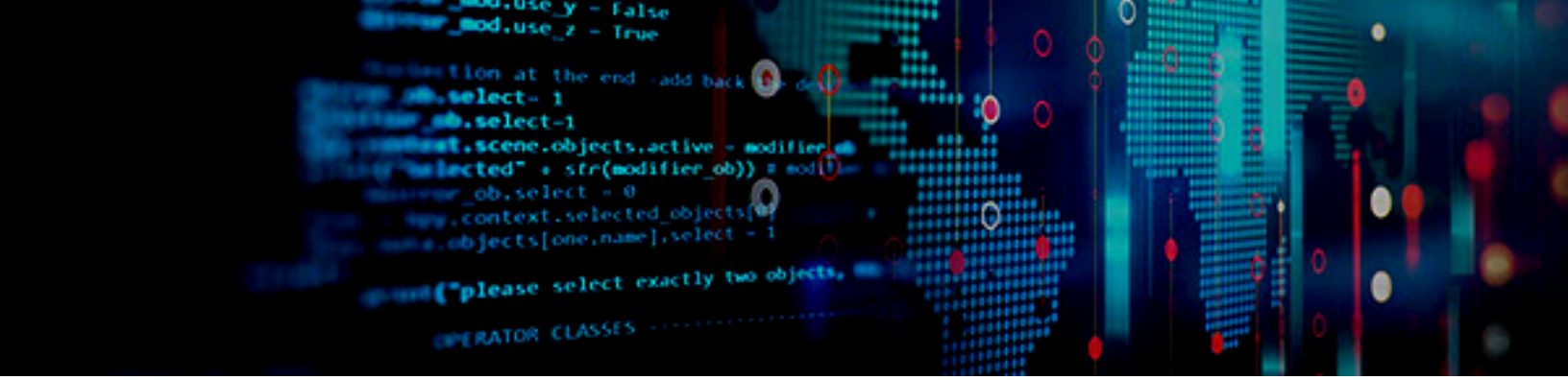
The Solution – ThreatResponder® Platform

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

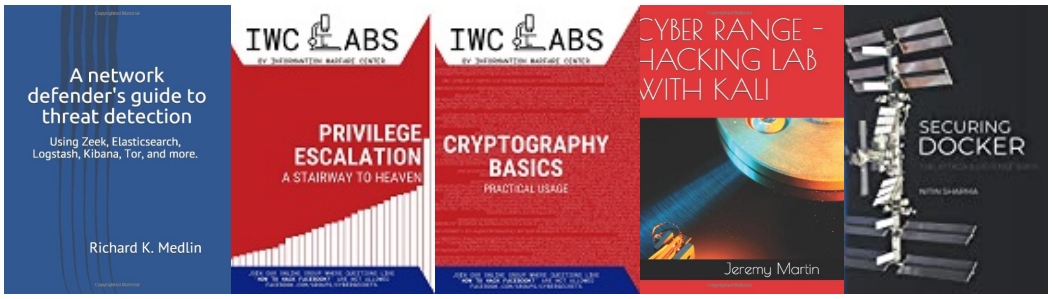


The Cyber Secrets publications on Amazon

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