Jan-09-23

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 9, 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

* Rackspace Blames Ransomware Woes On Zero-Day Attack
* User Data For 200 Million Twitter Users Just Went Up For Sale
* Saudi Arabia Jails Two Wikipedia Staff In Bid To Control Content
* US Bank Silvergate Hit With $8bn In Crypto Withdrawals
* First LastPass, Now Slack And CircleCI. The Hacks Go On And Will Likely Worsen
* Qualcomm, Lenovo Flag Multiple High Impact Firmware Vulnerabilities
* Meta Fined About $400 Million Over Use Of Data For Targeted Ads
* Ex-GE Engineer Gets Two Years In Prison After Stealing Turbine Tech For China
* Hundreds Of WordPress Sites Infected By Recently Discovered Backdoor
* PyTorch Dependency Poisoned With Malicious Code
* US Regulators Warn Banks Over Cryptocurrency Risks
* Scripps, Avalon Reach Settlements After Data Breaches
* Google Gets Off Easy In Location Tracking Lawsuits
* Bankman-Fried Set To Enter Not Guilty Plea In FTX Fraud Case
* Google Home Speakers Were Vulnerable To Eavesdropping Hackers
* Russia Launches Massive Missile Strike Against Ukraine
* North Korean Hacking Outfit Impersonates Venture Capital Firms
* Crypto Exchange Kraken To Stop Operations In Japan
* Cybersecurity Firm Links Piers Morgan Twitter Hack To Leak Of 400m Records
* US House Bans TikTok On Their Smartphones
* Military Device With Biometric Database Of 2K People Sold On eBay For $68
* TikTok Admits Using Its App To Spy On Reporters
* Crooks Copy Source Code From Okta's GitHub Repository
* J. Robert Oppenheimer Cleared Of "Black Mark" Against His Name After 68 Years
* Microsoft Fined $64 Million By France Over Cookies Used In Bing Searches

Krebs on Security

* 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
* ConnectWise Quietly Patches Flaw That Helps Phishers
* U.S. Govt. Apps Bundled Russian Code With Ties to Mobile Malware Developer

Dark Reading

* In Memoriam: Remembering Those Who Passed
* Russia-Linked Turla APT Sneakily Co-Opts Ancient Andromeda USB Infections
* Vice Society Releases Info Stolen From 14 UK Schools, Including Passport Scans
* CISOs Are Focused on These 3 Trends. Are You?
* PurpleUrchin Gang Embraces DevOps in Massive Cloud Malware Campaign
* From Ferrari to Ford, Cybersecurity Bugs Plague Automotive Safety
* Don't Be Blindsided by Software Bills of Materials
* ChatGPT Artificial Intelligence: An Upcoming Cybersecurity Threat?
* Rackspace Sunsets Email Service Downed in Ransomware Attack
* How Confidential Computing Can Change Cybersecurity
* 200M Twitter Profiles, With Email Addys, Dumped on Dark Web for Free
* LogRhythm Enhances Security Analytics With Expanded Security Operations Capabilities
* New Survey: 1 In 4 Schools Were Victims Of Cyber Attacks In the Last Year; Administrators To Increase
* Check Point Research Reports a 38% Increase In 2022 Global Cyberattacks
* CircleCI: Rotate Stored Secrets ASAP
* Bluebottle Continues Bank Heist Assault With Signed Malware
* Threat Actors Evade Detection Through Geofencing & Fingerprinting
* Maternal & Family Health Services Issues Notice Of Cybersecurity Incident
* DirectTrust and EHNAC Announce Closing Of Merger
* US Based ICOIN Technology Announces Secure Messaging Solution Using Hardware Wallet Encryption

The Hacker News

* Malicious PyPI Packages Using Cloudflare Tunnels to Sneak Through Firewalls
* Top SaaS Cybersecurity Threats in 2023: Are You Ready?
* Hackers Can Abuse Visual Studio Marketplace to Target Developers with Malicious Extensions
* Russian Turla Hackers Hijack Decade-Old Malware Infrastructure to Deploy New Backdoors
* Hackers Using CAPTCHA Bypass Tactics in Freejacking Campaign on GitHub
* Microsoft Reveals Tactics Used by 4 Ransomware Families Targeting macOS
* Dridex Malware Now Attacking macOS Systems with Novel Infection Method
* Rackspace Confirms Play Ransomware Gang Responsible for Recent Breach
* WhatsApp Introduces Proxy Support to Help Users Bypass Internet Censorship
* Blind Eagle Hackers Return with Refined Tools and Sophisticated Infection Chain
* Bluebottle Cybercrime Group Preys on Financial Sector in French-Speaking African Nations
* SpyNote Strikes Again: Android Spyware Targeting Financial Institutions
* Mitigate the LastPass Attack Surface in Your Environment with this Free Tool
* CircleCI Urges Customers to Rotate Secrets Following Security Incident
* The Evolving Tactics of Vidar Stealer: From Phishing Emails to Social Media

Security Week

* XDR and the Age-old Problem of Alert Fatigue
* Many of 13 New Mac Malware Families Discovered in 2022 Linked to China
* SASE Company Netskope Raises $401 Million
* Russian Turla Cyberspies Leveraged Other Hackers' USB-Delivered Malware
* User Documents Overwritten With Malicious Code in Recent Dridex Attacks on macOS
* Ransomware Hit 200 US Gov, Education and Healthcare Organizations in 2022
* Qualcomm UEFI Flaws Expose Microsoft, Lenovo, Samsung Devices to Attacks
* Rackspace Completes Investigation Into Ransomware Attack
* France Regulator Raps Apple Over App Store Ads
* More Political Storms for TikTok After US Government Ban
* Predictions 2023: Big Tech's Coming Security Shopping Spree
* Zoho Urges ManageEngine Users to Patch Serious SQL Injection Vulnerability
* 16 Car Makers and Their Vehicles Hacked via Telematics, APIs, Infrastructure
* Burger Chain Five Guys Discloses Data Breach Impacting Job Applicants
* Slack Says Hackers Stole Private Source Code Repositories
* Database Containing 235 Million Twitter User Records Available for Free
* Play Ransomware Group Used New Exploitation Method in Rackspace Attack
* Meta Hit With 390 Million Euro Fine Over EU Data Breaches
* Android's First Security Updates for 2023 Patch 60 Vulnerabilities
* Virtual Insanity: Protecting the Immersive Online World
* NIST Finalizes Cybersecurity Guidance for Ground Segment of Space Operations
* Rail Company Wabtec Says Data Stolen in Ransomware Attack
* High-Severity Command Injection Flaws Found in Fortinet's FortiTester, FortiADC
* Hacker Selling Data Allegedly Stolen From Volvo Cars Following Ransomware Attack
* Researcher Says Google Paid $100k Bug Bounty for Smart Speaker Vulnerabilities
* The Impact of Geopolitics on CPS Security

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* A Look Back at Mobile Government Cyberattacks Shows Increased Attacks and Weaker Security
* Ransomware and Fraudulent Funds Transfer are the Two Main Drivers of Cyber Loss
* New Crypto Scam Targets Flipper Zero Buyers Impersonating Legitimate Shops
* Phishing Campaigns Impersonate the UK Government
* These grim figures show that the ransomware problem isn't going away
* [Live Demo] Ridiculously Easy Security Awareness Training and Phishing
* CyberheistNews Vol 13 #01 [Heads Up] Giant LastPass Breach Can Supercharge Spear Phishing Attacks
* Using AI Large Language Models to Craft Phishing Campaigns
* There is a New Trend in Social Engineering with a Disgusting Name; "Pig-butchering"
* Finance and Insurance Is the Sector Most Impacted by Data Breaches In 2022

ISC2.org Blog

* Latest Cyberthreats and Advisories - January 6, 2023
* (ISC)² New Jersey Chapter Hosts International Event with 500 Attendees
* CISSP-ISSAPs - We Need Your Input
* Policy Brief - U.S. Cyber Threat Intelligence, Part 2: Summary, Recommendations & Challenges
* Latest Cyberthreats and Advisories - December 23, 2022

HackRead

* The Importance of Data Security for Digital Signage
* Russian Hackers Targeted Three US Nuclear Research Labs
* Hackers Exploiting OpenAI's ChatGPT to Deploy Malware
* Twitter Scraping Breach: 209 Million Accounts Leaked on Hacker Forum
* Chip Vulnerabilities Impacting Microsoft, Lenovo, and Samsung Devices
* Preventing Insider Attacks on Your HR System
* Top ERP Firm Exposing Half a Million Indian Job Seekers Data

Koddos

* The Importance of Data Security for Digital Signage
* Russian Hackers Targeted Three US Nuclear Research Labs
* Hackers Exploiting OpenAI's ChatGPT to Deploy Malware
* Twitter Scraping Breach: 209 Million Accounts Leaked on Hacker Forum
* Chip Vulnerabilities Impacting Microsoft, Lenovo, and Samsung Devices
* Preventing Insider Attacks on Your HR System
* Top ERP Firm Exposing Half a Million Indian Job Seekers Data

Naked Security

* 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
* US passes the Quantum Computing Cybersecurity Preparedness Act - and why not?
* The horror! The horror! NOTEPAD gets tabbed editing (very briefly)
* S3 Ep115: True crime stories - A day in the life of a cybercrime fighter [Audio + Text]
* Twitter data of "+400 million unique users" up for sale - what to do?

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

* 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
* A Perfect Storm: 7 Reasons Global Attacks Will Soar in 2023
* How Can the White House's New IoT Labels Improve Security?
* Outrageous Stories From Three Cyber Incident Responders
* The 13 Costliest Cyberattacks of 2022: Looking Back
* Twitter is the New Poster Child for Failing at Compliance
* The Most Prolific Ransomware Gangs of 2022
* How the CCPA is Shaping Other State's Data Privacy

InfoWorld

* Microsoft previews Graph API proxy for developers
* C++ wins programming language of the year award
* A Bloomberg terminal for Mastodon
* Did AI blow up your cloud bill?
* What is Cython? Python at the speed of C
* Snowflake to acquire Myst AI to provide time series forecasting
* Vue 3.3 to support externally imported types
* How to use the null object pattern in .NET
* Intro to SvelteKit 1.0: The full stack framework for Svelte
* SpiderLightning: Making WebAssembly cloud applications portable

C4ISRNET - Media for the Intelligence Age Military

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

The Hacker Corner

Conferences

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

Google Zero Day Project

* Exploiting CVE-2022-42703 - Bringing back the stack attack
* Mind the Gap

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.

* idekCTF 2022*
* Hack a Bit (Qualifier)
* Ugra CTF Quals 2023
* KnightCTF 2023
* Insomni'hack teaser 2023
* bi0sCTF 2022
* DiceCTF 2023
* LA CTF 2023
* HackTM CTF Quals 2023
* pbctf 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

* American Fuzzy Lop plus plus 4.05c
* SimpleRmiDiscoverer 0.1
* Faraday 4.3.2
* SQLMAP - Automatic SQL Injection Tool 1.7
* ModSecurity Backdoor Tool
* GNUnet P2P Framework 0.19.1
* Scapy Packet Manipulation Tool 2.5.0
* GRAudit Grep Auditing Tool 3.5
* cryptmount Filesystem Manager 6.1.1
* GNU Privacy Guard 2.4.0

Kali Linux Tutorials

* 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
* Juicy Potato : A Sugared Version Of RottenPotatoNG, With A Bit Of Juice
* NetLlix : Tool To Emulate & Test Exfiltration Of Data Over Different Network Protocols
* Squarephish : OAuth Device Code Authentication Flow & QR codes

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

* Memory Forensics At A Scale
* Cyber Threat Intelligence Summit and Training 2023
* SANS Threat Analysis Rundown
* SANS Threat Analysis Rundown (STAR)

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

* The Biggest Hacks of 2022! - ThreatWire
* Eufy Security Cameras Upload To The Cloud - ThreatWire
* 2022 Hak5 Payload Awards

The PC Security Channel [TPSC]

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

Eli the Computer Guy

* YouTube Moderation Bots are INSANE
* PYTHON is THE BEST CODING LANGUAGE
* 2023 New Years Resolution
* Why Technology Education is HARD

Security Now

* Leaving LastPass - How LastPass failed, Steve's next password manager, how to protect yourself
* Security Now Best of 2022

Troy Hunt

* Weekly Update 329

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

* Linux videobuf2 Use-After-Free
* Oracle Database Vault Metadata Exposure
* Linear eMerge E3-Series Access Controller Command Injection
* Nexxt Router Firmware 42.103.1.5095 Remote Code Execution
* Oracle DBMS_REDACT Dynamic Data Masking Bypass
* Linux PT_SUSPEND_SECCOMP Permission Bypass / Ptracer Death Race
* Packet Storm New Exploits For 2022
* Packet Storm New Exploits For December, 2022
* Chrome Synchronous Mojo Use-After-Free
* crewjam/saml Signature Bypass
* Oracle Unified Audit Policy Bypass
* SugarCRM Shell Upload
* BDWeb-Link LMS 1.11.5 SQL Injection
* Hughes Satellite Router Remote File Inclusion Cross Frame Scripting
* ProLink PRS1841 Backdoor Account
* Enlightenment 0.25.3 Privilege Escalation
* Courier Deprixa 2.5 Backdoor Account
* Consultine Consulting Business And Finance Website CMS 1.8 Backdoor Account
* Car Dealer Pro 2.01 Backdoor Account
* Botble 5.28.3 Backdoor Account
* Active Ecommerce CMS 6.4.0 Backdoor Account
* Student Attendance Management System 1.0 SQL Injection
* ProLink PRS1841 PLDT Router Backdoor
* OpenTSDB 2.4.0 Command Injection
* WordPress Yith WooCommerce Gift Cards Premium 3.19.0 Shell Upload

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

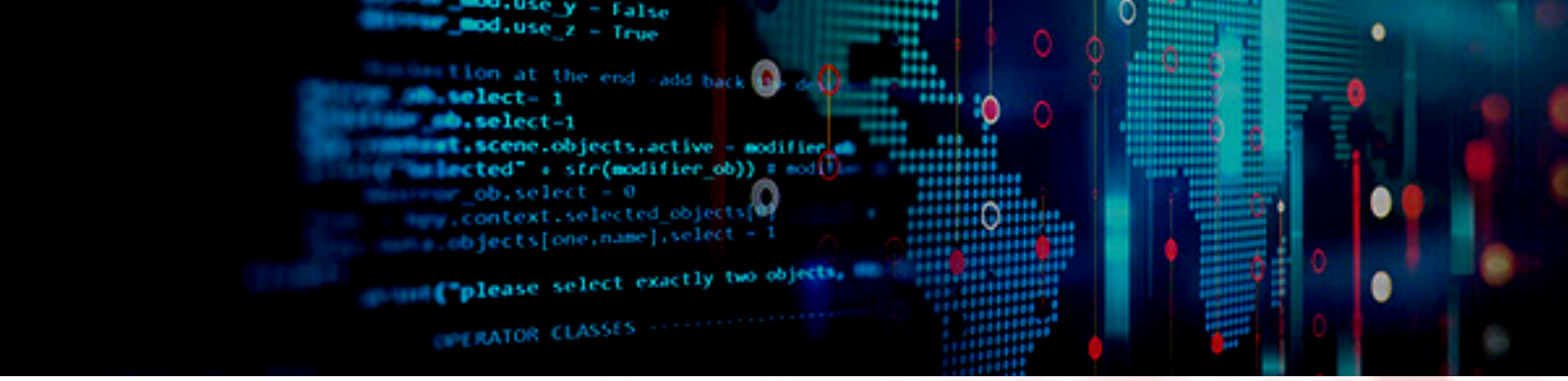
* [remote] SmartRG Router SR510n 2.6.13 - Remote Code Execution
* [webapps] CVAT 2.0 - Server Side Request Forgery
* [local] IOTransfer V4 - Unquoted Service Path
* [remote] AVEVA InTouch Access Anywhere Secure Gateway 2020 R2 - Path Traversal
* [remote] MSNSwitch Firmware MNT.2408 - Remote Code Execution
* [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*

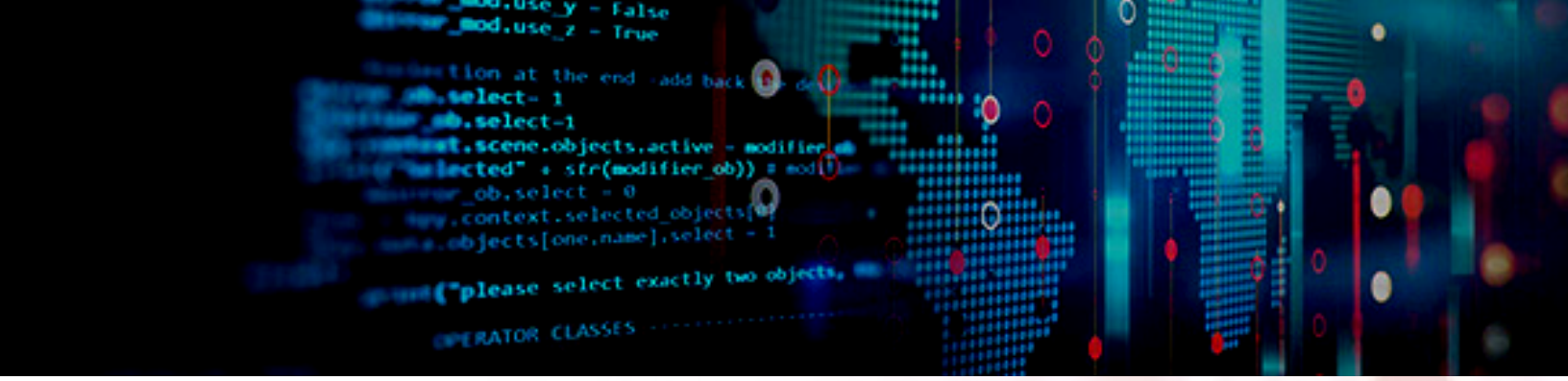
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://aguai.sp.gov.br/x7.htm
https://aguai.sp.gov.br/x7.htm notified by x7root
https://bkdd.enrekangkab.go.id/x7.htm
https://bkdd.enrekangkab.go.id/x7.htm notified by x7root
https://yms.gov.ye/Taih.php
https://yms.gov.ye/Taih.php notified by X
https://catr.gov.eg
https://catr.gov.eg notified by Restart
https://pta-samarinda.go.id
https://pta-samarinda.go.id notified by SABUNMANDI CYBER TEAM
https://coop.gov.lk/pwn.php
https://coop.gov.lk/pwn.php notified by F4st~03
https://gobiernoparroquialsancristobal.gob.ec/kurd.html
https://gobiernoparroquialsancristobal.gob.ec/kurd.html notified by 0x1998
https://gadbellavista.gob.ec/kurd.html
https://gadbellavista.gob.ec/kurd.html notified by 0x1998
https://11denoviembre.gob.ec/kurd.html
https://11denoviembre.gob.ec/kurd.html notified by 0x1998
https://gadchontaduro.gob.ec/kurd.html
https://gadchontaduro.gob.ec/kurd.html notified by 0x1998
https://gadsantamarthadecuba.gob.ec/kurd.html
https://gadsantamarthadecuba.gob.ec/kurd.html notified by 0x1998
https://www.adnap.gov.mz/tr.html
https://www.adnap.gov.mz/tr.html notified by LuXas
https://www.mgcas.gov.mz/tr.html
https://www.mgcas.gov.mz/tr.html notified by LuXas
https://www.idepa.gov.mz/tr.html
https://www.idepa.gov.mz/tr.html notified by LuXas
https://igreme.gov.mz/b.htm
https://igreme.gov.mz/b.htm notified by Mr. BDKR28
https://ifpelac.gov.mz/b.htm
https://ifpelac.gov.mz/b.htm notified by Mr. BDKR28
https://porteirinha.mg.gov.br/fake.php
https://porteirinha.mg.gov.br/fake.php notified by F4k3-ScR!pT (Bangladeshi Hacker)

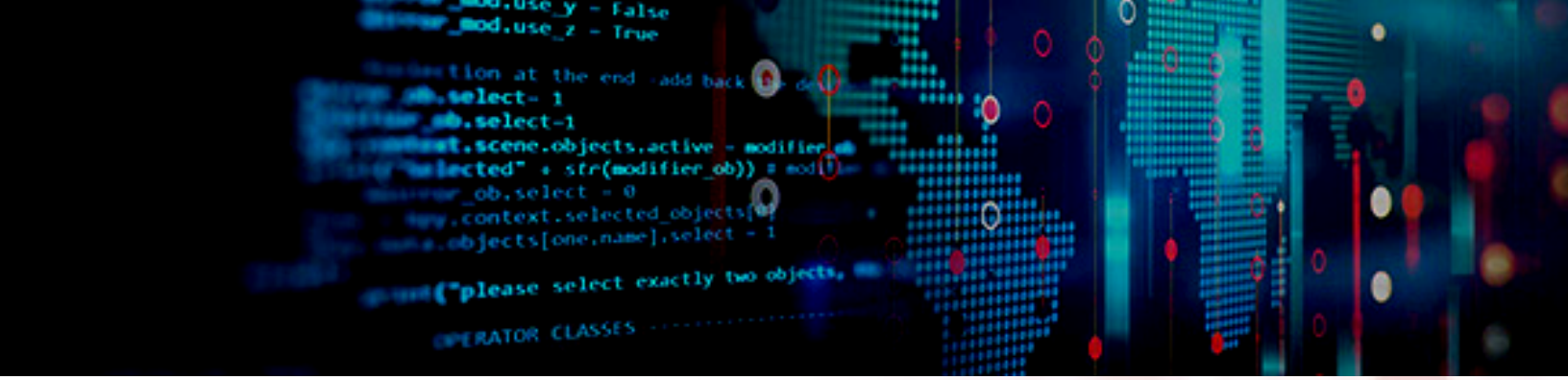


Dark Web News

Darknet Live

[Virtual Private Network in Online Security and Privacy]
[Youngsters are getting into cybercrime and darknet]
[Dark Web Child Abuse Sites Dismantled]
[I2P - The Invisible Internet Project]

Dark Web Link



Trend Micro Anti-Malware Blog

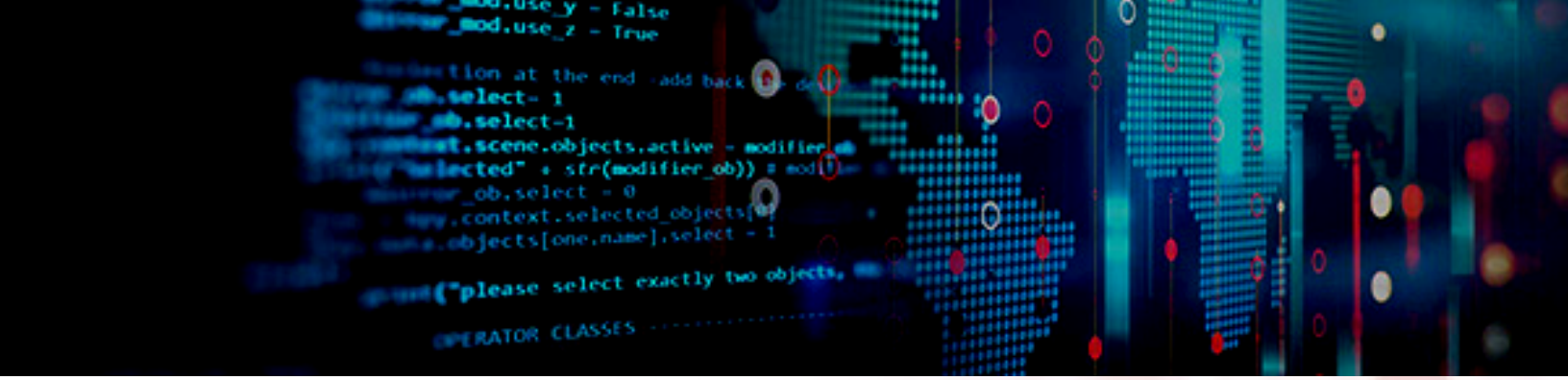
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

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
* Year in Review: Rapid7 Cybersecurity Research
* Rapid7 Announces Global Days Off to Support Employees in 2023
* 2022 Annual Metasploit Wrap-Up
* Understanding the Ecosystem of Smart Cities for the Purpose of Security Testing
* Refreshing Rapid7's Coordinated Vulnerability Disclosure Policy
* The 2022 Naughty and Nice List
* Hallmark Channel: Securing the Season
* Cloud Security and Compliance Best Practices: Highlights From The CSA Cloud Controls Matrix
* CVE-2022-41080, CVE-2022-41082: Rapid7 Observed Exploitation of `OWASSRF` in Exchange for RCE



Advisories

US-Cert Alerts & bulletins

* CISA Releases Three Industrial Systems Control Advisories
* Fortinet Releases Security Updates for FortiADC
* CISA Adds Two Known Exploited Vulnerabilities to Catalog
* CISA Releases Four Industrial Control Systems Advisories
* CISA Releases Six Industrial Control Systems Advisories
* Samba Releases Security Updates
* FBI, FDA OCI, and USDA Release Joint Cybersecurity Advisory Regarding Business Email Compromise Schem
* CISA Releases Forty-One Industrial Control Systems Advisories
* AA22-335A: #StopRansomware: Cuba Ransomware
* AA22-321A: #StopRansomware: Hive Ransomware
* Vulnerability Summary for the Week of December 26, 2022
* Vulnerability Summary for the Week of December 19, 2022

Zero Day Initiative Advisories

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, 2 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, 2 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, 2 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, 2 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, 2 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-20007: VMware

A CVSS score 5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L) severity vulnerability discovered by 'Guy Lederfein of Trend Micro Security Research' was reported to the affected vendor on: 2023-01-05, 4 days ago. The vendor is given until 2023-05-05 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19498: NETGEAR

A CVSS score 4.6 (AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Dmitry "InfoSecDJ" Janushkevich of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-01-04, 5 days ago. The vendor is given until 2023-05-04 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-19652: Schneider Electric

A CVSS score 8.1 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2023-01-04, 5 days ago. The vendor is given until 2023-05-04 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-19419: 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: 2023-01-04, 5 days ago. The vendor is given until 2023-05-04 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-19533: Schneider Electric

A CVSS score 8.1 (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2023-01-04, 5 days ago. The vendor is given until 2023-05-04 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-20009: NETGEAR

A CVSS score 8.0 (AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Dmitry "InfoSecDJ" Janushkevich of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-01-04, 5 days ago. The vendor is given until 2023-05-04 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-19660: NETGEAR

A CVSS score 6.3 (AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Dmitry "InfoSecDJ" Janushkevich of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-01-04, 5 days ago. The vendor is given until 2023-05-04 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-19636: 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 'hades_kito' was reported to the affected vendor on: 2023-01-04, 5 days ago. The vendor is given until 2023-05-04 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-19954: Microsoft

A CVSS score 7.8 (AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-01-04, 5 days ago. The vendor is given until 2023-05-04 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-19736: Western Digital

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 'Luca MORO (@johncool__) - moro.luca@gmail.com' was reported to the affected vendor on: 2022-12-29, 11 days ago. The vendor is given until 2023-04-28 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-19856: Western Digital

A CVSS score 6.5 (AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) severity vulnerability discovered by 'Sam Thomas (@_s_n_t) of Pentest Ltd (@pentestltd)' was reported to the affected vendor on: 2022-12-29, 11 days ago. The vendor is given until 2023-04-28 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-19727: Sonos

A CVSS score 5.4 (AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L) severity vulnerability discovered by 'Toan (suto) Pham and Tri Dang from qriousec.io' was reported to the affected vendor on: 2022-12-29, 11 days ago. The vendor is given until 2023-04-28 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-19698: Sonos

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 'Phan Thanh Duy (@PTDuy) & Nguyen Hoang Thach (@hi_im_d4rkn3ss) of STAR Labs SG Pte. Ltd.' was reported to the affected vendor on: 2022-12-29, 11 days ago. The vendor is given until 2023-04-28 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-19846: Sonos

A CVSS score 5.4 (AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L) severity vulnerability discovered by 'Phan Thanh Duy (@PTDuy) & Nguyen Hoang Thach (@hi_im_d4rkn3ss) of STAR Labs SG Pte. Ltd.' was reported to the affected vendor on: 2022-12-29, 11 days ago. The vendor is given until 2023-04-28 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-19797: Mikrotik

A CVSS score 7.5 (AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Angelboy(@scwuaptx) and NiNi (@terrynini38514) from DEVCORE Research Team' was reported to the affected vendor on: 2022-12-29, 11 days ago. The vendor is given until 2023-04-28 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-19767: Western Digital

A CVSS score 7.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Sam Thomas (@_s_n_t) of Pentest Ltd (@pentestltd)' was reported to the affected vendor on: 2022-12-29, 11 days ago. The vendor is given until 2023-04-28 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-19844: HP

A CVSS score 8.8 (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'hoangha2' was reported to the affected vendor on: 2022-12-29, 11 days ago. The vendor is given until 2023-04-28 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-19873: Nikon

A CVSS score 7.0 (AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2022-12-29, 11 days ago. The vendor is given until 2023-04-28 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-19946: D-Link

A CVSS score 6.8 (AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'VRI FALL 2022

(Minh Giang, Nicholas Zubrisky, Evan Qi)' was reported to the affected vendor on: 2022-12-29, 11 days ago. The vendor is given until 2023-04-28 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-5788-1

Ubuntu Security Notice 5788-1 - Hiroki Kurosawa discovered that curl incorrectly handled HSTS support when certain hostnames included IDN characters. A remote attacker could possibly use this issue to cause curl to use unencrypted connections. This issue only affected Ubuntu 22.04 LTS, and Ubuntu 22.10. It was discovered that curl incorrectly handled denials when using HTTP proxies. A remote attacker could use this issue to cause curl to crash, resulting in a denial of service, or possibly execute arbitrary code.

Ubuntu Security Notice USN-5789-1

Ubuntu Security Notice 5789-1 - 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. Jann Horn discovered that the Linux kernel did not properly track memory allocations for anonymous VMA mappings in some situations, leading to potential data structure reuse. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5782-2

Ubuntu Security Notice 5782-2 - USN-5782-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem.

Ubuntu Security Notice USN-5787-1

Ubuntu Security Notice 5787-1 - It was discovered that Libksba incorrectly handled parsing CRL signatures. A remote attacker could use this issue to cause Libksba to crash, resulting in a denial of service, or possibly execute arbitrary code.

Red Hat Security Advisory 2022-9098-01

Red Hat Security Advisory 2022-9098-01 - 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 4.10.46. Issues addressed include a code execution vulnerability.

Ubuntu Security Notice USN-5786-1

Ubuntu Security Notice 5786-1 - It was discovered that GNOME Files incorrectly handled certain filenames. An attacker could possibly use this issue to cause GNOME Files to crash, leading to a denial of service.

Red Hat Security Advisory 2023-0021-01

Red Hat Security Advisory 2023-0021-01 - WebKitGTK is the port of the portable web rendering engine WebKit to the GTK platform. Issues addressed include a code execution vulnerability.

Ubuntu Security Notice USN-5785-1

Ubuntu Security Notice 5785-1 - It was discovered that FreeRADIUS incorrectly handled multiple EAP-pwd handshakes. An attacker could possibly use this issue to cause a denial of service. This issue only affected Ubuntu 18.04 LTS. Shane Guan discovered that FreeRADIUS incorrectly handled memory when checking unknown SIM option sent by EAP-SIM supplicant. An attacker could possibly use this issue to cause a denial of service on the server. This issue only affected Ubuntu 16.04 ESM, Ubuntu 18.04 LTS and Ubuntu 20.04 LTS.

Red Hat Security Advisory 2022-9108-01

Red Hat Security Advisory 2022-9108-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. Issues addressed include a bypass vulnerability.

Red Hat Security Advisory 2022-9107-01

Red Hat Security Advisory 2022-9107-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the container images for Red Hat OpenShift Container Platform 4.11.21. There are no RPM packages for this release. Space precludes documenting all of the container images in this advisory.

Red Hat Security Advisory 2023-0016-01

Red Hat Security Advisory 2023-0016-01 - WebKitGTK is the port of the portable web rendering engine WebKit to the GTK platform. Issues addressed include a code execution vulnerability.

Ubuntu Security Notice USN-5784-1

Ubuntu Security Notice 5784-1 - It was discovered that usbredir incorrectly handled memory when serializing large amounts of data in the case of a slow or blocked destination. An attacker could possibly use this issue to cause applications using usbredir to crash, resulting in a denial of service, or possibly execute arbitrary code.

Red Hat Security Advisory 2023-0005-01

Red Hat Security Advisory 2023-0005-01 - The Byte Code Engineering Library is intended to give users a convenient way to analyze, create, and manipulate Java class files.

Red Hat Security Advisory 2023-0004-01

Red Hat Security Advisory 2023-0004-01 - The Byte Code Engineering Library is intended to give users a convenient way to analyze, create, and manipulate Java class files.

Debian Security Advisory 5310-1

Debian Linux Security Advisory 5310-1 - It was discovered that ruby-image-processing, a ruby package that provides higher-level image processing helpers, is prone to a remote shell execution vulnerability when using the #apply method to apply a series of operations coming from unsanitized user input.

Debian Security Advisory 5309-1

Debian Linux Security Advisory 5309-1 - Vulnerabilities have been discovered in the WPE WebKit web engine. hazbinhotel discovered that processing maliciously crafted web content may result in the disclosure of process memory. KirtiKumar Anandrao Ramchandani discovered that processing maliciously crafted web content may bypass Same Origin Policy. Dohyun Lee and Ryan Shin discovered that processing maliciously crafted web content may disclose sensitive user information. Various other issues have also been addressed.

Debian Security Advisory 5308-1

Debian Linux Security Advisory 5308-1 - Vulnerabilities have been discovered in the WebKitGTK web engine. hazbinhotel discovered that processing maliciously crafted web content may result in the disclosure of process memory. Maddie Stone discovered that processing maliciously crafted web content may lead to arbitrary code execution. KirtiKumar Anandrao Ramchandani discovered that processing maliciously crafted web content may bypass Same Origin Policy. Multiple other issues were also addressed.

Debian Security Advisory 5307-1

Debian Linux Security Advisory 5307-1 - ZeddYu Lu discovered that the FTP client of Apache Commons Net, a Java client API for basic Internet protocols, trusts the host from PASV response by default. A malicious server can redirect the Commons Net code to use a different host, but the user has to connect to the malicious server in the first place. This may lead to leakage of information about services running on the private network of the client.

Gentoo Linux Security Advisory 202212-06

Gentoo Linux Security Advisory 202212-6 - Multiple vulnerabilities have been found in OpenSSH, the worst of which could result in arbitrary code execution. Versions less than 9.1_p1 are affected.

Gentoo Linux Security Advisory 202212-07

Gentoo Linux Security Advisory 202212-7 - An integer overflow vulnerability has been found in libksba which could result in remote code execution. Versions less than 1.6.3 are affected.

Debian Security Advisory 5306-1

Debian Linux Security Advisory 5306-1 - Several vulnerabilities were discovered in gerbv, a Gerber file viewer, which could result in the execution of arbitrary code, denial of service or information disclosure if a specially crafted file is processed.

Debian Security Advisory 5305-1

Debian Linux Security Advisory 5305-1 - An integer overflow flaw was discovered in the CRL signature parser in libksba, an X.509 and CMS support library, which could result in denial of service or the execution of arbitrary code.

Apple Security Advisory 2022-12-13-9

Apple Security Advisory 2022-12-13-9 - Safari 16.2 addresses bypass, code execution, and use-after-free vulnerabilities.

[Apple Security Advisory 2022-12-13-8]

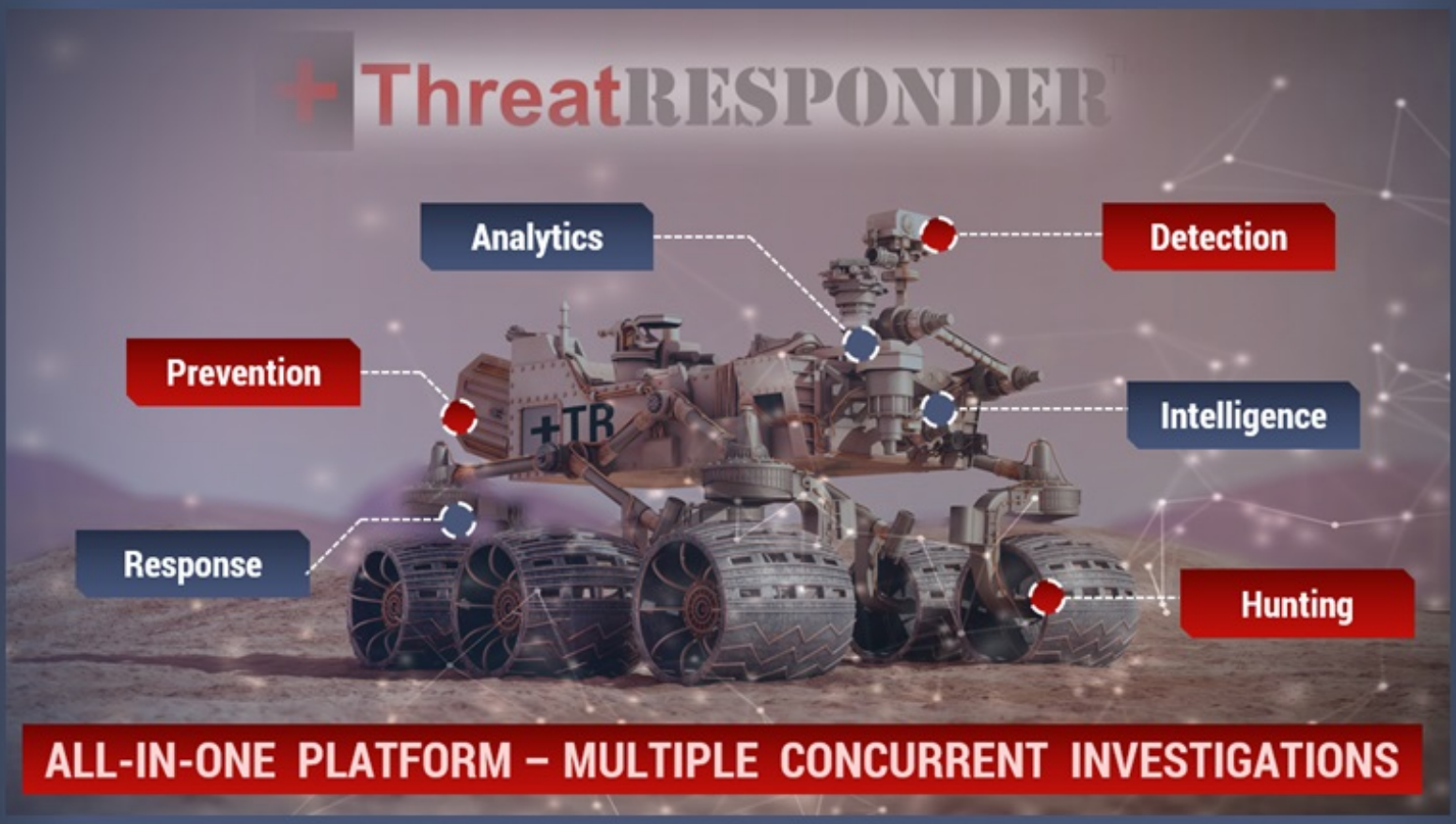
Apple Security Advisory 2022-12-13-8 - watchOS 9.2 addresses bypass, code execution, integer overflow, out of bounds write, spoofing, and use-after-free vulnerabilities.

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



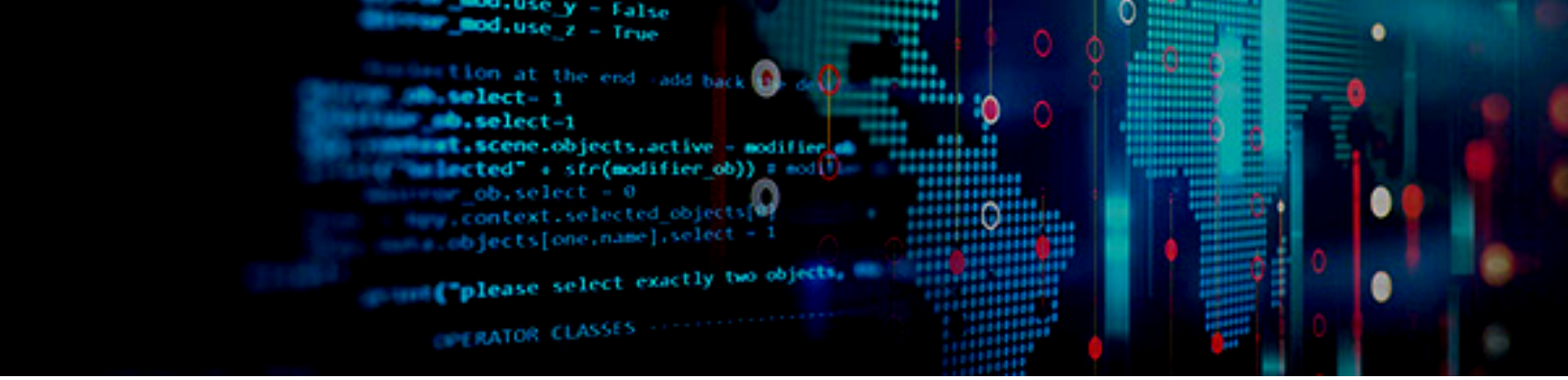
The Solution – ThreatResponder® Platform

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

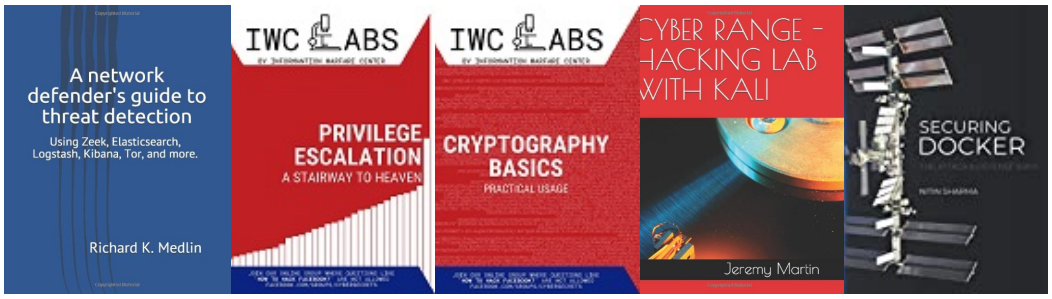


The Cyber Secrets publications on Amazon

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