Jul-24-23

CYBER WEEKLY AWARENESS REPORT

JOIN OUR ONLINE GROUP WHERE QUESTIONS LIKE "**HOW TO HACK FACEBOOK?**" ARE NOT ALLOWED
FACEBOOK.COM/GROUPS/CYBERSECRETS

ARGOS
APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity

July 24, 2023

The Cyber WAR (Weekly Awareness Report) is an Open Source Intelligence AKA OSINT resource focusing on advanced persistent threats and other digital dangers received by over ten thousand individuals. APTs fit into a cybercrime category directed at both business and political targets. Attack vectors include system compromise, social engineering, and even traditional espionage. Included are clickable links to news stories, vulnerabilities, exploits, & other industry risk.

Summary

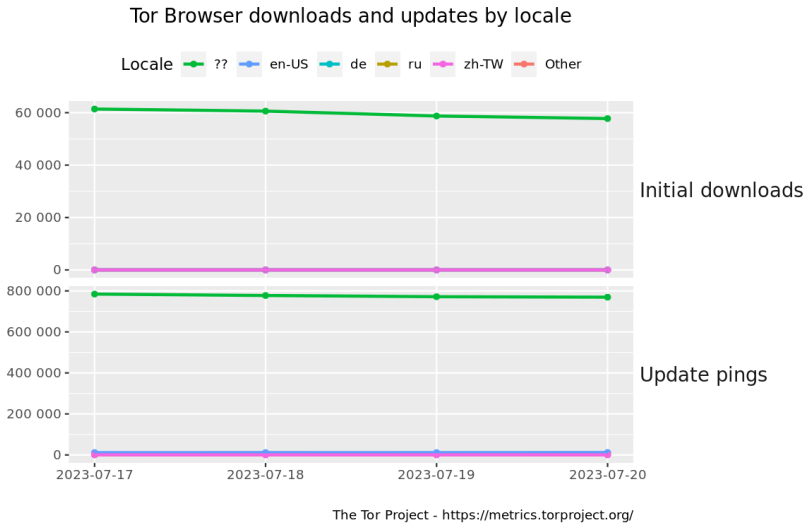
Internet Storm Center Infocon Status

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

Other IWC Publications

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

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



Interesting News

* Free Cyberforensics Training - CSI Linux Basics

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

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

Index of Sections

Packet Storm Security

* OpenMeetings Flaws Allow Hackers To Execute Code And Hijack
* NetScaler RCE Abused To Pilfer Critical Infra Active Directory Data
* Microsoft Key Stolen By Chinese Hackers Provided Access Far Beyond Outlook
* BMC Firmware Flaw Affecting Millions Gives Superuser Access
* DDoS Botnets Exploiting Recent Zyxel Vulnerability
* North Korean Hackers Breached A US Tech Company To Steal Crypto
* Apple Slams UK Surveillance Bill Proposals
* Google's New Security Pilot Program Will Ban Employee Internet Access
* Kevin Mitnick Passed Away
* The Tail Of The MOVEit Hack May Be Longer Than We Realize
* Two Jira Plugin Vulnerabilities In Attacker Crosshairs
* FIN8 Retools Backdoor Malware To Avoid Detection
* US Adds Euro Spyware Makers To Export Naughty List
* Mass Attack On WordPress Sites Targets Bug In WooCommerce Plugin
* Beijing Wants To Make The Great Firewall Of China Even Greater
* TOMRA Pulls Systems Offline Following Extensive Cyberattack
* Hacker Conversations: Inside The Mind Of Daniel Kelley, Ex-Blackhat
* Congress Is Going To Be Talking About UFOs Next Week
* Seven New Gadgets Added To Riskiest Connected Devices List
* Dating App Spills 340GB Of Steamy Data And 260,000 User Profiles
* UN Security Council To Hold First Talks On AI Risks
* JumpCloud Says Nation State Hackers Targeted Customers
* Email Hack Prompts Calls For Microsoft To Make Security Logs Free
* Fake PoC On GitHub Lures Researchers To Download Malware
* Adobe Patches Critical ColdFusion, InDesign Zero Day Bugs

Krebs on Security

* Few Fortune 100 Firms List Security Pros in Their Executive Ranks
* LeakedSource Owner Quit Ashley Madison a Month Before 2015 Hack
* SEO Expert Hired and Fired By Ashley Madison Turned on Company, Promising Revenge
* Apple & Microsoft Patch Tuesday, July 2023 Edition
* Top Suspect in 2015 Ashley Madison Hack Committed Suicide in 2014
* Who's Behind the DomainNetworks Snail Mail Scam?
* Russian Cybersecurity Executive Arrested for Alleged Role in 2012 Megahacks
* U.K. Cyber Thug "PlugwalkJoe" Gets 5 Years in Prison
* SMS Phishers Harvested Phone Numbers, Shipment Data from UPS Tracking Tool
* Why Malware Crypting Services Deserve More Scrutiny

Dark Reading

* What C-Suite Leaders Need to Know About XDR
* How to Put the Sec in DevSecOps
* BGP Software Vulnerabilities Under the Microscope in Black Hat Session
* Banks In Attackers' Crosshairs, Via Open Source Software Supply Chain
* Rootkit Attack Detections Increase at UAE Businesses
* CVSS 4.0 Is Here, but Prioritizing Patches Still a Hard Problem
* Saudi Arabia's Tuwaiq Academy Opens Cybersecurity Bootcamp
* Microsoft 365 Breach Risk Widens to Millions of Azure AD Apps
* White House, Big Tech Ink Commitments to Secure AI
* Meet the Finalists for the 2023 Pwnie Awards
* The Dark Side of AI
* North Korean Attackers Targeted Crypto Companies in JumpCloud Breach
* TrustArc Announces TRUSTe EU-US Data Privacy Framework Verification
* Deloitte Global Expands MXDR Cybersecurity SaaS Solution With Operational Technology and Identity Mod
* Mallox Ransomware Group Activity Shifts Into High Gear
* Critical Infrastructure Workers Better At Spotting Phishing
* Kevin Mandia Brings the HammerCon
* Estée Lauder Breached in Twin MOVEit Hacks, by Different Ransom Groups
* Apache OpenMeetings Wide Open to Account Takeover, Code Execution
* Docker Leaks API Secrets & Private Keys, as Cybercriminals Pounce

The Hacker News

* Banking Sector Targeted in Open-Source Software Supply Chain Attacks
* Apple Threatens to Pull iMessage and FaceTime from U.K. Amid Surveillance Demands
* Azure AD Token Forging Technique in Microsoft Attack Extends Beyond Outlook, Wiz Reports
* HotRat: New Variant of AsyncRAT Malware Spreading Through Pirated Software
* Sophisticated BundleBot Malware Disguised as Google AI Chatbot and Utilities
* Local Governments Targeted for Ransomware - How to Prevent Falling Victim
* DDoS Botnets Hijacking Zyxel Devices to Launch Devastating Attacks
* Citrix NetScaler ADC and Gateway Devices Under Attack: CISA Urges Immediate Action
* Mallox Ransomware Exploits Weak MS-SQL Servers to Breach Networks
* Critical Flaws in AMI MegaRAC BMC Software Expose Servers to Remote Attacks
* Apache OpenMeetings Web Conferencing Tool Exposed to Critical Vulnerabilities
* North Korean State-Sponsored Hackers Suspected in JumpCloud Supply Chain Attack
* A Few More Reasons Why RDP is Insecure (Surprise!)
* Turla's New DeliveryCheck Backdoor Breaches Ukrainian Defense Sector
* New P2PInfect Worm Targeting Redis Servers on Linux and Windows Systems

Security Week

* Microsoft Cloud Hack Exposed More Than Exchange, Outlook Emails
* In Other News: Military Emails Leaked, Google Restricts Internet Access, Chinese Spyware
* Russia Seeks 18 Years in Jail for Founder of Cybersecurity Firm
* Google Creates Red Team to Test Attacks Against AI Systems
* OpenMeetings Flaws Allow Hackers to Hijack Instances, Execute Code on Servers
* VirusTotal Provides Clarifications on Data Leak Affecting Premium Accounts
* Watch Now: Cloud & Data Security Summit Sessions
* Tech Titans Promise Watermarks to Expose AI Creations
* GitHub Warns of North Korean Social Engineering Attacks Targeting Tech Firm Employees
* Tampa General Hospital Says Patient Information Stolen in Ransomware Attack

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* Save $200 on Your Security Awareness and Culture Professional (SACP) Certification
* Microsoft was the Most Impersonated Brand in Q2, 2023
* European Union Healthcare Sees the Number of Cyber Incidents Double in 2023
* Business Email Compromise Now Has a $50 Billion Price Tag
* The Number of Data Compromises Jumps 50% in H1 2023, Outpacing Every Year on Record
* Kevin David Mitnick (Aug 6, 1963 - July 16, 2023)
* Threat Actors Add ".Zip" Domains to Phishbait
* [INFOGRAPHIC] KnowBe4's Content Library by the Numbers
* CyberheistNews Vol 13 #29 [Heads Up] Phishing Attacks Now Use QR Codes to Steal Your User Credentials
* [HEADS UP] See WormGPT, the new "ethics-free" Cyber Crime attack tool

ISC2.org Blog

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

HackRead

* VirusTotal issues apology for recent sensitive data leak
* 10 Essential Cybersecurity Tips for Small Businesses
* Phishers Exploiting Google Docs to Harvest Crypto Credentials
* Global CDN Service 'jsdelivr' Exposed Users to Phishing Attacks
* Roblox Data Breach: PII of Thousands of Developers Stolen
* The Metaverse is connected to cryptocurrencies - but not so much to Bitcoin
* Fake ChatGPT and AI pages on Facebook are spreading infostealers

Koddos

* VirusTotal issues apology for recent sensitive data leak
* 10 Essential Cybersecurity Tips for Small Businesses
* Phishers Exploiting Google Docs to Harvest Crypto Credentials
* Global CDN Service 'jsdelivr' Exposed Users to Phishing Attacks
* Roblox Data Breach: PII of Thousands of Developers Stolen
* The Metaverse is connected to cryptocurrencies - but not so much to Bitcoin
* Fake ChatGPT and AI pages on Facebook are spreading infostealers

Naked Security

* S3 Ep144: When threat hunting goes down a rabbit hole
* Google Virus Total leaks list of spooky email addresses
* Microsoft hit by Storm season - a tale of two semi-zero days
* Zimbra Collaboration Suite warning: Patch this 0-day right now (by hand)!
* S3 Ep143: Supercookie surveillance shenanigans
* Microsoft patches four zero-days, finally takes action against crimeware kernel drivers
* Apple silently pulls its latest zero-day update - what now?
* Urgent! Apple fixes critical zero-day hole in iPhones, iPads and Macs
* Serious Security: Rowhammer returns to gaslight your computer
* S3 Ep142: Putting the X in X-Ops

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

* What's new in the 2023 Cost of a Data Breach report
* What to do about the rise of financial fraud
* Sensitive data FOMO: You can't afford to miss out on data security
* X-Force certified containment: Responding to AD CS attacks
* Cloud security in the era of artificial intelligence
* The top 10 API security risks OWASP list for 2023
* BlotchyQuasar: X-Force Hive0129 targeting financial institutions in LATAM with a custom banking troja
* Crypto fraud in 2023: How can security teams fight
* Personal data vs. sensitive data: What is the difference?
* Are we doomed to make the same security mistakes with AI?

InfoWorld

* A new hope for software security
* How AI will impact the developer experience
* What can ChatGPT and LLMs really do for your business?
* Microsoft unveils TypeChat library for building natural language interfaces
* Megatrend alert: The rise of ubiquitous computing
* What is reactive programming? Programming with event streams
* GitHub Copilot Chat available in a preview for businesses
* JDK 21: The new features in Java 21
* JetBrains ships Qodana static code analysis tool
* How to handle null values in C#

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

* 5 Things That Make The DEF CON Experience Special
* The 5 Most Controversial DEF CON Talks Of All Time
* 6 Notable DEF CON Moments
* Best AI Conferences To Attend in 2023
* How To Organize A Conference? Here's How To Get It Right!
* 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

Google Zero Day Project

* Release of a Technical Report into Intel Trust Domain Extensions
* Multiple Internet to Baseband Remote Code Execution Vulnerabilities in Exynos Modems

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.

* TFC CTF 2023
* corCTF 2023
* DeconstruCT.F 2023
* Arab Security Cyber Wargames 2023 Qualifications
* ESCAPE CTF 2023 Preliminary
* Lexington Informatics Tournament CTF 2023
* Securinets CTF Quals 2023
* CTFZone 2023 Quals
* h4ckc0n 2023
* CCCamp 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

* jSQL Injection 0.88
* OpenSSH 9.3p2
* Suricata 7.0.0
* Faraday 4.5.1
* Faraday 4.5.0
* Wireshark Analyzer 4.0.7
* jSQL Injection 0.87
* Zed Attack Proxy 2.13.0 Cross Platform Package
* OATH Toolkit 2.6.9
* jSQL Injection 0.86

Kali Linux Tutorials

* PhoneSploit-Pro : An All-In-One Hacking Tool To Remotely Exploit Android Devices Using ADB And Metasp
* Kubei : A Flexible Kubernetes Runtime Scanner
* auditpolCIS : CIS Benchmark Testing Of Windows SIEM Configuration
* PortEx : Java Library To Analyse Portable Executable Files With A Special Focus On Malware Analysis A
* Vid2img-extract all frame from a given video
* 404 Frame - Infiltrating websites is now easy
* jupyter-kali
* Passwordless Authentication Should Become Mainstream by 2023
* Email2PhoneNumber: Obtain Phone Number via Email Address
* SOC-Multitool

GBHackers Analysis

* MITRE Releases Top 25 Most Dangerous Software Weaknesses
* AndroRAT - A Remote Access Trojan Compromise Android Devices and Inject Root Exploits
* Critical Vulnerability in Microsoft Azure Let Hackers Take Over the Complete Control of the Azure Acc
* SIM Swap Attack Let Hackers Port a Telephone Number to a New SIM to Hack WhatsApp & Bypass 2FA
* Massive Cyber Attack Across the World Against ISPs & Data Centres: More than 200,000 Cisco Switches H

Weekly Cyber Security Video and Podcasts

SANS DFIR

* Should Countries Ban Ransomware Payments? | Host: Ryan Chapman | July 25, 2023
* Upgrading Cloud Forensics with FOR509
* SANS DFIR Summit & Training 2023
* SANS Threat Analysis Rundown (STAR) with Katie Nickels

Defcon Conference

* DEF CON 30 - Cesare Pizzi - Old Malware, New tools: Ghidra and Commodore 64
* DEF CON 30 - Silk - Hacker Karaoke
* DEF CON 30 Car Hacking Village - Evadsnibor - Getting Naughty on CAN bus with CHV Badge
* DEF CON 30 - Silk - DEF CON Memorial Interview

Hak5

* State DMV Data Stolen via MOVEit Vulnerabilities & Reddit's API Change Triggers Hackers - ThreatWire
* Microsoft Fined For Violating Children's Privacy - ThreatWire
* Amazon FINED For Privacy Violations - ThreatWire

The PC Security Channel [TPSC]

* Best Browser Privacy? Edge vs Chrome vs Firefox vs Brave in Wireshark
* How to tell if your PC is Hacked? Process Forensics

Eli the Computer Guy

* YOUTUBE GOES PAY for PLAY - this is just getting sad...
* LLM (Large Language Model) for AI - What is an...
* Will AI Make CODERS OBSOLETE?
* Kemper Brown Jr CEO of Electronic Office (MSP - Managed Service Provider)

Security Now

* Satellite Insecurity, Part 1 - Kaspersky on MS flaw, WormGPT, Bitcoin addresses, Twitter DM change
* Rowhammer Indelible Fingerprinting - MOVEit SQLi flaw, China's OpenKylin v1, Firefox 115, Syncthing

Troy Hunt

* Weekly Update 357

Intel Techniques: The Privacy, Security, & OSINT Show

* 303-iOS Privacy & Security
* 302-Self-Hosted 4: The Next Level

Proof of Concept (PoC) & Exploits

Packet Storm Security

* WordPress Page Builder KingComposer 2.9.5 Open Redirection
* WordPress ChurcHope Responsive Themes 4.7.x Directory Traversal
* CMS-Bank Mellat Payment Manager 1.0.0 Cross Site Scripting
* RaidenFTPD 2.4.4005 Buffer Overflow
* CMS TSS-EST 1.0.0 SQL Injection
* Foody Friend 1.0 Arbitrary File Upload / Cross Site Scripting
* CMS Supported IRF-TH 2.0.6 Cross Site Scripting
* Wifi Soft Unibox Administration 3.0 / 3.1 SQL Injection
* CMS SAUDI SOFTECH 5.0.2 SQL Injection
* CMS NEXIN 2.0 Insecure Settings
* CMS Emlak Scripti 2 Cross Site Scripting
* Buzzy News Viral Lists Polls And Videos 2.0 Insecure Settings
* Listplace Directory Listing Platform 3.0 File Upload / Cross Site Scripting
* CMS Contabil Bandeirantes 1.0.0 Cross Site Request Forgery
* OpenSSH Forwarded SSH-Agent Remote Code Execution
* Online Piggery Management System 1.0 Shell Upload
* Hikvision Hybrid SAN Ds-a71024 SQL Injection
* CMS Nexin Adminisztracios Kozpont 1.2 Insecure Settings
* CMS NaiveScripters 3.0.1 Cross Site Scripting
* CMS iQ-Digital 2.0 Cross Site Scripting
* CMS porViaX 2.0 SQL Injection
* TP-Link TL-WR740N Directory Traversal
* Pluck 4.7.18 Remote Shell Upload
* Blackcat CMS 1.4 Shell Upload
* Backdrop CMS 1.25.1 Cross Site Scripting

CXSecurity

* ABB FlowX v4.00 Exposure of Sensitive Information
* RaidenFTPD 2.4.4005 Buffer Overflow
* pfSense Restore RRD Data Command Injection
* Bludit
* MOVEit SQL Injection
* Polycom BToE Connector 4.4.0.0 Buffer Overflow / Man-In-The-Middle
* WordPress Abandoned Cart Lite For WooCommerce 5.14.2 Authentication Bypass

Proof of Concept (PoC) & Exploits

Exploit Database

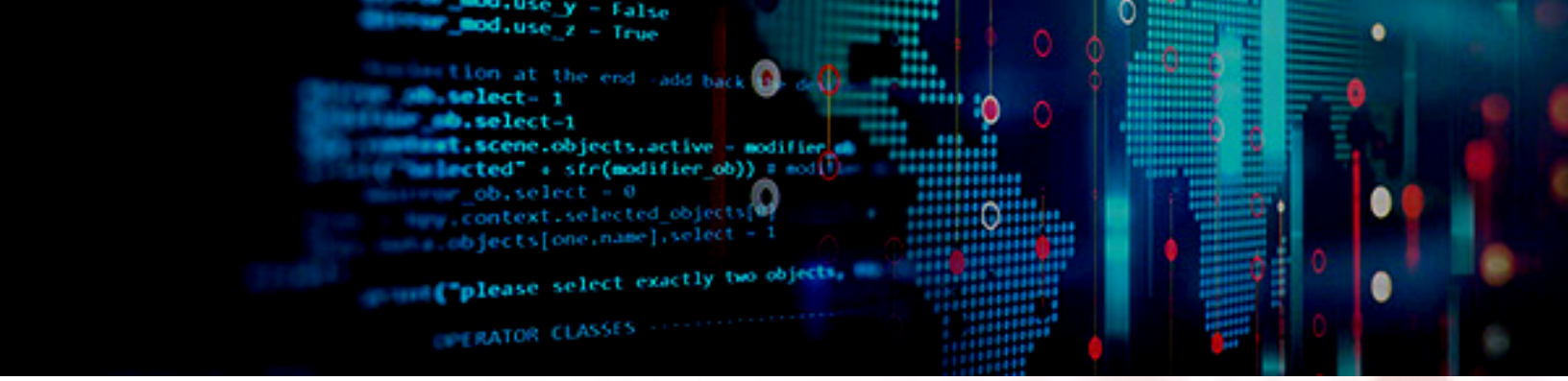
* [webapps] Perch v3.2 - Stored XSS
* [webapps] Perch v3.2 - Remote Code Execution (RCE)
* [webapps] RWS WorldServer 11.7.3 - Session Token Enumeration
* [webapps] PaulPrinting CMS - Multiple Cross Site Web Vulnerabilities
* [webapps] Aures Booking & POS Terminal - Local Privilege Escalation
* [webapps] Webile v1.0.1 - Multiple Cross Site Scripting
* [webapps] Boom CMS v8.0.7 - Cross Site Scripting
* [local] RaidenFTPD 2.4.4005 - Buffer Overflow (SEH)
* [webapps] Wifi Soft Unibox Administration 3.0 & 3.1 - SQL Injection
* [remote] Microsoft Office 365 Version 18.2305.1222.0 - Elevation of Privilege + RCE.
* [webapps] pfSense v2.7.0 - OS Command Injection
* [remote] Hikvision Hybrid SAN Ds-a71024 Firmware - Multiple Remote Code Execution
* [webapps] TP-Link TL-WR740N - Authenticated Directory Transversal
* [webapps] Blackcat Cms v1.4 - Remote Code Execution (RCE)
* [webapps] Blackcat Cms v1.4 - Stored XSS
* [webapps] ABB FlowX v4.00 - Exposure of Sensitive Information
* [webapps] Statamic 4.7.0 - File-Inclusion
* [webapps] CmsMadeSimple v2.2.17 - Stored Cross-Site Scripting (XSS)
* [webapps] CmsMadeSimple v2.2.17 - Remote Code Execution (RCE)
* [webapps] CmsMadeSimple v2.2.17 - session hijacking via Server-Side Template Injection (SSTI)
* [webapps] Online Piggery Management System v1.0 - unauthenticated file upload vulnerability
* [webapps] Backdrop Cms v1.25.1 - Stored Cross-Site Scripting (XSS)
* [webapps] Vaidya-Mitra 1.0 - Multiple SQLi
* [webapps] Joomla! com_booking component 2.4.9 - Information Leak (Account enumeration)
* [webapps] phpfm v1.7.9 - Authentication type juggling

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*

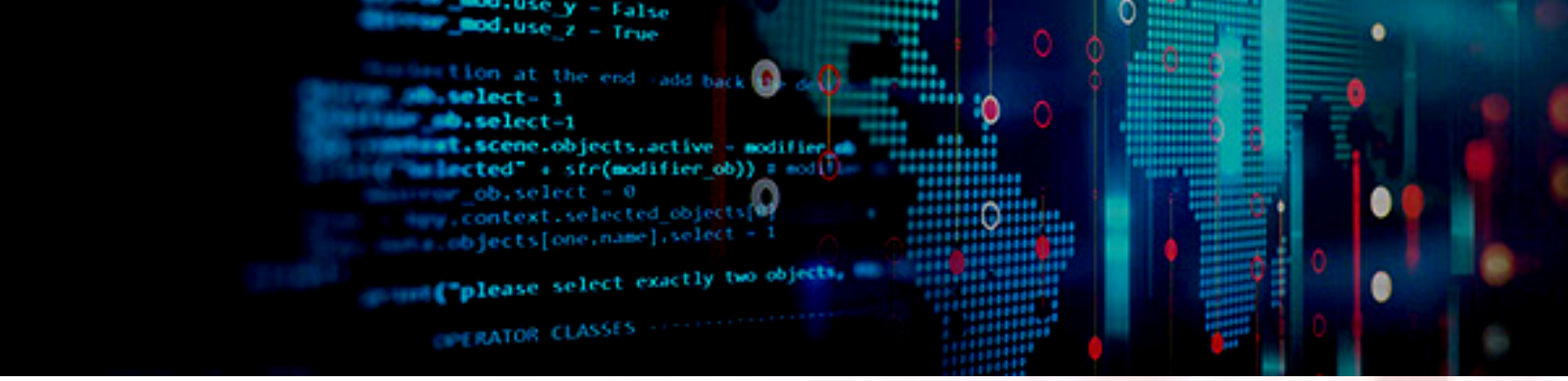
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://idea.gob.ve
http://idea.gob.ve notified by 0x1998
https://pn-sabang.go.id/readme.txt
https://pn-sabang.go.id/readme.txt notified by xNot_RespondinGx
https://tanabi.sp.gov.br/readme.txt
https://tanabi.sp.gov.br/readme.txt notified by xNot_RespondinGx
https://ppid.sukoharjokab.go.id/readme.txt
https://ppid.sukoharjokab.go.id/readme.txt notified by xNot_RespondinGx
https://kejari-pangkep.go.id/hehe.txt
https://kejari-pangkep.go.id/hehe.txt notified by KimiHmei7
http://guatemala.gob.gt/kurd.html
http://guatemala.gob.gt/kurd.html notified by 0x1998
http://mueang.chaiyaphum.doae.go.th
http://mueang.chaiyaphum.doae.go.th notified by 0x1998
http://bamnetnarong.chaiyaphum.doae.go.th
http://bamnetnarong.chaiyaphum.doae.go.th notified by 0x1998
http://sipp.pn-muarateweh.go.id/zz.html
http://sipp.pn-muarateweh.go.id/zz.html notified by xNot_RespondinGx
https://perpus.pn-muarateweh.go.id/zz.html
https://perpus.pn-muarateweh.go.id/zz.html notified by xNot_RespondinGx
https://survei.pn-muarateweh.go.id/zz.html
https://survei.pn-muarateweh.go.id/zz.html notified by xNot_RespondinGx
https://perpustakaan.pn-muarateweh.go.id/zz.html
https://perpustakaan.pn-muarateweh.go.id/zz.html notified by xNot_RespondinGx
https://vote.pn-muarateweh.go.id/zz.html
https://vote.pn-muarateweh.go.id/zz.html notified by xNot_RespondinGx
https://pn-muarateweh.go.id/zz.html
https://pn-muarateweh.go.id/zz.html notified by xNot_RespondinGx
https://nextlalpan.gob.mx/kurd.htm
https://nextlalpan.gob.mx/kurd.htm notified by 0x1998
https://satpolpp.muarojambikab.go.id/z.html
https://satpolpp.muarojambikab.go.id/z.html notified by GayAnon
https://ptsp.muarojambikab.go.id/z.html
https://ptsp.muarojambikab.go.id/z.html notified by GayAnon

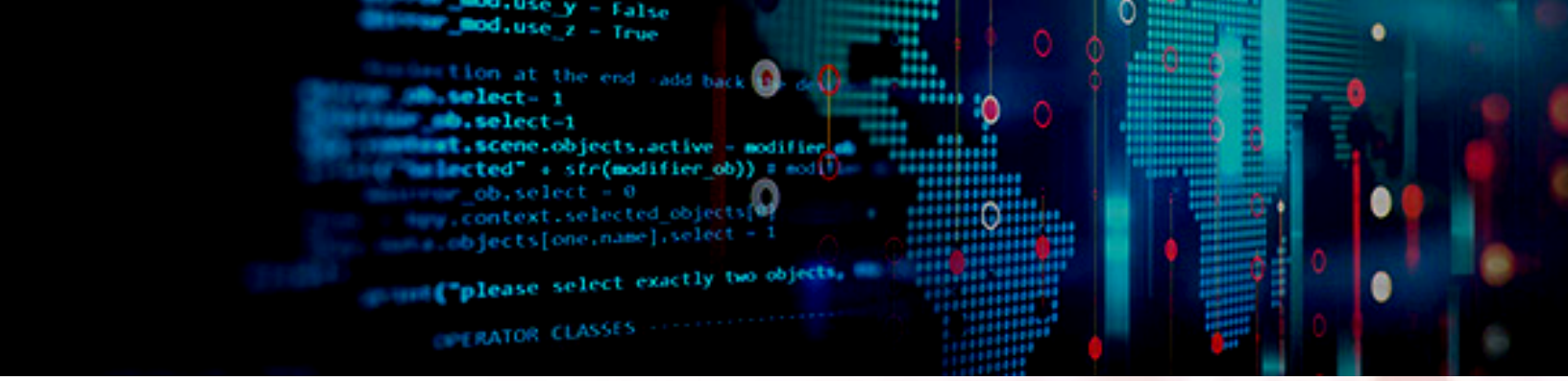


Dark Web News

Darknet Live

[Woman Pleads Guilty in the "Opiateconnect" Case]
[A Hitchhiker's Guide to Monero's Feather Wallet]
[Trio Sentenced for Distributing Counterfeit Oxycodone]
[Ross Ulbricht's Advisor "Variety Jones" Imprisoned]

Dark Web Link



Trend Micro Anti-Malware Blog

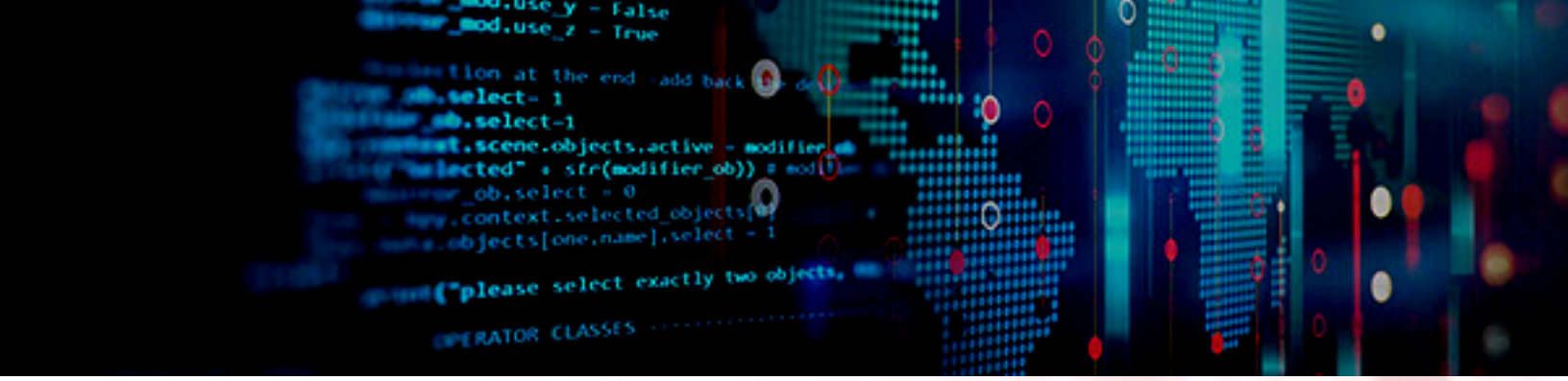
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

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

FireEye

* Metasploit Weekly Wrap up
* PenTales: Testing Security Health for a Healthcare Company
* The Japanese Technology and Media Attack Landscape
* CVE-2023-38205: Adobe ColdFusion Access Control Bypass [FIXED]
* Critical Zero-Day Vulnerability in Citrix NetScaler ADC and NetScaler Gateway
* Managing Risk Across Hybrid Environments with Executive Risk View
* Active Exploitation of Multiple Adobe ColdFusion Vulnerabilities
* [Lost Bots] S03 E04 A Security Leader's Playbook for the C-suite
* Metasploit Weekly Wrap-Up
* The Japanese Financial Services Attack Landscape



Advisories

US-Cert Alerts & bulletins

* Atlassian Releases Security Updates
* CISA Adds Two Known Exploited Vulnerabilities to Catalog
* CISA Releases One Industrial Control Systems Advisory
* CISA Releases Cybersecurity Advisory on Threat Actors Exploiting Citrix CVE-2023-3519
* CISA Adds One Known Exploited Vulnerability to Catalog
* Adobe Releases Security Updates for ColdFusion
* Citrix Releases Security Updates for NetScaler ADC and Gateway
* CISA Releases Seven Industrial Control Systems Advisories
* Threat Actors Exploiting Citrix CVE-2023-3519 to Implant Webshells
* Enhanced Monitoring to Detect APT Activity Targeting Outlook Online
* Vulnerability Summary for the Week of July 10, 2023
* Vulnerability Summary for the Week of July 3, 2023

Zero Day Initiative Advisories

ZDI-CAN-21790: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-07-20, 4 days ago. The vendor is given until 2023-11-17 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-21793: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-07-20, 4 days ago. The vendor is given until 2023-11-17 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-21797: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-07-20, 4 days ago. The vendor is given until 2023-11-17 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-21791: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-07-20, 4 days ago. The vendor is given until 2023-11-17 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-21344: Adobe
A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-07-20, 4 days ago. The vendor is given until 2023-11-17 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-21789: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-07-20, 4 days ago. The vendor is given until 2023-11-17 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-21782: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-07-20, 4 days ago. The vendor is given until 2023-11-17 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-21798: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-07-20, 4 days ago. The vendor is given until 2023-11-17 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-21665: 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 'TBD' was reported to the affected vendor on: 2023-07-20, 4 days ago. The vendor is given until 2023-11-17 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-21463: F5

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 'Alex Birnberg' was reported to the affected vendor on: 2023-07-20, 4 days ago. The vendor is given until 2023-11-17 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-21297: D-Link

A CVSS score 8.8 (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Sina Kheirkhah (@SinSinology) of Summoning Team (@SummoningTeam)' was reported to the affected vendor on: 2023-07-20, 4 days ago. The vendor is given until 2023-11-17 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-21605: Microsoft

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-07-20, 4 days ago. The vendor is given until 2023-11-17 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-21759: Kofax

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-07-20, 4 days ago. The vendor is given until 2023-11-17 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-21295: D-Link

A CVSS score 8.8 (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Sina Kheirkhah (@SinSinology) of Summoning Team (@SummoningTeam)' was reported to the affected vendor on: 2023-07-20, 4 days ago. The vendor is given until 2023-11-17 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-21442: D-Link

A CVSS score 8.8 (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Sina Kheirkhah

(@SinSinology) of Summoning Team (@SummoningTeam)' was reported to the affected vendor on: 2023-07-20, 4 days ago. The vendor is given until 2023-11-17 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-21755: Kofax

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-07-20, 4 days ago. The vendor is given until 2023-11-17 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-21763: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-07-18, 6 days ago. The vendor is given until 2023-11-15 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-21707: Delta Electronics

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: 2023-07-18, 6 days ago. The vendor is given until 2023-11-15 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-21553: Ashlar-Vellum

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-07-18, 6 days ago. The vendor is given until 2023-11-15 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-21765: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-07-18, 6 days ago. The vendor is given until 2023-11-15 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-21306: Adobe

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 'Anonymous' was reported to the affected vendor on: 2023-07-18, 6 days ago. The vendor is given until 2023-11-15 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-21767: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-07-18, 6 days ago. The vendor is given until 2023-11-15 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-21766: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-07-18, 6 days ago. The vendor is given until 2023-11-15 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-21764: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-07-18, 6 days ago. The vendor is given until 2023-11-15 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Red Hat Security Advisory 2023-4241-01

Red Hat Security Advisory 2023-4241-01 - Red Hat OpenShift Data Foundation is software-defined storage integrated with and optimized for the Red Hat OpenShift Data Foundation. Red Hat OpenShift Data Foundation is a highly scalable, production-grade persistent storage for stateful applications running in the Red Hat OpenShift Container Platform.

Red Hat Security Advisory 2023-4159-01

Red Hat Security Advisory 2023-4159-01 - The java-17-openjdk packages provide the OpenJDK 17 Java Runtime Environment and the OpenJDK 17 Java Software Development Kit. Issues addressed include denial of service and integer overflow vulnerabilities.

Red Hat Security Advisory 2023-4178-01

Red Hat Security Advisory 2023-4178-01 - The java-1.8.0-openjdk packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Software Development Kit. Issues addressed include an integer overflow vulnerability.

Red Hat Security Advisory 2023-4093-01

Red Hat Security Advisory 2023-4093-01 - 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 4.13.5. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2023-4091-01

Red Hat Security Advisory 2023-4091-01 - 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 4.13.5. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2023-4090-01

Red Hat Security Advisory 2023-4090-01 - 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 4.13.5.

Red Hat Security Advisory 2023-4238-01

Red Hat Security Advisory 2023-4238-01 - Red Hat OpenShift Data Foundation is software-defined storage integrated with and optimized for the Red Hat OpenShift Data Foundation. Red Hat OpenShift Data Foundation is a highly scalable, production-grade persistent storage for stateful applications running in the Red Hat OpenShift Container Platform.

Debian Security Advisory 5456-1

Debian Linux Security Advisory 5456-1 - 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-6239-1

Ubuntu Security Notice 6239-1 - It was discovered that ECDSA Util did not properly verify certain signature values. An attacker could possibly use this issue to bypass signature verification.

Red Hat Security Advisory 2023-4158-01

Red Hat Security Advisory 2023-4158-01 - The java-11-openjdk packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Software Development Kit. Issues addressed include denial of service and integer overflow vulnerabilities.

Ubuntu Security Notice USN-6237-2

Ubuntu Security Notice 6237-2 - USN-6237-1 fixed vulnerabilities in curl. The update caused a certificate wildcard handling regression on Ubuntu 22.04 LTS. This update fixes the problem. Hiroki Kurosawa discovered that curl incorrectly handled validating certain certificate wildcards. A remote attacker could possibly use this issue to spoof certain website certificates using IDN hosts. Hiroki Kurosawa discovered that curl incorrectly handled callbacks when certain options are set by applications. This could cause applications using curl to

misbehave, resulting in information disclosure, or a denial of service. It was discovered that curl incorrectly handled saving cookies to files. A local attacker could possibly use this issue to create or overwrite files. This issue only affected Ubuntu 22.10, and Ubuntu 23.04.

Red Hat Security Advisory 2023-4210-01

Red Hat Security Advisory 2023-4210-01 - The OpenJDK 17 packages provide the OpenJDK 17 Java Runtime Environment and the OpenJDK 17 Java Software Development Kit. This release of the Red Hat build of OpenJDK 17 for portable Linux serves as a replacement for the Red Hat build of OpenJDK 17 and includes security and bug fixes, and enhancements. For further information, refer to the release notes linked to in the References section. Issues addressed include denial of service and integer overflow vulnerabilities.

Red Hat Security Advisory 2023-4177-01

Red Hat Security Advisory 2023-4177-01 - The java-17-openjdk packages provide the OpenJDK 17 Java Runtime Environment and the OpenJDK 17 Java Software Development Kit. Issues addressed include denial of service and integer overflow vulnerabilities.

Red Hat Security Advisory 2023-4211-01

Red Hat Security Advisory 2023-4211-01 - The OpenJDK 17 packages provide the OpenJDK 17 Java Runtime Environment and the OpenJDK 17 Java Software Development Kit. This release of the Red Hat build of OpenJDK 17 for Windows serves as a replacement for the Red Hat build of OpenJDK 17 and includes security and bug fixes, and enhancements. For further information, refer to the release notes linked to in the References section. Issues addressed include denial of service and integer overflow vulnerabilities.

Red Hat Security Advisory 2023-4175-01

Red Hat Security Advisory 2023-4175-01 - The java-11-openjdk packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Software Development Kit. Issues addressed include denial of service and integer overflow vulnerabilities.

Red Hat Security Advisory 2023-4176-01

Red Hat Security Advisory 2023-4176-01 - The java-1.8.0-openjdk packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Software Development Kit. Issues addressed include an integer overflow vulnerability.

Red Hat Security Advisory 2023-4208-01

Red Hat Security Advisory 2023-4208-01 - The OpenJDK 11 packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Software Development Kit. This release of the Red Hat build of OpenJDK 11 for portable Linux serves as a replacement for the Red Hat build of OpenJDK 11 and includes security and bug fixes, and enhancements. For further information, refer to the release notes linked to in the References section. Issues addressed include denial of service and integer overflow vulnerabilities.

Red Hat Security Advisory 2023-4209-01

Red Hat Security Advisory 2023-4209-01 - The OpenJDK 8 packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Software Development Kit. This release of the Red Hat build of OpenJDK 8 for portable Linux serves as a replacement for Red Hat build of OpenJDK 8 and includes security and bug fixes as well as enhancements. For further information, refer to the release notes linked to in the References section. Issues addressed include an integer overflow vulnerability.

Red Hat Security Advisory 2023-4212-01

Red Hat Security Advisory 2023-4212-01 - The OpenJDK 8 packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Software Development Kit. This release of the Red Hat build of OpenJDK 8 for Windows serves as a replacement for the Red Hat build of OpenJDK 8 and includes security and bug fixes, and enhancements. For further information, refer to the release notes linked to in the References section. Issues addressed include an integer overflow vulnerability.

Red Hat Security Advisory 2023-4161-01

Red Hat Security Advisory 2023-4161-01 - The OpenJDK 11 packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Software Development Kit. This release of the Red Hat build of OpenJDK 11 for Windows serves as a replacement for the Red Hat build of OpenJDK 11 and includes security

and bug fixes, and enhancements. For further information, refer to the release notes linked to in the References section. Issues addressed include denial of service and integer overflow vulnerabilities.

Red Hat Security Advisory 2023-4230-01

Red Hat Security Advisory 2023-4230-01 - 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 a use-after-free vulnerability.

Gentoo Linux Security Advisory 202307-01

Gentoo Linux Security Advisory 202307-1 - Multiple vulnerabilities have been discovered in OpenSSH, the worst of which could result in remote code execution. Versions less than 9.3_p2 are affected.

Red Hat Security Advisory 2023-4170-01

Red Hat Security Advisory 2023-4170-01 - The java-17-openjdk packages provide the OpenJDK 17 Java Runtime Environment and the OpenJDK 17 Java Software Development Kit. Issues addressed include denial of service and integer overflow vulnerabilities.

Red Hat Security Advisory 2023-4169-01

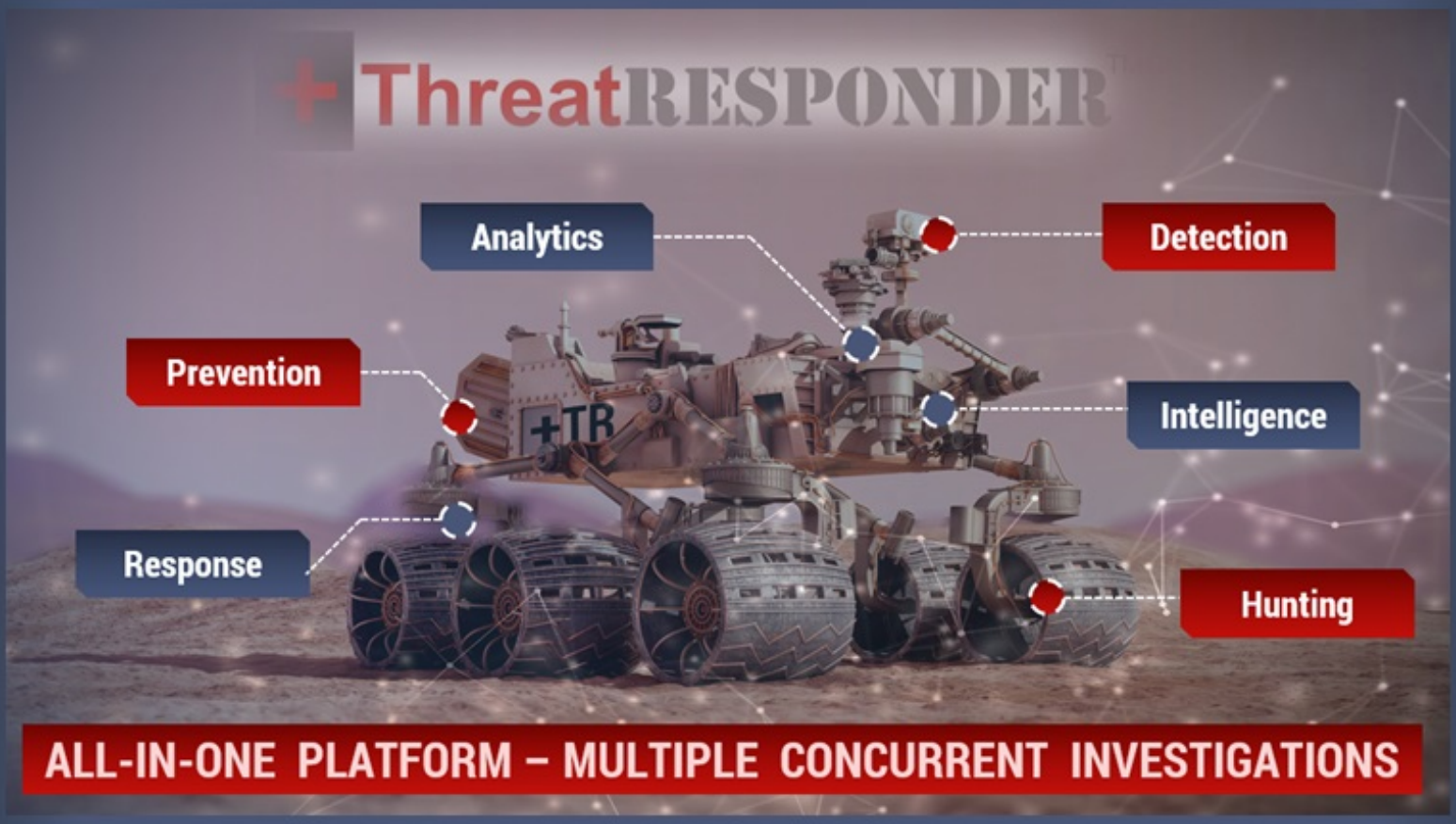
Red Hat Security Advisory 2023-4169-01 - The java-17-openjdk packages provide the OpenJDK 17 Java Runtime Environment and the OpenJDK 17 Java Software Development Kit. Issues addressed include denial of service and integer overflow vulnerabilities.

Are You...

- Spending several hours, days, or weeks conducting forensic investigations?
- Using different and unnecessary tools that pose correlation challenges?
- Wasting money on needless travels?
- Overworked, understaffed, and facing a backlog of cases?
- Uploading potentially sensitive files to VirusTotal or third-party sites?

Do DFIR Investigations Better

- Conduct DFIR investigations on any remote endpoint regardless of its geolocation – all on a single-pane of glass
- Perform in-depth forensics investigation dating back to the first day the target endpoint was installed
- Conduct full dynamic and static malware analyses with just a click of a mouse
- Conduct legally-defensible multiple DFIR cases simultaneously



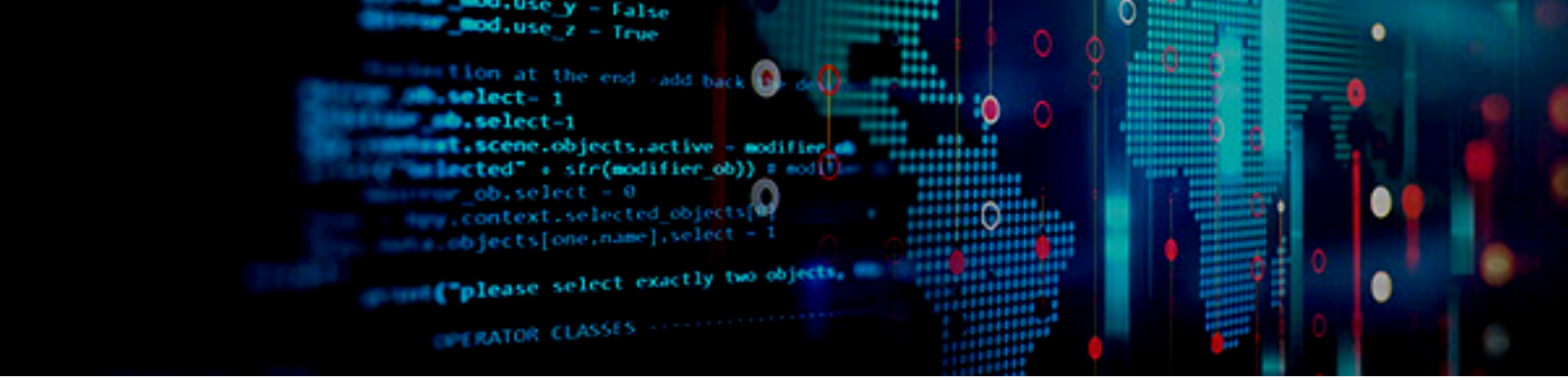
The Solution – ThreatResponder® Platform

ThreatResponder® Platform is an all-in-one cloud-native endpoint threat **detection**, **prevention**, **response**, **analytics**, **intelligence**, **investigation**, and **hunting** product

Get a Trial Copy

Mention **CODE: CIR-0119**

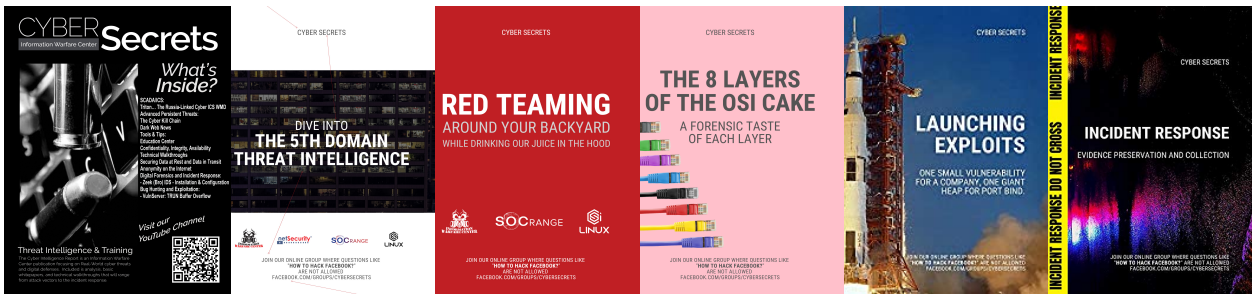
https://netsecurity.com



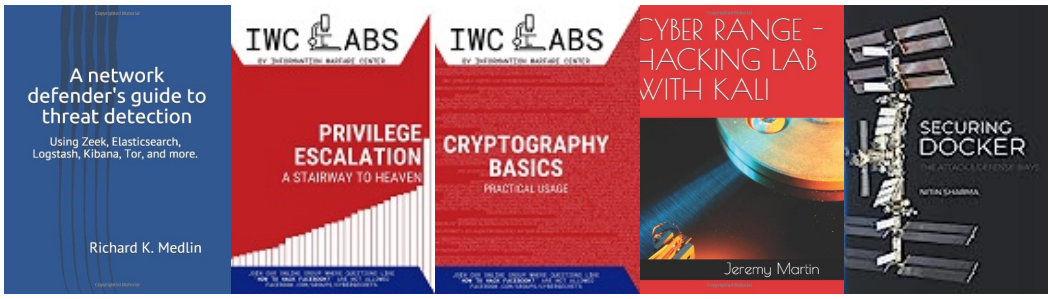
The Cyber Secrets publications on Amazon

The Cyber Weekl Awareness Report (WAR) is an Open Source Intelligence (AKA OSINT) resource centering around an array of subjects ranging from Exploits, Advanced Persistent Threat, National Infrastructure, Dark Web, Digital Forensics & Incident Response (DIFR), and the gambit of digital dangers.

Items that focus on cyber defense and DFIR usually spotlight capabilities in the CSI Linux environment. If interested in helping evolve, please let us know. The Cyber Secrets publications rotates between odd quarters issues focusing on Blue Team and the even issues on Red Team.



Other Publications from Information Warfare Center



CYBER WEEKLY AWARENESS REPORT

VISIT US AT **INFORMATIONWARFARECENTER.COM**

THE IWC ACADEMY
ACADEMY.INFORMATIONWARFARECENTER.COM

FACEBOOK GROUP
FACEBOOK.COM/GROUPS/CYBERSECRETS

CSI LINUX
CSILINUX.COM

CYBERSECURITY TV
CYBERSEC.TV

ARGOS
APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity

ThreatRESPONDER

Accredited Training Center
EC-Council

CYBERQ GROUP