Jul-04-22

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

July 4, 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

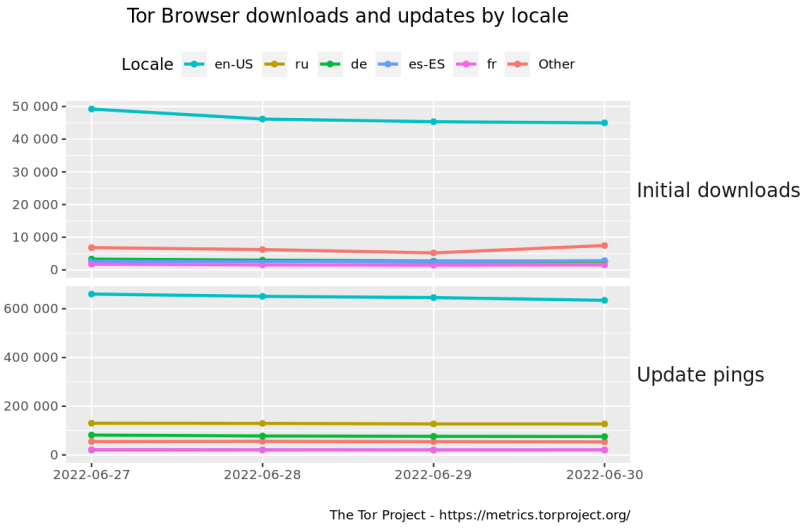
Internet Storm Center Infocon Status

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

* ZuoRAT Can Take Over Widely Used SOHO Routers
* Flagstar Bank Breach Another Example Of Hacker Threat To Financial Sector
* FBI Adds Missing Cryptoqueen To Top Ten Most Wanted List
* Microsoft Exchange Servers Worldwide Hit By Stealthy New Backdoor
* Jenkins Warns Of Security Holes In These 25 Plugins
* China Lured Graduate Jobseekers Into Digital Espionage
* Leaky Access Tokens Exposed Amazon Photos Of Users
* The Supreme Court Just Fucked The Planet
* Microsoft Warns Malware That Targets Linux Just Got A Big Update
* Bumblebee Fast Becoming Favorite For Ransomware Gangs
* FBI Warns Crooks Are Using Deep Fake Videos In Interviews For Remote Gigs
* Canadian Admits To Hacking Spree With Russian Cyber-Gang
* Patchable And Preventable Security Issues Lead Causes Of Q1 Attacks
* G7 To Tackle Cyber Threats And Disinformation From Russia
* Mitel VoIP Bug Exploited In Ransomware Attacks
* RansomHouse Hits AMD And Claims To Have Stolen 450 Gigs Of Data
* How To Watch Today's Surprise Hearing From The Jan. 6 Committee
* The Abortion Clues That Can Hide On Your Phone
* Russia's Killnet Hacker Group Says It Attacked Lithuania
* Contractor Loses Entire Japanese City's Personal Data In USB Fail
* Beijing Probes Security At Academic Journal Database
* UK Security Services Must Seek Approval To Access Telecoms Data, Judge Rules
* NSO Claims More Than 5 EU States Use Pegasus Spyware
* Beijing-Backed Attackers Use Ransomware As Decoy While They Conduct Espionage
* Google Warns Spyware Being Deployed Against Android, iOS

Krebs on Security

* The Link Between AWM Proxy & the Glupteba Botnet
* Meet the Administrators of the RSOCKS Proxy Botnet
* Why Paper Receipts are Money at the Drive-Thru
* Microsoft Patch Tuesday, June 2022 Edition
* Ransomware Group Debuts Searchable Victim Data
* "Downthem" DDoS-for-Hire Boss Gets 2 Years in Prison
* Adconion Execs Plead Guilty in Federal Anti-Spam Case
* KrebsOnSecurity in New Netflix Series on Cybercrime
* What Counts as "Good Faith Security Research?"
* Costa Rica May Be Pawn in Conti Ransomware Group's Bid to Rebrand, Evade Sanctions

Dark Reading

* ICYMI: A Microsoft Warning, Follina, Atlassian, and More
* OpenSea NFT Marketplace Faces Insider Hack
* Time Constraints Hamper Security Awareness Programs
* Criminals Use Deepfake Videos to Interview for Remote Work
* DragonForce Malaysia Releases LPE Exploit, Threatens Ransomware
* When It Comes to SBOMs, Do You Know the Ingredients in Your Ingredients?
* Microsoft Going Big on Identity with the Launch of Entra
* Google: Hack-for-Hire Groups Present a Potent Threat
* 18 Zero-Days Exploited So Far in 2022
* API Security Losses Total Billions, But It's Complicated
* Exchange Servers Backdoored Globally by SessionManager
* Study Reveals Traditional Data Security Tools Have a 60% Failure Rate Against Ransomware and Extortio
* A Fintech Horror Story: How One Company Prioritizes Cybersecurity
* NXM Announces Platform That Protects Space Infrastructure and IoT Devices From Cyberattacks
* Critical ManageEngine ADAudit Plus Vulnerability Allows Network Takeover, Mass Data Exfiltration
* Zero-Days Aren't Going Away Anytime Soon & What Leaders Need to Know
* Patch Now: Linux Container-Escape Flaw in Azure Service Fabric
* ZuoRAT Hijacks SOHO Routers From Cisco, Netgear
* Broken Authentication Vuln Threatens Amazon Photos Android App
* How to Master the Kill Chain Before Your Attackers Do

The Hacker News

* HackerOne Employee Caught Stealing Vulnerability Reports for Personal Gains
* TikTok Assures U.S. Lawmakers it's Working to Safeguard User Data From Chinese Staff
* Microsoft Warns About Evolving Capabilities of Toll Fraud Android Malware Apps
* Google Improves Its Password Manager to Boost Security Across All Platforms
* New 'SessionManager' Backdoor Targeting Microsoft IIS Servers in the Wild
* Solving the indirect vulnerability enigma - fixing indirect vulnerabilities without breaking your dep
* Amazon Quietly Patches 'High Severity' Vulnerability in Android Photos App
* Microsoft Warns of Cryptomining Malware Campaign Targeting Linux Servers
* Google Blocks Dozens of Malicious Domains Operated by Hack-for-Hire Groups
* U.S. FCC Commissioner Asks Apple and Google to Remove TikTok from App Stores
* What is Shadow IT and why is it so risky?
* Ex-Canadian Government Employee Pleads Guilty Over NetWalker Ransomware Attacks
* North Korean Hackers Suspected to be Behind $100M Horizon Bridge Hack
* New YTStealer Malware Aims to Hijack Accounts of YouTube Content Creators
* New UnRAR Vulnerability Could Let Attackers Hack Zimbra Webmail Servers

Security Week

* Experts: California Lacked Safeguards for Gun Owner Info
* Dutch Uni Gets Cyber Ransom Money Back... With Interest
* QuSecure Scores Post-Quantum Cybersecurity Contract Worth More Than $100M Annually
* Google: Half of 2022's Zero-Days Are Variants of Previous Vulnerabilities
* Google Blocks Domains of Hack-for-Hire Groups in Russia, India, UAE
* Cyberattack Disrupts Unemployment Benefits in Some States
* Oak9 Lands $8 Million in New Venture Investment
* North Korea Lazarus Hackers Blamed for $100 Million Horizon Bridge Heist
* Token Raises $13 Million for Its Biometric Authentication Ring
* Google Workspace Now Warns Admins of Sensitive Changes
* SOHO Routers in North America and Europe Targeted With 'ZuoRAT' Malware
* Feature: Securing the Metaverse and Web3
* Brocade Vulnerabilities Could Impact Storage Solutions of Several Major Companies
* Vulnerability in Amazon Photos Android App Exposed User Information
* RSAC22 and Infosecurity Europe, Three Weeks, Two Events
* Canadian NetWalker Ransomware Affiliate Pleads Guilty in US
* Cyberattack Hits Norway, Pro-Russian Hacker Group Fingered
* Azure Service Fabric Vulnerability Can Lead to Cluster Takeover
* Securing the Metaverse and Web3
* Firefox 102 Patches 19 Vulnerabilities, Improves Privacy
* CISA Calls for Expedited Adoption of Modern Authentication Ahead of Deadline
* MITRE Publishes 2022 List of 25 Most Dangerous Vulnerabilities
* CISA-Funded Project Enables Students With Disabilities to Learn Cybersecurity
* Normalyze Announces $22 Million for DSPM Technology
* Google Introduces New Capabilities for Cloud Armor Web Security Service
* CISA Says 'PwnKit' Linux Vulnerability Exploited in Attacks

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* [New FBI and CISA Alert] This ransomware strain uses RDP flaws to hack into your network
* Celebrity Crypto Scams Just Keep on Getting Worse
* [Heads Up] Online Fraud Now Sky-high With 'Tinder Swindler' Romance Scams Costing Hundreds of Million
* Wars and Lechery, Nothing Else Holds Fashion for Phishing Attacks
* Bad News to Ransom Payers: 80% of You Will Face a Second Attack Within 30 Days
* 80% of Organizations Await "Inevitable" Negative Consequences From Email-Born Cyberattacks
* New Evasive Phishing Techniques Help Cybercriminals Launch "Untraceable" Campaigns
* Innovative Way to Bypass MFA Using Microsoft WebView2 Is Familiar Nevertheless
* FBI Warns of Deepfakes Used to Apply for Remote Jobs
* CyberheistNews Vol 12 #26 [Heads Up] The FBI Warns That LinkedIn Fraudsters Are Now a Significant Thr

ISC2.org Blog

* How can you find and retain new cybersecurity talent?
* Four Steps to Using Metrics to Defend Your Security Budget
* How to Create Successful CISSP and CCSP Study Groups
* Center for Cyber Safety and Education Begins Program Updates to Increase Impact
* Infosecurity Europe: A show so secure a train strike couldn't break it!

HackRead

* What Are Common Cyber Threats to Manufacturers and How Can They Secure Themselves
* Report Claims Coinbase Selling User Geolocation Data to ICE
* Google cracks down on sites with ties to hack-for-hire groups in UAE, Russia, India
* Managed Cloud Hosting vs. Unmanaged Cloud Hosting: What's the Difference?
* New YTStealer Malware is Hijacking YouTube Channels
* NFT Marketplace OpenSea Suffers Data Breach- Users' Email IDs Leaked
* Importance of Digital Strategy and Automation for Businesses

Koddos

* What Are Common Cyber Threats to Manufacturers and How Can They Secure Themselves
* Report Claims Coinbase Selling User Geolocation Data to ICE
* Google cracks down on sites with ties to hack-for-hire groups in UAE, Russia, India
* Managed Cloud Hosting vs. Unmanaged Cloud Hosting: What's the Difference?
* New YTStealer Malware is Hijacking YouTube Channels
* NFT Marketplace OpenSea Suffers Data Breach- Users' Email IDs Leaked
* Importance of Digital Strategy and Automation for Businesses

Naked Security

* Facebook 2FA phish arrives just 28 minutes after scam domain created
* "Missing Cryptoqueen" hits the FBI's Ten Most Wanted list
* S3 Ep89: Sextortion, blockchain blunder, and an OpenSSL bugfix [Podcast + Transcript]
* Firefox 102 fixes address bar spoofing security hole (and helps with Follina!)
* Harmony blockchain loses nearly $100M due to hacked private keys
* FTC warns of LGBTQ+ extortion scams - be aware before you share!
* OpenSSL issues a bugfix for the previous bugfix
* S3 Ep88: Phone scammers, hacking bust, and data breach fines [Podcast + Transcript]
* Capital One identity theft hacker finally gets convicted
* Interpol busts 2000 suspects in phone scamming takedown

Threat Post

* ZuoRAT Can Take Over Widely Used SOHO Routers
* A Guide to Surviving a Ransomware Attack
* Leaky Access Tokens Exposed Amazon Photos of Users
* Patchable and Preventable Security Issues Lead Causes of Q1 Attacks
* Top Six Security Bad Habits, and How to Break Them
* Mitel VoIP Bug Exploited in Ransomware Attacks
* 'Killnet' Adversary Pummels Lithuania with DDoS Attacks Over Blockade
* Log4Shell Vulnerability Targeted in VMware Servers to Exfiltrate Data
* Google Warns Spyware Being Deployed Against Android, iOS Users
* Fancy Bear Uses Nuke Threat Lure to Exploit 1-Click 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

* What happens when there's not enough cloud?
* Identity, trust, and their role in modern applications
* Uno Platform advances WebAssembly support
* Traditional architecture still has a place in the cloud
* What is Flutter? Mobile app development for Android, iOS, and more
* What's new in Rust 1.62
* Choosing your Java IDE
* The best new features in .NET 6
* C# language specification approved
* How to deploy with Vercel and MongoDB Atlas without even trying

C4ISRNET - Media for the Intelligence Age Military

* US Navy, Air Force running 'capstone test' of new high-power microwave missile
* Booz Allen acquisition of defense firm EverWatch would harm NSA, US says
* NATO forging cyber response force amid growing Russian, Chinese threats
* Accelerating the Zero Trust Journey in Federal Government
* Webcast: Crisis Communications
* Marine Corps unveils information guidance as US rivals spew propaganda
* Space Force mulls new acquisition approach for next phase of medium, heavy launches
* National Guardsmen may soon use personal electronics in deployments
* Six proven steps to Zero Trust
* US Army awards $72 million for new phase in next-gen ground system effort

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

* 2022 0-day In-the-Wild Exploitation…so far
* The curious tale of a fake Carrier.app

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.

* Hacky Holidays - Unlock the City
* FAUST CTF 2022
* vsCTF 2022
* HTB Business CTF 2022: Dirty Money
* Crypto CTF 2022
* ImaginaryCTF 2022
* UACTF 2022
* 3kCTF-2022
* RED CTF
* TFC CTF 2022

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

* Queue Abstract Data Type Tool
* Blue Team Training Toolkit (BT3) 2.9
* Global Socket 1.4.36
* American Fuzzy Lop plus plus 4.01c
* MIMEDefang Email Scanner 3.0
* OpenSSL Toolkit 1.1.1p
* Wireshark Analyzer 3.6.6
* TOR Virtual Network Tunneling Tool 0.4.7.8
* Zeek 4.2.2
* Falco 0.32.0

Kali Linux Tutorials

* FindFunc : Advanced Filtering/Finding of Functions in IDA Pro
* Pocsploit : A Lightweight, Flexible And Novel Open Source Poc Verification Framework
* DroidDetective : A Machine Learning Malware Analysis Framework For Android Apps
* Frida-Ios-Hook : A Tool That Helps You Easy Trace Classes, Functions, And Modify The Return Valu
* Tornado : Anonymously Reverse Shell Over Tor Network Using Hidden Services Without Port forwarding
* Reposaur : The Open Source Compliance Tool For Development Platforms
* Findwall : Check If Your Provider Is Blocking You
* Frelatage : The Python Fuzzer That The World Deserves
* Fb_Friend_List_Scraper : OSINT Tool To Scrape Names And Usernames From Large Friend Lists
* Zphisher-GUI-Back_office : A Zphisher GUI Back-Office Plugin

GBHackers Analysis

* Critical PHP Flaws Allows Attackers to Execute Remote Code on QNAP NAS Devices
* Critical Flaws in MEGA Cloud Storage Let Attacker Decrypt User Data
* A 5-Year-Old Bug in Apple Safari Exploited in the Wild - Google Project Zero
* Ubuntu Desktop & Windows 11 Hacked - Pwn2Own Day 3
* Pwn2Own - Windows 11, Microsoft Teams Hacked & Exploiting 16 Zero-day Bugs

Weekly Cyber Security Video and Podcasts

SANS DFIR

* FOR585 Course Animation: Potential Crime Scene iPhone and Android
* FOR585 Course Animation: IMEI vs GSM
* FOR585 Course Animation: How WAL Gets Populated Initial State
* FOR585 Course Animation: Solid State Memory Properties

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

* Grabbing Windows Wi-Fi Passwords with the O.MG Cable | HakByte
* Live Hacking Q&A with Kody Kinzie and Nick Godshaw
* Abortion Rights are Privacy Rights - ThreatWire

The PC Security Channel [TPSC]

* Malwarebytes: Test vs Ransomware
* Windows Zero Day: MSDT Follina Exploit Demonstration

Eli the Computer Guy

* What is DNS (Domain Name System)
* eBeggar Wednesday - SLOW NEWS WEEK... nothing to see... move along...
* SILICON DERBY - The races begin!!!
* What is NAT and Port Forwarding (Network Address Translation)

Security Now

* The "Hertzbleed” Attack - 3rd Party FIDO2, Log4Shell, '311" Proposal
* Microsoft's Patchy Patches - 3rd Party Authenticators, MS-DFSNM, Safari Regression, Firefox Cookies

Troy Hunt

* Weekly Update 302

Intel Techniques: The Privacy, Security, & OSINT Show

* 268-CCW Permits, UNREDACTED 003, & Linux Questions
* 267-macOS Privacy & Security Revisited

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Packet Storm New Exploits For June, 2022
* Carel pCOWeb HVAC BACnet Gateway 2.1.0 Unauthenticated Directory Traversal
* PHP Library Remote Code Execution
* BigBlueButton 2.3 / 2.4.7 Cross Site Scripting
* Classified Listing 2.2.9 Cross Site Scripting
* TypeORM SQL Injection
* Backdoor.Win32.Coredoor.10.a MVID-2022-0618 Authentication Bypass
* Backdoor.Win32.EvilGoat.b MVID-2022-0619 Hardcoded Credential
* Backdoor.Win32.Cafeini.b MVID-2022-0617 Hardcoded Credential
* Fruits-Bazar 2021 1.0 SQL Injection
* Laundry Management System 1.0 SQL Injection
* AnyDesk 7.0.9 Arbitrary File Write / Denial Of Service
* OpenCart 3.x So Filter Shop By SQL Injection
* Zoo Management System 1.0 Cross Site Scripting
* WordPress Simple Page Transition 1.4.1 Cross Site Scripting
* Mailhog 1.0.1 Cross Site Scripting
* WordPress W-DALIL 2.0 Cross Site Scripting
* WordPress Weblizar 8.9 Code Execution
* Coffee Shop Cashiering System 1.0 SQL Injection
* Library Management System With QR Code 1.0 SQL Injection
* Library Management System With QR Code 1.0 Cross Site Scripting
* Library Management System With QR Code 1.0 Shell Upload
* WSO2 Management Console Cross Site Scripting
* Backdoor.Win32.InfecDoor.17.c MVID-2022-0614 Insecure Permissions
* Trojan-Mailfinder.Win32.VB.p MVID-2022-0616 Insecure Permissions

CXSecurity

* WiFi Mouse 1.7.8.5 Remote Code Execution
* Kitty 0.76.0.8 Stack Buffer Overflow
* phpIPAM 1.4.5 Remote Code Execution
* Pandora FMS 7.0NG.742 Remote Code Execution
* Navigate CMS 2.9.4 Server-Side Request Forgery (SSRF) (Authenticated)
* Atlassian Confluence Namespace OGNL Injection
* Microsoft Office Word MSDTJS Code Execution

Proof of Concept (PoC) & Exploits

Exploit Database

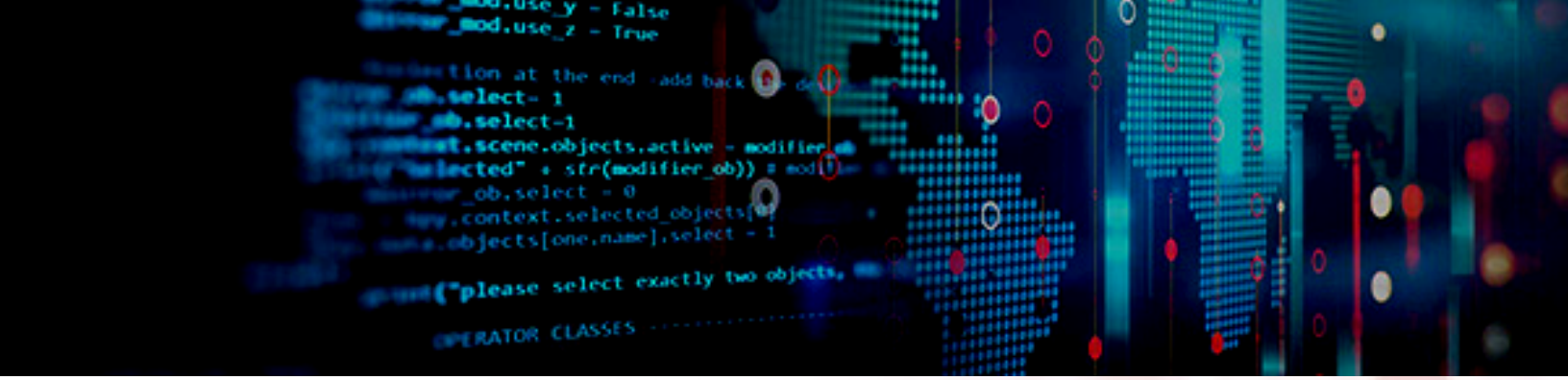
* [remote] WiFi Mouse 1.7.8.5 - Remote Code Execution(v2)
* [webapps] Mailhog 1.0.1 - Stored Cross-Site Scripting (XSS)
* [webapps] WSO2 Management Console (Multiple Products) - Unauthenticated Reflected Cross-Site Scriptin
* [webapps] WordPress Plugin Weblizar 8.9 - Backdoor
* [webapps] SolarView Compact 6.00 - 'pow' Cross-Site Scripting (XSS)
* [webapps] SolarView Compact 6.00 - 'time_begin' Cross-Site Scripting (XSS)
* [webapps] Old Age Home Management System 1.0 - SQLi Authentication Bypass
* [webapps] ChurchCRM 4.4.5 - SQLi
* [remote] Sourcegraph Gitserver 3.36.3 - Remote Code Execution (RCE)
* [webapps] phpIPAM 1.4.5 - Remote Code Execution (RCE) (Authenticated)
* [remote] TP-Link Router AX50 firmware 210730 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Pandora FMS v7.0NG.742 - Remote Code Execution (RCE) (Authenticated)
* [remote] Algo 8028 Control Panel - Remote Code Execution (RCE) (Authenticated)
* [local] HP LaserJet Professional M1210 MFP Series Receive Fax Service - Unquoted Service Path
* [remote] Virtua Software Cobranca 12S - SQLi
* [remote] Marval MSM v14.19.0.12476 - Cross-Site Request Forgery (CSRF)
* [remote] Marval MSM v14.19.0.12476 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Avantune Genialcloud ProJ 10 - Cross-Site Scripting (XSS)
* [local] Real Player 16.0.3.51 - 'external::Import()' Directory Traversal to Remote Code Execution (RC
* [local] Real Player v.20.0.8.310 G2 Control - 'DoGoToURL()' Remote Code Execution (RCE)
* [webapps] Confluence Data Center 7.18.0 - Remote Code Execution (RCE)
* [webapps] WordPress Plugin Motopress Hotel Booking Lite 4.2.4 - Stored Cross-Site Scripting (XSS)
* [remote] SolarView Compact 6.00 - Directory Traversal
* [remote] Schneider Electric C-Bus Automation Controller (5500SHAC) 1.10 - Remote Code Execution (RCE)
* [remote] Telesquare SDT-CW3B1 1.1.0 - OS Command Injection

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*

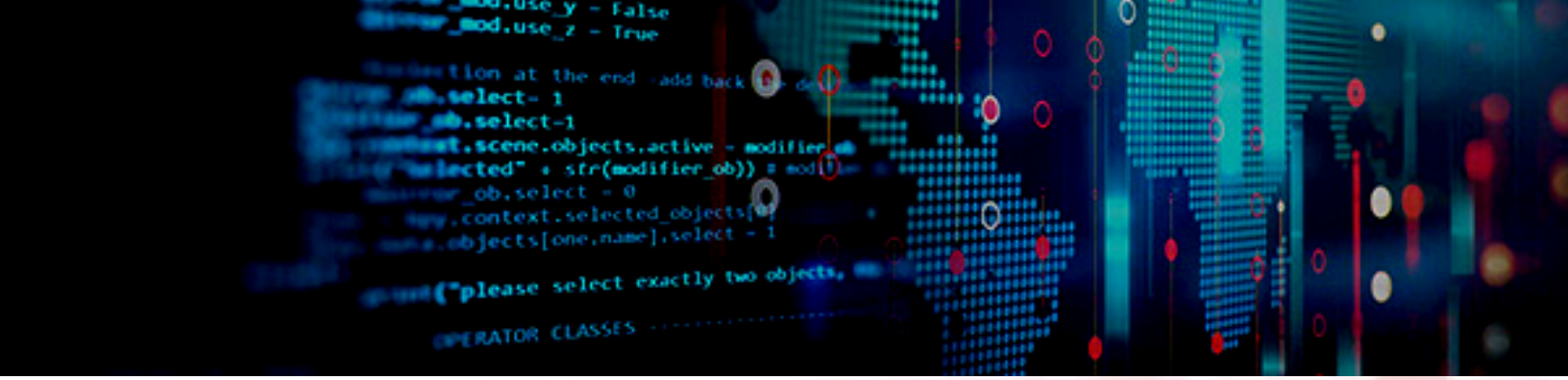
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://www.khaochot.go.th/Matigan.php
https://www.khaochot.go.th/Matigan.php notified by Matigan1337
http://zakat.ajk.gov.pk/1877.html
http://zakat.ajk.gov.pk/1877.html notified by CodeBoy1877
http://presidentajk.gov.pk/1877.html
http://presidentajk.gov.pk/1877.html notified by CodeBoy1877
http://pmajk.gov.pk/1877.html
http://pmajk.gov.pk/1877.html notified by CodeBoy1877
http://forest.ajk.gov.pk
http://forest.ajk.gov.pk notified by CodeBoy1877
http://information.ajk.gov.pk
http://information.ajk.gov.pk notified by CodeBoy1877
http://finance.ajk.gov.pk
http://finance.ajk.gov.pk notified by CodeBoy1877
http://electricity.ajk.gov.pk
http://electricity.ajk.gov.pk notified by CodeBoy1877
http://itb.ajk.gov.pk/1877.html
http://itb.ajk.gov.pk/1877.html notified by CodeBoy1877
http://auqaf.ajk.gov.pk
http://auqaf.ajk.gov.pk notified by CodeBoy1877
http://ajktourism.gov.pk/1877.html
http://ajktourism.gov.pk/1877.html notified by CodeBoy1877
http://aims.ajk.gov.pk
http://aims.ajk.gov.pk notified by CodeBoy1877
http://livestock.ajk.gov.pk/1877.html
http://livestock.ajk.gov.pk/1877.html notified by CodeBoy1877
http://ajk.gov.pk
http://ajk.gov.pk notified by CodeBoy1877
https://csr.cianjurkab.go.id/dzz.php
https://csr.cianjurkab.go.id/dzz.php notified by Gang Dz
http://yaicha.go.th/zz.html
http://yaicha.go.th/zz.html notified by xNot_RespondinGx
http://tln.go.th/zz.html
http://tln.go.th/zz.html notified by xNot_RespondinGx



Dark Web News

Darknet Live

Third and Final "EastSideHigh" Defendant Pleads Guilty

The third member of the "EastSideHigh” darkweb drug trafficking group pleaded guilty to drug manufacturing, distribution, and possession charges. __ Steven McCall with co-conspirators Binh Thanh Le and Allante Pires Steven McCall, 26, pleaded guilty to conspiracy to manufacture, distribute and possess with intent to distribute MDMA, Ketamine, and Alprazolam. Summary _ McCall and co-conspirators Binh Thanh Le and Allante Pires sold various drugs, including cocaine, MDMA, Ketamine, and Xanax, on the darkweb. The trio sold through a vendor account on Wallstreet Market and Dream Market under the username "EastSideHigh.” __ The EastSideHigh vendor profile on Wallstreet Market Le, the ringleader, was sentenced to eight years in prison on March 10, 2022, for the charges of conspiracy to manufacture, distribute and possess with intent to distribute MDMA, ketamine, and alprazolam. A judge ordered Le to forfeit more than 59 Bitcoin (currently worth more than $1.2 million), and $114,680 in cash, among other things. On June 3, 2022, Pires pleaded guilty to the same charges. His sentencing hearing was scheduled for September 8, 2022. __ Some of the products advertised by the vendor on Wallstreet Market During the investigation, law enforcement officers seized more than 19 kilograms of MDMA, almost seven kilograms of ketamine, nearly one kilogram of cocaine, more than 10,000 counterfeit Xanax pills, and over $114,000 in cash. At an office space in Stoughton, police found packages of drugs, [a laptop signed into the EastSideHigh account](/post/ecstasy-and-ketamine-vendor-eastsidehigh-busted-in-massachusetts/ 'Ecstasy and Ketamine Vendor "EastSideHigh” Busted in Massachusetts') on Wallstreet Market, and McCall. McCall was wearing a respirator and latex gloves when police arrested him at the office space. Background _ A background on the case from one of the previous EastsideHigh articles on Darknetlive: In February 2019, an undercover Homeland Security Investigations (HSI) agent notified Postal Inspector Gina Gentiluomo that EastSideHigh wanted to exchange Bitcoin for cash. The HSI agent communicated with EastSideHigh through a secure messaging application about the exchange. Inspector Gentiluomo then contacted the vendor, posing as the money launderer. Hotel Meeting _ In March 2019, Inspector Gentiluomo and another postal inspector (UC) met with Le at a hotel. The parties agreed to exchange $200,000 in Bitcoin in a wired hotel room. After Le had sent the Bitcoin to the address provided by the feds, the second postal inspector pretended to be having problems with his cellphone. He asked Le to open the wallet application on his phone and verify that the transaction had been completed. Le handed his unlocked phone to the postal inspector. After the postal inspector had possession of Le's phone, postal inspectors and state police entered the room and detained Le. After being advised of his rights per Miranda, Le voluntarily provided law enforcement officers with his password. After detaining Le, other officers approached Pires' Mercedes, which was still in the hotel's parking lot. They detained Pires and asked him about the keys on his key ring. Pires identified one as the key to the office space in Stoughton. Other law enforcement officers executed a search warrant at the office space where they encountered McCall wearing a respirator. The Search in Stoughton _ Inside the office space, the police found 11 pounds of ketamine, 5,000 grams of ecstasy pills, packaging materials, two digital scales, two

heat-sealing devices, a pill press, and $114,700 in cash. They also found a laptop with the EastSideHigh profile on Wallstreet Market on the screen. The police seized 18 kilograms of MDMA and more than $200,000 in Bitcoin by the end of the investigation. Le pleaded guilty to conspiracy to manufacture, distribute and possess with intent to distribute MDMA, Ketamine, and Alprazolam. On March 10, 2022, a judge sentenced Le to eight years in prison and three years of supervised release. The judge ordered Le to forfeit more than 59 Bitcoin, $114,680 in cash, the proceeds from a 2018 BMW M3 sale, a pill press, and a currency counter. The charge of conspiracy to manufacture, distribute and possess with intent to distribute MDMA, Ketamine, and alprazolam carries a mandatory minimum sentence of three years in prison and a maximum of 20 years in prison.
Brockton Man Pleads Guilty in Sophisticated Drug Trafficking Conspiracy that Operated Using the Dark Web | archive.is, archive.org, justice.gov (via darknetlive.com at https://darknetlive.com/post/third-eastsidehigh-defendant-pleads-guilty/)
Darkweb Oxy Buyer Sentenced for Owning Firearms

A man who admitted purchasing counterfeit oxycodone pills on the darkweb was sentenced to 18 months of probation for possessing firearms as a drug user. In an Omaha, Nebraska, court, Chief Judge Robert F. Rossiter, Jr. sentenced 46-year-old Edward Barta to 18 months of probation for one count of possession of firearms by a drug user. In late 2020, federal law enforcement officers intercepted a package of apparent oxycodone pills en route to 46-year-old Edward Barta's residence. Drug Enforcement Administration (DEA) agents tested two seized pills and learned the active ingredients were fentanyl and fentanyl 4-ANPP. On December 20, 2020, DEA agents executed a search warrant at Barta's residence in Omaha. During the search, agents found more pills and a pill grinder. They also found a Smith & Wesson M&P 9mm handgun, a Taurus Millennium G2, and a Mossberg 342KA rifle inside a locked safe in Barta's house. Barta told DEA agents that he had purchased 100 oxycodone pills from a vendor on the darkweb for $800 in Bitcoin. He said he had completed ten orders of between 60 and 80 pills per order. The report said Barta told investigators he ordered 100 oxycodone 30 mg pills from a dark web vendor in exchange for $800 and that he had made approximately ten prior orders of about 60 to 80 pills per order. Barta reported to the police that he took three pills daily to manage his chronic neck pain. In one court document, Barta's attorney provided some background on Barta's oxycodone purchases: "Mr. Barta suffers from chronic pain due a neck injury. Mr. Barta was under the care of a doctor for the pain, which ultimately led to a dependence on oxycodone. Despite being prescribed Duloxetine, it was not the proper amount for this pain. Mr. Barta sought oxycodone on the dark web for his personal use. He did not order an amount over a personal use amount, and thankfully was not killed when the oxycodone pills were later discovered to be fentanyl […].” "Mr. Barta finds himself before this Court on charges brought over a year after his law enforcement contact. Even though he was not arrested on December 20, 2020, Mr. Barta used the contact as a wakeup call, and immediately sought treatment. He did not wait for Christmas to be over; instead, he went to treatment and missed spending the holidays with his children. He is under the care of a treating physician who increased the Duloxetine to an amount in which gives Mr. Barta relief from pain. Mr. Barta continues to abstain from opioids.” In February 2021, a federal grand jury returned an indictment accusing Barta of possessing a firearm as a drug user. Although Barta entered a guilty plea, his attorney wrote that Barta did not know he had violated any laws by possessing firearms. "Mr. Barta did not know it was unlawful to be in possession of the firearms, and there is no evidence that Mr. Barta ever used the firearms. Mr. Barta had the firearms in locked cases and never discharged them.” Arguing for a base level reduction of eight points, Barta's attorney wrote that Barta's firearms were "solely possessed for collection purposes.” Interesting choices for collectors firearms. I will say that.

At least he is not collecting Hi-Points Chief Judge Robert F. Rossiter, Jr. sentenced Barta to 18 months without special conditions. Pretty decent outcome for Barta. He failed two drug tests for THC during pretrial release. Mr. Barta has been extremely successful on pretrial release. He had two (2) positive tests from taking Delta 8. When he failed the urine test, he stopped taking Delta 8, and had negative tests after the Delta 8 was no longer in his system. He completed treatment before these charges were even filed and is maintaining his sobriety. He has shown over a year of adhering to the court's orders and success. He realizes his addiction is life threatening and lifelong. He takes his sobriety seriously and would request a term of probation without

incarceration. Is the court simply accepting the attorney's statement as factual or can a lab actually differentiate between Delta 8 and Delta 9? Omaha Man sentenced to probation for possessing firearms as a drug user | archive.is, archive.org, rivercountry.newschannelnebraska.com Indictment pdf (via darknetlive.com at https://darknetlive.com/post/omaha-man-sentenced-to-probation-for-buying-oxys-on-darkweb/)

VPN Providers in India Required to Keep Logs Under New Law

VPN Providers with servers in India are required to maintain logs of customer names, I.P. addresses, and usage patterns. As of June 27, 2022, data centers, virtual private server (VPS) providers, cloud service providers, and virtual private network (VPN) service providers must comply with new data retention regulations. Service providers are required to maintain logs for five years with the following pieces of information: Validated names of subscribers/customers hiring the services Period of hire, including dates I.P.s allotted to / being used by the members Email address and I.P. address, and time stamp used at the time of registration / on-boarding The purpose for hiring services Validated address and contact numbers Ownership pattern of the subscribers/customers hiring services The Indian Computer Emergency Response Team (CERT-In) directive includes similar requirements for virtual asset service providers, virtual asset exchange providers, and custodian wallet providers. Exchanges and custodial wallet providers are required to maintain all Know Your Customer (KYC) information and records of financial transactions for five years.

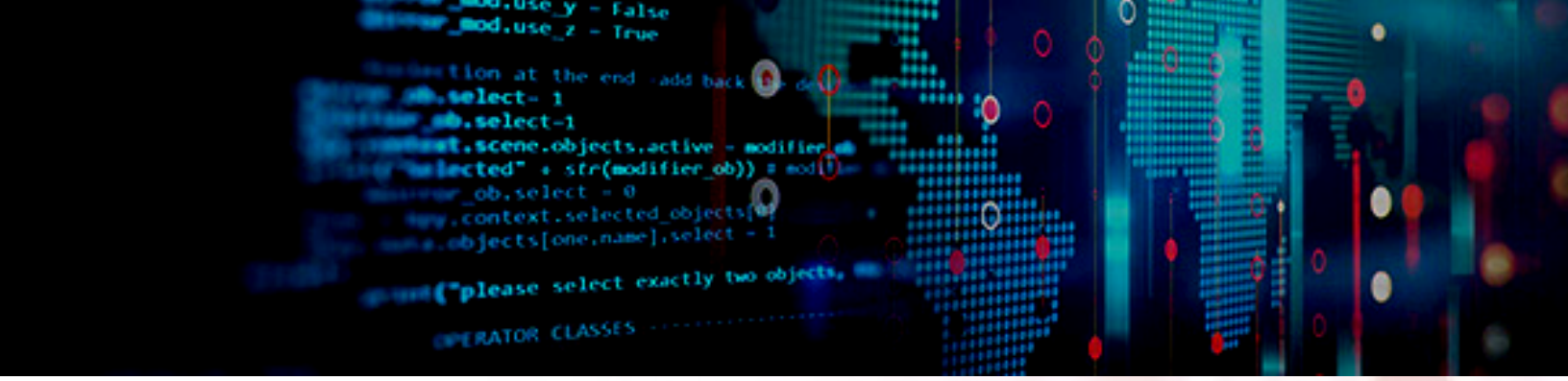
Arnab Goswami often hosts entertaining debates about topics relevant to India. Lots of yelling. In response to the regulations, some VPN providers have removed their servers in India. ExpressVPN: "Rest assured, our users will still be able to connect to VPN servers that will give them Indian I.P. addresses and allow them to access the internet as if they were located in India. These "virtual” India servers will instead be physically located in Singapore and the U.K.” "In terms of the user experience, there is minimal difference. For anyone wanting to connect to an Indian server, simply select the VPN server location "India (via Singapore)” or "India (via the U.K.).” "Virtual server locations are not new to ExpressVPN; in fact, we have been operating our "India (via the U.K.)” server location for several years. With virtual locations, the registered I.P. address matches the country you have chosen to connect to, while the server is physically located in another country. Virtual locations are used, where necessary, to provide faster, more reliable connections.” Mullvad, which is one of the most well-known and trusted VPN providers in the industry, added a section to its FAQ: There is a law to collect user data in India and other countries. Does this affect Mullvad? "Mullvad does not collect user data. Mullvad is based in Sweden and none of the Swedish regulations (https://mullvad.net/help/swedish-legislation/) can force VPN providers to secretly collect traffic-related data. We also have no servers, infrastructure or staff in India.” CERT-In Directions pdf (via darknetlive.com at https://darknetlive.com/post/vpn-services-in-india-required-to-maintain-logs/)

Drug Traffickers Are Increasingly Using Crypto in China

Although China's anti-drug measures have been generally successful, authorities have seen an increase in drug traffickers' use of the internet and cryptocurrencies. In 2021, China's anti-drug departments "earnestly implemented” General Secretary Xi Jinping's instructions on reducing illicit drug use. The measures have resulted in success by most standards. Although drug crimes and drug abuse have generally decreased, the Chinese government has noted an increase in drug money laundering via cryptocurrencies. In addition, people are increasingly turning to the internet to buy and sell drugs. General Figures By the end of 2021, there were 1.486 million drug users in China, down 17.5% from 2020; After three years of abstinence, 3.403 million people had relapsed, up 13.4% since 2020; 121,000 people used drugs for the first time, down 21.7% year on year; The number of existing drug abusers and newly discovered drug abusers decreased for five consecutive years; Among existing drug users, 556,000 abused heroin, 793,000 methamphetamine, 37,000 ketamine and 18,000 marijuana, down 19%, 18.5%, 9% and 10.7% respectively; Foreign suppliers account for the majority of drugs seized; Police seized 17.3 tons of methamphetamine, ketamine, and other "mainstream drugs,” of which 15.3 tons came from overseas and two tons from domestic manufacturers, down 21.7% and 48.2%, respectively; Police seized 690 kilograms of cocaine from South America in 2021. Cocaine seizures increased by 18.6%; People are importing more marijuana from North America. Police seized 308.9 kilograms of marijuana which is an increase, an increase of 4.5 times the amount of marijuana seized in 2020.

Most of the seized marijuana was found in mail packages shipped from the United States; Police destroyed 123 drug production sites and seized 1.2 tons of drugs at those sites, decreasing 26.4% and 89%, respectively; and "The circulation of drug funds has expanded from online bank transfers to cryptocurrency and in-game currency,” per the report. __ "neither fear hardship nor death” Postal System _ According to the report, the decrease in domestically available drugs changed how drug traffickers operated. Traditional methods of drug trafficking decreased while the use of the postal system and waterways increased. People used the internet to buy drugs more frequently than in previous years, although the report did not reveal the size of the increase. Internet-Based Drug Trafficking _ Police arrested 0.8 million people and seized 0.5 tons of drugs in connection with online drug trafficking, accounting for 10.4% and 2% of the national total. Of the 800,000 arrests, authorities secured only 500,000 convictions. Cryptocurrencies _ As the online drug market expands, people are increasingly using cryptocurrencies, game coins, and other online payment methods to pay or receive drug payments. According to the report's conclusion, China's anti-drug sector will continue to adapt to the changes in the drug trafficking environment. Targeting internet-based drug trafficking is one of the sector's top priorities. China Drug Crime Report 2021 | archive.org, nncc626.com (via darknetlive.com at https://darknetlive.com/post/china-sees-spike-in-online-drug-activity/)

Dark Web Link



Trend Micro Anti-Malware Blog

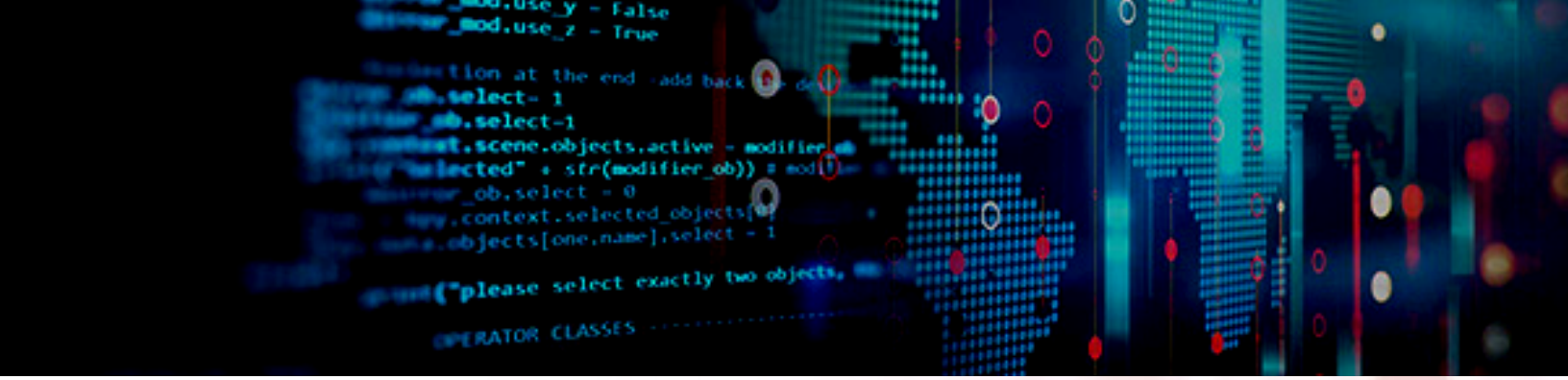
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

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

FireEye

* Metasploit Weekly Wrap-Up
* Rapid7 Belfast Recognized for "Company Connection" During COVID-19 Pandemic
* [The Lost Bots] Season 2, Episode 1: SIEM Deployment in 10 Minutes
* Application Security in 2022: Where Are We Now?
* For Ransomware Double-Extorters, It's All About the Benjamins - and Data From Healthcare and Pharma
* CVE-2021-3779: Ruby-MySQL Gem Client File Read (FIXED)
* API Security: Best Practices for a Changing Attack Surface
* Metasploit Weekly Wrap-Up
* Velociraptor Version 0.6.5: Table Transformations, Multi-Lingual Support, and Better VQL Error-Handli
* CVE-2022-31749: WatchGuard Authenticated Arbitrary File Read/Write (Fixed)



Advisories

US-Cert Alerts & bulletins

* CISA Adds One Known Exploited Vulnerability to Catalog
* #StopRansomware: MedusaLocker
* Mozilla Releases Security Updates for Firefox, Firefox ESR, and Thunderbird
* CISA Releases Guidance on Switching to Modern Auth in Exchange Online before October 1
* 2022 CWE Top 25 Most Dangerous Software Weaknesses
* CISA Adds Eight Known Exploited Vulnerabilities to Catalog
* Citrix Releases Security Updates for Hypervisor
* Malicious Cyber Actors Continue to Exploit Log4Shell in VMware Horizon Systems
* AA22-181A: #StopRansomware: MedusaLocker
* AA22-174A: Malicious Cyber Actors Continue to Exploit Log4Shell in VMware Horizon Systems
* Vulnerability Summary for the Week of June 20, 2022
* Vulnerability Summary for the Week of June 13, 2022

Zero Day Initiative Advisories

Packet Storm Security - Latest Advisories

Red Hat Security Advisory 2022-5481-01

Red Hat Security Advisory 2022-5481-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.11 ESR. Issues addressed include bypass, integer overflow, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-5245-01

Red Hat Security Advisory 2022-5245-01 - The curl packages provide the libcurl library and the curl utility for downloading files from servers using various protocols, including HTTP, FTP, and LDAP. Issues addressed include bypass and password leak vulnerabilities.

Red Hat Security Advisory 2022-5475-01

Red Hat Security Advisory 2022-5475-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.11. Issues addressed include bypass, integer overflow, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-5257-01

Red Hat Security Advisory 2022-5257-01 - libinput is a library that handles input devices for display servers and other applications that need to directly deal with input devices. Issues addressed include format string and privilege escalation vulnerabilities.

Red Hat Security Advisory 2022-5439-01

Red Hat Security Advisory 2022-5439-01 - The redhat-virtualization-host packages provide the Red Hat Virtualization Host. These packages include redhat-release-virtualization-host. Red Hat Virtualization Hosts are installed using a special build of Red Hat Enterprise Linux with only the packages required to host virtual machines. RHVH features a Cockpit user interface for monitoring the host's resources and performing administrative tasks. Issues addressed include heap overflow, privilege escalation, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-5249-01

Red Hat Security Advisory 2022-5249-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include buffer overflow, information leakage, privilege escalation, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-5251-01

Red Hat Security Advisory 2022-5251-01 - The pcre2 package contains a new generation of the Perl Compatible Regular Expression libraries for implementing regular expression pattern matching using the same syntax and semantics as Perl. Issues addressed include an out of bounds read vulnerability.

Red Hat Security Advisory 2022-5244-01

Red Hat Security Advisory 2022-5244-01 - Expat is a C library for parsing XML documents. Issues addressed include an integer overflow vulnerability.

Red Hat Security Advisory 2022-5479-01

Red Hat Security Advisory 2022-5479-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.11 ESR. Issues addressed include bypass, integer overflow, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-5476-01

Red Hat Security Advisory 2022-5476-01 - This is a kernel live patch module which is automatically loaded by the RPM post-install script to modify the code of a running kernel. Issues addressed include buffer overflow, privilege escalation, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-5263-01

Red Hat Security Advisory 2022-5263-01 - Kernel-based Virtual Machine is a full virtualization solution for Linux on a variety of architectures. The qemu-kvm packages provide the user-space component for running virtual machines that use KVM. Issues addressed include a memory leak vulnerability.

Red Hat Security Advisory 2022-5482-01

Red Hat Security Advisory 2022-5482-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This

update upgrades Thunderbird to version 91.11. Issues addressed include bypass, integer overflow, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-5242-01

Red Hat Security Advisory 2022-5242-01 - Vim is an updated and improved version of the vi editor. Issues addressed include buffer over-read, buffer overflow, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-5474-01

Red Hat Security Advisory 2022-5474-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.11 ESR. Issues addressed include bypass, integer overflow, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-5480-01

Red Hat Security Advisory 2022-5480-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.11. Issues addressed include bypass, integer overflow, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-5250-01

Red Hat Security Advisory 2022-5250-01 - The libxml2 library is a development toolbox providing the implementation of various XML standards. Issues addressed include integer overflow and out of bounds write vulnerabilities.

Red Hat Security Advisory 2022-5252-01

Red Hat Security Advisory 2022-5252-01 - The libarchive programming library can create and read several different streaming archive formats, including GNU tar, cpio, and ISO 9660 CD-ROM images. Libarchive is used notably in the bsdtar utility, scripting language bindings such as python-libarchive, and several popular desktop file managers. Issues addressed include an out of bounds read vulnerability.

Ubuntu Security Notice USN-5499-1

Ubuntu Security Notice 5499-1 - Florian Kohnhuser discovered that curl incorrectly handled returning a TLS server's certificate chain details. A remote attacker could possibly use this issue to cause curl to stop responding, resulting in a denial of service. Harry Sintonen discovered that curl incorrectly handled certain FTP-KRB messages. An attacker could possibly use this to perform a machine-in-the-middle attack.

Red Hat Security Advisory 2022-5467-01

Red Hat Security Advisory 2022-5467-01 - PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server. Issues addressed include a buffer overflow vulnerability.

Red Hat Security Advisory 2022-5316-01

Red Hat Security Advisory 2022-5316-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include buffer overflow, memory leak, and out of bounds read vulnerabilities.

Red Hat Security Advisory 2022-5317-01

Red Hat Security Advisory 2022-5317-01 - The libxml2 library is a development toolbox providing the implementation of various XML standards. Issues addressed include integer overflow and out of bounds write vulnerabilities.

Red Hat Security Advisory 2022-5470-01

Red Hat Security Advisory 2022-5470-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.11. Issues addressed include bypass, integer overflow, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-5472-01

Red Hat Security Advisory 2022-5472-01 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.11 ESR. Issues addressed include bypass, integer overflow, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-5471-01

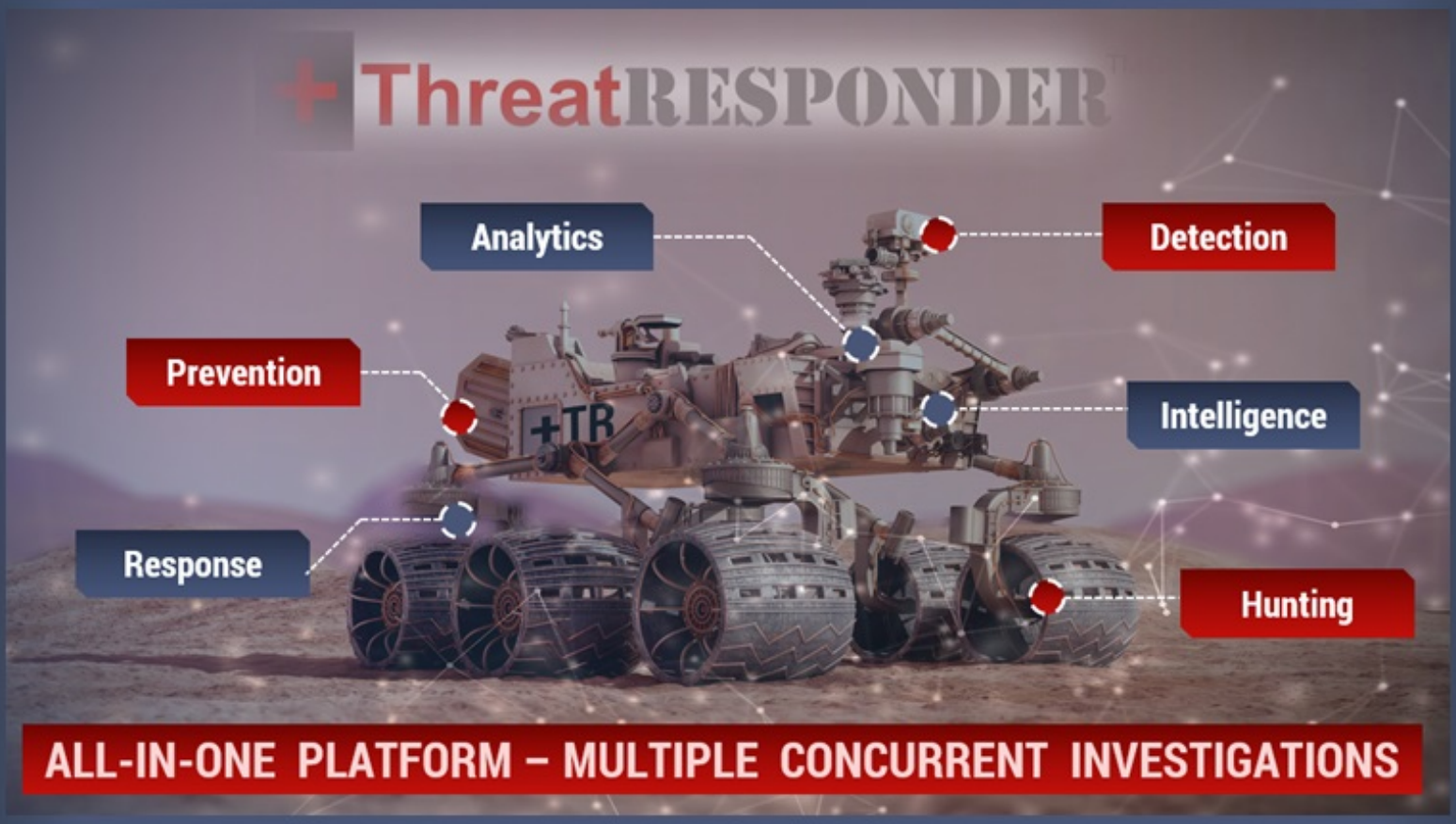
Red Hat Security Advisory 2022-5471-01 - PHP is an HTML-embedded scripting language commonly used with the Apache HTTP Server. Issues addressed include a buffer overflow vulnerability.

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



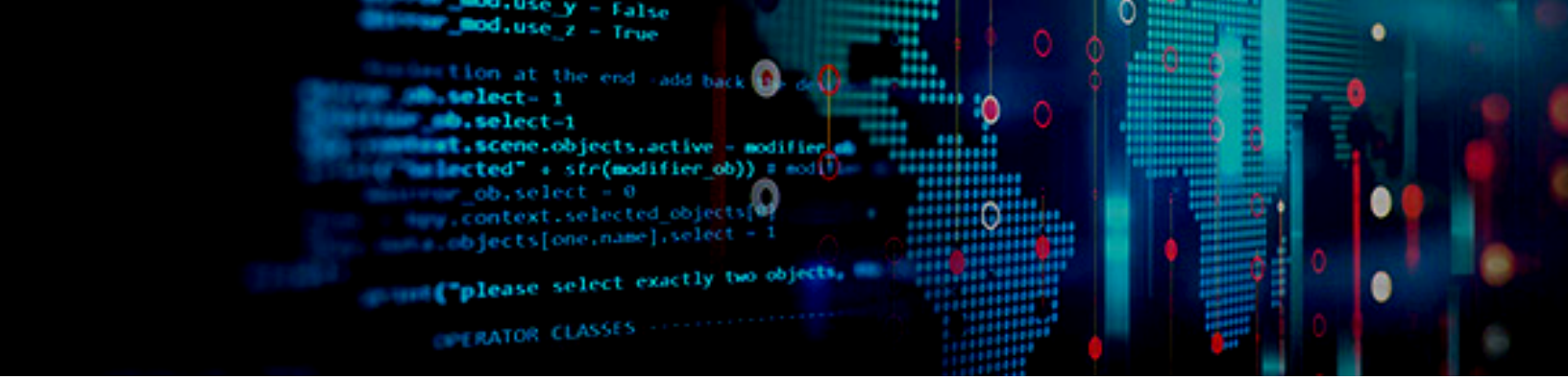
The Solution – ThreatResponder® Platform

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

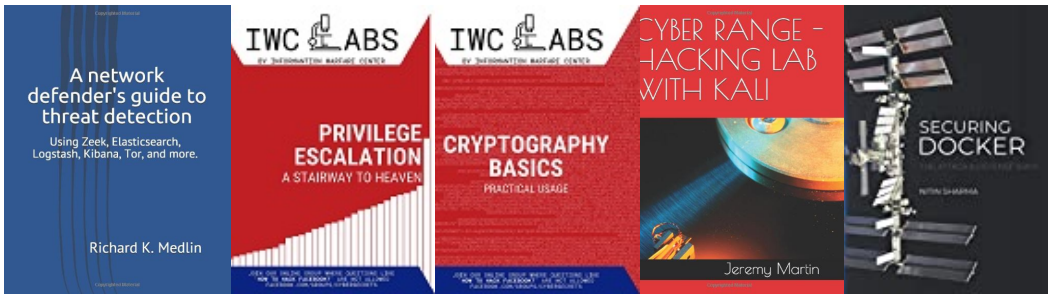


The Cyber Secrets publications on Amazon

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.

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