Apr-11-22

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

April 11, 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

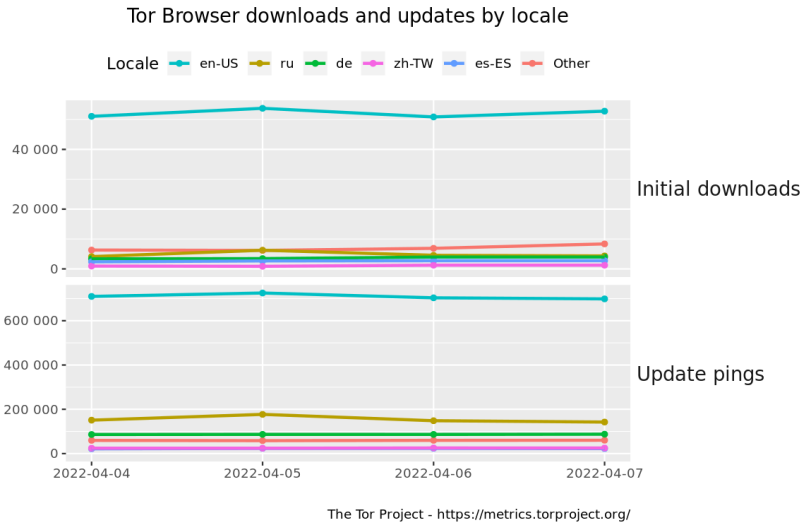
Internet Storm Center Infocon Status

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

Other IWC Publications

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

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



Interesting News

* Free Cyberforensics Training - CSI Linux Basics

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

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

Index of Sections

Packet Storm Security

* China Uses AI Software To Improve Its Surveillance Capabilities
* FIN7 Hacking Group Member Sentenced To Five Years Behind Bars
* Play-To-Earn Game Token Collapses After Hacker Cashes Out
* Facebook Says Ukraine Military Accounts Were Hacked To Post Calls To Surrender
* China Accused Of Cyber Attacks On Indian Power Grid
* US Government Disrupts Botnet Controlled By Russian Government Hackers
* Fintech SSRF Flaw Allowed For Compromise Of Bank Accounts
* Amazon Secures Rockets For Broadband Project
* Critical Remote Code Execution Bug In Workspace ONE Access
* WatchGuard Failed To Explicitly Disclose Critical Flaw Exploited By Russian Hackers
* This New Malware Targets AWS Lambda Environments
* Block Claims Ex-Employee Downloaded Customer Data After Leaving
* Authorities Fully Behead Hydra Dark Marketplace
* Identify Fraud Skyrockets As Hackers Stick To Pre-Pandemic Techniques
* Mandiant Shareholder Sues To Block $5.4B Google Deal
* Hackers Hijacked Crypto Wallets With Stolen MailChimp Data
* Zyxel Patches Critical Hijacking Vulnerability
* FIN7 Hackers Evolve Operations With Ransomware, Novel Backdoor
* GitHub Advanced Security Now Scans For Secrets With Each Push
* A Hacker Gang's Members Are In Jail. It's Still Stealing Data.
* Emma Sleep Company Admits Checkout Cyber Attack
* Borat RAT Malware: A Unique Triple Threat That Is Far From Funny
* China Accused Of Cyber Attacks On Ukraine Before Russian Invasion
* Ukraine Accuses Russia Of Using WhatsApp Bot Farm To Ask Military To Surrender
* Ubiquiti Sues Brian Krebs Alleging Defamation

Krebs on Security

* Actions Target Russian Govt. Botnet, Hydra Dark Market
* The Original APT: Advanced Persistent Teenagers
* Fake Emergency Search Warrants Draw Scrutiny from Capitol Hill
* Hackers Gaining Power of Subpoena Via Fake "Emergency Data Requests"
* Estonian Tied to 13 Ransomware Attacks Gets 66 Months in Prison
* A Closer Look at the LAPSUS$ Data Extortion Group
* 'Spam Nation' Villain Vrublevsky Charged With Fraud
* Pro-Ukraine 'Protestware' Pushes Antiwar Ads, Geo-Targeted Malware
* Lawmakers Probe Early Release of Top RU Cybercrook
* Report: Recent 10x Increase in Cyberattacks on Ukraine

Dark Reading

* Google Removes Dangerous Banking Malware From Play Store
* Microsoft Sinkholes Russian Hacking Group's Domains Targeting Ukraine
* BakerHostetler Launches 2022 Data Security Incident Response Report - Resilience And Perseverance
* Software-as-a-Service Rules the Cloud
* ByteChek Founder AJ Yawn Brings Discipline to Everything He Does
* Security Nihilism Is Putting Your Company - and Its Employees - at Risk
* Mandiant to Use CrowdStrike Technology in Its Incident Response Services
* SeeMetrics to Help CISOs Measure Security Success
* BlackCat Purveyor Shows Ransomware Operators Have 9 Lives
* Ukrainian Member of Notorious FIN7 Cybercrime Group Sentenced
* Scan This: There's Danger in QR Codes
* Top Application Security Mitigations in Q1 of 2022
* Nord Security Raises First Outside Capital at $1.6B Valuation
* Keysight Delivers Zero Trust Test Solution
* Blumira Unveils Cloud SIEM With Integrated Detection and Response for SMBs
* The Blurring Line, and Growing Risk, Between Physical and Digital Supply Chains
* BeyondTrust Announces CEO Transition
* Nearly Two-Thirds of Ransomware Victims Paid Ransoms Last Year, Finds "2022 Cyberthreat Defense Repor
* Zoom's Bug Bounty Programs Soar to $1.8M
* Nearly 40% of Macs Left Exposed to 2 Zero-Day Exploits

The Hacker News

* Researchers warn of FFDroider and Lightning info-stealers targeting users in the wild
* Microsoft's New Autopatch Feature to Help Businesses Keep Their Systems Up-to-Date
* Hackers Exploiting Spring4Shell Vulnerability to Deploy Mirai Botnet Malware
* Chinese Hacker Groups Continue to Target Indian Power Grid Assets
* Researchers Connect BlackCat Ransomware with Past BlackMatter Malware Activity
* Ukrainian FIN7 Hacker Gets 5-Year Sentence in the United States
* Microsoft Obtains Court Order to Take Down Domains Used to Target Ukraine
* New Octo Banking Trojan Spreading via Fake Apps on Google Play Store
* First Malware Targeting AWS Lambda Serverless Platform Discovered
* Hamas-linked Hackers Targeting High-Ranking Israelis Using 'Catfish' Lures
* Into the Breach: Breaking Down 3 SaaS App Cyber Attacks in 2022
* SharkBot Banking Trojan Resurfaces On Google Play Store Hidden Behind 7 New Apps
* Researchers Uncover How Colibri Malware Stays Persistent on Hacked Systems
* FBI Shut Down Russia-linked "Cyclops Blink" Botnet That Infected Thousands of Devices
* VMware Releases Critical Patches for New Vulnerabilities Affecting Multiple Products

Security Week

* High-End Tools Manufacturer Snap-on Discloses Data Breach
* Accounts Deceivable: Email Scam Costliest Type of Cybercrime
* Third Member of FIN7 Cybercrime Gang Sentenced to US Prison
* Spring4Shell Vulnerability Exploited by Mirai Botnet
* Blockchain Security Firm CertiK Raises $88 Million at $2 Billion Valuation
* Microsoft Disrupts Infrastructure Used by Russia's Hackers in Ukraine Attacks
* Google Updates Target API Level Requirements for Android Apps
* Windows Autopatch Aims to Make Patch Tuesday 'Just Another Tuesday' for Enterprises
* SharkBot Android Malware Continues Popping Up on Google Play
* Facebook Battles Cyber Campaigns Targeting Ukraine
* Healthcare and the Other CIA
* Nudge Security Bags $7M Seed Round
* Google Teams Up With GitHub for Supply Chain Security
* VPN Provider Nord Security Reaches Unicorn Status With $100 Million Funding
* India Claims It Foiled Chinese Cyberattack on Disputed Border
* BlackCat Ransomware Targets Industrial Companies
* Zoom Paid Out $1.8 Million in Bug Bounties in 2021
* VMware Patches Five Critical Vulnerabilities in Workspace ONE Access
* Microsoft Adds On-Premises Exchange, SharePoint, Skype to Bug Bounty Program
* Hamas-Linked Hackers Using Sexy 'Catfish' Lures, New Malware
* FBI Disables "Cyclops Blink" Botnet Controlled by Russian Intelligence Agency
* US Charges Russian Oligarch, Dismantles Cybercrime Operation
* Apple Leaves Big Sur, Catalina Exposed to Critical Flaws: Intego
* Denonia: First Malware Targeting AWS Lambda
* Tufin Agrees to $570 Million Acquisition With 30-Day 'Go Shop' Option
* Google Doubles Rewards for Nest and Fitbit Vulnerabilities

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* KnowBe4's PhishER Platform Named a Leader in the Spring 2022 G2 Grid Report for Security Orchestratio
* The Ransomware Hostage Rescue Checklist: Your Step-by-Step Guide to Preventing and Surviving an Ranso
* Phishbait Invokes Russia's Ministry of Internal Affairs (Road Safety Division)
* "Human Error" Ranked as the Top Cybersecurity Threat While Budgets Remain Misaligned
* Multi-Million Dollar Scam Call Center Shut Down by Multinational Police Efforts
* Mailchimp Phishing Attack Results in Potential Hit on 100K Trezor Crypto Wallets
* "Europol Calling" (Not Necessarily)
* Microsoft Warns of Lapsus$ "Targeting Organizations for Data Exfiltration and Destruction"
* Info Stealer Malware Vidar Uses Microsoft Help Files to Launch Attacks
* Ransomware Victims See Ransom Demands and Payments Increase as The Number of Published Data Victims S

ISC2.org Blog

* What Do You Mean My Email Isn't Free?
* What is Neurodiversity? Understanding Neurodiversity and its Prominence in Cybersecurity
* Associate of (ISC)² Spotlight: Angel Sayani
* WINNING TACTICS FOR SECURITY AWARENESS INNOVATIONS via EXPERIENCE (1 of 2)
* Summary of March Inside (ISC)2 Webinar: Stay Vigilant

HackRead

* FBI Disrupts Cyclops Blink Botnet Used by Russian Intelligence Directorate
* Hamas Hackers Posing as Women to Con Snr Israeli Officials into Installing Malware
* Factors to Consider when Choosing a Robotic Arm
* Brand Protection is Essential for Cybersecurity
* 5 Common Database Management Challenges & How to Solve Them
* Anonymous Affiliate NB65 Breach State-Run Russian Broadcaster; Leak 786GB of Data
* Germany Shuts Down Russian Dark Web Market Hydra; Seizes $25M in BTC

Koddos

* FBI Disrupts Cyclops Blink Botnet Used by Russian Intelligence Directorate
* Hamas Hackers Posing as Women to Con Snr Israeli Officials into Installing Malware
* Factors to Consider when Choosing a Robotic Arm
* Brand Protection is Essential for Cybersecurity
* 5 Common Database Management Challenges & How to Solve Them
* Anonymous Affiliate NB65 Breach State-Run Russian Broadcaster; Leak 786GB of Data
* Germany Shuts Down Russian Dark Web Market Hydra; Seizes $25M in BTC

Naked Security

* Popular Ruby Asciidoc toolkit patched against critical vuln - get the update now!
* S3 Ep77: Bugs, busts and old-school PDP-11 hacking [Podcast]
* Serious Security: Darkweb drugs market Hydra taken offline by German police
* Firefox 99 is out - no major bugs, but update anyway!
* Google's monthly Android updates patch numerous "get root" holes
* LAPSUS$ hacks continue despite two hacker suspects in court
* Apple pushes out two emergency 0-day updates - get 'em now!
* Two different "VMware Spring" bugs at large - we cut through the confusion
* S3 Ep76: Deadbolt, LAPSUS$, Zlib, and a Chrome 0-day [Podcast]
* "VMware Spring Cloud Function" Java bug gives instant remote code execution - update now!

Threat Post

* Google Play Bitten by Sharkbot Info-stealer 'AV Solution'
* SSRF Flaw in Fintech Platform Allowed for Compromise of Bank Accounts
* MacOS Malware: Myth vs. Truth - Podcast
* Attackers Spoof WhatsApp Voice-Message Alerts to Steal Info
* Authorities Fully Behead Hydra Dark Marketplace
* No-Joke Borat RAT Propagates Ransomware, DDoS
* Apple Rushes Out Patches for 0-Days in MacOS, iOS
* Belarusian 'Ghostwriter' Actor Picks Up BitB for Ukraine-Related Attacks
* Automaker Cybersecurity Lagging Behind Tech Adoption, Experts Warn
* QNAP Customers Adrift, Waiting on Fix for OpenSSL Bug

Null-Byte

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

IBM Security Intelligence

Unfortunately, at the time of this report, the IBM Security Intelligence Blog resource was not availible.

InfoWorld

* InfoWorld's 2022 Technology of the Year Award winners
* So you want to change cloud providers
* Use of consumption apps in the enterprise
* Redwood web framework hits 1.0 release milestone
* GitHub enhances secret scanning for tighter code security
* A closer look at traditional solutions and cloud
* A brief history of the agile methodology
* What's new in Rust 1.60
* Databricks targets data pipeline automation with Delta Live Tables
* Software testing: Automating installations and functional tests

C4ISRNET - Media for the Intelligence Age Military

* SPACECOM requests more funding for key space domain awareness center
* Cyber Mission Force could continue growing, says commander
* US Space Force to test experimental navigation satellite in upcoming Army exercise
* US Cyber Command reinforces Ukraine and allies amid Russian onslaught
* US Space Force wants funding for two more MUOS satellites
* Navy working with services on data, but Project Overmatch details remain scarce
* Intelligence agencies accelerate use of commercial space imagery to support Ukraine
* Pentagon launches 5G challenge with millions up for grabs
* ULA expects Amazon deal to drive down Space Force's Vulcan launch costs
* The US Navy had cybersecurity wrong. Expect change.

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

* CVE-2021-30737, @xerub's 2021 iOS ASN.1 Vulnerability
* FORCEDENTRY: Sandbox Escape

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.

* DCTF 2022
* CrewCTF 2022
* TAMUctf 2022
* *CTF 2022
* WPICTF 2022
* b01lers CTF
* MidnightFlag - INFEKTION 2022
* RuCTF 2022
* PatriotCTF
* Digital Overdose Conference 2022 CTF

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

* Web Machine: (N7)
* The Planets: Earth
* Jangow: 1.0.1
* Red: 1
* Napping: 1.0.1

Tools & Techniques

Packet Storm Security Tools Links

* OpenSSH 9.0p1
* Wireshark Analyzer 3.6.3
* Adversary3 1.0
* nfstream 6.4.3
* OpenSSL Toolkit 3.0.2
* OpenSSL Toolkit 1.1.1n
* Falco 0.31.1
* UFONet 1.8
* Samhain File Integrity Checker 4.4.7
* GRAudit Grep Auditing Tool 3.4

Kali Linux Tutorials

* PyShell : Multiplatform Python WebShell
* Authz0 : An Automated Authorization Test Tool
* Hacc The Hub : Open Source Self-Hosted Cyber Security Learning Platform
* IOC Scraper : A Fast And Reliable Service That Enables You To Extract IOCs
* Chaya : Advance Image Steganography
* Ocr-Recon : Tool To Find A Particular String In A List Of URLs Using Tesseract'S OCR Capabilities
* Litefuzz : A Multi-Platform Fuzzer For Poking At Userland Binaries And Servers
* Searpy : Search Engine Toolkit
* CAPEv2 : Malware Configuration And Payload Extraction
* BruteShark : Network Analysis Tool

GBHackers Analysis

* 15-Year-old Security Vulnerability In The PEAR PHP Repository Permits Supply Chain Attack
* Honda Bug Let Attackers Unlock and Start the Car
* Hundreds of HP Printer Models Affected by Critical Remote Code Execution
* CISA Has Added 15 New Flaws to the List of Actively Exploited Vulnerabilities
* FBI Warns that Hackers Gain Network Access by Exploiting MFA and "PrintNightmare" Vulnerability

Weekly Cyber Security Video and Podcasts

SANS DFIR

* CTI Summit Wrap Up Panel
* Integrated Intelligence
* Lone Wolf Actors: How Ransomware Evolved into Freelance Work
* 10 años de inteligencia sobre ciberamenazas: De Berkeley Lab y IEEE/ACM Supercomputing a Google

Defcon Conference

* DEF CON 29 Ham Radio Village - Kurtis Kopf - An Introduction to RF Test Equipment
* DEF CON 29 Ham Radio Village - Tyler Gardner - Amateur Radio Mesh Networking
* DEF CON 29 Ham Radio Village - Bryan Fields - Spectrum Coordination for Amateur Radio
* DEF CON 29 Ham Radio Village - Eric Escobar - Getting started with low power/long distance Comms

Hak5

* Wyze Cameras Have A Three Year Old Flaw - ThreatWire
* Live Hacking Q&A with Kody Kinzie: Deleting Your Online Footprint, Kody's Eureka Moment, and More!
* NEW ZERO DAY: Are you ready for POP_CALC?

The PC Security Channel [TPSC]

* Bitdefender Free Antivirus (New) Tested
* Is Kaspersky safe to use?

Eli the Computer Guy

* Apple AIRTAG STALKING
* Muslim Apps HACKED by US DEFENSE CONTRACTOR
* RUSSIA HACKS UK SPECIAL FORCES PHONES to TARGET SOLDIERS in UKRAINE
* Russian Food App HACKED - YANDEX Leaks MILITARY and INTELLIGENCE info

Security Now

* Port Knocking - Wyze Gets Spanked, FinFisher Bites the Dust, Spring4Shell, LAPSUS$ Update
* Targeted Exploitation - Ukrainian ISP Challenges, Kaspersky Labs Banned in the US, Chrome 0-Day

Troy Hunt

* Weekly Update 290

Intel Techniques: The Privacy, Security, & OSINT Show

* 256-Extreme Privacy Fatigue

* 255-Dedicated VPN IP Addresses

Proof of Concept (PoC) & Exploits

Packet Storm Security

* AeroCMS 0.0.1 Shell Upload
* Movie Seat Reservation System 1.0 File Disclosure / SQL Injection
* Car Rental System 1.0 SQL Injection
* Simple House Rental System 1 Shell Upload
* Social Codia SMS 1 Shell Upload
* E-Commerce Website 1.1.0 Shell Upload
* Musical World 1 Shell Upload
* E-Commerce Website 1.0 Shell Upload
* PHPGurukul Zoo Management System 1.0 Shell Upload
* Social Codia SMS 1 Cross Site Scripting
* AeroCMS 0.0.1 Cross Site Scripting
* PHPGurukul Zoo Management System 1.0 SQL Injection
* Reprise License Manager 14.2 Cross Site Scripting / Information Disclosure
* WordPress SiteGround Security 1.2.5 Authentication Bypass
* Online Sports Complex Booking System 1.0 Cross Site Scripting
* School Club Application System 1.0 Local File Inclusion
* Backdoor.Win32.XLog.21 Authentication Bypass / Race Condition
* Backdoor.Win32.Verify.h Remote Command Execution
* KLiK Social Media Website 1.0 SQL Injection
* WordPress WP Downgrade Cross Site Scripting
* WordPress UpdraftPlus Cross Site Scripting
* qdPM 9.2 Cross Site Request Forgery
* minewebcms 1.15.2 Cross Site Scripting
* WordPress Hummingbird Cross Site Scripting
* ICEHRM 31.0.0.0S Cross Site Request Forgery

CXSecurity

* Small HTTP Server 3.06 Remote Buffer Overflow
* Zenario CMS 9.0.54156 Remote Code Execution
* ALLMediaServer 1.6 Buffer Overflow
* Atom CMS 1.0.2 Shell Upload
* PostgreSQL 11.7 Remote Code Execution
* Trend Micro Virtual Mobile Infrastructure 6.0.1278 Denial Of Service
* Xlight FTP 3.9.3.2 Buffer Overflow

Proof of Concept (PoC) & Exploits

Exploit Database

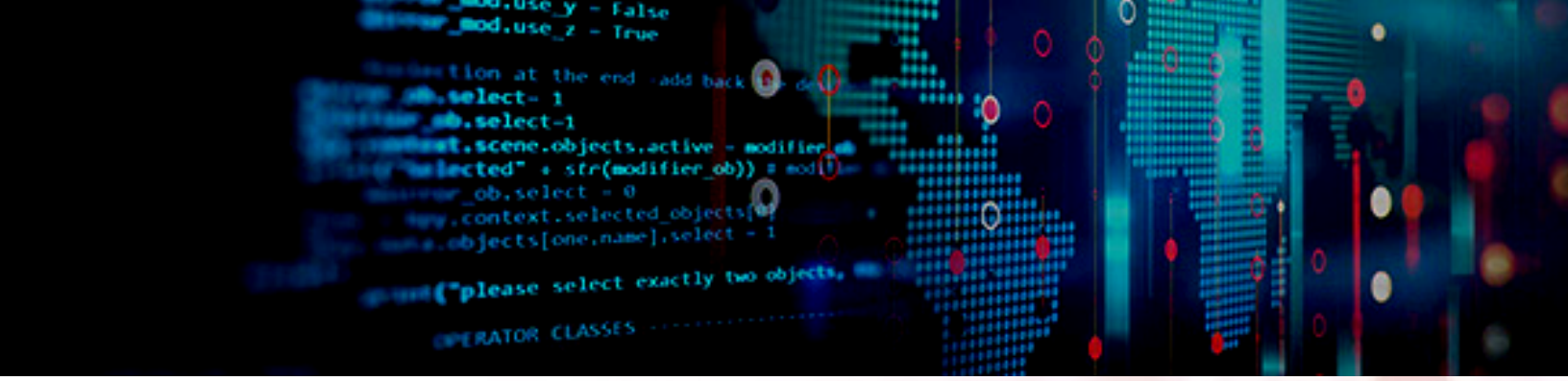
* [webapps] Razer Sila - Command Injection
* [webapps] Razer Sila - Local File Inclusion (LFI)
* [webapps] Telesquare TLR-2855KS6 - Arbitrary File Deletion
* [webapps] Telesquare TLR-2855KS6 - Arbitrary File Creation
* [remote] Franklin Fueling Systems Colibri Controller Module 1.8.19.8580 - Local File Inclusion (LFI)
* [webapps] SAM SUNNY TRIPOWER 5.0 - Insecure Direct Object Reference (IDOR)
* [local] MiniTool Partition Wizard - Unquoted Service Path
* [local] binutils 2.37 - Objdump Segmentation Fault
* [remote] Opmon 9.11 - Cross-site Scripting
* [remote] Kramer VIAware - Remote Code Execution (RCE) (Root)
* [webapps] ICEHRM 31.0.0.0S - Cross-site Request Forgery (CSRF) to Account Deletion
* [webapps] qdPM 9.2 - Cross-site Request Forgery (CSRF)
* [webapps] minewebcms 1.15.2 - Cross-site Scripting (XSS)
* [local] Sherpa Connector Service v2020.2.20328.2050 - Unquoted Service Path
* [webapps] KLiK Social Media Website 1.0 - 'Multiple' SQLi
* [webapps] Zenario CMS 9.0.54156 - Remote Code Execution (RCE) (Authenticated)
* [webapps] WordPress Plugin Easy Cookie Policy 1.6.2 - Broken Access Control to Stored XSS
* [remote] Kramer VIAware 2.5.0719.1034 - Remote Code Execution (RCE)
* [remote] PostgreSQL 9.3-11.7 - Remote Code Execution (RCE) (Authenticated)
* [webapps] CSZ CMS 1.2.9 - 'Multiple' Blind SQLi(Authenticated)
* [webapps] WordPress Plugin admin-word-count-column 2.2 - Local File Read
* [webapps] WordPress Plugin video-synchro-pdf 1.7.4 - Local File Inclusion
* [webapps] WordPress Plugin cab-fare-calculator 1.0.3 - Local File Inclusion
* [webapps] WordPress Plugin Curtain 1.0.2 - Cross-site Request Forgery (CSRF)
* [webapps] Drupal avatar_uploader v7.x-1.0-beta8 - 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*

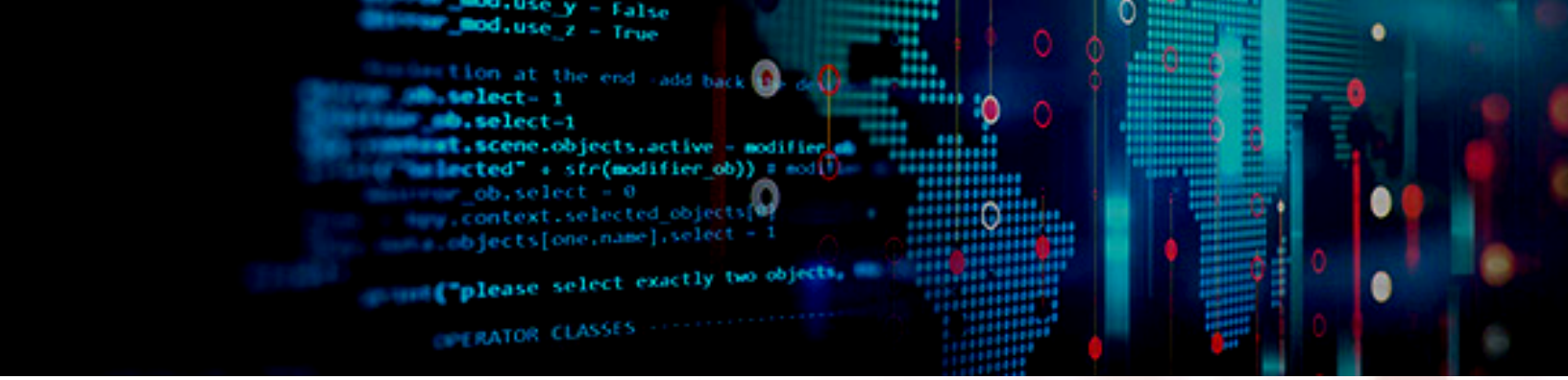
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://www.passaportequalificaq.gov.pt/index.html
https://www.passaportequalificaq.gov.pt/index.html notified by dock0d1
http://www.nrccrsp.gov.bd
http://www.nrccrsp.gov.bd notified by AnonCoders
https://www.declarations.gov.mw/kz.html
https://www.declarations.gov.mw/kz.html notified by Mr.Kro0oz.305
https://modul.pusdiklat.bmkg.go.id/readme.html
https://modul.pusdiklat.bmkg.go.id/readme.html notified by AnonSec Team
http://panmas.depok.go.id
http://panmas.depok.go.id notified by Mr.Kro0oz.305
http://mwe.go.ug/ko.html
http://mwe.go.ug/ko.html notified by Mr.Kro0oz.305
http://taqeem.gov.sa/hi.txt
http://taqeem.gov.sa/hi.txt notified by Mr.Kro0oz.305
http://pejsib.gob.pe/vz.txt
http://pejsib.gob.pe/vz.txt notified by aDriv4
https://munichallabamba.gob.pe/kz.html
https://munichallabamba.gob.pe/kz.html notified by Mr.Kro0oz.305
http://www.catriel.gob.ar
http://www.catriel.gob.ar notified by Mr.Kro0oz.305
http://ms4.sbcounty.gov/security.txt
http://ms4.sbcounty.gov/security.txt notified by Elliot
https://epay.pkns.gov.my
https://epay.pkns.gov.my notified by ./meicookies
https://etender.pkns.gov.my
https://etender.pkns.gov.my notified by ./meicookies
https://matomo.pkns.gov.my
https://matomo.pkns.gov.my notified by ./meicookies
https://maklumbalas.pkns.gov.my
https://maklumbalas.pkns.gov.my notified by ./meicookies
https://careline.pkns.gov.my
https://careline.pkns.gov.my notified by ./meicookies
https://aduan.pkns.gov.my
https://aduan.pkns.gov.my notified by ./meicookies



Dark Web News

Darknet Live

Romania: Five Arrested for Running Murder-for-Hire Scams

Romanian law enforcement arrested the alleged operators of fraudulent murder-for-hire sites. Police in Romania arrested five people for inciting murder, money laundering, and organized crime charges. According to a press release from the Directorate for Investigating Organized Crime and Terrorism (DIICOT), the suspects operated fake hitman sites on the darkweb. Romanian police arrested five suspects at request of authorities in the US. Police with the DCCO - the Service for Combating Cybercrime searched seven houses in Gorj and Hunedoara and arrested five alleged operators of the fake murder-for-hire sites. Investigators seized 18 mobile phones, ten laptops, 15 memory sticks, seven bank cards, 13 HDDs, an electronic wallet, a DVR, and various documents during the searches. The arrests were conducted at the request of United States law enforcement. "Authorities in the United States of America has determined that this group consists of five or more persons located in Romania, who acted in a coordinated manner to administer those sites and to launder money obtained as a result of instigating crimes.” Representatives of Homeland Security Investigations and the US Embassy in Bucharest were present for the activities. According to the announcement, the suspects allegedly scammed would-be customers out of 500,000 euros ($543,842). "Yura,” the fraudster behind dozens of contract-killing sites, including Besa Mafia, Costa Nostra, and Crimebay, likely lives in Romania. Chris Monteiro, the "vigilante hacker” who has been hacking darkweb murder-for-hire sites since at least 2016, linked Yura to an IP address in Romania. Santosh Sharma, a freelancer who once did SEO work for Yura, said, "[Yura] was based in Romania.” Bratva Mafia is a new and unimproved version of Besa Mafia. It seems probable that police raided people with an alleged connection to Yura's sites and possibly Yura himself. However, the UK's National Crime Agency and Bulgarian police seized Crime Bay in May 2017. Monteiro stopped hearing from Yura and assumed the police had arrested him. But Yura returned in December 2017 and later launched Cosa Nostra. So, who knows. Monteiro believes Yura earned $6,539,800 vs. the estimated $543,842 listed in the press release. Seems like a significant discrepancy. archive.is (via darknetlive.com at https://darknetlive.com/post/romania-five-arrested-for-running-murder-for-hire-scams/)

German Police Seized Some of Hydra Market's Servers

Authorities in Germany announced the seizure of Hydra Market's servers and 23 million euros worth of Bitcoin associated with the market. Germany's Federal Criminal Police Office (BKA) seized servers in Germany allegedly used by the administrators of Hydra Market, the largest darkweb marketplace. Authorities also seized Bitcoins worth $25,186,840 (23 million euros). According to the announcement, the Bitcoins are "attributed” to the market. The BKA's banner is not currently loading for me. Law enforcement agencies in Germany and the United States have been investigating the market since August 2021. The investigation involved the BKA, the Central Office for Combating Cybercrime of the Frankfurt am Main Public Prosecutor's Office (ZIT), the United States Internal Revenue Service - Criminal Investigation (IRS-CI), the Federal Bureau of Investigation (FBI), Homeland Security Investigations (HSI), the Department of

Justice (DOJ), the Drug Enforcement Administration (DEA), and the United States Postal Investigation Service (USPIS). Hydra's "previously unknown operators and administrators” are under investigation for the operation of a criminal platform on the internet, enabling the trade of illegal narcotics and money laundering. The spokesman for the Central Office for Combating Internet Crime (ZIT) of the Frankfurt Public Prosecutor's Office, Sebastian Onion, said that investigators have not yet identified any suspects in the case. "Therefore, the investigations are far from over,” Onion said. A screenshot of Hydra Hydra is the largest darkweb marketplace, and sales on the platform amounted "to at least 1.23 billion euros in 2020 alone.” Hydra has been operating since as early as 2015, authorities said. More than 17 million customers and 19,000 vendors have registered accounts on the platform. Hydra's Bitcoin mixer made investigations "extremely difficult for law enforcement agencies.” The announcement follows the March 10 arrest of the founder of the payment service company Chronopay, Pavel Vrublevsky. Russian law enforcement arrested Vrublevsky and three co-conspirators for defrauding hundreds of thousands of people through scams, including phishing and fake lottery sites. I wrote about the case but never published it due to the lack of information. Pavel Vrublevsky | Kommersant Per the Russian media outlet Kommersant's report, Vrublevsky and his co-conspirators allegedly operated another payment service called Inferno Pay. Inferno Pay is "a cryptocurrency token and payment API that can be used on multiple websites, both new and existing, eliminating chargebacks and fraudulent activity,” according to the service's website. Through Inferno Pay, which appears to be a shitcoin for the so-called "porn industry,” Vrublevsky allegedly "provided cash-out services” to Hydra. If the report in Kommersant is correct, it appears as if Vrublevsky provided money-laundering services to Hydra's administrators in the past. I am doubtful of any connection between Vrublevsky's arrest and the recent seizure of Hydra's servers. For Hydra, though, all this amounts to is the loss of $25 million in Bitcoin and server infrastructure in Germany, I suspect. The seizure banner no longer loads for me. Perhaps we will see a repeat of the Doxbin saga where law enforcement agencies and site administrators publish competing onion service descriptors. archive.is/archive.org/bka.de "Professional criminals” in the US involved in the drug trade... just sad. Many such cases. I guess it is fair to speculate that Hydra's administrators have made enough money that keeping the market online becomes pointless. Which is essentially what Empire's admins did, I think. (via darknetlive.com at https://darknetlive.com/post/german-police-seized-some-of-hydra-markets-servers/)

Florida Darkweb Vendor Forfeits $34 Million in Crypto

A darkweb vendor in Florida forfeited $34 million worth of illicitly earned cryptocurrency. According to an announcement from the U.S. Attorney's Office for the Southern District of Florida, a judge entered a default judgment in favor of the United States against $34 million* worth of cryptocurrency seized from a darkweb vendor. The forfeiture includes 640.26804512 BTC, 640.2716098 Bitcoin Cash, 640.2715428 Bitcoin Gold, 640.2716043 Bitcoin S.V., and 919.30711258 ETH. According to prosecutors, the forfeiture is "one of the largest cryptocurrency forfeiture actions ever filed by the United States.” The majority of Bitcoin sent to the defendant's wallet came from a darkweb market. The forfeiture action results from an investigation into a prolific seller of hacked online account information on an unspecified darkweb marketplace. According to investigators, in January 2017, the vendor (identified only as "Moniker 1”) had completed more than 100,000 transactions. This number increased during the investigation. The completed transactions included several purchases by undercover law enforcement officers, including: On or about January 29, 2016, an undercover law enforcement officer purchased ten (10) Netflix accounts usernames and passwords from Moniker 1 on a Dark Web marketplace for approximately 0.00132443 bitcoins; On or about April 20, 2016, an undercover law enforcement officer purchased one World Wrestling Entertainment account username and password from Moniker 1 on a Dark Web marketplace for approximately 0.01134 bitcoins; On or about September 14, 2016, an undercover law enforcement officer purchased sixty Uber accounts usernames and passwords from Moniker 1 on a Dark Web marketplace for approximately 0.0824 bitcoins; On or about March 7, 2017, an undercover law enforcement officer purchased three (3) Xfinity accounts usernames and passwords from Moniker 1 on a Dark Web marketplace for approximately 0.040

bitcoins; and On or about March 13, 2017, an undercover law enforcement officer purchased one (1) HBOGO account username and password and one (1) Showtime account username and password from Moniker 1 on a Dark Web marketplace for approximately 0.0118 bitcoins. Court documents identified Alphabay as a market used by the defendant. The defendant admitted conducting "transactions using Bitcoin, Ethereum, and other cryptocurrencies” on Silk Road, Agora, Nucleus, AlphaBay, Dream Market, Abraxas, Sheep, and Evolution. I think only Alphabay and Dream meet the conditions for the market where investigators conducted undercover purchases. The defendant transacted on several markets but specifically admitted selling only on AlphaBay. "In or around 2016, law enforcement agents identified two residences in Florida linked to Moniker 1 after Moniker 1 provided the addresses as the shipping address when he or she previously purchased narcotics from Dark Web marketplaces,” according to court documents. The person associated with the shipping addresses lived at a residence in Parkland, Florida. Investigators identified the resident. Then, presumably using a pen register, investigators monitored internet traffic to and from the Comcast I.P. address associated with the residence. "Internet traffic to and from the Comcast I.P. address between in or around December 2016 and March 2017 revealed numerous internet connections from the Parkland Residence on the TOR network. In addition, the internet traffic data showed correlations between when the TOR network was accessed at the Parkland Residence and when messages were received from Moniker 1 by the law enforcement officer(s) making the undercover purchases.” Police identified the defendant's PNC bank account and obtained copies of their transaction history. The transactions made by the defendant were "consistent with that of a Dark Web vendor converting virtual currency into cash using LocalBitcoins.com,” according to court documents. On May 16, 2017, law enforcement agents executed a federal search warrant for the defendant's residence in Parkland. The items seized by police included a laptop owned by the defendant. The seizures of the defendant's various cryptocurrency wallets took place from May 2017 through June 2017. On May 16, 2017, police seized 919.30711258 ETH from the Ethereum wallet address 0x71949d87258c4ca6827730c337f80907d73c7800. In June 2017, police seized 418.51177 BTC from the Bitcoin wallet address 12EZr5x8mFpxS6ypNobhPXmyj4BbRkm6GW and 221.76 BTC "formerly held” in the same wallet. Blockchain analysis revealed that approximately ninety-six percent of the Bitcoin in the defendant's wallet came from darkweb marketplaces or exchanges. Over fifty percent of outgoing transfers were made to peer-to-peer exchanges, including LocalBitcoins.com. "Individual 1 told law enforcement agents that he or she obtained the ether in the Ethereum 7800 Wallet by converting bitcoins earned from unlawful online Dark Web transactions involving the sale of hacked online account information. Individual 1 converted the bitcoins to ether using a virtual currency exchange that did not require users to provide personal identifying information until in or around 2019, thus, providing an additional layer of anonymity.” Based on information from other court documents, ShapeShift appears to be the exchange referenced above. "Law enforcement agents were able to confirm that Individual 1 exchanged bitcoins obtained from Dark Web marketplaces for the ether held in the Ethereum 7800 Wallet through an analysis of the blockchain history for both the Ethereum 7800 Wallet and Bitcoin m6GW Wallet, the transactional activity at Virtual Currency Exchange 1, and historical exchange rates for the transaction dates.” "A review of the Ethereum blockchain history showed that approximately 919.30711258 ether was deposited into the Ethereum 7800 Wallet via nine (9) transactions between on or about March 16 and 17, 2017. These deposits were traced back to a known Ethereum address associated with Virtual Currency Exchange 1. "Further, a review of the blockchain Bitcoin history showed that approximately thirty-two (32) bitcoins were sent via nine (9) transactions from the Bitcoin m6GW Wallet to other Bitcoin addresses, and from those addresses, transfers were made to Virtual Currency Exchange 1.” "When these blockchain histories were compared with historical exchange rates, the same transfer amounts for the nine (9) transactions were shown on each respective blockchain, further confirming that bitcoins from the Bitcoin m6GW Wallet were converted to the ether coins eventually seized from the Ethereum 7800 Wallet.” The defendant told investigators that they had "only sold hacked online account information on AlphaBay.” With the defendant's cooperation, law enforcement officers withdrew 2.65995166 BTC from the defendant's vendor account on AlphaBay. In 2021, the defendant signed a consent to forfeiture. On

November 3, 2021, the government published a notice about the action on forfeiture.gov. Nobody filed a claim against the action (the defendant was the only claimant). As a result, U.S. District Court Judge Rodney Smith entered a default judgment in favor of the United States, which forfeited the defendant's right, title, and interest in the seized cryptocurrency. According to the press release, this case was the result of a so-called "Operation TORnado,” which is apparently a "joint investigation that stems from the ongoing efforts by OCDETF.” *The complaint for forfeiture lists the value of the seized cryptocurrency as $47 million. The $34 million number appears in the USAO's announcement. archive.is/archive.org/justice.gov Verified Complaint for Forfeiture in rem: pdf (via darknetlive.com at https://darknetlive.com/post/florida-darkweb-vendor-forfeits-34-million-in-crypto/)

USPIS Boston: 24 Kilos of Cocaine Seized in March 2022

During the first two weeks of March 2022, postal inspectors intercepted packages containing a combined total of 24 kilograms of cocaine and 3.5 kilograms of fentanyl. Leonard C Boyle, United States Attorney for the District of Connecticut, and Ketty Larco-Ward, Inspector in Charge of the U.S. Postal Inspection Service, Boston Division, today announced the results of an interdiction related to the use of the U.S. Mail to ship drugs and drug proceeds. During the first two weeks of March 2022, the U.S. Postal Inspection Service's Narcotics and Bulk Cash Trafficking Task Force conducted an interdiction that resulted in the seizure of more than 30 suspicious parcels that had been shipped through the U.S. Mail to Connecticut. Court-authorized searches of the parcels revealed a total of approximately 24 kilograms of cocaine, 3.5 kilograms of fentanyl, 11 kilograms of marijuana, other drugs, and $420,000 in cash. They certainly were not simply opening random suspicious packages as they entered the mail stream. The U.S. Postal Inspection Service's Narcotics and Bulk Cash Trafficking Task Force includes members from the U.S. Postal Inspection Service, the U.S. Postal Service - Office of the Inspector General, the Connecticut Army National Guard, and the Hartford, New Britain, Meriden and Town of Groton Police Departments. "The Narcotics and Bulk Trafficking Task Force has been doing an extraordinary job identifying drug traffickers who use the mail, and then seizing large quantities of drugs shipped to Connecticut and cash mailed in return to drug suppliers,” said U.S. Attorney Boyle. "Our office will continue to work with investigators to secure search warrants for suspicious parcels to decrease the flow of deadly narcotics into Connecticut, and prosecute those involved. A large portion of the cash seized in these investigations will help fund future law enforcement efforts.” "The U.S. Postal Inspection Service aims to identify, disrupt, and dismantle Drug Trafficking Organizations across the country,” said Ketty Larco-Ward, Inspector in Charge of the U.S. Postal Inspection Service, Boston Division. "Postal Inspectors accomplish this by focusing on illicit drug mailers and distribution rings, maintaining an aggressive drug parcel-detection program, and seeking prosecution of mailers and recipients of illegal drugs. Combatting illicit drugs in the mail is a top priority and we will continue to coordinate with our law enforcement partners as we prioritize our resources in areas with high levels of illicit drug activity.” archive.is justice.gov/usao-ct/pr/us-attorney-us-postal-inspection-service-announce-result-drug-cash-trafficking (via darknetlive.com at https://darknetlive.com/post/uspis-boston-24-kilos-of-cocaine-seized-in-march-2022/)

Dark Web Link

Top Darknet Markets 2022: The Outstanding Performances To Consider Now

The darknet markets are subject to availability and one of the many factors that contributes to the working of these dark web markets is their performances. The top darknet markets 2022 is the example where each of the marketplaces in the Tor network has proven its performance over and over again. So, in this article [...] The post Top Darknet Markets 2022: The Outstanding Performances To Consider Now appeared first on Dark Web Link | Deep web Onion Links | Darknet News.

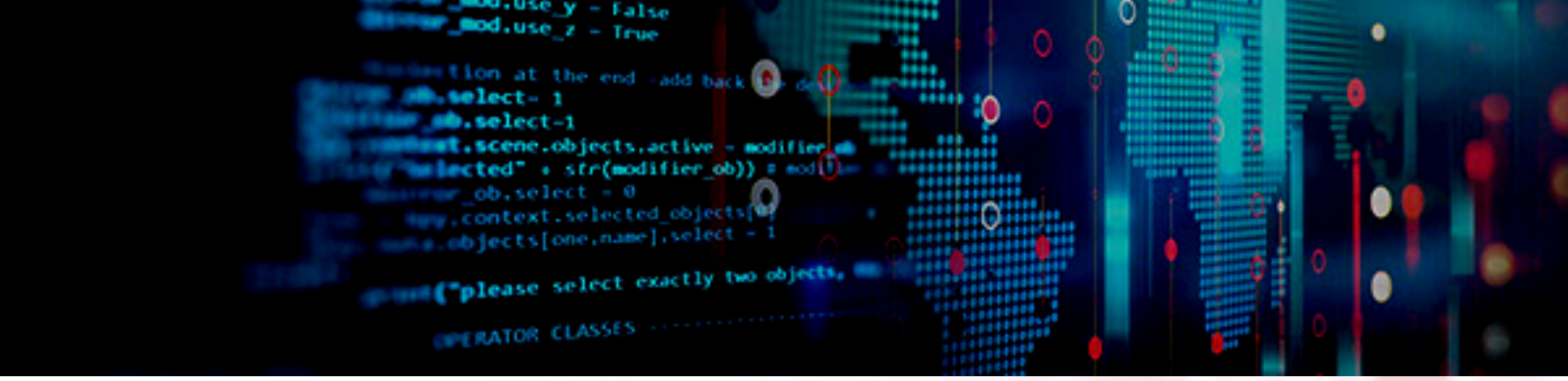
Breaking Bad Forum On The Darknet Is Revolutionary

The Breaking Bad Forum housed by the Tor network is a revolutionary darknet site indeed! So many forums exist on the dark web. But nothing could match the vibe of something like Breaking Bad. In this article, we will take you through the various aspects of the new forum. Breaking Bad Forum: A Gist Breaking [...] The post

Breaking Bad Forum On The Darknet Is Revolutionary appeared first on Dark Web Link | Deep web Onion Links | Darknet News.

White House Market Plans Retirement: What Important Things You Missed?

One of the latest darknet markets that accepted monero (XMR) as their payment modes have announced their retirement. The dark web market is none other than White House Market (WHM). As soon as the White House Market plans retirement and the news went live, there has been chaos all over the darknet sphere and there [...] The post White House Market Plans Retirement: What Important Things You Missed? appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Trend Micro Anti-Malware Blog

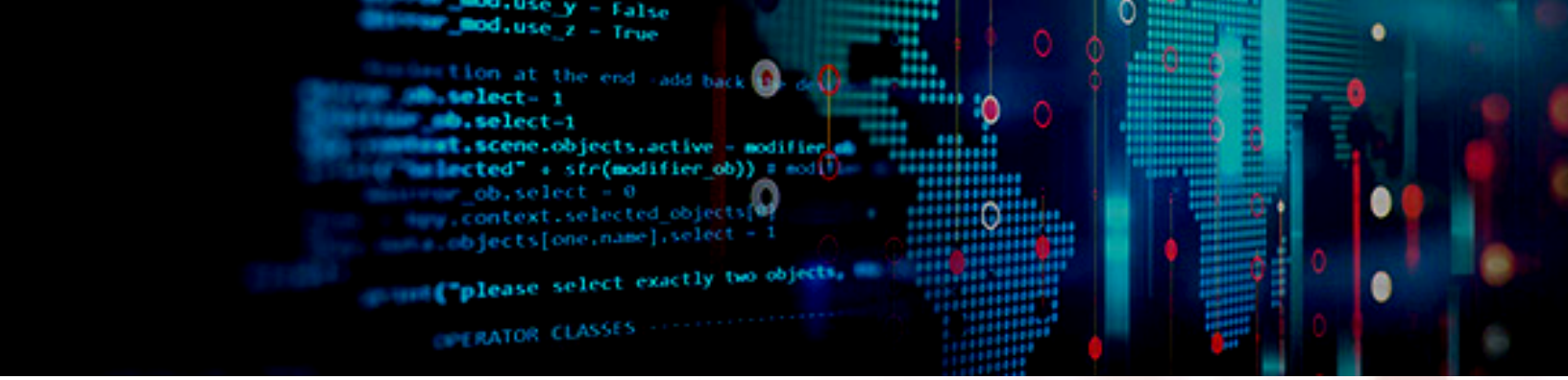
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

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

FireEye

* Metasploit Wrap-Up
* 7 Rapid Questions: Meet Adrian Stewart, Aspiring Pilot Turned Product Manager
* Lessons in IoT Hacking: How to Dead-Bug a BGA Flash Memory Chip
* The Forecast Is Flipped: Flipping L&D in New Hire Training
* MDR Plus Threat Intel: 414 New Detections in 251 Days (You're Welcome)
* What's New in InsightIDR: Q1 2022 in Review
* Security for All: How the Rapid7 Cybersecurity Foundation Will Expand Access and Inclusion
* Cloud Pentesting, Pt. 3: The Impact of Ecosystem Maturity
* Sharpen Your IR Capabilities With Rapid7's Detection and Response Workshop
* Securing Your Applications Against Spring4Shell (CVE-2022-22965)



Advisories

US-Cert Alerts & bulletins

* AA22-083A: Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targe
* AA22-076A: Strengthening Cybersecurity of SATCOM Network Providers and Customers
* Vulnerability Summary for the Week of March 28, 2022
* Vulnerability Summary for the Week of March 21, 2022

Zero Day Initiative Advisories

ZDI-CAN-17083: 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: 2022-04-06, 5 days ago. The vendor is given until 2022-08-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-17079: 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: 2022-04-06, 5 days ago. The vendor is given until 2022-08-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-17082: 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: 2022-04-06, 5 days ago. The vendor is given until 2022-08-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-17078: 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: 2022-04-06, 5 days ago. The vendor is given until 2022-08-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-17068: 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: 2022-04-06, 5 days ago. The vendor is given until 2022-08-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-17070: Adobe
A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-04-06, 5 days ago. The vendor is given until 2022-08-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-17069: 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: 2022-04-06, 5 days ago. The vendor is given until 2022-08-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-17071: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-04-06, 5 days ago. The vendor is given until 2022-08-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-17067: 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: 2022-04-06, 5 days ago. The vendor is given until 2022-08-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-17065: 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: 2022-04-06, 5 days ago. The vendor is given until 2022-08-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-17066: 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: 2022-04-06, 5 days ago. The vendor is given until 2022-08-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-17064: 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: 2022-04-06, 5 days ago. The vendor is given until 2022-08-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-17063: 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: 2022-04-06, 5 days ago. The vendor is given until 2022-08-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16967: 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 'kdot' was reported to the affected vendor on: 2022-04-06, 5 days ago. The vendor is given until 2022-08-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-17062: 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: 2022-04-06, 5 days ago. The vendor is given until 2022-08-04 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16951: 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 'kdot' was reported to the affected vendor on: 2022-04-01, 10 days ago. The vendor is given until 2022-07-30 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-16957: 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 'kdot' was reported to the affected vendor on: 2022-04-01, 10 days ago. The vendor is given until 2022-07-30 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-16919: 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: 2022-04-01, 10 days ago. The vendor is given until 2022-07-30 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-16952: 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 'kdot' was reported to the affected vendor on: 2022-04-01, 10 days ago. The vendor is given until 2022-07-30 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-16679: Sante

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 'Eunice' was reported to the affected vendor on: 2022-04-01, 10 days ago. The vendor is given until 2022-07-30 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-15727: 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 'Anonymous' was reported to the affected vendor on: 2022-04-01, 10 days ago. The vendor is given until 2022-07-30 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-17032: Google

A CVSS score 4.5 (AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Eduardo Braun Prado' was reported to the affected vendor on: 2022-04-01, 10 days ago. The vendor is given until 2022-07-30 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-17016: Linux

A CVSS score 6.7 (AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:L) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) and Reno Robert of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-04-01, 10 days ago. The vendor is given until 2022-07-30 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-15728: D-Link

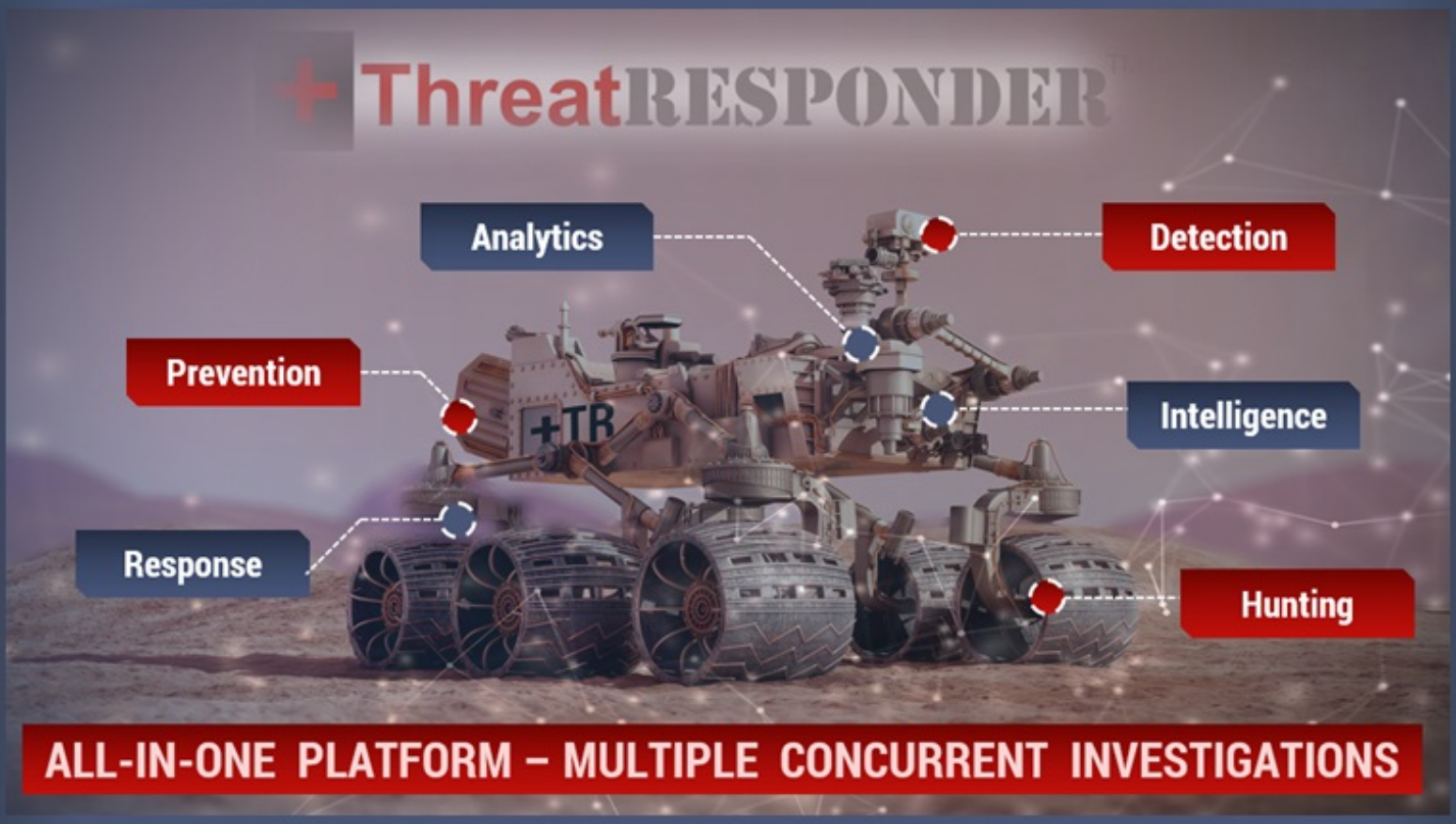
A CVSS score 8.8 (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-04-01, 10 days ago. The vendor is given until 2022-07-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Are You...

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

Do DFIR Investigations Better

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



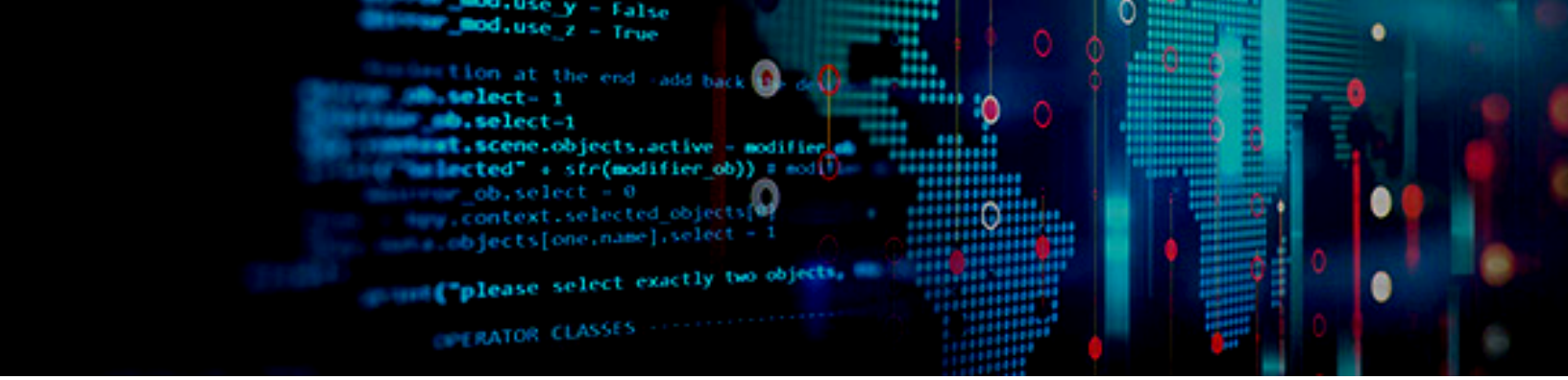
The Solution – ThreatResponder® Platform

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

Get a Trial Copy

Mention **CODE: CIR-0119**

https://netsecurity.com

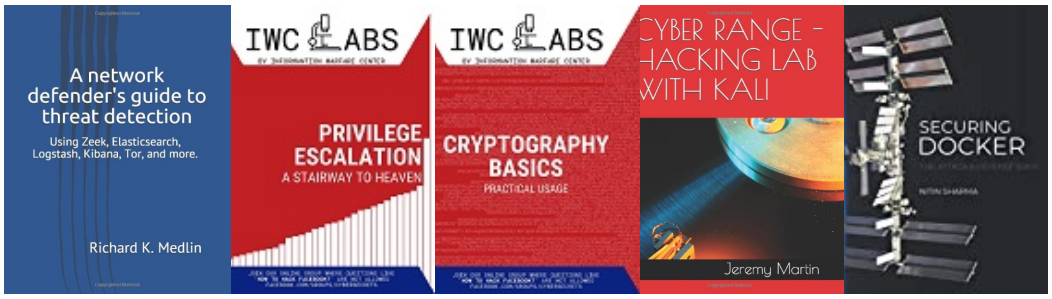


The Cyber Secrets publications on Amazon

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

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

Other Publications from Information Warfare Center



CYBER WEEKLY AWARENESS REPORT

VISIT US AT **INFORMATIONWARFARECENTER.COM**

THE IWC ACADEMY
ACADEMY.INFORMATIONWARFARECENTER.COM

FACEBOOK GROUP
FACEBOOK.COM/GROUPS/CYBERSECRETS

CSI LINUX
CSILINUX.COM

CYBERSECURITY TV
CYBERSEC.TV

ARGOS
APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity

ThreatRESPONDER

Accredited Training Center
EC-Council

CYBERQ GROUP