Apr-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

April 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

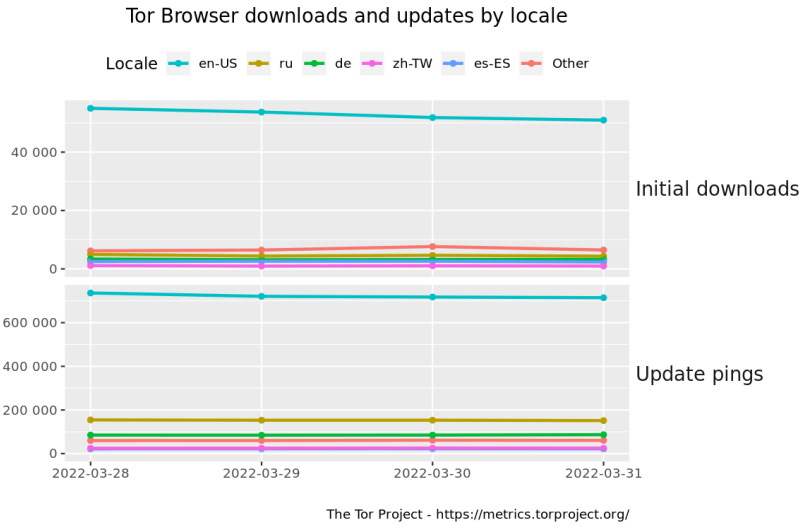
Internet Storm Center Infocon Status

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

* Ukraine Accuses Russia Of Using WhatsApp Bot Farm To Ask Military To Surrender
* Ubiquiti Sues Brian Krebs Alleging Defamation
* Deep Panda Returns With Log4Shell Exploits, New Fire Chili Rootkit
* Apple Rushes Out Patches For Two Zero Days Threatening Users
* More Charged In UK Lapsus$ Investigation
* RCE Spring4shell Hits Java Spring Framework
* Are Tech Companies Removing Evidence Of War Crimes?
* FBI Efforts To Disrupt Business Email Compromise Scams Leads To 65 Arrests
* QNAP Customers Adrift, Waiting On Fix For OpenSSL Bug
* Nvidia DGX Systems Prone To Side Channel, Covert Attacks
* Researchers Used A Decommissioned Satellite To Broadcast Hacker TV
* Fake Cops Stole User Data From Meta And Apple
* Hackers Who Stole $50 Mil In Crypto Say They Will Refund Some Victims
* MSHTML Flaw Exploited To Attack Russian Dissidents
* Hackers Steal $625 Million From Ronin Network In Largest Ever Crypto Theft
* Company Official: Hackers Are Still Inside Viasat
* Ukraine Security Agency Shutters Russian Disinformation Bot Farms
* Lapsus$ And SolarWinds Hackers Both Use The Same Old Trick To Bypass MFA
* Ukraine Internet Provider Suffers Cyber Attack
* Exchange Servers Speared In IcedID Phishing Campaign
* Creepy Spyware Company Goes Broke
* Morgan Stanley Wealth Management Accounts Breached In Vishing Attack
* Hundreds More Packages Found In Malicious npm Factory
* FCC Puts Kaspersky On Security Threat List
* Sophos Patches Critical Remote Code Execution Vulnerability In Firewall

Krebs on Security

* Fake Emergency Search Warrants Draw Scrutiny from Capitol Hill
* Hackers Gaining Power of Subpoena Via Fake "Emergency Data Requests"
* Estonian Tied to 13 Ransomware Attacks Gets 66 Months in Prison
* A Closer Look at the LAPSUS$ Data Extortion Group
* 'Spam Nation' Villain Vrublevsky Charged With Fraud
* Pro-Ukraine 'Protestware' Pushes Antiwar Ads, Geo-Targeted Malware
* Lawmakers Probe Early Release of Top RU Cybercrook
* Report: Recent 10x Increase in Cyberattacks on Ukraine
* Microsoft Patch Tuesday, March 2022 Edition
* Internet Backbone Giant Lumen Shuns .RU

Dark Reading

* Apple's Zero-Day Woes Continue
* NSA Employee Indicted for Sending Classified Data Outside the Agency
* What You Need to Know About PCI DSS 4.0's New Requirements
* More Than Ever, Security Matters
* Vulnerabilities in Rockwell Automation PLCs Could Enable Stuxnet-Like Attacks
* Spring Fixes Zero-Day Vulnerability in Framework and Spring Boot
* Ransomware: Should Companies Ever Pay Up?
* Companies Going to Greater Lengths to Hire Cybersecurity Staff
* Global BEC Crackdown Nets 65 Suspects
* U.S. Cyber Command Adds APUS as Member in Newly Formed Academic Network
* Protecting Your Organization Against a New Class of Cyber Threats: HEAT
* Nation-State Hackers Ramp Up Ukraine War-Themed Attacks
* Zero-Day Vulnerability Discovered in Java Spring Framework
* CISA, DOE Warn of Attacks on Uninterruptible Power Supply (UPS) Devices
* Smart Cities: Secure by Design? It Takes a Village
* Cybercriminals Fighting Over Cloud Workloads for Cryptomining
* Cloud Security Architecture Needs to Be Strategic, Realistic, and Based on Risk
* How Security Complexity Is Being Weaponized
* How to Prevent the Next Log4j-Style Zero-Day Vulnerability
* Log4j Attacks Continue Unabated Against VMware Horizon Servers

The Hacker News

* Experts Shed Light on BlackGuard Infostealer Malware Sold on Russian Hacking Forums
* Beastmode DDoS Botnet Exploiting New TOTOLINK Bugs to Enslave More Routers
* 15-Year-Old Bug in PEAR PHP Repository Could've Enabled Supply Chain Attacks
* British Police Charge Two Teenagers Linked to LAPSUS$ Hacker Group
* GitLab Releases Patch for Critical Vulnerability That Could Let Attackers Hijack Accounts
* Russian Wiper Malware Likely Behind Recent Cyberattack on Viasat KA-SAT Modems
* Critical Bugs in Rockwell PLC Could Allow Hackers to Implant Malicious Code
* Chinese Hackers Target VMware Horizon Servers with Log4Shell to Deploy Rootkit
* Results Overview: 2022 MITRE ATT&CK Evaluation - Wizard Spider and Sandworm Edition
* North Korean Hackers Distributing Trojanized DeFi Wallet Apps to Steal Victims' Crypto
* Zyxel Releases Patches for Critical Bug Affecting Business Firewall and VPN Devices
* Apple Issues Patches for 2 Actively Exploited Zero-Days in iPhone, iPad and Mac Devices
* Security Patch Releases for Critical Zero-Day Bug in Java Spring Framework
* Bugs in Wyze Cams Could Let Attackers Takeover Devices and Access Video Feeds
* New Python-based Ransomware Targeting JupyterLab Web Notebooks

Security Week

* UK Charges Alleged Lapsus$ Gang Members With Hacking
* Experts Warn Defenders: Don't Relax on Log4j
* FBI Warns of Ransomware Attacks Targeting Local Governments
* PCI Data Security Standard v4.0 Released to Address Emerging Threats
* New Vulnerabilities Allow Stuxnet-Style Attacks Against Rockwell PLCs
* Trend Micro Patches Apex Central Zero-Day Exploited in Targeted Attacks
* Spring4Shell Exploitation Attempts Confirmed as Patches Are Released
* Antimatter Emerges From Stealth Mode With $12M to Secure Customer Data
* UK Spy Chief Warns Russia Looking for Cyber Targets
* Apple Ships Emergency Patches for 'Actively Exploited' macOS, iOS Flaws
* New Modem Wiper Malware May be Connected to Viasat Hack
* Skiff Banks $10.5M for E2E Encrypted Workplace Collaboration
* WATCH: Fireside Chat With McDonald's CISO Shaun Marion
* Cybersecurity Vendors Assessing Impact of Recent OpenSSL Vulnerability
* FBI: 65 People Arrested Worldwide in BEC Bust
* IT Giant Globant Confirms Source Code Repository Breach
* The Importance of Open Source to an XDR Architecture
* SaaS Security Startup Wing Emerges From Stealth With $26 Million in Funding
* FBI Warns of Phishing Attacks Targeting US Election Officials
* Spring4Shell: Spring Flaws Lead to Confusion, Concerns of New Log4Shell-Like Threat
* Hackers Got User Data From Meta With Forged Request
* Satellite Modems Nexus of Worst Cyberattack of Ukraine War
* Cyera Emerges From Stealth Mode With $60M to Protect Cloud Data
* Investors Bet on Cyberpion in Attack Surface Management Space
* Chrome Browser Gets Major Security Update
* Remote 'Brokenwire' Hack Prevents Charging of Electric Vehicles

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* Your KnowBe4 Fresh Content Updates from March 2022
* Simple Facebook Phishing Scam Takes an Unexpected Turn to Throw Potential Victims Off the Scent
* Cisco: Web 3.0 Will be the Next Frontier for Social Engineering and Phishing Attacks
* Cost of Internet Crimes in 2021 Increase 64% Exceeding $6.9 Billion
* Obvious Phishbait, But Someone Will Bite
* FBI Warns of Phishing Attacks Targeting Election Officials
* A Lack of Employee Cyber Hygiene is the Next Big Threat
* Ransomware Attack Volume Increases by 18% As the Number of Variants Jumps to 34 in Only One Quarter
* Mobile Device Usage Have Led to Security Incidents in Nearly Half of Organizations
* CyberheistNews Vol 12 #13 [Heads Up] Published Zelenskyy Deepfake Video Demonstrates the Modern War
i

ISC2.org Blog

* Summary of March Inside (ISC)2 Webinar: Stay Vigilant
* Report: U.S. Workers Worry About Cyberattacks
* HOW CAN YOU WIN BIG IN VEGAS? - Global Achievement Awards Nominations Open Now
* Tips from a CISO: How to Create a Security Program
* GOING FOR (ISC)² CERTIFICATION? GET THE FACTS BEFORE YOU CHOOSE A TRAINING PROVIDER

HackRead

* How Internet Censorship Affects You - Pros and Cons
* Ukraine Leaks Personal Details of 620 Alleged FSB Agents
* $625m Stolen From Ronin Network - The Blockchain Behind Axie Infinity Game
* Anonymous Hacks 2 Russian Industrial Firms, Leak 112GB of Data for Ukraine
* Update Chrome Browser Now - Google Releases Emergency Security Update
* RAV Antivirus: How to Protect Your Data in 2022
* US Adds Kaspersky to List of Firms Posing Threat to National Security

Koddos

* How Internet Censorship Affects You - Pros and Cons
* Ukraine Leaks Personal Details of 620 Alleged FSB Agents
* $625m Stolen From Ronin Network - The Blockchain Behind Axie Infinity Game
* Anonymous Hacks 2 Russian Industrial Firms, Leak 112GB of Data for Ukraine
* Update Chrome Browser Now - Google Releases Emergency Security Update
* RAV Antivirus: How to Protect Your Data in 2022
* US Adds Kaspersky to List of Firms Posing Threat to National Security

Naked Security

* Apple pushes out two emergency 0-day updates - get 'em now!
* Two different "VMware Spring" bugs at large - we cut through the confusion
* S3 Ep76: Deadbolt, LAPSUS$, Zlib, and a Chrome 0-day [Podcast]
* "VMware Spring Cloud Function" Java bug gives instant remote code execution - update now!
* World Backup Day: 5 data recovery tips for everyone!
* Zlib data compressor fixes 17-year-old security bug - patch, errrm, now
* Google Chrome patches mysterious new zero-day bug - update now
* UK police arrest 7 hacking suspects - have they bust the LAPSUS$ gang?
* S3 Ep75: Okta hack, CryptoRom, OpenSSL, and CafePress [Podcast]
* Serious Security: DEADBOLT - the ransomware that goes straight for your backups

Threat Post

* Apple Rushes Out Patches for 0-Days in MacOS, iOS
* Belarusian 'Ghostwriter' Actor Picks Up BitB for Ukraine-Related Attacks
* Automaker Cybersecurity Lagging Behind Tech Adoption, Experts Warn
* QNAP Customers Adrift, Waiting on Fix for OpenSSL Bug
* A Blockchain Primer and a Bored Ape Headscratcher - Podcast
* RCE Bug in Spring Cloud Could Be the Next Log4Shell, Researchers Warn
* Cyberattackers Target UPS Backup Power Devices in Mission-Critical Environments
* Lapsus$ 'Back from Vacation'
* Google Chrome Bug Actively Exploited as Zero-Day
* MSHTML Flaw Exploited to Attack Russian Dissidents

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

* GitHub Copilot available for Microsoft Visual Studio 2022
* Visual Studio Code 1.66 shines on JavaScript heap profiles, CSS formatting
* Is distributed data realistic?
* What is Git? Version control for collaborative programming
* Docker raises $105M funding round to fuel its focus on developers
* A quick guide to blockchain
* React 18 arrives with concurrent renderer, automatic batching
* Solomon Hykes' Dagger raises $20M and launches public beta
* WSO2 launches low-code, cloud-native PaaS for API development
* Azure Percept: A machine learning quick starter

C4ISRNET - Media for the Intelligence Age Military

* US Army picks L3Harris and Thales for radio modernization
* Turkish drones won't give Ukraine the edge it needs
* US Army on track to award TITAN competitive prototyping contracts in the coming months
* US Space Force awards contract for simulation and war gaming environment
* Proposed US Army budget funds third Multi-Domain Task Force
* Russian efforts in Ukraine have not yet spilled over into cyberattacks on US, says lawmaker
* Army Software Factory tackling problems big and small
* Pentagon slows $9 billion cloud competition, citing more work to be done
* Marine Corps wants money for ships, missiles, sensors
* Navy dramatically increases funding for secretive Project Overmatch

The Hacker Corner

Conferences

* 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?
* Our Guide To Cybersecurity Marketing Campaigns

Google Zero Day Project

* FORCEDENTRY: Sandbox Escape
* Racing against the clock -- hitting a tiny kernel race window

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.

* nullcon HackIM 2022
* HackPack CTF 2022
* @HackDay Qualification 2022
* PlaidCTF 2022
* Winja CTF | Nullcon Berlin 2022
* JerseyCTF II
* BTH_CTF{Ring_Zero_to_Hero}
* Securinets CTF Quals 2022
* DCTF 2022
* CrewCTF 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

* Wireshark Analyzer 3.6.3
* Adversary3 1.0
* nfstream 6.4.3
* OpenSSL Toolkit 3.0.2
* OpenSSL Toolkit 1.1.1n
* Falco 0.31.1
* UFONet 1.8
* Samhain File Integrity Checker 4.4.7
* GRAudit Grep Auditing Tool 3.4
* Packet Fence 11.2.0

Kali Linux Tutorials

* DRAKVUF Sandbox : Automated Hypervisor-Level Malware Analysis System
* Checkov : Prevent Cloud Misconfigurations During Build-Time For Terraform
* StayKit : Cobalt Strike Kit For Persistence
* Katoolin3 : Get Your Favourite Kali Linux Tools On Debian/Ubuntu/Linux Mint
* NTLMRecon : Enumerate Information From NTLM Authentication Enabled Web Endpoints
* JNDI-Injection-Exploit : A Tool Which Generates JNDI Links Can Start Several Servers
* OpenSquat : Detection Of Phishing Domains And Domain Squatting.
* Win-Brute-Logon : Crack Any Microsoft Windows Users Password Without Any Privilege
* Scylla : The Simplistic Information Gathering Engine
* Jatayu : Stealthy Stand Alone PHP Web Shell

GBHackers Analysis

* Honda Bug Let Attackers Unlock and Start the Car
* Hundreds of HP Printer Models Affected by Critical Remote Code Execution
* CISA Has Added 15 New Flaws to the List of Actively Exploited Vulnerabilities
* FBI Warns that Hackers Gain Network Access by Exploiting MFA and "PrintNightmare" Vulnerability
* QNAP Escalation Vulnerability Let Attackers Gain Administrator Privileges and Inject Malicious Code

Weekly Cyber Security Video and Podcasts

SANS DFIR

* 10 años de inteligencia sobre ciberamenazas: De Berkeley Lab y IEEE/ACM Supercomputing a Google
* The First Purpose: Rediscovering Warning Analysis for CTI
* Building Strategic Return on Investment Through Cyber Intelligence
* Técnicas CTI para la caracterización de un ataque con ransomware

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

* NEW ZERO DAY: Are you ready for POP_CALC?
* Live Hacking Q&A with Kody Kinzie: WiFi CTF, QR Code Hacking, 3D Printing Fireworks, and More!
* LAPSUS$ Hacker Group Arrests; Okta Breached - ThreatWire

The PC Security Channel [TPSC]

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

Eli the Computer Guy

* Buzzfeed News STRIKE - FAILING employees DEMAND more money
* Apple Studio Display is AMAZING - sheeple are in awe
* Mac Studio SUCKS - Overgrown SmartPhone
* Graphics Card PRICES DROPPING - Biden lowers tariffs for computer parts

Security Now

* Targeted Exploitation - Ukrainian ISP Challenges, Kaspersky Labs Banned in the US, Chrome 0-Day
* Use After Free - OpenSSL Bug, Cybercrime Reporting Law, Node.js Supply Chain Compromise

Troy Hunt

* Weekly Update 289

Intel Techniques: The Privacy, Security, & OSINT Show

* 256-Extreme Privacy Fatigue

* 255-Dedicated VPN IP Addresses

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Packet Storm New Exploits For March, 2022
* WordPress Uleak Security Dashboard 1.2.3 Cross Site Scripting
* Spring Cloud Function SpEL Injection
* IdeaRE RefTree Path Traversal
* IdeaRE RefTree Shell Upload
* Chrome DeserializeFromMessage Validation Issue
* EG Free AntiVirus 2020 Privilege Escalation / Unquoted Service Path
* Spoofer 1.4.6 Privilege Escalation / Unquoted Service Path
* Medical Hub Directory Site 1.0 SQL Injection
* Message System 1.0 SQL Injection
* Message System 1.0 Cross Site Scripting
* Chrome safe_browsing::ThreatDetails::OnReceivedThreatDOMDetails Use-After-Free
* Joomla! 4.1.0 Zip Slip File Overwrite / Path Traversal
* WordPress Easy Cookie Policy 1.6.2 Cross Site Scripting
* WordPress CleanTalk 5.173 Cross Site Scripting
* Kramer VIAware 2.5.0719.1034 Remote Code Execution
* PostgreSQL 11.7 Remote Code Execution
* Medical Hub Directory Site 1.0 SQL Injection
* Medical Hub Directory Site 1.0 Shell Upload
* Medical Hub Directory Site 1.0 Cross Site Scripting
* Medical Hub Directory Site 1.0 Local File Inclusion
* CSZ CMS 1.2.9 SQL Injection
* WordPress Video-Synchro-PDF 1.7.4 Local File Inclusion
* WordPress Cab-Fare-Calculator 1.0.3 Local File Inclusion
* Atom CMS 1.0.2 Shell Upload

CXSecurity

* Atom CMS 1.0.2 Shell Upload
* PostgreSQL 11.7 Remote Code Execution
* Trend Micro Virtual Mobile Infrastructure 6.0.1278 Denial Of Service
* Xlight FTP 3.9.3.2 Buffer Overflow
* Amazing CD Ripper 1.2 Buffer Overflow
* Moodle 3.11.5 SQL Injection
* Dirty Pipe Local Privilege Escalation

Proof of Concept (PoC) & Exploits

Exploit Database

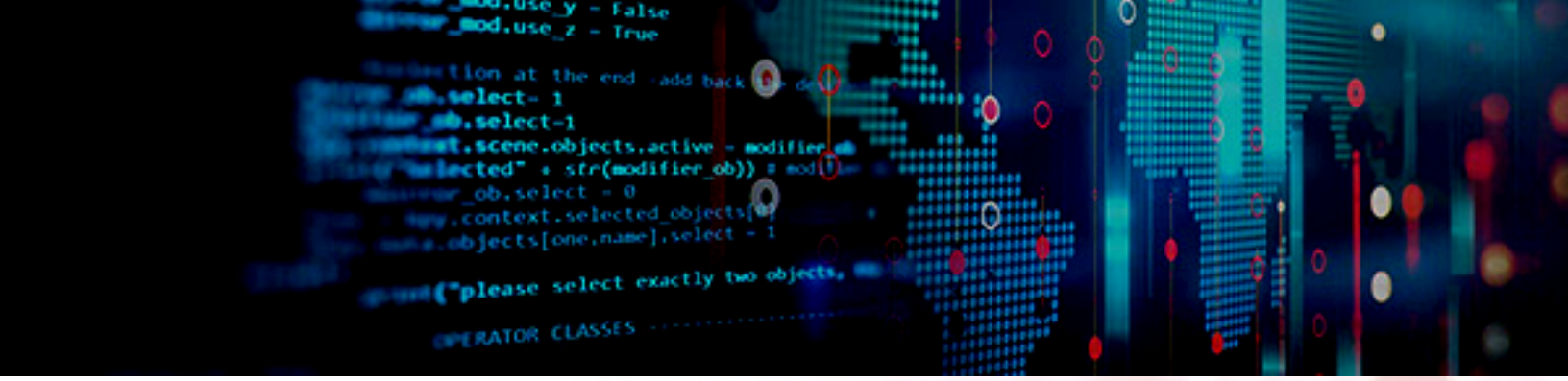
* [webapps] WordPress Plugin Easy Cookie Policy 1.6.2 - Broken Access Control to Stored XSS
* [remote] Kramer VIAware 2.5.0719.1034 - Remote Code Execution (RCE)
* [remote] PostgreSQL 9.3-11.7 - Remote Code Execution (RCE) (Authenticated)
* [webapps] CSZ CMS 1.2.9 - 'Multiple' Blind SQLi(Authenticated)
* [webapps] WordPress Plugin admin-word-count-column 2.2 - Local File Read
* [webapps] WordPress Plugin video-synchro-pdf 1.7.4 - Local File Inclusion
* [webapps] WordPress Plugin cab-fare-calculator 1.0.3 - Local File Inclusion
* [webapps] WordPress Plugin Curtain 1.0.2 - Cross-site Request Forgery (CSRF)
* [webapps] Drupal avatar_uploader v7.x-1.0-beta8 - Cross Site Scripting (XSS)
* [webapps] Atom CMS 2.0 - Remote Code Execution (RCE)
* [webapps] ImpressCMS 1.4.2 - Remote Code Execution (RCE)
* [webapps] WordPress Plugin amministrazione-aperta 3.7.3 - Local File Read - Unauthenticated
* [local] ProtonVPN 1.26.0 - Unquoted Service Path
* [remote] ICT Protege GX/WX 2.08 - Client-Side SHA1 Password Hash Disclosure
* [remote] ICT Protege GX/WX 2.08 - Stored Cross-Site Scripting (XSS)
* [local] Sysax FTP Automation 6.9.0 - Privilege Escalation
* [remote] Ivanti Endpoint Manager 4.6 - Remote Code Execution (RCE)
* [remote] iRZ Mobile Router - CSRF to RCE
* [webapps] ICEHRM 31.0.0.0S - Cross-site Request Forgery (CSRF) to Account Takeover
* [webapps] Wordpress Plugin iQ Block Country 1.2.13 - Arbitrary File Deletion via Zip Slip (Authentica
* [remote] Apache APISIX 2.12.1 - Remote Code Execution (RCE)
* [webapps] Tiny File Manager 2.4.6 - Remote Code Execution (RCE)
* [webapps] Pluck CMS 4.7.16 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Moodle 3.11.5 - SQLi (Authenticated)
* [local] VIVE Runtime Service - 'ViveAgentService' Unquoted Service Path

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*

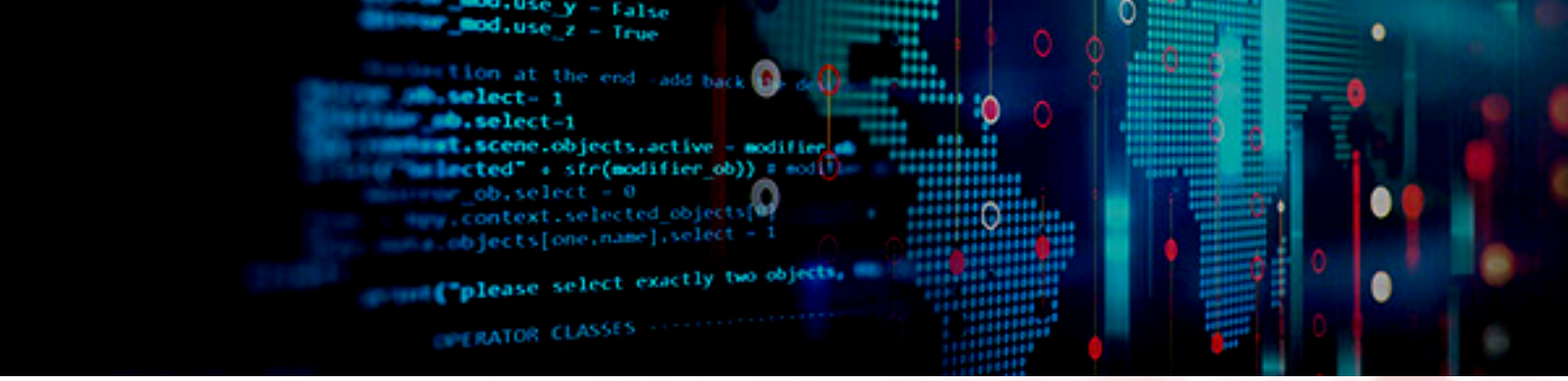
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://e-parcerias.cge.ce.gov.br/scc-ws-web/dock.htm
https://e-parcerias.cge.ce.gov.br/scc-ws-web/dock.htm notified by dock0d1
http://servidoronline.seplag.ce.gov.br/servidoronline/dck.html
http://servidoronline.seplag.ce.gov.br/servidoronline/dck.html notified by dock0d1
https://indicacaocoordenador.capes.gov.br/indicacaocoordenador/
https://indicacaocoordenador.capes.gov.br/indicacaocoordenador/ notified by dock0d1
http://rede.cultura.ce.gov.br
http://rede.cultura.ce.gov.br notified by theMx0nday
http://culturadendicasa.secult.ce.gov.br
http://culturadendicasa.secult.ce.gov.br notified by theMx0nday
https://consultapublica.secult.ce.gov.br
https://consultapublica.secult.ce.gov.br notified by son1x
https://sic.secult.ce.gov.br
https://sic.secult.ce.gov.br notified by son1x
https://leialdirblanc.secult.ce.gov.br
https://leialdirblanc.secult.ce.gov.br notified by son1x
https://bece.cultura.ce.gov.br
https://bece.cultura.ce.gov.br notified by son1x
https://auxiliosetoreventos.secult.ce.gov.br
https://auxiliosetoreventos.secult.ce.gov.br notified by son1x
https://agentesdeleitura.secult.ce.gov.br
https://agentesdeleitura.secult.ce.gov.br notified by son1x
http://www.hcdandacollo.gob.ar
http://www.hcdandacollo.gob.ar notified by 1877
http://www.andacollo.gob.ar
http://www.andacollo.gob.ar notified by 1877
http://www.picunleufu.gob.ar
http://www.picunleufu.gob.ar notified by 1877
http://www.cbn.gov.pk
http://www.cbn.gov.pk notified by Hunter Gujjar
http://www.cbokara.gov.pk
http://www.cbokara.gov.pk notified by Hunter Gujjar
http://www.cbdikhan.gov.pk
http://www.cbdikhan.gov.pk notified by Hunter Gujjar



Dark Web News

Darknet Live

Darkowl's Observations About Alphabay Are Ridiculous

DarkOwl, a company specializing in so-called "darknet intelligence,” believes there is "something larger transpiring” with the AlphaBay relaunch. I do not want to make any claims about the legitimacy of DeSnake or AlphaBay. His return is one of the most surprising things I have witnessed unfold in this sector. The relaunch elicited mixed reactions from users on Dread, XSS, Twitter, and elsewhere for obvious reasons. Feedback appears to be a mix of legitimate concerns (there is no way to prove the original DeSnake did not sell his PGP key to someone else) and unverified or downright incorrect claims (the feds verified that Cazes controlled DeSnake's account). Even in the indictment, feds separated DeSnake and alpha02. The cybersecurity company DarkOwl believes "something larger transpiring than a simple relaunch of the former marketplace.” However, the observations highlighted by the company's analysts that supposedly support their theory are just silly. The following points are from a DarkOwl blog post. Registration for the market and the forum seem unnecessarily complicated, including errors if the pin code started with '0' and asking for the user's "real name.” The concept of a real name is irrelevant in the darknet unless the administration is possibly trying to catch someone not in the "right-state-of-mind” slip-up and actually put their real name into that field. The DDoS protection and bot detection measures are excessive for a brand new marketplace. While navigating the domain manually, DarkOwl analysts regularly had to reset their Tor circuit and refresh their identity to simply view the vendor listings. The market includes an outrageous number of strict rules delineated as "global AlphaBay” versus rules specifically for "buyers” and "vendors.” There are no weapons allowed (where the previous AlphaBay had a weapons category), no Fentanyl sales allowed (where the previous AlphaBay had a 'Fent and RCs' category), no COVID-19 vaccine or cures can be offered, no ransomware sold or advertised, and no Commonwealth of Independent States (CIS) related countries activities allowed. The "About-Us” and Frequently Asked Questions (FAQ) sections are a laborious read with over 13,000 words combined - 8,200 for the FAQ section alone. Conversely, the original AlphaBay's FAQ was a mere 277 words. The overt exclusion of CIS countries is peculiar, especially given that DeSnake and alpha02 were openly active in Russian carding communities. According to DarkOwl Vision's archived documents, Russian speakers were present on the original AlphayBay forum and in interviews alpha02 spoke of how they "work with our Russian colleagues to enable each of us to enrich our base of vendors and buyers,” and clearly was not excluding users located in Russia. AlphaBay now only accepts the cryptocurrency Monero, and heavily promotes that users access it via I2P instead of Tor, calling their Tor services "mirrors” to the main I2P eepsite. DeSnake's detailed instructions for installing I2P on Dread fail to mention the potential risks of peer discovery and de-anonymization through known techniques like Eclipse and Sybil attacks in conjunction with flood-fill takeovers. Interestingly, the last known Monero-I2P-centric market was Liberitas, which went offline in June 2019 after a very short stint on the I2P network. DarkOwl could not confirm any prior darknet experience from the moderators DeSnake has installed as Staff on the market and forum. The new AlphaBay Marketplace refuses donations. It is unheard of that a darknet service would decline and discourage donations. A

fully-functional darknet marketplace will indeed provide sufficient financial resources in the future; yet refusing them from the start is unreal. DarkOwl has been active in this scene for a long time. They have some legitimately informative analysis on marketplaces. Surely their analysts know that these observations about AlphaBay are not any more convincing than random statements on Dread. To their credit, they did not publish outright lies. Although I am not sure it "is unheard of” that a market would not solicit donations. DarkOwl's statements in the rest of the blog post seem to imply that DeSnake is now much wordier than he used to be (although the word count bullet point in the list above only suggests that DeSnake did not write the original FAQ which is not relevent). I cannot really disagree with this and it might be a legitimate point in support of a theory of some sort. As to th i2p point, this person on Dread who claims to be a former LEO wrote that LE markets will encourage use of i2p.
dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/486ac94a84cdac803ed4 darkowl.com / archive.is bonus from 2017 with some of the same characters: Admins and staff of the largest darknet drug marketplace - Alphabay - have been doxxed on reddit even after paying an extortion amount of $45,000 (archive.org) (via darknetlive.com at https://darknetlive.com/post/darkowls-observations-about-alphabay-are-ridiculous/)

EU Parliament Votes for More Crypto Surveillance

Two European Parliament committees voted in favor of changes to the Transfer of Funds Regulation that target transactions to and from unhosted wallets. The Committee on Economic and Monetary Affairs and the Committee on Civil Liberties, Justice and Home Affairs voted in favor of amendments to the Transfer of Funds Regulation that "impose a host of new privacy invasions on wallet users,” according to Coinbase's Chief Legal Officer. The amendments are ostensibly aimed at cracking down on money laundering, but critics have voiced their concerns about the effects the amendments will have on privacy. And exchanges are naturally concerned about their ability to do business. "the possible anonymity offered by crypto assets transactions make crypto-assets particularly suitable for criminals” Coinbase CEO Brian Armstrong explained the impact the changes would have on a thread on Twitter. "Every crypto transaction (and not just those with a 1,000 euro threshold, as is the case with fiat) would be 'travel rule eligible,'” Armstrong wrote. "This means before you can send or receive crypto from a self-hosted wallet, Coinbase will be required to collect, store, and verify information on the other party, which is a not our customer, before the transfer is allowed.” "Moreover, any time you receive 1,000 euros or more in crypto from a self-hosted wallet, Coinbase will be required to report you to the authorities. This applies even if there is no indication of suspicious activity,” Armstrong explained. Unstoppable Finance (@UnstoppableDeFI) also shared information in a thread on Twitter about the impact the EU's proposal would have on smaller exchanges. "As this is completely unfeasible, we expect that companies like Coinbase would only allow transfers to unhosted wallets linked to their own customers and verified through a private key signing (which makes these transfers more complicated and costly),” the user wrote. "Smaller crypto companies with fewer resources might even go so far as to not allow any transfers to self-custody wallets anymore. This in turn, would cripple their competitiveness, and European users would turn towards foreign providers instead.” In December, Slovenian Finance Minister Andrej Šircelj said that the proposal would "[close] the gaps in our financial systems that are malevolently used by criminals to launder unlawful gains or finance terrorist activities.” Paul Grewal, the Chief Legal Officer at Coinbase, published a blog post in March expanding on the concerns outlined above. "Among the worst of the proposed provisions are new obligations on exchanges to collect, verify and report information on non-customers using self-hosted wallets. For instance, one provision requires exchanges to not only collect personal data about wallet users who are not their customers, but to also verify the data's accuracy before allowing a transfer to one of their customers. In fiat terms, this would basically mean you cannot take money out of your bank account to send to someone else until you share personal data with your financial institution about that person and verify their identity. Not only is this verification requirement nearly impossible to do but requiring exchanges to engage in extensive data collection, verification, and retention about non-customers runs against core EU data protection principles of data minimization and proportionality.” "Another dangerous provision would require exchanges to inform "competent

authorities” of every single transfer from a non-customer's self-hosted wallet equal to or greater than 1,000 EUR — regardless of any suspicion of bad activity. The proposal even leaves the door open to a total ban on transfers to self-hosted wallets even though there is no evidence that such a ban would have any impact on illicit activity at all. Like we said, bad facts make bad policy.” I have seen complaints from people, including some of the people quoted in this article, about the potential for bad actors (allegedly worse than the government) to access the information gathered by exchanges for nefarious purposes (i.e., only the government is allowed to take your money). @UnstoppableDeFi linked to a tweet from ZeroHedge about the shooting of "a 33-year-old French cryptocurrency expert at point-blank range” over a $450,000 Richard Mille watch. The victim, who lives in Honk Kong but was visiting New York, believes his attacker had followed him for "hours or days.” Yeah OK. While the attacker might have been following the 33-year-old for some time, I doubt that it had anything to do with his background in cryptocurrency. The shooting took place days after Los Angeles police warned that "wearing expensive jewelry in public could make them a target for thieves.” It surprises me that someone on the streets of the US would recognize a Richard Mille watch. The narrative above seems like the kind of take that can rally support from the average person without any interest in cryptocurrency (like how the push to legalize CBD "for health purposes” is obviously a foot in the door to marijuana legalization). The people committing such primitive robberies can simply look for crypto-rich people who openly flash their status on Twitter and Instagram. Also, does the EU matter at all? draft proposal: pdf votes: pdf (via darknetlive.com at https://darknetlive.com/post/eu-parliament-votes-for-more-crypto-surveillance/)

Man Convicted for Buying Grenades on the Darkweb

The Public Prosecution Service in the Netherlands asked a court to impose a sentence of 36 months imprisonment on a man convicted of attempting to import hand grenades from the United States. According to a press release from the Public Prosecution Service, in addition to being convicted of attempting to import two hand grenades purchased through the dark web, the 42-year-old defendant was also found guilty of selling dextroamphetamine and GBL on the Dark Web. The investigation that resulted in the defendant's arrest and conviction began on March 20, 2017, after the National International Legal Aid Center (LIRC) received information that a resident of the Netherlands was trying to purchase hand grenades on the darkweb. Grenade detonators/igniters Authorities made a controlled delivery of a package that contained two deactivated detonators to the address the defendant had given the "weapons vendor” when purchasing the grenades. Investigators arrested the 42-year-old and the other house occupants after completing the delivery. "My client was waiting for another package he ordered via the dark web, with memory cards,” Johan Mühren, the defendant's attorney, said. "Not [waiting for] a package with two hand grenades in it, but because he accepted the package, the police also think he had made the order.” Searches on properties associated with the 42-year-old resulted in the seizure of many pills and an undisclosed amount of money in a safe. The investigators also found and seized manuals on the production of explosives and methamphetamine. Further investigations revealed that the buyer inquired through email about purchasing 500 grams of Semtex, C-4, and four detonators from the US-based vendor. The investigators also found out that the defendant had distributed dextroamphetamine and GBL through the darkweb. The public prosecutor asked the court to sentence the defendant to a total of 3 years in prison, of which one year will be conditional. The prosecutor also demanded that the defendant forfeit 311,797 euros. archive.is archive.org [DNL: That Europol picture is a genuine Europol graphic by the way.] kek. (via darknetlive.com at https://darknetlive.com/post/man-convicted-for-buying-grenades-on-the-darkweb/)

West Virginian Admits Buying Drugs on the Darkweb

A West Virginia man pleaded guilty to importing and reselling drugs purchased through the darkweb. According to court documents, 42-year-old Joshua Lee Parsons of West Virginia admitted to purchasing a wide variety of drugs, including methamphetamine and heroin, on the darkweb. Parsons resold the drugs locally. The investigations that resulted in Parsons' arrest began on February 24, 2021, after the United States Customs and Border Protection at the John F. Kennedy International Mail Center in New York intercepted a

suspicious incoming package addressed to Parsons' residence. When opening the package, the customs officers found 49 grams of heroin. Joshua Lee Parsons | @WVMugshots The investigators subsequently made a controlled delivery of the package to Parsons' home on March 8, 2021. After making the delivery, the investigators executed a search warrant at the residence. The search resulted in the seizure of various drugs, including approximately 66 grams of methamphetamine packaged in 103 separate packages. The investigators also found and seized a loaded handgun. Parsons confessed in the interview that followed his arrest and told the investigators wanted to resell the methamphetamine found in his possession. Parsons also told the investigators that he had placed another order on the darkweb and was expecting to receive a methamphetamine package. The investigators intercepted the package on March 15, 2021, and seized approximately 223 grams of methamphetamine. On March 17, 2022, Parsons pleaded guilty to possession with intent to distribute 50 grams or more of methamphetamine. He will be sentenced on June 30, 2022, and will face a mandatory minimum of 10 years in prison. [DNL: In addition to LEOs from Homeland Security Investigations, the USPIS, and state police, members of the West Virginia National Guard Reconnaissance and Aerial Interdiction Detachment assisted in the execution of a search warrant at Parsons' house. Seems atypical for such a unspectacular case.] archive.is/archive.org indictment, plea (via darknetlive.com at https://darknetlive.com/post/west-virginian-admits-buying-drugs-on-the-darkweb/)

Dark Web Link

Top Darknet Markets 2022: The Outstanding Performances To Consider Now

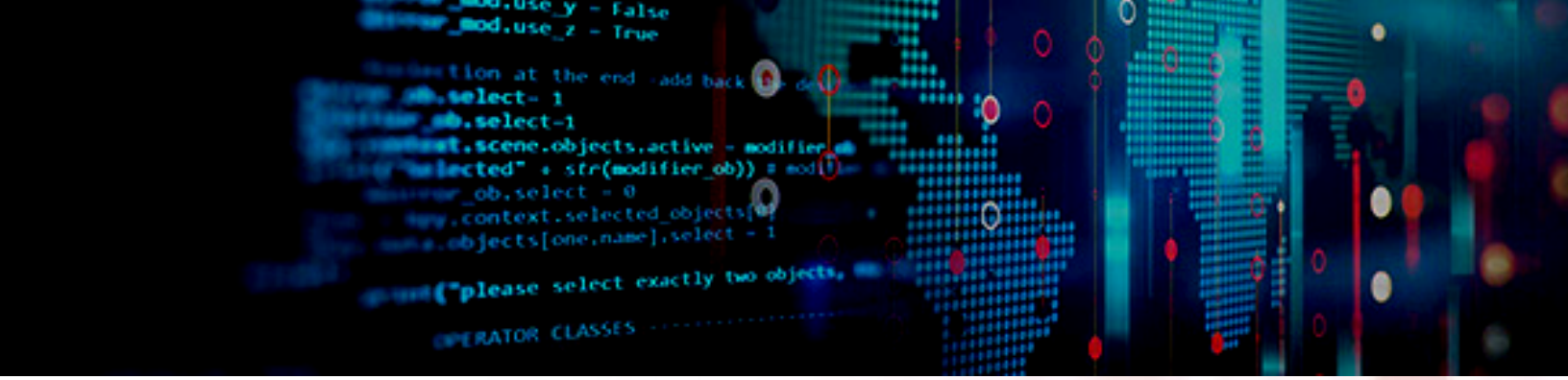
The darknet markets are subject to availability and one of the many factors that contributes to the working of these dark web markets is their performances. The top darknet markets 2022 is the example where each of the marketplaces in the Tor network has proven its performance over and over again. So,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

Breaking Bad Forum On The Darknet Is Revolutionary

The Breaking Bad Forum housed by the Tor network is a revolutionary darknet site indeed! So many forums exist on the dark web. But nothing could match the vibe of something like Breaking Bad. In this article, we will take you through the various aspects of the new forum. Breaking Bad Forum: A Gist Breaking [...] The post Breaking Bad Forum On The Darknet Is Revolutionary appeared first on Dark Web Link | Deep web Onion Links | Darknet News.

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

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



Trend Micro Anti-Malware Blog

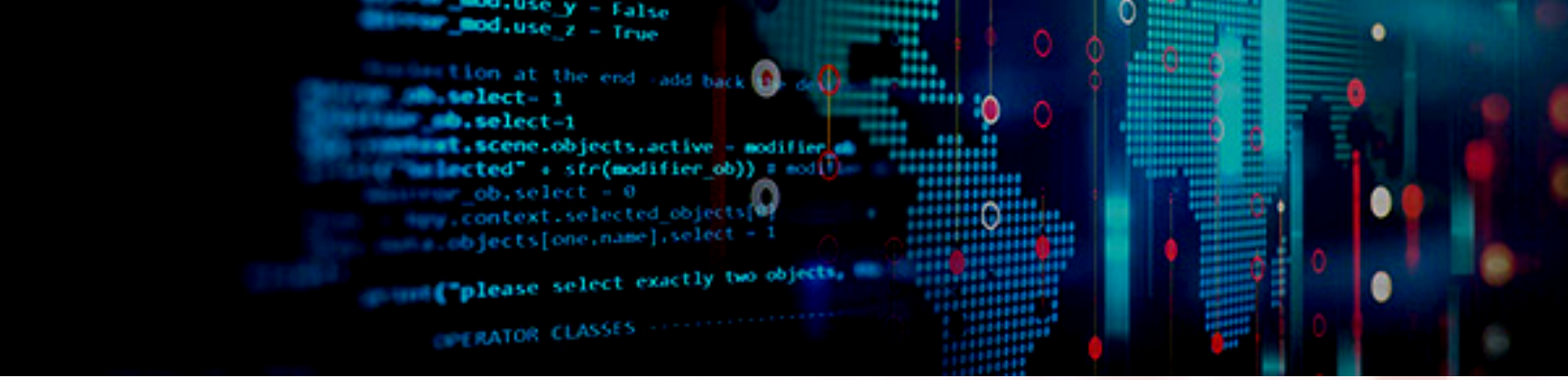
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

* RiskIQ Threat Intelligence Roundup: Campaigns Targeting Ukraine and Global Malware Infrastructure
* RiskIQ Threat Intelligence Supercharges Microsoft Threat Detection and Response
* RiskIQ Intelligence Roundup: Spoofed Sites and Surprising Infrastructure Connections
* RiskIQ Threat Intelligence Roundup: QBot, Magecart, Agent Tesla Headline Hijacked Infrastructure
* 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

FireEye

* Securing Your Applications Against Spring4Shell (CVE-2022-22965)
* Metasploit Weekly Wrap-Up
* Update on Spring4Shell's Impact on Rapid7 Solutions and Systems
* MITRE Engenuity ATT&CK Evaluation: InsightIDR Drives Strong Signal-to-Noise
* 4 Fallacies That Keep SMBs Vulnerable to Ransomware, Pt. 2
* Spring4Shell: Zero-Day Vulnerability in Spring Framework (CVE-2022-22965)
* [Security Nation] David Rogers on IoT Security Legislation
* Demystifying XDR: The Time for Implementation Is Now
* Cloud Pentesting, Pt. 2: Testing Across Different Deployments
* CVE-2022-1026: Kyocera Net View Address Book Exposure



Advisories

US-Cert Alerts & bulletins

* Apple Releases Security Updates
* Spring Releases Security Updates Addressing "Spring4Shell" and Spring Cloud Function Vulnerabilities
* CISA Releases Security Advisories for Rockwell Automation Products
* FBI Releases PIN on Ransomware Straining Local Governments and Public Services
* CISA Adds Seven Known Exploited Vulnerabilities to Catalog
* FBI Releases PIN on Phishing Campaign against U.S. Election Officials
* Google Releases Security Updates for Chrome
* Mitigating Attacks Against Uninterruptable Power Supply Devices
* AA22-083A: Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targe
* AA22-076A: Strengthening Cybersecurity of SATCOM Network Providers and Customers
* Vulnerability Summary for the Week of March 21, 2022
* Vulnerability Summary for the Week of March 14, 2022

Zero Day Initiative Advisories

ZDI-CAN-16957: Adobe
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'kdot' was reported to the affected vendor on: 2022-04-01, 3 days ago. The vendor is given until 2022-07-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-16919: Adobe
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-04-01, 3 days ago. The vendor is given until 2022-07-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-16952: Adobe
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'kdot' was reported to the affected vendor on: 2022-04-01, 3 days ago. The vendor is given until 2022-07-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-16679: Sante
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Eunice' was reported to the affected vendor on: 2022-04-01, 3 days ago. The vendor is given until 2022-07-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-15727: D-Link
A CVSS score 8.8 (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-04-01, 3 days ago. The vendor is given until 2022-07-30 to

publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-17032: Google

A CVSS score 4.5 (AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Eduardo Braun Prado' was reported to the affected vendor on: 2022-04-01, 3 days ago. The vendor is given until 2022-07-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-17016: Linux

A CVSS score 6.7 (AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:L) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) and Reno Robert of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-04-01, 3 days ago. The vendor is given until 2022-07-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15728: D-Link

A CVSS score 8.8 (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-04-01, 3 days ago. The vendor is given until 2022-07-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16777: 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 'KMFL' was reported to the affected vendor on: 2022-04-01, 3 days ago. The vendor is given until 2022-07-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-15935: D-Link

A CVSS score 8.8 (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-04-01, 3 days ago. The vendor is given until 2022-07-30 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-17000: 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: 2022-03-30, 5 days ago. The vendor is given until 2022-07-28 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-17002: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-03-30, 5 days ago. The vendor is given until 2022-07-28 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-16998: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-03-30, 5 days ago. The vendor is given until 2022-07-28 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-17001: 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: 2022-03-30, 5 days ago. The vendor is given until 2022-07-28 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-17012: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of

Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-03-30, 5 days ago. The vendor is given until 2022-07-28 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-16795: Microsoft

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2022-03-30, 5 days ago. The vendor is given until 2022-07-28 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-16774: Advantech

A CVSS score 8.2 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2022-03-30, 5 days ago. The vendor is given until 2022-07-28 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-16509: ICONICS

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 'Chris Anastasio and Steven Seeley of Incite Team' was reported to the affected vendor on: 2022-03-30, 5 days ago. The vendor is given until 2022-07-28 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-16778: Foxit

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Suyue Guo and Wei You from Renmin University of China' was reported to the affected vendor on: 2022-03-30, 5 days ago. The vendor is given until 2022-07-28 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-16796: Microsoft

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2022-03-30, 5 days ago. The vendor is given until 2022-07-28 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-16768: Microsoft

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2022-03-30, 5 days ago. The vendor is given until 2022-07-28 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-16747: Advantech

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 '@rgod777' was reported to the affected vendor on: 2022-03-30, 5 days ago. The vendor is given until 2022-07-28 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-16797: Microsoft

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2022-03-30, 5 days ago. The vendor is given until 2022-07-28 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-16828: Foxit

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'KMFL' was reported to the affected vendor on: 2022-03-30, 5 days ago. The vendor is given until 2022-07-28 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

Apple Security Advisory 2022-03-31-2

Apple Security Advisory 2022-03-31-2 - macOS Monterey 12.3.1 addresses code execution, out of bounds read, and out of bounds write vulnerabilities.

Ubuntu Security Notice USN-5362-1

Ubuntu Security Notice 5362-1 - Nick Gregory discovered that the Linux kernel incorrectly handled network offload functionality. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. Enrico Barberis, Pietro Frigo, Marius Muench, Herbert Bos, and Cristiano Giuffrida discovered that hardware mitigations added by ARM to their processors to address Spectre-BTI were insufficient. A local attacker could potentially use this to expose sensitive information.

Ubuntu Security Notice USN-5361-1

Ubuntu Security Notice 5361-1 - It was discovered that the VFIO PCI driver in the Linux kernel did not properly handle attempts to access disabled memory spaces. A local attacker could use this to cause a denial of service. Mathy Vanhoef discovered that the Linux kernel's WiFi implementation did not properly verify certain fragmented frames. A physically proximate attacker could possibly use this issue to inject or decrypt packets.

Ubuntu Security Notice USN-5358-2

Ubuntu Security Notice 5358-2 - It was discovered that the network traffic control implementation 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. It was discovered that the IPsec implementation in the Linux kernel did not properly allocate enough memory when performing ESP transformations, leading to a heap-based buffer overflow. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5357-2

Ubuntu Security Notice 5357-2 - It was discovered that the IPsec implementation in the Linux kernel did not properly allocate enough memory when performing ESP transformations, leading to a heap-based buffer overflow. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5360-1

Ubuntu Security Notice 5360-1 - It was discovered that Tomcat incorrectly performed input verification. A remote attacker could possibly use this issue to intercept sensitive information. It was discovered that Tomcat did not properly deserialize untrusted data. An attacker could possibly use this issue to execute arbitrary code. It was discovered that Tomcat did not properly validate the input length. An attacker could possibly use this to trigger an infinite loop, resulting in a denial of service.

Ubuntu Security Notice USN-5359-1

Ubuntu Security Notice 5359-1 - Danilo Ramos discovered that rsync incorrectly handled memory when performing certain zlib deflating operations. An attacker could use this issue to cause rsync to crash, resulting in a denial of service, or possibly execute arbitrary code.

Ubuntu Security Notice USN-5356-1

Ubuntu Security Notice 5356-1 - Alexandre Bartel discovered that DOSBox incorrectly handled long lines in certain files. An attacker could possibly use this issue to execute arbitrary code. Alexandre Bartel discovered that DOSBox incorrectly performed access control over certain directories. An attacker could possibly use this issue to execute arbitrary code.

Ubuntu Security Notice USN-5358-1

Ubuntu Security Notice 5358-1 - It was discovered that the network traffic control implementation 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. It was discovered that the IPsec implementation in the Linux kernel did not properly allocate enough memory when performing ESP transformations, leading to a heap-based buffer overflow. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-5357-1

Ubuntu Security Notice 5357-1 - It was discovered that the IPsec implementation in the Linux kernel did not properly allocate enough memory when performing ESP transformations, leading to a heap-based buffer

overflow. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.
Ubuntu Security Notice USN-5355-2
Ubuntu Security Notice 5355-2 - USN-5355-1 fixed a vulnerability in zlib. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. Danilo Ramos discovered that zlib incorrectly handled memory when performing certain deflating operations. An attacker could use this issue to cause zlib to crash, resulting in a denial of service, or possibly execute arbitrary code.
Ubuntu Security Notice USN-5355-1
Ubuntu Security Notice 5355-1 - Danilo Ramos discovered that zlib incorrectly handled memory when performing certain deflating operations. An attacker could use this issue to cause zlib to crash, resulting in a denial of service, or possibly execute arbitrary code.
Ubuntu Security Notice USN-5354-1
Ubuntu Security Notice 5354-1 - It was discovered that Twisted incorrectly filtered HTTP headers when clients are being redirected to another origin. A remote attacker could use this issue to obtain sensitive information. It was discovered that Twisted incorrectly processed SSH handshake data on connection establishments. A remote attacker could use this issue to cause Twisted to crash, resulting in a denial of service.
Ubuntu Security Notice USN-5351-2
Ubuntu Security Notice 5351-2 - USN-5351-1 fixed a vulnerability in Paramiko. This update provides the corresponding update for Ubuntu 16.04 ESM. Jan Schejbal discovered that Paramiko incorrectly handled permissions when writing private key files. A local attacker could possibly use this issue to gain access to private keys.
Ubuntu Security Notice USN-5350-1
Ubuntu Security Notice 5350-1 - It was discovered that Chromium incorrectly handled certain inputs. An attacker could possibly use this issue to execute arbitrary code.
Red Hat Security Advisory 2022-1102-01
Red Hat Security Advisory 2022-1102-01 - The httpd packages provide the Apache HTTP Server, a powerful, efficient, and extensible web server. Issues addressed include an HTTP request smuggling vulnerability.
Red Hat Security Advisory 2022-1106-01
Red Hat Security Advisory 2022-1106-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include privilege escalation and use-after-free vulnerabilities.
Red Hat Security Advisory 2022-1107-01
Red Hat Security Advisory 2022-1107-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include privilege escalation and use-after-free vulnerabilities.
Red Hat Security Advisory 2022-1112-01
Red Hat Security Advisory 2022-1112-01 - OpenSSL is a toolkit that implements the Secure Sockets Layer and Transport Layer Security protocols, as well as a full-strength general-purpose cryptography library.
Red Hat Security Advisory 2022-1104-01
Red Hat Security Advisory 2022-1104-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include privilege escalation and use-after-free vulnerabilities.
Red Hat Security Advisory 2022-1110-01
Red Hat Security Advisory 2022-1110-01 - Red Hat Decision Manager is an open source decision management platform that combines business rules management, complex event processing, Decision Model & Notation execution, and Business Optimizer for solving planning problems. It automates business decisions and makes that logic available to the entire business. This release of Red Hat Decision Manager 7.12.1 serves as an update to Red Hat Decision Manager 7.12.0, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include code execution, denial of service, information leakage, and traversal vulnerabilities.
Red Hat Security Advisory 2022-1103-01
Red Hat Security Advisory 2022-1103-01 - 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 privilege escalation

and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-1108-01

Red Hat Security Advisory 2022-1108-01 - Red Hat Process Automation Manager is an open source business process management suite that combines process management and decision service management and enables business and IT users to create, manage, validate, and deploy process applications and decision services. This release of Red Hat Process Automation Manager 7.12.1 serves as an update to Red Hat Process Automation Manager 7.12.0, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include code execution, denial of service, information leakage, and traversal vulnerabilities.

Ubuntu Security Notice USN-5313-2

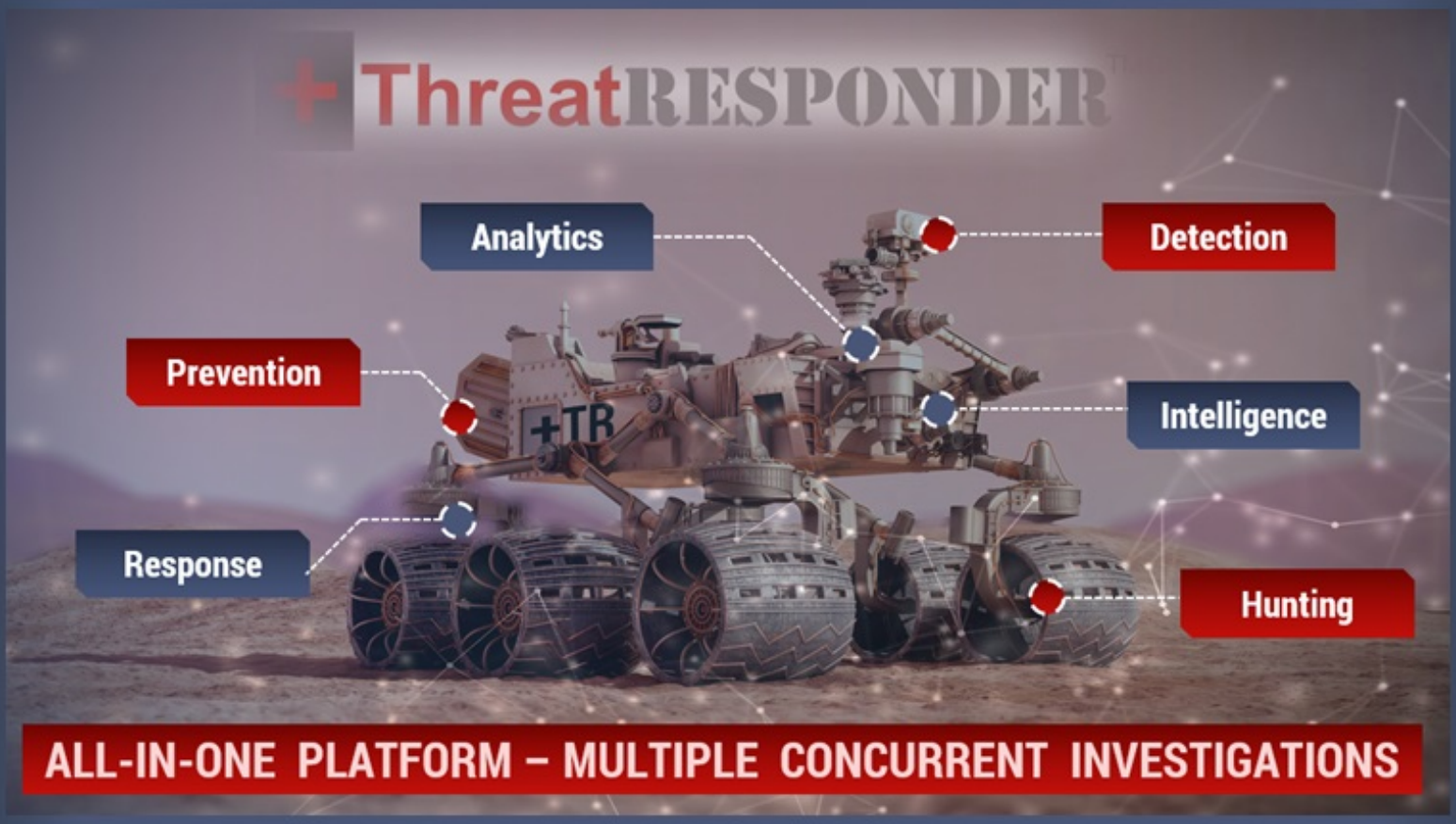
Ubuntu Security Notice 5313-2 - USN-5313-1 fixed vulnerabilities and added features in OpenJDK. Unfortunately, that update introduced a regression in OpenJDK 11 that could impact interoperability with some popular HTTP/2 servers making it unable to connect to said servers. This update fixes the problem.

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



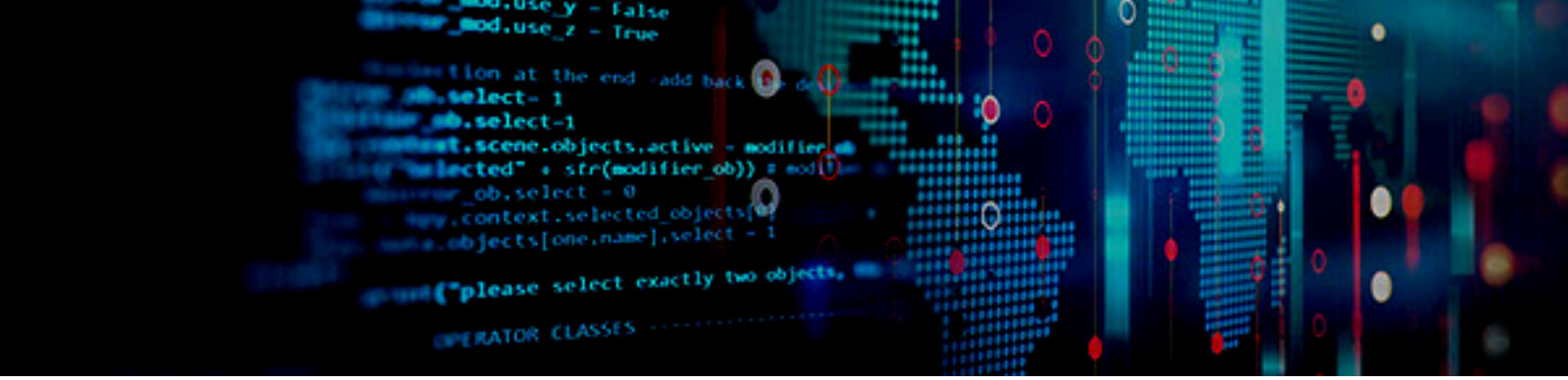
The Solution – ThreatResponder® Platform

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

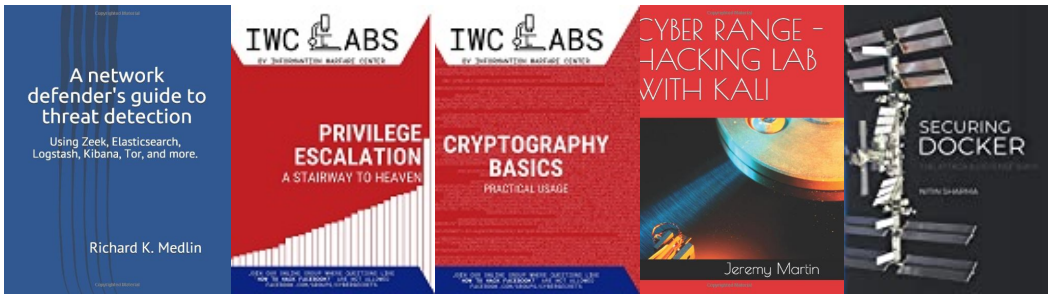


The Cyber Secrets publications on Amazon

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