Dec-05-22

CYBER WEEKLY AWARENESS REPORT

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

ARGOS APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity®

CYBER WEEKLY AWARENESS REPORT

December 5, 2022

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

Summary

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

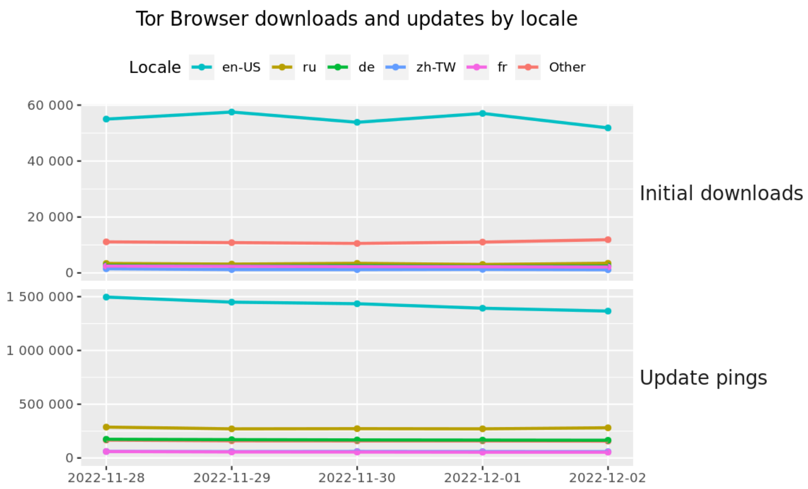
Internet Storm Center Infocon Status

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.



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

Current News

The Hacker Corner:

Cyber Range Content

Tools & Techniques

InfoSec Media for the Week

Exploits and Proof of Concepts

Cyber Crime & Malware Files/Links Latest Identified

Advisories

Information Warfare Center Products

LATEST NEWS

Packet Storm Security

* FBI Warning: This Ransomware Gang Has Hit Over 100 Targets And Made More Than $60 Million
* AI Bot ChatGPT Stuns Academics With Essay Writing Skills / Usability
* Rackspace Customers Rage As Email Outage Continues
* Journalist Sues NSO After Being Hacked By Pegasus Spyware
* US Air Force Reveals The B-21 Raider Stealth Bomber
* Rackspace Rocked By Security Incident
* Darknet Markets Generate Millions In Revenue Selling Stolen Personal Data
* New Malware Is Nuking Data In Russian Courts
* After FTX Collapse, Pressure Builds For Tougher Crypto Rules
* Proton Calendar On iOS Encrypts More Of Your Work/Life Cloud Data
* Mozilla, Microsoft Drop TrustCor As Root Certificate Authority
* Nvidia Patches 29 GPU Driver Bugs That Could Lead To Code Execution, Device Takeover
* Researchers Used A Sirius XM Bug To Easily Hijack A Bunch Of Different Cars
* Browser Zero Days Linked To Commercial IT Firm In Spain
* My Secret Life As An 11-Year-Old BBS SysOp
* The Exodus From Elon Musk's Twitter Has Begun. Should The Infosec Community Care?
* Intruders Gain Access To User Data In LastPass Incident
* Lockheed Martin's Army Cyber Training Platform Goes Civilian
* SF Votes To Give Cop Robots Permission To Kill
* How Secure A Twitter Replacement Is Mastodon?
* It Took Nearly 500 Years For Researchers To Crack Charles V's Secret Code
* Crypto Firm BlockFi Files For Bankruptcy After FTX Collapse
* Meta Fined 265M Euros By Irish Data Protection Commission
* Community Health Informs 1.5M Of Unauthorized Disclosure
* Google Says Google Should Do A Better Job Of Patching Android Devices

Krebs on Security

* Judge Orders U.S. Lawyer in Russian Botnet Case to Pay Google
* ConnectWise Quietly Patches Flaw That Helps Phishers
* U.S. Govt. Apps Bundled Russian Code With Ties to Mobile Malware Developer
* Researchers Quietly Cracked Zeppelin Ransomware Keys
* Disneyland Malware Team: It's a Puny World After All
* Top Zeus Botnet Suspect "Tank" Arrested in Geneva
* Lawsuit Seeks Food Benefits Stolen By Skimmers
* Patch Tuesday, November 2022 Election Edition
* LinkedIn Adds Verified Emails, Profile Creation Dates
* Hacker Charged With Extorting Online Psychotherapy Service

LATEST NEWS

Dark Reading

* Wiper, Disguised as Fake Ransomware, Targets Russian Orgs
* Hive Social Buzzing With Security Flaws, Analysts Warn
* Cybersecurity Should Focus on Managing Risk
* Cyberattack Shuts Down French Hospital
* The New External Attack Surface: 3 Elements Every Organization Should Monitor
* Palo Alto Networks Announces Medical IoT Security to Protect Connected Devices Critical to Patient Ca
* OpenSSF Membership Exceeds 100, With Many New Members Dedicated to Securing Open Source Software
* Infostealer Malware Market Booms, as MFA Fatigue Sets In
* The Privacy War Is Coming
* Ransomware Professionalization Grows as RaaS Takes Hold
* Malware Authors Inadvertently Take Down Own Botnet
* Concern Over DDoS Attacks Falls Despite Rise in Incidents
* SiriusXM, MyHyundai Car Apps Showcase Next-Gen Car Hacking
* Newsroom Sues NSO Group for Pegasus Spyware Compromise
* Where Advanced Cyberttackers Are Heading Next: Disruptive Hits, New Tech
* SOC Turns to Homegrown Machine Learning to Catch Cyber Intruders
* A Risky Business: Choosing the Right Methodology
* AWS Unveils Amazon Security Lake at re:Invent 2022
* LastPass Discloses Second Breach in Three Months
* Artifact Poisoning in GitHub Actions Imports Malware via Software Pipelines

The Hacker News

* New BMC Supply Chain Vulnerabilities Affect Servers from Dozens of Manufacturers
* Russian Courts Targeted by New CryWiper Data Wiper Malware Posing as Ransomware
* When Being Attractive Gets Risky - How Does Your Attack Surface Look to an Attacker?
* SiriusXM Vulnerability Lets Hackers Remotely Unlock and Start Connected Cars
* North Korean Hackers Spread AppleJeus Malware Disguised as Cryptocurrency Apps
* Critical Ping Vulnerability Allows Remote Attackers to Take Over FreeBSD Systems
* Google Rolls Out New Chrome Browser Update to Patch Yet Another Zero-Day Vulnerability
* Hackers Sign Android Malware Apps with Compromised Platform Certificates
* CISA Warns of Multiple Critical Vulnerabilities Affecting Mitsubishi Electric PLCs
* The Value of Old Systems
* Researchers Disclose Supply-Chain Flaw Affecting IBM Cloud Databases for PostgreSQL
* Hackers Exploiting Redis Vulnerability to Deploy New Redigo Malware on Servers
* What the CISA Reporting Rule Means for Your IT Security Protocol
* Watch Out! These Android Keyboard Apps With 2 Million Installs Can be Hacked Remotely
* Cuba Ransomware Extorted Over $60 Million in Ransom Fees from More than 100 Entities

LATEST NEWS

Security Week

* Apple Faces Critics Over Its Privacy Policies
* SIM Swapper Who Stole $20 Million Sentenced to Prison
* Balance Theory Scores Seed Funding for Secure Workspace Collaboration
* Redigo: New Backdoor Targeting Redis Servers
* Critical Vulnerabilities Force Twitter Alternative Hive Social Offline
* US Agencies Told to Assess IoT/OT Security Risks to Boost Critical Infrastructure Protection
* Cybersecurity M&A Roundup: 35 Deals Announced in November 2022
* Google Patches Ninth Chrome Zero-Day of 2022
* Rackspace Shuts Down Hosted Exchange Systems Due to Security Incident
* French Hospital Cancels Operations After Cyberattack
* FBI Director Raises National Security Concerns About TikTok
* Hypr Raises $25 Million for Passwordless Authentication Platform
* Three Innocuous Linux Vulnerabilities Chained to Obtain Full Root Privileges
* Report: California Gun Data Breach Was Unintentional
* IBM Cloud Vulnerability Exposed Users to Supply Chain Attacks
* Over 100 Organizations Hit by Cuba Ransomware: CISA, FBI
* Mitsubishi Electric PLCs Exposed to Attacks by Engineering Software Flaws
* Google Migrating Android to Memory-Safe Programming Languages
* Wipers Are Widening: Here's Why That Matters
* 'Schoolyard Bully' Android Trojan Targeted Facebook Credentials of 300,000 Users
* Investors Double Down on Pangea Cyber API Security Bet
* Albanian IT Staff Charged With Negligence Over Cyberattack
* Several Car Brands Exposed to Hacking by Flaw in Sirius XM Connected Vehicle Service
* GoTo, LastPass Notify Customers of New Data Breach Related to Previous Incident
* El Salvador Journalists Sue NSO Group in US Over Alleged Pegasus Attacks
* Nvidia Patches Many Vulnerabilities in Windows, Linux Display Drivers

Infosecurity Magazine

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* Credential Phishing with Apple Gift Card Lures
* Inside NATO's Efforts To Plan For A Future Cyberwar
* New Threat Group Already Evolves Delivery Tactics to Include Google Ads
* Latest Netflix-Impersonated Phishing Attacks Surge in Frequency by 78% Since October
* It's Official: COVID-related Phishing is Dead as Scammers Return to Impersonating Famous Brands
* Ransomware Attacks on Holidays and Weekends Increase and Take a Greater Toll on Organizations
* Your KnowBe4 Fresh Content Updates from November 2022
* Spoofing-as-a-Service Site Taken Down
* [Keep An Eye Out] Beware of New Holiday Gift Card Scams
* CyberheistNews Vol 12 #48 [Eye Opener] Microsoft Warns Against Recent, Complex, Ransomware Campaign

ISC2.org Blog

* What It Takes to be a Cybersecurity Professional: The Non-Technical Skills You Need
* Latest Cyberthreats and Advisories - December 2, 2022
* Achieving Data Security and Analytics with AI - Member Recap from (ISC)&sup2; Security Congress 2022
* (ISC)&sup2; Board of Directors Election Results
* Are Deepfakes Really a Security Threat? - Member Recap from (ISC)&sup2; Security Congress 2022

HackRead

* The Best Ways to Automate SBOM Creation
* French Hospital Suspends Operations After Crippling Cyber Attack
* Data of Israeli Employees from 29 Logistics Firms Sold Online
* Behind The Success Of Phenomenon Game Fortnite
* App Flaw Allowed Honda and Nissan Cars Hack by Knowing VIN number
* North Korean APT37 Unleashes Dolphin Backdoor on South Korea
* CryWiper Masquerading as Ransomware to Target Russian Courts

Koddos

* The Best Ways to Automate SBOM Creation
* French Hospital Suspends Operations After Crippling Cyber Attack
* Data of Israeli Employees from 29 Logistics Firms Sold Online
* Behind The Success Of Phenomenon Game Fortnite
* App Flaw Allowed Honda and Nissan Cars Hack by Knowing VIN number
* North Korean APT37 Unleashes Dolphin Backdoor on South Korea
* CryWiper Masquerading as Ransomware to Target Russian Courts

LATEST NEWS

Naked Security

* Ping of death! FreeBSD fixes crashtastic bug in network tool
* Number Nine! Chrome fixes another 2022 zero-day, Edge patched too
* Apple pushes out iOS security update that's more tight-lipped than ever
* LastPass admits to customer data breach caused by previous breach
* The CHRISTMA EXEC network worm - 35 years and counting!
* S3 Ep111: The business risk of a sleazy "nudity unfilter" [Audio + Text]
* Serious Security: MD5 considered harmful - to the tune of $600,000
* TikTok "Invisible Challenge" porn malware puts us all at risk
* Chrome fixes 8th zero-day of 2022 - check your version now (Edge too!)
* Voice-scamming site "iSpoof" seized, 100s arrested in massive crackdown

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

* Did Brazil DSL Modem Attacks Change Device Security?
* Who Carries the Weight of a Cyberattack?
* Transitioning to Quantum-Safe Encryption
* Securing Your SAP Environments: Going Beyond Access Control
* How Do You Plan to Celebrate National Computer Security Day?
* Deploying Security Automation to Your Endpoints
* Worms of Wisdom: How WannaCry Shapes Cybersecurity Today
* Emotional Blowback: Dealing With Post-Incident Stress
* RansomExx Upgrades to Rust
* Why Operational Technology Security Cannot Be Avoided

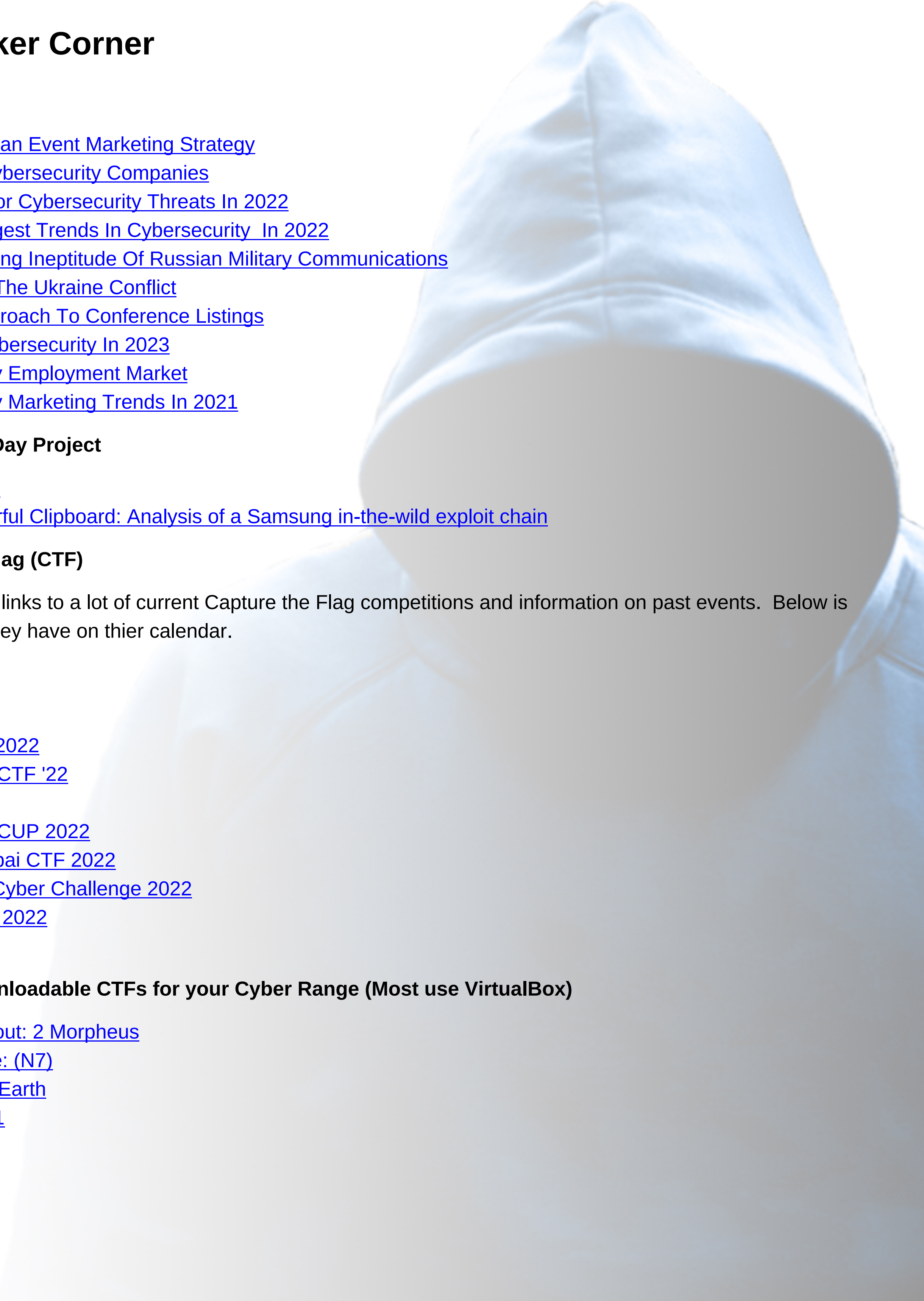
InfoWorld

* AWS is changing
* What are headless architectures and composable systems?
* 5 things developers love about their work, and 5 things they don't
* AWS re:Invent 2022 roundup: Data management, AI, compute take center stage
* Kotlin 1.8.0 beta introduces experimental functions
* Cloud computing gets back to basics
* What is DevSecOps? Securing devops pipelines
* Informatica data science framework connects with Amazon SageMaker
* AWS updates its machine learning service SageMaker
* How to use EF Core query types in ASP.NET Core 7

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 Plan an Event Marketing Strategy
* Zero Trust Cybersecurity Companies
* Types of Major Cybersecurity Threats In 2022
* The Five Biggest Trends In Cybersecurity In 2022
* The Fascinating Ineptitude Of Russian Military Communications
* Cyberwar In The Ukraine Conflict
* Our New Approach To Conference Listings
* Marketing Cybersecurity In 2023
* Cybersecurity Employment Market
* Cybersecurity Marketing Trends In 2021

Google Zero Day Project

* Mind the Gap
* A Very Powerful Clipboard: Analysis of a Samsung in-the-wild exploit chain

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.

* Shakti CTF
* Ph0wn 2022
* KITCTFCTF 2022
* Hackappatoi CTF '22
* RCTF 2022
* Russian CTFCUP 2022
* BSides Mumbai CTF 2022
* STEM CTF: Cyber Challenge 2022
* INTENT CTF 2022
* Jule 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

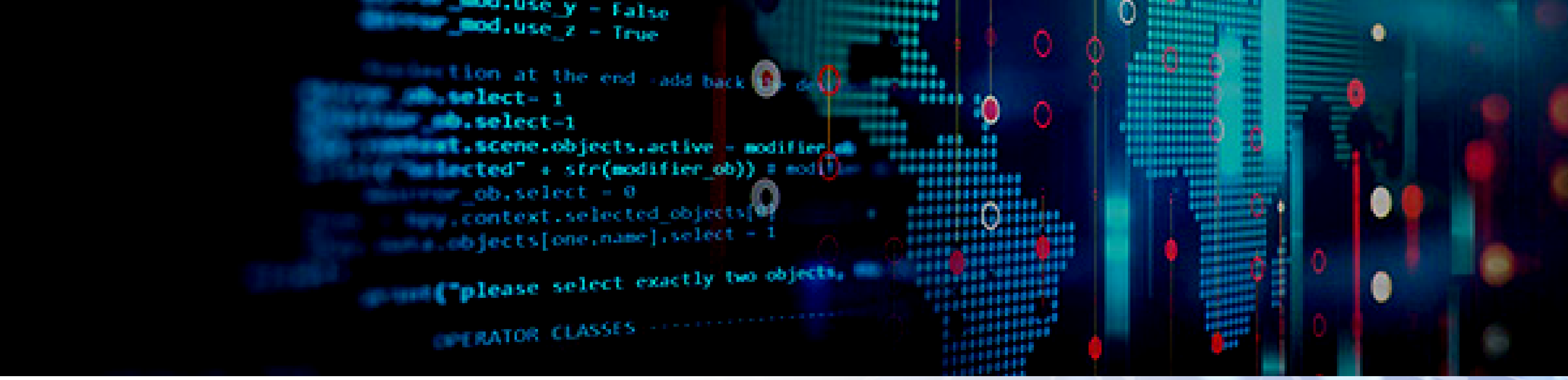
* Clam AntiVirus Toolkit 1.0.0
* Suricata IDPE 6.0.9
* Falco 0.33.1
* Zeek 5.0.4
* Packet Fence 12.1.0
* Stegano 0.11.1
* I2P 2.0.0
* TOR Virtual Network Tunneling Tool 0.4.7.11
* Zeek 5.0.3
* GNUnet P2P Framework 0.18.1

Kali Linux Tutorials

* D4TA-HUNTER : GUI Osint Framework With Kali Linux
* Pycrypt : Python Based Crypter That Can Bypass Any Kinds Of Antivirus Products
* EvilTree : A Remake Of The Classic "Tree" Command
* Kubeeye : Tool To Find Various Problems On Kubernetes
* MSMAP : Memory WebShell Generator
* SharpSCCM : A C# Utility For Interacting With SCCM
* Octopii : An AI-powered Personal Identifiable Information (PII) Scanner
* Scrcpy : Display And Control Your Android Device
* Ox4Shell : Deobfuscate Log4Shell Payloads With Ease
* Is This App Download Safe? A Guide To Secure Your Mobile Device

GBHackers Analysis

* High-Severity RCE Bug in F5 Products Let Attackers Hack the Complete Systems
* Samsung Galaxy Store Flaw Allows Remote Attacker to Run Code on Affected Phones
* Hackers Actively Exploiting Cisco AnyConnect Secure Flaw to Perform DLL Hijacking
* 22-Yrs-Old SQLite Bug Let Hackers Perform Code Execution & DOS Attack On Control Programs
* Apache Commons "Text4Shell" Flaw Could Trigger Code Execution With Malicious Input



Weekly Cyber Security Video and Podcasts

SANS DFIR

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

Defcon Conference

* DEF CON 30 - Cesare Pizzi - Old Malware, New tools: Ghidra and Commodore 64
* DEF CON 30 BiC Village - Segun Olaniyan- Growth Systems for Cybersecurity Enthusiasts
* DEF CON 30 - Silk - DEF CON Memorial Interview
* DEF CON 30 Car Hacking Village - Evadsnibor - Getting Naughty on CAN bus with CHV Badge

Hak5

* Twitter API Bug Affects Millions of Users - ThreatWire
* OS Detection - USB Rubber Ducky
* Live Hacking Q&A with Kody and Michael

The PC Security Channel [TPSC]

* Fake MSI Afterburner with Hidden Malware
* Do you need antivirus on your phone?

Eli the Computer Guy

* TWITTER FILES RELEASED by ELON MUSK - kinda dumb
* BACKMARKET REVIEW for Used MacBook Pro's
* CNN LAYOFFS - MSM is FAILING
* DOORDASH LAYOFFS - Tech industry is imploding

Security Now

* Freebie Bots & Evil Cameras - iSpoofer no more, Boa server vulnerability, CISA on Mastodon
* Wi-Peep - FBI purchased Pegasus, Passkey support directory, Quantum decryption deadline, Firefox 107

Troy Hunt

* Weekly Update 324

Intel Techniques: The Privacy, Security, & OSINT Show

* 285-Travel Security Revisited
* 284-Password Managers & 2FA Revisited

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Drupal H5P Module 2.0.0 Zip Slip Traversal
* Automotive Shop Management System 1.0 SQL Injection
* Zillya Total Security 3.0.2367.0 / 3.0.2368.0 Local Privilege Escalation
* Packet Storm New Exploits For November, 2022
* Backdoor.Win32.Delf.gj MVID-2022-0663 Information Disclosure
* IBM Websphere Application Server 7.0 Cross Site Scripting
* perfSONAR 4.4.5 Cross Site Request Forgery
* perfSONAR 4.4.4 Open Proxy / Relay
* Microsoft Exchange ProxyNotShell Remote Code Execution
* OX App Suite 7.10.6 Cross Site Scripting / SSRF / Resource Consumption
* Hirschmann (Belden) BAT-C2 8.8.1.0R8 Command Injection
* Remote Control Collection Remote Code Execution
* Concrete CMS 9.1.3 XPATH Injection
* vBulletin 5.5.2 PHP Object Injection
* Backdoor.Win32.Autocrat.b MVID-2022-0660 Weak Hardcoded Credential
* Win32.Ransom.Conti MVID-2022-0662 Cryptography Logic Flaw
* Trojan.Win32.DarkNeuron.gen MVID-2022-0661 Named Pipe NULL DACL
* Helmet Store Showroom 1.0 SQL Injection
* Sanitization Management System 1.0 SQL Injection
* Chrome blink::LocalFrameView::PerformLayout Use-After-Free
* XNU vm_object Use-After-Free
* XNU Dangling PTE Entry
* F5 BIG-IP iControl Remote Command Execution
* Ecommerce 1.0 Cross Site Scripting / Open Redirect
* Backdoor.Win32.Serman.a MVID-2022-0659 Unauthenticated Open Proxy

CXSecurity

* Microsoft Exchange ProxyNotShell Remote Code Execution
* vBulletin 5.5.2 PHP Object Injection
* Remote Control Collection Remote Code Execution
* F5 BIG-IP iControl Remote Command Execution
* ChurchInfo 1.2.13-1.3.0 Remote Code Execution
* ZTE ZXHN-H108NS Stack Buffer Overflow / Denial Of Service
* Gitea Git Fetch Remote Code Execution

Proof of Concept (PoC) & Exploits

Exploit Database

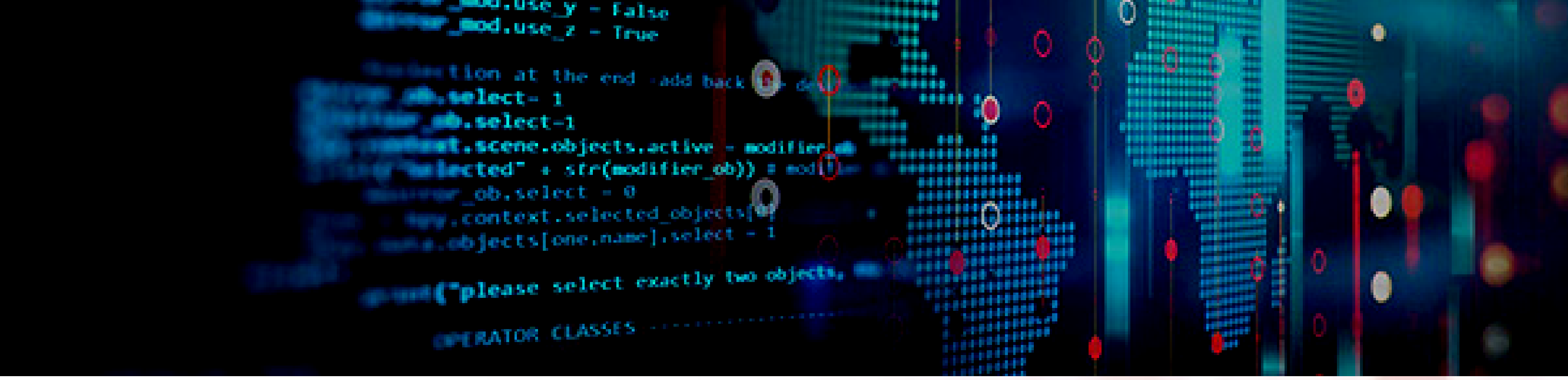
* [remote] SmartRG Router SR510n 2.6.13 - Remote Code Execution
* [webapps] CVAT 2.0 - Server Side Request Forgery
* [local] IOTransfer V4 - Unquoted Service Path
* [remote] AVEVA InTouch Access Anywhere Secure Gateway 2020 R2 - Path Traversal
* [remote] MSNSwitch Firmware MNT.2408 - Remote Code Execution
* [webapps] Open Web Analytics 1.7.3 - Remote Code Execution
* [webapps] Wordpress Plugin ImageMagick-Engine 1.7.4 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Wordpress Plugin Zephyr Project Manager 3.2.42 - Multiple SQLi
* [webapps] Testa 3.5.1 Online Test Management System - Reflected Cross-Site Scripting (XSS)
* [webapps] Aero CMS v0.0.1 - SQLi
* [webapps] Wordpress Plugin 3dady real-time web stats 1.0 - Stored Cross Site Scripting (XSS)
* [webapps] Wordpress Plugin WP-UserOnline 2.88.0 - Stored Cross Site Scripting (XSS)
* [remote] Teleport v10.1.1 - Remote Code Execution (RCE)
* [webapps] Feehi CMS 2.1.1 - Remote Code Execution (Authenticated)
* [webapps] TP-Link Tapo c200 1.1.15 - Remote Code Execution (RCE)
* [remote] WiFiMouse 1.8.3.4 - Remote Code Execution (RCE)
* [remote] Wifi HD Wireless Disk Drive 11 - Local File Inclusion
* [local] Blink1Control2 2.2.7 - Weak Password Encryption
* [webapps] Bookwyrm v0.4.3 - Authentication Bypass
* [webapps] Buffalo TeraStation Network Attached Storage (NAS) 1.66 - Authentication Bypass
* [remote] Airspan AirSpot 5410 version 0.3.4.1 - Remote Code Execution (RCE)
* [remote] Mobile Mouse 3.6.0.4 - Remote Code Execution (RCE)
* [webapps] Gitea 1.16.6 - Remote Code Execution (RCE) (Metasploit)
* [webapps] WordPress Plugin Netroics Blog Posts Grid 1.0 - Stored Cross-Site Scripting (XSS)
* [webapps] WordPress Plugin Testimonial Slider and Showcase 2.2.6 - Stored Cross-Site Scripting (XSS)

Exploit Database for offline use

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

```
user@yourlinux:~$ searchsploit keyword1 keyword2
```

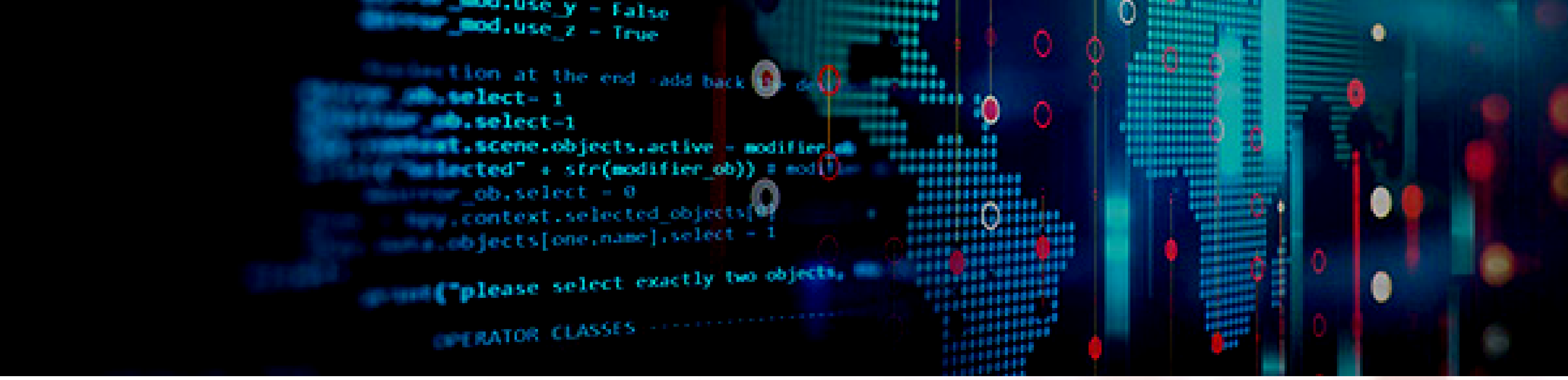
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://mumin.gob.ar/readme.html
http://mumin.gob.ar/readme.html notified by Mr.Rm19
http://ict.ayutthaya2.go.th/oni.html
http://ict.ayutthaya2.go.th/oni.html notified by Team Anon Force
http://audit.ayutthaya2.go.th/oni.html
http://audit.ayutthaya2.go.th/oni.html notified by Team Anon Force
https://www.ixtlahuacan.gob.mx
https://www.ixtlahuacan.gob.mx notified by mr.anderson
http://tfsconpg02ext.partners.extranet.microsoft.com
http://tfsconpg02ext.partners.extranet.microsoft.com notified by ZoRRoKiN
https://fsp.gov.pk/delta.txt
https://fsp.gov.pk/delta.txt notified by deltaboys
https://khcnbackan.gov.vn/read.html
https://khcnbackan.gov.vn/read.html notified by ./Niz4r
https://itrsudsoedarso.kalbarprov.go.id/0x.html
https://itrsudsoedarso.kalbarprov.go.id/0x.html notified by UnM@SK
http://sisfo.bbt.kemenperin.go.id/0x.html
http://sisfo.bbt.kemenperin.go.id/0x.html notified by UnM@SK
https://bp3airtanah.dpupesdm.jogjaprov.go.id/0x.html
https://bp3airtanah.dpupesdm.jogjaprov.go.id/0x.html notified by UnM@SK
https://data.polmankab.go.id/0x.html
https://data.polmankab.go.id/0x.html notified by UnM@SK
http://aplikasi.pa-pacitan.go.id/0x.html
http://aplikasi.pa-pacitan.go.id/0x.html notified by UnM@SK
https://inhouse.imi.gov.my/0x.html
https://inhouse.imi.gov.my/0x.html notified by UnM@SK
https://pekerja.sulutprov.go.id/0x.html
https://pekerja.sulutprov.go.id/0x.html notified by UnM@SK
https://reservasi.rsud.sukoharjokab.go.id/0x.html
https://reservasi.rsud.sukoharjokab.go.id/0x.html notified by UnM@SK
https://sismadak.rsud.sukoharjokab.go.id/0x.html
https://sismadak.rsud.sukoharjokab.go.id/0x.html notified by UnM@SK
https://karir.rsud.sukoharjokab.go.id/0x.html
https://karir.rsud.sukoharjokab.go.id/0x.html notified by UnM@SK

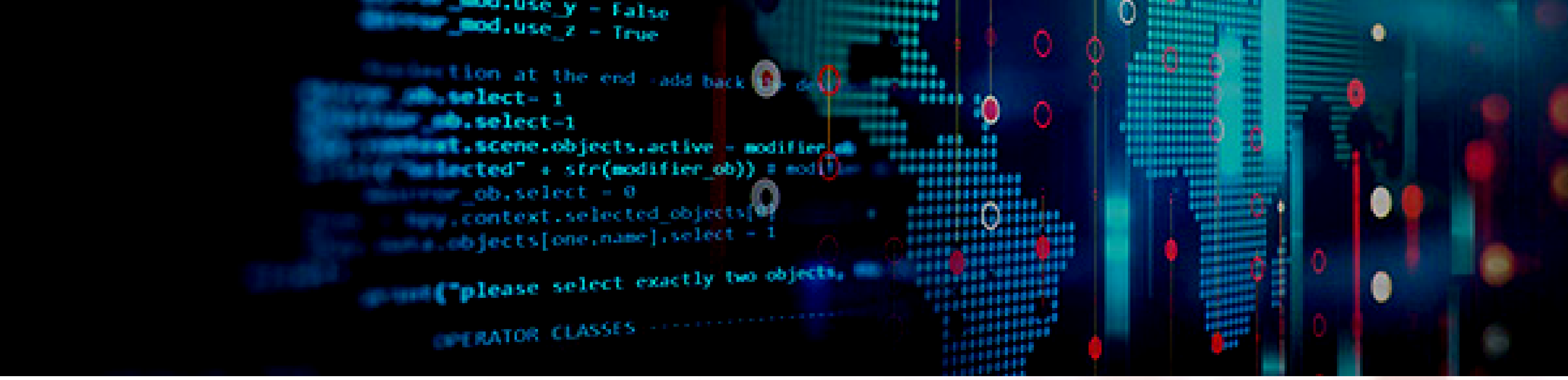


Dark Web News

Darknet Live

[Training by OSCE on cryptocurrencies and Dark Web investigations in Kyrgyzstan]
[Interpol Seizes $130 Million Worldwide from Cybercriminals]
[Vendor Narco710 Arrested]
[Russian LockBit Ransomware Operator Arrested in Canada]

Dark Web Link


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
lected" + str(modifier_ob)) # mod
ob.select = 0
py.context.selected_objects[0]
objects[one.name].select = 1
("please select exactly two objects
OPERATOR CLASSES

Trend Micro Anti-Malware Blog

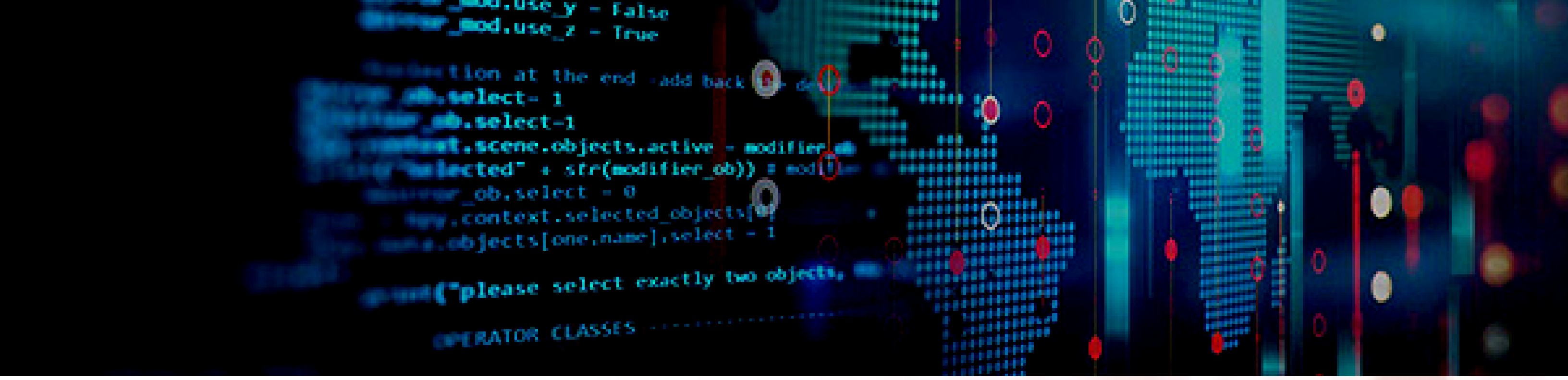
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

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&nbsp
* 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

* Leaked Android Platform Certificates Create Risks for Users
* Metasploit Weekly Wrap-Up
* Velociraptor Version 0.6.7: Better Offline Collection, Encryption, and an Improved NTFS Parser Dig De
* Powerlifting in the Cybersecurity Skills Gap
* Can Cloud Security Be Easier Than Complex?
* Rapid7 Integration For AWS Verified Access
* InsightIDR Launches Integration With New AWS Security Data Lake Service
* Unifying Threat Findings to Elevate Your Runtime Cloud Security
* Reducing Risk In The Cloud with Agentless Vulnerability Management
* Metasploit Weekly Wrap-Up



Advisories

US-Cert Alerts & bulletins

* CISA Adds One Known Exploited Vulnerability to Catalog
* #StopRansomware: Cuba Ransomware
* CISA Releases Three Industrial Control Systems Advisories
* CISA Releases Seven Industrial Control Systems Advisories
* CISA Adds Two Known Exploited Vulnerabilities to Catalog
* CISA Releases Eight Industrial Control Systems Advisories
* CISA, NSA, and ODNI Release Guidance for Customers on Securing the Software Supply Chain
* #StopRansomware: Hive
* AA22-335A: #StopRansomware: Cuba Ransomware
* AA22-321A: #StopRansomware: Hive Ransomware
* Vulnerability Summary for the Week of November 28, 2022
* Vulnerability Summary for the Week of November 21, 2022

Zero Day Initiative Advisories

ZDI-CAN-19746: Western Digital
A CVSS score 8.0 (AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Discovered by: Claroty Research - Vera Mens, Noam Moshe, Uri Katz, Sharon Brizinov' was reported to the affected vendor on: 2022-12-02, 3 days ago. The vendor is given until 2023-04-01 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19678: Western Digital
A CVSS score 8.0 (AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Claroty Research - Vera Mens, Noam Moshe, Uri Katz, Sharon Brizinov' was reported to the affected vendor on: 2022-12-02, 3 days ago. The vendor is given until 2023-04-01 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19604: Synology
A CVSS score 5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Claroty Research - Vera Mens, Noam Moshe, Uri Katz, Sharon Brizinov' was reported to the affected vendor on: 2022-12-02, 3 days ago. The vendor is given until 2023-04-01 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19744: Synology
A CVSS score 5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Discovered by: Claroty Research - Vera Mens, Noam Moshe, Uri Katz, Sharon Brizinov' was reported to the affected vendor on: 2022-12-02, 3 days ago. The vendor is given until 2023-04-01 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19743: Synology
A CVSS score 4.3 (AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Discovered by: Claroty Research - Vera Mens, Noam Moshe, Uri Katz, Sharon Brizinov' was reported to the affected vendor

on: 2022-12-02, 3 days ago. The vendor is given until 2023-04-01 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19741: Synology

A CVSS score 8.0 (AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Discovered by: Claroty Research - Vera Mens, Noam Moshe, Uri Katz, Sharon Brizinov' was reported to the affected vendor on: 2022-12-02, 3 days ago. The vendor is given until 2023-04-01 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19708: Synology

A CVSS score 7.5 (AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Claroty Research - Vera Mens, Noam Moshe, Uri Katz, Sharon Brizinov' was reported to the affected vendor on: 2022-12-02, 3 days ago. The vendor is given until 2023-04-01 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19742: Synology

A CVSS score 5.7 (AV:A/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H) severity vulnerability discovered by 'Discovered by: Claroty Research - Vera Mens, Noam Moshe, Uri Katz, Sharon Brizinov' was reported to the affected vendor on: 2022-12-02, 3 days ago. The vendor is given until 2023-04-01 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19191: Trend Micro

A CVSS score 7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Lynn and Lays (@_L4ys)' was reported to the affected vendor on: 2022-12-02, 3 days ago. The vendor is given until 2023-04-01 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19192: Trend Micro

A CVSS score 7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Lynn and Lays (@_L4ys)' was reported to the affected vendor on: 2022-12-02, 3 days ago. The vendor is given until 2023-04-01 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19188: Trend Micro

A CVSS score 7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Lynn and Lays (@_L4ys)' was reported to the affected vendor on: 2022-12-02, 3 days ago. The vendor is given until 2023-04-01 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-18935: Microsoft

A CVSS score 5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L) severity vulnerability discovered by 'insu of 78ResearchLab' was reported to the affected vendor on: 2022-12-02, 3 days ago. The vendor is given until 2023-04-01 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19648: SolarWinds

A CVSS score 7.2 (AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Piotr Bazydlo (@chudypb) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-12-02, 3 days ago. The vendor is given until 2023-04-01 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19107: VBASE

A CVSS score 5.5 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2022-12-02, 3 days ago. The vendor is given until 2023-04-01 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19530: X.Org

A CVSS score 7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Jan-Niklas

Sohn' was reported to the affected vendor on: 2022-12-02, 3 days ago. The vendor is given until 2023-04-01 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19621: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-11-30, 5 days ago. The vendor is given until 2023-03-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19620: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-11-30, 5 days ago. The vendor is given until 2023-03-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19606: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-11-30, 5 days ago. The vendor is given until 2023-03-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19516: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-11-30, 5 days ago. The vendor is given until 2023-03-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19515: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-11-30, 5 days ago. The vendor is given until 2023-03-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19617: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-11-30, 5 days ago. The vendor is given until 2023-03-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19517: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-11-30, 5 days ago. The vendor is given until 2023-03-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19605: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-11-30, 5 days ago. The vendor is given until 2023-03-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-19406: Delta Electronics

A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-11-30, 5 days ago. The vendor is given until 2023-03-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Ubuntu Security Notice USN-5760-1

Ubuntu Security Notice 5760-1 - It was discovered that libxml2 incorrectly handled certain XML files. An attacker could possibly use this issue to cause a crash. It was discovered that libxml2 incorrectly handled certain XML files. An attacker could possibly use this issue to expose sensitive information or cause a crash. It was discovered that libxml2 incorrectly handled certain XML files. An attacker could possibly use this issue to execute arbitrary code.

Ubuntu Security Notice USN-5759-1

Ubuntu Security Notice 5759-1 - It was discovered that LibBPF incorrectly handled certain memory operations under certain circumstances. An attacker could possibly use this issue to cause LibBPF to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue only affected Ubuntu 22.10. It was discovered that LibBPF incorrectly handled certain memory operations under certain circumstances. An attacker could possibly use this issue to cause LibBPF to crash, resulting in a denial of service, or possibly execute arbitrary code.

Debian Security Advisory 5295-1

Debian Linux Security Advisory 5295-1 - A security issue was discovered in Chromium, which could result in the execution of arbitrary code.

Debian Security Advisory 5294-1

Debian Linux Security Advisory 5294-1 - Jhead, a tool for manipulating EXIF data embedded in JPEG images, allowed attackers to execute arbitrary OS commands by placing them in a JPEG filename and then using the regeneration -rgt50, -autorot or -ce option. In addition a buffer overflow error in exif.c has been addressed which could lead to a denial of service (application crash).

Debian Security Advisory 5293-1

Debian Linux Security Advisory 5293-1 - Multiple security issues were discovered in Chromium, which could result in the execution of arbitrary code, denial of service or information disclosure.

Ubuntu Security Notice USN-5756-2

Ubuntu Security Notice 5756-2 - Jann Horn discovered that the Linux kernel did not properly track memory allocations for anonymous VMA mappings in some situations, leading to potential data structure reuse. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. It was discovered that a memory leak existed in the IPv6 implementation of the Linux kernel. A local attacker could use this to cause a denial of service.

Ubuntu Security Notice USN-5755-2

Ubuntu Security Notice 5755-2 - It was discovered that the NFSD implementation in the Linux kernel did not properly handle some RPC messages, leading to a buffer overflow. A remote attacker could use this to cause a denial of service or possibly execute arbitrary code. Jann Horn discovered that the Linux kernel did not properly track memory allocations for anonymous VMA mappings in some situations, leading to potential data structure reuse. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Red Hat Security Advisory 2022-8767-01

Red Hat Security Advisory 2022-8767-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include an out of bounds write vulnerability.

Red Hat Security Advisory 2022-8765-01

Red Hat Security Advisory 2022-8765-01 - The kernel-rt packages provide the Real Time Linux Kernel, which enables fine-tuning for systems with extremely high determinism requirements. Issues addressed include an out of bounds write vulnerability.

Red Hat Security Advisory 2022-8768-01

Red Hat Security Advisory 2022-8768-01 - 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 an out of bounds write vulnerability.

Red Hat Security Advisory 2022-8750-01

Red Hat Security Advisory 2022-8750-01 - OpenShift Virtualization is Red Hat's virtualization solution designed for Red Hat OpenShift Container Platform. Issues addressed include denial of service and out of bounds read vulnerabilities.

Ubuntu Security Notice USN-5758-1

Ubuntu Security Notice 5758-1 - Jann Horn discovered that the Linux kernel did not properly track memory allocations for anonymous VMA mappings in some situations, leading to potential data structure reuse. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. It was discovered that the video4linux driver for Empia based TV cards in the Linux kernel did not properly perform reference counting in some situations, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5757-2

Ubuntu Security Notice 5757-2 - Jann Horn discovered that the Linux kernel did not properly track memory allocations for anonymous VMA mappings in some situations, leading to potential data structure reuse. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. It was discovered that the video4linux driver for Empia based TV cards in the Linux kernel did not properly perform reference counting in some situations, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5757-1

Ubuntu Security Notice 5757-1 - Jann Horn discovered that the Linux kernel did not properly track memory allocations for anonymous VMA mappings in some situations, leading to potential data structure reuse. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. It was discovered that the video4linux driver for Empia based TV cards in the Linux kernel did not properly perform reference counting in some situations, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5756-1

Ubuntu Security Notice 5756-1 - Jann Horn discovered that the Linux kernel did not properly track memory allocations for anonymous VMA mappings in some situations, leading to potential data structure reuse. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. It was discovered that a memory leak existed in the IPv6 implementation of the Linux kernel. A local attacker could use this to cause a denial of service.

Ubuntu Security Notice USN-5755-1

Ubuntu Security Notice 5755-1 - It was discovered that the NFSD implementation in the Linux kernel did not properly handle some RPC messages, leading to a buffer overflow. A remote attacker could use this to cause a denial of service or possibly execute arbitrary code. Jann Horn discovered that the Linux kernel did not properly track memory allocations for anonymous VMA mappings in some situations, leading to potential data structure reuse. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Debian Security Advisory 5292-1

Debian Linux Security Advisory 5292-1 - The Qualys Research Team discovered a race condition in the snapd-confine binary which could result in local privilege escalation.

Ubuntu Security Notice USN-5743-2

Ubuntu Security Notice 5743-2 - USN-5743-1 fixed a vulnerability in LibTIFF. This update provides the corresponding updates for Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 22.04 LTS and Ubuntu 22.10. It was discovered that LibTIFF incorrectly handled certain malformed images. If a user or automated system were tricked into opening a specially crafted image, a remote attacker could crash the application, leading to a denial of service, or possibly execute arbitrary code with user privileges.

Ubuntu Security Notice USN-5754-1

Ubuntu Security Notice 5754-1 - It was discovered that the NFSD implementation in the Linux kernel did not properly handle some RPC messages, leading to a buffer overflow. A remote attacker could use this to cause a denial of service or possibly execute arbitrary code. It was discovered that a memory leak existed in the IPv6 implementation of the Linux kernel. A local attacker could use this to cause a denial of service.

Ubuntu Security Notice USN-5753-1

Ubuntu Security Notice 5753-1 - The Qualys Research Team discovered that a race condition existed in the snapd snap-confine binary when preparing the private /tmp mount for a snap. A local attacker could possibly use this issue to escalate privileges and execute arbitrary code.

Ubuntu Security Notice USN-5752-1

Ubuntu Security Notice 5752-1 - David Bouman and Billy Jheng Bing Jhong discovered that a race condition existed in the io_uring subsystem 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 execute arbitrary code. Soenke Huster discovered that an integer overflow vulnerability existed in the WiFi driver stack in the Linux kernel, leading to a buffer overflow. A physically proximate attacker could use this to cause a denial of service or possibly execute arbitrary code.

Intel Data Center Manager 4.1.1.45749 Authentication Bypass / Spoofing

Intel Data Center Manager versions 4.1.1.45749 and below suffer from an authentication bypass vulnerability via spoofing.

Ubuntu Security Notice USN-5718-2

Ubuntu Security Notice 5718-2 - USN-5718-1 fixed a vulnerability in pixman. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. Maddie Stone discovered that pixman incorrectly handled certain memory operations. A remote attacker could use this issue to cause pixman to crash, resulting in a denial of service, or possibly execute arbitrary code.

Ubuntu Security Notice USN-5750-1

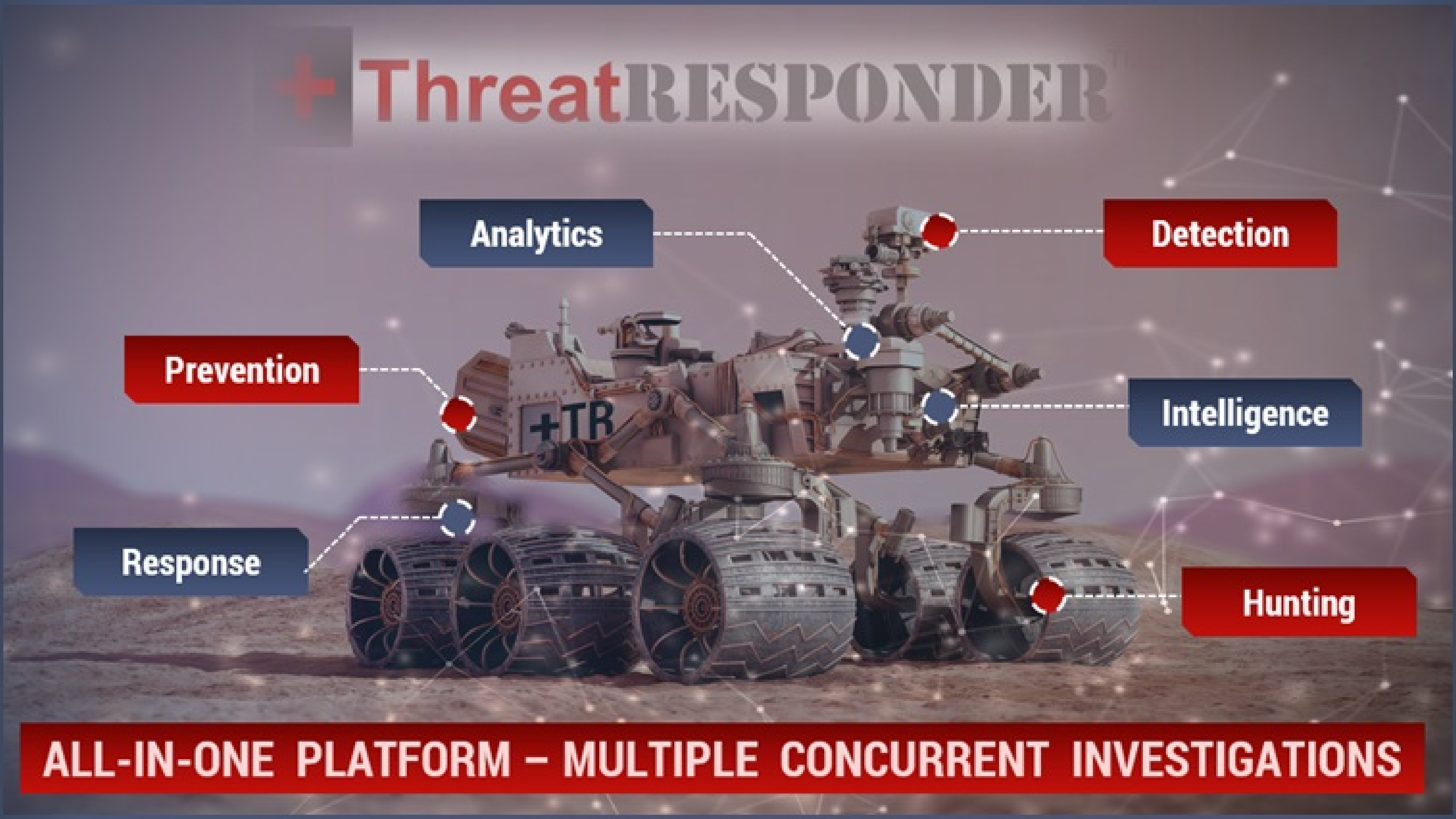
Ubuntu Security Notice 5750-1 - It was discovered that GnuTLS incorrectly handled certain memory operations. A remote attacker could possibly use this issue to cause GnuTLS to crash, resulting in a denial of service.

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



ALL-IN-ONE PLATFORM – MULTIPLE CONCURRENT INVESTIGATIONS

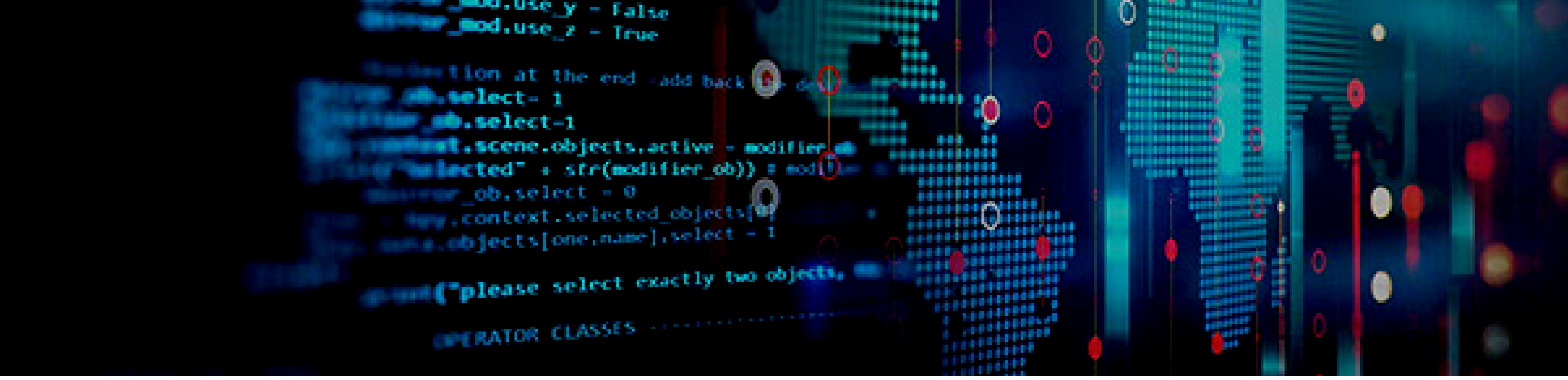
The Solution – ThreatResponder® Platform

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



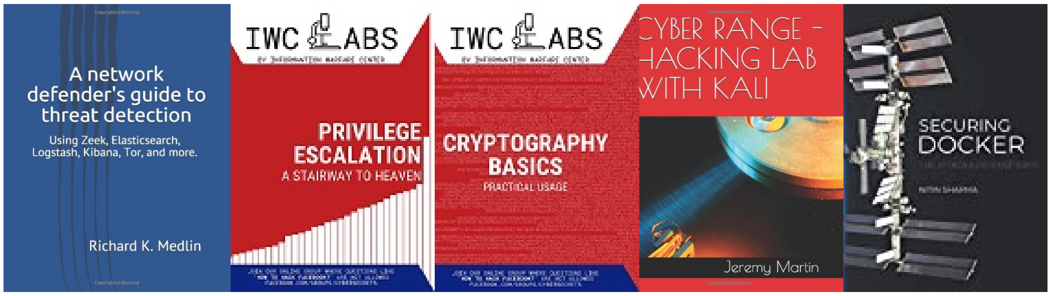
The Cyber Secrets publications on Amazon

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 WHILE DRINKING OUR JUICE IN THE HOOD
THE 8 LAYERS OF THE OSI CAKE A FORENSIC TASTE OF EACH LAYER
LAUNCHING EXPLOITS ONE SMALL VULNERABILITY FOR A COMPANY, ONE GIANT HEAP FOR PORT BIND.
INCIDENT RESPONSE DO NOT CROSS
INCIDENT RESPONSE EVIDENCE PRESERVATION AND COLLECTION

Other Publications from Information Warfare Center


A network defender's guide to threat detection
Using Zeek, Elasticsearch, Logstash, Kibana, Tor, and more.
Richard K. Medlin
IWC LABS
PRIVILEGE ESCALATION A STAIRWAY TO HEAVEN
IWC LABS
CRYPTOGRAPHY BASICS PRACTICAL USAGE
CYBER RANGE - HACKING LAB WITH KALI
Jeremy Martin
SECURING DOCKER

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

CSI LINUX

netSecurity®

ThreatRESPONDER

Accredited Training Center EC-Council

CYBERQ GROUP