Jul-31-23

CYBER WEEKLY AWARENESS REPORT

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

July 31, 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.

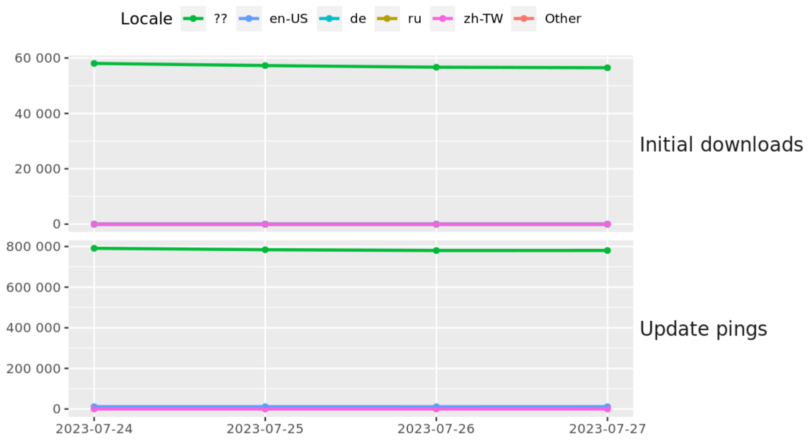
INTERNET STORM CENTER
infocon:GREEN
http://isc.sans.edu

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.

Tor Browser downloads and updates by locale



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

Interesting News

* Free Cyberforensics Training - CSI Linux Basics

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

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

Index of Sections

LATEST NEWS

Packet Storm Security

* Exploitation Of Recent Citrix ShareFile RCE Vulnerability Begins
* US Senator Blasts Microsoft For Negligent Cybersecurity Practices
* MOVEit Bug Tied To Breach Of Up To 11M Records Via Govt Contractor
* NATO Probes Hacktivist Crew's Boasts Of Stolen Data
* Russia Throws Group-IB Founder In The Clink For Treason
* The UFO Hearing Got Pretty Interesting
* Infostealer Incidents More Than Doubled In Q1 2023
* Axis Door Controller Vulnerability Exposes Facilities to Threats
* Two New Vulnerabilities Could Affect 40% Of Ubuntu Cloud Workloads
* Privacy Group Challenges Ryanair's Use Of Facial Recognition
* SEC Approves New Cyber Reporting Regulations For Public Companies
* New AI Phishing Tool FraudGPT Tied To Same Group Behind WormGPT
* Crypto Bills To Face Congressional Committee Vote
* Dozens Of Organizations Targeted By Akira Ransomware
* Congress Is About To Stream UFO Hearings On YouTube At 10AM EST
* Ivanti Zero-Day Vuln Exploited In Attack On Norwegian Government
* China-Backed Hackers Suspected In NetScaler RCE Attacks
* Apple Patches Another Kernel Flaw Exploited In Operation Triangulation
* AMD Zenbleed Chip Bug Leaks Secrets Fast And Easy
* Researchers Find Backdoor In Encrypted Police And Military Radios
* MOVEit Hack Could Earn Cybercriminals $100 Million
* Los Angeles SIM Swapper Pleads Guilty To Cybercrime Charges
* WebBoss.io CMS Concerns: A Tale Of Neglect And Unresponsiveness
* OpenMeetings Flaws Allow Hackers To Execute Code And Hijack
* NetScaler RCE Abused To Pilfer Critical Infra Active Directory Data

Krebs on Security

* Russia Sends Cybersecurity CEO to Jail for 14 Years
* Who and What is Behind the Malware Proxy Service SocksEscort?
* 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

LATEST NEWS

Dark Reading

* Healthcare Innovation: A Safe and Secure Approach
* Hack Crew Responsible for Stolen Data, NATO Investigates Claims
* CherryBlos Malware Uses OCR to Pluck Android Users' Cryptocurrency
* Stark#Mule Malware Campaign Targets Koreans, Uses US Army Documents
* Senator Blasts Microsoft for Negligence in 365 Email Breach
* Choose the Best Biometrics Authentication for Your Use Case
* Another AI Pitfall: Digital Mirroring Opens New Cyberattack Vector
* IT Ops and Security Teams Need Automation, Not Couples Therapy
* Cyclops Launches From Stealth With Generative AI-Based Search Tool
* Why CISOs Should Get Involved With Cyber Insurance Negotiation
* Despite Post-Log4j Security Gains, Developers Can Still Improve
* 7 in 10 MSPs Name Data Security and Network Security As Their Top IT Priorities for 2023
* CompTIA ChannelCon Technology Vendor Fair Highlights Tech Solutions
* Ryanair Hit With Lawsuit Over Use of Facial Recognition Technology
* Millions of People Affected in MOVEit Attack on US Gov't Vendor
* TSA Updates Pipeline Cybersecurity Requirements
* Group-IB Co-Founder Sentenced to 14 Years in Russian Penal Colony
* Israeli-Trained Azerbaijan Cyber Students Mark Inaugural Graduation
* What Will CISA's Secure Software Development Attestation Form Mean?
* Ubuntu Linux Cloud Workloads Face Rampant Root Take Takeovers

The Hacker News

* AVRecon Botnet Leveraging Compromised Routers to Fuel Illegal Proxy Service
* Fruity Trojan Uses Deceptive Software Installers to Spread Remcos RAT
* Multiple Flaws Found in Ninja Forms Plugin Leave 800,000 Sites Vulnerable
* New Android Malware CherryBlos Utilizing OCR to Steal Sensitive Data
* RFP Template for Browser Security
* Apple Sets New Rules for Developers to Prevent Fingerprinting and Data Misuse
* Hackers Deploy "SUBMARINE" Backdoor in Barracuda Email Security Gateway Attacks
* Ivanti Warns of Another Endpoint Manager Mobile Vulnerability Under Active Attack
* IcedID Malware Adapts and Expands Threat with Updated BackConnect Module
* STARK#MULE Targets Koreans with U.S. Military-themed Document Lures
* A Data Exfiltration Attack Scenario: The Porsche Experience
* Hackers Abusing Windows Search Feature to Install Remote Access Trojans
* BlueBravo Deploys GraphicalProton Backdoor Against European Diplomatic Entities
* Major Security Flaw Discovered in Metabase BI Software - Urgent Update Required
* Cybersecurity Agencies Warn Against IDOR Bugs Exploited for Data Breaches

LATEST NEWS

Security Week

* US, Australia Issue Warning Over Access Control Vulnerabilities in Web Applications
* In Other News: Data Breach Cost Rises, Russia Targets Diplomats, Tracker Alerts in Android
* Exploitation of Recent Citrix ShareFile RCE Vulnerability Begins
* Industry Reactions to New SEC Cyber Incident Disclosure Rules: Feedback Friday
* Zimbra Patches Exploited Zero-Day Vulnerability
* CoinsPaid Blames North Korean Hackers for $37 Million Cryptocurrency Heist
* Weintek Weincloud Vulnerabilities Allowed Manipulation, Damaging of ICS Devices
* US Senator Wyden Accuses Microsoft of 'Cybersecurity Negligence'
* European Threat Intelligence Firm QuoIntelligence Raises $5.5 Million in Seed Funding
* Head of US Cybersecurity Agency Sees Progress on Election Security, With More Work Needed for 2024

Infosecurity Magazine

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* Researchers uncover surprising method to hack the guardrails of LLMs
* Your KnowBe4 Fresh Content Updates from July 2023
* SEC Implements New Rule Requiring Firms to Disclose Cybersecurity Breaches in 4 Days
* Facebook Scams Impersonate AI Tools
* Russia-Based Global Cybersecurity Vendor Group-IB Exits the Russian Market
* Phishing Email Attack Numbers "Decline" While Malware Volumes Increase 15%
* How KnowBe4 Can Help You Fight Spear Phishing
* [Live Demo] Customizing Your Compliance Training to Increase Effectiveness
* New IBM report reveals the cost of a data breach now tops $4.45 million
* Beware of the Barbie Scam: What You Need to Know After the Recent Movie Release

ISC2.org Blog

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

HackRead

* Modern Warfare 2 Servers Were Offline Amid Malware Attack
* Original BreachForums Breached, PII Data of 210K Users Sold Online
* N. Korean Lazarus Group Suspected in $37.3M CoinsPaid Crypto Heist
* Malvertising Attack Drops BlackCat Ransomware via Fake Search Results
* Data Leak Exposes 572 GB of Student, Faculty Info from Accreditation Org
* Vulnerabilities exposed Peloton treadmills to malware and DoS attacks
* Benefits of hiring a Java web application development company

Koddos

* Modern Warfare 2 Servers Were Offline Amid Malware Attack
* Original BreachForums Breached, PII Data of 210K Users Sold Online
* N. Korean Lazarus Group Suspected in $37.3M CoinsPaid Crypto Heist
* Malvertising Attack Drops BlackCat Ransomware via Fake Search Results
* Data Leak Exposes 572 GB of Student, Faculty Info from Accreditation Org
* Vulnerabilities exposed Peloton treadmills to malware and DoS attacks
* Benefits of hiring a Java web application development company

LATEST NEWS

Naked Security

* S3 Ep145: Bugs With Impressive Names!
* Zenbleed: How the quest for CPU performance could put your passwords at risk
* Apple ships that recent "Rapid Response" spyware patch to everyone, fixes a second zero-day
* Hacking police radios: 30-year-old crypto flaws in the spotlight
* 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

Threat Post

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

Null-Byte

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

LATEST NEWS

IBM Security Intelligence

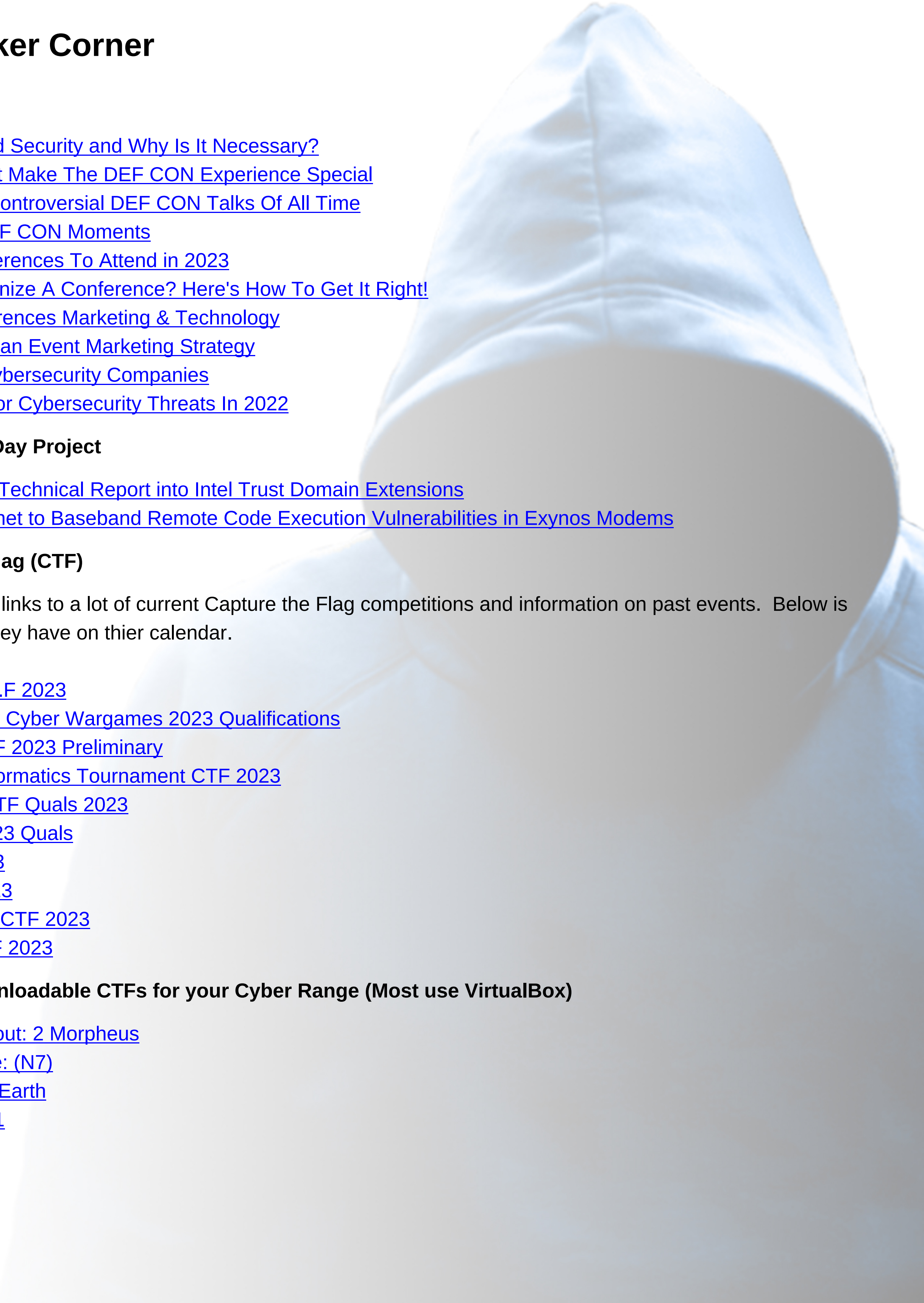
* AI reduces data breach lifecycles and costs
* The rise of malicious Chrome extensions targeting Latin America
* How credential stuffing works (and how to stop it)
* QRadar SIEM reduces incident investigation time by 90%
* Combining EPP and EDR tools can boost your endpoint security
* What's new in 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

InfoWorld

* The open source licensing war is over
* Ease into similarity search with Google's PaLM API
* The lost art of cloud application engineering
* AWS updates Amazon Bedrock service with new large language models
* 6 performance tips for Entity Framework Core 7
* The power of process mining in Power Automate
* AWS' Entity Resolution service to help enterprises improve data quality
* Reactive programming with RxJava
* Get started with Python type hints
* Teradata acquires Stemma to boost AI-based data search for analytics

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

* What is Cloud Security and Why Is It Necessary?
* 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

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.

* 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
* CYBERGON CTF 2023
* Bauhinia CTF 2023

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

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

Tools & Techniques

Packet Storm Security Tools Links

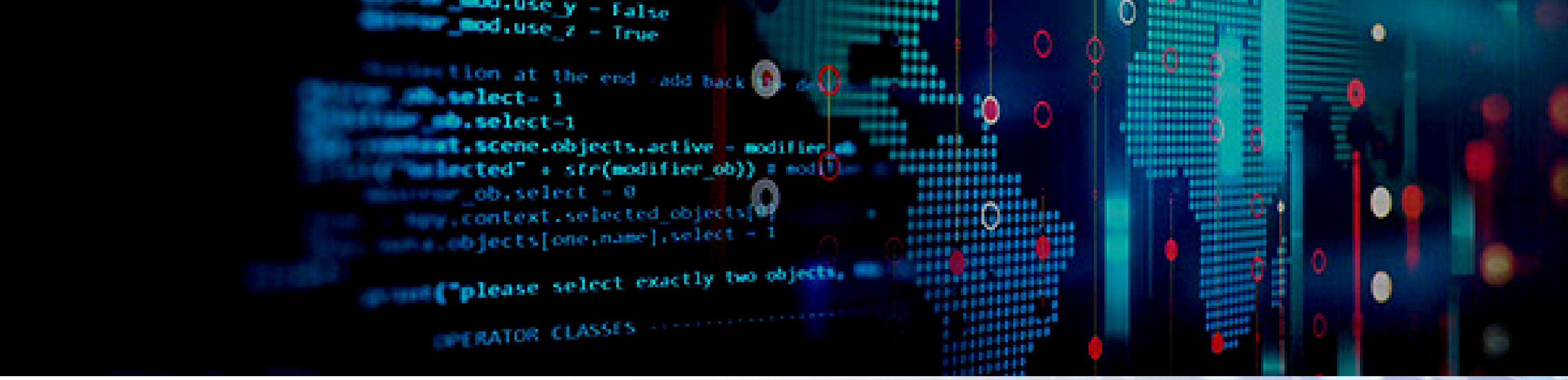
* TOR Virtual Network Tunneling Tool 0.4.7.14
* jSQL Injection 0.90
* Logwatch 7.9
* jSQL Injection 0.89
* jSQL Injection 0.88
* OpenSSH 9.3p2
* Suricata 7.0.0
* Faraday 4.5.1
* Faraday 4.5.0
* Wireshark Analyzer 4.0.7

Kali Linux Tutorials

* Fuzztruction : Academic Prototype Of A Fuzzer
* FirebaseExploiter : Vulnerability Discovery Tool That Discovers Firebase Database Which Are Open And
* Dedicated Devices and How your Organization Can Benefit From Them
* Bearer : Code Security Scanning Tool (SAST) That Discover, Filter And Prioritize Security Risks
* hardCIDR : Linux Bash Script
* 7 Risks & Challenges Dynamic Application Security Testing Solves
* 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

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



_mod.use_z = True
ob.select= 1
ob.select=1
.scene.objects.active = modifier_ob
"selected" + str(modifier_ob)) # modif
_ob.select = 0
.context.selected_objects[0]
.objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES

Weekly Cyber Security Video and Podcasts

SANS DFIR

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

Defcon Conference

* DEF CON 31 Trailer!
* 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

Hak5

* Introducing the NEW &#128063; Packet Squirrel
* What is the Cyber Trust Mark? & Major ColdFusion & Microsoft Exchange Hacks Underway! - ThreatWire
* State DMV Data Stolen via MOVEit Vulnerabilities & Reddit's API Change Triggers Hackers - 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

* Will AI KILL JOURNALISM
* Will AI REPLACE HOLLYWOOD WRITERS
* WormGPT - What is... (Super Scary AI HACKING TOOL)
* YOUTUBE GOES PAY for PLAY - this is just getting sad...

Security Now

* Satellite Insecurity, Part 2 - Apple vs EU, Cyber Resilience Act, Web Environment Integrity
* Satellite Insecurity, Part 1 - Kaspersky on MS flaw, WormGPT, Bitcoin addresses, Twitter DM change

Troy Hunt

* Weekly Update 358

Intel Techniques: The Privacy, Security, & OSINT Show

* 304-Linux Privacy & Security
* 303-iOS Privacy & Security

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Western Digital MyCloud Unauthenticated Command Injection
* Joomla Solidres 2.13.3 Cross Site Scripting
* XLAgenda 4.4 Cross Site Request Forgery
* WonderCMS 0.6-Beta Password Disclosure
* xForUp Simple File Uploader 1.0 SQL Injection
* B-OBEC V.092019 SQL Injection
* BMIT BMS 2.1 SQL Injection
* AMSS++ 5.21.09 SQL Injection
* AMS Logistics 2.2 SQL Injection
* Aicte India LMS 3.0 SQL Injection
* Buzzy News Viral Lists Polls And Videos 2.5.1 Insecure Settings
* Cloud Base Multiple School Generate And Management System 4.6.0 SQL Injection
* Ciuis CRM 1.0.7 Local File Inclusion
* Job Portal CMS 2.3.0.2 SQL Injection
* RoomCast TA-2400 Cleartext Private Key / Improper Access Control
* VMWare Aria Operations For Networks Remote Command Execution
* ETSI WEBstore 2023 Cross Site Scripting
* Journal Management Software 1.2.4 SQL Injection
* Joomla VirtueMart 2.6.12.2 SQL Injection
* Joomla JSN Gruve Pro 2.1.0 Directory Traversal
* Availability Booking Calendar PHP XSS / Arbitrary File Upload
* Joomla HotelGuide 1.0 Cross Site Scripting
* Joomla Jomestate 4.0 SQL Injection
* Joomla Fireboard 1.3 SQL Injection
* WordPress File Manager Advanced Shortcode 2.3.2 Remote Code Execution

CXSecurity

* WordPress File Manager Advanced Shortcode 2.3.2 Remote Code Execution
* 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

Proof of Concept (PoC) & Exploits

Exploit Database

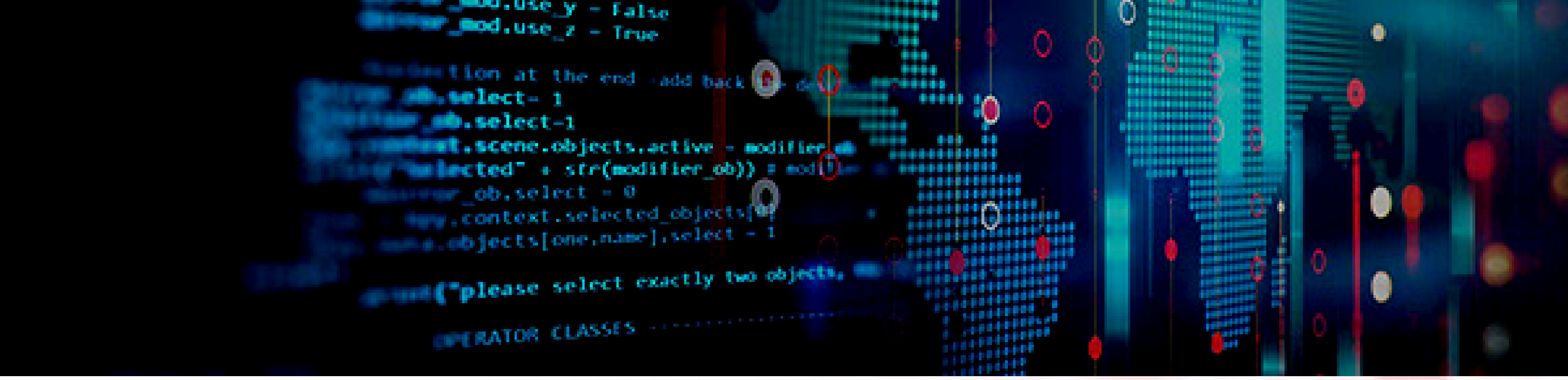
* [local] mRemoteNG v1.77.3.1784-NB - Cleartext Storage of Sensitive Information in Memory
* [webapps] copyparty 1.8.2 - Directory Traversal
* [webapps] copyparty v1.8.6 - Reflected Cross Site Scripting (XSS)
* [local] GreenShot 1.2.10 - Insecure Deserialization Arbitrary Code Execution
* [webapps] WordPress Plugin AN_Gradebook 5.0.1 - SQLi
* [webapps] Joomla VirtueMart Shopping Cart 4.0.12 - Reflected XSS
* [webapps] October CMS v3.4.4 - Stored Cross-Site Scripting (XSS) (Authenticated)
* [webapps] Joomla HikaShop 4.7.4 - Reflected XSS
* [webapps] mooDating 1.2 - Reflected Cross-site scripting (XSS)
* [webapps] Perch v3.2 - Persistent Cross Site Scripting (XSS)
* [webapps] Availability Booking Calendar v1.0 - Multiple Cross-site scripting (XSS)
* [webapps] Zomplog 3.9 - Cross-site scripting (XSS)
* [webapps] zomplog 3.9 - Remote Code Execution (RCE)
* [local] Keeper Security desktop 16.10.2 & Browser Extension 16.5.4 - Password Dumping
* [webapps] RosarioSIS 10.8.4 - CSV Injection
* [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] Dooblou WiFi File Explorer 1.13.3 - Multiple Vulnerabilities
* [webapps] PaulPrinting CMS - (Search Delivery) Cross Site Scripting
* [webapps] Active Super Shop CMS v2.5 - HTML Injection Vulnerabilities
* [webapps] Boom CMS v8.0.7 - Cross Site Scripting

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.


mod.use_y = False
mod.use_z = True
tion at the end -add back
ob.select= 1
ob.select=1
t.scene.objects.active = modifier_ob
"elected" + str(modifier_ob)) # modi
ob.select = 0
.context.selected_objects[0]
objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES

Latest Hacked Websites

Published on Zone-h.org

http://baristandmanado.kemenperin.go.id

http://baristandmanado.kemenperin.go.id notified by Shizuo1337

https://dinkes.luwukab.go.id/dph.html

https://dinkes.luwukab.go.id/dph.html notified by Mrj Haxcore

http://goberchimaltenango.gob.gt/dph.html

http://goberchimaltenango.gob.gt/dph.html notified by Mrj Haxcore

https://kasawotc.go.ug/Cyb3r.html

https://kasawotc.go.ug/Cyb3r.html notified by Cyb3r_Drag0nz_Team

https://litbang.kalbarprov.go.id/zz.html

https://litbang.kalbarprov.go.id/zz.html notified by xNot_RespondinGx

https://esdm.sultraprov.go.id/z.html

https://esdm.sultraprov.go.id/z.html notified by GayAnon

https://spbe.muarojambikab.go.id/z.html

https://spbe.muarojambikab.go.id/z.html notified by GayAnon

https://rsudsungaibahar.muarojambikab.go.id/z.html

https://rsudsungaibahar.muarojambikab.go.id/z.html notified by GayAnon

https://ppid.muarojambikab.go.id/z.html

https://ppid.muarojambikab.go.id/z.html notified by GayAnon

https://pkmsimpangsungaiduren.muarojambikab.go.id/z.html

https://pkmsimpangsungaiduren.muarojambikab.go.id/z.html notified by GayAnon

https://pkmpondokmeja.muarojambikab.go.id/z.html

https://pkmpondokmeja.muarojambikab.go.id/z.html notified by GayAnon

https://pkmmuarakumpeh.muarojambikab.go.id/z.html

https://pkmmuarakumpeh.muarojambikab.go.id/z.html notified by GayAnon

https://newsiko.muarojambikab.go.id/z.html

https://newsiko.muarojambikab.go.id/z.html notified by GayAnon

https://kedemangan.muarojambikab.go.id/z.html

https://kedemangan.muarojambikab.go.id/z.html notified by GayAnon

https://kemingkingdalam.muarojambikab.go.id/z.html

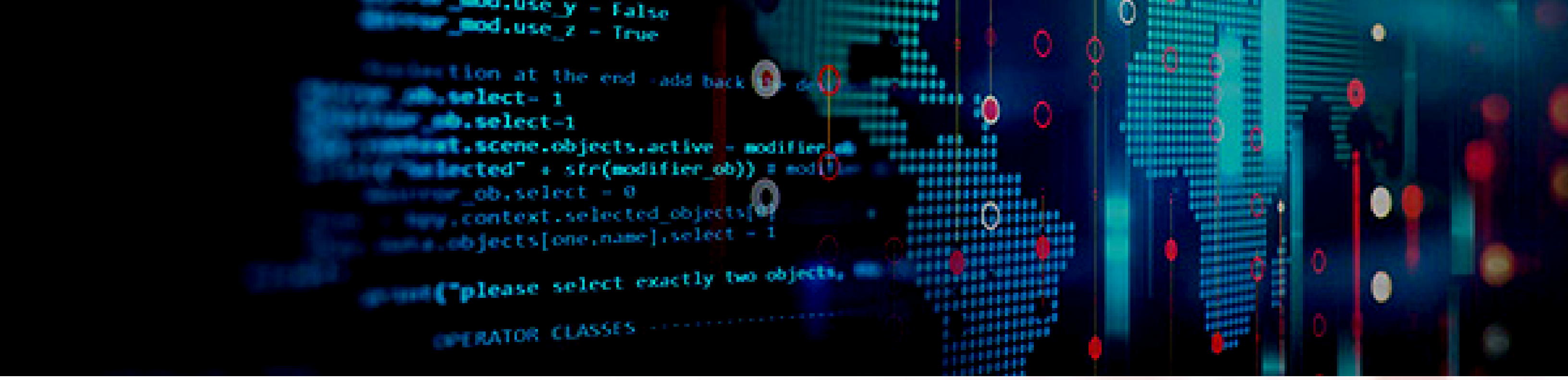
https://kemingkingdalam.muarojambikab.go.id/z.html notified by GayAnon

https://kominfo.layanan.muarojambikab.go.id/z.html

https://kominfo.layanan.muarojambikab.go.id/z.html notified by GayAnon

https://monitoring.muarojambikab.go.id/z.html

https://monitoring.muarojambikab.go.id/z.html notified by GayAnon

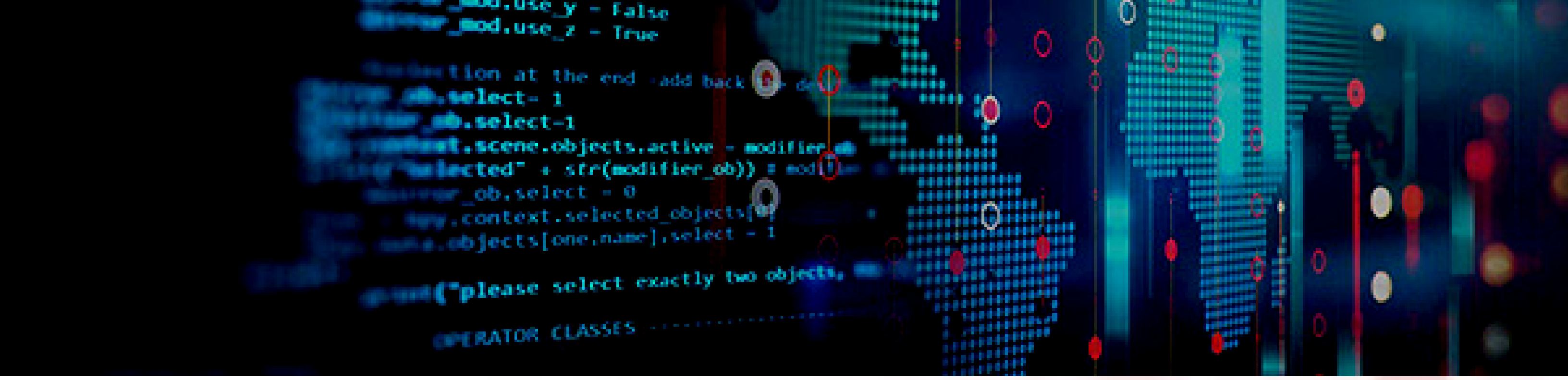

_mod.use_y = False
_mod.use_z = True
tion at the end -add back
_ob.select= 1
_ob.select=1
.scene.objects.active = modifier_ob
"selected" + str(modifier_ob)) # modi
_ob.select = 0
.context.selected_objects[0]
.objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES

Dark Web News

Darknet Live

SSNOB Marketplace Admin Pleads Guilty
Nevada Woman Sentenced for Attempting to Hire a Hitman
Woman Pleads Guilty in the "Opiateconnect" Case
A Hitchhiker's Guide to Monero's Feather Wallet

Dark Web Link



Trend Micro Anti-Malware Blog

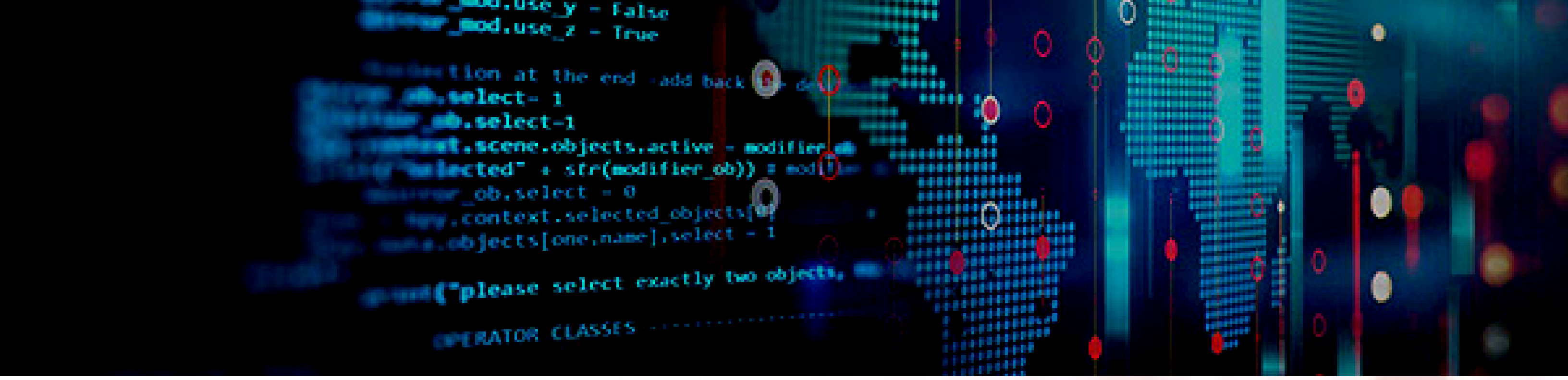
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

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

FireEye

* Metasploit Weekly Wrap up
* PenTales: There Are Many Ways to Infiltrate the Cloud
* CVE-2023-35078: Critical API Access Vulnerability in Ivanti Endpoint Manager Mobile
* 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



Advisories

US-Cert Alerts & bulletins

* CISA Releases Malware Analysis Reports on Barracuda Backdoors
* Ivanti Releases Security Updates for EPMM to address CVE-2023-35081
* CISA Releases Five Industrial Control Systems Advisories
* CISA and Partners Release Joint Cybersecurity Advisory on Preventing Web Application Access Control A
* CISA Adds One Known Exploited Vulnerability to Catalog
* CISA Releases Analysis of FY22 Risk and Vulnerability Assessments
* CISA Adds One Known Exploited Vulnerability to Catalog
* Apple Releases Security Updates for Multiple Products
* Preventing Web Application Access Control Abuse
* Threat Actors Exploiting Citrix CVE-2023-3519 to Implant Webshells
* Vulnerability Summary for the Week of July 17, 2023
* Vulnerability Summary for the Week of July 10, 2023

Zero Day Initiative Advisories

ZDI-CAN-21691: 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 'Anonymous' was reported to the affected vendor on: 2023-07-27, 4 days ago. The vendor is given until 2023-11-24 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21812: 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 'Anonymous' was reported to the affected vendor on: 2023-07-27, 4 days ago. The vendor is given until 2023-11-24 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21512: VMware
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 'Gwangun Jung (@pr0Ln) at THEORI' was reported to the affected vendor on: 2023-07-27, 4 days ago. The vendor is given until 2023-11-24 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21810: 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: 2023-07-27, 4 days ago. The vendor is given until 2023-11-24 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21807: 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:

2023-07-27, 4 days ago. The vendor is given until 2023-11-24 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21811: 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: 2023-07-27, 4 days ago. The vendor is given until 2023-11-24 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21769: Apple

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2023-07-27, 4 days ago. The vendor is given until 2023-11-24 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21809: 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: 2023-07-27, 4 days ago. The vendor is given until 2023-11-24 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21829: Kofax

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: 2023-07-27, 4 days ago. The vendor is given until 2023-11-24 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21808: 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: 2023-07-27, 4 days ago. The vendor is given until 2023-11-24 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21608: X.Org

A CVSS score 7.4 (AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Sri' was reported to the affected vendor on: 2023-07-27, 4 days ago. The vendor is given until 2023-11-24 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21460: 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 'NT AUTHORITY\ANONYMOUS LOGON' was reported to the affected vendor on: 2023-07-26, 5 days ago. The vendor is given until 2023-11-23 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-21783: Trimble

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: 2023-07-26, 5 days ago. The vendor is given until 2023-11-23 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-21343: Adobe

A CVSS score 9.1 (AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-07-26, 5 days ago. The vendor is given until 2023-11-23 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-21819: TP-Link

A CVSS score 6.8 (AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Peter Girnus and Nicholas Zubrisky of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-07-26, 5 days ago. The vendor is given until 2023-11-23 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-21788: Trimble

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: 2023-07-26, 5 days ago. The vendor is given until 2023-11-23 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-21785: Trimble

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: 2023-07-26, 5 days ago. The vendor is given until 2023-11-23 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-21784: Trimble

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: 2023-07-26, 5 days ago. The vendor is given until 2023-11-23 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-21786: Trimble

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 & Jimmy Calderon (@vectors2final) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-07-26, 5 days ago. The vendor is given until 2023-11-23 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-21800: Trimble

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: 2023-07-26, 5 days ago. The vendor is given until 2023-11-23 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-21799: Trimble

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: 2023-07-26, 5 days ago. The vendor is given until 2023-11-23 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-21787: Trimble

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: 2023-07-26, 5 days ago. The vendor is given until 2023-11-23 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-21806: Hewlett Packard Enterprise

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 'Sina Kheirkhah (@SinSinology) of Summoning Team (@SummoningTeam)' was reported to the affected vendor on: 2023-07-26, 5 days ago. The vendor is given until 2023-11-23 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-21296: 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: 2023-07-26, 5 days ago. The vendor is given until 2023-11-23 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

Ubuntu Security Notice USN-6259-1

Ubuntu Security Notice 6259-1 - Jos Wetzels, Stanislav Dashevskyi, and Amine Amri discovered that Open-iSCSI incorrectly handled certain checksums for IP packets. An attacker could possibly use this issue to expose sensitive information. Jos Wetzels, Stanislav Dashevskyi, Amine Amri discovered that Open-iSCSI incorrectly handled certain parsing TCP MSS options. An attacker could possibly use this issue to cause a crash or cause unexpected behavior.

Ubuntu Security Notice USN-6260-1

Ubuntu Security Notice 6260-1 - It was discovered that the NTFS file system implementation in the Linux kernel did not properly check buffer indexes in certain situations, leading to an out-of-bounds read vulnerability. A local attacker could possibly use this to expose sensitive information. Stonejiajia, Shir Tamari and Sagi Tzadik discovered that the OverlayFS implementation in the Ubuntu Linux kernel did not properly perform permission checks in certain situations. A local attacker could possibly use this to gain elevated privileges.

Red Hat Security Advisory 2023-4226-01

Red Hat Security Advisory 2023-4226-01 - 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 4.13.6.

Red Hat Security Advisory 2023-4225-01

Red Hat Security Advisory 2023-4225-01 - 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 4.13.6.

Debian Security Advisory 5460-1

Debian Linux Security Advisory 5460-1 - It was discovered that Curl performed incorrect file path handling when saving cookies to files, which could lead to the creation or overwriting of files.

Ubuntu Security Notice USN-5193-3

Ubuntu Security Notice 5193-3 - USN-5193-1 fixed several vulnerabilities in X.Org. This update provides the corresponding update for Ubuntu 16.04 ESM. Jan-Niklas Sohn discovered that the X.Org X Server incorrectly handled certain inputs. An attacker could use this issue to cause the server to crash, resulting in a denial of service, or possibly execute arbitrary code and escalate privileges.

Ubuntu Security Notice USN-6258-1

Ubuntu Security Notice 6258-1 - It was discovered that LLVM Toolchain did not properly manage memory under certain circumstances. If a user were tricked into opening a specially crafted MLIR file, an attacker could possibly use this issue to cause LLVM Toolchain to crash, resulting in a denial of service. It was discovered that LLVM Toolchain did not properly manage memory under certain circumstances. If a user were tricked into opening a specially crafted MLIR file, an attacker could possibly use this issue to cause LLVM Toolchain to crash, resulting in a denial of service. This issue only affected llvm-toolchain-15.

Ubuntu Security Notice USN-6257-1

Ubuntu Security Notice 6257-1 - It was discovered that Open VM Tools incorrectly handled certain authentication requests. A fully compromised ESXi host can force Open VM Tools to fail to authenticate host-to-guest operations, impacting the confidentiality and integrity of the guest virtual machine.

Ubuntu Security Notice USN-6256-1

Ubuntu Security Notice 6256-1 - Jiasheng Jiang discovered that the HSA Linux kernel driver for AMD Radeon GPU devices did not properly validate memory allocation in certain situations, leading to a null pointer dereference vulnerability. A local attacker could use this to cause a denial of service. Zheng Wang discovered that the Intel i915 graphics driver in the Linux kernel did not properly handle certain error conditions, leading to a double-free. A local attacker could possibly use this to cause a denial of service.

Ubuntu Security Notice USN-6255-1

Ubuntu Security Notice 6255-1 - It was discovered that the IP-VLAN network driver for the Linux kernel did not properly initialize memory in some situations, leading to an out-of- bounds write vulnerability. An attacker could use this to cause a denial of service or possibly execute arbitrary code. Mingi Cho discovered that the netfilter subsystem in the Linux kernel did not properly validate the status of a nft chain while performing a lookup by id, leading to a use-after-free vulnerability. An attacker could use this to cause a denial of service or possibly execute arbitrary code.

Red Hat Security Advisory 2023-4290-01

Red Hat Security Advisory 2023-4290-01 - OpenShift sandboxed containers 1.4.1 is now available. Red Hat Product Security has rated this update as having a security impact of Moderate. A compliance problem was found in the Red Hat OpenShift Container Platform. Red Hat discovered that when FIPS mode was enabled, not all of the cryptographic modules in use were FIPS-validated.

Red Hat Security Advisory 2023-4293-01

Red Hat Security Advisory 2023-4293-01 - The Migration Toolkit for Containers (MTC) 1.7.11 is now available. Red Hat Product Security has rated this update as having a security impact of Moderate.

Ubuntu Security Notice USN-6254-1

Ubuntu Security Notice 6254-1 - Jordy Zomer and Alexandra Sandulescu discovered that syscalls invoking the do_prlimit function in the Linux kernel did not properly handle speculative execution barriers. A local attacker could use this to expose sensitive information. It was discovered that a race condition existed in the btrfs file system implementation in the Linux kernel, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly expose sensitive information.

Red Hat Security Advisory 2023-4286-01

Red Hat Security Advisory 2023-4286-01 - Red Hat OpenShift Dev Spaces provides a cloud developer workspace server and a browser-based IDE built for teams and organizations. Dev Spaces runs in OpenShift and is well-suited for container-based development.

Red Hat Security Advisory 2023-4287-01

Red Hat Security Advisory 2023-4287-01 - Red Hat OpenShift Data Foundation is software-defined storage integrated with and optimized for the Red Hat OpenShift Container Platform. Red Hat OpenShift Data Foundation is a highly scalable, production-grade persistent storage for stateful applications running in the Red Hat OpenShift Container Platform.

Ubuntu Security Notice USN-6252-1

Ubuntu Security Notice 6252-1 - It was discovered that the ext4 file system implementation in the Linux kernel contained a use-after-free vulnerability. An attacker could use this to construct a malicious ext4 file system image that, when mounted, could cause a denial of service. It was discovered that the sound subsystem in the Linux kernel contained a race condition in some situations. A local attacker could use this to cause a denial of service.

Ubuntu Security Notice USN-6251-1

Ubuntu Security Notice 6251-1 - It was discovered that the IP-VLAN network driver for the Linux kernel did not properly initialize memory in some situations, leading to an out-of- bounds write vulnerability. An attacker could use this to cause a denial of service or possibly execute arbitrary code. Shir Tamari and Sagi Tzadik discovered that the OverlayFS implementation in the Ubuntu Linux kernel did not properly perform permission checks in certain situations. A local attacker could possibly use this to gain elevated privileges.

Ubuntu Security Notice USN-6253-1

Ubuntu Security Notice 6253-1 - It wad discovered that libvirt incorrectly handled locking when processing certain requests. A local attacker could possibly use this issue to cause libvirt to stop responding or crash, resulting in a denial of service.

Debian Security Advisory 5459-1

Debian Linux Security Advisory 5459-1 - Tavis Ormandy discovered that under specific microarchitectural circumstances, a vector register in "Zen 2" CPUs may not be written to 0 correctly. This flaw allows an attacker to leak register contents across concurrent processes, hyper threads and virtualized guests.

Red Hat Security Advisory 2023-4283-01

Red Hat Security Advisory 2023-4283-01 - OpenStack Networking is a virtual network service for OpenStack.

Just as OpenStack Compute provides an API to dynamically request and configure virtual servers, OpenStack Networking provides an API to dynamically request and configure virtual networks. These networks connect 'interfaces' from other OpenStack services. The OpenStack Networking API supports extensions to provide advanced network capabilities.

Red Hat Security Advisory 2023-4282-01

Red Hat Security Advisory 2023-4282-01 - The redhat-virtualization-host packages provide the Red Hat Virtualization Host. These packages include redhat-release-virtualization-host, ovirt-node, and rhev-hypervisor. Red Hat Virtualization Hosts are installed using a special build of Red Hat Enterprise Linux with only the packages required to host virtual machines. RHVH features a Cockpit user interface for monitoring the host's resources and performing administrative tasks. Issues addressed include a bypass vulnerability.

Ubuntu Security Notice USN-6250-1

Ubuntu Security Notice 6250-1 - Stonejiajia, Shir Tamari and Sagi Tzadik discovered that the OverlayFS implementation in the Ubuntu Linux kernel did not properly perform permission checks in certain situations. A local attacker could possibly use this to gain elevated privileges. It was discovered that the IP-VLAN network driver for the Linux kernel did not properly initialize memory in some situations, leading to an out-of- bounds write vulnerability. An attacker could use this to cause a denial of service or possibly execute arbitrary code.

Red Hat Security Advisory 2023-4276-01

Red Hat Security Advisory 2023-4276-01 - An update is now available for Red Hat DevWorkspace Operator. Red Hat Product Security has rated this update as having a security impact of Moderate.

Debian Security Advisory 5458-1

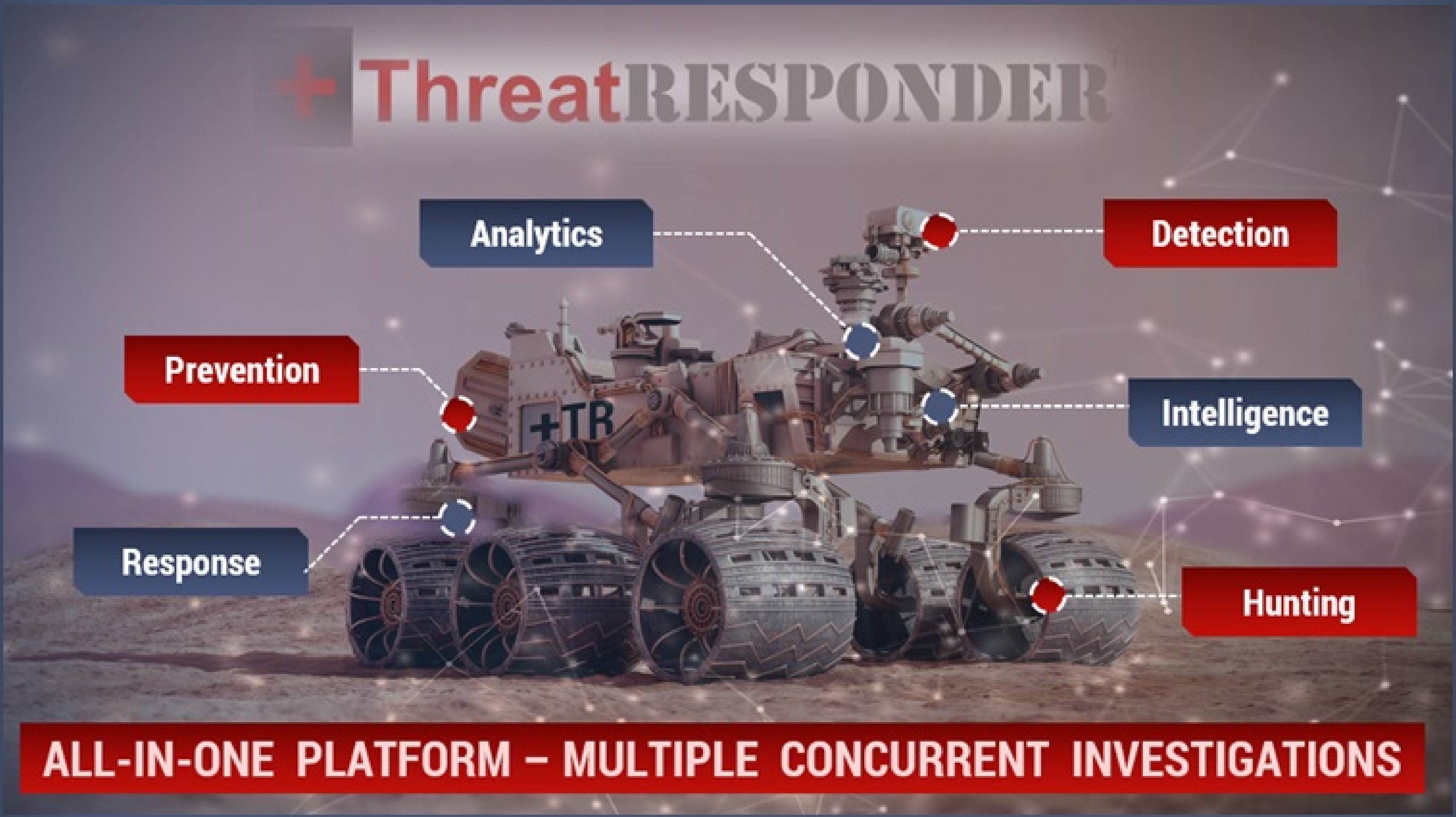
Debian Linux Security Advisory 5458-1 - Several vulnerabilities have been discovered in the OpenJDK Java runtime, which may result in bypass of sandbox restrictions, information disclosure, reduced cryptographic strength of the AES implementation, directory traversal or denial of service.

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



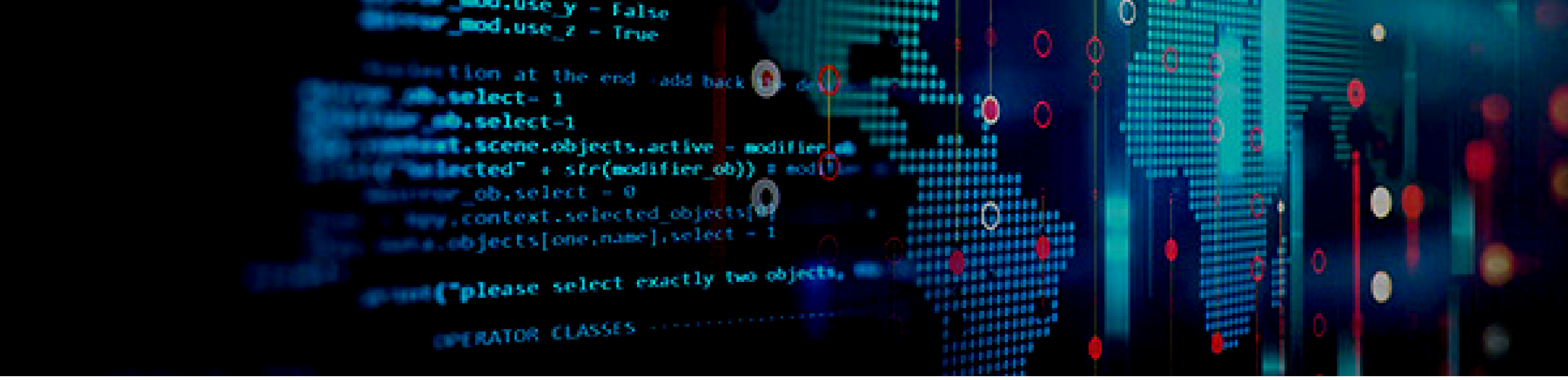
The Solution – ThreatResponder® Platform

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



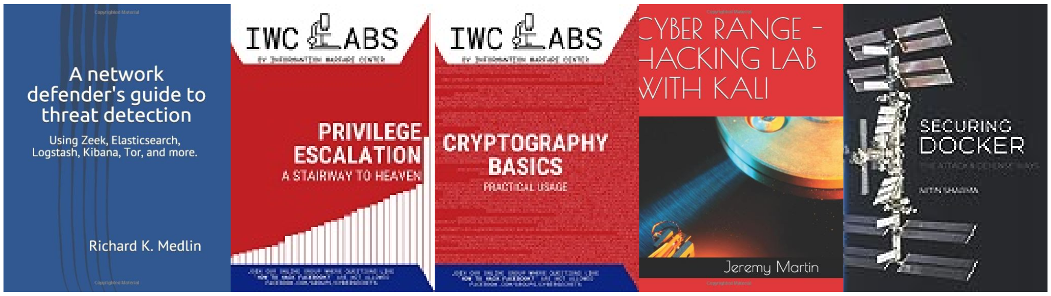
The Cyber Secrets publications on Amazon

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.

CYBER Secrets
What's Inside?
Threat Intelligence & Training
DIVE INTO THE 5TH DOMAIN THREAT INTELLIGENCE
RED TEAMING AROUND YOUR BACKYARD
THE 8 LAYERS OF THE OSI CAKE
LAUNCHING EXPLOITS
INCIDENT RESPONSE

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