Jan-16-23

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

January 16, 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

* Critical Vulnerability Gets Fortinet VPN Customers Infected
* Vulnerability With 9.8 Severity In Control Web Panel Under Active Exploit
* Meta Alleges Surveillance Firm Collected Data On 600,000 Users Via Fake Accounts
* Twitter Says Leaked Emails Not Hacked From Its Systems
* Telegram Bots Used For Credential Phishing Increased By 800% In 2022
* Guardian Confirms It Was Hit By Ransomware Attack
* Think Tank Says China Would Probably Lose If It Tries To Invade Taiwan
* FTX Recovers Over $5 Billion Of Assets
* Crypto Crime Hits Record $20 Billion In 2022, Report Says
* Hundreds Of SugarCRM Servers Infected With Critical In-The-Wild Exploit
* VALL-E AI Can Mimic A Person's Voice From A Three Second Snippet
* New FDA Authority For Medical Device Security Signals Big Changes For Manufacturers
* First Patch Tuesday Of The Year Explodes With In-The-Wild Exploit Fix
* Malicious Threat Actor Impersonating Crypto Firm On Telegram
* Health Insurer Aflac Blames US Partner For Leak Of Japanese Cancer Info
* A Fifth Of Passwords Used By Federal Agency Cracked In Security Audit
* The FBI Won't Say Whether It Hacked Dark Web ISIS Site
* Hackers Targeted Danish Central Bank Website
* Cybercriminals Are Already Using ChatGPT To Own You
* US Supremes Deny Pegasus Spyware Maker's Immunity Claim
* Researchers Could Track The GPS Location Of All Of California's New Digital License Plates
* Shareholders Ask To Revive SolarWinds Orion Breach Lawsuit
* Decryptor Released For The MegaCortex Ransomware Victims
* Russian Hackers Targeted US Nuclear Research Labs
* What Twitter's 200 Million Email Leak Really Means

Krebs on Security

* Microsoft Patch Tuesday, January 2023 Edition
* Identity Thieves Bypassed Experian Security to View Credit Reports
* Happy 13th Birthday, KrebsOnSecurity!
* The Equifax Breach Settlement Offer is Real, For Now
* Hacked Ring Cams Used to Record Swatting Victims
* Six Charged in Mass Takedown of DDoS-for-Hire Sites
* Microsoft Patch Tuesday, December 2022 Edition
* FBI's Vetted Info Sharing Network 'InfraGard' Hacked
* New Ransom Payment Schemes Target Executives, Telemedicine
* Judge Orders U.S. Lawyer in Russian Botnet Case to Pay Google

Dark Reading

* Why Mean Time to Repair Is Not Always A Useful Security Metric
* Norton LifeLock Warns on Password Manager Account Compromises
* Malware Comes Standard With This Android TV Box on Amazon
* Sneaky New Stealer Woos Corporate Workers Through Fake Zoom Downloads
* CircleCI, LastPass, Okta, and Slack: Cyberattackers Pivot to Target Core Enterprise Tools
* Cloudflare Wins CISA Contract for Registry and Authoritative Domain Name System (DNS) Services
* Fast-Track Secure Development Using Lite Threat Modeling
* WEF's Global Risks Report 2023 Keeps Cybersecurity on the Agenda
* Researchers Find 'Digital Crime Haven' While Investigating Magecart Activity
* $20K Buys Insider Access to Telegram Servers, Dark Web Ad Claims
* Software Supply Chain Security Needs a Bigger Picture
* Darktrace Publishes 2022 Cyberattack Trend Data For Energy, Healthcare & Retail Sectors Globally
* Cloudflare Expands Relationship With Microsoft
* SailPoint Acquires SecZetta to Provide Identity Security for Non-Employee Identities
* Critical Cisco SMB Router Flaw Allows Authentication Bypass, PoC Available
* Securing the World's Energy Systems: Where Physical Security and Cybersecurity Must Meet
* Big Prizes, Cash on Offer for Joining 'DDosia' Anti-Ukraine Cyberattack Project
* Kubernetes-Related Security Projects to Watch in 2023
* 1 in 3 Organizations Do Not Provide Any Cybersecurity Training to Remote Workers Despite a Majority o
* Hack the Box Secures $55 Million in Series B Funding Led by Carlyle

The Hacker News

* New Backdoor Created Using Leaked CIA's Hive Malware Discovered in the Wild
* Malware Attack on CircleCI Engineer's Laptop Leads to Recent Security Incident
* Cacti Servers Under Attack as Majority Fail to Patch Critical Vulnerability
* TikTok Fined $5.4 Million by French Regulator for Violating Cookie Laws
* Cisco Issues Warning for Unpatched Vulnerabilities in EoL Business Routers
* Beware: Tainted VPNs Being Used to Spread EyeSpy Surveillanceware
* Cybercriminals Using Polyglot Files in Malware Distribution to Fly Under the Radar
* Get Unified Cloud and Endpoint Security: Only $1 for 1,000 Assets for all of 2023!
* FortiOS Flaw Exploited as Zero-Day in Attacks on Government and Organizations
* IcedID Malware Strikes Again: Active Directory Domain Compromised in Under 24 Hours
* Over 100 Siemens PLC Models Found Vulnerable to Firmware Takeover
* Experts Detail Chromium Browser Security Flaw Putting Confidential Data at Risk
* Patch Where it Hurts: Effective Vulnerability Management in 2023
* Twitter Denies Hacking Claims, Assures Leaked User Data Not from its System
* Alert: Hackers Actively Exploiting Critical "Control Web Panel" RCE Vulnerability

Security Week

* NSA Director Pushes Congress to Renew Surveillance Powers
* Most Cacti Installations Unpatched Against Exploited Vulnerability
* Exploitation of Control Web Panel Vulnerability Starts After PoC Publication
* Juniper Networks Kicks Off 2023 With Patches for Over 200 Vulnerabilities
* Fortinet Says Recently Patched Vulnerability Exploited to Hack Governments
* Pro-Russian Group DDoS-ing Governments, Critical Infrastructure in Ukraine, NATO Countries
* Tesla Returns as Pwn2Own Hacker Takeover Target
* Twitter Finds No Evidence of Vulnerability Exploitation in Recent Data Leaks
* Cisco Warns of Critical Vulnerability in EoL Small Business Routers
* The Guardian Confirms Personal Information Compromised in Ransomware Attack
* Threema Under Fire After Downplaying Security Research
* Sophisticated 'Dark Pink' APT Targets Government, Military Organizations
* Recently Disclosed Vulnerability Exploited to Hack Hundreds of SugarCRM Servers
* Severe Vulnerabilities Allow Hacking of Asus Gaming Router
* Cyber Incident Hits UK Postal Service, Halts Overseas Mail
* Red Hat Announces General Availability of Malware Detection Service
* 'No Evidence' of Cyberattack Related to FAA Outage, White House Says
* Investors Bet Big on Subscription-Based Security Skills Training
* Chrome 109 Patches 17 Vulnerabilities
* Cybercrime Group Exploiting Old Windows Driver Vulnerability to Bypass Security Products
* British Manufacturing Firm Morgan Advanced Materials Investigating Cyberattack
* 251k Impacted by Data Breach at Insurance Firm Bay Bridge Administrators
* SAP's First Security Updates for 2023 Resolve Critical Vulnerabilities
* Unpatchable Hardware Vulnerability Allows Hacking of Siemens PLCs
* EU Tells TikTok Chief To Respect Data Privacy Laws
* Microsoft Patch Tuesday: 97 Windows Vulns, 1 Exploited Zero-Day

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* [Ache In the Head] The Problems With Your Not-So-Secure Email Gateway
* [Heads Up] Phishing Attacks Are Now The Top Vector For Ransomware Delivery
* Government Workers as Phishing Targets
* 21% of federal agency passwords cracked in their security audit
* Italian Cybercriminal Pleads Guilty to Phishing for Book Manuscripts
* Password Managers Can Be Hacked Lots of Ways and Yes, You Should Still Use Them
* CyberheistNews Vol 13 #02 [Bad Taste] There Is a New Trend in Social Engineering With a Disgusting Na
* The Good, the Bad and the Truth About Password Managers
* Phishing in the Service of Espionage
* A Look Back at Mobile Government Cyberattacks Shows Increased Attacks and Weaker Security

ISC2.org Blog

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

HackRead

* This is How to Start Your Own Cybersecurity Business
* Android TV Box Sold on Amazon Contain Malware
* Europol Busts Crypto Fraud Call Centers
* Russian Hackers Eager to Bypass OpenAI's Restrictions to Abuse ChatGPT
* 5 B2B Data Privacy Startups to Check Out in 2023
* Mikko Hypponen's opinion on the technological revolution
* Credential Stealing Flaw in Google Chrome Impacted 2.5 Billion Users

Koddos

* This is How to Start Your Own Cybersecurity Business
* Android TV Box Sold on Amazon Contain Malware
* Europol Busts Crypto Fraud Call Centers
* Russian Hackers Eager to Bypass OpenAI's Restrictions to Abuse ChatGPT
* 5 B2B Data Privacy Startups to Check Out in 2023
* Mikko Hypponen's opinion on the technological revolution
* Credential Stealing Flaw in Google Chrome Impacted 2.5 Billion Users

Naked Security

* S3 Ep117: The crypto crisis that wasn't (and farewell forever to Win 7) [Audio + Text]
* Microsoft Patch Tuesday: One 0-day; Win 7 and 8.1 get last-ever patches
* Popular JWT cloud security library patches "remote" code execution hole
* CircleCI - code-building service suffers total credential compromise
* RSA crypto cracked? Or perhaps not!
* S3 Ep116: Last straw for LastPass? Is crypto doomed? [Audio + Text]
* Serious Security: How to improve cryptography, resist supply chain attacks, and handle data breaches
* Inside a scammers' lair: Ukraine busts 40 in fake bank call-centre raid
* PyTorch: Machine Learning toolkit pwned from Christmas to New Year
* Naked Security 33 1/3 - Cybersecurity predictions for 2023 and beyond

Threat Post

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

Null-Byte

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

IBM Security Intelligence

* Why SMB Cybersecurity May Be Changing for the Better
* Now You SIEM, Now You Don't -Six Failures of Cybersecurity
* How Security Teams Combat Disinformation and Misinformation
* 6 Roles That Can Easily Transition to a Cybersecurity Team
* A View Into Web(View) Attacks in Android
* RomCom RAT Attack Analysis: Fake It to Make It
* DNSChanger and the Global Scope of Cybersecurity
* California v. Congress: Data Protection Law Showdown
* 3 Reasons to Make EDR Part of Your Incident Response Plan
* Laid Off by Big Tech? Cybersecurity is a Smart Career Move

InfoWorld

* What kind of future will AI bring enterprise IT?
* Architecting for SaaSification
* JavaScript, Java, and Python skills top demand
* Poor cloud architecture and operations are killing cloud ROI
* Lists and people on Mastodon
* Kotlin 1.8.0 adds recursive copy, delete for directories
* DataStax acquires machine learning services firm Kaskada
* Interest in React, Angular, and Vue is waning
* How to use OpenAPI in ASP.NET Core
* Using JavaScript and forms

C4ISRNET - Media for the Intelligence Age Military

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

The Hacker Corner

Conferences

* Virtual Conferences Marketing & Technology
* How To Plan an Event Marketing Strategy
* Zero Trust Cybersecurity Companies
* Types of Major Cybersecurity Threats In 2022
* The Five Biggest Trends In Cybersecurity In 2022
* The Fascinating Ineptitude Of Russian Military Communications
* Cyberwar In The Ukraine Conflict
* Our New Approach To Conference Listings
* Marketing Cybersecurity In 2023
* Cybersecurity Employment Market

Google Zero Day Project

* DER Entitlements: The (Brief) Return of the Psychic Paper
* Exploiting CVE-2022-42703 - Bringing back the stack attack

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.

* KnightCTF 2023
* Insomni'hack teaser 2023
* bi0sCTF 2022
* MHSCTF 2023 (Online)
* DiceCTF 2023
* LA CTF 2023
* HackTM CTF Quals 2023
* pbctf 2023
* hxp CTF 2022
* DaVinciCTF 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

* tcpdump 4.99.3
* I2P 2.1.0
* Zeek 5.0.5
* tcpdump 4.99.2
* GNUnet P2P Framework 0.19.2
* cryptmount Filesystem Manager 6.2.0
* American Fuzzy Lop plus plus 4.05c
* SimpleRmiDiscoverer 0.1
* Faraday 4.3.2
* SQLMAP - Automatic SQL Injection Tool 1.7

Kali Linux Tutorials

* Protecting Kubernetes Deployments with Azure Sentinel
* Reconator - Automated Recon for Pentesting & Bug Bounty
* FarsightAD : PowerShell Script That Aim To Help Uncovering (Eventual) Persistence Mechanisms
* Havoc : Modern and malleable post-exploitation command and control framework
* OFRAK : Unpack, Modify, And Repack Binaries
* Autobloody : Tool To Automatically Exploit Active Directory Privilege Escalation Paths Shown By Blood
* S3Crets Scanner : Hunting For Secrets Uploaded To Public S3 Buckets
* Pen Andro - An Automated Android Penetration Testing Tool
* ZPhisher : Automated Phishing Tool For Pentesters
* The Hackingsage/Hacktronian - A Pentesting Tool for Linux and Android

GBHackers Analysis

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

Weekly Cyber Security Video and Podcasts

SANS DFIR

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

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

* ChatGPT Malware - ThreatWire
* The Biggest Hacks of 2022! - ThreatWire
* Eufy Security Cameras Upload To The Cloud - ThreatWire

The PC Security Channel [TPSC]

* Kaspersky vs Windows Defender
* Best Virus Removal Tools: Cleaning a deeply infected system

Eli the Computer Guy

* YOUTUBE STEALING MONEY FROM CREATORS - revenue clawback in new tos
* CODERS MOST ANNOYING QUESTION
* PROGRAMMING DJANGO the WRONG WAY
* YouTube Moderation Bots are INSANE

Security Now

* 1 - LastPass Aftermath, LastPass vault de-obfuscator, LastPass iteration count folly
* Leaving LastPass - How LastPass failed, Steve's next password manager, how to protect yourself

Troy Hunt

* Weekly Update 330

Intel Techniques: The Privacy, Security, & OSINT Show

* 287-Listener Questions, UNREDACTED 5, & OSINT 10
* 286-Closing Out 2022

Proof of Concept (PoC) & Exploits

Packet Storm Security

* libCoreEntitlements CEContextQuery Arbitrary Entitlement Returns
* WebKit CSSCrossfadeValue::crossfadeChanged Use-After-Free
* Academy LMS 5.11 Cross Site Scripting
* ChiKoi New-MVC-SHOP 1.0 Cross Site Scripting
* WordPress Slider Revolution 4.x.x Shell Upload
* WordPress Slider Revolution 4.9.2 Directory Traversal
* WordPress Slider Revolution 4.6.5 Directory Traversal
* WordPress Slider Revolution 4.1.3 Directory Traversal
* WordPress Slider Revolution 4.1.2 Directory Traversal
* WordPress Slider Revolution 3.0.8 Directory Traversal
* WordPress Profile Builder 3.0.5 SQL Injection
* Global Education And Technoworld 4.1 Backup Disclosure
* Laravel 9.47.0 Information Disclosure
* eCart Web 5.0.0 Cross Site Scripting
* Online Food Ordering System 2.0 Shell Upload
* Foloosi Shopping 5.5.7 Insecure Settings
* Flex 5.22 Insecure Settings
* ChiKoi 1.0 SQL Injection
* Deprixa Pro 7.5 Insecure Settings
* Blesta 5.4.1 Insecure Settings
* 2ad Guestbook 2.0 Database Disclosure
* Online Food Ordering System 2.0 SQL Injection
* Gold Filled CRM 2.0 Arbitrary File Upload
* Windows Kernel NtNotifyChangeMultipleKeys Use-After-Free
* WordPress Royal Elementor 1.3.59 XSS / CSRF / Insufficient Access Controls

CXSecurity

* VMware vCenter vScalation Privilege Escalation
* Microsoft Exchange ProxyNotShell Remote Code Execution
* vBulletin 5.5.2 PHP Object Injection
* Remote Control Collection Remote Code Execution
* F5 BIG-IP iControl Remote Command Execution
* ChurchInfo 1.2.13-1.3.0 Remote Code Execution
* ZTE ZXHN-H108NS Stack Buffer Overflow / Denial Of Service

Proof of Concept (PoC) & Exploits

Exploit Database

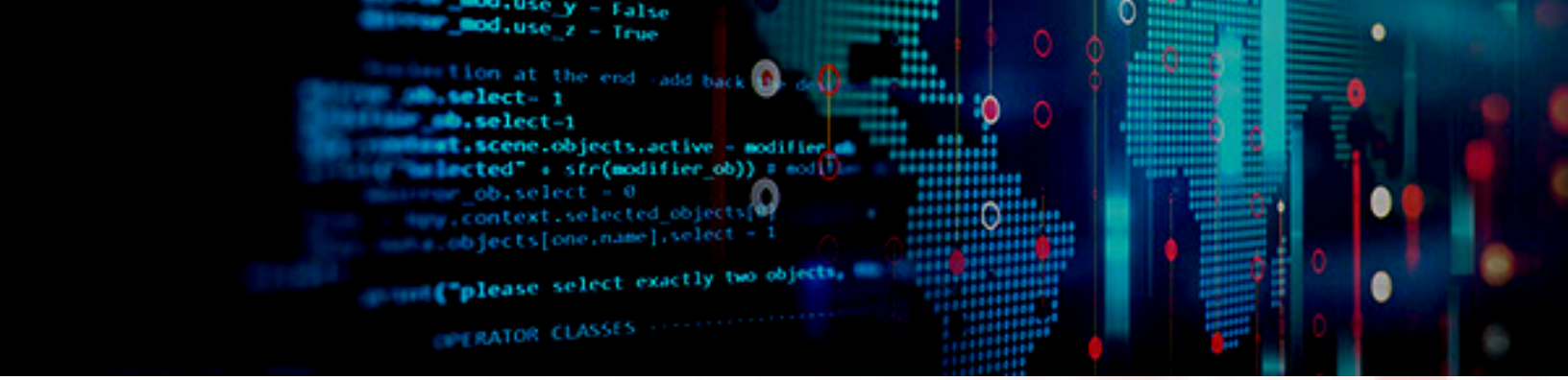
* [remote] SmartRG Router SR510n 2.6.13 - Remote Code Execution
* [webapps] CVAT 2.0 - Server Side Request Forgery
* [local] IOTransfer V4 - Unquoted Service Path
* [remote] AVEVA InTouch Access Anywhere Secure Gateway 2020 R2 - Path Traversal
* [remote] MSNSwitch Firmware MNT.2408 - Remote Code Execution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

Exploit Database for offline use

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

user@yourlinux:~$ *searchsploit keyword1 keyword2*

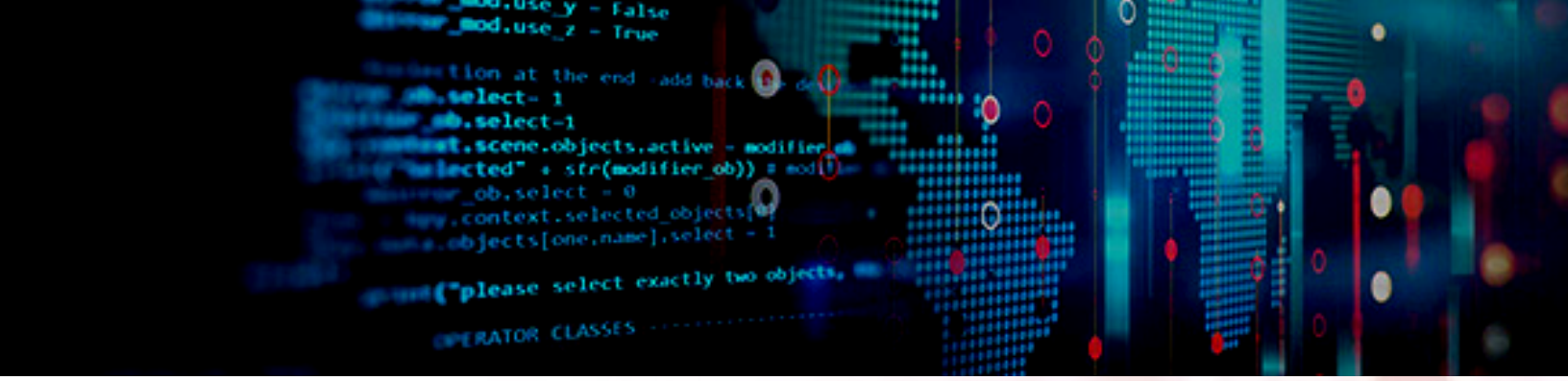
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://www.kejari-palu.go.id/ft.html
https://www.kejari-palu.go.id/ft.html notified by Indonesja Attacker
https://pttun-medan.go.id/pwn.htm
https://pttun-medan.go.id/pwn.htm notified by UnM@SK
http://dukcapil.singkawangkota.go.id/miaw.php
http://dukcapil.singkawangkota.go.id/miaw.php notified by SABUNMANDI CYBER TEAM
https://info.water.gov.my/owari.html
https://info.water.gov.my/owari.html notified by ./KeyzNet
http://dkp.surabaya.go.id/owari.html
http://dkp.surabaya.go.id/owari.html notified by ./KeyzNet
http://www.research.doae.go.th/tak_ash4.htm
http://www.research.doae.go.th/tak_ash4.htm notified by Ashiyane Digital Security Team
http://www.plan.doae.go.th/tak_ash4.htm
http://www.plan.doae.go.th/tak_ash4.htm notified by Ashiyane Digital Security Team
https://pa-karawang.go.id/pwn.htm
https://pa-karawang.go.id/pwn.htm notified by UnM@SK
https://tenders.housingandurban.go.ke/index.htm
https://tenders.housingandurban.go.ke/index.htm notified by Mc'Sl0vv
https://stakeholders.ncpd.go.ke/index.htm
https://stakeholders.ncpd.go.ke/index.htm notified by Mc'Sl0vv
https://services.icta.go.ke/index.htm
https://services.icta.go.ke/index.htm notified by Mc'Sl0vv
https://scmis.isc.go.ke/index.htm
https://scmis.isc.go.ke/index.htm notified by Mc'Sl0vv
https://sas.icta.go.ke/index.htm
https://sas.icta.go.ke/index.htm notified by Mc'Sl0vv
https://registration.connected.go.ke/index.htm
https://registration.connected.go.ke/index.htm notified by Mc'Sl0vv
https://register.icorce.go.ke/index.htm
https://register.icorce.go.ke/index.htm notified by Mc'Sl0vv
https://register.connected.go.ke/index.htm
https://register.connected.go.ke/index.htm notified by Mc'Sl0vv
https://portal.pppkenya.go.ke/index.htm
https://portal.pppkenya.go.ke/index.htm notified by Mc'Sl0vv

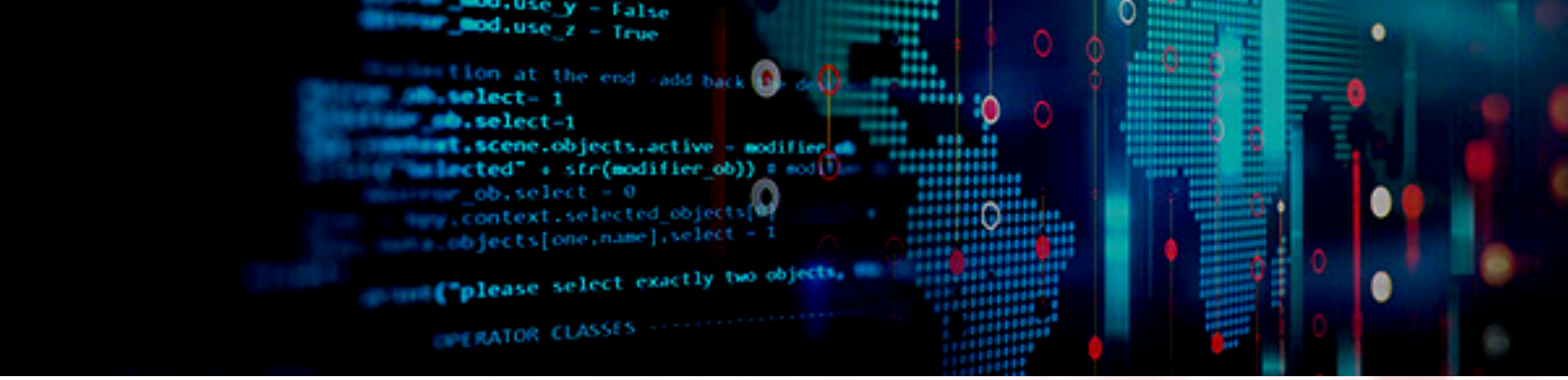


Dark Web News

Darknet Live

[French Man Sentenced to Prison for Money Laundering]
[Helix Admin's Brother Stole Seized Bitcoin]
[Virtual Private Network in Online Security and Privacy]
[Youngsters are getting into cybercrime and darknet]

Dark Web Link



Trend Micro Anti-Malware Blog

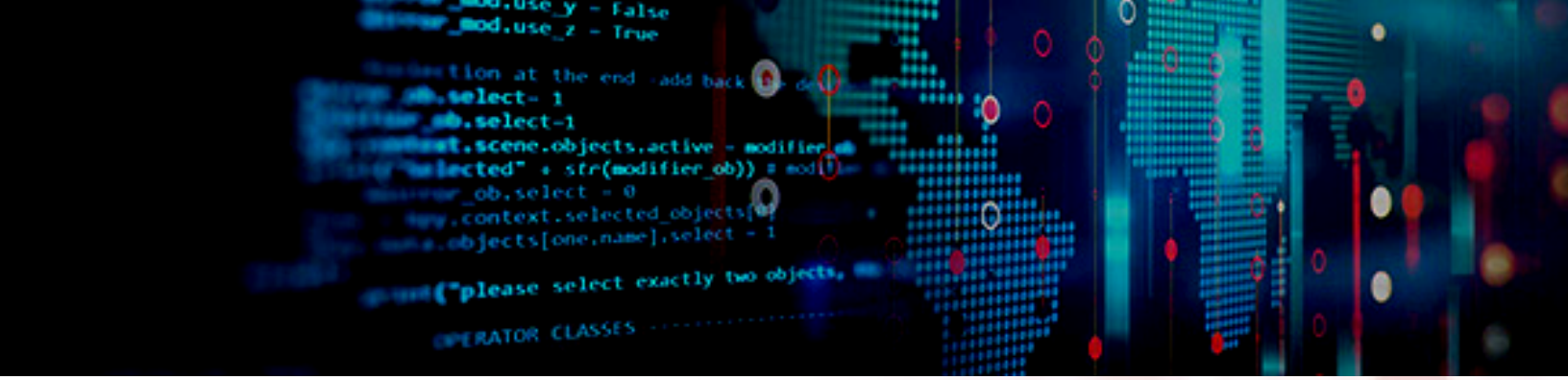
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

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
* Dated, Vulnerable, Insecure Tech Is All Over the News. Hooray.
* Recog Release v3.0.3
* Increasing The Sting of HIVE Ransomware
* Ditch The Duct Tape: Reduce Security Sprawl With XDR
* Patch Tuesday - January 2023
* Year in Review: Rapid7 Vulnerability Management
* Metasploit Weekly Wrap-Up
* Year in Review: Rapid7 Cybersecurity Research
* Rapid7 Announces Global Days Off to Support Employees in 2023



Advisories

US-Cert Alerts & bulletins

* Juniper Networks Releases Security Updates for Multiple Products
* Drupal Releases Security Update to Address Vulnerability in Private Taxonomy Terms
* CISA Releases Twelve Industrial Control Systems Advisories
* NCSC-UK Releases Guidance on Using MSP for Administering Cloud Services
* Adobe Releases Security Updates for Multiple Products
* Microsoft Releases January 2023 Security Updates
* CISA Adds Two Known Exploited Vulnerabilities to Catalog
* CISA Releases Two Industrial Control Systems Advisories
* AA22-335A: #StopRansomware: Cuba Ransomware
* AA22-321A: #StopRansomware: Hive Ransomware
* Vulnerability Summary for the Week of January 2, 2023
* Vulnerability Summary for the Week of December 26, 2022

Zero Day Initiative Advisories

ZDI-CAN-20033: ManageEngine
A CVSS score 7.2 (AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Simon Humbert of Trend Micro Security Research' was reported to the affected vendor on: 2023-01-12, 4 days ago. The vendor is given until 2023-05-12 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-20158: Autodesk
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-01-12, 4 days ago. The vendor is given until 2023-05-12 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-20157: Autodesk
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-01-12, 4 days ago. The vendor is given until 2023-05-12 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-20159: Autodesk
A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-01-12, 4 days ago. The vendor is given until 2023-05-12 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-19878: Ashlar-Vellum
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: 2023-01-11, 5 days ago. The vendor is given until 2023-05-11 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-19928: Ashlar-Vellum

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: 2023-01-11, 5 days ago. The vendor is given until 2023-05-11 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-19576: Trimble

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: 2023-01-11, 5 days ago. The vendor is given until 2023-05-11 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-19420: Schneider Electric

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2023-01-11, 5 days ago. The vendor is given until 2023-05-11 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-19879: Ashlar-Vellum

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: 2023-01-11, 5 days ago. The vendor is given until 2023-05-11 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-19956: Ashlar-Vellum

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: 2023-01-11, 5 days ago. The vendor is given until 2023-05-11 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-20046: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-01-11, 5 days ago. The vendor is given until 2023-05-11 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-19631: Trimble

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2023-01-11, 5 days ago. The vendor is given until 2023-05-11 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-19898: TP-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 'Reported by Xiaobye, working with DEVCORE Internship Program' was reported to the affected vendor on: 2023-01-11, 5 days ago. The vendor is given until 2023-05-11 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-20045: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-01-11, 5 days ago. The vendor is given until 2023-05-11 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-19876: Ashlar-Vellum

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: 2023-01-11, 5 days ago. The vendor is given until 2023-05-11 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-19226: PaperCut

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Piotr Bazydlo (@chudypb) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-01-10, 6 days ago. The vendor is given until 2023-05-10 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-18987: PaperCut

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-01-10, 6 days ago. The vendor is given until 2023-05-10 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-19598: Microsoft

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 'Team BT5 (BoB 11th)' was reported to the affected vendor on: 2023-01-10, 6 days ago. The vendor is given until 2023-05-10 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-20031: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-01-07, 9 days ago. The vendor is given until 2023-05-07 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-20035: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-01-07, 9 days ago. The vendor is given until 2023-05-07 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-19531: Schneider Electric

A CVSS score 6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2023-01-07, 9 days ago. The vendor is given until 2023-05-07 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-20036: PDF-XChange

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-01-07, 9 days ago. The vendor is given until 2023-05-07 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-20037: PDF-XChange

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-01-07, 9 days ago. The vendor is given until 2023-05-07 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-20034: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-01-07, 9 days ago. The vendor is given until 2023-05-07 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 2023-0163-01

Red Hat Security Advisory 2023-0163-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This asynchronous patch is a security update for Red Hat JBoss Enterprise Application Platform 7.4. Issues addressed include a server-side request forgery vulnerability.

Red Hat Security Advisory 2023-0163-01

Red Hat Security Advisory 2023-0163-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This asynchronous patch is a security update for Red Hat JBoss Enterprise Application Platform 7.4. Issues addressed include a server-side request forgery vulnerability.

Ubuntu Security Notice USN-5803-1

Ubuntu Security Notice 5803-1 - Kyle Zeng discovered that the sysctl implementation in the Linux kernel contained a stack-based buffer overflow. A local attacker could use this to cause a denial of service or execute arbitrary code. Tamas Koczka discovered that the Bluetooth L2CAP handshake implementation in the Linux kernel contained multiple use-after-free vulnerabilities. A physically proximate attacker could use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5801-1

Ubuntu Security Notice 5801-1 - It was discovered that Vim makes illegal memory calls when pasting brackets in Ex mode. An attacker could possibly use this to crash Vim, access or modify memory, or execute arbitrary commands. This issue affected only Ubuntu 20.04 and 22.04 It was discovered that Vim makes illegal memory calls when making certain retab calls. An attacker could possibly use this to crash Vim, access or modify memory, or execute arbitrary commands.

Ubuntu Security Notice USN-5802-1

Ubuntu Security Notice 5802-1 - It was discovered that the NFSD implementation in the Linux kernel did not properly handle some RPC messages, leading to a buffer overflow. A remote attacker could use this to cause a denial of service or possibly execute arbitrary code. Tamás Koczka discovered that the Bluetooth L2CAP handshake implementation in the Linux kernel contained multiple use-after-free vulnerabilities. A physically proximate attacker could use this to cause a denial of service or possibly execute arbitrary code.

Red Hat Security Advisory 2023-0164-01

Red Hat Security Advisory 2023-0164-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This asynchronous patch is a security update for Red Hat JBoss Enterprise Application Platform 7.4. Issues addressed include a server-side request forgery vulnerability.

Red Hat Security Advisory 2023-0017-01

Red Hat Security Advisory 2023-0017-01 - 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 4.8.56. Issues addressed include bypass, cross site request forgery, cross site scripting, denial of service, and man-in-the-middle vulnerabilities.

Ubuntu Security Notice USN-5800-1

Ubuntu Security Notice 5800-1 - It was discovered that Heimdal incorrectly handled certain SPNEGO tokens. A remote attacker could possibly use this issue to cause a denial of service. Evgeny Legerov discovered that Heimdal incorrectly handled memory when performing certain DES decryption operations. A remote attacker could use this issue to cause a denial of service, or possibly execute arbitrary code.

Red Hat Security Advisory 2023-0160-01

Red Hat Security Advisory 2023-0160-01 - PostgreSQL is an advanced object-relational database management system.

Debian Security Advisory 5316-1

Debian Linux Security Advisory 5316-1 - Several out-of-memory, stack overflow or HTTP request smuggling

vulnerabilities have been discovered in Netty, a Java NIO client/server socket framework, which may allow attackers to cause a denial of service or bypass restrictions when used as a proxy.

Red Hat Security Advisory 2023-0114-01

Red Hat Security Advisory 2023-0114-01 - The kernel-rt packages provide the Real Time Linux Kernel, which enables fine-tuning for systems with extremely high determinism requirements.

Red Hat Security Advisory 2023-0110-01

Red Hat Security Advisory 2023-0110-01 - SQLite is a C library that implements an SQL database engine. A large subset of SQL92 is supported. A complete database is stored in a single disk file. The API is designed for convenience and ease of use. Applications that link against SQLite can enjoy the power and flexibility of an SQL database without the administrative hassles of supporting a separate database server.

Debian Security Advisory 5315-1

Debian Linux Security Advisory 5315-1 - XStream serializes Java objects to XML and back again. Versions prior to 1.4.15-3+deb11u2 may allow a remote attacker to terminate the application with a stack overflow error, resulting in a denial of service only via manipulation of the processed input stream. The attack uses the hash code implementation for collections and maps to force recursive hash calculation causing a stack overflow. This update handles the stack overflow and raises an InputManipulationException instead.

Red Hat Security Advisory 2023-0123-01

Red Hat Security Advisory 2023-0123-01 - This is a kernel live patch module which is automatically loaded by the RPM post-install script to modify the code of a running kernel.

Red Hat Security Advisory 2023-0128-01

Red Hat Security Advisory 2023-0128-01 - IBM Java SE version 8 includes the IBM Java Runtime Environment and the IBM Java Software Development Kit. This update upgrades IBM Java SE 8 to version 8 SR7-FP20. Issues addressed include a randomization vulnerability.

Red Hat Security Advisory 2023-0113-01

Red Hat Security Advisory 2023-0113-01 - PostgreSQL is an advanced object-relational database management system.

Red Hat Security Advisory 2023-0100-01

Red Hat Security Advisory 2023-0100-01 - The systemd packages contain systemd, a system and service manager for Linux, compatible with the SysV and LSB init scripts. It provides aggressive parallelism capabilities, uses socket and D-Bus activation for starting services, offers on-demand starting of daemons, and keeps track of processes using Linux cgroups.

Red Hat Security Advisory 2023-0116-01

Red Hat Security Advisory 2023-0116-01 - A library that provides Abstract Syntax Notation One parsing and structures management, and Distinguished Encoding Rules encoding and decoding functions.

Red Hat Security Advisory 2023-0099-01

Red Hat Security Advisory 2023-0099-01 - Kernel-based Virtual Machine offers a full virtualization solution for Linux on numerous hardware platforms. The virt:rhel module contains packages which provide user-space components used to run virtual machines using KVM. The packages also provide APIs for managing and interacting with the virtualized systems. Issues addressed include an out of bounds read vulnerability.

Red Hat Security Advisory 2023-0101-01

Red Hat Security Advisory 2023-0101-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system.

Red Hat Security Advisory 2023-0103-01

Red Hat Security Advisory 2023-0103-01 - Expat is a C library for parsing XML documents. Issues addressed include a use-after-free vulnerability.

Debian Security Advisory 5314-1

Debian Linux Security Advisory 5314-1 - It was discovered that missing input sanitising in the ctags functionality of Emacs may result in the execution of arbitrary shell commands.

Red Hat Security Advisory 2023-0089-01

Red Hat Security Advisory 2023-0089-01 - LibreOffice is an open source, community-developed office productivity suite. It includes key desktop applications, such as a word processor, a spreadsheet, a presentation manager, a formula editor, and a drawing program. LibreOffice replaces OpenOffice and provides a similar but enhanced and extended office suite. Issues addressed include a script execution vulnerability.

Red Hat Security Advisory 2023-0095-01

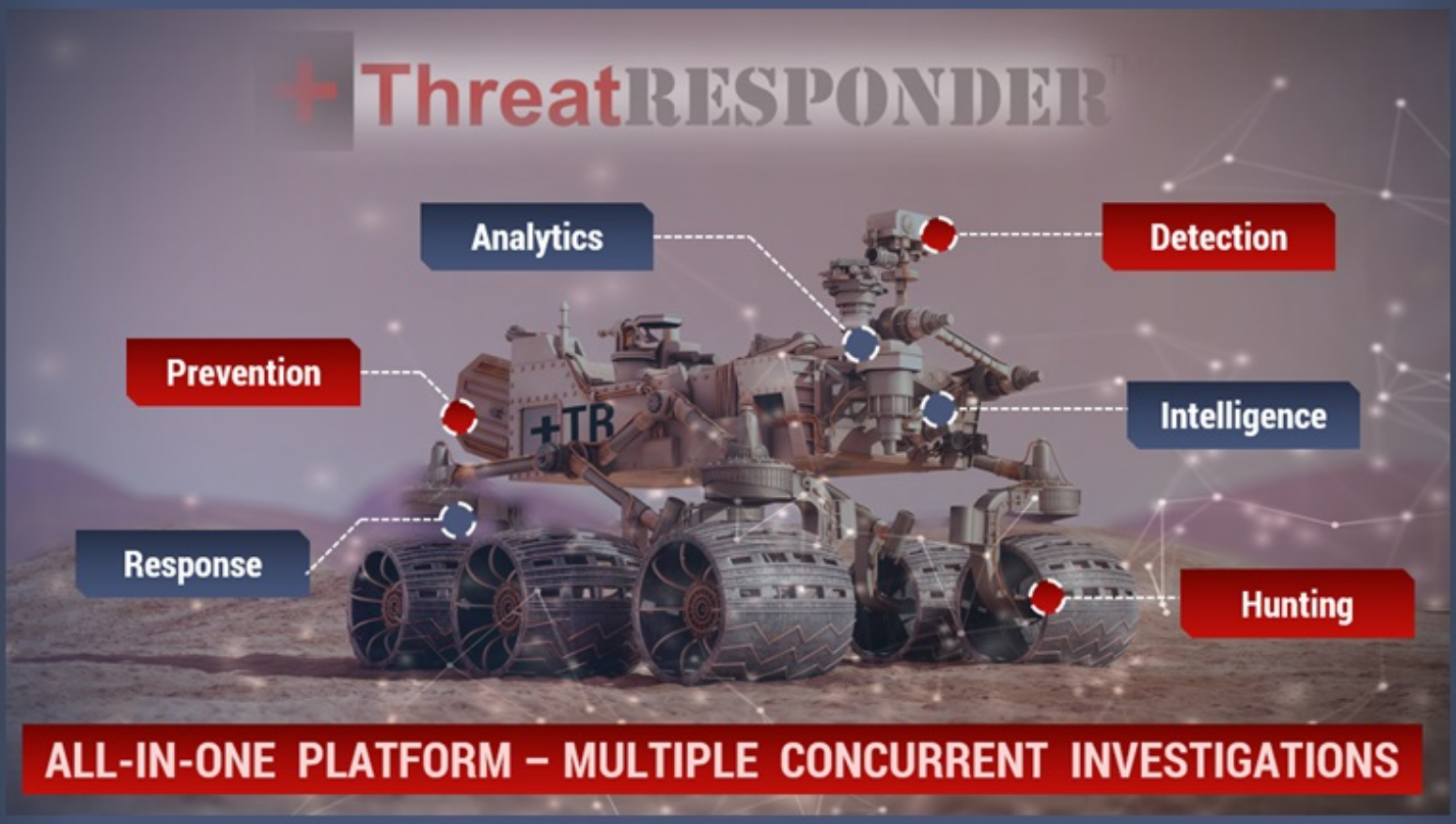
Red Hat Security Advisory 2023-0095-01 - The libtiff packages contain a library of functions for manipulating Tagged Image File Format files. Issues addressed include buffer overflow, denial of service, double free, and out of bounds read vulnerabilities.

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



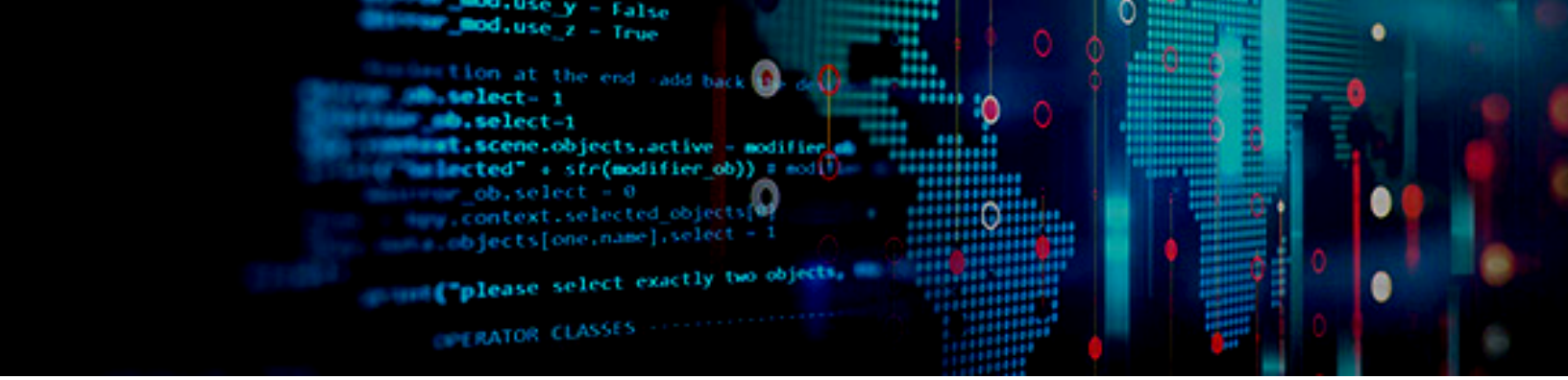
The Solution – ThreatResponder® Platform

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

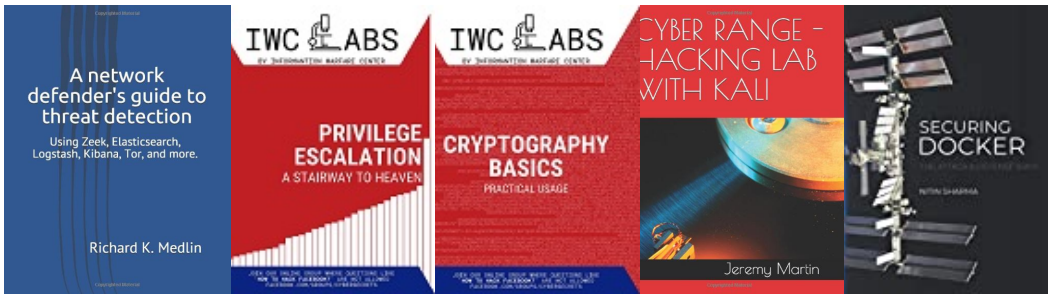


The Cyber Secrets publications on Amazon

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