Apr-10-23

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

April 10, 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

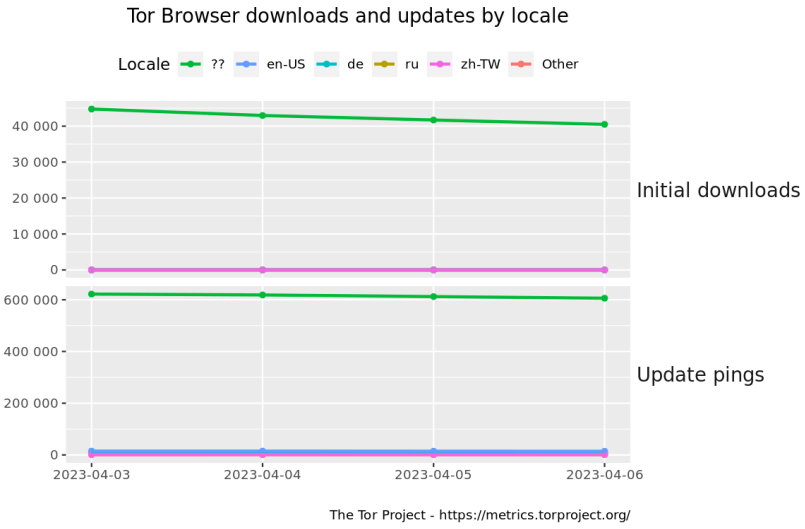
Internet Storm Center Infocon Status

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

* MSI Hit By Cyberattack, Warns Against Installing Knock-Off Firmware
* Dish Network Lawsuits Pile Up After Crippling Ransomware Attack
* Nexx Fixes Vulnerability By Breaking Customers' Devices
* Leaked Pentagon Documents Provide Rare Window Into Depth Of US Intelligence On Allies And Foes
* Vimeo To Pay $2.25M In AI-Related Biometric Privacy Lawsuit
* ACRO Yanks Portal Offline Amid Cyber Security Incident
* Robin Hood Hacker Suspected Of Selling Stolen Info Cuffed
* CAN Do Attitude: How Thieves Steal Cars Using Network Bus
* President Biden Delivers Remarks On "Risks Of Artificial Intelligence"
* Hackers Can Remotely Open Smart Garage Doors Across The World
* Log4j Bug Abused In New Proxyjacking Attacks To Resell Bandwidth , Abuse Enterprise Cloud
* JavaScript Malware Infects eFile.com Service Since Mid-March
* Popular Cybercrime Website Shut Down By Police
* Uber Driver Info Stolen Yet Again: This Time From Law Firm
* Microsoft Will Block Dangerous Extensions In OneNote
* UK's Offensive Hacking Unit Takes On Military Opponents And Terrorist Groups
* Hey Siri, Use This Ultrasound Attack To Disarm A Smart-Home System
* TikTok Fined Â£12.7m For UK Data Protection Law Breaches
* Feds Seize $112 Million From Accounts Used In Crypto Currency Scams
* Azure Bug Could Have Allowed Access To Critical Systems
* TMX Finance Breach Affects Nearly Five Million Customers
* Western Digital Confirms Digital Burglary, Calls In Law Enforcement
* Hackers Exploit WordPress Plugin Flaw That Gives Full Control Of Millions Of Sites
* Pinduoduo Is Straight Up Malware
* ChatGPT Banned In Italy Over Privacy Concerns

Krebs on Security

* FBI Seizes Bot Shop 'Genesis Market' Amid Arrests Targeting Operators, Suppliers
* A Serial Tech Investment Scammer Takes Up Coding?
* German Police Raid DDoS-Friendly Host 'FlyHosting'
* UK Sets Up Fake Booter Sites To Muddy DDoS Market
* Google Suspends Chinese E-Commerce App Pinduoduo Over Malware
* Why You Should Opt Out of Sharing Data With Your Mobile Provider
* Feds Charge NY Man as BreachForums Boss "Pompompurin"
* Microsoft Patch Tuesday, March 2023 Edition
* Two U.S. Men Charged in 2022 Hacking of DEA Portal
* Who's Behind the NetWire Remote Access Trojan?

Dark Reading

* Russia's Joker DPR Claims Access to Ukraine Troop Movement Data
* How and Why to Put Multicloud to Work
* Rethinking Cybersecurity's Structure & the Role of the Modern CISO
* Almost Half of Former Employees Say Their Passwords Still Work
* Microsoft, Fortra & Health-ISAC Team Up to Remove Illicit Cobalt Strike Tools
* TikTok, Other Mobile Apps Violate Privacy Regulations
* Close the Permissions Gap With Identity And Access Management For Multicloud Workforces
* Printers Pose Persistent Yet Overlooked Threat
* Bad Actors Will Use Large Language Models - but Defenders Can, Too
* Cybercriminals 'CAN' Steal Your Car, Using Novel IoT Hack
* Fight AI With AI
* Twitter 'Shadow Ban' Bug Gets Official CVE
* 'BEC 3.0' Is Here With Tax-Season QuickBooks Cyberattacks
* Australia Is Scouring the Earth for Cybercriminals - the US Should Too
* It Takes AI Security to Fight AI Cyberattacks
* What to Discuss at RSA Conference - and It's Not ChatGPT
* Styx Marketplace Provides Hub for Financial Cybercrime
* The Pope's Security Gets a Boost With Vatican's MDM Move
* Noname Security Announces Hardened API Security Platform
* BlackBerry Introduces Integrated Solution to Assure Secure Bi-Directional Response Communications Dur

The Hacker News

* Estonian National Charged in U.S. for Acquiring Electronics and Metasploit Pro for Russian Military
* Hackers Flood NPM with Bogus Packages Causing a DoS Attack
* Top 10 Cybersecurity Trends for 2023: From Zero Trust to Cyber Insurance
* Over 1 Million WordPress Sites Infected by Balada Injector Malware Campaign
* Protecting your business with Wazuh: The open source security platform
* CISA Warns of 5 Actively Exploited Security Flaws: Urgent Action Required
* Taiwanese PC Company MSI Falls Victim to Ransomware Attack
* Iran-Based Hackers Caught Carrying Out Destructive Attacks Under Ransomware Guise
* Apple Releases Updates to Address Zero-Day Flaws in iOS, iPadOS, macOS, and Safari
* Expert-Led Webinar: Learn Proven Strategies to Secure Your Identity Perimeter
* Researchers Discover Critical Remote Code Execution Flaw in vm2 Sandbox Library
* Researchers Uncover Thriving Phishing Kit Market on Telegram Channels
* Microsoft Takes Legal Action to Disrupt Cybercriminals' Illegal Use of Cobalt Strike Tool
* Are Source Code Leaks the New Threat Software vendors Should Care About?
* CISA Warns of Critical ICS Flaws in Hitachi, mySCADA, ICL, and Nexx Products

Security Week

* MSI Confirms Cyberattack, Issues Firmware Download Guidance
* Microsoft: Iranian Gov Hackers Caught in Azure Wiper Attacks
* Veritas Vulnerabilities Exploited in Ransomware Attacks Added to CISA 'Must Patch' List
* Most Attack Paths Are Dead Ends, but 2% Lead to Critical Assets: Report
* Apple Ships Urgent iOS Patch for Newly Exploited Zero-Days
* DoJ: Estonian Man Tried to Acquire US-Made Hacking Tools for Russia
* Watch: How to Build Resilience Against Emerging Cyber Threats
* Secret US Documents on Ukraine War Plan Spill Onto Internet: Report
* Tesla Retail Tool Vulnerability Led to Account Takeover
* Sophos Patches Critical Code Execution Vulnerability in Web Security Appliance

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* Alarming Tax Phishing Campaign Targets US with Malware
* [INFOGRAPHIC] The Forrester Total Economic Impactâ„¢ of KnowBe4 by the Numbers
* Your KnowBe4 Fresh Content Updates from March 2023
* Recently Exposed North Korean Threat Actor APT43 Targeting Organizations With Spear Phishing
* New Emotet Phishing Campaign Pretends to be the IRS Delivering W-9 Forms
* FBI: Business Email Compromise Attacks Are Being Used to Make Bulk Goods Purchases from Vendors
* 1 in 8 Email Threats Now Make It Past Email Security Solutions
* "We are hurtling toward a glitchy, spammy, scammy, AI-powered internet."
* FBI: 870 Critical Infrastructure Organizations Were the Victim of Ransomware in 2022
* That's Not Actually Mr. Musk, That's a Scam

ISC2.org Blog

* IDENTITY MANAGEMENT DAY 2023: Advice from Cyber Pros
* Push Notification Is More Secure Than SMS 2FA, So Why the Reluctance to Enable It?
* LATEST CYBERTHREATS AND ADVISORIES - APRIL 7, 2023
* (ISC)² Supports Cyber Newcomers
* CYBERSECURITY INDUSTRY NEWS REVIEW - APRIL 4, 2023

HackRead

* Alcasec Hacker, aka "Robin Hood of Spanish Hackers," Arrested
* What is Cloud Mining and How Does it Work?
* Cybercriminals Exploit CAN Injection Hack to Steal Cars
* How to Create a Mobile Application for Android OS Step by Step?
* How to Create and Manage Groups on iPhone
* Phishers Now Actively Automating Scams with Telegram
* Tesla Employees Allegedly Shared Customers' Private Videos and Photos

Koddos

* Alcasec Hacker, aka "Robin Hood of Spanish Hackers," Arrested
* What is Cloud Mining and How Does it Work?
* Cybercriminals Exploit CAN Injection Hack to Steal Cars
* How to Create a Mobile Application for Android OS Step by Step?
* How to Create and Manage Groups on iPhone
* Phishers Now Actively Automating Scams with Telegram
* Tesla Employees Allegedly Shared Customers' Private Videos and Photos

Naked Security

* Popular server-side JavaScript security sandbox "vm2" patches remote execution hole
* Apple issues emergency patches for spyware-style 0-day exploits - update now!
* S3 Ep129: When spyware arrives from someone you trust
* Hack and enter! The "secure" garage doors that anyone can open from anywhere - what you need to know
* Einstein tilings - the amazing "Hat" shape that never repeats!
* Researchers claim they can bypass Wi-Fi encryption (briefly, at least)
* World Backup Day is here again - 5 tips to keep your precious data safe
* Supply chain blunder puts 3CX telephone app users at risk
* S3 Ep128: So you want to be a cybercriminal? [Audio + Text]
* Cops use fake DDoS services to take aim at wannabe cybercriminals

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 LockBit Changed Cybersecurity Forever
* Using a Private Version of ChatGPT as an Enabler for Risk and Compliance
* How to Defend Against Extortion Groups Like Lapsus$
* X-Force Identifies Vulnerability in IoT Platform
* Locks, Stocks and Brokers: Hackers and Insider Trading
* New Generation of Phishing Hides Behind Trusted Services
* The Important Role of SOAR in Cybersecurity
* Is It Time to Start Hiding Your Work Emails?
* 2022 Industry Threat Recap: Finance and Insurance
* And Stay Out! Blocking Backdoor Break-Ins

InfoWorld

* The AI singularity is here
* Build AI apps faster with low-code and no-code
* C rival Zig language cracks Tiobe index top 50
* How generative AI can hurt cloud operations
* Modern data infrastructures don't do ETL
* Meta open-sources 'significantly faster' build system
* How to use the unit of work pattern in ASP.NET Core
* The Mastodon plugin is now available on the Steampipe Hub
* Here's why Oracle is offering Database 23c free to developers
* ECMAScript 2023 spec for JavaScript adds methods for arrays

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

* 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
* The Fascinating Ineptitude Of Russian Military Communications
* Cyberwar In The Ukraine Conflict
* Our New Approach To Conference Listings
* Marketing Cybersecurity In 2023

Google Zero Day Project

* Multiple Internet to Baseband Remote Code Execution Vulnerabilities in Exynos Modems
* Exploiting null-dereferences in the Linux kernel

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.

* YetiCTF2023
* HackPack CTF 2023
* Midnight Flag - Black Box
* PlaidCTF 2023
* Summit CTF
* Wayne State University - Capture-The-Flag
* Texas Security Awareness Week 2023
* JerseyCTF III
* CyberHavoc CTF
* Space Heroes CTF

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

* tcpdump 4.99.4
* AIDE 0.18.2
* GNUnet P2P Framework 0.19.4
* Global Socket 1.4.40
* GRR 3.4.6.7
* OpenSSL Toolkit 3.1.0
* OpenSSH 9.3p1
* I2P 2.2.0
* Packet Fence 12.2.0
* AIDE 0.18.1

Kali Linux Tutorials

* Blackbird - OSINT Tool to Find Accounts Using Username
* GPT_Vuln-analyzer : Uses ChatGPT API To Create Vulnerability Reports Based On Nmap Scan
* Ator : Authentication Token Obtain and Replace Extender
* Fingerprintx - Tool to Fingerprint Services Running on Ports
* NimPlant : A Light-Weight First-Stage C2 Implant Written In Nim
* Tool-X - Single Click Installer For 70 Hacking Tools on Android
* Subfinder - A New Tool to Discover Subdomains for Websites
* Hunxploit04 - A new OSINT Tools for Information Gathering
* FindUncommonShares A Python Equivalent Of PowerView's Invoke-ShareFinder.ps1 Allowing To Quickly Fin
* CertVerify : A Scanner That Files With Compromised Or Untrusted Code Signing Certificates

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

* Cloud-Powered DFIR: Harnessing the cloud to improve investigator efficiency
* Breaking the Ransomware Tool Set: When a Threat Actor Opsec
* The Way to a Stakeholder's Heart is by Providing Value: Measuring Success of Your CTI Program
* The Report Writer's Grimoire

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

* Should AI Training Be Paused? - ThreatWire
* Cerebral App Leaks Telehealth Medical Data - ThreatWire
* NEW Powershell features in DuckyScript 3.0

The PC Security Channel [TPSC]

* 3CX: How this malware hacked almost every business
* Windows Defender ATP Any Good?

Eli the Computer Guy

* Python Intro - Hands on Class
* CHATGPT INTRO - Silicon Dojo Seminar
* DJANGO INTRO - Seminar for Silicon Dojo
* PYTHON INTRO - Seminar for Silicon Dojo

Security Now

* Zombie Software - ChatGPT Ban, Hacking the Pentagon
* Microsoft's Email Extortion - Pwn2Own, Edge Crypto Wallet

Troy Hunt

* Weekly Update 342

Intel Techniques: The Privacy, Security, & OSINT Show

* 292-Vital News & Updates
* 291-Mobile App Security & Audio Transcription

Proof of Concept (PoC) & Exploits

Packet Storm Security

* ChurchCRM 4.5.1 SQL Injection
* NotrinosERP 0.7 SQL Injection
* Roxy Fileman 1.4.5 Shell Upload
* Chrome base::SampleVectorBase::MoveSingleSampleToCounts Heap Buffer Overflow
* Chrome base::debug::ActivityUserData::ActivityUserData Heap Buffer Overflow
* Windows Kernel Registry Key Issue
* BrainyCP 1.0 Remote Code Execution
* X2CRM 6.6 / 6.9 Cross Site Scripting
* pfsenseCE 2.6.0 Protection Bypass
* Online Computer And Laptop Store 1.0 Shell Upload
* Goanywhere Encryption Helper 7.1.1 Remote Code Execution
* WebsiteBaker 2.13.3 Cross Site Scripting
* ZCBS / ZBBS / ZPBS 4.14k Cross Site Scripting
* ESET Service 16.0.26.0 Unquoted Service Path
* dotclear 2.25.3 Shell Upload
* Paradox Security Systems IPR512 Denial Of Service
* Palo Alto Cortex XSOAR 6.5.0 Cross Site Scripting
* Symantec Messaging Gateway 10.7.4 Cross Site Scripting
* Medicine Tracker System 1.0 SQL Injection
* ActFax 10.10 Unquoted Service Path
* Online Appointment System 1.0 Cross Site Scripting
* ENTAB ERP 1.0 Information Disclosure
* Restaurant Management System 1.0 SQL Injection
* Altenergy Power Control Software C1.2.5 Command Injection
* Icinga Web 2.10 Arbitrary File Disclosure

CXSecurity

* pdfkit v0.8.7.2 Command Injection
* Kimai-1.30.10 SameSite Cookie-Vulnerability session hijacking
* sudo 1.9.12p1 Privilege Escalation
* TP-Link TL-WR902AC firmware 210730 (V3) Remote Code Execution (RCE) (Authenticated)
* Scdbg 1.0 Buffer overflow DoS
* Sysax Multi Server 6.95 Password Denial of Service (PoC)
* Scdbg 1.0 Denial Of Service

Proof of Concept (PoC) & Exploits

Exploit Database

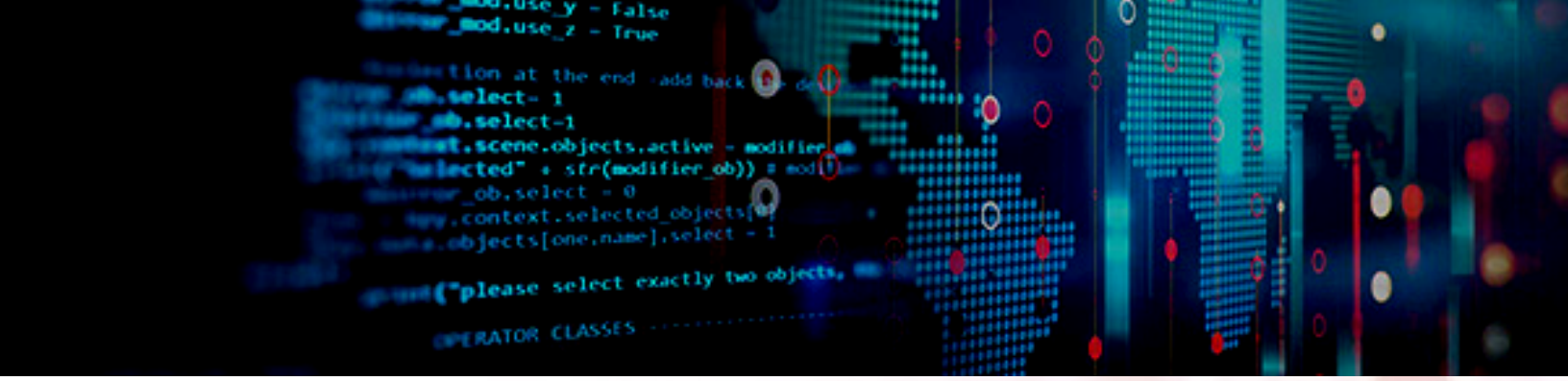
* [local] Microsoft Edge (Chromium-based) Webview2 1.0.1661.34 - Spoofing
* [webapps] Online Computer and Laptop Store 1.0 - Remote Code Execution (RCE)
* [webapps] BrainyCP V1.0 - Remote Code Execution
* [dos] Paradox Security Systems IPR512 - Denial Of Service
* [webapps] Roxy Fileman 1.4.5 - Arbitrary File Upload
* [webapps] ever gauzy v0.281.9 - JWT weak HMAC secret
* [webapps] dotclear 2.25.3 - Remote Code Execution (RCE) (Authenticated)
* [webapps] pfsenseCE v2.6.0 - Anti-brute force protection bypass
* [local] ESET Service 16.0.26.0 - 'Service ekrn' Unquoted Service Path
* [webapps] Pentaho BA Server EE 9.3.0.0-428 - Remote Code Execution (RCE) (Unauthenticated)
* [webapps] WebsiteBaker v2.13.3 - Cross-Site Scripting (XSS)
* [dos] Microsoft Windows 11 - 'cmd.exe' Denial of Service
* [webapps] ZCBS/ZBBS/ZPBS v4.14k - Reflected Cross-Site Scripting (XSS)
* [webapps] X2CRM v6.6/6.9 - Reflected Cross-Site Scripting (XSS) (Authenticated)
* [webapps] X2CRM v6.6/6.9 - Stored Cross-Site Scripting (XSS) (Authenticated)
* [webapps] Online-Pizza-Ordering -1.0 - Remote Code Execution (RCE)
* [webapps] Palo Alto Cortex XSOAR 6.5.0 - Stored Cross-Site Scripting (XSS)
* [webapps] Symantec Messaging Gateway 10.7.4 - Stored Cross-Site Scripting (XSS)
* [local] Stonesoft VPN Client 6.2.0 / 6.8.0 - Local Privilege Escalation
* [webapps] Suprema BioStar 2 v2.8.16 - SQL Injection
* [webapps] Goanywhere Encryption helper 7.1.1 - Remote Code Execution (RCE)
* [webapps] Medicine Tracker System v1.0 - Sql Injection
* [webapps] Online Appointment System V1.0 - Cross-Site Scripting (XSS)
* [local] RSA NetWitness Platform 12.2 - Incorrect Access Control / Code Execution
* [webapps] ENTAB ERP 1.0 - Username PII leak

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*

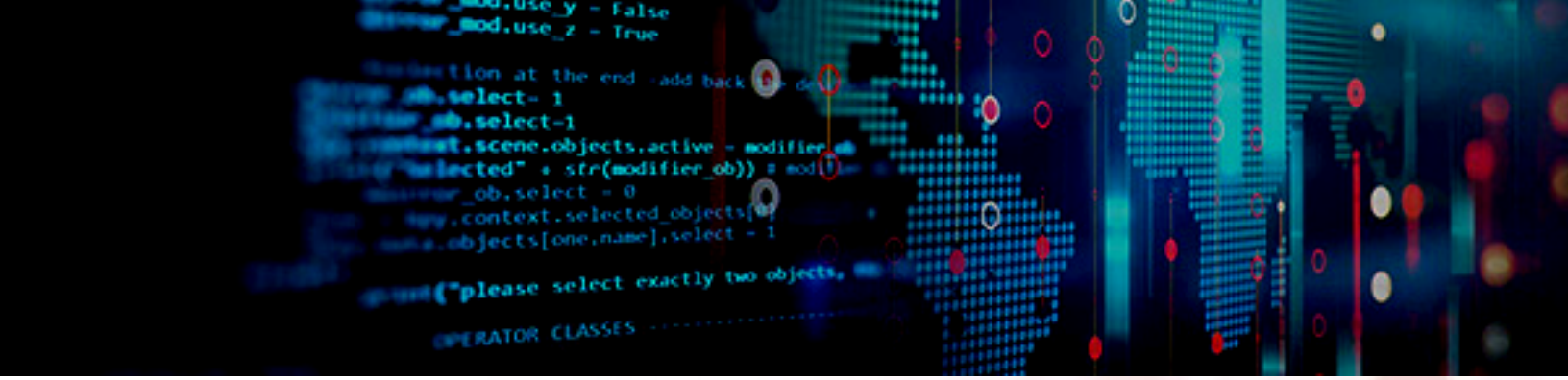
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://lifelibrary.m-society.go.th/kurd.html
https://lifelibrary.m-society.go.th/kurd.html notified by 0x1998
https://mitigazione-rischioidrogeologico.regione.campania.it/kurd.html
https://mitigazione-rischioidrogeologico.regione.campania.it/kurd.html notified by 0x1998
https://bumnetnarong.chaiyaphum.police.go.th/kurd.html
https://bumnetnarong.chaiyaphum.police.go.th/kurd.html notified by 0x1998
http://info.army3.mi.th/kurd.html
http://info.army3.mi.th/kurd.html notified by 0x1998
https://disdikbud.mukomukokab.go.id/lol.txt
https://disdikbud.mukomukokab.go.id/lol.txt notified by xNot_RespondinGx
https://setda.mukomukokab.go.id/lol.txt
https://setda.mukomukokab.go.id/lol.txt notified by xNot_RespondinGx
http://inspektorat.mukomukokab.go.id/lol.txt
http://inspektorat.mukomukokab.go.id/lol.txt notified by xNot_RespondinGx
https://diskominfo.mukomukokab.go.id/lol.txt
https://diskominfo.mukomukokab.go.id/lol.txt notified by xNot_RespondinGx
https://bkpsdm.mukomukokab.go.id/lol.txt
https://bkpsdm.mukomukokab.go.id/lol.txt notified by xNot_RespondinGx
https://umkm.badungkab.go.id/back.html
https://umkm.badungkab.go.id/back.html notified by Moroccan Revolution
https://job.ocsc.go.th/ma.html
https://job.ocsc.go.th/ma.html notified by Moroccan Revolution
http://mjob.ocsc.go.th/ma.html
http://mjob.ocsc.go.th/ma.html notified by Moroccan Revolution
https://recadastramento.tenenteananias.rn.gov.br
https://recadastramento.tenenteananias.rn.gov.br notified by B1G0D1N
https://publicacoes.tenenteananias.rn.gov.br/login.php
https://publicacoes.tenenteananias.rn.gov.br/login.php notified by B1G0D1N
https://jom.martins.rn.gov.br
https://jom.martins.rn.gov.br notified by B1G0D1N
https://publicacoes.martins.rn.gov.br/login.php
https://publicacoes.martins.rn.gov.br/login.php notified by B1G0D1N
http://covid.martins.rn.gov.br
http://covid.martins.rn.gov.br notified by B1G0D1N

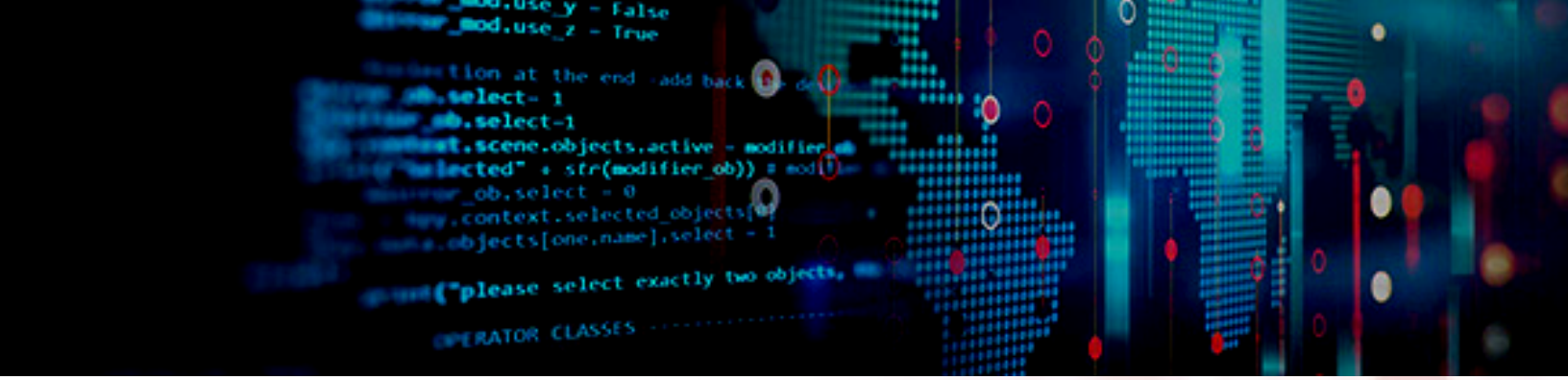


Dark Web News

Darknet Live

US Treasury Sanctions Genesis Market
UK Trio Imprisoned for Distributing Counterfeit Xanax
Austrian Duo Purchased Ecstasy on the Dark Web
Polish Man Sentenced for Distributing Drugs on the Dark Web

Dark Web Link



Trend Micro Anti-Malware Blog

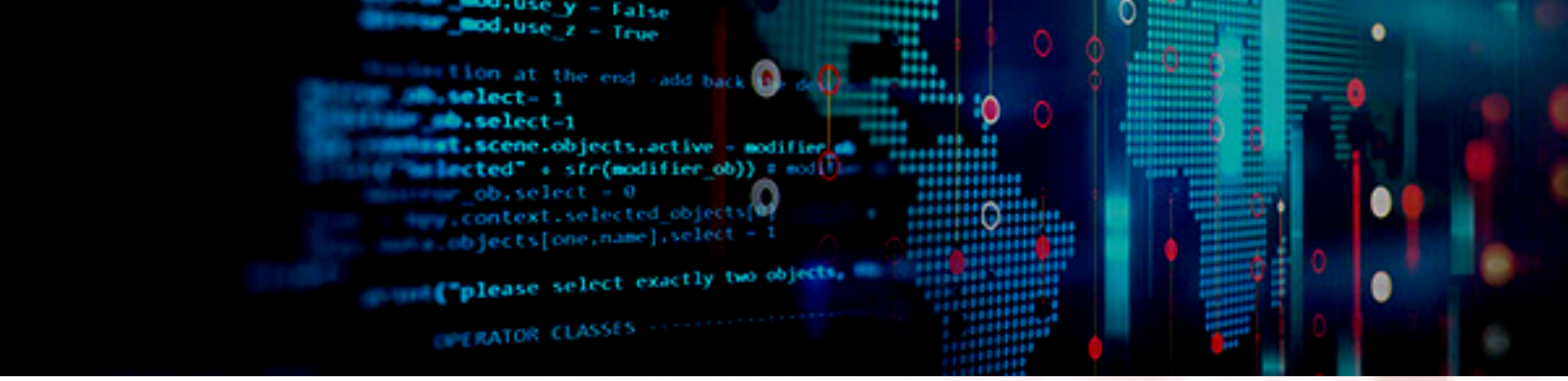
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

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

FireEye

* Metasploit Weekly Wrap-Up
* [The Lost Bots] S03E02: Finding unknowns, even spy balloons
* Using InsightVM Remediation Projects To Ensure Accountability
* Metasploit Weekly Wrap-up
* What's New in InsightVM and Nexpose: Q1 2023 in Review
* Velociraptor Version 0.6.8 Available Now
* Rapid7 Announces Partner of the Year Awards 2023 Winners
* Backdoored 3CXDesktopApp Installer Used in Active Threat Campaign
* Executive Webinar: Confronting Security Fears to Control Cyber Risk, Part Three
* Multiple Vulnerabilities in Rocket Software UniRPC server (Fixed)



Advisories

US-Cert Alerts & bulletins

* CISA Adds Two Known Exploited Vulnerabilities to Catalog
* CISA Adds Five Known Exploited Vulnerabilities to Catalog
* Cisco Releases Security Advisories for Multiple Products
* CISA Releases Seven Industrial Control Systems Advisories
* CISA Releases One Industrial Control Systems Advisory
* CISA Adds One Known Exploited Vulnerability to Catalog
* Mozilla Releases Security Update for Thunderbird 102.9.1
* Samba Releases Security Updates for Multiple Versions of Samba
* #StopRansomware: LockBit 3.0
* Threat Actors Exploit Progress Telerik Vulnerability in U.S. Government IIS Server
* Vulnerability Summary for the Week of September 18, 2006
* Vulnerability Summary for the Week of June 25, 2012

Zero Day Initiative Advisories

ZDI-CAN-20853: BlueZ
A CVSS score 5.4 (AV:A/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:L) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-04-07, 3 days ago. The vendor is given until 2023-08-05 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-20854: BlueZ
A CVSS score 5.4 (AV:A/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:L) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-04-07, 3 days ago. The vendor is given until 2023-08-05 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-20771: Microsoft
A CVSS score 4.4 (AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Nitesh Surana (@_niteshsurana) & David Fiser (@anu4is) of Project Nebula, Trend Micro Research' was reported to the affected vendor on: 2023-04-07, 3 days ago. The vendor is given until 2023-08-05 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-20663: PDF-XChange
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2023-04-07, 3 days ago. The vendor is given until 2023-08-05 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-20798: Triangle MicroWorks
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 'Uri Katz of

Claroty Team82' was reported to the affected vendor on: 2023-04-06, 4 days ago. The vendor is given until 2023-08-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20562: Ashlar-Vellum

A CVSS score 7.0 (AV:L/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-04-06, 4 days ago. The vendor is given until 2023-08-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20797: Triangle MicroWorks

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 'Uri Katz of Claroty Team82' was reported to the affected vendor on: 2023-04-06, 4 days ago. The vendor is given until 2023-08-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20661: 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 & Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2023-04-06, 4 days ago. The vendor is given until 2023-08-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20615: Triangle MicroWorks

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 'Uri Katz of Claroty Team82' was reported to the affected vendor on: 2023-04-06, 4 days ago. The vendor is given until 2023-08-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20799: Triangle MicroWorks

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 'Uri Katz of Claroty Team82' was reported to the affected vendor on: 2023-04-06, 4 days ago. The vendor is given until 2023-08-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20785: Delta Electronics

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Piotr Bazydlo (@chudypb) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-04-06, 4 days ago. The vendor is given until 2023-08-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20450: Parallels

A CVSS score 8.2 (AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'war10ck' was reported to the affected vendor on: 2023-04-06, 4 days ago. The vendor is given until 2023-08-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20273: Microsoft

A CVSS score 6.5 (AV:N/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: 2023-04-06, 4 days ago. The vendor is given until 2023-08-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20527: Linux

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 'Nassim Asrir' was reported to the affected vendor on: 2023-04-06, 4 days ago. The vendor is given until 2023-08-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20784: Microsoft

A CVSS score 9.9 (AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Nitesh Surana (@_niteshsurana) of Trend Micro Research' was reported to the affected vendor on: 2023-04-06, 4 days ago. The vendor is given until 2023-08-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20720: Microsoft

A CVSS score 5.0 (AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'vcslab of Team Viettel (@vcslab)' was reported to the affected vendor on: 2023-04-05, 5 days ago. The vendor is given until 2023-08-03 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-20735: 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 'Thomas Imbert (@masthoon) from Synacktiv (@Synacktiv)' was reported to the affected vendor on: 2023-04-05, 5 days ago. The vendor is given until 2023-08-03 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-20751: Microsoft

A CVSS score 7.5 (AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'vcslab of Team Viettel (@vcslab)' was reported to the affected vendor on: 2023-04-05, 5 days ago. The vendor is given until 2023-08-03 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-20807: Microsoft

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: 2023-03-31, 10 days ago. The vendor is given until 2023-07-29 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-20669: Oracle

A CVSS score 6.0 (AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N) severity vulnerability discovered by 'Bien Pham (@bienpnn) from Qrious Security (@qriousec)' was reported to the affected vendor on: 2023-03-30, 11 days ago. The vendor is given until 2023-07-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20743: 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 'AbdulAziz Hariri of Haboob SA' was reported to the affected vendor on: 2023-03-30, 11 days ago. The vendor is given until 2023-07-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20746: 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 'AbdulAziz Hariri of Haboob SA' was reported to the affected vendor on: 2023-03-30, 11 days ago. The vendor is given until 2023-07-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20744: 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 'AbdulAziz Hariri of Haboob SA' was reported to the affected vendor on: 2023-03-30, 11 days ago. The vendor is given until 2023-07-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20747: 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 'AbdulAziz Hariri of Haboob SA' was reported to the affected vendor on: 2023-03-30, 11 days ago. The vendor is given until 2023-07-28 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Debian Security Advisory 5384-1

Debian Linux Security Advisory 5384-1 - Multiple security vulnerabilities have been discovered in OpenImageIO, a library for reading and writing images. Buffer overflows and out-of-bounds read and write programming errors may lead to a denial of service (application crash) or the execution of arbitrary code if a malformed image file is processed.

Red Hat Security Advisory 2023-1549-01

Red Hat Security Advisory 2023-1549-01 - Virtual Network Computing is a remote display system which allows users to view a computing desktop environment not only on the machine where it is running, but from anywhere on the Internet and from a wide variety of machine architectures. TigerVNC is a suite of VNC servers and clients. Issues addressed include privilege escalation and use-after-free vulnerabilities.

Ubuntu Security Notice USN-6003-1

Ubuntu Security Notice 6003-1 - Xi Lu discovered that Emacs did not properly handle certain inputs. An attacker could possibly use this issue to execute arbitrary commands.

Red Hat Security Advisory 2023-1670-01

Red Hat Security Advisory 2023-1670-01 - The httpd packages provide the Apache HTTP Server, a powerful, efficient, and extensible web server.

Red Hat Security Advisory 2023-1525-01

Red Hat Security Advisory 2023-1525-01 - 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 4.9.59.

Ubuntu Security Notice USN-6001-1

Ubuntu Security Notice 6001-1 - Xuewei Feng, Chuanpu Fu, Qi Li, Kun Sun, and Ke Xu discovered that the TCP implementation in the Linux kernel did not properly handle IPID assignment. A remote attacker could use this to cause a denial of service or inject forged data. Ke Sun, Alyssa Milburn, Henrique Kawakami, Emma Benoit, Igor Chervatyuk, Lisa Aichele, and Thais Moreira Hamasaki discovered that the Spectre Variant 2 mitigations for AMD processors on Linux were insufficient in some situations. A local attacker could possibly use this to expose sensitive information.

Ubuntu Security Notice USN-6000-1

Ubuntu Security Notice 6000-1 - It was discovered that the Upper Level Protocol subsystem in the Linux kernel did not properly handle sockets entering the LISTEN state in certain protocols, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. It was discovered that the NVMe driver in the Linux kernel did not properly handle reset events in some situations. A local attacker could use this to cause a denial of service.

Ubuntu Security Notice USN-5996-1

Ubuntu Security Notice 5996-1 - It was discovered that Liblouis incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service.

Ubuntu Security Notice USN-5998-1

Ubuntu Security Notice 5998-1 - It was discovered that the SocketServer component of Apache Log4j 1.2 incorrectly handled deserialization. An attacker could possibly use this issue to execute arbitrary code. This issue only affected Ubuntu 16.04 ESM. It was discovered that the JMSSink component of Apache Log4j 1.2 incorrectly handled deserialization. An attacker could possibly use this issue to execute arbitrary code.

Red Hat Security Advisory 2023-1666-01

Red Hat Security Advisory 2023-1666-01 - 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.

Debian Security Advisory 5383-1

Debian Linux Security Advisory 5383-1 - It was discovered that Ghostscript, the GPL PostScript/PDF interpreter, is prone to a buffer overflow vulnerability in the (T)BCP encoding filters, which could result in the

execution of arbitrary code if malformed document files are processed (despite the -dSAFER sandbox being enabled).

Debian Security Advisory 5381-1

Debian Linux Security Advisory 5381-1 - Several security vulnerabilities have been discovered in the Tomcat servlet and JSP engine.

Debian Security Advisory 5382-1

Debian Linux Security Advisory 5382-1 - It was reported that cairosvg, a SVG converter based on Cairo, can send requests to external hosts when processing specially crafted SVG files with external file resource loading. An attacker can take advantage of this flaw to perform a server-side request forgery or denial of service. Fetching of external files is disabled by default with this update.

Ubuntu Security Notice USN-5999-1

Ubuntu Security Notice 5999-1 - It was discovered that trim-newlines incorrectly handled certain inputs. If a user or an automated system were tricked into opening a specially crafted input file, a remote attacker could possibly use this issue to cause a denial of service.

Ubuntu Security Notice USN-5997-1

Ubuntu Security Notice 5997-1 - It was discovered that IPMItool was not properly checking the data received from a remote LAN party. A remote attacker could possibly use this issue to to cause a crash or arbitrary code execution.

Red Hat Security Advisory 2023-1661-01

Red Hat Security Advisory 2023-1661-01 - AMQ Broker is a high-performance messaging implementation based on ActiveMQ Artemis. It uses an asynchronous journal for fast message persistence, and supports multiple languages, protocols, and platforms. This release of Red Hat AMQ Broker 7.11.0 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, information leakage, and traversal vulnerabilities.

Red Hat Security Advisory 2023-1660-01

Red Hat Security Advisory 2023-1660-01 - 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.

Red Hat Security Advisory 2023-1639-01

Red Hat Security Advisory 2023-1639-01 - OpenShift API for Data Protection enables you to back up and restore application resources, persistent volume data, and internal container images to external backup storage. OADP enables both file system-based and snapshot-based backups for persistent volumes. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2023-1662-01

Red Hat Security Advisory 2023-1662-01 - 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.

Red Hat Security Advisory 2023-1659-01

Red Hat Security Advisory 2023-1659-01 - 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.

Red Hat Security Advisory 2023-1630-01

Red Hat Security Advisory 2023-1630-01 - Red Hat Satellite is a system management solution that allows organizations to configure and maintain their systems without the necessity to provide public Internet access to their servers or other client systems. Issues addressed include an information leakage vulnerability.

Red Hat Security Advisory 2023-1504-01

Red Hat Security Advisory 2023-1504-01 - 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 4.11.34.

Red Hat Security Advisory 2023-1591-01

Red Hat Security Advisory 2023-1591-01 - The pcs packages provide a command-line configuration system for

the Pacemaker and Corosync utilities.

Red Hat Security Advisory 2023-1600-01

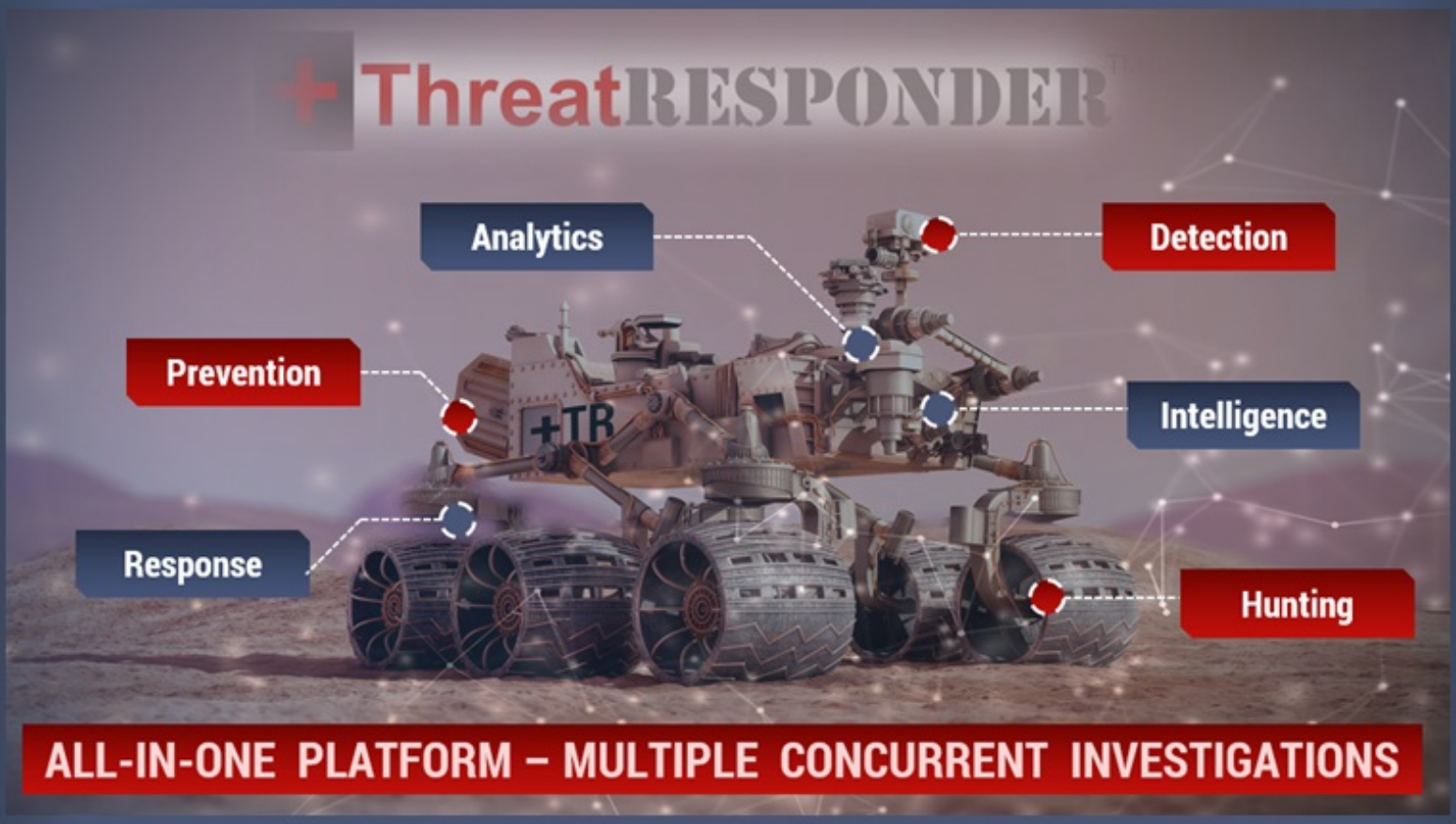
Red Hat Security Advisory 2023-1600-01 - Virtual Network Computing is a remote display system which allows users to view a computing desktop environment not only on the machine where it is running, but from anywhere on the Internet and from a wide variety of machine architectures. TigerVNC is a suite of VNC servers and clients. Issues addressed include privilege escalation and use-after-free vulnerabilities.

Are You...

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

Do DFIR Investigations Better

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



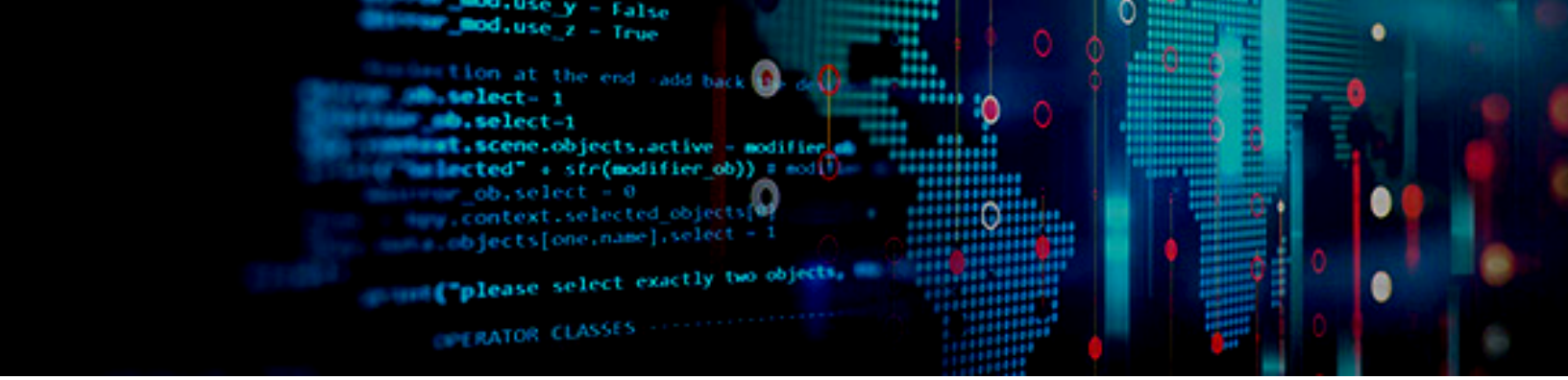
The Solution – ThreatResponder® Platform

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

Get a Trial Copy

Mention **CODE: CIR-0119**

https://netsecurity.com

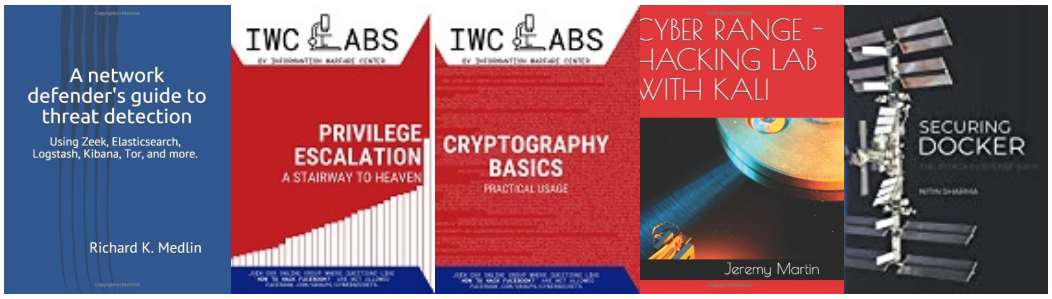


The Cyber Secrets publications on Amazon

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

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

Other Publications from Information Warfare Center



CYBER WEEKLY AWARENESS REPORT

VISIT US AT **INFORMATIONWARFARECENTER.COM**

THE IWC ACADEMY
ACADEMY.INFORMATIONWARFARECENTER.COM

FACEBOOK GROUP
FACEBOOK.COM/GROUPS/CYBERSECRETS

CSI LINUX
CSILINUX.COM

CYBERSECURITY TV
CYBERSEC.TV

ARGOS
APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity

ThreatRESPONDER

Accredited Training Center
EC-Council

CYBERQ GROUP