Dec-26-22

# 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®

# CYBER WEEKLY AWARENESS REPORT

## December 26, 2022

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:GREEN http://isc.sans.edu

*Internet Storm Center Infocon Status*

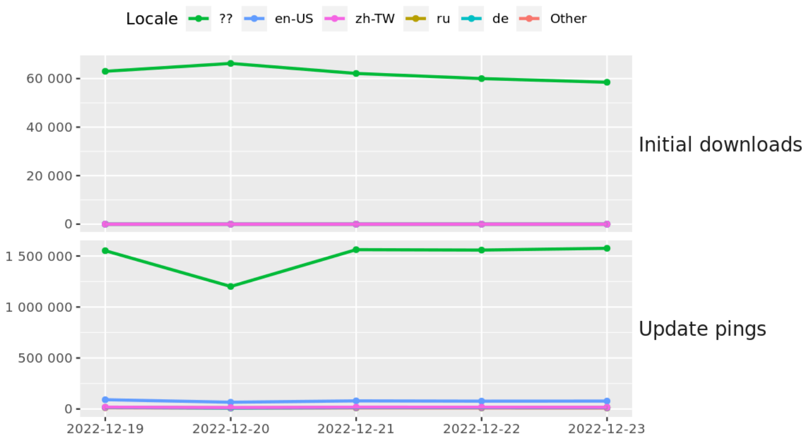
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

## Other IWC Publications

*Cyber Secrets books and ebook series can be found on Amazon.com at.* [amzn.to/2UuIG9B](amzn.to/2UuIG9B)

Cyber Secrets was originally a video series and is on both [YouTube](YouTube).

Tor Browser downloads and updates by locale



The Tor Project - https://metrics.torproject.org/

## 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](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](Cyber Secrets Facebook group here).

# Index of Sections

Current News

The Hacker Corner:

Cyber Range Content

Tools & Techniques

InfoSec Media for the Week

Exploits and Proof of Concepts

Cyber Crime & Malware Files/Links Latest Identified

Advisories

Information Warfare Center Products

# LATEST NEWS

**Packet Storm Security**

* Microsoft Fined $64 Million By France Over Cookies Used In Bing Searches
* LastPass Admits Attackers Have A Copy Of Customers' Password Vaults
* Meta To Settle Cambridge Analytica Case For Mere $725 Million
* Judge Forces SBF To Move Back With Parents On $250 Million Bail
* Full January 6 Investigation Report Released Telling Us What We Already Knew
* Godfather Malware Makes Banking Apps An Offer They Can't Refuse
* Apple Accused Of Censoring Apps In Hong Kong And Russia
* Microsoft Fixes Hyper-V VM Problem Caused By Patch Tuesday
* Kremlin-Backed Hackers Targeted A Large Petroleum Refinery
* FTX Boss Sam Bankman-Fried Flying To US To Face Fraud Charges
* Guardian Newspaper Hit By Suspected Ransomware Attack
* Swatters Used Ring Cameras To Livestream Attacks, Taunt Police
* Trojanized Windows 10 Installers Hit Ukrainian Government
* The Risk Of Escalation From Cyberattacks Has Never Been Greater
* McGraw Hill's S3 Buckets Exposed 100k Students' Grades / Info
* Over 67,000 DraftKings Betting Accounts Hit By Hackers
* Email Hijackers Scam Food Out Of Businesses, Not Just Money
* Singapore's Crypto Ambitions Shaken By FTX Collapse
* Digging Into The Numbers One Year After Log4Shell
* Musk Poll Backfires Telling Him To Step Down
* Scientists May Have Found The First Water Worlds
* Meta Warns Spyware Still Being Used To Target People On Social Media
* Microsoft Discovers Windows / Linux Botnet Used In DDoS Attacks
* Elon Musk Bans Journalists After Reinstating Literal Nazis
* Prosecutors Charge Six, Seize 48 Domains Over DDoS-For-Hire Services

**Krebs on Security**

* 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
* Researchers Quietly Cracked Zeppelin Ransomware Keys

# LATEST NEWS

**Dark Reading**

* Container Verification Bug Allows Malicious Images to Cloud Up Kubernetes
* LastPass Cops to Massive Breach Including Customer Vault Data
* Videoconferencing Worries Grow, With SMBs in Cyberattack Crosshairs
* Google: With Cloud Comes APIs & Security Headaches
* Fool Me Thrice? How to Avoid Double and Triple Ransomware Extortion
* Security Is a Second-Class Citizen in High-Performance Computing
* What Kind of Data Gets Stolen When a Developer is Compromised?
* New Brand of Security Threats Surface in the Cloud
* Inside the Next-Level Fraud Ring Scamming Billions Off Holiday Retailers
* Biden Signs Post-Quantum Cybersecurity Guidelines Into Law
* Passwordless Authentication Market to Be Worth $55.7 Billion by 2030: Grand View Research, Inc.
* Security on a Shoestring? Cloud, Consolidation Best Bets for Businesses
* Google WordPress Plug-in Bug Allows AWS Metadata Theft
* Threat Modeling in the Age of OpenAI's Chatbot
* 'Sextortion,' Business Disruption, and a Massive Attack: What Could Be in Store for 2023
* Zerobot Adds Brute Force, DDoS to Its IoT Attack Arsenal
* Supply Chain Risks Got You Down? Keep Calm and Get Strategic!
* Ransomware Attackers Bypass Microsoft's ProxyNotShell Mitigations With Fresh Exploit
* Heartland Alliance Provides Notice of Data Security Incident
* Best Practices for Securing and Governing Your Multicloud Deployment

**The Hacker News**

* GuLoader Malware Utilizing New Techniques to Evade Security Software
* 2022 Top Five Immediate Threats in Geopolitical Context
* PrivateLoader PPI Service Found Distributing Info-Stealing RisePro Malware
* W4SP Stealer Discovered in Multiple PyPI Packages Under Various Names
* FrodoPIR: New Privacy-Focused Database Querying System
* Researchers Warn of Kavach 2FA Phishing Attacks Targeting Indian Govt. Officials
* Accelerate Your Incident Response
* Vice Society Ransomware Attackers Adopt Robust Encryption Methods
* France Fines Microsoft â‚¬60 Million for Using Advertising Cookies Without User Consent
* LastPass Admits to Severe Data Breach, Encrypted Password Vaults Stolen
* FIN7 Cybercrime Syndicate Emerges as a Major Player in Ransomware Landscape
* The Era of Cyber Threat Intelligence Sharing
* Critical Security Flaw Reported in Passwordstate Enterprise Password Manager
* Two New Security Flaws Reported in Ghost CMS Blogging Software
* Zerobot Botnet Emerges as a Growing Threat with New Exploits and Capabilities

# LATEST NEWS

**Security Week**

* Microsoft Patches Azure Cross-Tenant Data Access Flaw
* Facebook Agrees to Pay $725 Million to Settle Privacy Suit
* BetMGM Confirms Breach as Hackers Offer to Sell Data of 1.5 Million Customers
* China's ByteDance Admits Using TikTok Data to Track Journalists
* LastPass Says Password Vault Data Stolen in Data Breach
* Zerobot IoT Botnet Adds More Exploits, DDoS Capabilities
* Five Ways TikTok Is Seen as Threat to US National Security
* Over 50 New CVE Numbering Authorities Announced in 2022
* France Seeks to Protect Hospitals After Series of Cyberattacks
* FBI Recommends Ad Blockers as Cybercriminals Impersonate Brands in Search Engine Ads
* Researchers Link Royal Ransomware to Conti Group
* Okta Source Code Stolen by Hackers
* Ransomware Attack Causes Disruption at British Newspaper The Guardian
* Companies Announced Billions in US Government Cybersecurity Contracts in 2022
* France Fines Microsoft 60 Million Euros Over Advertising Cookies
* Godfather Android Banking Trojan Targeting Over 400 Applications
* Cyber Insurance Analytics Firm CyberCube Raises $50 Million
* Critical Vulnerabilities Found in Passwordstate Enterprise Password Manager
* Russian APT Gamaredon Changes Tactics in Attacks Targeting Ukraine
* Is Enterprise VPN on Life Support or Ripe for Reinvention?
* Two Men Arrested for JFK Airport Taxi Hacking Scheme
* Ransomware Uses New Exploit to Bypass ProxyNotShell Mitigations
* Critical Vulnerability in Hikvision Wireless Bridges Allows CCTV Hacking
* Industrial Giant Thyssenkrupp Again Targeted by Cybercriminals
* Congress Moves to Ban TikTok From US Government Devices
* DraftKings Data Breach Impacts Personal Information of 68,000 Customers

**Infosecurity Magazine**

# LATEST NEWS

**KnowBe4 Security Awareness Training Blog RSS Feed**

* Microsoft Warns of Signed Drivers Being Used to Terminate AV and EDR Processes
* The Number of Phishing Attacks Grows 15% in One Quarter, Reaching an All-Time High
* New Polymorphic Wiper Malware Leaves Attacked Environments "Unrecoverable"
* Spear Phishing Campaign Targets Japanese Political Organizations
* "How I lost my dog and almost my Google credentials..."
* KnowBe4 Named a Leader in the Winter 2023 G2 Grid Report for Security Orchestration, Automation, and
* KnowBe4 Named a Leader in the Winter 2023 G2 Grid Report for Security Awareness Training
* Ivanti Report Shows Cybersecurity Practitioners Concentrating on Right Threats
* 'Tis the season for Scam-Folly Fa La La La La
* XLL Files Used to Deliver Malware

**ISC2.org Blog**

* Latest Cyberthreats and Advisories - December 23, 2022
* (ISC)&sup2; Top-Ranked Webinars of 2022 by Region
* Seasons Greetings from (ISC)2
* Policy Brief - U.S. Cyber Threat Intelligence, Part 1: Introduction & Background
* (ISC)2 CEO Discusses UK and Global Cyber Challenges at Chatham House

**HackRead**

* LastPass: Hackers Stole User Data and Encrypted Password Vaults
* Online Casinos DraftKings and BetMGM Hacked; Data of Millions at Risk
* Android-Based Digital Signage: Key Features and Benefits
* Sale or No Sale; Hacker Leaks FBI's InfraGard database Online
* Cybersecurity Awareness Training in Companies: Why You Can't Do Without It
* Media Giant Guardian Hit By Suspected Ransomware Attack
* Cyber Threats Increasingly Target Video Games

**Koddos**

* LastPass: Hackers Stole User Data and Encrypted Password Vaults
* Online Casinos DraftKings and BetMGM Hacked; Data of Millions at Risk
* Android-Based Digital Signage: Key Features and Benefits
* Sale or No Sale; Hacker Leaks FBI's InfraGard database Online
* Cybersecurity Awareness Training in Companies: Why You Can't Do Without It
* Media Giant Guardian Hit By Suspected Ransomware Attack
* Cyber Threats Increasingly Target Video Games

# LATEST NEWS

**Naked Security**

* LastPass finally admits: Those crooks who got in? They did steal your password vaults, after all&hell
* S3 Ep114: Preventing cyberthreats - stop them before they stop you! [Audio + Text]
* "Suspicious login" scammers up their game - take care at Christmas
* Microsoft dishes the dirt on Apple's "Achilles heel" shortly after fixing similar Windows bug
* OneCoin scammer Sebastian Greenwood pleads guilty, "Cryptoqueen" still missing
* S3 Ep113: Pwning the Windows kernel - the crooks who hoodwinked Microsoft [Audio + Text]
* Apple patches everything, finally reveals mystery of iOS 16.1.2
* Patch Tuesday: 0-days, RCE bugs, and a curious tale of signed malware
* COVID-bit: the wireless spyware trick with an unfortunate name
* Pwn2Own Toronto: 54 hacks, 63 new bugs, $1 million in bounties

**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

# LATEST NEWS

**IBM Security Intelligence**

* How the CCPA is Shaping Other State's Data Privacy
* What Can We Learn From Recent Cyber History?
* Beware of What Is Lurking in the Shadows of Your IT
* When Logs Are Out, Enhanced Analytics Stay In
* Don't Wait to Embrace CISA's Vulnerability Management Rules
* 4 Most Common Cyberattack Patterns from 2022
* How Reveton Ransomware-as-a-Service Changed Cybersecurity
* The Cybersecurity Takeaway from Twitter's Verification Chaos
* 5 Ways to Improve Holiday Retail and Wholesale Cybersecurity
* How to Embed Gen Z in Your Organization's Security Culture

**InfoWorld**

* Build a customer-facing app like a SaaS company
* The fundamentals of Kubernetes cost management
* R tutorials: Learn R programming for data science
* 3 cloud architecture best practices for industry clouds
* Visual Studio 2022 adds C++ atomics
* How to use symmetric and asymmetric encryption in C#
* Why zero knowledge matters
* Introducing Cadl: Microsoft's concise API design language
* How Steampipe enables KPIs as code
* Eclipse GlassFish catches up with Jakarta EE 10

**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.

* ASIS CTF Finals 2022
* TetCTF 2023
* Real World CTF 5th
* IrisCTF 2023
* idekCTF 2022*
* Hack a Bit (Qualifier)
* KnightCTF 2023
* Insomni'hack teaser 2023
* DiceCTF 2023
* LA CTF 2023

### VulnHub Downloadable CTFs for your Cyber Range (Most use VirtualBox)

* Matrix-Breakout: 2 Morpheus
* Web Machine: (N7)
* The Planets: Earth
* Jangow: 1.0.1
* Red: 1

# Tools & Techniques

### Packet Storm Security Tools Links

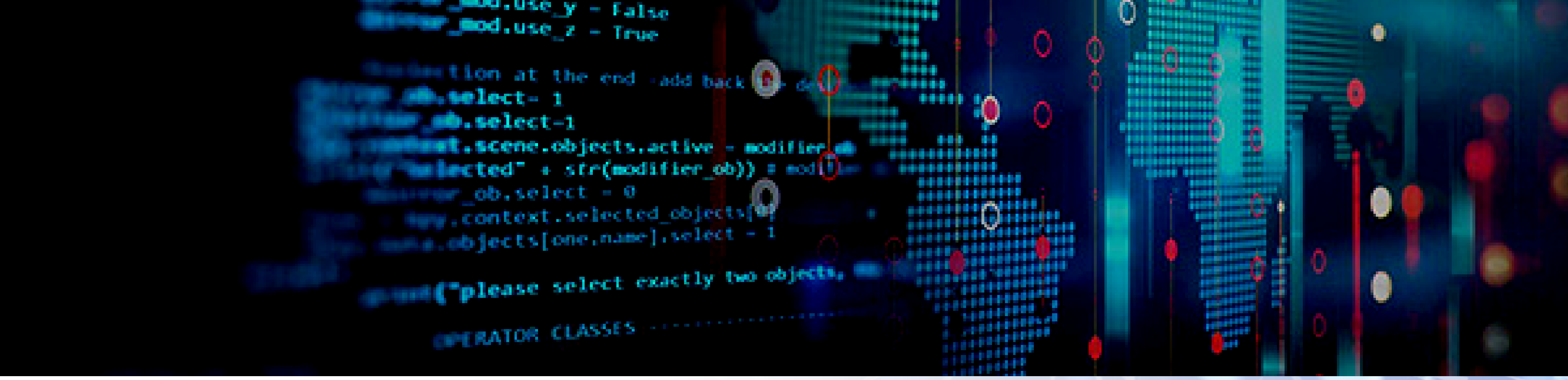
* GRAudit Grep Auditing Tool 3.5
* cryptmount Filesystem Manager 6.1.1
* GNU Privacy Guard 2.4.0
* GNU Privacy Guard 2.2.41
* Faraday 4.3.1
* Adversary3 3.0
* Global Socket 1.4.39
* Wireshark Analyzer 4.0.2
* TOR Virtual Network Tunneling Tool 0.4.7.12
* GNUnet P2P Framework 0.19.0

### Kali Linux Tutorials

* NetLlix : Tool To Emulate & Test Exfiltration Of Data Over Different Network Protocols
* Squarephish : OAuth Device Code Authentication Flow & QR codes
* HTTPLoot : An Automated Tool Which Can Simultaneously Crawl, Fill Forms, Trigger Error/Debug Pages
* What Is SASE and What Security Threats Can it Prevent?
* Kali Linux 2022.4 : Penetration Testing and Ethical Hacking Linux Distribution
* Shennina : Automating Host Exploitation With AI
* laZzzy : Shellcode Loader, Developed Using Different Open-Source Libraries, That Demonstrates Differe
* Octosuite : Advanced Github OSINT Framework
* Codecepticon : .NET Application That Allows You To Obfuscate C#, VBA/VB6 (Macros), And PowerShell Sou
* Legitify : Detect & Remediate Misconfigurations & Security Risks Across All Your GitHub Assets

### GBHackers Analysis

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



## Weekly Cyber Security Video and Podcasts

**SANS DFIR**

* SANS Threat Analysis Rundown (STAR)
* Analysis Paralysis? Setting the Right Goal for Your Incident Analysis
* Hunting Threat Actors Using OSINT
* Updates in DFIR

**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]**

* Best Virus Removal Tools: Cleaning a deeply infected system
* Fake MSI Afterburner with Hidden Malware

**Eli the Computer Guy**

* 30 Day Break - Elon Musk Broke Me...
* ELON MUSK DESTROYS TESLA... Stock is tanking due to Twitter
* ELON MUSK FIGHTING "WOKE MIND VIRUS" at TWITTER
* BLUE APRON LAYOFFS - Tech Sector IMPLODING

**Security Now**

* A Generic WAF Bypass - Pwn2Own Toronto, URSNIF malware, Vivaldi Mastodon support, Bye Bye SHA-1
* Apple Encrypts the Cloud - Chrome Passkeys, Telegram malware, SYNC.com outage, Rackspace lawsuits

**Troy Hunt**

* Weekly  Update 327

**Intel Techniques: The Privacy, Security, & OSINT Show**

* 286-Closing Out 2022
* 285-Travel Security Revisited

# Proof of Concept (PoC) & Exploits

## Packet Storm Security

* OpenTSDB 2.4.0 Command Injection
* WordPress Yith WooCommerce Gift Cards Premium 3.19.0 Shell Upload
* Stock Management System 2022 1.0 From Erick Cesar SQL Injection
* Eclipse Business Intelligence Reporting Tool 4.11.0 Remote Code Execution
* 4images 1.9 Remote Command Execution
* Senayan Library Management System 9.2.2 SQL Injection
* Senayan Library Management System 9.2.2 Cross Site Scripting
* Senayan Library Management System 9.2.1 SQL Injection
* Senayan Library Management System 9.2.1 Cross Site Scripting
* Senayan Library Management System 9.2.0 SQL Injection
* Senayan Library Management System 9.2.0 Cross Site Scripting
* Senayan Library Management System 9.1.1 SQL Injection
* Senayan Library Management System 9.1.1 Cross Site Scripting
* Bangresta 1.0 SQL Injection
* SOUND4 IMPACT/FIRST/PULSE/Eco 2.x Unauthenticated Factory Reset
* SOUND4 IMPACT/FIRST/PULSE/Eco 2.x upload.cgi Code Execution
* SOUND4 IMPACT/FIRST/PULSE/Eco 2.x traceroute.php Conditional Command Injection
* SOUND4 IMPACT/FIRST/PULSE/Eco 2.x username Command Injection
* SOUND4 IMPACT/FIRST/PULSE/Eco 2.x password Command Injection
* SOUND4 IMPACT/FIRST/PULSE/Eco 2.x services Command Injection
* SOUND4 IMPACT/FIRST/PULSE/Eco 2.x Unauthenticated File Disclosure
* SOUND4 IMPACT/FIRST/PULSE/Eco 2.x ping.php Command Injection
* SOUND4 IMPACT/FIRST/PULSE/Eco 2.x Radio Steam Disclosure
* SOUND4 IMPACT/FIRST/PULSE/Eco 2.x dns.php Command Injection
* SOUND4 IMPACT/FIRST/PULSE/Eco 2.x Information Disclosure

## 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

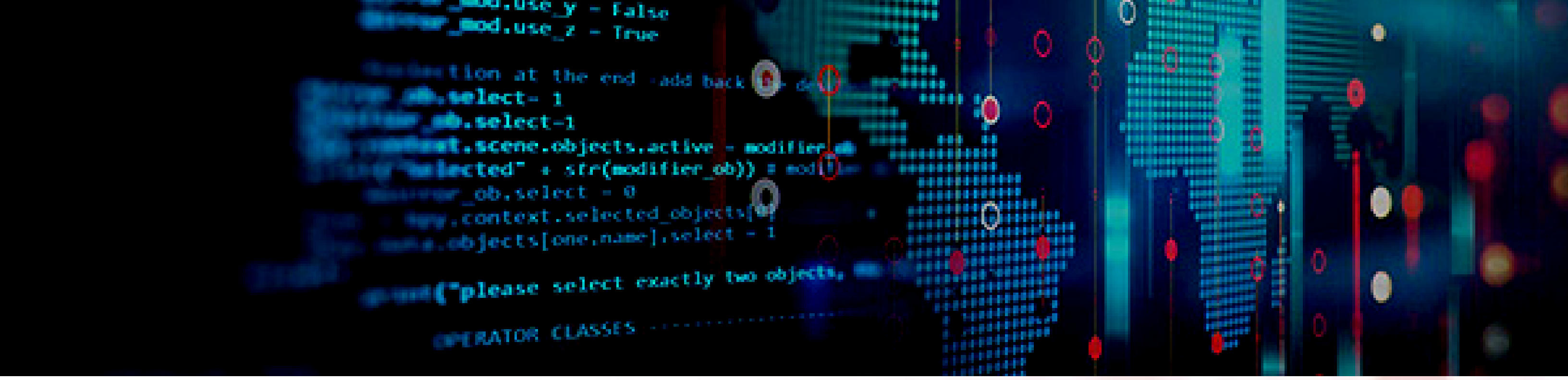
* [remote] SmartRG Router SR510n 2.6.13 - Remote Code Execution
* [webapps] CVAT 2.0 - Server Side Request Forgery
* [local] IOTransfer V4 - Unquoted Service Path
* [remote] AVEVA InTouch Access Anywhere Secure Gateway 2020 R2 - Path Traversal
* [remote] MSNSwitch Firmware MNT.2408 - Remote Code Execution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

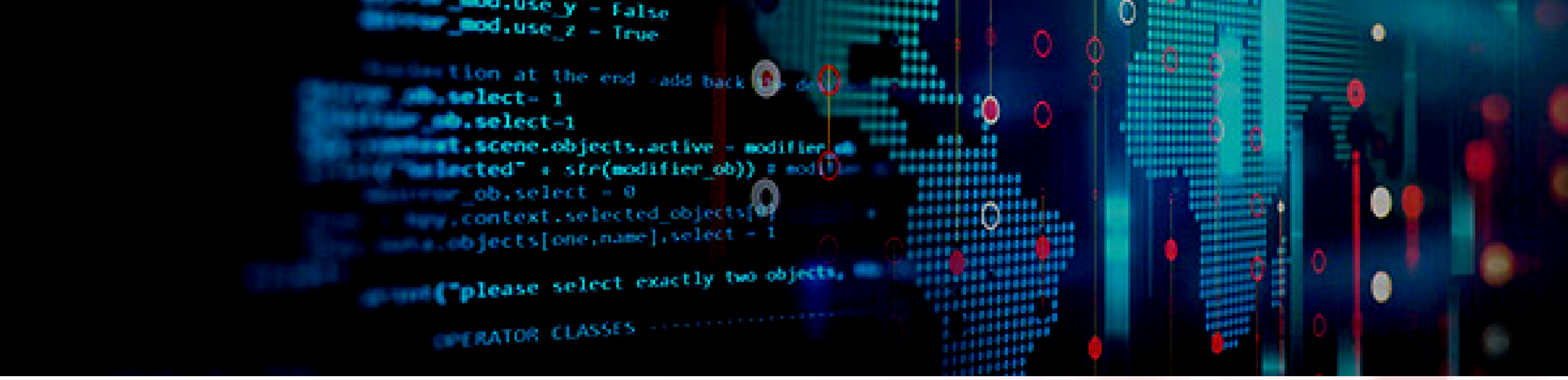
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



# Latest Hacked Websites

**Published on Zone-h.org**

https://pusdiklat.perpusnas.go.id/public/media/tinymce/f.jpg
https://pusdiklat.perpusnas.go.id/public/media/tinymce/f.jpg notified by XMFFX
http://dpmd.mojokertokab.go.id/readme.php
http://dpmd.mojokertokab.go.id/readme.php notified by UCEN HAXOR
http://pesat.dilmil-semarang.go.id/end.html
http://pesat.dilmil-semarang.go.id/end.html notified by ./KeyzNet
https://sinaga.dilmil-semarang.go.id/end.html
https://sinaga.dilmil-semarang.go.id/end.html notified by ./KeyzNet
http://sipp.dilmil-semarang.go.id/end.html
http://sipp.dilmil-semarang.go.id/end.html notified by ./KeyzNet
http://etebaspura.dilmil-semarang.go.id/end.html
http://etebaspura.dilmil-semarang.go.id/end.html notified by ./KeyzNet
https://skp.bkd.probolinggokab.go.id
https://skp.bkd.probolinggokab.go.id notified by ./KeyzNet
https://survey.dpmptsp.dompukab.go.id
https://survey.dpmptsp.dompukab.go.id notified by ./KeyzNet
https://dpmptsp.dompukab.go.id
https://dpmptsp.dompukab.go.id notified by ./KeyzNet
https://plafon.pa-enrekang.go.id/end.html
https://plafon.pa-enrekang.go.id/end.html notified by ./KeyzNet
https://sipp.pa-enrekang.go.id
https://sipp.pa-enrekang.go.id notified by ./KeyzNet
https://new.pa-enrekang.go.id/end.html
https://new.pa-enrekang.go.id/end.html notified by ./KeyzNet
https://ekominfo.sumenepkab.go.id
https://ekominfo.sumenepkab.go.id notified by ./KeyzNet
https://112.sumenepkab.go.id
https://112.sumenepkab.go.id notified by ./KeyzNet
https://www.jdih.pa-simalungun.go.id/!.php
https://www.jdih.pa-simalungun.go.id/!.php notified by White Cyber Illusion
https://www.v1.pa-simalungun.go.id/!.php
https://www.v1.pa-simalungun.go.id/!.php notified by White Cyber Illusion
https://sidang.pa-simalungun.go.id/!.php
https://sidang.pa-simalungun.go.id/!.php notified by White Cyber Illusion

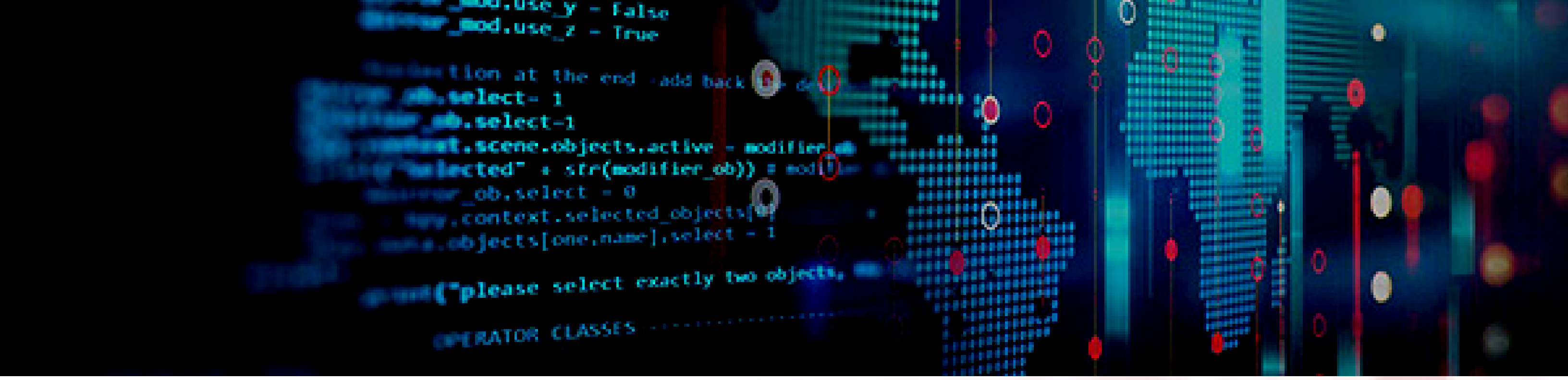


# Dark Web News

### Darknet Live

[Youngsters are getting into cybercrime and darknet]()
[Dark Web Child Abuse Sites Dismantled]()
[I2P - The Invisible Internet Project]()
[Two Men Charged for Distributing Fentanyl on the Dark Web]()

### Dark Web Link



## Trend Micro Anti-Malware Blog

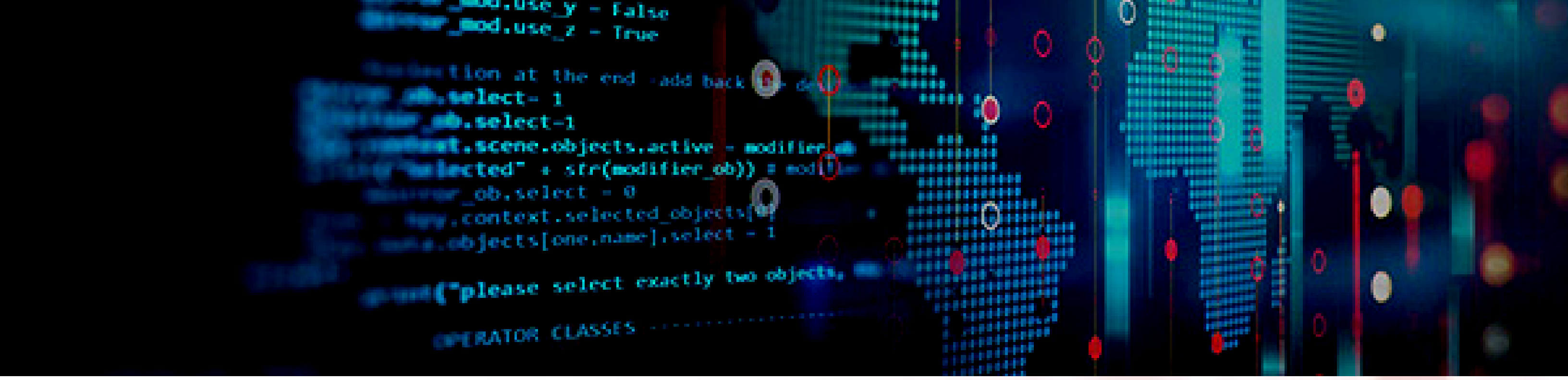
*Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.*

## 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&nbsp
* 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

* 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
* Never Mind the Ears, Here's Security Nation
* Cengage LTI Session Management Leakage
* ICYMI: 10 Cybersecurity Acronyms You Should Know in 2023
* [The Lost Bots] S02E06: Play "Experts or Scuttlebutt?" With Us
* Metasploit Weekly Wrap-Up
* Spoiler Alert: Your Favorite Content Might Not Be Secure
* Cloud Audit: Compliance + Automation



# Advisories

### US-Cert Alerts & bulletins

* 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
* Drupal Releases Security Updates to Address Vulnerabilities in H5P and File (Field) Paths
* CISA Consolidates Twitter Accounts
* CISA Adds One Known Exploited Vulnerability to Catalog
* AA22-335A: #StopRansomware: Cuba Ransomware
* AA22-321A: #StopRansomware: Hive Ransomware
* Vulnerability Summary for the Week of December 12, 2022
* Vulnerability Summary for the Week of December 5, 2022

### Zero Day Initiative Advisories

ZDI-CAN-19535: D-Link
A CVSS score 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Andrea Micalizzi aka rgod' was reported to the affected vendor on: 2022-12-23, 3 days ago. The vendor is given until 2023-04-22 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-19496: D-Link
A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Andrea Micalizzi aka rgod' was reported to the affected vendor on: 2022-12-23, 3 days ago. The vendor is given until 2023-04-22 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-19497: D-Link
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 'Andrea Micalizzi aka rgod' was reported to the affected vendor on: 2022-12-23, 3 days ago. The vendor is given until 2023-04-22 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-19910: D-Link
A CVSS score 8.8 (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Nicholas Zubrisky' was reported to the affected vendor on: 2022-12-23, 3 days ago. The vendor is given until 2023-04-22 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-19527: D-Link
A CVSS score 8.1 (AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H) severity vulnerability discovered by 'Andrea

Micalizzi aka rgod' was reported to the affected vendor on: 2022-12-23, 3 days ago. The vendor is given until 2023-04-22 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-19534: D-Link

A CVSS score 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Andrea Micalizzi aka rgod' was reported to the affected vendor on: 2022-12-23, 3 days ago. The vendor is given until 2023-04-22 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-19659: D-Link

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: 2022-12-23, 3 days ago. The vendor is given until 2023-04-22 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-19580: Advantech

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 'Esjay (@esj4y)' was reported to the affected vendor on: 2022-12-23, 3 days ago. The vendor is given until 2023-04-22 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-19529: D-Link

A CVSS score 6.5 (AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H) severity vulnerability discovered by 'Andrea Micalizzi aka rgod' was reported to the affected vendor on: 2022-12-23, 3 days ago. The vendor is given until 2023-04-22 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-19572: D-Link

A CVSS score 5.9 (AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2022-12-23, 3 days ago. The vendor is given until 2023-04-22 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-19571: D-Link

A CVSS score 8.2 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:L) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2022-12-23, 3 days ago. The vendor is given until 2023-04-22 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-19579: Advantech

A CVSS score 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Esjay (@esj4y)' was reported to the affected vendor on: 2022-12-23, 3 days ago. The vendor is given until 2023-04-22 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-19553: D-Link

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 'rgod' was reported to the affected vendor on: 2022-12-23, 3 days ago. The vendor is given until 2023-04-22 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-19502: Ivanti

A CVSS score 7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2022-12-23, 3 days ago. The vendor is given until 2023-04-22 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-19573: D-Link

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 'rgod' was reported to the affected vendor on: 2022-12-23, 3 days ago. The vendor is given until 2023-04-22 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-19503: Ivanti

A CVSS score 7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2022-12-23, 3 days ago. The vendor is given until 2023-04-22 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-19654: Schneider Electric

A CVSS score 6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2022-12-23, 3 days ago. The vendor is given until 2023-04-22 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-19513: Ivanti

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 'rgod' was reported to the affected vendor on: 2022-12-23, 3 days ago. The vendor is given until 2023-04-22 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-19653: Schneider Electric

A CVSS score 6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2022-12-23, 3 days ago. The vendor is given until 2023-04-22 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-19603: KeySight

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: 2022-12-23, 3 days ago. The vendor is given until 2023-04-22 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-19239: 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: 2022-12-23, 3 days ago. The vendor is given until 2023-04-22 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-19547: 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 'Anonymous' was reported to the affected vendor on: 2022-12-22, 4 days ago. The vendor is given until 2023-04-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19548: 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 'Anonymous' was reported to the affected vendor on: 2022-12-22, 4 days ago. The vendor is given until 2023-04-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19549: D-Link

A CVSS score 6.5 (AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-12-22, 4 days ago. The vendor is given until 2023-04-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

**Packet Storm Security - Latest Advisories**

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.

Apple Security Advisory 2022-12-13-7

Apple Security Advisory 2022-12-13-7 - tvOS 16.2 addresses bypass, code execution, integer overflow, out of bounds write, spoofing, and use-after-free vulnerabilities.

Apple Security Advisory 2022-12-13-6

Apple Security Advisory 2022-12-13-6 - macOS Big Sur 11.7.2 addresses bypass, code execution, and integer overflow vulnerabilities.

Apple Security Advisory 2022-12-13-5

Apple Security Advisory 2022-12-13-5 - macOS Monterey 12.6.2 addresses bypass, code execution, and integer overflow vulnerabilities.

Apple Security Advisory 2022-12-13-4

Apple Security Advisory 2022-12-13-4 - macOS Ventura 13.1 addresses bypass, code execution, out of bounds access, out of bounds write, spoofing, and use-after-free vulnerabilities.

Apple Security Advisory 2022-12-13-3

Apple Security Advisory 2022-12-13-3 - iOS 16.1.2 addresses a code execution vulnerability.

Apple Security Advisory 2022-12-13-2

Apple Security Advisory 2022-12-13-2 - iOS 15.7.2 and iPadOS 15.7.2 addresses bypass, code execution, integer overflow, out of bounds write, and spoofing vulnerabilities.

Apple Security Advisory 2022-12-13-1

Apple Security Advisory 2022-12-13-1 - iOS 16.2 and iPadOS 16.2 addresses bypass, code execution, out of bounds write, spoofing, and use-after-free vulnerabilities.

Debian Security Advisory 5304-1

Debian Linux Security Advisory 5304-1 - Jan-Niklas Sohn discovered several vulnerabilities in X server extensions in the X.Org X server, which may result in privilege escalation if the X server is running privileged.

Gentoo Linux Security Advisory 202212-03

Gentoo Linux Security Advisory 202212-3 - Multiple vulnerabilities have been discovered in Oracle Virtualbox, the worst of which could result in privilege escalation from a guest to the host. Versions less than 6.1.40 are affected.

Gentoo Linux Security Advisory 202212-05

Gentoo Linux Security Advisory 202212-5 - Multiple vulnerabilities have been discovered in NSS, the worst of which could result in arbitrary code execution. Versions less than 3.79.2 are affected.

Gentoo Linux Security Advisory 202212-01

Gentoo Linux Security Advisory 202212-1 - Multiple vulnerabilities have been found in curl, the worst of which could result in arbitrary code execution. Versions less than 7.86.0 are affected.

Gentoo Linux Security Advisory 202212-04

Gentoo Linux Security Advisory 202212-4 - A vulnerability has been discovered in LibreOffice which could result in arbitrary script execution via crafted links. Versions less than 7.3.6.2 are affected.

Gentoo Linux Security Advisory 202212-02

Gentoo Linux Security Advisory 202212-2 - Multiple vulnerabilities have been discovered in Unbound, the worst of which could result in denial of service. Versions less than 1.16.3 are affected.

Debian Security Advisory 5303-1

Debian Linux Security Advisory 5303-1 - Multiple security issues were discovered in Thunderbird, which could result in the execution of arbitrary code or information disclosure.

Debian Security Advisory 5302-1

Debian Linux Security Advisory 5302-1 - Multiple security issues were discovered in Chromium, which could result in the execution of arbitrary code, denial of service or information disclosure.

Ubuntu Security Notice USN-5783-1

Ubuntu Security Notice 5783-1 - Tam&aacute;s 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 2022-9073-01

Red Hat Security Advisory 2022-9073-01 - Node.js is a software development platform for building fast and scalable network applications in the JavaScript programming language. Issues addressed include bypass and denial of service vulnerabilities.

Red Hat Security Advisory 2022-9068-01

Red Hat Security Advisory 2022-9068-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 102.6.0 ESR. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2022-9082-01

Red Hat Security Advisory 2022-9082-01 - 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. Issues addressed include buffer overflow, out of bounds write, and privilege escalation vulnerabilities.

Red Hat Security Advisory 2022-9075-01

Red Hat Security Advisory 2022-9075-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 102.6.0. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2022-9076-01

Red Hat Security Advisory 2022-9076-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 102.6.0. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2022-9070-01

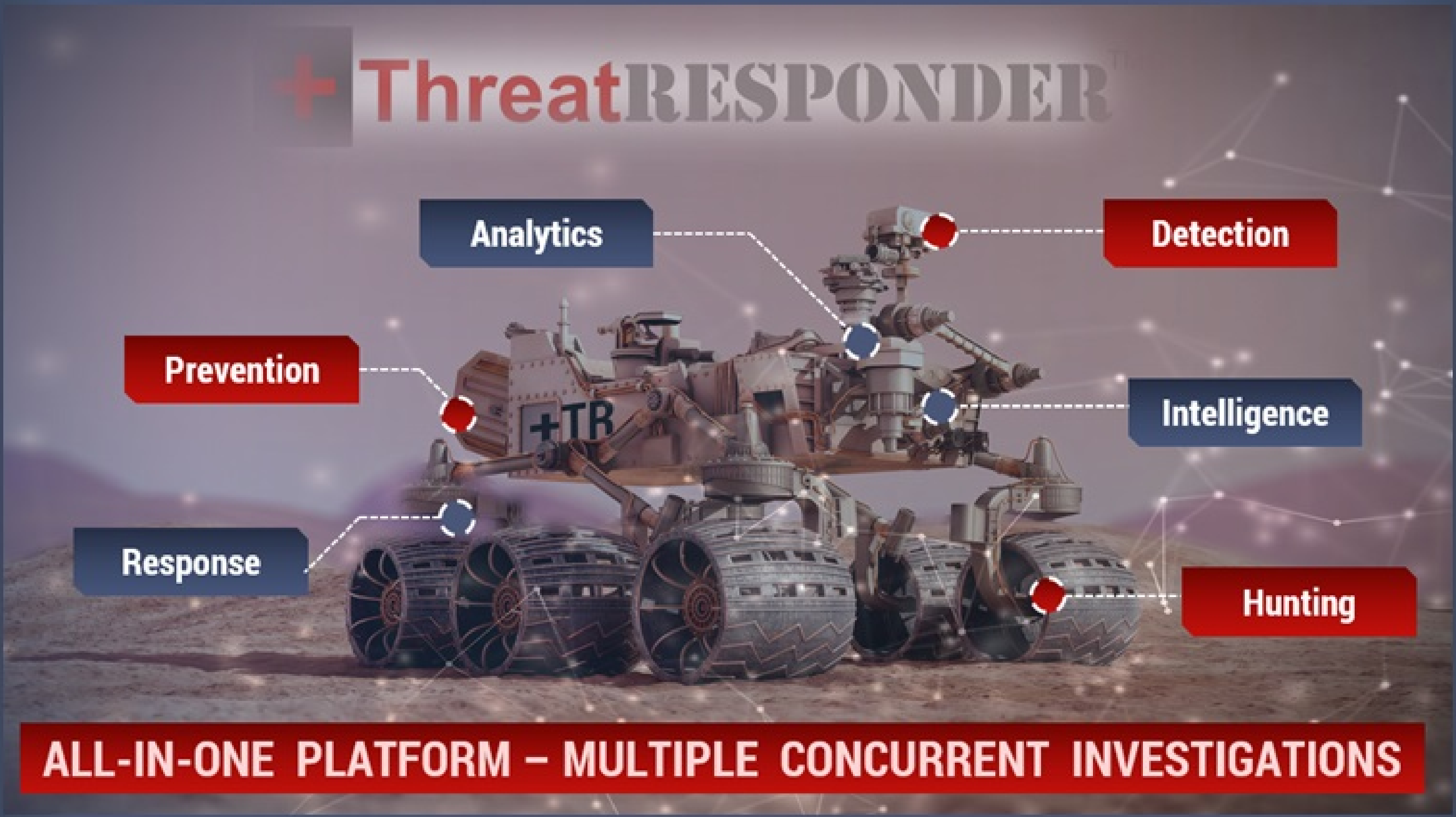
Red Hat Security Advisory 2022-9070-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 102.6.0 ESR. Issues addressed include a use-after-free vulnerability.

## 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



ALL-IN-ONE PLATFORM – MULTIPLE CONCURRENT INVESTIGATIONS

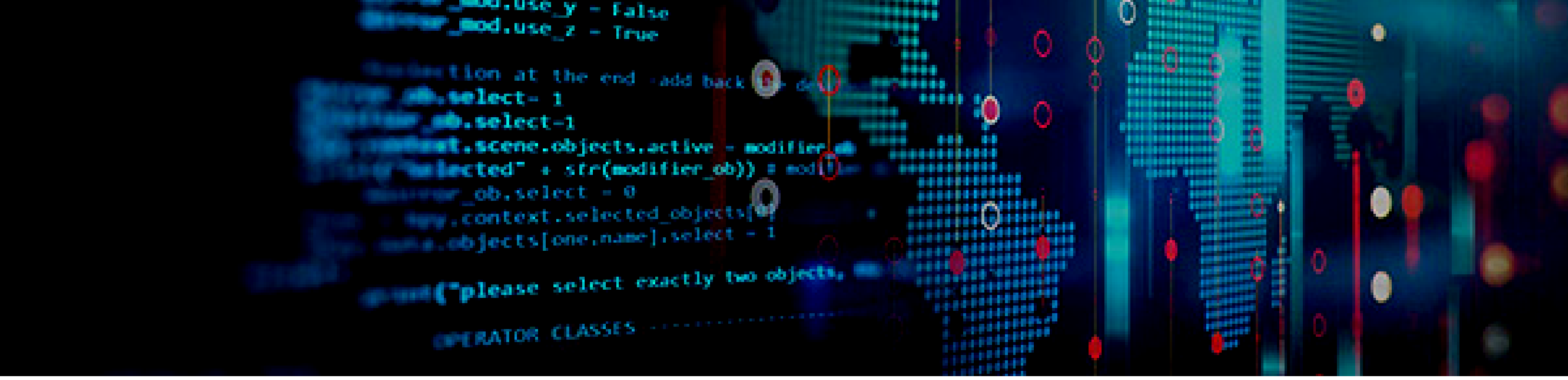
## The Solution – ThreatResponder® Platform

**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**

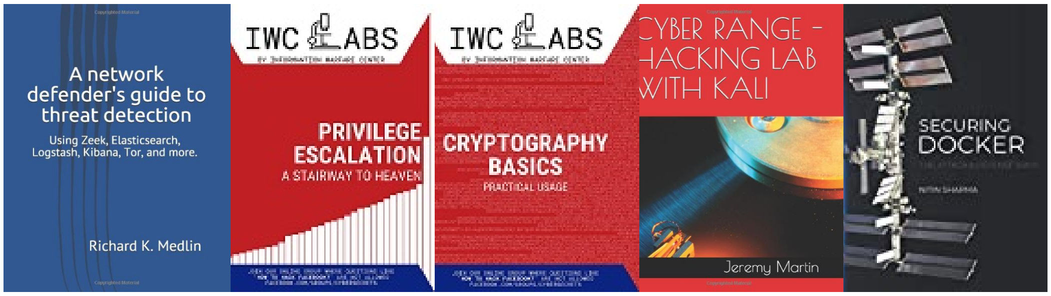


## The Cyber Secrets publications on Amazon

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

CSI LINUX

netSecurity®

ThreatRESPONDER

Accredited Training Center EC-Council

CYBERQ GROUP