Dec-19-22

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

December 19, 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

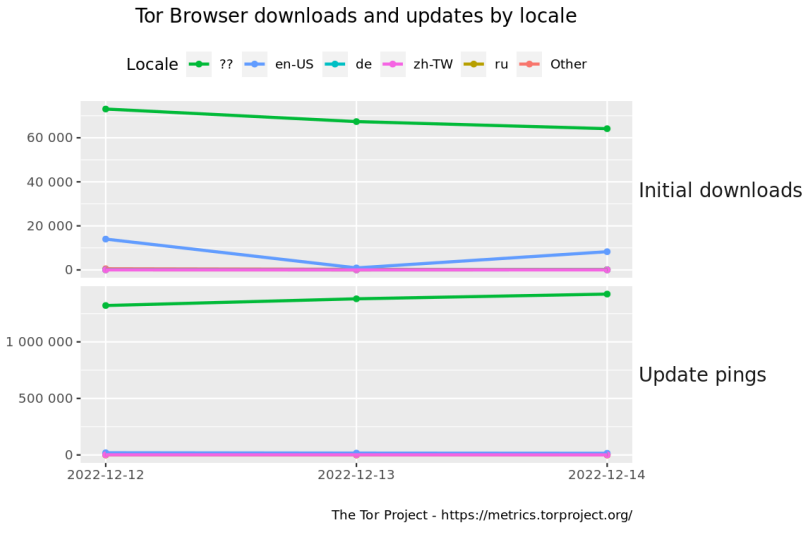
Internet Storm Center Infocon Status

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

Other IWC Publications

Cyber Secrets books and ebook series can be found on Amazon.com at. amzn.to/2UuIG9B

Cyber Secrets was originally a video series and is on both YouTube.



Interesting News

* Free Cyberforensics Training - CSI Linux Basics

Download the distro and take the course to learn what CSI Linux can add to your arsenal. This include a case management solution, document templates (reports and legal docs), and more GUI options for gathering digital evidence while storing it to the ongoing case.
https://training.csilinux.com/course/view.php?id=5

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

Index of Sections

Packet Storm Security

* 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
* FTX Crypto Boss Sam Bankman-Fried Denied Bail In Bahamas
* Google Launches New Tool To Identify Open Source Vulnerabilities
* Iran-Linked Charming Kitten Espionage Gang Phishing Politicians
* Elon Musk Takes Legal Action To Bully Student That Tracks His Plane With PUBLIC Data
* Microsoft Digital Certificates Have Once Again Been Abused To Sign Malware
* NSA Warns Chinese Hackers Are Exploiting Citrix Gear
* TPG Reveals Emails Of 15,000 iiNet / Westnet Customers Exposed In Hack
* Teqtivity Pwn Results In Uber Staff Info Leak
* Twitter Disbands Its Trust And Safety Council
* Binance Temporarily Pauses Withdrawals
* FTX Founder Charged With Fraud In Crypto Exchange's Collapse
* This Evasive New Cyberattack Can Bypass Air-Gapped Systems To Steal Data From The Most Sensitive Netw
* Pwn2Own Pays Out Almost $1m To Ethical Hackers
* Musk, The Anti-Censorship Crusader, Allegedly Shadowbanned An Account Tracking His Private Jet
* UK Arrests Five For Selling Dodgy Point Of Sale Software
* DOJ Divided Over Charging Binance Over Crypto Crimes

Krebs on Security

* 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
* Disneyland Malware Team: It's a Puny World After All
* Top Zeus Botnet Suspect "Tank" Arrested in Geneva

Dark Reading

* Sophisticated DarkTortilla Malware Serves Imposter Cisco, Grammarly Pages
* T-Mobile Carrier Scammer Gets Decade in the Slammer
* Threat Intelligence Through Web Scraping
* Fortnite Developer Epic Games Slapped With $275M Penalty
* Malicious Python Trojan Impersonates SentinelOne Security Client
* Security Skills Command Premiums in Tight Market
* Bugcrowd Launches Bug Bounty Program for Australian-Based Navitas
* Rethinking Risk After the FTX Debacle
* Holiday Spam, Phishing Campaigns Challenge Retailers
* GitHub Expands Secret Scanning, 2FA Across Platform
* Cyber Threats Loom as 5B People Prepare to Watch World Cup Final
* Researcher Bypasses Akamai WAF
* New Botnet Targeting Minecraft Servers Poses Potential Enterprise Threat
* FBI: Criminals Using BEC Attacks to Scavenge Food Shipments
* Organizations Unprepared for Upcoming Data Privacy Regulations
* With SASE Definition Still Cloudy, Forum Proposes Standard
* Iran-Backed Charming Kitten APT Eyes Kinetic Ops, Kidnapping
* Chinese APT Group MirrorFace Interferes in Japanese Elections
* Compliance Is Not Enough: How to Manage Your Customer Data
* Zero Trust in the Era of Edge

The Hacker News

* Researchers Discover Malicious PyPI Package Posing as SentinelOne SDK to Steal Data
* Glupteba Botnet Continues to Thrive Despite Google's Attempts to Disrupt It
* Cybercrime (and Security) Predictions for 2023
* New Agenda Ransomware Variant, Written in Rust, Aiming at Critical Infrastructure
* Facebook Cracks Down on Spyware Vendors from U.S., China, Russia, Israel, and India
* Google Takes Gmail Security to the Next Level with Client-Side Encryption
* Samba Issues Security Updates to Patch Multiple High-Severity Vulnerabilities
* Trojanized Windows 10 Installer Used in Cyberattacks Against Ukrainian Government Entities
* Ex-Twitter employee Gets 3.5 Years Jail for Spying on Behalf of Saudi Arabia
* Cyber Security Is Not a Losing Game - If You Start Right Now
* GitHub Announces Free Secret Scanning for All Public Repositories
* Goodbye SHA-1: NIST Retires 27-Year-Old Widely Used Cryptographic Algorithm
* Minecraft Servers Under Attack: Microsoft Warns About Cross-Platform DDoS Botnet
* CISA Alert: Veeam Backup and Replication Vulnerabilities Being Exploited in Attacks
* Researchers Uncover MirrorFace Cyber Attacks Targeting Japanese Political Entities

Security Week

* FoxIt Patches Code Execution Flaws in PDF Tools
* Malicious PyPI Module Poses as SentinelOne SDK
* Google Workspace Gets Client-Side Encryption in Gmail
* Cisco Warns of Many Old Vulnerabilities Being Exploited in Attacks
* Glupteba Botnet Still Active Despite Google's Disruption Efforts
* US Puts 3 Dozen More Chinese Companies on Trade Blacklist
* US Food Companies Warned of BEC Attacks Stealing Food Product Shipments
* NIST to Retire 27-Year-Old SHA-1 Cryptographic Algorithm
* GitHub Announces Free Secret Scanning, Mandatory 2FA
* Microsoft Reclassifies Windows Flaw After IBM Researcher Proves Remote Code Execution
* Social Blade Confirms Breach After Hacker Offers to Sell User Data
* Meta Paid Out $16 Million in Bug Bounties Since 2011
* Ex-Twitter Worker Gets Prison Time in Saudi 'Spy' Case
* API Security Firm FireTail Raises $5 Million
* Chinese Cyberspies Targeted Japanese Political Entities Ahead of Elections
* Email Hack Hits 15,000 Business Customers of Australian Telecoms Firm TPG
* Hacker Claims Breach of FBI's Critical-Infrastructure Portal
* US Charges Six in Operation Targeting 48 DDoS-for-Hire Websites
* US Government Agencies Issue Guidance on Threats to 5G Network Slicing
* CISA Warns Veeam Backup & Replication Vulnerabilities Exploited in Attacks
* Google Announces Vulnerability Scanner for Open Source Developers
* High-Severity Memory Safety Bugs Patched With Latest Chrome 108 Update
* SAP's December 2022 Security Updates Patch Critical Vulnerabilities
* Security Firms Warn Microsoft of Signed Drivers Used to Kill EDR, AV Processes
* EU Moves Closer to Sewing Up New Data Transfer Deal With US
* Apple Patches Zero-Day Vulnerability Exploited Against iPhones

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* Social Engineering, Money Mules, and Job Seekers
* Hospitals Warned of Royal Ransomware Attacks by U.S. Department of Health
* Less Than One-Third of Organizations Leverage Multiple Authentication Factors to Secure Their Environ
* Ten Charged with BEC Healthcare Scheme That Took More than $11 Million
* Cybersecurity Experts Weigh in on Modern Email Attacks
* Interest in Infostealer Malware Within Cyberattacks Spikes as MFA Fatigue Attacks Increase
* October and November Have Been the Two Busiest Months for Ransomware
* Utility Bill is the New Phishbait for Cybercriminals
* Look Out For Scammers This Holiday Season on Social Media
* Ughh. FBI's Vetted Threat Sharing Network 'InfraGard' Hacked

ISC2.org Blog

* SSCP Members - We Need Your Input
* LATEST CYBERTHREATS AND ADVISORIES - DECEMBER 16, 2022
* 2022 (ISC)² Member Bloggers
* (ISC)² Annual Meeting Outcomes - Bylaws Amendments and 2023 Board of Directors
* Calling All CISSPs! Help Shape the CISSP Exam

HackRead

* Hacker Halts Sale of FBI's High-Profile InfraGard Database
* Microsoft Alert: DDoS Botnet Hit Private Minecraft Servers
* Mastodon Account Suspended from Twitter Following Ban on Server Links
* Hackers Breach TPG Telecoms' Email Host to Steal Client Data
* The State of Cybersecurity: Why Industry Experts Are Optimistic
* 48 DDoS-hiring Services Busted by FBI in Major Sweep
* SEC Charges 8 Social Media Influencers Over Securities Fraud

Koddos

* Hacker Halts Sale of FBI's High-Profile InfraGard Database
* Microsoft Alert: DDoS Botnet Hit Private Minecraft Servers
* Mastodon Account Suspended from Twitter Following Ban on Server Links
* Hackers Breach TPG Telecoms' Email Host to Steal Client Data
* The State of Cybersecurity: Why Industry Experts Are Optimistic
* 48 DDoS-hiring Services Busted by FBI in Major Sweep
* SEC Charges 8 Social Media Influencers Over Securities Fraud

Naked Security

* 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
* S3 Ep112: Data breaches can haunt you more than once! [Audio + Text]
* Credit card skimming - the long and winding road of supply chain failure
* SIM swapper sent to prison for 2FA cryptocurrency heist of over $20m
* Number Nine! Chrome fixes another 2022 zero-day, Edge patched too

Threat Post

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

Null-Byte

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

IBM Security Intelligence

* 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
* How Posture Management Prevents Catastrophic Cloud Breaches
* 5 Holiday Cybersecurity Tips That Make a Real Impact
* Critical Remote Code Execution Vulnerability in SPNEGO Extended Negotiation Security Mechanism
* How to Implement Cloud Identity and Access Governance
* Cybersecurity Trends: IBM's Predictions for 2023
* How The Talent Shortage Changes the Approach to Cybersecurity

InfoWorld

* What's new in Rust 1.66
* Why don't cloud providers integrate?
* When to architect for the edge
* 10 databases supporting in-database machine learning
* SvelteKit 1.0 brings a full stack to Svelte
* Low-code DevOps Center aims to ease app development on Salesforce
* The best way to pursue cloud sustainability
* How to work with endpoint filters in ASP.NET Core 7
* Error tracking with Sentry, Python, and Django
* Time series forecasting with ARMA and InfluxDB

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.

* Damncon 2022
* niteCTF
* ASIS CTF Finals 2022
* Real World CTF 5th
* IrisCTF 2023
* KnightCTF 2023
* LA CTF 2023
* pbctf 2023
* WPICTF 2023
* LINE 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

* 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
* Faraday 4.3.0
* Clam AntiVirus Toolkit 1.0.0
* Suricata IDPE 6.0.9
* Falco 0.33.1

Kali Linux Tutorials

* 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
* Burp Suite Tutorial - A Web Application Penetration Testing Tool - Beginners Guide
* Pyramid : A Tool To Help Operate In EDRs' Blind Spots
* Metasploit Framework - A Beginner's Guide for Penetration Testing & Exploit Development
* AzureGraph : Azure AD Enumeration Over MS Graph
* Whatweb - A Scanning Tool to Find Security Vulnerabilities in Web App
* SIEM - Security Information and Event Management Tools - A Beginner's Guide
* R4Ven : Track IP And GPS Location
* Klyda : Highly Configurable Script For Dictionary/Spray Attacks Against Online Web Applications

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

* Analysis Paralysis? Setting the Right Goal for Your Incident Analysis
* Hunting Threat Actors Using OSINT
* Updates in DFIR
* Threat Hunting in Microsoft 365 Environment

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

* 2022 Hak5 Payload Awards
* Twitter API Bug Affects Millions of Users - ThreatWire
* OS Detection - USB Rubber Ducky

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

* Apple Encrypts the Cloud - Chrome Passkeys, Telegram malware, SYNC.com outage, Rackspace lawsuits
* LastPass Again - South Dakota bans TikTok, Anker Eufy Camera debacle, Mozilla yanks trusted root

Troy Hunt

* Weekly Update 326

Intel Techniques: The Privacy, Security, & OSINT Show

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

Proof of Concept (PoC) & Exploits

Packet Storm Security

* 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
* SOUND4 IMPACT/FIRST/PULSE/Eco 2.x Persistent Cross Site Scripting
* SOUND4 IMPACT/FIRST/PULSE/Eco 2.x Directory Traversal / File Write
* SOUND4 IMPACT/FIRST/PULSE/Eco 2.x Hardcoded Credentials
* SOUND4 IMPACT/FIRST/PULSE/Eco 2.x ICMP Flood Attack
* SOUND4 IMPACT/FIRST/PULSE/Eco 2.x username SQL Injection
* SOUND4 IMPACT/FIRST/PULSE/Eco 2.x password SQL Injection
* SOUND4 IMPACT/FIRST/PULSE/Eco 2.x Disconnect Webmonitor User Denial Of Service
* SOUND4 IMPACT/FIRST/PULSE/Eco 2.x Insufficient Session Expiration
* SOUND4 IMPACT/FIRST/PULSE/Eco 2.x Authorization Bypass

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

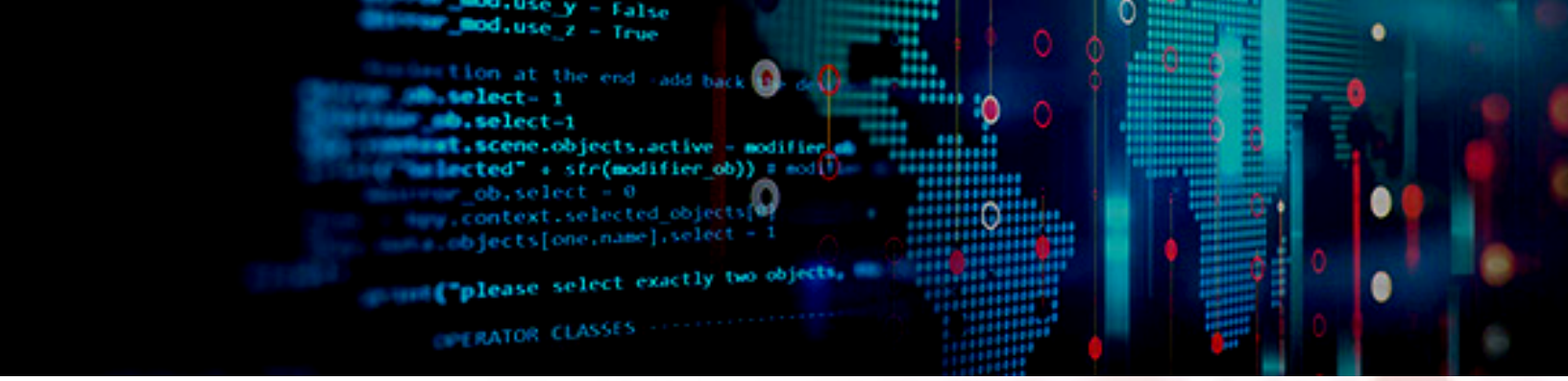
* [remote] SmartRG Router SR510n 2.6.13 - Remote Code Execution
* [webapps] CVAT 2.0 - Server Side Request Forgery
* [local] IOTransfer V4 - Unquoted Service Path
* [remote] AVEVA InTouch Access Anywhere Secure Gateway 2020 R2 - Path Traversal
* [remote] MSNSwitch Firmware MNT.2408 - Remote Code Execution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

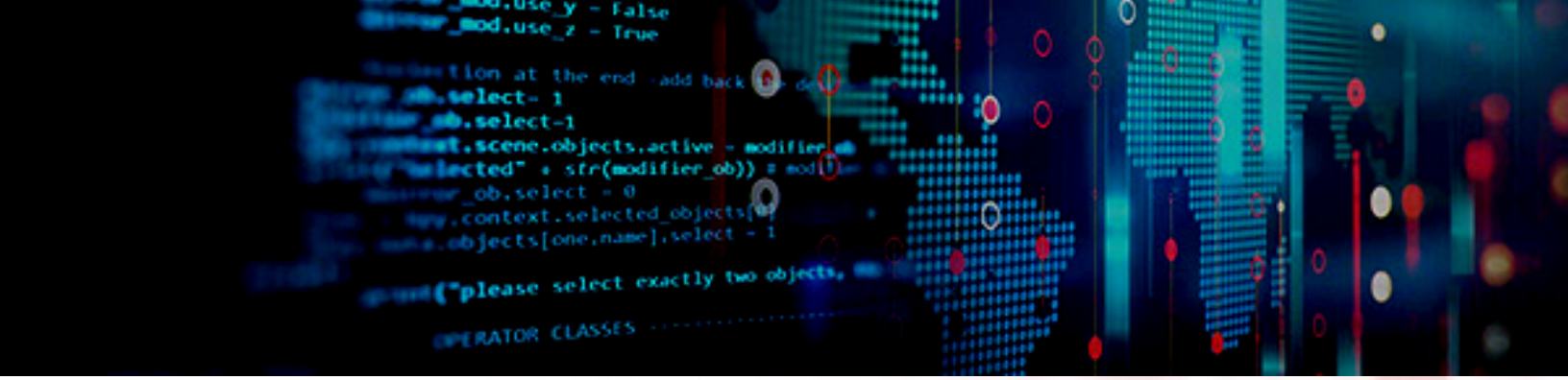
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://sysreq.saae.iguatu.ce.gov.br
https://sysreq.saae.iguatu.ce.gov.br notified by sh3ll0
https://helpdesk.saae.iguatu.ce.gov.br
https://helpdesk.saae.iguatu.ce.gov.br notified by sh3ll0
https://bies.saae.iguatu.ce.gov.br
https://bies.saae.iguatu.ce.gov.br notified by sh3ll0
https://siros.saae.iguatu.ce.gov.br
https://siros.saae.iguatu.ce.gov.br notified by sh3ll0
https://backup.saae.iguatu.ce.gov.br/index.html
https://backup.saae.iguatu.ce.gov.br/index.html notified by sh3ll0
https://ouvidoria.saae.iguatu.ce.gov.br
https://ouvidoria.saae.iguatu.ce.gov.br notified by sh3ll0
https://atendimento.saae.iguatu.ce.gov.br
https://atendimento.saae.iguatu.ce.gov.br notified by sh3ll0
https://protocolo.saae.iguatu.ce.gov.br
https://protocolo.saae.iguatu.ce.gov.br notified by sh3ll0
http://sanfelipegto.gob.mx/end.html
http://sanfelipegto.gob.mx/end.html notified by ./KeyzNet
https://assinador.recife.pe.gov.br/sok.txt
https://assinador.recife.pe.gov.br/sok.txt notified by CyberTeam
http://emis.mon.gov.mk/sok.txt
http://emis.mon.gov.mk/sok.txt notified by CyberTeam
https://pa-malili.go.id/images/r00t.txt
https://pa-malili.go.id/images/r00t.txt notified by Hemker Martabak
https://pa-wonosobo.go.id/images/r00t.txt
https://pa-wonosobo.go.id/images/r00t.txt notified by Hemker Martabak
http://mosaic.mit.edu/0x.txt
http://mosaic.mit.edu/0x.txt notified by /Rayzky_
https://tipstream-media-staging.razer.com/gece2.html?a=1
https://tipstream-media-staging.razer.com/gece2.html?a=1 notified by ZoRRoKiN
http://bbsmy.oppo.com/gece2.html?a=1
http://bbsmy.oppo.com/gece2.html?a=1 notified by ZoRRoKiN
https://bienestaranimal.gov.py
https://bienestaranimal.gov.py notified by 1877

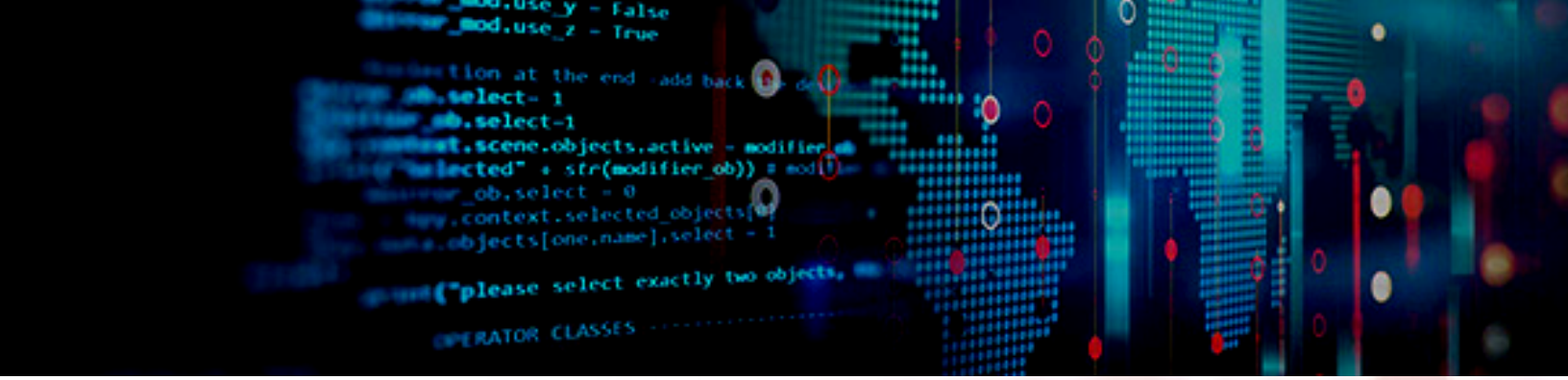


Dark Web News

Darknet Live

[Two Men Charged for Distributing Fentanyl on the Dark Web]
[Phishing Attacks Explained]
[Australian Fraudster Sentenced to Prison]
[Darknet markets and stolen data - A big profiting business]

Dark Web Link



Trend Micro Anti-Malware Blog

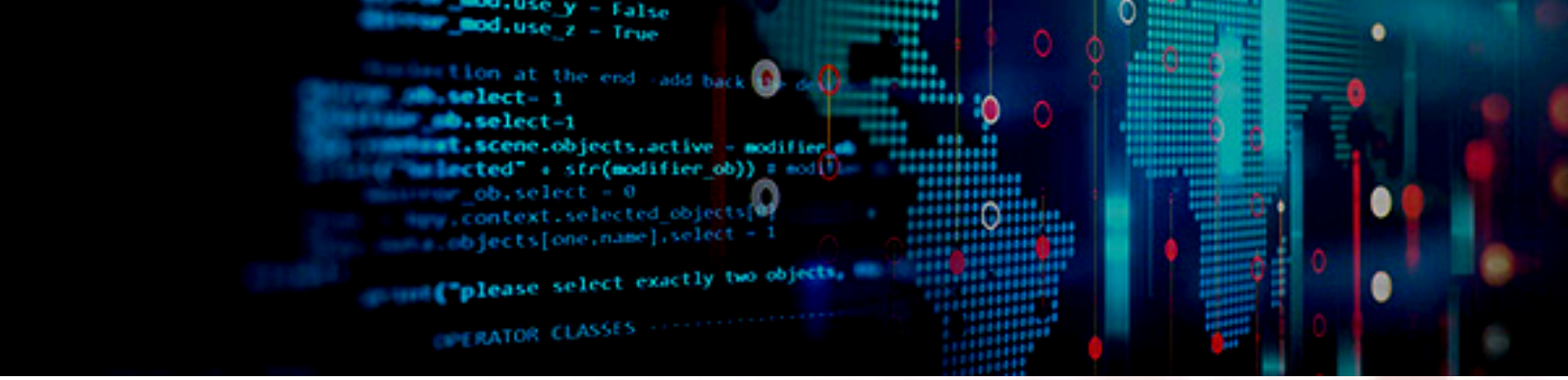
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

* Skimming for Sale: Commodity Skimming and Magecart Trends in Q1 2022
* RiskIQ Threat Intelligence Roundup: Phishing, Botnets, and Hijacked Infrastructure
* RiskIQ Threat Intelligence Roundup: Trickbot, Magecart, and More Fake Sites Targeting Ukraine
* RiskIQ Threat Intelligence Roundup: Campaigns Targeting Ukraine and Global Malware Infrastructure
* RiskIQ Threat Intelligence Supercharges Microsoft Threat Detection and Response
* RiskIQ Intelligence Roundup: Spoofed Sites and Surprising Infrastructure Connections
* RiskIQ Threat Intelligence Roundup: QBot, Magecart, Agent Tesla Headline Hijacked Infrastructure
* RiskIQ Threat Intelligence Roundup: C2 and Nation-State Threat Infrastructure
* Jupyter Notebooks Make RiskIQ Data a Digital 'Mech Suit' for Threat Intelligence Analysts
* "Offshore" Shinjiru Provides Bulletproof Services to Cyberattackers

FireEye

* [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
* CVE-2022-27518: Critical Fix Released for Exploited Citrix ADC, Gateway Vulnerability
* Patch Tuesday - December 2022
* Tis the Season to Be Wary: Three Holiday Shopping Scams To Watch For
* CVE-2022-42475: Critical Unauthenticated Remote Code Execution Vulnerability in FortiOS; Exploitation
* Rapid7 Recognized as a Top Place to Work for 11th Consecutive Year
* Metasploit Wrap-Up



Advisories

US-Cert Alerts & bulletins

* 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
* Apple Releases Security Updates for Multiple Products
* Microsoft Releases December 2022 Security Updates
* AA22-335A: #StopRansomware: Cuba Ransomware
* AA22-321A: #StopRansomware: Hive Ransomware
* Vulnerability Summary for the Week of December 5, 2022
* Vulnerability Summary for the Week of November 28, 2022

Zero Day Initiative Advisories

ZDI-CAN-19349: Apple
A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'jzhu' was reported to the affected vendor on: 2022-12-16, 3 days ago. The vendor is given until 2023-04-15 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-19403: Microsoft
A CVSS score 6.5 (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Nitesh Surana (@_niteshsurana) of Project Nebula, Trend Micro Research' was reported to the affected vendor on: 2022-12-16, 3 days ago. The vendor is given until 2023-04-15 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-19402: Microsoft
A CVSS score 5.5 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by ' Nitesh Surana (@_niteshsurana) of Project Nebula, Trend Micro Research' was reported to the affected vendor on: 2022-12-16, 3 days ago. The vendor is given until 2023-04-15 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-19776: SolarWinds
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 'Piotr Bazydlo (@chudypb) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-12-16, 3 days ago. The vendor is given until 2023-04-15 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-19830: SolarWinds
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 'Piotr Bazydlo

(@chudypb) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-12-16, 3 days ago. The vendor is given until 2023-04-15 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-19824: Microsoft

A CVSS score 5.4 (AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N) severity vulnerability discovered by 'Nitesh Surana (@_niteshsurana) of Project Nebula, Trend Micro Research' was reported to the affected vendor on: 2022-12-16, 3 days ago. The vendor is given until 2023-04-15 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-19745: Western Digital

A CVSS score 8.0 (AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Discovered by: Claroty Research - Vera Mens, Noam Moshe, Uri Katz, Sharon Brizinov' was reported to the affected vendor on: 2022-12-02, 17 days ago. The vendor is given until 2023-04-01 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-19746: Western Digital

A CVSS score 8.0 (AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Discovered by: Claroty Research - Vera Mens, Noam Moshe, Uri Katz, Sharon Brizinov' was reported to the affected vendor on: 2022-12-02, 17 days ago. The vendor is given until 2023-04-01 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-19678: Western Digital

A CVSS score 8.0 (AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Claroty Research - Vera Mens, Noam Moshe, Uri Katz, Sharon Brizinov' was reported to the affected vendor on: 2022-12-02, 17 days ago. The vendor is given until 2023-04-01 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-19604: Synology

A CVSS score 5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Claroty Research - Vera Mens, Noam Moshe, Uri Katz, Sharon Brizinov' was reported to the affected vendor on: 2022-12-02, 17 days ago. The vendor is given until 2023-04-01 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-19744: Synology

A CVSS score 5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Discovered by: Claroty Research - Vera Mens, Noam Moshe, Uri Katz, Sharon Brizinov' was reported to the affected vendor on: 2022-12-02, 17 days ago. The vendor is given until 2023-04-01 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-19743: Synology

A CVSS score 4.3 (AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Discovered by: Claroty Research - Vera Mens, Noam Moshe, Uri Katz, Sharon Brizinov' was reported to the affected vendor on: 2022-12-02, 17 days ago. The vendor is given until 2023-04-01 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-19741: Synology

A CVSS score 8.0 (AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Discovered by: Claroty Research - Vera Mens, Noam Moshe, Uri Katz, Sharon Brizinov' was reported to the affected vendor on: 2022-12-02, 17 days ago. The vendor is given until 2023-04-01 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-19708: Synology

A CVSS score 7.5 (AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Claroty Research - Vera Mens, Noam Moshe, Uri Katz, Sharon Brizinov' was reported to the affected vendor on: 2022-12-02, 17 days ago. The vendor is given until 2023-04-01 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-19742: Synology

A CVSS score 5.7 (AV:A/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H) severity vulnerability discovered by 'Discovered by: Claroty Research - Vera Mens, Noam Moshe, Uri Katz, Sharon Brizinov' was reported to the affected vendor on: 2022-12-02, 17 days ago. The vendor is given until 2023-04-01 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-19191: Trend Micro

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 'Lynn and Lays (@_L4ys)' was reported to the affected vendor on: 2022-12-02, 17 days ago. The vendor is given until 2023-04-01 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-19192: Trend Micro

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 'Lynn and Lays (@_L4ys)' was reported to the affected vendor on: 2022-12-02, 17 days ago. The vendor is given until 2023-04-01 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-19188: Trend Micro

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 'Lynn and Lays (@_L4ys)' was reported to the affected vendor on: 2022-12-02, 17 days ago. The vendor is given until 2023-04-01 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-18935: Microsoft

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 'insu of 78ResearchLab' was reported to the affected vendor on: 2022-12-02, 17 days ago. The vendor is given until 2023-04-01 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-19648: SolarWinds

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 'Piotr Bazydlo (@chudypb) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-12-02, 17 days ago. The vendor is given until 2023-04-01 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-19107: VBASE

A CVSS score 5.5 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2022-12-02, 17 days ago. The vendor is given until 2023-04-01 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-19530: X.Org

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 'Jan-Niklas Sohn' was reported to the affected vendor on: 2022-12-02, 17 days ago. The vendor is given until 2023-04-01 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-19621: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-11-30, 19 days ago. The vendor is given until 2023-03-30 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-19620: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-11-30, 19 days ago. The vendor is given until 2023-03-30 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

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 - Tamás Koczka discovered that the Bluetooth L2CAP handshake implementation in the Linux kernel contained multiple use-after-free vulnerabilities. A physically proximate attacker could use this to cause a denial of service or possibly execute arbitrary code.

Red Hat Security Advisory 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.

Red Hat Security Advisory 2022-9066-01

Red Hat Security Advisory 2022-9066-01 - 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 2022-9074-01

Red Hat Security Advisory 2022-9074-01 - 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 2022-9071-01

Red Hat Security Advisory 2022-9071-01 - 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 2022-9078-01

Red Hat Security Advisory 2022-9078-01 - 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 2022-9080-01

Red Hat Security Advisory 2022-9080-01 - 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 2022-9081-01

Red Hat Security Advisory 2022-9081-01 - 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 2022-8893-01

Red Hat Security Advisory 2022-8893-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the container images for Red Hat OpenShift Container Platform 4.11.20.

Red Hat Security Advisory 2022-9079-01

Red Hat Security Advisory 2022-9079-01 - 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 2022-9072-01

Red Hat Security Advisory 2022-9072-01 - 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 2022-9065-01

Red Hat Security Advisory 2022-9065-01 - 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 2022-9069-01

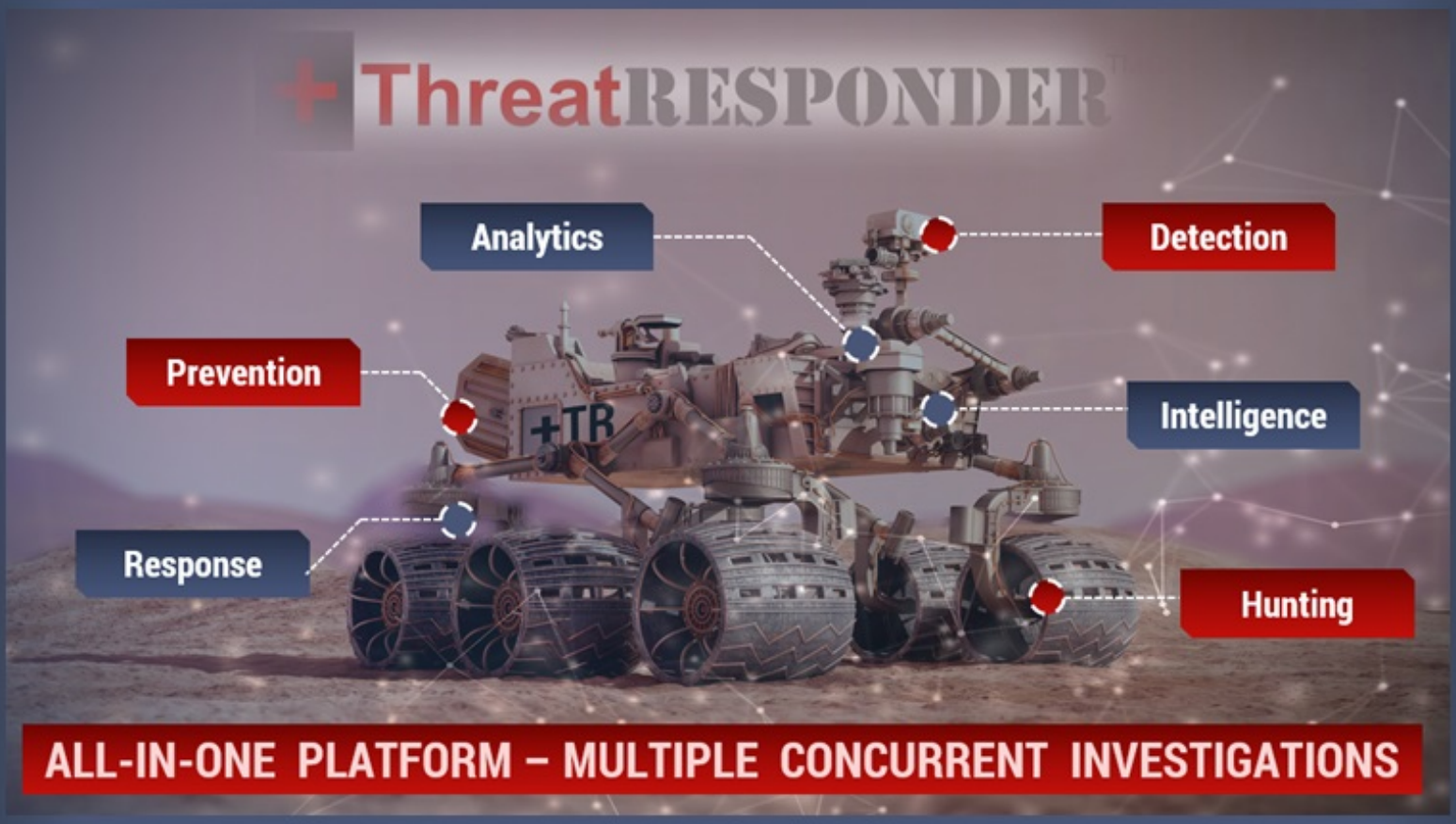
Red Hat Security Advisory 2022-9069-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 102.6.0 ESR. Issues addressed include a use-after-free vulnerability.

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



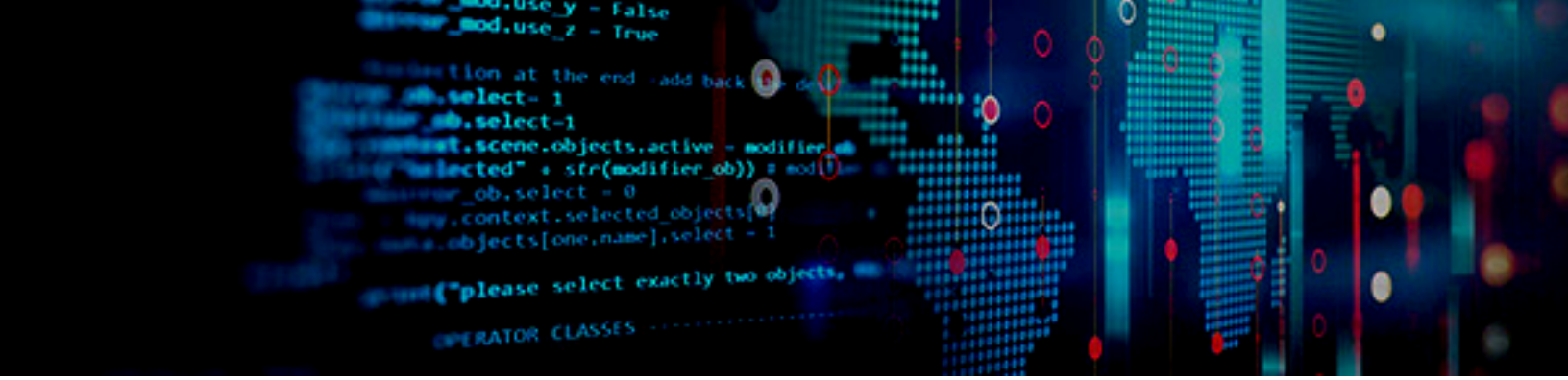
The Solution – ThreatResponder® Platform

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

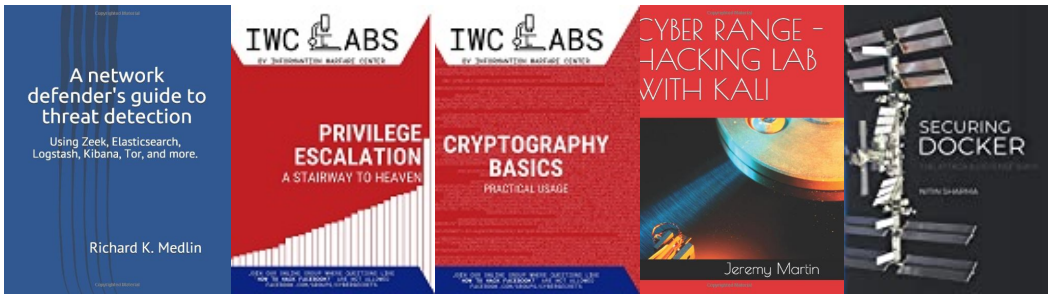


The Cyber Secrets publications on Amazon

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