Feb-22-22

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

February 22, 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

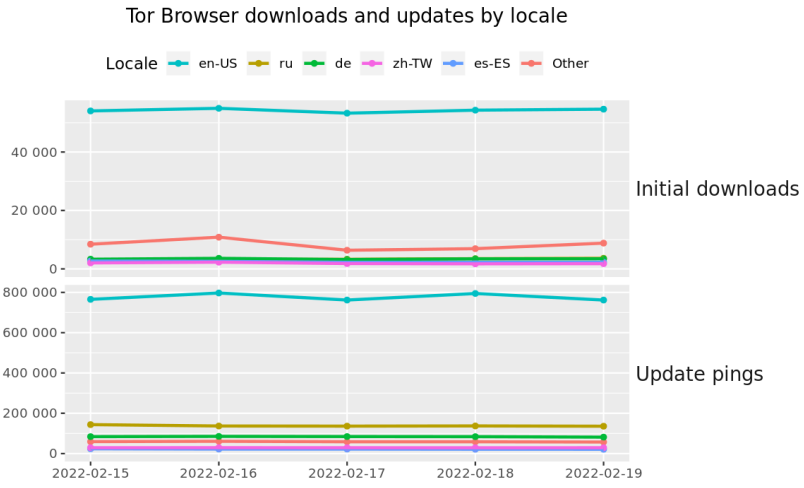
Internet Storm Center Infocon Status

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

* Security Spend To Reach $1 Billion In Brazil In 2022
* US To Attack Cyber Criminals First, Ask Questions Later
* Linux Snap Package Tool Fixes Make-Me-Root Bugs
* Hacker Uses Phishing Attack To Steal $1.7 Million In NFTs From OpenSea Users
* WTF Is Our Most Critical Cybersecurity Resource? And How Can We Preserve It?
* Severe WordPress Plug-In UpdraftPlus Bug Threatens Backups
* Baby Goland-Based Botnet Already Pulling In $3k/Month For Operators
* VMware Horizon Servers Are Under Attack By Iranian State Hackers
* New RCE Flaw Added To Adobe Security Advisory
* Taiwan Cracks Down On China Spying On Tech Firms
* Thanks, Dad: Jammer Used To Stop Kids Going Online, Wipes Out A Town's Internet By Mistake
* US Says Russian State Actors Lurked In Defense Contractor Networks For Months
* Google Expands Privacy Sandbox To Android
* Businessman Admits To Working As Spyware Broker In US / Mexico
* Microsoft Teams Targeted With Takeover Trojans
* How The Initial Access Broker Market Leads To Ransomware Attacks
* Right Wingers Try To Spin DNS Traffic Logged As Intercepting Emails
* Critical VMware Bugs Open ESXi, Fusion, Workstation To Attackers
* Emotet Now Spreading Through Malicious Excel Files
* Chinese MI6 Informant Gives Information About Huawei
* Linux Kernel Patches Remote Stack Overflow Bug
* EU To Launch Probe Over Use Of Cloud Services By Public Sector
* Google To Pay Up To $91,337 For Exploits Of New Linux And Kubernetes Bugs
* TA2541: APT Has Been Shooting RATs At Aviation For Years
* GitBleed - Finding Secrets In Mirrored Git Repositories

Krebs on Security

* Red Cross Hack Linked to Iranian Influence Operation?
* Wazawaka Goes Waka Waka
* Russian Govt. Continues Carding Shop Crackdown
* Microsoft Patch Tuesday, February 2022 Edition
* IRS To Ditch Biometric Requirement for Online Access
* How Phishers Are Slinking Their Links Into LinkedIn
* Fake Investor John Bernard Sinks Norwegian Green Shipping Dreams
* Who Wrote the ALPHV/BlackCat Ransomware Strain?
* Scary Fraud Ensues When ID Theft & Usury Collide
* Crime Shop Sells Hacked Logins to Other Crime Shops

Dark Reading

* Open Source Code: The Next Major Wave of Cyberattacks
* Key Application Security Metrics Show Few Signs of Improvement
* Why You Need An Adversary-First Approach to Threats in the Cloud
* Free Cybersecurity Tools and Services List Published by CISA
* Axiomatics Introduces Orchestrated Authorization
* Ukraine DDoS: 'Cyberattack' or Not?
* Enterprises Look Beyond Antivirus Software for Remote Workers
* Ransomware Adds New Wrinkle in Russian Cybercrime Market
* If the Cloud Is More Secure, Then Why Is Everything Still Broken?
* NSA Issues Guidance for Selecting Strong Cisco Password Types
* Confluera Cloud Research Finds Cybersecurity Concern as Biggest Obstacle to Cloud and Multicloud Adop
* Darktrace Artificial Intelligence Stops Cyberattack at Italian Electronics Distributor
* Attackers Hone Their Playbooks, Become More Agile
* Neustar Security Services Report Highlights Shifts in Threat Landscape Amid Maturing Cybercrime Econo
* Security Teams Expect Attackers to Go After End Users First
* Software-Developer Security Vendor Snyk Buys Cloud Security Company
* 4 Keys to Bridging the Gap Between Security and Developers
* How to Fight Tomorrow's Novel Software Supply Chain Attacks
* Russian Actors Targeting US Defense Contractors in Cyber Espionage Campaign, CISA Warns
* How Proactive Threat Hunting Redefines the Zero-Day

The Hacker News

* Chinese Hackers Target Taiwan's Financial Trading Sector with Supply Chain Attack
* Hackers Backdoor Unpatched Microsoft SQL Database Servers with Cobalt Strike
* New Android Banking Trojan Spreading via Google Play Store Targets Europeans
* Iranian State Broadcaster IRIB Hit by Destructive Wiper Malware
* A Free Solution to Protect Your Business from 6 Biggest Cyber Threats in 2022
* Hackers Exploiting Infected Android Devices to Register Disposable Accounts
* Master Key for Hive Ransomware Retrieved Using a Flaw in its Encryption Algorithm
* Justice Department Appoints First Director of National Cryptocurrency Enforcement Team
* U.S. Cybersecurity Agency Publishes List of Free Security Tools and Services
* Critical Flaw Uncovered in WordPress Backup Plugin Used by Over 3 Million Sites
* Microsoft Warns of 'Ice Phishing' Threat on Web3 and Decentralized Networks
* PseudoManuscrypt Malware Spreading the Same Way as CryptBot Targets Koreans
* New Linux Privilege Escalation Flaw Uncovered in Snap Package Manager
* Iranian Hackers Targeting VMware Horizon Log4j Flaws to Deploy Ransomware
* 4 Cloud Data Security Best Practices All Businesses Should Follow Today

Security Week

* Mobile Malware Attacks Dropped in 2021 but Sophistication Increased
* Webinar Today: Highly Evasive Adaptive Threats (HEAT)
* Cookware Distribution Giant Meyer Discloses Data Breach
* Israeli Probe Finds Police Spied on Citizen With Pegasus
* SynSaber Launches Palm-Sized Threat Sensor for OT Environments
* Beyond Identity Becomes Unicorn With $100 Million Series C Funding Round
* Wiper Used in Attack on Iran National Media Network
* Coinbase Pays $250K for 'Market-Nuking' Security Flaw
* Researchers Devise Method to Decrypt Hive Ransomware-Encrypted Data
* At Olympics, Cybersecurity Worries Linger in Background
* CISA Warns Critical Infrastructure Organizations of Foreign Influence Operations
* Conti Ransomware 'Acquires' TrickBot as It Thrives Amid Crackdowns
* Vulnerability in UpdraftPlus Plugin Exposed Millions of WordPress Site Backups
* European Cybersecurity Agencies Issue Resilience Guidance for Decision Makers
* US, Britain Accuse Russia of Cyberattacks Targeting Ukraine
* CISA Creates List of Free Cybersecurity Tools and Services for Defenders
* Fast-Growing Golang-Based 'Kraken' Botnet Emerges
* Microsoft Teams Abused for Malware Distribution in Recent Attacks
* Patch for Actively Exploited Flaw in Adobe Commerce and Magento Bypassed
* NSA Provides Guidance on Cisco Device Passwords
* VMware NSX Data Center Flaw Can Expose Virtual Systems to Attacks
* Google Introduces 'Privacy Sandbox' for Ads on Android
* Intel Software and Firmware Updates Patch 18 High-Severity Vulnerabilities
* Are You Prepared for 2022's More Destructive Ransomware?
* FBI Warns of BEC Scams Abusing Virtual Meeting Platforms

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* New Phishing Campaign Angles for Monzo Banking Customers
* 20 Year-Old "Right-to-Left Override" Functionality Used in Attacks to Trick Microsoft 365 Users Out o
* New QBot Attack Only Takes 30 Minutes to Elevate Privileges and Steal Data
* Phishing Campaign Targets NFT Speculators
* [Heads Up] There Is A Whole New Type of Blockchain Scam Called "Ice phishing"
* Conti Ransomware Attacks Reap in $180 Million in 2021 as Average Ransomware Payments Rise by 34%
* Coinbase's QR Code Superbowl Ad Only Helps Normalize QR-Based Scams
* Scammers Use a Mix of Stolen Credentials, Inbox Rules, and a Rogue Outlook Client Install to Phish In
* Traits of Most Scams
* Phishing Attacks on Social Media Doubled Over 2021

ISC2.org Blog

* (ISC)² PULSE SURVEY: LOG4J REMEDIATION EXPOSES REAL-WORLD TOLL OF THE CYBERSECURITY WORKFORCE GA
* New Report by U.K. NCSC Highlights the Impact of Diversity on the Cybersecurity Workforce
* HOW TO TAKE THE CISSP EXAM ONLINE - REGISTRATION IS OPEN!
* Celebrating the Black History of Cybersecurity
* WANT TO SPEAK AT (ISC)² SECURITY CONGRESS 2022? THE CALL FOR SPEAKERS IS NOW OPEN

HackRead

* Kids luxury clothing store Melijoe exposed 200GB of customers' data
* CISA Publishes List of Free Cybersecurity Tools and Services
* Phishing scam: NFTs Worth $1.7M Stolen from OpenSea Users
* Kraken botnet bypass Windows Defender to steal crypto wallet data
* Croatian Police arrests minor over A1 Telecom data breach & ransom demand
* Hackers are using Microsoft Teams chat to spread malware
* Man pleads guilty to selling WhatsApp hacking tool, Signal Jammers & StingRays

Koddos

* Kids luxury clothing store Melijoe exposed 200GB of customers' data
* CISA Publishes List of Free Cybersecurity Tools and Services
* Phishing scam: NFTs Worth $1.7M Stolen from OpenSea Users
* Kraken botnet bypass Windows Defender to steal crypto wallet data
* Croatian Police arrests minor over A1 Telecom data breach & ransom demand
* Hackers are using Microsoft Teams chat to spread malware
* Man pleads guilty to selling WhatsApp hacking tool, Signal Jammers & StingRays

Naked Security

* French speakers blasted by sextortion scams with no text or links
* Irony alert! PHP fixes security flaw in input validation code
* S3 Ep70: Bitcoin, billing blunders, and 0-day after 0-day after 0-day [Podcast + Transcript]
* VMware fixes holes that could allow virtual machine escapes
* Google announces zero-day in Chrome browser - update now!
* Adobe fixes zero-day exploit in e-commerce code: update now!
* Power company pays out $3 trillion compensation to astonished customer
* Apple zero-day drama for Macs, iPhones and iPads - patch now!
* S3 Ep69: WordPress woes, Wormhole holes, and a Microsoft change of heart [Podcast + Transcript]
* Self-styled "Crocodile of Wall Street" arrested with husband over Bitcoin megaheist

Threat Post

* NFT Investors Lose $1.7M in OpenSea Phishing Attack
* New Critical RCE Bug Found in Adobe Commerce, Magento
* Severe WordPress Plug-In UpdraftPlus Bug Threatens Backups
* Iranian State Broadcaster Clobbered by 'Clumsy, Buggy' Code
* Baby Golang-Based Botnet Already Pulling in $3K/Month for Operators
* Ukrainian DDoS Attacks Should Put US on Notice-Researchers
* Microsoft Teams Targeted With Takeover Trojans
* Kill Cloud Risk: Get Everybody to Stop Fighting Over App Security - Podcast
* TrickBot Ravages Customers of Amazon, PayPal and Other Top Brands
* Massive LinkedIn Phishing, Bot Attacks Feed on the Job-Hungry

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

* The lowdown on low code and no code in the cloud
* Building and running microservices at scale: A CTO's view
* Vercel, Netlify, and the new era of serverless PaaS
* 5 reasons software architects should embrace low code
* TypeScript usage growing by leads and bounds - report
* Why open source is essential in a cloud era
* Microsoft .NET 7 zeroes in on containers and cloud
* What is OLTP? The backbone of ecommerce
* IT spending will be mostly cloud soon. Are you ready?
* Rust language is fun but challenging - survey

C4ISRNET - Media for the Intelligence Age Military

* Cross-Domain Technologies Are the Key to JADC2
* White House accuses Russia of cyberattacks targeting Ukraine
* Navy doesn't want to keep guessing whether its information warfare systems work
* Ukraine, UK, Poland announce security pact amid heightened tensions
* US Space Force aims for more resilient architecture by 2026
* Unmanned or minimally manned vessels could deploy alongside strike groups as soon as 2027
* CISA accuses Russia-backed hackers of stealing info from U.S. defense contractors
* Gilday calls for more collaboration with allies on operations, tech development
* Submarine maintenance backlogs and delays take toll on fleet's development work at sea
* US Army tests mobile communications gear for armored units

The Hacker Corner

Conferences

* Our New Approach To Conference Listings
* Marketing Cybersecurity In 2022
* Cybersecurity Employment Market
* Cybersecurity Marketing Trends
* Is It Worth Public Speaking?
* Our Guide To Cybersecurity Marketing Campaigns
* How To Choose A Cybersecurity Marketing Agency
* The Hybrid Conference Model
* Best Ways To Market A Conference
* Marketing To Cybersecurity Companies

Google Zero Day Project

* A walk through Project Zero metrics
* Zooming in on Zero-click Exploits

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.

* SUSCTF 2022
* TSJ CTF 2022
* Ugra CTF Quals 2022
* Codegate CTF 2022 Preliminary
* D^3CTF 2022
* FooBar CTF 2022
* DaVinciCTF 2022
* UTCTF 2022
* picoCTF 2022
* zer0pts 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

* OpenStego Free Steganography Solution 0.8.4
* TestSSL 3.0.7
* Collabfiltrator 2.1
* Wireshark Analyzer 3.6.2
* nfstream 6.4.2
* nfstream 6.4.1
* GNU Privacy Guard 2.2.34
* TOR Virtual Network Tunneling Tool 0.4.6.10
* Scanmycode Community Edition
* Hydra Network Logon Cracker 9.3

Kali Linux Tutorials

* Spray365 : Makes Spraying Microsoft Accounts Through Two-Step Password Spraying Approach
* SQLbit : Just Another Script For Automatize Boolean-Based Blind SQL Injectionsv
* Mesh-Kridik : An Open-Source Security Checker That Performs Security Checks On A Kubernetes Cluster
* Web Cache Vulnerability Scanner : A Go-based CLI Tool For Testing Web Cache Poisoning
* MUI : A GUI Plugin For Binary Ninja To Interact And View The Progress Of Manticore
* ￼How To Get The User Manuals Of Popular Xiaomi Products
* Umay : IoT Malware Similarity Analysis Platform
* MultiPotato : Another Potato to get SYSTEM via SeImpersonate privileges
* TrojanSourceFinder : Help Find Trojan Source Vulnerability In Code
* Mariana Trench : Security Focused Static Analysis Tool For Android And Java Applications

GBHackers Analysis

* VMware Issues Patches for Shell Injection and Privilege Vulnerability
* Critical Magento 0-Day Let Attackers Execute Arbitrary Code
* ACTINIUM Hackers Group Targeting Government, Military, NGO to Steal Sensitive Data
* ESET Antivirus Flaw Let Attackers to Escalate Privileges & Execute Arbitrary Code
* How To Protect Your Business From Hackers

Weekly Cyber Security Video and Podcasts

SANS DFIR

* SANS Threat Analysis Rundown
* Network Forensics: Tools of the Trade… At Scale and on a Budget
* You Get What You Ask For: Building Intelligent Teams for CTI Success - CTI Summit 2022
* SANS Threat Analysis Rundown

Defcon Conference

* DEF CON 29 Recon Village - Anthony Kava - GOV Doppelgänger Your Häx Dollars at Work
* DEF CON 29 Red Team Village - CTF Day 2
* DEF CON 29 Recon Village - Ben S - Future of Asset Management
* DEF CON 29 Recon Village - Ryan Elkins - How to Build Cloud Based Recon Automation at Scale

Hak5

* Hacking Stay-Logged-In Cookies with Owasp Zap | HakByte
* Online Card Skimmers Hit E-Commerce, Two Arrested For Allegedly Laundering Bitcoin - ThreatWire
* How Hackers Use PwnKit to Get Root Access in Seconds

The PC Security Channel [TPSC]

* Standard vs Admin User: Ransomware Test
* Malwarebytes 2022: Test vs Malware

Eli the Computer Guy

* Black Lives Matter is a Fraud
* Security System Installed - Cancel YouTube, Subscribe to Life
* Facebook is Dead
* Canadian Freedom Convoy Created a Transnational Revolution

Security Now

* InControl - PHP Everywhere, Magento Emergency, Project Zero Stats, Goodbye WMIC, SeriousSAM
* The Inept Panda - China Olympics, SAMBA CVS 9.9 Vulnerability, Microsoft Office 3rd Party Macros

Troy Hunt

* Weekly Update 283

Intel Techniques: The Privacy, Security, & OSINT Show

* 251-Six Important Show Updates
* 250-Consequences of Product Refunds

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Chrome RenderFrameHostImpl Use-After-Free
* Cyclades Serial Console Server 3.3.0 Privilege Escalation
* Simple Real Estate Portal System 1.0 SQL Injection
* Microweber 1.2.11 Shell Upload
* Dbltek GoIP GHSFVT-1.1-67-5 Local File Inclusion
* FileCloud 21.2 Cross Site Request Forgery
* WordPress Perfect Survey 1.5.1 SQL Injection
* WordPress WP User Frontend 3.5.25 SQL Injection
* Thinfinity VirtualUI 2.5.26.2 Information Disclosure
* Thinfinity VirtualUI 2.5.41.0 IFRAME Injection
* Auto Spare Parts Management 1.0 SQL Injection
* HMA VPN 5.3 Unquoted Service Path
* Microsoft Gaming Services 2.52.13001.0 Unquoted Service Path
* Cab Management System 1.0 SQL Injection
* Cab Management System 1.0 Remote Code Execution
* WordPress MasterStudy LMS 2.7.5 Account Creation
* WordPress dzs-zoomsounds 6.60 Shell Upload
* Fortinet Fortimail 7.0.1 Cross Site Scripting
* Hotel Druid 3.0.3 Remote Code Execution
* Cosmetics And Beauty Product Online Store 1.0 SQL Injection
* Cosmetics And Beauty Product Online Store 1.0 Cross Site Scripting
* TOSHIBA DVD PLAYER Navi Support Service 1.00.0000 Unquoted Service Path
* Bluetooth Application 5.4.277 Unquoted Service Path
* File Santizer For HP ProtectTools 5.0.1.3 Unquoted Service Path
* Intel Management Engine Components 6.0.0.1189 Unquoted Service Path

CXSecurity

* Servisnet Tessa MQTT Credentials Dump (Unauthenticated) (Metasploit)
* Hotel Druid 3.0.3 Remote Code Execution
* Tiny File Manager 2.4.3 Shell Upload
* Ignition Remote Code Execution
* Nagios XI Autodiscovery Shell Upload
* Grandstream GXV31XX settimezone Unauthenticated Command Execution
* Strapi CMS 3.0.0-beta.17.4 Privilege Escalation

Proof of Concept (PoC) & Exploits

Exploit Database

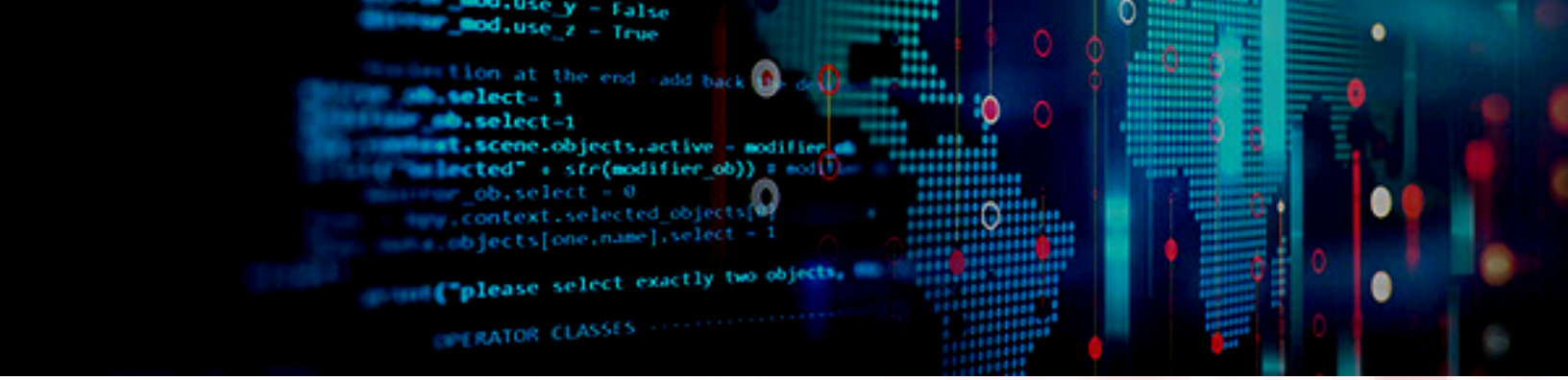
* [local] Microsoft Gaming Services 2.52.13001.0 - Unquoted Service Path
* [webapps] Dbltek GoIP - Local File Inclusion
* [webapps] FileCloud 21.2 - Cross-Site Request Forgery (CSRF)
* [local] Cyclades Serial Console Server 3.3.0 - Local Privilege Escalation
* [webapps] WordPress Plugin WP User Frontend 3.5.25 - SQLi (Authenticated)
* [webapps] Thinfinity VirtualUI 2.5.26.2 - Information Disclosure
* [webapps] Thinfinity VirtualUI 2.5.41.0 - IFRAME Injection
* [webapps] Cab Management System 1.0 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Microweber 1.2.11 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Cab Management System 1.0 - 'id' SQLi (Authenticated)
* [webapps] WordPress Plugin Perfect Survey - 1.5.1 - SQLi (Unauthenticated)
* [local] HMA VPN 5.3 - Unquoted Service Path
* [local] Connectify Hotspot 2018 'ConnectifyService' - Unquoted Service Path
* [local] File Sanitizer for HP ProtectTools 5.0.1.3 - 'HPFSService' Unquoted Service Path
* [local] Intel(R) Management Engine Components 6.0.0.1189 - 'LMS' Unquoted Service Path
* [local] Bluetooth Application 5.4.277 - 'BlueSoleilCS' Unquoted Service Path
* [local] TOSHIBA DVD PLAYER Navi Support Service - 'TNaviSrv' Unquoted Service Path
* [webapps] Fortinet Fortimail 7.0.1 - Reflected Cross-Site Scripting (XSS)
* [local] Wondershare UBackit 2.0.5 - 'wsbackup' Unquoted Service Path
* [local] Wondershare FamiSafe 1.0 - 'FSService' Unquoted Service Path
* [local] Wondershare MobileTrans 3.5.9 - 'ElevationService' Unquoted Service Path
* [local] Wondershare Dr.Fone 11.4.9 - 'DFWSIDService' Unquoted Service Path
* [webapps] Hotel Druid 3.0.3 - Remote Code Execution (RCE)
* [webapps] WordPress Plugin dzs-zoomsounds 6.60 - Remote Code Execution (RCE) (Unauthenticated)
* [webapps] WordPress Plugin MasterStudy LMS 2.7.5 - Unauthenticated Admin Account Creation

Exploit Database for offline use

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

user@yourlinux:~$ *searchsploit keyword1 keyword2*

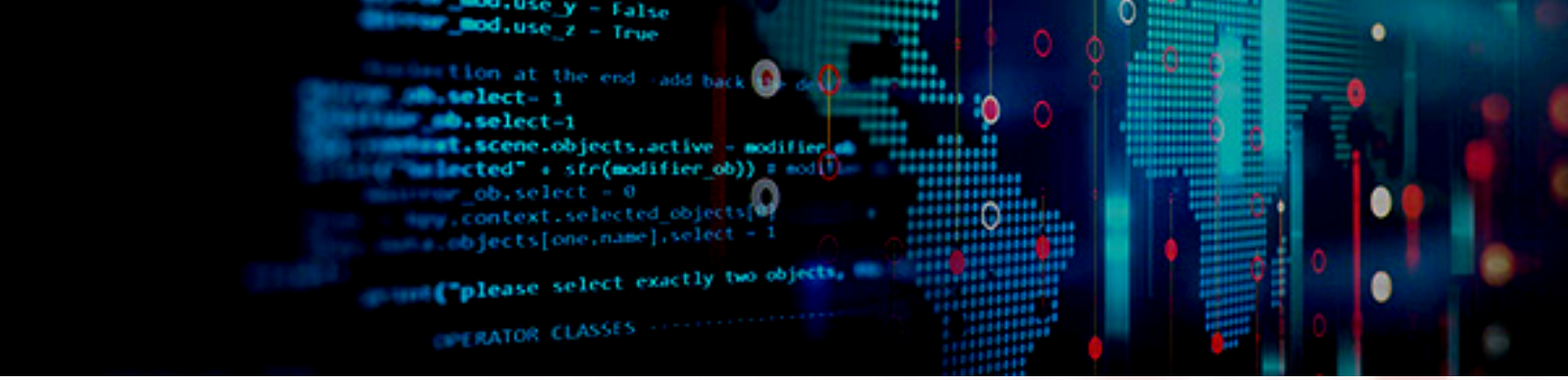
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://belemdobrejodocruz.pb.gov.br/1337.txt
http://belemdobrejodocruz.pb.gov.br/1337.txt notified by Hunter Bajwa
http://pmsbt.rn.gov.br/1337.txt
http://pmsbt.rn.gov.br/1337.txt notified by Hunter Bajwa
http://www.pa-dompu.go.id/crot.txt
http://www.pa-dompu.go.id/crot.txt notified by AnonCoders Taliban
http://perpustakaan.pa-dompu.go.id/crot.txt
http://perpustakaan.pa-dompu.go.id/crot.txt notified by AnonCoders Taliban
http://slide.pn-bireuen.go.id/crot.txt
http://slide.pn-bireuen.go.id/crot.txt notified by AnonCoders Taliban
http://surat.pn-bireuen.go.id/crot.txt
http://surat.pn-bireuen.go.id/crot.txt notified by AnonCoders Metro Lampung Indonesia
http://sireva.lan.go.id/index.html
http://sireva.lan.go.id/index.html notified by ./KeyzNet
http://pn-sibolga.go.id/asu.txt
http://pn-sibolga.go.id/asu.txt notified by Black_X12
https://www.dannok.go.th/kz.html
https://www.dannok.go.th/kz.html notified by Mr.Kro0oz.305
https://kota-madiun.kpu.go.id
https://kota-madiun.kpu.go.id notified by AnonCoders
https://kab-sukabumi.kpu.go.id
https://kab-sukabumi.kpu.go.id notified by AnonCoders
https://kab-kayongutara.kpu.go.id
https://kab-kayongutara.kpu.go.id notified by AnonCoders
https://kota-palu.kpu.go.id
https://kota-palu.kpu.go.id notified by AnonCoders
https://kab-ketapang.kpu.go.id
https://kab-ketapang.kpu.go.id notified by AnonCoders
https://kab-donggala.kpu.go.id
https://kab-donggala.kpu.go.id notified by AnonCoders
https://kota-depok.kpu.go.id
https://kota-depok.kpu.go.id notified by AnonCoders
https://kab-lahat.kpu.go.id
https://kab-lahat.kpu.go.id notified by AnonCoders



Dark Web News

Darknet Live

Fent Vendor "XanaxKing2" Sentenced to 30 Years in Prison

A California man was sentenced to 360 months in prison after he was found guilty of distributing fentanyl analogues through the dark web. US District Judge Michael A. Shipp sentenced 30-year-old Andrew Tablack, of Beverly Hills, California, to 30 years in prison. A jury convicted Tablack of one count of manufacturing, supplying, and possessing with intent to manufacture and distribute cyclopropyl fentanyl pills and one count of conspiracy to Manufacture and Distribute Fentanyl pills. This picture, which is is frequently used in other fent-related articles, originally came from a DEA bust in this case IIRC. An investigation led by the Organized Crime Drug Enforcement Task Force (OCDETF) resulted in Tablack's arrest and subsequent imprisonment. The task force's investigation revealed that Tablack and his accomplice Stephan Durham, 43, masterminded a fentanyl pill production operation from California. According to court records, the duo produced and distributed fentanyl-laced pills from at least March 2017 through December 2017. The duo produced and distributed hundreds of thousands of fentanyl analogue pills throughout the United States using a vendor account on a darkweb marketplace. Investigators identified Tablack as the vendor "XanaxKing2.” A 2017 investigation by the Drug Enforcement Administration (DEA) resulted in the seizure of approximately 300,000 pills containing cyclopropyl fentanyl at a residence in Monmouth County, New Jersey. During the investigation, the DEA found packages of cyclopropyl fentanyl pills at other homes in Monmouth County. Investigators later identified Tablack as the source of the drugs.

Pill presses put you on a list. Taskforce members examined shipping records and found that a company in California had purchased nine pill presses. The supplier of the presses had shipped them to an industrial property leased to the same company. Further investigation revealed that Durham, Tablack's co-defendant, owned the company. Investigators intercepted packages addressed to the property leased by Durham's company. The packages, which originated in China, contained fentanyl, fentanyl analogues, and other material used in the pill production process. Court documents revealed that the fentanyl supplier had disguised the drugs as food items or beauty products. Police arrested both defendants in December 2017. Officers seized large amounts of cryptocurrencies, electronic devices, and a Rolls Royce Wraith during the raids. Approximately 106,260.01646951 Waves seized on or about December 20, 2017; Approximately 275,000 Syscoin seized on or about December 20, 2017; Approximately 159,211.67613520 Shift seized on or about December 20, 2017; Approximately 95,016.989 Waves seized on or about December 20, 2017; Approximately 25,165.16586896 Ark seized on or about December 20, 2017; Approximately 7,268.81134075 OmiseGo seized on or about December 20, 2017; Approximately 17.48646464 Bitcoin seized on or about March 19, 2018; Approximately $5,400.00 in United States currency seized on or about December 20, 2017; One 2015 Rolls-Royce Wraith Sedan One Apple iPhone 7 Plus, 32GB capacity, seized on or about December 20, 2017; One Apple iPhone 7, seized on or about December 20, 2017; One Apple iPhone 6 Plus (broken), seized on or about December 20, 2017; One Apple iPhone 6 Plus, seized on or about December 20, 2017; One Samsung Cellular Phone, seized on or about December 20, 2017; One Dell Inspiron Laptop, seized on or about December 20, 2017; One Ledger Blue Security Device, seized on or about December 20, 2017; Two Ledger

Nano S Digital Currency Hardware Wallets, seized on or about December 20, 2017; One Apple iPhone SE, seized on or about December 20, 2017; One Apple iPad Pro, seized on or about December 20, 2017; A press seized by the DEA. During the height of the "XanaxKing2” operation, Tablack distributed approximately 400,000 pills every month. In February 2022, Judge Shipp sentenced Tablack to 30 years in prison and three years of supervised release. The judge also ordered Tablack to forfeit the cryptocurrencies and electronic devices seized by law enforcement. Indictment pdf (via darknetlive.com at https://darknetlive.com/post/xanaxking2-sentenced-to-30-years-in-prison/)

DOJ Appoints a Director for the Crypto Enforcement Team

The Justice Department selected the Director of the newly-created National Cryptocurrency Enforcement Team (NCET). Eun Young Choi will serve as the first Director of the National Cryptocurrency Enforcement Team (NCET). The DOJ announced the NCET in October 2021 as a "focal point” for the Justice Department's efforts in investigating crimes committed or enabled by cryptocurrency. It will involve prosecutors with a background in financial crime and the Federal Bureau of Investigation's new Virtual Asset Exploitation Unit. According to the DOJ, the goal of the NCET is to: "[I]dentify, investigate, support and pursue the department's cases involving the criminal use of digital assets, with a particular focus on virtual currency exchanges, mixing and tumbling services, infrastructure providers, and other entities that are enabling the misuse of cryptocurrency and related technologies to commit or facilitate criminal activity.” Eun Young Choi assumed her role on February 17, 2022. "With the rapid innovation of digital assets and distributed ledger technologies, we have seen a rise in their illicit use by criminals who exploit them to fuel cyberattacks and ransomware and extortion schemes; traffic in narcotics, hacking tools and illicit contraband online; commit thefts and scams, and launder the proceeds of their crimes,” said Assistant Attorney General Kenneth A. Polite Jr. of the Justice Department's Criminal Division. "The NCET will serve as the focal point for the department's efforts to tackle the growth of crime involving these technologies. Eun Young is an accomplished leader on cyber and cryptocurrency issues, and I am pleased that she will continue her service as the NCET's inaugural Director, spearheading the department's efforts in this area.” "The department has been at the forefront of investigating and prosecuting crimes involving digital currencies since their inception,” said Director Choi. "The NCET will play a pivotal role in ensuring that as the technology surrounding digital assets grows and evolves, the department in turn accelerates and expands its efforts to combat their illicit abuse by criminals of all kinds. I am excited to lead the NCET's incredible and talented team of attorneys and to get to work on this important priority for the department. I want to thank Assistant Attorney General Polite and the Criminal Division's leadership for this opportunity.” archive.org (via darknetlive.com at https://darknetlive.com/post/doj-appoints-a-director-for-the-cryptocurrency-enforcement-team/)

Canadian Government Wants to Crack Down on Crypto

In an attempt to stop protesters from honking, Canadian officials are broadening the anti-money laundering and terrorist financing rules to include cryptocurrency and other digital assets. The Emergencies Act, which the Canadian government invoked to crack down on unauthorized honking, ushered in various regulations intended to prevent honkers from using a bank account or receiving funding from outside sources, including cryptocurrency. Prime Minister Justin Trudeau and Deputy Prime Minister & Minister of Finance Chrystia Freeland. Deputy Prime Minister and Minister of Finance, Chrystia Freeland: "[W]e are broadening the scope of Canada's anti-money laundering and terrorist financing rules so that they cover crowdfunding platforms and the payment service providers they use. These changes cover all forms of transactions, including digital assets such as cryptocurrencies. This is terrorism.

The illegal blockades have highlighted the fact that crowdfunding platforms, and some of the payment service providers they use, are not fully captured under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act.” It is not entirely clear how the Canadian government could regulate cryptocurrency. They could control the on-ramps and off-ramps. But they already do that. Trudeau will not involve the military. | Ontario Provincial Police "Our banks and financial institutions are already obligated to report to the Financial Transactions and Reports Analysis Centre of Canada, or FINTRAC. As of today, all crowdfunding platforms, and the payment service providers they use, must register with FINTRAC

and must report large and suspicious transactions to FINTRAC. This will help mitigate the risk that these platforms receive illicit funds; increase the quality and quantity of intelligence received by FINTRAC, and make more information available to support investigations by law enforcement into these illegal blockades.” The announcement also revealed that the Canadian government authorized financial services in Canada to freeze the accounts of suspected honkers. The order included banks or other financial service providers and permitted them to immediately freeze accounts suspected of being "affiliated with these illegal blockades.” This action will not require a court order. "[T]he government is issuing an order with immediate effect, under the Emergencies Act, authorizing Canadian financial institutions to temporarily cease providing financial services where the institution suspects that an account is being used to further the illegal blockades and occupations.” Reading between the lines, it appears as if the federal government will be directing banks to freeze accounts. Financial services should identify and freeze accounts independently, but the announcement referenced the government's role in the financial crackdown. "Federal government institutions will have a new broad authority to share relevant information with banks and other financial service providers to ensure that we can all work together to put a stop to the funding of these illegal blockades.” __ Chrystia Freeland Freeland said she "spoke directly with the heads of Canadian banks” before the announcement. It seems clear that any regulation of cryptocurrency will be regulation of the on-ramps, off-ramps, and the bank accounts of cryptocurrency users who used such a ramp. As an aside, Freeland also authored the book Plutocrats. The book describes the ongoing concentration of wealth into the pockets of oligarchs and plutocrats. The book has been described as a thinly-veiled apologia for said transfer of wealth. Fitting, if true. I have only just started reading the book. It is far from the top of my reading list, though, so I will have to wait to form my own opinion. archive.org, archive.is, .onion As another aside and since I have not really been following the terrorismâ„¢ in Canada, what is the deal with the bridge blockades? Are they media ops? Wouldn't holding the roads to and from the bridges in question be just as ridiculous? (via darknetlive.com at https://darknetlive.com/post/canadian-government-wants-to-crack-down-on-crypto/)

German Man Arrested for Buying Amphetamine on the Darkweb

Authorities in Bavaria, Germany, arrested a man suspected of reselling large quantities of amphetamine purchased through the darkweb. In a joint press release, the police headquarters in Lower Franconia and the public prosecutor's office in Würzburg disclosed that a 20-year-old man from Würzburg, Lower Franconia, had allegedly ordered a total of approximately 5.5 kilograms of amphetamine from the darkweb. Prosecutors said that the defendant had intended to distribute the amphetamine. An investigation into the 20-year-old's drug trafficking operation was launched on February 7, 2022, after customs officers intercepted a suspicious package addressed to the 20-year-old. Customs notified the police, who acquired a search warrant for the box and found a kilogram of amphetamine contained within it. Investigators acquired and executed a search warrant at the 20-year-old's residence on the same day. The search allegedly led to the discovery of extensive drug trafficking evidence. The investigators also established that the 20-year-old had ordered a total of approximately 5.5 kilograms of amphetamine on six occasions. At the Wurzburg district court, the defendant was charged with a drug trafficking crime. The presiding judge ordered that the defendant remains in detention pending trial. archive.org, archive.is, onion (via darknetlive.com at https://darknetlive.com/post/german-man-arrested-for-buying-amphetamine-on-the-darkweb/)

Dark Web Link

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

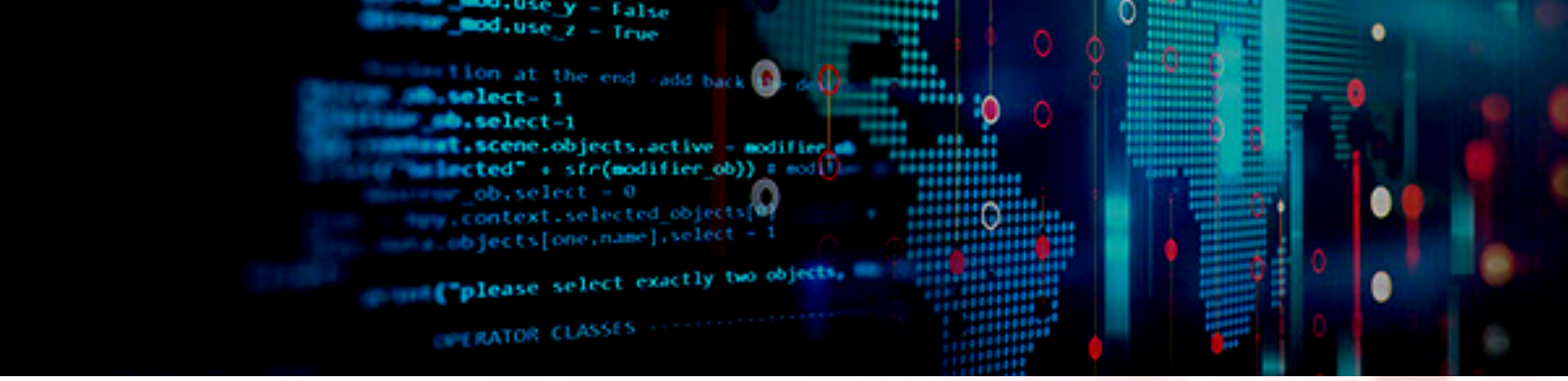
One of the latest darknet markets that accepted monero (XMR) as their payment modes have announced their retirement. The dark web market is none other than White House Market (WHM). As soon as the White House Market plans retirement and the news went live, there has been chaos all over the darknet sphere 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.

Faucibarriers Against 'Dark Web People' Distressing His Daughters And Wife With Vicious Threats

Dr. Anthony Fauci's life and career are chronicled in a new National Geographic documentary. Fauci rails about pestering phone calls from “Dark web” persons in the film.Dr. Anthony Fauci grew up in Brooklyn's Bensonhurst neighbourhood, where he learnt early on that “you didn't take any shit from anyone.” During the HIV/AIDS crisis in the United [...] The post Faucibarriers Against 'Dark Web People' Distressing His Daughters And Wife With Vicious Threats appeared first on Dark Web Link | Deep web Onion Links | Darknet News.

Onionshare: Safe Communications Stand Used By Journalists And Whistleblowers Covers Data Exposure Bug

Two flaws in a technology used by whistleblowers and the media to securely communicate material have been addressed, potentially jeopardising the file-sharing system's anonymity. OnionShare is an open source utility for Windows, macOS, and Linux that allows users to remain anonymous while doing things like file sharing, hosting websites, and communicating. The service, which is [...] The post Onionshare: Safe Communications Stand Used By Journalists And Whistleblowers Covers Data Exposure Bug appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Trend Micro Anti-Malware Blog

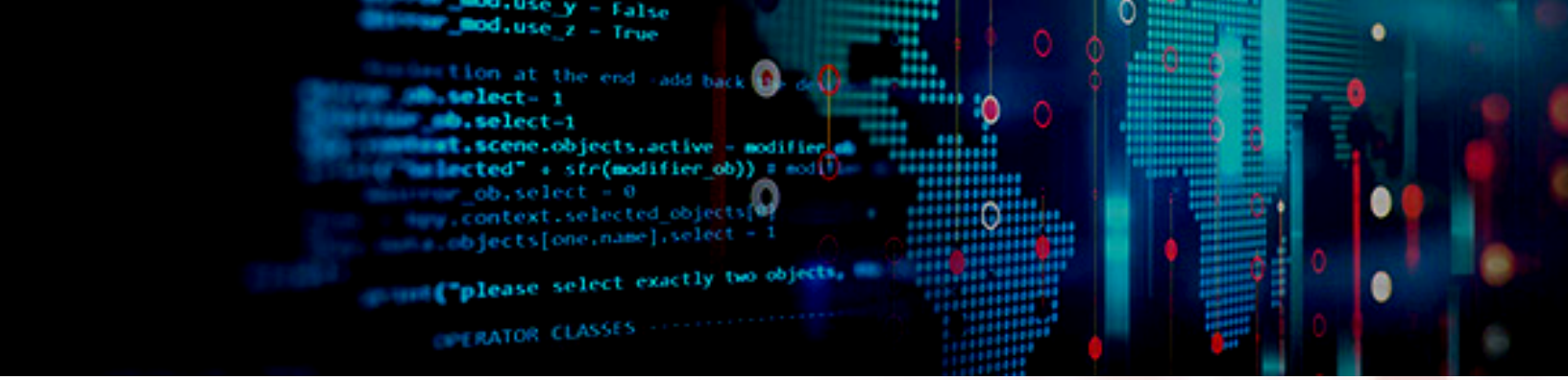
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

* RiskIQ Threat Intelligence Roundup: QBot, Magecart, Agent Tesla Headline Hijacked Infrastructure
* RiskIQ Threat Intelligence Roundup: C2 and Nation-State Threat Infrastructure
* Jupyter Notebooks Make RiskIQ Data a Digital 'Mech Suit' for Threat Intelligence Analysts
* "Offshore" Shinjiru Provides Bulletproof Services to Cyberattackers
* Retailers Using WooCommerce are at Risk of Magecart Attacks
* 5 Tips to Stay on the Offensive and Safeguard Your Attack Surface
* New E-Commerce Cybersecurity Guide Helps Brands be Proactive This Holiday Shopping Season
* New Aggah Campaign Hijacks Clipboards to Replace Cryptocurrency Addresses
* The Vagabon Kit Highlights 'Frankenstein' Trend in Phishing
* Watch On-Demand: Five Security Intelligence Must-Haves For Next-Gen Attack Surface Management

FireEye

* Metasploit Weekly Wrap-Up
* What's New in InsightVM and Nexpose: Q4 2021 in Review
* Log4Shell 2 Months Later: Security Strategies for the Internet's New Normal
* Cloud Security and Compliance: The Ultimate Frenemies of Financial Services
* [Security Nation] Amit Serper on Finding Leaks in Autodiscover
* The Future of Finserv Security: Cloud Expert and Former CISO Anthony Johnson Weighs In
* Prudent Cybersecurity Preparation for the Potential Russia-Ukraine Conflict
* How InsightAppSec Detects Log4Shell: Your Questions Answered
* Dropping Files on a Domain Controller Using CVE-2021-43893
* Metasploit Wrap-Up



Advisories

US-Cert Alerts & bulletins

* CISA Insights: Foreign Influence Operations Targeting Critical Infrastructure
* NCSC-NZ Releases Advisory on Cyber Threats Related to Russia-Ukraine Tensions
* CISA Compiles Free Cybersecurity Services and Tools for Network Defenders
* NSA Best Practices for Selecting Cisco Password Types
* Cisco Releases Security Updates for Email Security Appliance
* Drupal Releases Security Updates
* Mozilla Releases Security Update for Thunderbird
* VMware Releases Security Updates for Multiple Products
* AA22-047A: Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain
* AA22-040A: 2021 Trends Show Increased Globalized Threat of Ransomware
* Vulnerability Summary for the Week of February 14, 2022
* Vulnerability Summary for the Week of February 7, 2022

Zero Day Initiative Advisories

ZDI-CAN-16683: FreeBSD
A CVSS score 8.2 (AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-02-18, 4 days ago. The vendor is given until 2022-06-18 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-16687: FreeBSD
A CVSS score 8.2 (AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Reno Robert and Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-02-18, 4 days ago. The vendor is given until 2022-06-18 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-16538: 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: 2022-02-18, 4 days ago. The vendor is given until 2022-06-18 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-16570: Bentley
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: 2022-02-16, 6 days ago. The vendor is given until 2022-06-16 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-16336: Centreon
A CVSS score 6.5 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-02-16, 6 days ago. The vendor is given until 2022-06-16 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-16650: Trend Micro

A CVSS score 4.4 (AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-02-16, 6 days ago. The vendor is given until 2022-06-16 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-16335: Centreon

A CVSS score 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-02-16, 6 days ago. The vendor is given until 2022-06-16 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-16573: Bentley

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: 2022-02-16, 6 days ago. The vendor is given until 2022-06-16 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-16581: Bentley

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: 2022-02-16, 6 days ago. The vendor is given until 2022-06-16 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-16651: Trend Micro

A CVSS score 4.4 (AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-02-16, 6 days ago. The vendor is given until 2022-06-16 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-16523: Foxit

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 'Anonymous' was reported to the affected vendor on: 2022-02-16, 6 days ago. The vendor is given until 2022-06-16 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-16605: Trend Micro

A CVSS score 4.4 (AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-02-16, 6 days ago. The vendor is given until 2022-06-16 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-16553: 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: 2022-02-16, 6 days ago. The vendor is given until 2022-06-16 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-16537: 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 'Mark Vincent Yason (@MarkYason)' was reported to the affected vendor on: 2022-02-16, 6 days ago. The vendor is given until 2022-06-16 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-16565: Trend Micro

A CVSS score 4.4 (AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L) severity vulnerability discovered by 'Michael

DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-02-16, 6 days ago. The vendor is given until 2022-06-16 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-16244: Measuresoft

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 'rgod' was reported to the affected vendor on: 2022-02-16, 6 days ago. The vendor is given until 2022-06-16 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-16595: Trend Micro

A CVSS score 4.4 (AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-02-16, 6 days ago. The vendor is given until 2022-06-16 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-16606: Trend Micro

A CVSS score 4.4 (AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-02-16, 6 days ago. The vendor is given until 2022-06-16 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-16594: Trend Micro

A CVSS score 4.4 (AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-02-16, 6 days ago. The vendor is given until 2022-06-16 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-16566: Trend Micro

A CVSS score 4.4 (AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-02-16, 6 days ago. The vendor is given until 2022-06-16 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-16536: 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: 2022-02-16, 6 days ago. The vendor is given until 2022-06-16 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-16567: 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: 2022-02-11, 11 days ago. The vendor is given until 2022-06-11 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-16337: Dell

A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Andrea Micalizzi aka rgod (@rgod777)' was reported to the affected vendor on: 2022-02-10, 12 days ago. The vendor is given until 2022-06-10 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-16410: 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 'Tran Van Khang - khangkito (VinCSS)' was reported to the affected vendor on: 2022-02-09, 13 days ago. The vendor is given until 2022-06-09 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Red Hat Security Advisory 2022-0582-01

Red Hat Security Advisory 2022-0582-01 - Ruby is an extensible, interpreted, object-oriented, scripting language. It has features to process text files and to perform system management tasks. Issues addressed include HTTP request smuggling, HTTP response splitting, code execution, denial of service, information leakage, and spoofing vulnerabilities.

Datarobot Remote Code Execution

Datarobot suffers from a remote code execution vulnerability.

Red Hat Security Advisory 2022-0581-01

Red Hat Security Advisory 2022-0581-01 - Ruby is an extensible, interpreted, object-oriented, scripting language. It has features to process text files and to perform system management tasks. Issues addressed include HTTP request smuggling, HTTP response splitting, code execution, denial of service, information leakage, and spoofing vulnerabilities.

Ubuntu Security Notice USN-5295-1

Ubuntu Security Notice 5295-1 - It was discovered that the Packet network protocol implementation in the Linux kernel contained a double-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. Jann Horn discovered a race condition in the Unix domain socket implementation in the Linux kernel that could result in a read-after-free. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

WordPress UpdraftPlus 1.22.2 Backup Disclosure

WordPress UpdraftPlus versions 1.16.7 through 1.22.2 suffer from a backup disclosure vulnerability.

Ubuntu Security Notice USN-5292-3

Ubuntu Security Notice 5292-3 - USN-5292-1 fixed several vulnerabilities in snapd. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. James Troup discovered that snap did not properly manage the permissions for the snap directories. A local attacker could possibly use this issue to expose sensitive information. Ian Johnson discovered that snapd did not properly validate content interfaces and layout paths. A local attacker could possibly use this issue to inject arbitrary AppArmor policy rules, resulting in a bypass of intended access restrictions. The Qualys Research Team discovered that snapd did not properly validate the location of the snap-confine binary. A local attacker could possibly use this issue to execute other arbitrary binaries and escalate privileges. The Qualys Research Team discovered that a race condition existed in the snapd snap-confine binary when preparing a private mount namespace for a snap. A local attacker could possibly use this issue to escalate privileges and execute arbitrary code.

Ubuntu Security Notice USN-5292-2

Ubuntu Security Notice 5292-2 - USN-5292-1 fixed vulnerabilities in snapd. This update provides the corresponding update for the riscv64 architecture. James Troup discovered that snap did not properly manage the permissions for the snap directories. A local attacker could possibly use this issue to expose sensitive information.

Ubuntu Security Notice USN-5294-1

Ubuntu Security Notice 5294-1 - It was discovered that the Packet network protocol implementation in the Linux kernel contained a double-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. Szymon Heidrich discovered that the USB Gadget subsystem in the Linux kernel did not properly restrict the size of control requests for certain gadget types, leading to possible out of bounds reads or writes. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5292-1

Ubuntu Security Notice 5292-1 - James Troup discovered that snap did not properly manage the permissions for the snap directories. A local attacker could possibly use this issue to expose sensitive information. Ian Johnson discovered that snapd did not properly validate content interfaces and layout paths. A local attacker could possibly use this issue to inject arbitrary AppArmor policy rules, resulting in a bypass of intended access

restrictions.

Red Hat Security Advisory 2022-0580-01

Red Hat Security Advisory 2022-0580-01 - Red Hat Openshift GitOps is a declarative way to implement continuous deployment for cloud native applications. Issues addressed include a traversal vulnerability.

Ubuntu Security Notice USN-5291-1

Ubuntu Security Notice 5291-1 - It was discovered that libarchive incorrectly handled symlinks. If a user or automated system were tricked into processing a specially crafted archive, an attacker could possibly use this issue to change modes, times, ACLs, and flags on arbitrary files. It was discovered that libarchive incorrectly handled certain RAR archives. If a user or automated system were tricked into processing a specially crafted RAR archive, an attacker could use this issue to cause libarchive to crash, resulting in a denial of service, or possibly execute arbitrary code.

Red Hat Security Advisory 2022-0491-01

Red Hat Security Advisory 2022-0491-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.7.43. Issues addressed include a cross site request forgery vulnerability.

Red Hat Security Advisory 2022-0548-01

Red Hat Security Advisory 2022-0548-01 - Ruby is an extensible, interpreted, object-oriented, scripting language. It has features to process text files and to perform system management tasks.

WordPress Cozmoslabs Profile Builder 3.6.1 Cross Site Scripting

WordPress Cozmoslabs Profile Builder plugin versions 3.6.1 and below suffer from a cross site scripting vulnerability.

Ubuntu Security Notice USN-5267-3

Ubuntu Security Notice 5267-3 - USN-5267-1 fixed vulnerabilities in the Linux kernel. This update provides the corresponding updates for the Linux kernel for Raspberry Pi devices. It was discovered that the Bluetooth subsystem in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Red Hat Security Advisory 2022-0492-01

Red Hat Security Advisory 2022-0492-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the container images for Red Hat OpenShift Container Platform 4.7.43.

Red Hat Security Advisory 2022-0485-01

Red Hat Security Advisory 2022-0485-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.8.31. Issues addressed include a code execution vulnerability.

Red Hat Security Advisory 2022-0493-01

Red Hat Security Advisory 2022-0493-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.7.43. Issues addressed include a code execution vulnerability.

Red Hat Security Advisory 2022-0546-01

Red Hat Security Advisory 2022-0546-01 - Ruby is an extensible, interpreted, object-oriented, scripting language. It has features to process text files and to perform system management tasks.

Red Hat Security Advisory 2022-0547-01

Red Hat Security Advisory 2022-0547-01 - Ruby is an extensible, interpreted, object-oriented, scripting language. It has features to process text files and to perform system management tasks.

Red Hat Security Advisory 2022-0544-01

Red Hat Security Advisory 2022-0544-01 - Ruby is an extensible, interpreted, object-oriented, scripting

language. It has features to process text files and to perform system management tasks. Issues addressed include code execution, denial of service, and spoofing vulnerabilities.

Algorithmia MSOL Remote Code Execution

Algorithmia MSOL suffers from a remote code execution vulnerability.

Red Hat Security Advisory 2022-0543-01

Red Hat Security Advisory 2022-0543-01 - Ruby is an extensible, interpreted, object-oriented, scripting language. It has features to process text files and to perform system management tasks. Issues addressed include code execution, denial of service, and spoofing vulnerabilities.

Zepl Notebook Sandbox Escape

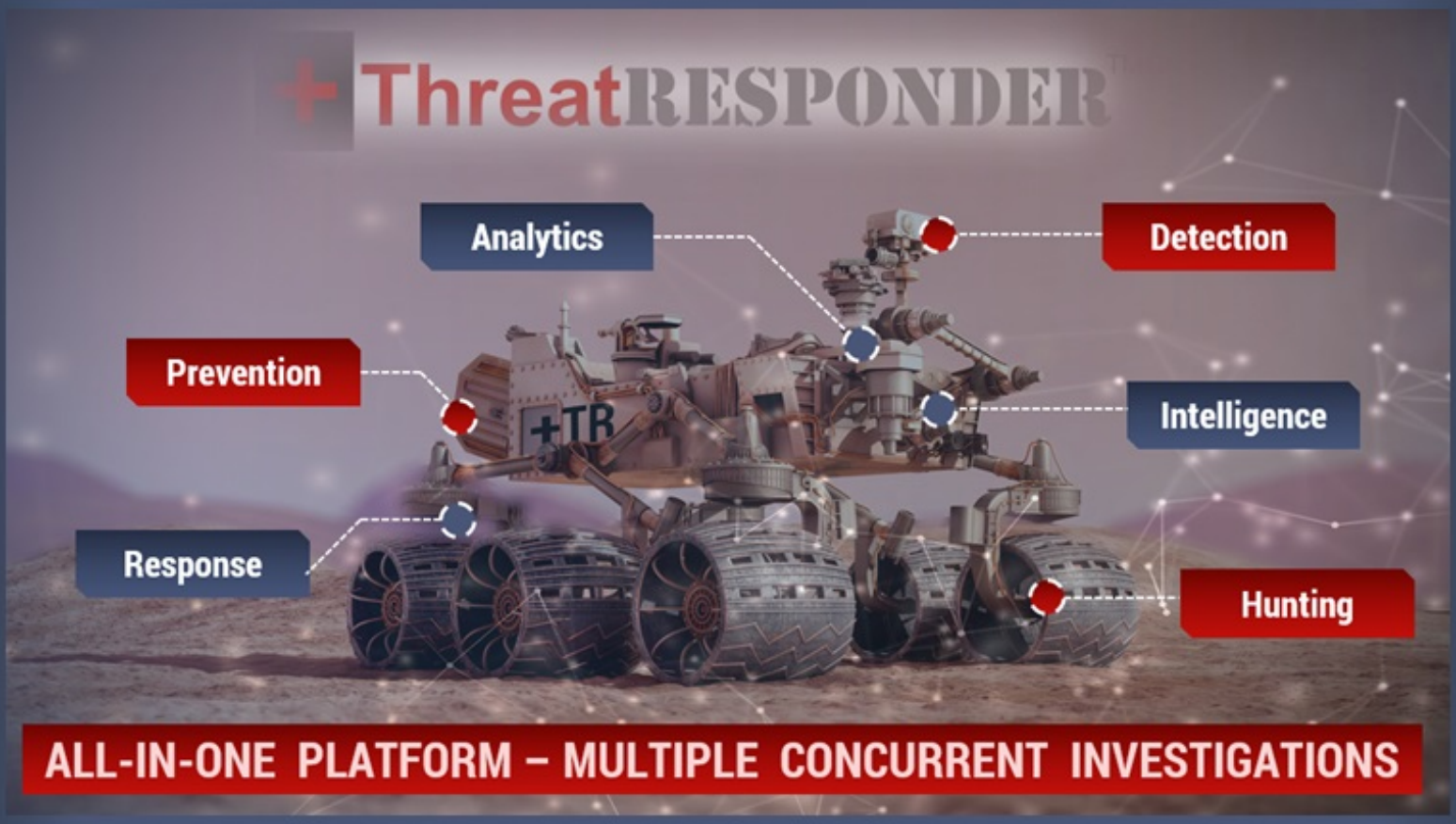
Zepl Notebook suffers from a sandbox escape vulnerability.

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



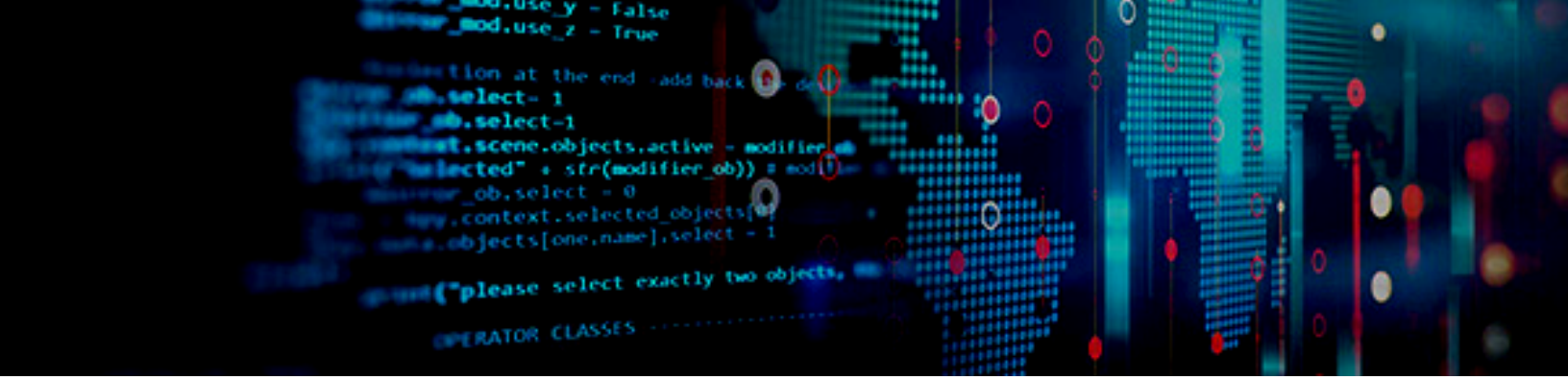
The Solution – ThreatResponder® Platform

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

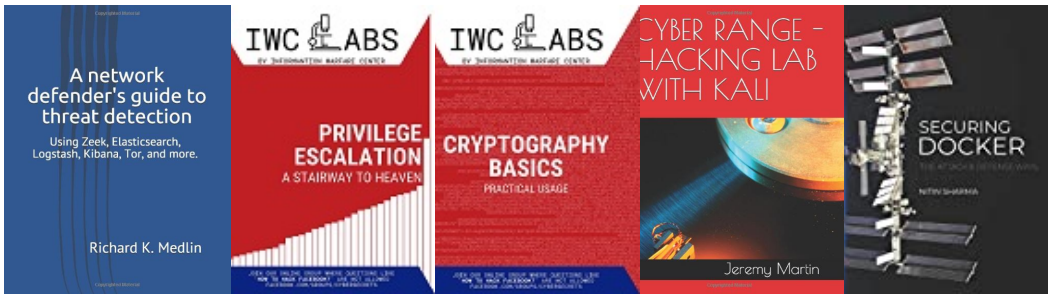


The Cyber Secrets publications on Amazon

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