Nov-28-22

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

November 28, 2022

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

Summary

Internet Storm Center Infocon Status

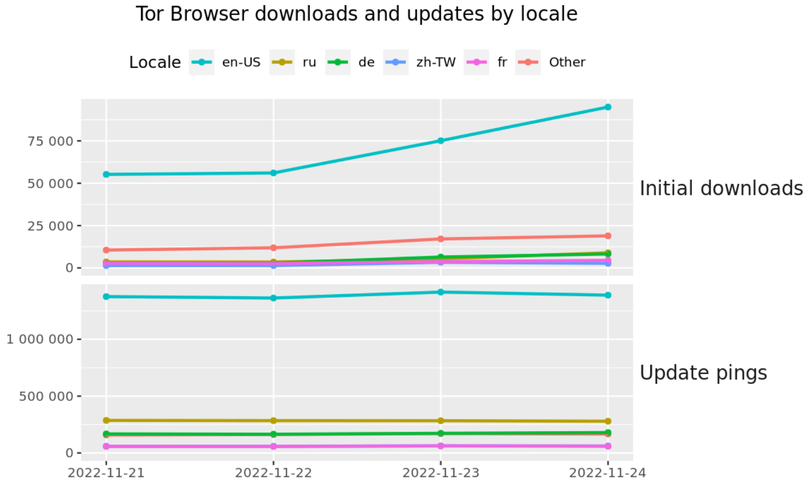
INTERNET STORM CENTER
infocon:GREEN
http://isc.sans.edu

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

* Gangs Of Cybercriminals Are Expanding Across Africa
* MEPs' Spyware Inquiry Targeted By Disinformation Campaign
* Chinese Bots Flood Twitter In Attempt To Obscure Covid Protests
* Twitter Lacks Transparency In Misinformation Fight
* US Bans Sales Of Huawei, ZTE Tech Amid Security Fears
* Hacker Attempts To Sell Data Of 500m WhatsApp Users On Dark Web
* Google Issues Emergency Chrome Security Update For All Users
* Musk To Abused Twitter Users: Your Tormentors Are Coming Back
* Iranian Hacker Group Publishes Video Of Jerusalem Attacks
* UK Bans Chinese CCTV Cameras On Sensitive Government Sites
* U.S. Navy Forced To Pay Software Company For Piracy
* Meta Claims US Military Link To Online Propaganda Campaign
* European Parliament Putin Things Back Together After Cyber Attack
* Elon Musk Hires PlayStation 3 Hacker To Fix Twitter
* AWS Fixes Confused Deputy Vulnerability In AppSync
* Sneaky Ways Cops Could Access Data To Widely Prosecute Abortions In The US
* SocGholish Finds Success Through Novel Email Techniques
* DraftKings Gamblers Lose $300,000 To Credential Stuffing Attack
* WikiLeaks' Website Is Falling Apart
* DraftKings Says There Is No Evidence Systems Were Breached
* Enterprise Healthcare Warned Of Lorenz Ransomware
* Microsoft's Attempt To Harden Kerberos Broke It
* 73 Percent Of Retail Applications Contain Security Flaws, But Only A Quarter Are Fixed
* World Cup Phishing Emails Spike In Middle Eastern Countries
* A Leak Details Apple's Secret Dirt On A Trusted Security Startup

Krebs on Security

* 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
* Accused 'Raccoon' Malware Developer Fled Ukraine After Russian Invasion
* Battle with Bots Prompts Mass Purge of Amazon, Apple Employee Accounts on LinkedIn
* How Card Skimming Disproportionally Affects Those Most In Need

LATEST NEWS

Dark Reading

* KnowBe4 Launches New Mobile Learner App for Cybersecurity Learning
* NanoLock Brings Built-In Meter-Level Cybersecurity to Renesas Customers
* Bring Your Own Key - A Placebo?
* Slippery RansomExx Malware Moves to Rust, Evading VirusTotal
* For Gaming Companies, Cybersecurity Has Become a Major Value Proposition
* How Development Teams Should Respond to Text4Shell
* Why Africa's Telecoms Must Actively Collaborate to Combat Fraud
* 'Patch Lag' Leaves Millions of Android Devices Vulnerable
* Hot Ticket: 'Aurora' Go-Based InfoStealer Finds Favor Among Cyber-Threat Actors
* Microsoft: Popular IoT SDKs Leave Critical Infrastructure Wide Open to Cyberattack
* Penetration Testing Market Size Is Projected to Reach $5.28B Globally by 2028
* Where Are We Heading With Data Privacy Regulations?
* Cybersecurity Pros Put Mastodon Flaws Under the Microscope
* Adversarial AI Attacks Highlight Fundamental Security Issues
* Ducktail Cyberattackers Add WhatsApp to Facebook Business Attack Chain
* DraftKings Account Takeovers Frame Sports-Betting Cybersecurity Dilemma
* Cyber Due Diligence in M&As Uncovers Threats, Improves Valuations
* How Work From Home Shaped the Road to SASE for Enterprises
* Enterprises Pay $1,200 Per Employee Annually to Fight Cyberattacks Against Cloud Collab Apps
* Google Blocks 231B Spam, Phishing Emails in Past 2 Weeks

The Hacker News

* Researchers Detail AppSync Cross-Tenant Vulnerability in Amazon Web Services
* The 5 Cornerstones for an Effective Cyber Security Awareness Training
* Over a Dozen New BMC Firmware Flaws Expose OT and IoT Devices to Remote Attacks
* Elon Musk Confirms Twitter 2.0 will Bring End-to-End Encryption to Direct Messages
* All You Need to Know About Emotet in 2022
* U.S. Bans Chinese Telecom Equipment and Surveillance Cameras Over National Security Risk
* Russia-based RansomBoggs Ransomware Targeted Several Ukrainian Organizations
* Update Chrome Browser Now to Patch New Actively Exploited Zero-Day Flaw
* Dell, HP, and Lenovo Devices Found Using Outdated OpenSSL Versions
* U.K. Police Arrest 142 in Global Crackdown on 'iSpoof' Phone Spoofing Service
* Interpol Seized $130 Million from Cybercriminals in Global "HAECHI-III" Crackdown Operation
* New RansomExx Ransomware Variant Rewritten in the Rust Programming Language
* Millions of Android Devices Still Don't Have Patches for Mali GPU Flaws
* Boost Your Security with Europe's Leading Bug Bounty Platform
* Bahamut Cyber Espionage Hackers Targeting Android Users with Fake VPN Apps

LATEST NEWS

Security Week

* Project Zero Flags 'Patch Gap' Problems on Android
* Irish Regulator Fines Meta 265 Million Euros Over Data Breach
* Hack-for-Hire Group Targets Android Users With Malicious VPN Apps
* Crackdown on African Cybercrime Leads to Arrests, Infrastructure Takedown
* Twitter Data Breach Bigger Than Initially Reported
* Cisco ISE Vulnerabilities Can Be Chained in One-Click Exploit
* Google Patches Eighth Chrome Zero-Day of 2022
* US Bans Huawei, ZTE Telecoms Gear Over Security Risk
* EU Parliament Website Attacked After MEPs Slam Russian 'Terrorism'
* Proofpoint: Watch Out for Nighthawk Hacking Tool Abuse
* Cross-Tenant AWS Vulnerability Exposed Account Resources
* Facebook Parent Meta Links Influence Campaign to US Military
* Microsoft Warns of Boa Web Server Risks After Hackers Target It in Power Grid Attacks
* CISA Updates Infrastructure Resilience Planning Framework
* Multi-Purpose Botnet and Infostealer 'Aurora' Rising to Fame
* Leaked Algolia API Keys Exposed Data of Millions of Users
* BMC Firmware Vulnerabilities Expose OT, IoT Devices to Remote Attacks
* Vietnam-Based Ducktail Cybercrime Operation Evolving, Expanding
* Digesting CISA's Cross-Sector Cybersecurity Performance Goals
* Microsoft Releases Out-of-Band Update After Security Patch Causes Kerberos Issues
* Cisco Secure Email Gateway Filters Bypassed Due to Malware Scanner Issue
* US Offshore Oil and Gas Infrastructure at Significant Risk of Cyberattacks
* California County Says Personal Information Compromised in Data Breach
* 33 Attorneys General Send Letter to FTC on Commercial Surveillance Rules
* Google Making Cobalt Strike Pentesting Tool Harder to Abuse
* PoC Code Published for High-Severity macOS Sandbox Escape Vulnerability

Infosecurity Magazine

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* Users Can Engage with Training Anytime with KnowBe4's Mobile Learner App
* There's No Such Thing as a Free Yeti, Only Social Engineering Tactics
* WhatsApp data breach sees nearly 500 million user records up for sale
* [Send This To Your Users] 5 Top Scams To Watch Out For This Holiday Season
* Cybersecurity incidents cost organizations $1,197 per employee, per year
* A Recent, Complex, Ransomware Campaign
* New Instagram Support Phishing Attack Fakes "Unusual Logon" Experience Well Enough to Fool Victims
* Image-Based Phishing and Phone Scams Continue to Get Past Security Scanners
* CyberheistNews Vol 12 #47 [Heads Up] Watch Out for This Tricky New Tactic Called Clone Phishing
* World Cup Phishing Attacks Doubled And Will Increase

ISC2.org Blog

* 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
* Latest Cyberthreats and Advisories - November 18, 2022
* OT: The New Gold Mine for Hackers and How CDS Can Secure It

HackRead

* Iran's Fars News Agency website hacked as part of anti-govt protests
* Nearly 500 million WhatsApp User Records Sold Online
* How to Create ISO Files from Discs - 3 Best Ways
* Top 6 Cell Phone Tracker Apps for Parental Control
* Moses Staff Hackers Publish Footage of Jerusalem Explosion
* Watch Out Gamers: Hackers Exploiting MSI Afterburner to Deliver Coin Miner
* How to use Linked Helper 2 as a LinkedIn Data Export Tool

Koddos

* Iran's Fars News Agency website hacked as part of anti-govt protests
* Nearly 500 million WhatsApp User Records Sold Online
* How to Create ISO Files from Discs - 3 Best Ways
* Top 6 Cell Phone Tracker Apps for Parental Control
* Moses Staff Hackers Publish Footage of Jerusalem Explosion
* Watch Out Gamers: Hackers Exploiting MSI Afterburner to Deliver Coin Miner
* How to use Linked Helper 2 as a LinkedIn Data Export Tool

LATEST NEWS

Naked Security

* Chrome fixes 8th zero-day of 2022 - check your version now
* Voice-scamming site "iSpoof" seized, 100s arrested in massive crackdown
* S3 Ep110: Spotlight on cyberthreats - an expert speaks [Audio + Text]
* Multimillion dollar CryptoRom scam sites seized, suspects arrested in US
* How to hack an unpatched Exchange server with rogue PowerShell code
* How social media scammers buy time to steal your 2FA codes
* Black Friday and retail season - watch out for PayPal "money request" scams
* S3 Ep109: How one leaked email password could drain your business [Audio + Transcript]
* Firefox fixes fullscreen fakery flaw - get the update now!
* Log4Shell-like code execution hole in popular Backstage dev tool

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

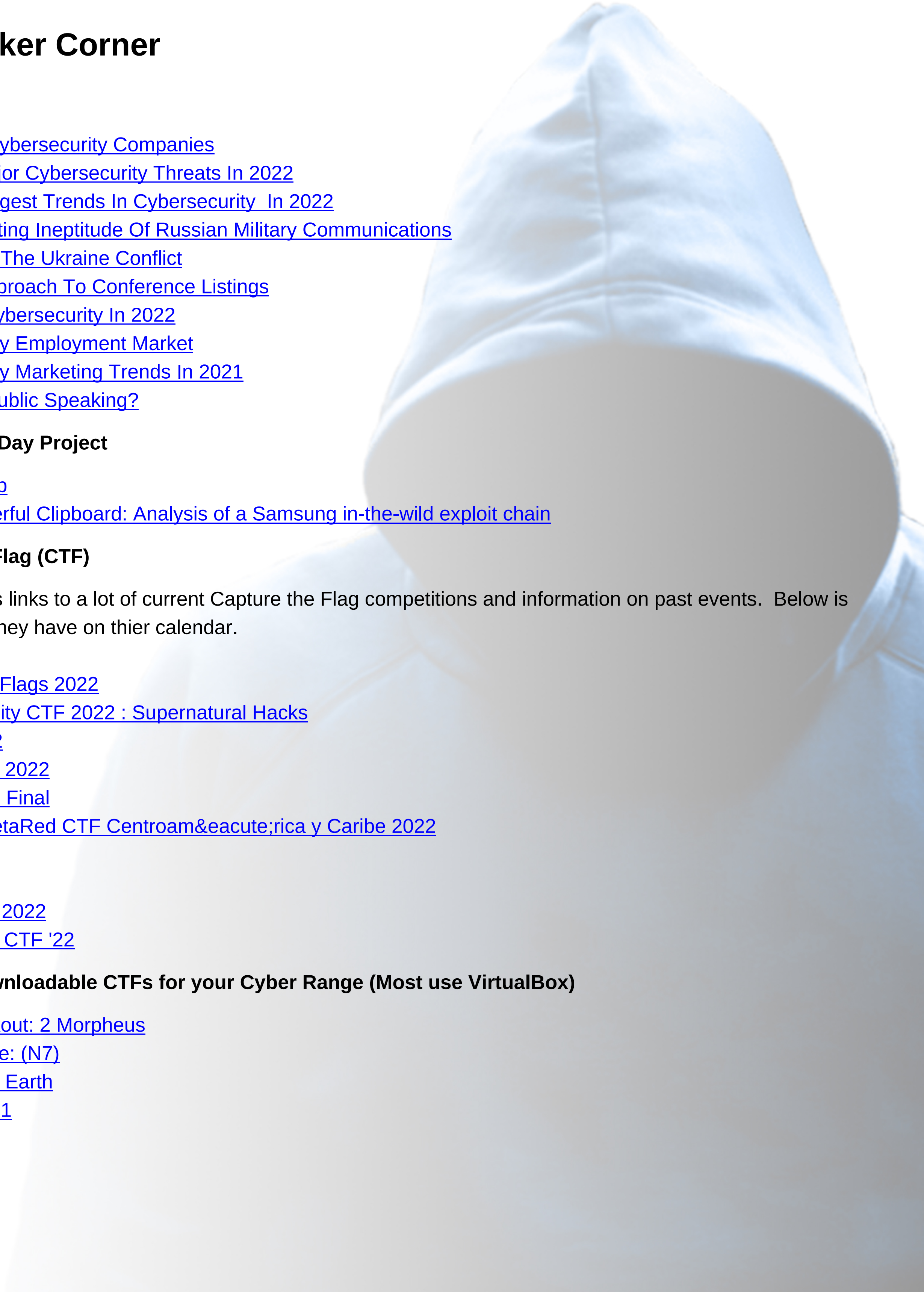
* Worms of Wisdom: How WannaCry Shapes Cybersecurity Today
* Emotional Blowback: Dealing With Post-Incident Stress
* RansomExx Upgrades to Rust
* Why Operational Technology Security Cannot Be Avoided
* Resilient Companies Have a Disaster Recovery Plan
* What People Get Wrong About Incident Responders
* Tech Stack Diversity: Security Benefits and Costs
* Moving at the Speed of Business - Challenging Our Assumptions About Cybersecurity
* Effectively Enforce a Least Privilege Strategy
* How the DNSChanger Shutdown Changed Cybersecurity

InfoWorld

* AWS releases Wickr, its encrypted messaging service for enterprises
* What AWS customers really care about
* 5 risks of AI and machine learning that modelops remediates
* 5 operations every cloud architect should automate
* ML.NET 2.0 enhances text classification
* What is the JRE? Introduction to the Java Runtime Environment
* Integrating Web3 technologies with Azure Devops
* JDK 20: The new features in Java 20
* IBM sues Micro Focus for mainframe software copyright infringement
* What's coming for cloud computing in 2023

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

* 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 2022
* Cybersecurity Employment Market
* Cybersecurity Marketing Trends In 2021
* Is It Worth Public Speaking?

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.

* STACK The Flags 2022
* HTB University CTF 2022 : Supernatural Hacks
* TUCTF 2022
* InfoSec CTF 2022
* M*CTF 2022 Final
* 6th stage MetaRed CTF Centroam&eacute;rica y Caribe 2022
* Shakti CTF
* Ph0wn 2022
* KITCTFCTF 2022
* Hackappatoi CTF '22

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

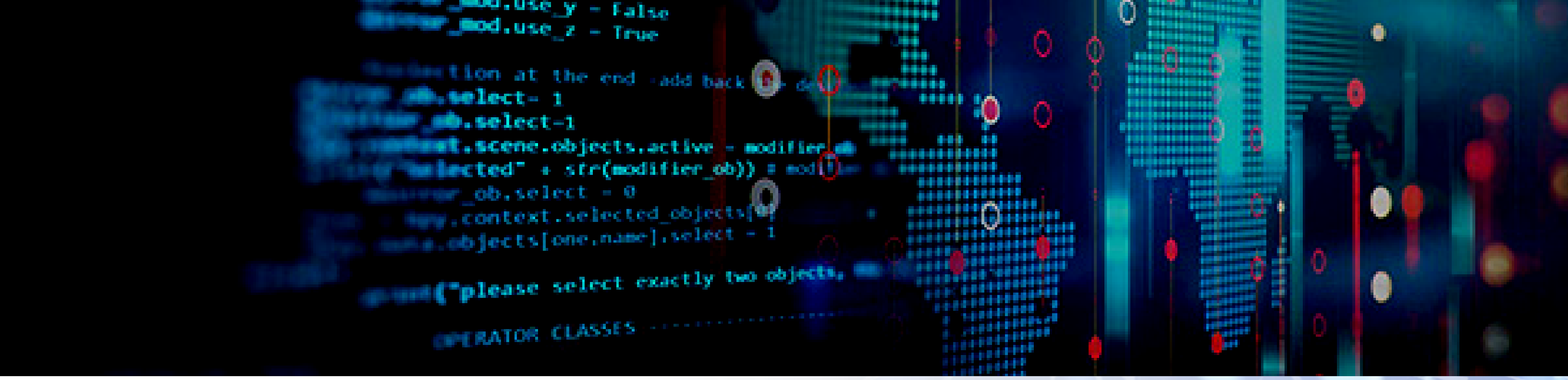
* Falco 0.33.1
* Zeek 5.0.4
* Packet Fence 12.1.0
* Stegano 0.11.1
* I2P 2.0.0
* TOR Virtual Network Tunneling Tool 0.4.7.11
* Zeek 5.0.3
* GNUnet P2P Framework 0.18.1
* OpenSSL Toolkit 3.0.7
* OpenSSL Toolkit 1.1.1s

Kali Linux Tutorials

* Octopii : An AI-powered Personal Identifiable Information (PII) Scanner
* Scrcpy : Display And Control Your Android Device
* Ox4Shell : Deobfuscate Log4Shell Payloads With Ease
* Stegowiper : A Powerful And Flexible Tool To Apply Active Attacks For Disrupting Stegomalware
* Sandbox Scryer : Tool For Producing Threat Hunting And Intelligence Data From Public Sandbox Detonati
* Wodat : Windows Oracle Database Attack Toolkit
* ODAT : Oracle Database Attacking Tool
* Slicer : Tool To Automate The Boring Process Of APK Recon
* Nuvola : Tool To Dump & Perform Automatic And Manual Security Analysis On AWS
* Dismember : Scan Memory For Secrets And More

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

* Hunting Threat Actors Using OSINT
* Updates in DFIR
* Threat Hunting in Microsoft 365 Environment
* WhatsApp with Your iMessage, Dude?!

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

* OS Detection - USB Rubber Ducky
* Live Hacking Q&A with Kody and Michael
* Google Pixel Lockscreen Bypass - ThreatWire

The PC Security Channel [TPSC]

* Do you need antivirus on your phone?
* Fileless Ransomware: Powershell Netwalker

Eli the Computer Guy

* FTX DISASTER - Cryptocurrency is STUPID
* ALEX JONES on TWITTER - #RIPTwitter
* TRUMP BACK ON TWITTER - #RIPTwitter
* #RIPTwitter - Twitter Employees Flee/ Offices on Lockdown

Security Now

* Wi-Peep - FBI purchased Pegasus, Passkey support directory, Quantum decryption deadline, Firefox 107
* Memory-Safe Languages - Shennina Framework, Shufflecake, The Helm, LightSpeed vulnerabilities

Troy Hunt

* Weekly Update 323

Intel Techniques: The Privacy, Security, & OSINT Show

* 284-Password Managers & 2FA Revisited
* 283-Announcements, Updates, & News

Proof of Concept (PoC) & Exploits

Packet Storm Security

* 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
* ChurchInfo 1.2.13-1.3.0 Remote Code Execution
* F5 BIG-IP iControl Cross Site Request Forgery
* Roxy Fileman 1.4.6 Remote Shell Upload
* Boa Web Server 0.94.13 / 0.94.14 Authentication Bypass
* Microsoft Outlook 2019 16.0.13231.20262 Remote Code Execution
* Microsoft Outlook 2019 16.0.12624.20424 Out-Of-Bounds Read
* ZTE ZXHN-H108NS Authentication Bypass
* WordPress BeTheme 26.5.1.4 PHP Object Injection
* Backdoor.Win32.Oblivion.01.a MVID-2022-0658 Insecure Transit
* ZTE ZXHN-H108NS Stack Buffer Overflow / Denial Of Service
* ClicShopping 3.402 Cross Site Scripting
* Trojan.Win32.Platinum.gen MVID-2022-0657 Code Execution
* AppleAVD AppleAVDUserClient::decodeFrameFig Memory Corruption

CXSecurity

* 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
* VMware NSX Manager XStream Unauthenticated Remote Code Execution
* MSNSwitch Firmware MNT.2408 Remote Code Execution
* Automated Tank Gauge (ATG) Remote Configuration Disclosure

Proof of Concept (PoC) & Exploits

Exploit Database

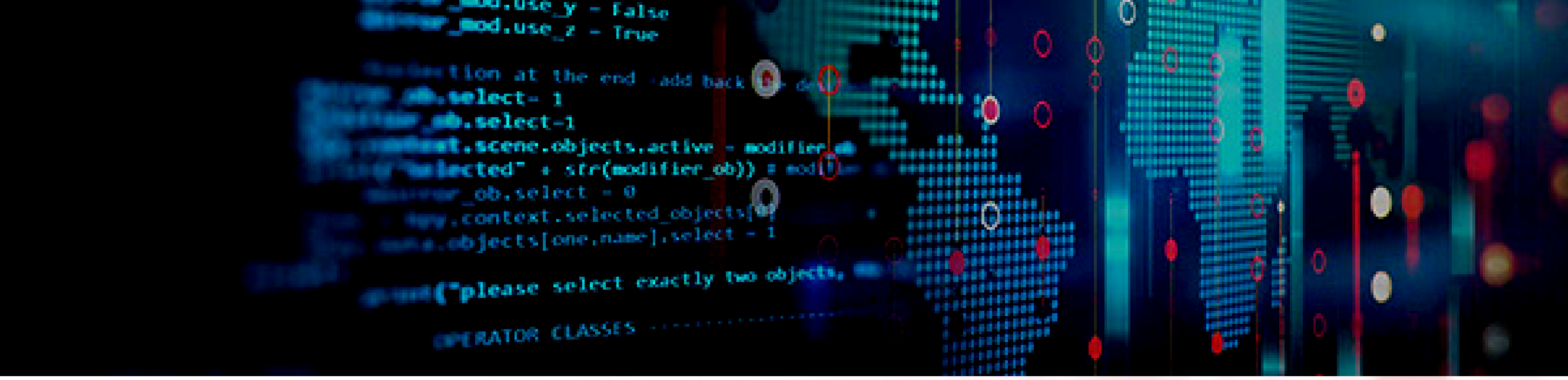
* [remote] SmartRG Router SR510n 2.6.13 - Remote Code Execution
* [webapps] CVAT 2.0 - Server Side Request Forgery
* [local] IOTransfer V4 - Unquoted Service Path
* [remote] AVEVA InTouch Access Anywhere Secure Gateway 2020 R2 - Path Traversal
* [remote] MSNSwitch Firmware MNT.2408 - Remote Code Execution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

Exploit Database for offline use

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

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

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



Latest Hacked Websites

Published on Zone-h.org

https://bakesbangpol.palopokota.go.id/zzz.htm

https://bakesbangpol.palopokota.go.id/zzz.htm notified by Fuck malaysia

https://covid19.palopokota.go.id/zzz.htm

https://covid19.palopokota.go.id/zzz.htm notified by Fuck malaysia

https://dinkes.palopokota.go.id/zzz.htm

https://dinkes.palopokota.go.id/zzz.htm notified by Fuck malaysia

http://damkar.palopokota.go.id/zzz.htm

http://damkar.palopokota.go.id/zzz.htm notified by Fuck malaysia

https://dppkb.palopokota.go.id/zzz.htm

https://dppkb.palopokota.go.id/zzz.htm notified by Fuck malaysia

https://diskominfo.palopokota.go.id/zzz.htm

https://diskominfo.palopokota.go.id/zzz.htm notified by Fuck malaysia

https://disdukcapil.palopokota.go.id/zzz.htm

https://disdukcapil.palopokota.go.id/zzz.htm notified by Fuck malaysia

https://dprd.palopokota.go.id/zzz.htm

https://dprd.palopokota.go.id/zzz.htm notified by Fuck malaysia

https://diskan.palopokota.go.id/zzz.htm

https://diskan.palopokota.go.id/zzz.htm notified by Fuck malaysia

http://pontap.palopokota.go.id/zzz.htm

http://pontap.palopokota.go.id/zzz.htm notified by Fuck malaysia

https://portal.palopokota.go.id/zzz.htm

https://portal.palopokota.go.id/zzz.htm notified by Fuck malaysia

https://rsudpalemmai.palopokota.go.id/zzz.htm

https://rsudpalemmai.palopokota.go.id/zzz.htm notified by Fuck malaysia

http://saberpungli.palopokota.go.id/zzz.htm

http://saberpungli.palopokota.go.id/zzz.htm notified by Fuck malaysia

http://setda.palopokota.go.id/zzz.htm

http://setda.palopokota.go.id/zzz.htm notified by Fuck Malaysia

https://rsudswg.palopokota.go.id/zzz.htm

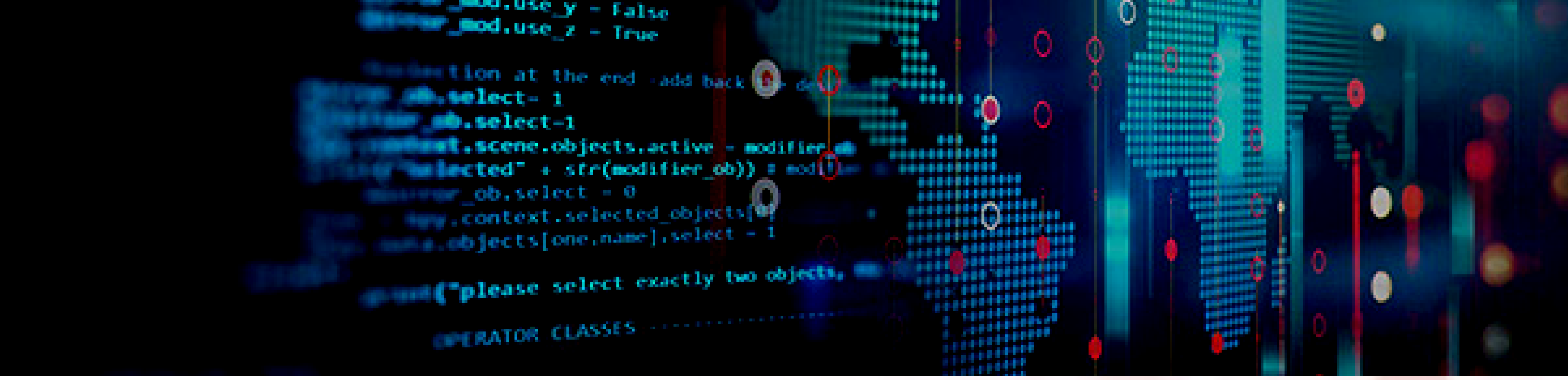
https://rsudswg.palopokota.go.id/zzz.htm notified by Indonesia Attacker #OpMalaysia

https://balitsereal-litbang-ppid.pertanian.go.id/assets/foto/33/32822/foto_32822.gif

https://balitsereal-litbang-ppid.pertanian.go.id/assets/foto/33/32822/foto_32822.gif notified by UnM@SK

https://ditjennak-ppid.pertanian.go.id//assets/foto/33/32822/foto_32822.gif

https://ditjennak-ppid.pertanian.go.id//assets/foto/33/32822/foto_32822.gif notified by UnM@SK

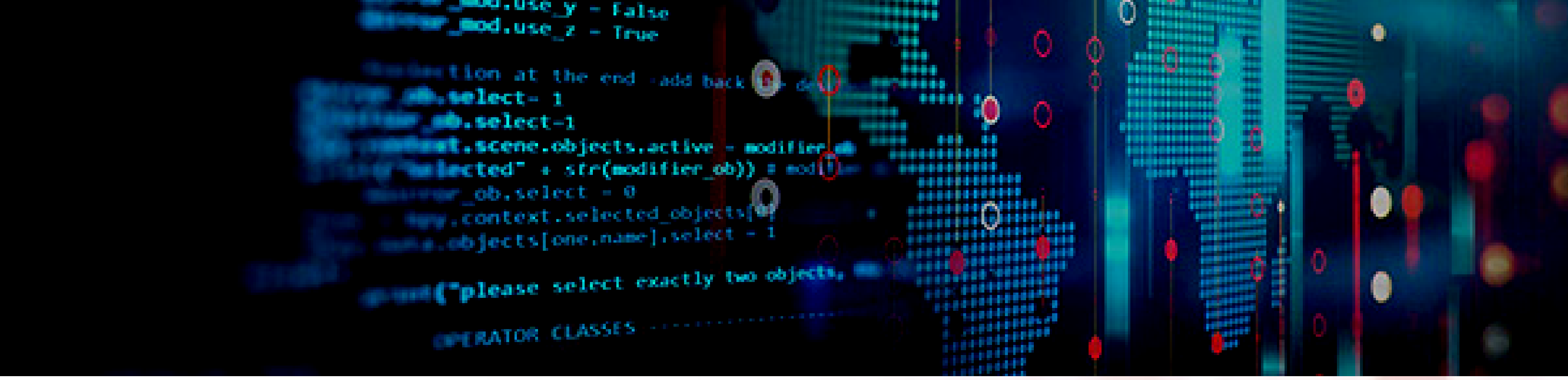


Dark Web News

Darknet Live

Vendor Narco710 Arrested
Russian LockBit Ransomware Operator Arrested in Canada
What is DDOS and How it Affects Darknet Markets
Feds Seize 3.36 Billion Worth of Cryptocurrency Connected to Silk Road

Dark Web Link



Trend Micro Anti-Malware Blog

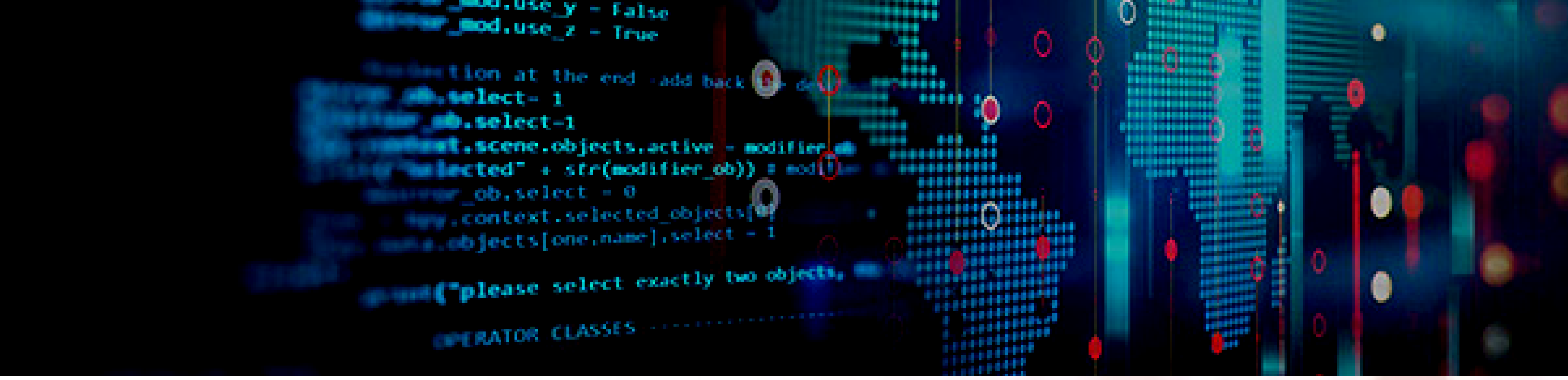
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

* Skimming for Sale: Commodity Skimming and Magecart Trends in Q1 2022
* RiskIQ Threat Intelligence Roundup: Phishing, Botnets, and Hijacked Infrastructure
* RiskIQ Threat Intelligence Roundup: Trickbot, Magecart, and More Fake Sites Targeting Ukraine
* RiskIQ Threat Intelligence Roundup: Campaigns Targeting Ukraine and Global Malware Infrastructure
* RiskIQ Threat Intelligence Supercharges Microsoft Threat Detection and Response
* RiskIQ Intelligence Roundup: Spoofed Sites and Surprising Infrastructure Connections
* RiskIQ Threat Intelligence Roundup: QBot, Magecart, Agent Tesla Headline Hijacked Infrastructure&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

* Metasploit Weekly Wrap-Up
* Aligning to AWS Foundational Security Best Practices With InsightCloudSec
* Search Made Easy: InsightIDR's Secret Weapon for Efficiency and Efficacy
* Metasploit Weekly Wrap-Up
* Better Cloud Security Shouldn't Require Bigger Budgets
* Rapid7 and HashiCorp Partner to Secure Terraform-based Cloud Infrastructure Deployments
* Rapid7 Takes Home 2 Awards and a Highly Commended Recognition at the 2022 Belfast Telegraph IT Awards
* CVE-2022-41622 and CVE-2022-41800 (FIXED): F5 BIG-IP and iControl REST Vulnerabilities and Exposures
* How to Develop a SOAR Workflow to Automate a Critical Daily Task
* CVE-2022-27510: Critical Citrix ADC and Gateway Remote Authentication Bypass Vulnerabilities



Advisories

US-Cert Alerts & bulletins

* CISA Releases Eight Industrial Control Systems Advisories
* CISA, NSA, and ODNI Release Guidance for Customers on Securing the Software Supply Chain
* #StopRansomware: Hive
* CISA Releases Two Industrial Control Systems Advisories
* Cisco Releases Security Updates for Identity Services Engine
* Samba Releases Security Updates
* Mozilla Releases Security Updates&#8239;for Multiple Products
* CISA and FBI Release Advisory on Iranian Government-Sponsored APT Actors Compromising Federal Network
* AA22-321A: #StopRansomware: Hive Ransomware
* AA22-320A: Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, C
* Vulnerability Summary for the Week of November 14, 2022
* Vulnerability Summary for the Week of November 7, 2022

Zero Day Initiative Advisories

ZDI-CAN-19059: ZTE
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 'Rafal Goryl (@voix44er)' was reported to the affected vendor on: 2022-11-24, 4 days ago. The vendor is given until 2023-03-24 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-18899: VIPRE
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 'Dennis Herrmann (@dhn_)' was reported to the affected vendor on: 2022-11-24, 4 days ago. The vendor is given until 2023-03-24 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-19396: VIPRE
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 'Yulin Sung - Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-11-24, 4 days ago. The vendor is given until 2023-03-24 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-19397: VIPRE
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 'Yulin Sung - Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-11-24, 4 days ago. The vendor is given until 2023-03-24 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-19395: VIPRE

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 'Yulin Sung - Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-11-24, 4 days ago. The vendor is given until 2023-03-24 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-19394: VIPRE

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 'Yulin Sung - Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-11-24, 4 days ago. The vendor is given until 2023-03-24 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-19222: 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 'Pap Gergo' was reported to the affected vendor on: 2022-11-23, 5 days ago. The vendor is given until 2023-03-23 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-19463: 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 'Dmitry "InfoSecDJ" Janushkevich of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-11-23, 5 days ago. The vendor is given until 2023-03-23 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-19460: 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 'Dmitry "InfoSecDJ" Janushkevich of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-11-23, 5 days ago. The vendor is given until 2023-03-23 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-19462: 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 'Dmitry "InfoSecDJ" Janushkevich of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-11-23, 5 days ago. The vendor is given until 2023-03-23 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-19348: Apple

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'jzhu' was reported to the affected vendor on: 2022-11-23, 5 days ago. The vendor is given until 2023-03-23 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-19086: Trend Micro

A CVSS score 7.3 (AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Xavier DANEST - Decathlon' was reported to the affected vendor on: 2022-11-23, 5 days ago. The vendor is given until 2023-03-23 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-19461: 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 'Dmitry "InfoSecDJ" Janushkevich of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-11-23, 5 days ago. The vendor is given until 2023-03-23 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-19475: Foxit

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: 2022-11-23, 5 days ago. The vendor is given until 2023-03-23 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-19464: 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 'Dmitry "InfoSecDJ" Janushkevich of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-11-23, 5 days ago. The vendor is given until 2023-03-23 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-19476: Foxit

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: 2022-11-23, 5 days ago. The vendor is given until 2023-03-23 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-19355: NETGEAR

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 'Rocco Calvi and Steven Seeley of Incite Team' was reported to the affected vendor on: 2022-11-23, 5 days ago. The vendor is given until 2023-03-23 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-19477: Foxit

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: 2022-11-23, 5 days ago. The vendor is given until 2023-03-23 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-19478: Foxit

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: 2022-11-23, 5 days ago. The vendor is given until 2023-03-23 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-19500: Microsoft

A CVSS score 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Guy Lederfein of Trend Micro Security Research' was reported to the affected vendor on: 2022-11-23, 5 days ago. The vendor is given until 2023-03-23 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-19483: PDF-XChange

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 'Suyue Guo and Wei You from Renmin University of China' was reported to the affected vendor on: 2022-11-23, 5 days ago. The vendor is given until 2023-03-23 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-19469: 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: 2022-11-23, 5 days ago. The vendor is given until 2023-03-23 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-19227: Autodesk

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 'Filip Dragovi\xc4\x87' was reported to the affected vendor on: 2022-11-23, 5 days ago. The vendor is given until 2023-03-23 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-19342: Delta Electronics

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 'Natnael Samson (@NattiSamson)' was reported to the affected vendor on: 2022-11-21, 7 days ago. The vendor is given until 2023-03-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Red Hat Security Advisory 2022-8639-01

Red Hat Security Advisory 2022-8639-01 - Kerberos is a network authentication system, which can improve the security of your network by eliminating the insecure practice of sending passwords over the network in unencrypted form. It allows clients and servers to authenticate to each other with the help of a trusted third party, the Kerberos key distribution center. Issues addressed include an integer overflow vulnerability.

Red Hat Security Advisory 2022-8638-01

Red Hat Security Advisory 2022-8638-01 - Kerberos is a network authentication system, which can improve the security of your network by eliminating the insecure practice of sending passwords over the network in unencrypted form. It allows clients and servers to authenticate to each other with the help of a trusted third party, the Kerberos key distribution center. Issues addressed include an integer overflow vulnerability.

Red Hat Security Advisory 2022-8643-01

Red Hat Security Advisory 2022-8643-01 - Varnish Cache is a high-performance HTTP accelerator. It stores web pages in memory so web servers don't have to create the same web page over and over again, giving the website a significant speed up.

Red Hat Security Advisory 2022-8646-01

Red Hat Security Advisory 2022-8646-01 - Varnish Cache is a high-performance HTTP accelerator. It stores web pages in memory so web servers don't have to create the same web page over and over again, giving the website a significant speed up.

Red Hat Security Advisory 2022-8649-01

Red Hat Security Advisory 2022-8649-01 - Varnish Cache is a high-performance HTTP accelerator. It stores web pages in memory so web servers don't have to create the same web page over and over again, giving the website a significant speed up.

Red Hat Security Advisory 2022-8640-01

Red Hat Security Advisory 2022-8640-01 - Kerberos is a network authentication system, which can improve the security of your network by eliminating the insecure practice of sending passwords over the network in unencrypted form. It allows clients and servers to authenticate to each other with the help of a trusted third party, the Kerberos key distribution center. Issues addressed include an integer overflow vulnerability.

Red Hat Security Advisory 2022-8648-01

Red Hat Security Advisory 2022-8648-01 - Kerberos is a network authentication system, which can improve the security of your network by eliminating the insecure practice of sending passwords over the network in unencrypted form. It allows clients and servers to authenticate to each other with the help of a trusted third party, the Kerberos key distribution center. Issues addressed include an integer overflow vulnerability.

Red Hat Security Advisory 2022-8650-01

Red Hat Security Advisory 2022-8650-01 - Varnish Cache is a high-performance HTTP accelerator. It stores web pages in memory so web servers don't have to create the same web page over and over again, giving the website a significant speed up.

Red Hat Security Advisory 2022-8644-01

Red Hat Security Advisory 2022-8644-01 - Varnish Cache is a high-performance HTTP accelerator. It stores web pages in memory so web servers don't have to create the same web page over and over again, giving the website a significant speed up.

Debian Security Advisory 5290-1

Debian Linux Security Advisory 5290-1 - Apache Commons Configuration, a Java library providing a generic configuration interface, performs variable interpolation, allowing properties to be dynamically evaluated and expanded. Starting with version 2.4 and continuing through 2.7, the set of default Lookup instances included interpolators that could result in arbitrary code execution or contact with remote servers.

Ubuntu Security Notice USN-5744-1

Ubuntu Security Notice 5744-1 - It was discovered that libICE was using a weak mechanism to generate the session cookies. A local attacker could possibly use this issue to perform a privilege escalation attack.

Red Hat Security Advisory 2022-8634-01

Red Hat Security Advisory 2022-8634-01 - OpenShift API for Data Protection enables you to back up and restore application resources, persistent volume data, and internal container images to external backup storage. OADP enables both file system-based and snapshot-based backups for persistent volumes.

Debian Security Advisory 5289-1

Debian Linux Security Advisory 5289-1 - Multiple security issues were discovered in Chromium, which could result in the execution of arbitrary code.

Debian Security Advisory 5288-1

Debian Linux Security Advisory 5288-1 - It was discovered that a buffer overflow in GraphicsMagick, a collection of image processing tools, could potentially result in the execution of arbitrary code when processing a malformed MIFF image.

Red Hat Security Advisory 2022-8647-01

Red Hat Security Advisory 2022-8647-01 - Varnish Cache is a high-performance HTTP accelerator. It stores web pages in memory so web servers don't have to create the same web page over and over again, giving the website a significant speed up.

Red Hat Security Advisory 2022-8645-01

Red Hat Security Advisory 2022-8645-01 - Varnish Cache is a high-performance HTTP accelerator. It stores web pages in memory so web servers don't have to create the same web page over and over again, giving the website a significant speed up.

Red Hat Security Advisory 2022-8641-01

Red Hat Security Advisory 2022-8641-01 - Kerberos is a network authentication system, which can improve the security of your network by eliminating the insecure practice of sending passwords over the network in unencrypted form. It allows clients and servers to authenticate to each other with the help of a trusted third party, the Kerberos key distribution center. Issues addressed include an integer overflow vulnerability.

Red Hat Security Advisory 2022-8637-01

Red Hat Security Advisory 2022-8637-01 - Kerberos is a network authentication system, which can improve the security of your network by eliminating the insecure practice of sending passwords over the network in unencrypted form. It allows clients and servers to authenticate to each other with the help of a trusted third party, the Kerberos key distribution center. Issues addressed include an integer overflow vulnerability.

Ubuntu Security Notice USN-5743-1

Ubuntu Security Notice 5743-1 - 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-5742-1

Ubuntu Security Notice 5742-1 - It was discovered that JBIG-KIT incorrectly handled decoding certain large image files. If a user or automated system using JBIG-KIT were tricked into opening a specially crafted file, an attacker could possibly use this issue to cause a denial of service.

Ubuntu Security Notice USN-5741-1

Ubuntu Security Notice 5741-1 - It was discovered that Exim incorrectly handled certain regular expressions. An attacker could use this issue to cause Exim to crash, resulting in a denial of service, or possibly execute arbitrary code.

Ubuntu Security Notice USN-5736-1

Ubuntu Security Notice 5736-1 - It was discovered that ImageMagick incorrectly handled certain values when processing PDF files. If a user or automated system using ImageMagick were tricked into opening a specially crafted PDF file, an attacker could exploit this to cause a denial of service. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 ESM and Ubuntu 18.04 LTS. Zhang Xiaohui discovered that ImageMagick incorrectly handled certain values when processing image data. If a user or automated system using ImageMagick were tricked into opening a specially crafted image, an attacker could exploit this to cause a denial of service. This issue only affected Ubuntu 18.04 LTS and Ubuntu 22.10.

Red Hat Security Advisory 2022-8535-01

Red Hat Security Advisory 2022-8535-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the container images for Red Hat OpenShift Container Platform 4.11.16. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-8534-01

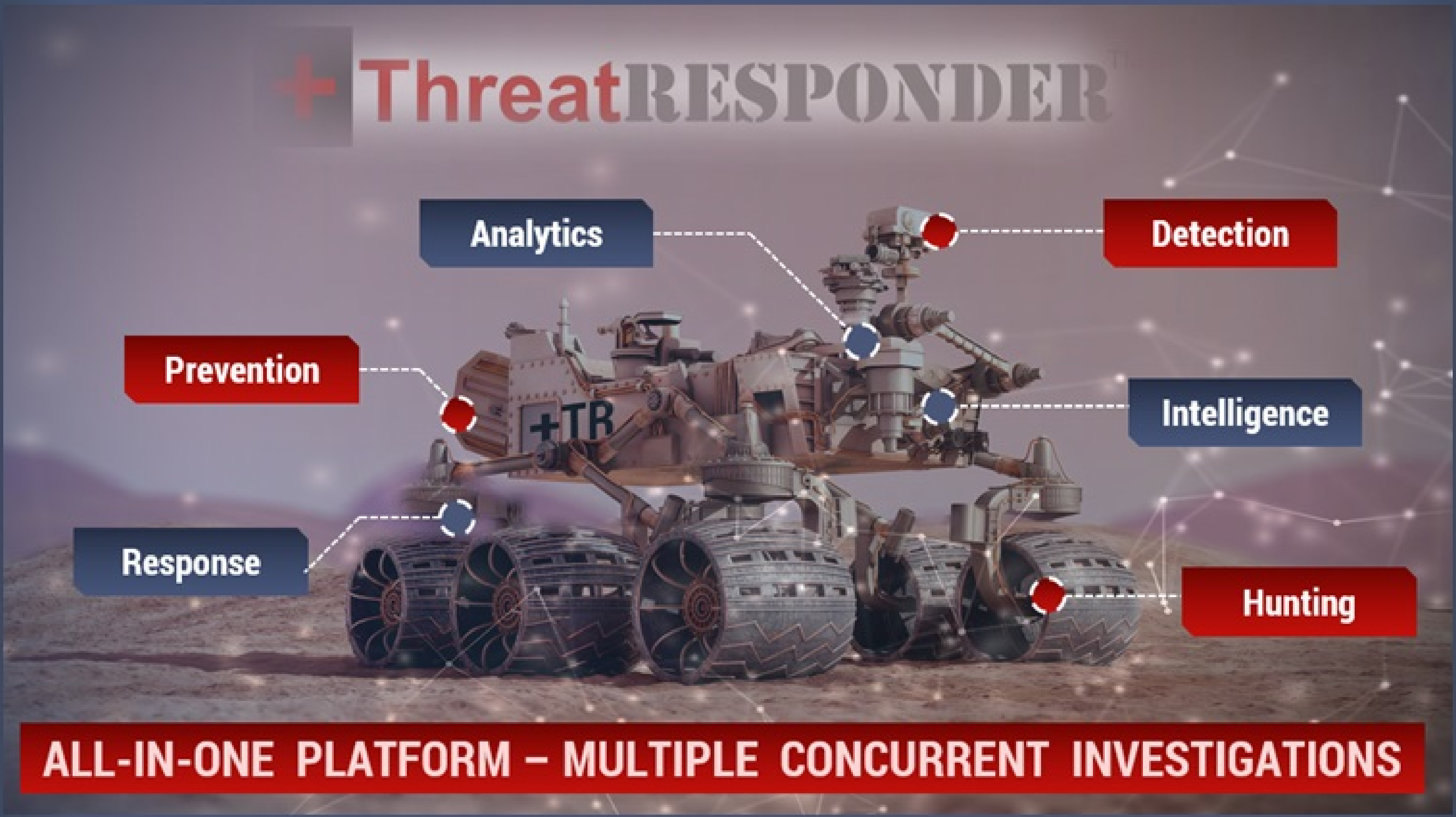
Red Hat Security Advisory 2022-8534-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.11.16. Issues addressed include a denial of service vulnerability.

Are You…

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

Do DFIR Investigations Better

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



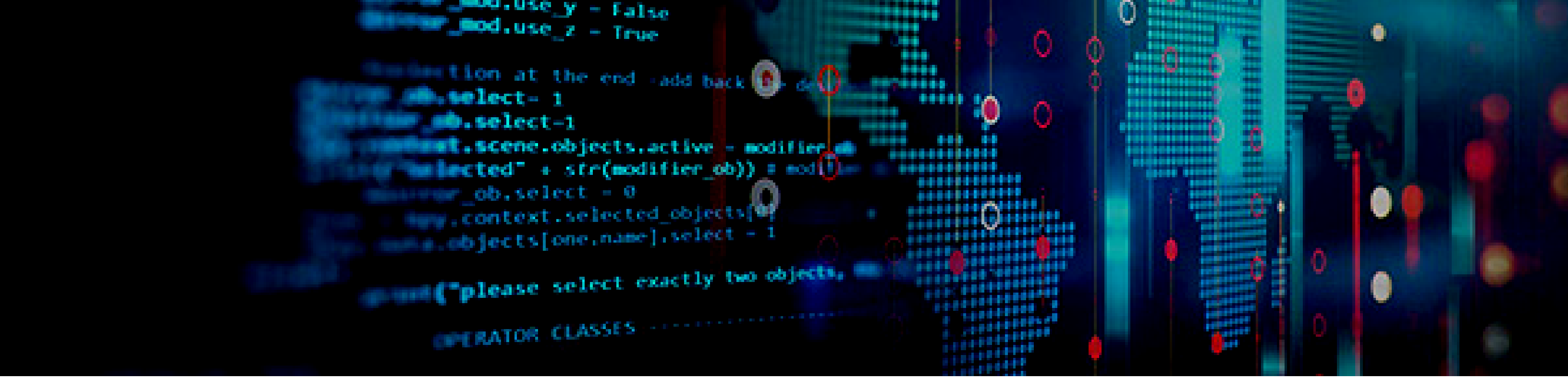
The Solution – ThreatResponder® Platform

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

Get a Trial Copy

Mention **CODE: CIR-0119**

https://netsecurity.com

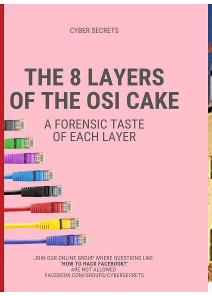


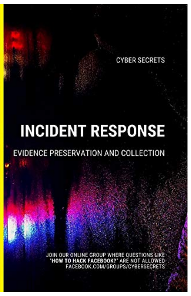
The Cyber Secrets publications on Amazon

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

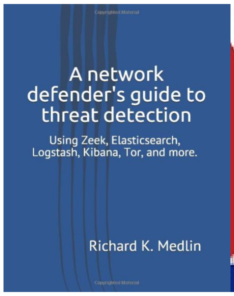
Items that focus on cyber defense and DFIR usually spotlight capabilities in the CSI Linux environment. If interested in helping evolve, please let us know. The Cyber Secrets publications rotates between odd quarters issues focusing on Blue Team and the even issues on Red Team.

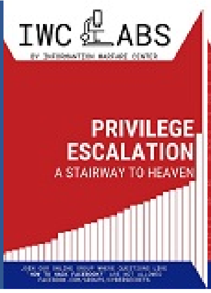
CYBER Secrets
Information Warfare Center
What's Inside?
Visit our YouTube Channel
Threat Intelligence & Training

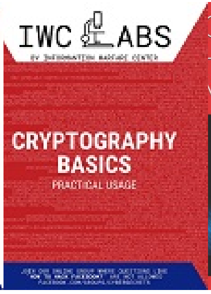


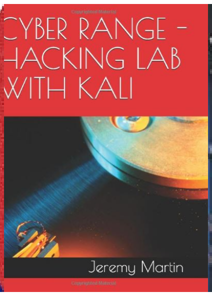


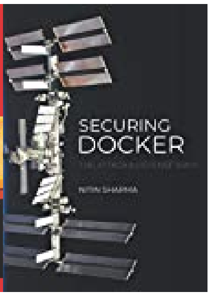
Other Publications from Information Warfare Center











CYBER WEEKLY AWARENESS REPORT

VISIT US AT **INFORMATIONWARFARECENTER.COM**

THE IWC ACADEMY
ACADEMY.INFORMATIONWARFARECENTER.COM

FACEBOOK GROUP
FACEBOOK.COM/GROUPS/CYBERSECRETS

CSI LINUX
CSILINUX.COM

CYBERSECURITY TV
CYBERSEC.TV

ARGOS APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity®

ThreatRESPONDER

Accredited Training Center EC-Council

CYBERQ GROUP