Nov-08-21

# 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


## November 8, 2021

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

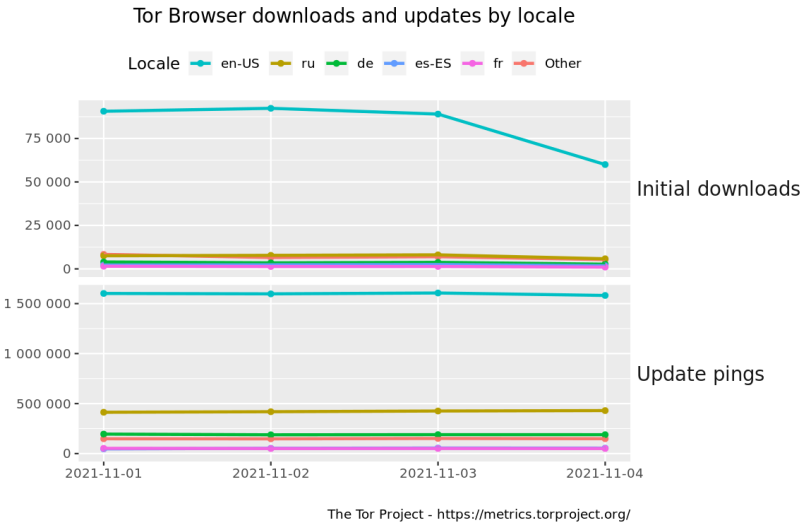
*Internet Storm Center Infocon Status*


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

* Subscribe to this OSINT resource to recieve it in in your inbox.  The Cyber WAR (Weekly Awareness Reports) keep you up to date with the current cyber threat landscape.

* The newest issue in the Cyber Secrets series (#6) - Incident Response: Evidence Preservation and Collection is now availible on Amazon!! This issue Incident Responce and Threat Hunting topics.  Great for any security team.

* * Our active Facebook group discusses the gambit of cyber security issues.  Join the Cyber Secrets Facebook group here.

# Index of Sections


**Packet Storm Security**

* Apple's Federighi Delivers Dramatic Speech On Dangers Of Sideloading
* Beijing Fingers Foreign Spies For Data Mischief
* US Offers $10 Million Bounty For Colonial Pipeline Hackers
* Mystery Surrounds Labour Party Ransomware Attack
* Microsoft Just Expanded Its Malware Protection For Linux Servers
* US Indicts UK Resident PlugwalkJoe For Cryptocurrency Theft
* Remote Code Execution Flaw Patched In Linux Kernel TIPC Module
* Senate Panel Passes Slew Of Cybersecurity Bills
* Ukraine Doxes Russian Government Hackers' Phone Calls
* Code Compiled To WebAssembly May Lack Standard Security Defenses
* Almost Half Of Rootkits Are Used Against Government Organizations
* Squid Game Crypto Scammers Rips Off Investors For Millions
* US Sanctions Could Cut Off NSO From Tech It Relies On
* Facebook To Shutdown Facial Recognition System And Delete 1 Billion Faceprints
* New Federal Order Narrows Agency Patching Focus To Known, Exploited Vulnerabilities
* Google Just Tripled Its Bounty For Linux Kernel Bugs
* Pirate Sports Streamer Gets Busted, Pivots To Extortion
* Trojan Source Hides Invisible Bugs In Source Code
* The Booming Underground Market For Bots That Steal Your 2FA Codes
* Android Has Its Head In The Sand With AbstractEmu Malware
* Signal Unveils How Far US Law Enforcement Will Go To Get Information About People
* Microsoft Found A Way To Evade SIP On macOS
* China's Personal Data Protection Law Kicks In Today
* Ransomware Has Disrupted Almost 1,000 Schools In The US This Year
* Suspected REvil Gang Insider Identified

**Krebs on Security**

* 'Tis the Season for the Wayward Package Phish
* The 'Groove' Ransomware Gang Was a Hoax
* 'Trojan Source' Bug Threatens the Security of All Code
* Zales.com Leaked Customer Data, Just Like Sister Firms Jared, Kay Jewelers Did in 2018
* FBI Raids Chinese Point-of-Sale Giant PAX Technology
* Conti Ransom Gang Starts Selling Access to Victims
* Missouri Governor Vows to Prosecute St. Louis Post-Dispatch for Reporting Security Vulnerability
* How Coinbase Phishers Steal One-Time Passwords
* Patch Tuesday, October 2021 Edition
* What Happened to Facebook, Instagram, & WhatsApp?


**Dark Reading**

* 3 Ways to Deal With the Trojan Source Attack
* SecureAuth Buys Acceptto to Deliver Low-Friction Authentication to Enterprises
* US Defense Contractor Discloses Data Breach
* Who's Minding Your Company's Crypto Decisions?
* How InfoSec Should Use the Minimum Viable Secure Product Checklist
* To Secure DevOps, Security Teams Must be Agile
* 4 Tips on How Small to Midsize Businesses Can Combat Cyberattacks
* How Is Zero Trust Different From Traditional Security?
* API Security Issues Hinder Application Delivery
* Ripping Off the Blindfold: Illuminating OT Environments
* US Offers $10M Reward For ID, Location of DarkSide Leadership
* Phishing Attack Blends Spoofed Amazon Order and Fraudulent Customer Service Agents
* Appsian Security Announces Acquisition of Q Software, a Leader in JD Edwards Security and Compliance
* Having Trouble Finding Cybersecurity Talent? You Might Be the Problem
* Coalfire Expands Application Security Vision With Major Upgrade to Application Security Platform, Thr
* How to Avoid Another Let's Encrypt-Like Meltdown
* Researchers Scan the Web to Uncover Malware Infections
* CISA Issues New Directive for Patching Known Exploited Vulnerabilities
* 5 MITRE ATT&CK Tactics Most Frequently Detected by Cisco Secure Firewalls
* Cloud Data Security Startup Launches

**The Hacker News**

* BlackBerry Uncovers Initial Access Broker Linked to 3 Distinct Hacker Groups
* Types of Penetration Testing
* Critical Flaws in Philips TASY EMR Could Expose Patient Data
* Two NPM Packages With 22 Million Weekly Downloads Found Backdoored
* Ukraine Identifies Russian FSB Officers Hacking As Gamaredon Group
* U.S. Federal Agencies Ordered to Patch Hundreds of Actively Exploited Flaws
* U.S. Offers $10 Million Reward for Information on DarkSide Ransomware Group
* Hardcoded SSH Key in Cisco Policy Suite Lets Remote Hackers Gain Root Access
* Critical RCE Vulnerability Reported in Linux Kernel's TIPC Module
* Our journey to API security at Raiffeisen Bank International
* US Sanctions Pegasus-maker NSO Group and 3 Others For Selling Spyware
* BlackMatter Ransomware Reportedly Shutting Down; Latest Analysis Released
* Product Overview - Cynet Centralized Log Management
* Mekotio Banking Trojan Resurfaces with New Attacking and Stealth Techniques
* Facebook to Shut Down Facial Recognition System and Delete Billions of Records


**Security Week**

* Six Arrested for Roles in Clop Ransomware Operation
* Report: 6 Palestinian Rights Activists Hacked by NSO Spyware
* Experts Analyze Proposed Bill Allowing Private Entities to 'Hack Back'
* The AP Interview: Justice Dept. Conducting Cyber Crackdown
* Babuk Ransomware Seen Exploiting ProxyShell Vulnerabilities
* 'Critical Severity' Warning: Malware Found in Widely Deployed npm Packages
* Device Exploits Earn Hackers Over $1 Million at Pwn2Own Austin 2021
* FBI: Scams Involving Cryptocurrency ATMs and QR Codes on the Rise
* Researchers Release PoC Tool Targeting BrakTooth Bluetooth Vulnerabilities
* Hungarian Official: Government Bought, Used Pegasus Spyware
* Industry Reactions to New 'Trojan Source' Attack: Feedback Friday
* US Offers $10 Million Bounty in Hunt for DarkSide Ransomware Operators
* Cisco Plugs Critical Holes in Catalyst PON Enterprise Switches
* Linux Foundation Fixes 'Dangerous' Code Execution Kernel Bug
* Mozilla Rolling Out 'Site Isolation' With Release of Firefox 94
* Ukraine Names Russian FSB Officers Involved in Gamaredon Cyberattacks
* Engaging Customers on an Uncertain Journey
* House Passes Two Bills to Improve Small Business Cybersecurity
* Compliance-as-a-Service Platform Laika Raises $35 Million
* Twitter Hacker Charged Over Theft of $784,000 in Cryptocurrency
* US Puts New Controls on Israeli Spyware Company NSO Group
* Application Security Startup Wabbi Raises Over $2 Million in Seed Funding
* BlackMatter Ransomware Gang Announces Shutdown
* Microsoft Announces New Endpoint Security Solution for SMBs
* CISA Lists 300 Exploited Vulnerabilities That Organizations Need to Patch

**Infosecurity Magazine**


**KnowBe4 Security Awareness Training Blog RSS Feed**

* Preparing for Black Friday Scams
* How Not To Get Phished: It Is the Message Not the Medium
* Your KnowBe4 Fresh Content Updates from October 2021
* FBI Warns that Financial Events are Occasions for Extortion
* CyberheistNews Vol 11 #43 [HEADS UP] Nuclear Ransomware 3.0: It Is About To Get Much Worse
* Not that You Would, but Looking for a Sugar Daddy's a Bad Idea
* Hacking Your Organization: 7 Steps Cybercriminals Use to Take Total Control of Your Network
* Misconceptions and Assumptions about Cybersecurity
* Multi-Stage Vishing Attacks are Coming to an Inbox Near You
* Eight Romance Phishing Scammers with Ties to Nigerian Organized Crime Arrested After Stealing Nearly

**ISC2.org Blog**

* We Heard You: Updates to the (ISC)² Ethics Questions
* CCSP vs. Microsoft Certified: Azure Administrator Associate - How Does Vendor Focus Factor In?
* CISSPs from Around the Globe: An Interview with Dr. Christina Izuakor
* The Threat of Insecure Interfaces and APIs
* Meet Roela Santos, Honoree of the 2021 (ISC)² Julie Peeler Franz "Do It for The Children" Volunt

**HackRead**

* Is a Consolidated Approach Better for WAAP Security?
* Twitter hacker charged in sim swapping, cryptocurrency scheme
* Top 10 Things Everyone Should be Doing During Development
* US offers $10m reward for decisive info on DarkSide ransomware gang
* Ransom fail: Iranian hackers leak trove of Israeli LGBTQ dating app data
* BlackMatter ransomware gang is reportedly quitting operation
* Facebook to end facial recognition and delete billions of records

**Koddos**

* Is a Consolidated Approach Better for WAAP Security?
* Twitter hacker charged in sim swapping, cryptocurrency scheme
* Top 10 Things Everyone Should be Doing During Development
* US offers $10m reward for decisive info on DarkSide ransomware gang
* Ransom fail: Iranian hackers leak trove of Israeli LGBTQ dating app data
* BlackMatter ransomware gang is reportedly quitting operation
* Facebook to end facial recognition and delete billions of records


**Naked Security**

* "Customer complaint" email scam preys on your fear of getting into trouble at work
* S3 Ep57: Europol v. Ransomware, Shrootless bug, and Linux browser flamewars [Podcast]
* Facebook to throw out face recognition, delete all template data
* Europol announces "targeting" of 12 suspects in ransomware attacks
* Microsoft documents "SHROOTLESS" hack patched in latest Apple updates
* Microsoft Edge finally arrives on Linux - "Official" build lands in repos
* S3 Ep56: Cryptotrading rodent, ransomware hackback, and a Docusign phish [Podcast]
* Apple ships Monterey with security updates, fixes 0-day in Watch and TV products, updates iDevices
* Banking scam uses Docusign phish to thieve 2FA codes
* Cybersecurity Awareness Month: Listen up - CYBERSECURITY FIRST!

**Threat Post**

* Native Tribal Casinos Taking Millions in Ransomware Losses
* BrakTooth Bluetooth Bugs Bite: Exploit Code, PoC Released
* Beyond the Basics: Tips for Building Advanced Ransomware Resiliency
* Google Ads for Faux Cryptowallets Net Scammers At Least $500K
* Proofpoint Phish Harvests Microsoft O365, Google Logins
* Feds Offer $10 Million Bounty for DarkSide Info
* US Bans Trade With Pegasus Spyware Maker
* 3 Guideposts for Building a Better Incident-Response Plan
* Free Discord Nitro Offer Used to Steal Steam Credentials
* Critical Linux Kernel Bug Allows Remote Takeover

**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**

* Zero Trust: What NIST's Guidelines Mean for Your Resources
* How to Deal With Unpatched Software Vulnerabilities Right Now
* 6 Potential Long-Term Impacts of a Data Breach
* Non-Traditional Cybersecurity Career Paths - One Experience Informs Another
* Maritime Cybersecurity: A Rising Tide Lifts all Boats
* Report: Cost of a Data Breach in Energy and Utilities
* An Attack Against Time
* Using Open-Source Intelligence for Mergers and Acquisitions
* Taking Threat Detection and Response to the Next Level with Open XDR
* The Future of Cybersecurity: What Will it Look Like in 2031?

**InfoWorld**

* All your serverless are belong to us
* GitHub Copilot preview gives me hope
* The case against monorepos
* More evidence we're in a multicloud world
* How to improve StringBuilder performance in C#
* The RED method: A new strategy for monitoring microservices
* How to use Docker for Java development
* What's new in Angular 13
* GitHub introduces code review controls
* TypeScript delays ESM support for Node.js

**C4ISRNET - Media for the Intelligence Age Military**

* Webcast: The Future of Ground Systems
* The Army wants to change how it sustains critical technology and communications gear
* Find out what's in the cyberwarrior's toolkit
* DoD unveils next iteration of sprawling cybersecurity initiative
* General Dynamics' Europe team dips into remote-controlled vehicles, ground robots
* No updated software, not mission capable. Army looks to include software for unit readiness reporting
* Space sector exec: Spain must stand out among its neighbors in nascent domain
* National Reconnaissance Office wants satellite imagery from commercial providers
* Marine Corps will use AI to revamp recruiting and retention models
* NATO ups the ante on disruptive tech, artificial intelligence

# The Hacker Corner

**Conferences**

* Marketing Cybersecurity In 2021
* Cybersecurity Employment Market
* Cybersecurity Marketing Trends
* Is It Worth Public Speaking?
* Our Guide To Cybersecurity Marketing Campaigns
* How To Choose A Cybersecurity Marketing Agency
* The "New" Conference Concept: The Hybrid
* Best Ways To Market A Conference
* Marketing To Cybersecurity Companies
* Upcoming Black Hat Events (2021)

**Google Zero Day Project**

* Windows Exploitation Tricks: Relaying DCOM Authentication
* Using Kerberos for Authentication Relay Attacks

**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.

* HK Cyber Security New Generation CTF Challenge 2021
* Winja CTF | c0c0n 2021
* K3RN3LCTF
* CSAW CTF Final Round 2021
* JUST CTF 2021
* Intent CTF 2021
* SPbCTF's Student CTF 2021 Finals
* MetaRed International CTF 2021 - 4th STAGE
* Hackfest CTF 13th Edition - Competitive
* N1CTF 2021

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

* Web Machine: (N7)
* The Planets: Earth
* Jangow: 1.0.1
* Red: 1
* Napping: 1.0.1

# Tools & Techniques

### Packet Storm Security Tools Links

* Faraday 3.18.1
* Clam AntiVirus Toolkit 0.104.1
* GRAudit Grep Auditing Tool 3.2
* TOR Virtual Network Tunneling Tool 0.4.6.8
* Zeek 4.1.1
* GNU Privacy Guard 2.3.3
* GNU Privacy Guard 2.2.32
* Faraday 3.18.0
* AntiRansom 5
* nfstream 6.3.5

### Kali Linux Tutorials

* SubCrawl : A Modular Framework For Discovering Open Directories, Identifying Unique Content Through S
* PowerShx : Run Powershell Without Software Restrictions
* PortBender : TCP Port Redirection Utility
* PEASS-ng : Privilege Escalation Awesome Scripts SUITE new generation
* Metabadger : Prevent SSRF Attacks On AWS EC2 Via Automated Upgrades To The More Secure Instance Metad
* How to Detect and Prevent Brute Force Attacks?
* Benefits & Drawbacks of Open-Source Software
* Limelighter : A Tool For Generating Fake Code Signing Certificates Or Signing Real Ones
* LazyCSRF : A More Useful CSRF PoC Generator
* Karma_V2 : A Passive Open Source Intelligence (OSINT) Automated Reconnaissance (Framework)

### GBHackers Analysis

* Hackers Exploit Microsoft Exchange Vulnerabilities To Drop Babuk Ransomware
* Unauthenticated RCE Flaw in Gitlab Exploited Widely by Hackers
* Two European Men Sentenced for Providing 'Bulletproof Hosting' to Hackers
* Iranian Hackers Attack the US & Israeli Defense Technology - Microsoft Warns
* Company That Routes Billions of SMS For U.S Carriers Silently Says It Was Hacked

# Weekly Cyber Security Video and Podcasts

**SANS DFIR**

* Hunting and Scoping A Ransomware Attack
* Compose Your Hunts With Reusable Knowledge and Share Your Huntbook With the Community
* Hunting backdoors in Active Directory Environment
* AC3 Threat Sightings: El Poder de la Observación

**Defcon Conference**

* DEF CON 29 Recon Village - Anthony Kava - GOV Doppelgänger Your Häx Dollars at Work
* DEF CON 29 Red Team Village -  CTF Day 2
* DEF CON 29 Recon Village - Ben S -  Future of Asset Management
* DEF CON 29 Recon Village - Ryan Elkins - How to Build Cloud Based Recon Automation at Scale

**Hak5**

* Copy Files from an Unlocked Computer In Seconds w/ the Bash Bunny | HakByte
* CyberAttackers Use Squid Game To Lure In Victims  - ThreatWire
* Spot Known WiFi Devices Nearby w/ the WiFi Nugget | HakByte

**The PC Security Channel [TPSC]**

* Windows 11 vs Ransomware
* Vice Society Ransomware & Print Nightmare

**Eli the Computer Guy**

* OSHA IGNORING VACCINE REACTIONS for EMPLOYERS
* BIDEN PUNISHES ANTIVAXERS - INSANE FINES from OSHA
* ZILLOW LAYOFFS - 2000 employees FIRED
* TESLA AUTOPILOT SYSTEM CRASH... glitches at 70 mph..?

**Security Now**

* "Trojan Source” - Chrome 0-days, Windows 11 confusion, VoIP DDos attacks, Dune
* The More Things Change... - Gummy Browsers Attack, What Happened to REvil, Comms Hub, Win 11 Fixes

**Troy Hunt**

* Weekly Update 268

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

* 240-Privacy, Security, & OSINT Updates
* 239-Health Portals, Vulnerability Reports, and Voice Cloning


# Proof of Concept (PoC) & Exploits

### Packet Storm Security

* Pentaho Business Analytics / Pentaho Business Server 9.1 SQL Injection
* HealthForYou 1.11.1 / HealthCoach 2.9.2 Missing Password Policy
* Pentaho Business Analytics / Pentaho Business Server 9.1 User Enumeration
* Backdoor.Win32.Jokerdoor Buffer Overflow
* Pentaho Business Analytics / Pentaho Business Server 9.1 Authentication Bypass
* PHP Event Calendar Lite Edition Cross Site Scripting
* IBM Sterling B2B Integrator Cross Site Scripting
* Backdoor.Win32.Ncx.b Code Execution
* ImportExportTools NG 10.0.4 HTML Injection
* Pentaho Business Analytics / Pentaho Business Server 9.1 Insufficient Access Control
* PHP Event Calendar Lite Edition SQL Injection
* Backdoor.Win32.Ncx.b Buffer Overflow
* Pentaho Business Analytics / Pentaho Business Server 9.1 Filename Bypass
* Payment Terminal 2.x / 3.x Cross Site Scripting
* Pentaho Business Analytics / Pentaho Business Server 9.1 Remote Code Execution
* 10-Strike Network Inventory Explorer Pro 9.31 Unquoted Service Path
* Backdoor.Win32.Optix.03.b Code Execution
* Khamenei.ir SQL Injection
* GitLab Unauthenticated Remote ExifTool Command Injection
* Opencart 3 Extension TMD Vendor System SQL Injection
* Fuel CMS 1.4.1 Remote Code Execution
* i3 International Annexxus Cameras Ax-n 5.2.0 Application Logic Flaw
* Ericsson Network Location MPS GMPC21 Privilege Escalation
* Ericsson Network Location MPS GMPC21 Remote Code Execution
* Dynojet Power Core 2.3.0 Unquoted Service Path

### CXSecurity

* Fuel CMS 1.4.1 Remote Code Execution
* GitLab Unauthenticated Remote ExifTool Command Injection
* Opencart 3 Extension TMD Vendor System SQL Injection
* YouTube Video Grabber 1.9.9.1 Buffer Overflow
* Apache HTTP Server 2.4.50 Remote Code Execution
* Sophos UTM WebAdmin SID Command Injection
* Druva inSync Windows Client 7.5.2 - Local Privilege Escalation


# Proof of Concept (PoC) & Exploits

### Exploit Database

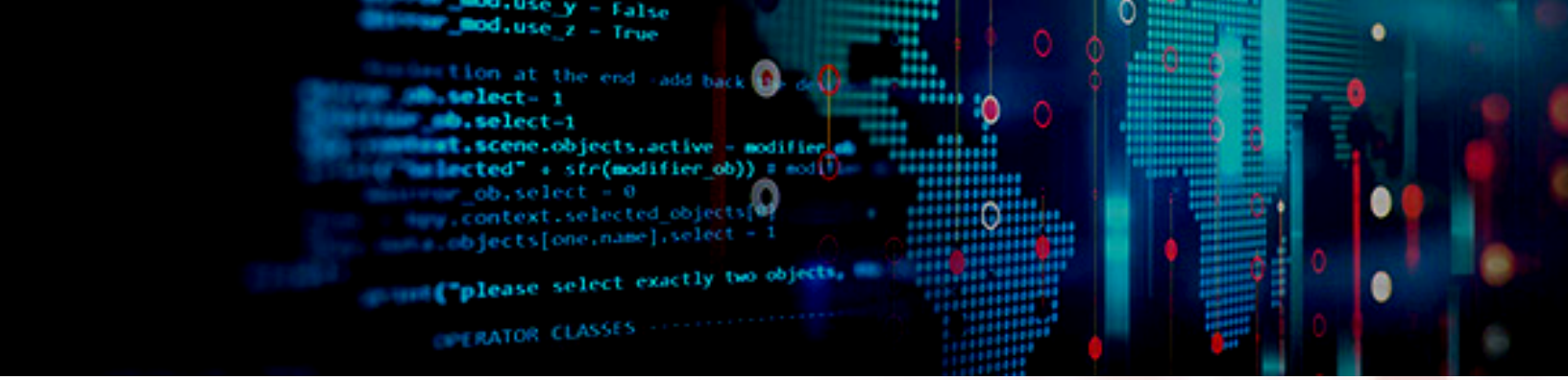
* [webapps] FusionPBX 4.5.29 - Remote Code Execution (RCE) (Authenticated)
* [local] zlog 1.2.15 - Buffer Overflow
* [webapps] WordPress Plugin Backup and Restore 1.0.3 - Arbitrary File Deletion
* [webapps] Froxlor 0.10.29.1 - SQL Injection (Authenticated)
* [webapps] Money Transfer Management System 1.0 - Authentication Bypass
* [webapps] Kmaleon 1.1.0.205 - 'tipocomb' SQL Injection (Authenticated)
* [webapps] Simple Client Management System 1.0 - 'multiple' Stored Cross-Site Scripting (XSS)
* [webapps] Simple Client Management System 1.0 - SQLi (Authentication Bypass)
* [webapps] ImportExportTools NG 10.0.4 - HTML Injection
* [webapps] Payment Terminal 3.1 - 'Multiple' Cross-Site Scripting (XSS)
* [local] 10-Strike Network Inventory Explorer Pro 9.31 - 'srvInventoryWebServer' Unquoted Service Path
* [webapps] Opencart 3 Extension TMD Vendor System - Blind SQL Injection
* [webapps] Ultimate POS 4.4 - 'name' Cross-Site Scripting (XSS)
* [webapps] Vanguard 2.1 - 'Search' Cross-Site Scripting (XSS)
* [webapps] Isshue Shopping Cart 3.5 - 'Title' Cross Site Scripting (XSS)
* [webapps] Mult-e-Cart Ultimate 2.4 - 'id' SQL Injection
* [webapps] PHP Melody 3.0 - Persistent Cross-Site Scripting (XSS)
* [webapps] PHP Melody 3.0 - 'vid' SQL Injection
* [webapps] PHP Melody 3.0 - 'Multiple' Cross-Site Scripting (XSS)
* [webapps] Sonicwall SonicOS 6.5.4 - 'Common Name' Cross-Site Scripting (XSS)
* [local] RDP Manager 4.9.9.3 - Denial-of-Service (PoC)
* [webapps] Simplephpscripts Simple CMS 2.1 - 'Multiple' SQL Injection
* [webapps] Simplephpscripts Simple CMS 2.1 - 'Multiple' Stored Cross-Site Scripting (XSS)
* [webapps] OpenAM 13.0 - LDAP Injection
* [webapps] WordPress Plugin Popup Anything 2.0.3 - 'Multiple' Stored Cross-Site Scripting (XSS)

### Exploit Database for offline use

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

user@yourlinux:~$ *searchsploit keyword1 keyword2*

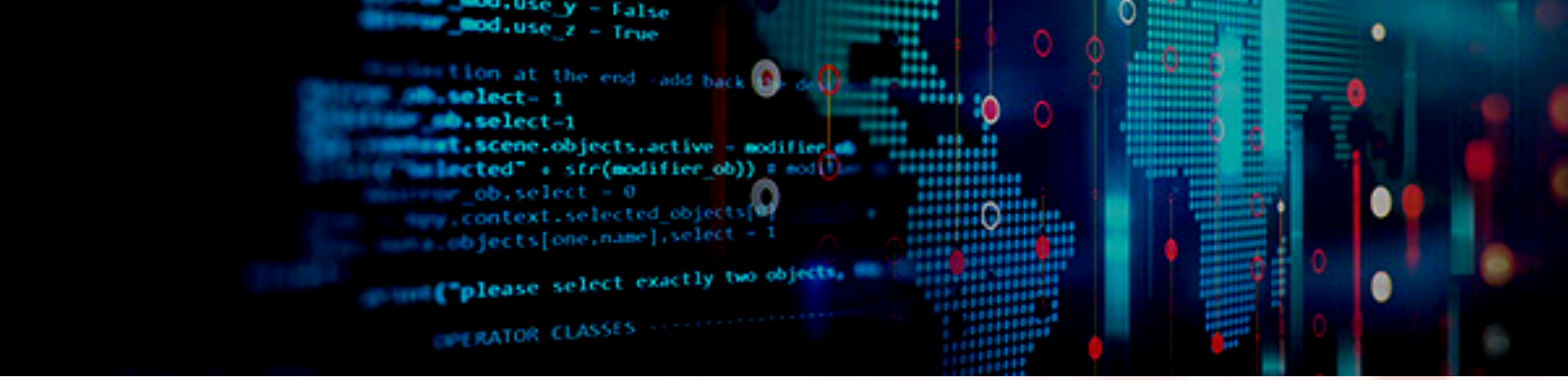
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



# Latest Hacked Websites

**Published on Zone-h.org**

http://arsip.pa-purwodadi.go.id/try.txt
http://arsip.pa-purwodadi.go.id/try.txt notified by DuaL_Personal
http://sipp.pa-purwodadi.go.id/try.txt
http://sipp.pa-purwodadi.go.id/try.txt notified by DuaL_Personal
http://sipp.pa-bangkinang.go.id/try.txt
http://sipp.pa-bangkinang.go.id/try.txt notified by DuaL_Personal
http://pustakaonline.pa-bangkinang.go.id/try.txt
http://pustakaonline.pa-bangkinang.go.id/try.txt notified by DuaL_Personal
http://sipp.pa-kediri.go.id/try.txt
http://sipp.pa-kediri.go.id/try.txt notified by DuaL_Personal
http://disnakerin.majalengkakab.go.id
http://disnakerin.majalengkakab.go.id notified by Unknown Al
https://www.mf.gov.dz
https://www.mf.gov.dz notified by Moroccan Revolution
http://dgpp-mf.gov.dz
http://dgpp-mf.gov.dz notified by Moroccan Revolution
https://damancgst.gov.in/z.html
https://damancgst.gov.in/z.html notified by Zer0FauLT
http://www.irmnch.gop.pk/slep.html
http://www.irmnch.gop.pk/slep.html notified by Mr.Kro0oz.305
http://kthospital.gov.sd
http://kthospital.gov.sd notified by Mloki
https://www.galya.go.th/0x.txt
https://www.galya.go.th/0x.txt notified by ./unn0rmaL
http://bumiayu-selopampang.temanggungkab.go.id/ar.html
http://bumiayu-selopampang.temanggungkab.go.id/ar.html notified by Unknown Al ∞
http://bojong-tretep.temanggungkab.go.id/ar.html
http://bojong-tretep.temanggungkab.go.id/ar.html notified by Unknown Al ∞
http://bonjor-tretep.temanggungkab.go.id/ar.html
http://bonjor-tretep.temanggungkab.go.id/ar.html notified by Unknown Al ∞
http://butuh-temanggung.temanggungkab.go.id/ar.html
http://butuh-temanggung.temanggungkab.go.id/ar.html notified by Unknown Al ∞
http://bulu-bulu.temanggungkab.go.id/ar.html
http://bulu-bulu.temanggungkab.go.id/ar.html notified by Unknown Al ∞



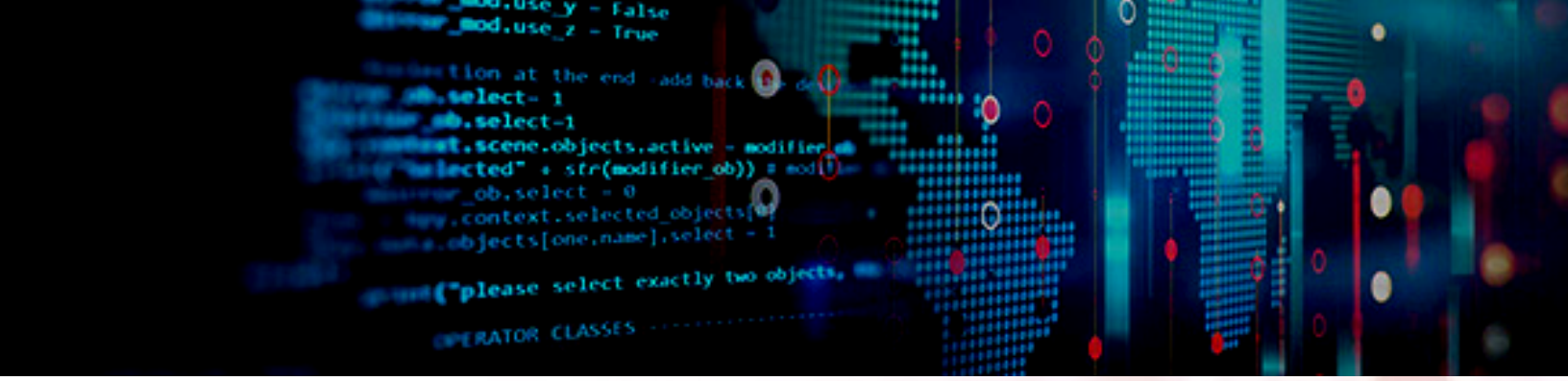
# Dark Web News

**Darknet Live**

West Virginia Man Sentenced to Prison for Reselling Meth
A West Virginia man was sentenced to 120 months in prison for selling methamphetamine purchased on the darkweb. (via darknetlive.com)
StExo Ordered to Forfeit Â£490,000 in Bitcoin
Thomas White, one of the people responsible for creating Silk Road 2.0, was ordered to forfeit Â£493,550 in Bitcoin. (via darknetlive.com)
Tennessee Man Pleads Guilty to a Murder-for-hire Plot
A retired teacher pleaded guilty to attempting to hire a hitman on the dark web to kill his wife. (via darknetlive.com)
Virginia Woman Arrested for Trying to Hire a Hitman
Authorities in Virginia arrested a woman for allegedly trying to hire a hitman on the darkweb. (via darknetlive.com)

**Dark Web Link**

White House Market Plans Retirement: What Important Things You Missed?
One of the latest darknet markets that accepted monero (XMR) as their payment modes have announced their retirement. The dark web market is none other than White House Market (WHM). As soon as the White House Market plans retirement and the news went live, there has been chaos all over the darknet sphere and there [...] The post White House Market Plans Retirement: What Important Things You Missed? appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Faucibarriers Against 'Dark Web People' Distressing His Daughters And Wife With Vicious Threats
Dr. Anthony Fauci's life and career are chronicled in a new National Geographic documentary. Fauci rails about pestering phone calls from “Dark web” persons in the film.Dr. Anthony Fauci grew up in Brooklyn's Bensonhurst neighbourhood, where he learnt early on that “you didn't take any shit from anyone.” During the HIV/AIDS crisis in the United [...] The post Faucibarriers Against 'Dark Web People' Distressing His Daughters And Wife With Vicious Threats appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Onionshare: Safe Communications Stand Used By Journalists And Whistleblowers Covers Data Exposure Bug
Two flaws in a technology used by whistleblowers and the media to securely communicate material have been addressed, potentially jeopardising the file-sharing system's anonymity. OnionShare is an open source utility for Windows, macOS, and Linux that allows users to remain anonymous while doing things like file sharing, hosting websites, and communicating. The service, which is [...] The post Onionshare: Safe Communications Stand Used By Journalists And Whistleblowers Covers Data Exposure Bug appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



## Trend Micro Anti-Malware Blog

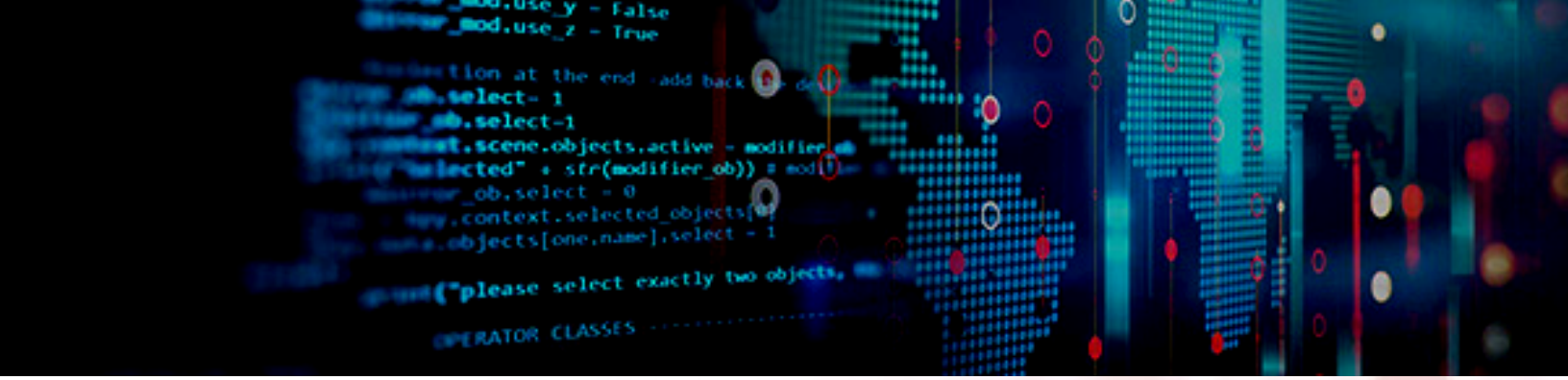
* Our New Blog
* How Unsecure gRPC Implementations Can Compromise APIs, Applications
* XCSSET Mac Malware: Infects Xcode Projects, Performs UXSS Attack on Safari, Other Browsers, Leverages
* August Patch Tuesday Fixes Critical IE, Important Windows Vulnerabilities Exploited in the Wild
* Water Nue Phishing Campaign Targets C-Suite's Office 365 Accounts
* Mirai Botnet Exploit Weaponized to Attack IoT Devices via CVE-2020-5902
* Ensiko: A Webshell With Ransomware Capabilities
* Updates on ThiefQuest, the Quickly-Evolving macOS Malware
* Patch Tuesday: Fixes for 'Wormable' Windows DNS Server RCE, SharePoint Flaws
* New Mirai Variant Expands Arsenal, Exploits CVE-2020-10173

## RiskIQ

*Unfortunately, at the time of this report, the RiskIQ resource was not availible.*

## FireEye

* Metasploit Wrap-Up
* New NPM library hijacks (coa and rc)
* 2022 Planning: The Path to Effective Cybersecurity Maturity
* Trojan Source CVE-2021-42572: No Panic Necessary
* Hands-On IoT Hacking: Rapid7 at DefCon 29 IoT Village, Part 3
* [Security Nation] Pete Cooper and Irene Pontisso of the UK Cabinet Office on Their Cybersecurity Cult
* Building Threat-Informed Defenses: Rapid7 Experts Share Their Thoughts on MITRE ATT&CK
* InsightVM Scan Diagnostics: Troubleshooting Credential Issues for Authenticated Scanning
* A Matter of Perspective: Agent-Based and Agentless Approaches to Cloud Security, Part 2
* Solving the Access Goldilocks Problem: RBAC for InsightAppSec Is Here



# Advisories

**US-Cert Alerts & bulletins**

* BrakTooth Proof of Concept Tool Demonstrates Bluetooth Vulnerabilities
* Cisco Releases Security Updates for Multiple Products
* FBI Releases PIN on Attacks Using Significant Financial Events for Extortion
* Mozilla Releases Security Updates for Firefox, Firefox ESR, and Thunderbird
* CISA Issues BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities
* Google Releases Security Updates for Chrome
* GoCD Authentication Vulnerability
* NSA-CISA Series on Securing 5G Cloud Infrastructures
* AA21-291A: BlackMatter Ransomware
* AA21-287A: Ongoing Cyber Threats to U.S. Water and Wastewater Systems
* Vulnerability Summary for the Week of October 25, 2021
* Vulnerability Summary for the Week of October 18, 2021

**Zero Day Initiative Advisories**

ZDI-CAN-15671: Autodesk
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-10-29, 10 days ago. The vendor is given until 2022-02-26 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-15667: Autodesk
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-10-29, 10 days ago. The vendor is given until 2022-02-26 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-15449: 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 'chudy' was reported to the affected vendor on: 2021-10-29, 10 days ago. The vendor is given until 2022-02-26 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-15448: 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 'chudy' was reported to the affected vendor on: 2021-10-29, 10 days ago. The vendor is given until 2022-02-26 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-15665: Autodesk
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-10-29, 10 days ago. The vendor

is given until 2022-02-26 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-15668: Autodesk

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-10-29, 10 days ago. The vendor is given until 2022-02-26 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-15669: Autodesk

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-10-29, 10 days ago. The vendor is given until 2022-02-26 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-15664: Autodesk

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-10-29, 10 days ago. The vendor is given until 2022-02-26 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-15666: Autodesk

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2021-10-29, 10 days ago. The vendor is given until 2022-02-26 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-15296: Microsoft

A CVSS score 6.1 (AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'Abdelhamid Naceri' was reported to the affected vendor on: 2021-10-27, 12 days ago. The vendor is given until 2022-02-24 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-15587: Microsoft

A CVSS score 7.2 (AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Zymo Security' was reported to the affected vendor on: 2021-10-27, 12 days ago. The vendor is given until 2022-02-24 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-15187: Microsoft

A CVSS score 2.7 (AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Alex Birnberg of Zymo Security' was reported to the affected vendor on: 2021-10-27, 12 days ago. The vendor is given until 2022-02-24 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-15446: Microsoft

A CVSS score 4.7 (AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Zymo Security' was reported to the affected vendor on: 2021-10-27, 12 days ago. The vendor is given until 2022-02-24 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-15522: Autodesk

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-10-27, 12 days ago. The vendor is given until 2022-02-24 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-15443: Microsoft

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 'Thomas

Bouzerar (@MajorTomSec) from Synacktiv (@Synacktiv)' was reported to the affected vendor on: 2021-10-27, 12 days ago. The vendor is given until 2022-02-24 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-15047: Trend Micro

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 'Elias Martinez (filenotfound - https://www.linkedin.com/in/eli-martinez07/)' was reported to the affected vendor on: 2021-10-27, 12 days ago. The vendor is given until 2022-02-24 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-15585: Microsoft

A CVSS score 2.5 (AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Jaanus K\xc3\xa4\xc3\xa4p, Clarified Security' was reported to the affected vendor on: 2021-10-27, 12 days ago. The vendor is given until 2022-02-24 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-15521: Autodesk

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2021-10-27, 12 days ago. The vendor is given until 2022-02-24 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-15445: Microsoft

A CVSS score 2.2 (AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Zymo Security' was reported to the affected vendor on: 2021-10-27, 12 days ago. The vendor is given until 2022-02-24 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-15675: Autodesk

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2021-10-27, 12 days ago. The vendor is given until 2022-02-24 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-14740: Orckestra

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 'Le Ngoc Anh - Sun* Cyber Security Research Team' was reported to the affected vendor on: 2021-10-25, 14 days ago. The vendor is given until 2022-02-22 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-15056: xhyve

A CVSS score 7.5 (AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Alisa Esage of Zero Day Engineering (zerodayengineering.com)' was reported to the affected vendor on: 2021-10-22, 17 days ago. The vendor is given until 2022-02-19 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-15541: WordPress

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 'ngocnb and khuyenn from GiaoHangTietKiem JSC' was reported to the affected vendor on: 2021-10-22, 17 days ago. The vendor is given until 2022-02-19 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-15301: Ivanti

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 'chudy' was reported to the affected vendor on: 2021-10-22, 17 days ago. The vendor is given until 2022-02-19 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

**Packet Storm Security - Latest Advisories**

Red Hat Security Advisory 2021-4134-01

Red Hat Security Advisory 2021-4134-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.3.0. Issues addressed include bypass, spoofing, and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-4130-01

Red Hat Security Advisory 2021-4130-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.3.0. Issues addressed include bypass, spoofing, and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-4132-01

Red Hat Security Advisory 2021-4132-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.3.0. Issues addressed include bypass, spoofing, and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-4133-01

Red Hat Security Advisory 2021-4133-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.3.0. Issues addressed include bypass, spoofing, and use-after-free vulnerabilities.

Ubuntu Security Notice USN-5132-1

Ubuntu Security Notice 5132-1 - Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, spoof another origin, or execute arbitrary code.

Red Hat Security Advisory 2021-4008-01

Red Hat Security Advisory 2021-4008-01 - 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 4.6.49.

Ubuntu Security Notice USN-5131-1

Ubuntu Security Notice 5131-1 - Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, bypass security restrictions, spoof the browser UI, confuse the user, conduct phishing attacks, or execute arbitrary code. It was discovered that the 'Copy Image Link' context menu action would copy the final image URL after redirects. If a user were tricked into copying and pasting a link for an embedded image that triggered authentication flows back to the page, an attacker could potentially exploit this to steal authentication tokens. Various other issues were also addressed.

Red Hat Security Advisory 2021-4123-01

Red Hat Security Advisory 2021-4123-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.3.0 ESR. Issues addressed include bypass, spoofing, and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-4122-01

Red Hat Security Advisory 2021-4122-01 - 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 use-after-free vulnerabilities.

Red Hat Security Advisory 2021-4116-01

Red Hat Security Advisory 2021-4116-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.3.0 ESR. Issues addressed include bypass, spoofing, and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-4112-01

Red Hat Security Advisory 2021-4112-01 - The Advanced Virtualization module provides the user-space component for running virtual machines that use KVM in environments managed by Red Hat products. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2021-4107-01

Red Hat Security Advisory 2021-4107-01 - Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. Issues addressed include a bypass vulnerability.

Red Hat Security Advisory 2021-4106-01

Red Hat Security Advisory 2021-4106-01 - Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. Issues addressed include a bypass vulnerability.

Red Hat Security Advisory 2021-4104-01

Red Hat Security Advisory 2021-4104-01 - OpenShift Virtualization is Red Hat's virtualization solution designed for Red Hat OpenShift Container Platform.

Red Hat Security Advisory 2021-4103-01

Red Hat Security Advisory 2021-4103-01 - OpenShift Virtualization is Red Hat's virtualization solution designed for Red Hat OpenShift Container Platform. This advisory contains OpenShift Virtualization 4.9.0 RPMs. Issues addressed include a denial of service vulnerability.

Ubuntu Security Notice USN-5128-1

Ubuntu Security Notice 5128-1 - Goutham Pacha Ravi, Jahson Babel, and John Garbutt discovered that user credentials in Ceph could be manipulated in certain environments. An attacker could use this to gain unintended access to resources. This issue only affected Ubuntu 18.04 LTS. It was discovered that Ceph contained an authentication flaw, leading to key reuse. An attacker could use this to cause a denial of service or possibly impersonate another user. This issue only affected Ubuntu 21.04. Various other issues were also addressed.

Red Hat Security Advisory 2021-4100-01

Red Hat Security Advisory 2021-4100-01 - This release of Red Hat Integration - Service registry 2.0.2.GA serves as a replacement for 2.0.1.GA, and includes the below security fixes. Issues addressed include a cross site scripting vulnerability.

Red Hat Security Advisory 2021-4097-01

Red Hat Security Advisory 2021-4097-01 - WebKitGTK is the port of the portable web rendering engine WebKit to the GTK platform. Issues addressed include code execution and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-4088-01

Red Hat Security Advisory 2021-4088-01 - The kernel-rt packages provide the Real Time Linux Kernel, which enables fine-tuning for systems with extremely high determinism requirements. Issues addressed include buffer overflow, out of bounds write, and use-after-free vulnerabilities.

Red Hat Security Advisory 2021-4089-01

Red Hat Security Advisory 2021-4089-01 - IBM Java SE version 8 includes the IBM Java Runtime Environment and the IBM Java Software Development Kit. This update upgrades IBM Java SE 8 to version 8 SR6-FP35.

Ubuntu Security Notice USN-5121-2

Ubuntu Security Notice 5121-2 - USN-5009-1 fixed vulnerabilities in Mailman. This update provides the corresponding updates for Ubuntu 20.04 LTS. It was discovered that Mailman allows arbitrary content injection. An attacker could use this to inject malicious content. It was discovered that Mailman improperly sanitize the MIME content. An attacker could obtain sensitive information by sending a special type of attachment.

Red Hat Security Advisory 2021-4057-01

Red Hat Security Advisory 2021-4057-01 - Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2021-4059-01

Red Hat Security Advisory 2021-4059-01 - The curl packages provide the libcurl library and the curl utility for downloading files from servers using various protocols, including HTTP, FTP, and LDAP.

Red Hat Security Advisory 2021-4058-01

Red Hat Security Advisory 2021-4058-01 - Samba is an open-source implementation of the Server Message

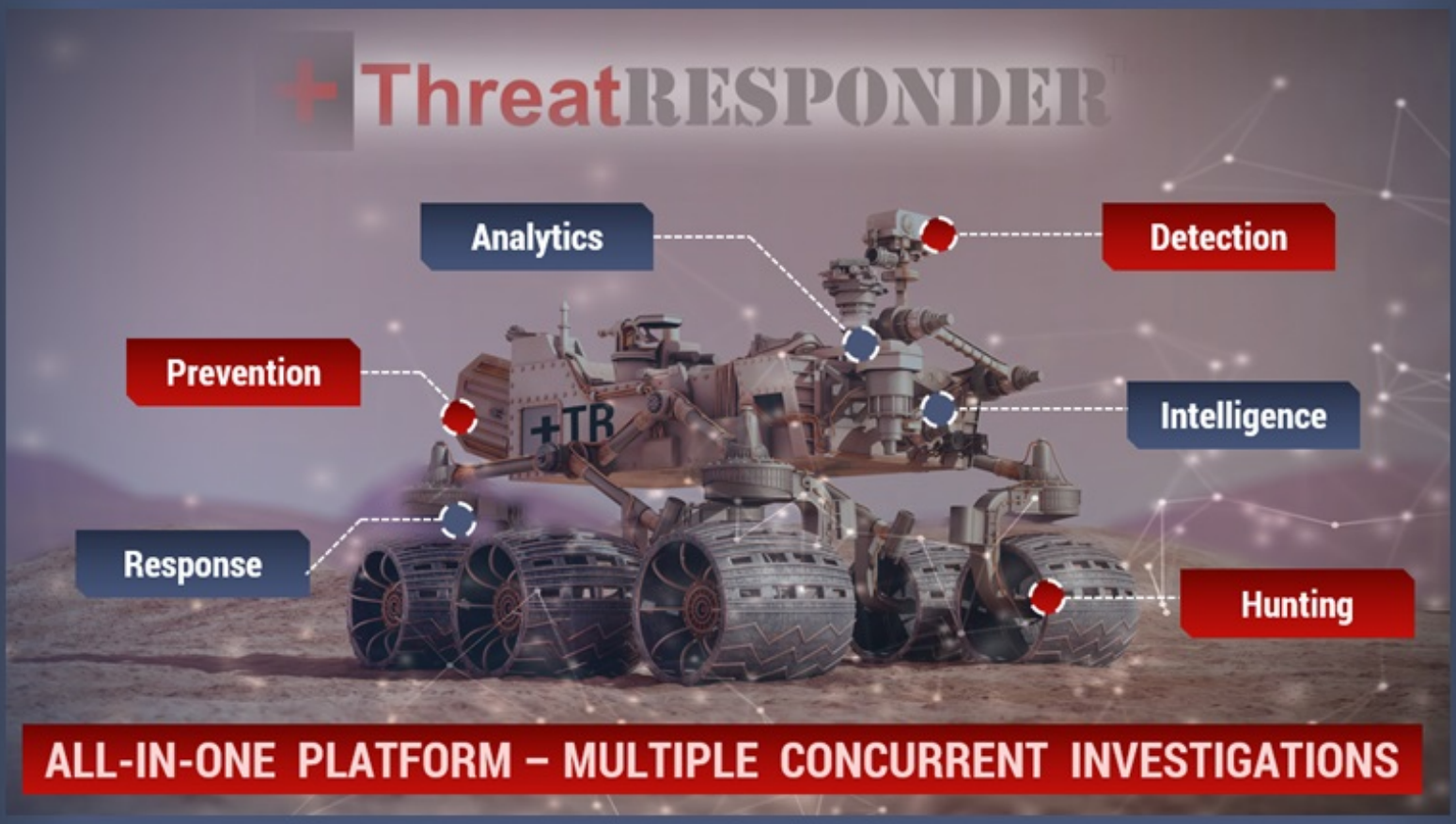
Block protocol and the related Common Internet File System protocol, which allow PC-compatible machines to share files, printers, and various information.

## 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



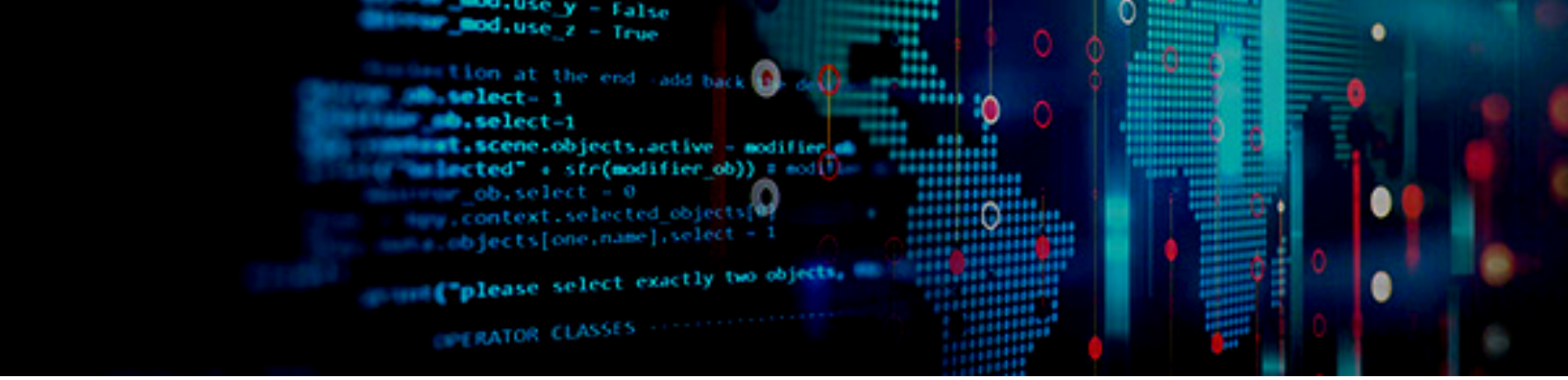

## The Solution – ThreatResponder® Platform

**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**

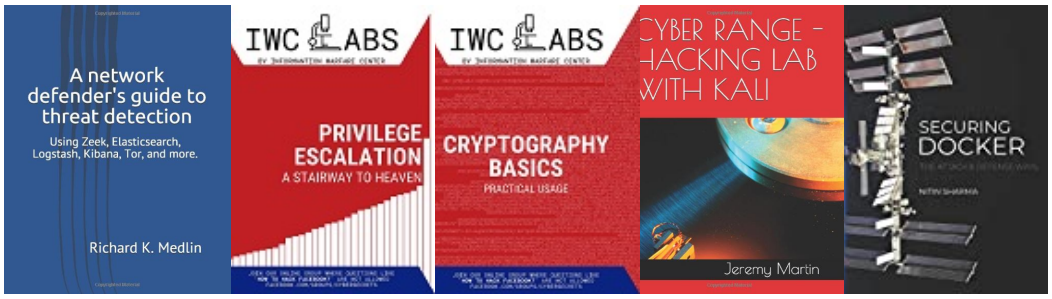


# The Cyber Secrets publications on Amazon

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