Jan-24-22

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

January 24, 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

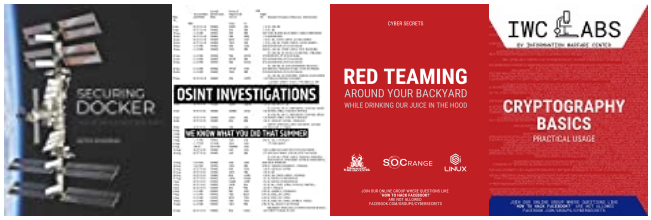
Internet Storm Center Infocon Status

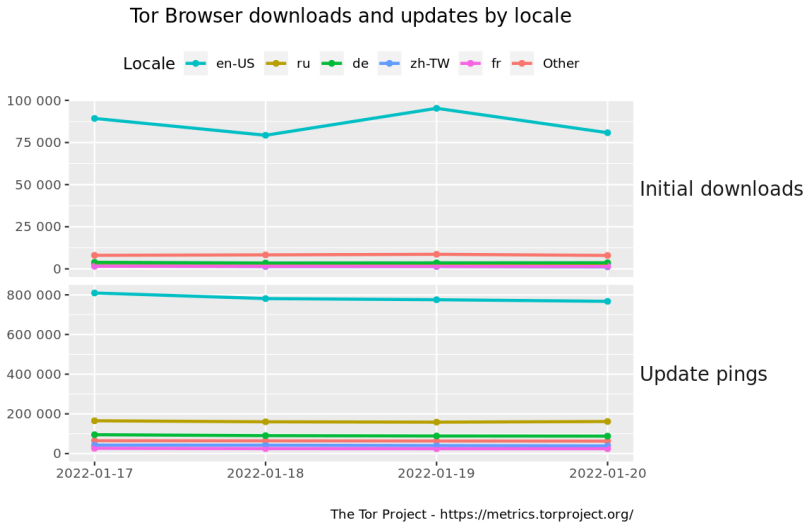
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

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

* EU Wants To Build Its Own DNS Infrastructure With Built-In Filtering Capabilities
* Spamhaus Botnet Threat Update: Q4-2021
* Chinese APT Deploys MoonBounce Implant In UEFI Firmware
* 2FA Bypassed In $34.6M Crypto.com Heist
* Nasty Linux Kernel Bug Found And Fixed
* MPs Criticize Cyber Agency For Not Aiding China Rights Group After It Was Hacked
* New York Mayor Adams To Receive First Paycheck In Cryptocurrency
* White Hat Hackers Returns $1 Million Stolen In Crypto Theft Disaster
* Red Cross Begs Attackers Not To Leak Stolen Data For 515k People
* Cheap Malware Is Behind A Rise In Attacks On Cryptocurrency Wallets
* Safari Is Apparently Failing To Respect Same Origin Policy
* Microsoft Patches The Patch That Broke VPN
* Crypto.com Says Alleged $15 Million Hack Was Just An Incident
* Zoom Vulnerabilities Impact Clients, MMR Servers
* Cloned Dept. Of Labor Site Hawks Fake Government Contracts
* Beijing Olympic App Flaws Allow Man-In-The-Middle Attacks
* This New Ransomware Comes With A Small But Dangerous Payload
* Microsoft Warns Of Destructive Disk Wiper Targeting Ukraine
* Critical ManageEngine Desktop Server Bug Opens Orgs To Malware
* Organizations Face A Losing Battle Against Vulnerabilities
* 10 Nations Coordinate Shutdown Of Ransomware VPN Service
* Panic As Kosovo Pulls The Plug On Its Energy Guzzling Bitcoin Miners
* North Korean Hackers Stole Nearly $400 Million In Crypto Last Year
* Tonga Comms May Be Down For Two Weeks Due To Tsunami
* Linux Malware Is On The Rise. Here Are Three Top Threats Right Now

Krebs on Security

Dark Reading

* IT Leaders Consider Security Tech a Part of Business Transformation
* Fraud Is On the Rise, and It's Going to Get Worse
* REvil Ransomware Gang Arrests Trigger Uncertainty, Concern in Cybercrime Forums
* Looking Beyond Biden's Binding Security Directive
* Biden Broadens NSA Oversight of National Security Systems
* (ISC)² Appoints Jon France, CISSP, as Chief Information Security Officer
* Researchers Discover Dangerous Firmware-Level Rootkit
* Automating Response Is a Marathon, Not a Sprint
* Red Cross Hit via Third-Party Cyberattack
* Enterprises Are Sailing Into a Perfect Storm of Cloud Risk
* 4 Ways to Develop Your Team's Cyber Skills
* Cisco's Kenna Security Research Shows the Relative Likelihood of an Organization Being Exploited
* FireEye & McAfee Enterprise Renamed as Trellix
* What Happens to My Organization If APIs Are Compromised?
* Nigerian Police Arrest 11 Individuals in BEC Crackdown
* Revamped Community-Based DDoS Defense Tool Improves Filtering
* 1Password Raises $620M Series C, Now Valued at $6.8B
* 5 AI and Cybersecurity Predictions for 2022
* When Patching Security Flaws, Smarter Trumps Faster
* Cloud Adoption Widens the Cybersecurity Skills Gap

The Hacker News

* Emotet Now Using Unconventional IP Address Formats to Evade Detection
* High-Severity Rust Programming Bug Could Lead to File, Directory Deletion
* Experts Find Strategic Similarities b/w NotPetya and WhisperGate Attacks on Ukraine
* Molerats Hackers Hiding New Espionage Attacks Behind Public Cloud Infrastructure
* Hackers Planted Secret Backdoor in Dozens of WordPress Plugins and Themes
* Critical Bugs in Control Web Panel Expose Linux Servers to RCE Attacks
* Chinese Hackers Spotted Using New UEFI Firmware Implant in Targeted Attacks
* U.S. Sanctions 4 Ukrainians for Working with Russia to Destabilize Ukraine
* Cisco Issues Patch for Critical RCE Vulnerability in RCM for StarOS Software
* Google Details Two Zero-Day Bugs Reported in Zoom Clients and MMR Servers
* Interpol Busted 11 Members of Nigerian BEC Cybercrime Gang
* DoNot Hacking Team Targeting Government and Military Entities in South Asia
* A Trip to the Dark Site - Leak Sites Analyzed
* New BHUNT Password Stealer Malware Targeting Cryptocurrency Wallets
* Hackers Attempt to Exploit New SolarWinds Serv-U Bug in Log4Shell Attacks

Security Week

* Cloud Security Provider Anitian Raises $55 Million
* CISA Releases Final IPv6 Security Guidance for Federal Agencies
* DoH Makes It Difficult to Track Botnets: Spamhaus
* F5 Patches Two Dozen Vulnerabilities in BIG-IP
* Industry Reactions to Biden Cybersecurity Memo: Feedback Friday
* High-Severity Vulnerabilities Patched in McAfee Enterprise Product
* Dark Web Chatter: What Other Russian Hackers Are Saying About the REvil Arrests
* FBI Warns Organizations of Diavol Ransomware Attacks
* Insurance and Fintech Firm Acrisure Launches Cyber Services Division
* Nigerian Authorities Arrest 11 Members of Prolific BEC Fraud Group
* Security Scanners Across Europe Tied to China Govt, Military
* Prolific Chinese APT Caught Using 'MoonBounce' UEFI Firmware Implant
* Cyber Insights 2022: Nation-States
* Cisco Patches Critical Vulnerability in RCM for StarOS
* Seven Ways to Ensure Successful Cross-Team Security Initiatives
* Resurrected jQuery UI Library Haunts Websites, Enterprise Products
* Software Supply Chain Attacks Tripled in 2021: Study
* SolarWinds Patches Serv-U Vulnerability Propagating Log4j Attacks
* Data of 7 Million OpenSubtitles Users Leaked After Hack Despite Site Paying Ransom
* Red Cross Appeals to Hackers After Major Cyberattack
* NSA Authorized to Issue Binding Operational Directives to Boost NSS Cybersecurity
* Google Pays Out Over $100,000 for Vulnerabilities Patched With Chrome 97 Update
* Living Off the "Edge" of the Land
* Kaspersky Launches New Service for Removing Malicious Domains
* Red Cross Falls Victim to Massive Cyberattack

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* FBI: US Defense Industry Organizations Targeted with USB-Based Ransomware Attacks
* New U.K. Vishing Scam Offers Significant Phone Plan Discounts in Exchange for your Phone Provider's O
* In Order to Have Good Security Culture, Behaviour Comes First
* DHL is Now the Most Spoofed Brand in Phishing
* Ransomware Attacks are Growing in Number, But Not in Sophistication
* Google Docs Comment Feature is the Key to a New Wave of Phishing Campaigns
* Half of All Organizations Hit by Ransomware Experience Productivity Loss
* KnowBe4's Top-Clicked Phishing Email Results for Q4 2021 Compare the U.S. and EMEA [INFOGRAPHIC]
* A Cyberespionage Group Uses Social Engineering
* CyberheistNews Vol 12 #03 FBI: Beware of a New Google Voice Authentication Scam - Even if You Don't U

ISC2.org Blog

* TIME TO HIT THE BOOKS! TRAINING COURSE IS AVAILABLE FOR CANDIDATES PREPARING FOR THE NEW (ISC)²
* No Excuses: Get Your (ISC)² Certification Done in 2022
* A Cybersecurity Role Has Topped List of Best Jobs
* Help Shape The CSSLP Exam
* The Future of Work without Workers

HackRead

* OpenSubtitles Hacked- Data Breach Affected 7 Million Subscribers
* Multichain hack: Hacker returns $1 million, keeps $150k as bug bounty
* How to Transfer Your Data between iPhone and Computer Safely
* The Risks of Using Online Video Converter
* VirusTotal hacking - Hackers can access trove of stolen credentials on VirusTotal
* Guardio Review: Can This Browser Extension Really Protect You From Cybercrime?
* FBI - Malicious QR codes stealing login and financial data

Koddos

* OpenSubtitles Hacked- Data Breach Affected 7 Million Subscribers
* Multichain hack: Hacker returns $1 million, keeps $150k as bug bounty
* How to Transfer Your Data between iPhone and Computer Safely
* The Risks of Using Online Video Converter
* VirusTotal hacking - Hackers can access trove of stolen credentials on VirusTotal
* Guardio Review: Can This Browser Extension Really Protect You From Cybercrime?
* FBI - Malicious QR codes stealing login and financial data

Naked Security

* Cryptocoin broker Crypto.com says 2FA bypass led to $35m theft
* S3 Ep66: Cybercrime busts, wormable Windows, and the crisis of featuritis [Podcast + Transcript]
* Serious Security: Apple Safari leaks private data via database API - what you need to know
* Romance scammer who targeted 670 women gets 28 months in jail
* Serious Security: Linux full-disk encryption bug fixed - patch now!
* REvil ransomware crew allegedly busted in Russia, says FSB
* S3 Ep65: Supply chain conniption, NetUSB hole, Honda flashback, FTC muscle [Podcast + Transcript]
* Wormable Windows HTTP hole - what you need to know
* Home routers with NetUSB support could have critical kernel hole
* JavaScript developer destroys own projects in supply chain "lesson"

Threat Post

* The Internet's Most Tempting Targets
* Merck Awarded $1.4B Insurance Payout over NotPetya Attack
* 20K WordPress Sites Exposed by Insecure Plugin REST-API
* McAfee Bug Can Be Exploited to Gain Windows SYSTEM Privileges
* Spyware Blitzes Compromise, Cannibalize ICS Networks
* 2FA Bypassed in $34.6M Crypto.com Heist: What We Can Learn
* Critical Cisco StarOS Bug Grants Root Access via Debug Mode
* Microsoft: Attackers Tried to Login to SolarWinds Serv-U Via Log4j Bug
* Pervasive Apple Safari Bug Exposes Web-Browsing Data, Google IDs
* Red Cross Begs Attackers Not to Leak Stolen Data for 515K People

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

* Magecart Attacks Continue to 'Skim' Software Supply Chains
* What Your Team Can Learn From the DHS Cybersecurity Hiring Program
* Reactive Cybersecurity: How to Get it Right
* Cybersecurity Trends: IBM's Predictions for 2022
* Insider Threats: How to Combat Workplace Disinformation
* 3 Cloud Security Trends to Watch in 2022
* What It Takes to Build the Blue Team of Tomorrow
* The State of Credential Stuffing Attacks
* Small Business Cybersecurity: What Will Be Different in 2022?
* The Great Resignation: How to Acquire and Retain Cybersecurity Talent

InfoWorld

* Rust 1.58.1 fixes dangerous race condition
* What's new in Rust 1.58 and Rust 1.58.1
* The forces behind enterprise cloud spending trends
* What is Google Cloud Anthos? Managed Kubernetes everywhere
* JDK 18: The new features in Java 18
* Understand Diffie-Hellman key exchange
* Faker NPM package back on track after malicious coding incident
* Securing Azure Kubernetes networking with Calico
* Airtable review: Flexible low-code/no-code in the cloud
* Suse open sources NeuVector container security platform

C4ISRNET - Media for the Intelligence Age Military

* Space Force expands on-orbit 'neighborhood watch' mission with two new tracking satellites
* New NATO policy positions the alliance as a broker, not an owner, in space race
* AFRL partners with SpaceX to explore Rocket Cargo potential
* Contractors demonstrate single-user drone swarm at DARPA experiment
* National Reconnaissance Office awards five contracts for commercial satellite radar capabilities
* At Project Convergence, Army's new battle command system demonstrated expanded capability
* New DARPA research could make night vision goggles smaller
* Military may take months to gauge 5G safety risks to aircraft
* Webcast: Managing the Military's Data
* Get ready for 'computer-assisted' shooting with the Army's new optic

The Hacker Corner

Conferences

* Marketing Cybersecurity In 2021
* 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 "New" Conference Concept: The Hybrid
* Best Ways To Market A Conference
* Marketing To Cybersecurity Companies
* Upcoming Black Hat Events (2021)

Google Zero Day Project

* Zooming in on Zero-click Exploits
* A deep dive into an NSO zero-click iMessage exploit: Remote Code Execution

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.

* Insomni'hack teaser 2022
* DiceCTF 2022
* Cyber Grabs CTF 0x03 Junior
* STAY ~/ CTF 2022
* Hayyim CTF 2022
* Decompetition v2.0
* #kksctf open / 5th anniversary edition
* VU CYBERTHON 2022
* CInsects CTF 2022
* TSJ 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

* GRAudit Grep Auditing Tool 3.3
* AIDE 0.17.4
* Clam AntiVirus Toolkit 0.104.2
* Proxmark3 4.14831
* Faraday 3.19.0
* Haveged 1.9.17
* Haveged 1.9.16
* SQLMAP - Automatic SQL Injection Tool 1.6
* Wireshark Analyzer 3.6.1
* Wapiti Web Application Vulnerability Scanner 3.0.9

Kali Linux Tutorials

* Kit_Hunter : A Basic Phishing Kit Scanner For Dedicated And Semi-Dedicated Hosting
* Digital-Forensics-Lab : Free Hands-On Digital Forensics Labs For Students And Faculty
* OffensiveRust : Rust Weaponization For Red Team Engagements
* 4-ZERO-3 : 403/401 Bypass Methods + Bash Automation
* DetectionLabELK : A Fork From DetectionLab With ELK Stack Instead Of Splunk
* Cracken : A Fast Password Wordlist Generator, Smartlist Creation And Password Hybrid-Mask Analysis To
* FakeDataGen : Full Valid Fake Data Generator
* ELFXtract : An Automated Analysis Tool Used For Enumerating ELF Binaries
* LOLBins : PyQT5 App For LOLBAS And GTFOBins
* Redherd Framework : A Collaborative And Serverless Framework For Orchestrating A Geographically Distr

GBHackers Analysis

* Critical Flaw With Zoho Desktop Central Let Attackers to Bypass Authentication
* Chinese Hackers Exploiting Log4Shell Vulnerability & Attack Internet-Facing Systems
* Bugs With URL Parsing Libraries Could Allow DoS, RCE, Spoofing & More
* 5 Most Fearsome Hacks in 2022
* Elephant Beetle Hacking Group Attack Organizations To Steal Financial Data

Weekly Cyber Security Video and Podcasts

SANS DFIR

* SANS Threat Analysis Rundown
* Inside FOR608: Enterprise-Class Incident Response & Threat Hunting - Course Preview
* Applying DS/ML to Forensics and Incident Response: An Interview with Jess Garcia
* SANS STAR Live Stream

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

* Bypassing Brute-Force Protection with Burpsuite
* Millions of Routers Affected by RCE; Ukraine Under Digital Siege - ThreatWire
* OMG Cable - Android Reverse Shell - Payload & Detections

The PC Security Channel [TPSC]

* Clop: Ransomware vs Police
* Norton is now a Crypto Miner

Eli the Computer Guy

* NETFLIX STOCK TANKS - will the streaming bubble burst
* JOE BIDEN GETTING WORSE - even democrats don't want him
* COVID CANCELS ADELE - Half of Staff Infected
* MICROSOFT BUYS ACTIVISION BLIZZARD and DESTROYS GAMING - time to hike mt kilimanjaro...

Security Now

* Anatomy of a Log4j Exploit - Buggy KCode, WordPress Security
* URL Parsing Vulnerabilities - US CISA on Log4J, WordPress Security Update, What Is a Pluton

Troy Hunt

* Weekly Update 279

Intel Techniques: The Privacy, Security, & OSINT Show

* 247-Weekly Recap
* 246-Android Sanitization

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Backdoor.Win32.Wollf.16 Hardcoded Credential
* Backdoor.Win32.Wollf.16 Authentication Bypass
* Banco Guayaquil 8.0.0 Cross Site Scripting
* Online Project Time Management 1.0 SQL Injection
* Grandstream GXV3175 Unauthenticated Command Execution
* VMware vCenter Server Unauthenticated Log4Shell JNDI Injection Remote Code Execution
* Ransomware Builder Babuk Insecure Permissions
* Backdoor.Win32.Wisell Remote Command Execution
* CollectorStealerBuilder Panel 2.0.0 Man-In-The-Middle
* CollectorStealerBuilder Panel 2.0.0 Insecure Credential Storage
* VulturiBuilder Insecure Permissions
* WordPress Email Template Designer - WP HTML Mail 3.0.9 Cross Site Scripting
* Archeevo 5.0 Local File Inclusion
* Landa Driving School Management System 2.0.1 Arbitrary File Upload
* Online Resort Management System 1.0 SQL Injection
* Simple Chatbot Application 1.0 Shell Upload
* Simple Chatbot Application 1.0 SQL Injection
* Nyron 1.0 SQL Injection
* OpenBMCS 2.4 Secret Disclosure
* OpenBMCS 2.4 Remote File Inclusion / Server-Side Request Forgery
* AgentTesla Builder Web Panel SQL Injection
* AgentTesla Builder Web Panel Cross Site Scripting
* OpenBMCS 2.4 Remote Privilege Escalation
* OpenBMCS 2.4 SQL Injection
* Chaos Ransomware Builder 4 Insecure Permissions

CXSecurity

* VMware vCenter Server Unauthenticated Log4Shell JNDI Injection Remote Code Execution
* Grandstream GXV3175 Unauthenticated Command Execution
* Worktime 10.20 Build 4967 DLL Hijacking
* SonicWall SMA 100 Series Authenticated Command Injection
* Log4Shell HTTP Header Injection
* Automox Agent 32 Local Privilege Escalation
* Siemens S7 Layer 2 Denial of Service (DoS)

Proof of Concept (PoC) & Exploits

Exploit Database

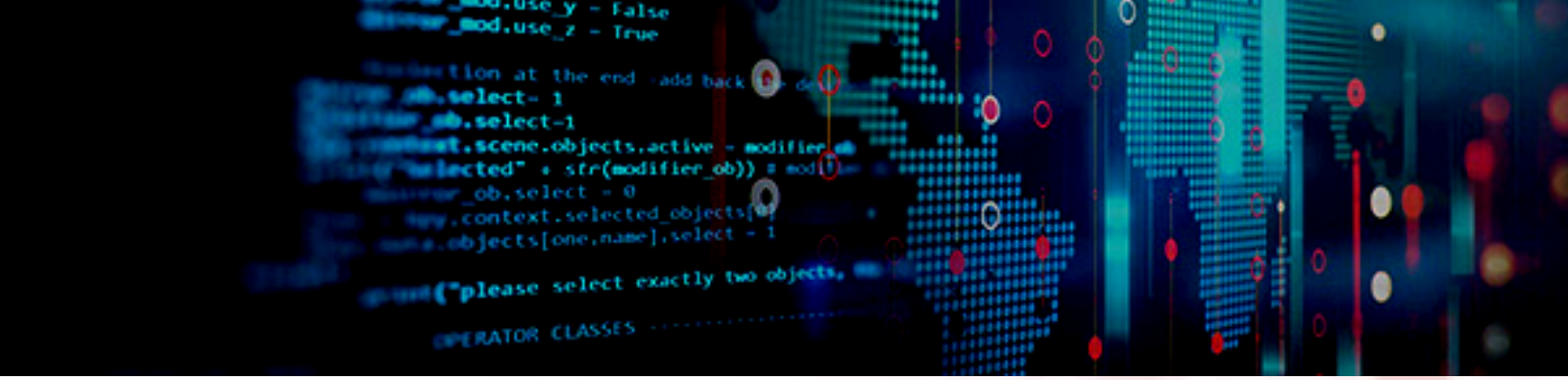
* [webapps] Affiliate Pro 1.7 - 'Multiple' Cross Site Scripting (XSS)
* [webapps] Rocket LMS 1.1 - Persistent Cross Site Scripting (XSS)
* [webapps] uDoctorAppointment v2.1.1 - 'Multiple' Cross Site Scripting (XSS)
* [webapps] Creston Web Interface 1.0.0.2159 - Credential Disclosure
* [webapps] Nyron 1.0 - SQLi (Unauthenticated)
* [webapps] Simple Chatbot Application 1.0 - 'message' Blind SQLi
* [webapps] Simple Chatbot Application 1.0 - Remote Code Execution (RCE)
* [webapps] OpenBMCS 2.4 - Information Disclosure
* [webapps] OpenBMCS 2.4 - Server Side Request Forgery (SSRF) (Unauthenticated)
* [webapps] OpenBMCS 2.4 - Create Admin / Remote Privilege Escalation
* [webapps] OpenBMCS 2.4 - SQLi (Authenticated)
* [webapps] OpenBMCS 2.4 - Cross Site Request Forgery (CSRF)
* [webapps] Online Resort Management System 1.0 - SQLi (Authenticated)
* [remote] Archeevo 5.0 - Local File Inclusion
* [local] WorkTime 10.20 Build 4967 - Unquoted Service Path
* [webapps] WordPress Core 5.8.2 - 'WP_Query' SQL Injection
* [webapps] Online Diagnostic Lab Management System 1.0 - SQL Injection (Unauthenticated)
* [webapps] Online Diagnostic Lab Management System 1.0 - Stored Cross Site Scripting (XSS)
* [webapps] Online Diagnostic Lab Management System 1.0 - Account Takeover (Unauthenticated)
* [webapps] SalonERP 3.0.1 - 'sql' SQL Injection (Authenticated)
* [webapps] Hospitals Patient Records Management System 1.0 - 'doctors' Stored Cross Site Scripting (XS
* [webapps] Hospitals Patient Records Management System 1.0 - 'room_list' Stored Cross Site Scripting (
* [webapps] Hospitals Patient Records Management System 1.0 - 'room_types' Stored Cross Site Scripting
* [webapps] WordPress Plugin Frontend Uploader 1.3.2 - Stored Cross Site Scripting (XSS) (Unauthenticat
* [local] Microsoft Windows Defender - Detections Bypass

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*

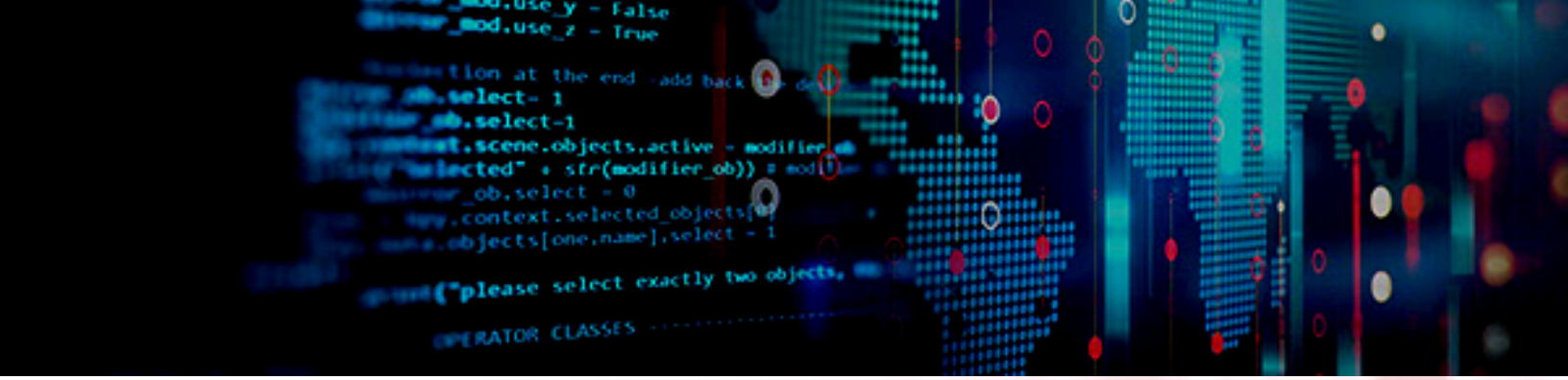
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://concejocalimaeldarien.gov.co/CR4P5.html
http://concejocalimaeldarien.gov.co/CR4P5.html notified by Mr.CR4P5
https://pandeglangkab.go.id/ma.txt
https://pandeglangkab.go.id/ma.txt notified by Moroccan Revolution
http://sales.sp.gov.br/o.htm
http://sales.sp.gov.br/o.htm notified by chinafans
https://fafpa.gov.bf/pwnd.html
https://fafpa.gov.bf/pwnd.html notified by 0x1998
https://baganuur.cd.gov.mn/Ok.html
https://baganuur.cd.gov.mn/Ok.html notified by AnonCoders United Kingdom of Great Britain and Northern Ireland
https://bhzh.cd.gov.mn/Ok.html
https://bhzh.cd.gov.mn/Ok.html notified by AnonCoders United Kingdom of Great Britain and Northern Ireland
http://zamiinuud.cd.gov.mn/Ok.html
http://zamiinuud.cd.gov.mn/Ok.html notified by AnonCoders United Kingdom of Great Britain and Northern Ireland
http://chon1.go.th/mei.php
http://chon1.go.th/mei.php notified by ./G1L4N6_ST86
https://loei1.go.th/mei.php
https://loei1.go.th/mei.php notified by ./G1L4N6_ST86
http://kazimkarabekirtarim.gov.tr/o.htm
http://kazimkarabekirtarim.gov.tr/o.htm notified by chinafans
https://donyailocal.go.th/kz.html
https://donyailocal.go.th/kz.html notified by Mr.Kro0oz.305
https://bankhwao.go.th/kz.html
https://bankhwao.go.th/kz.html notified by Mr.Kro0oz.305
https://bunlung.go.th/kz.html
https://bunlung.go.th/kz.html notified by Mr.Kro0oz.305
https://www.aeb.gov.lk/1.php
https://www.aeb.gov.lk/1.php notified by -1
http://www.lopburi1.go.th/mei.php
http://www.lopburi1.go.th/mei.php notified by I WILL VERY BIG SURPRISE QIYAMAT SOON ;)
https://sukhothai1.go.th/mei.php
https://sukhothai1.go.th/mei.php notified by AnonSec Team
http://laotechmart.most.gov.la/!.php
http://laotechmart.most.gov.la/!.php notified by eRRoR 7rB



Dark Web News

Darknet Live

Ex-Pro Skater Heads to Prison for Supplying Vendors with Meth

A former professional skateboarder in California was sentenced to 97 months in prison for selling methamphetamine and laundering Bitcoin for undercover federal assets. United States District Judge David O. Carter sentenced Evan Jaime Hernandez, 35, of Long Beach, California, to 97 months in federal prison. In July 2021, Hernandez pleaded guilty to one count of distribution of methamphetamine and one count of laundering of monetary instruments. Hernandez and Dwayne Michael Carter Jr. aka Lil Wayne Investigators identified Hernandez as the supplier of at least two darkweb vendors who sold the meth on "one of the world's largest darknet marketplaces.” Court documents identified two of the vendors as William Glarner IV (aka "Billy”) and Brian Vancleave. Court documents that I have seen do not disclose the usernames of the accounts controlled by the co-conspirators. Glarner is currently serving a 10-year prison sentence after being convicted of one count of possession with intent to distribute methamphetamine in June 2019. What we do know about Glarner is that he had conducted at least 1,500 transactions through his vendor accounts. He also had or used three different "monickers” on different marketplaces. It is not clear if the three accounts were different identities altogether or simply different variants of the same username on three markets, etc. Methamphetamine seized during the investigation into the Glarner duo The Glarner investigation netted Glarner IV as well as his father, Glarner III. A federal grand jury convicted Glarner III of one count of possession to distribute methamphetamine and two counts of attempted distribution of methamphetamine. A federal judge sentenced him to 15 years in prison in September 2019. In the comments section for the article on the Glarner III sentencing, someone left a comment asking if the Glarner duo used the username "Billiedakidd.” I was not able to find a vendor under that name. There is a "Billy” with an account on Black Market Reloaded but no other activity. A "Billythekid” account may have existed in 2019 but I am unable to find a matching Recon profile. There is not much information available about Vancleave. On March 9, 2018, Hernandez agreed to sell approximately two pounds of methamphetamine to a confidential source working for Homeland Security.

Feds searched an iCloud backup assosciated with Glarner IV and identified a meth supplier. Investigations (HSI). Hernandez believed the HSI source was a money launderer. On March 21, 2018, Hernandez sold approximately 894.9 grams of methamphetamine to the CS for $5,000. Hernandez was also responsible for laundering Bitcoin for the darkweb operations conducted by Glarner and Vancleave. Hernandez utilized the services of the HSI source to exchange Bitcoin, which was proceeds from illicit activity, into cash. Hernandez conducted four Bitcoin-cash transactions with this CS, all of which affected interstate commerce. For example, on September 5, 2018, Hernandez exchanged approximately 7.95 Bitcoin for $50,000 in U.S. currency. During this transaction, Hernandez discussed the status of darkweb markets. The source of the exchanged Bitcoin was drug trafficking. In total, Hernandez conducted four Bitcoin-cash exchanges that totaled approximately $171,300. One of the illicit transactions was listed in court documents as: 599863397de44ea98d947e837e7919b50e833e5a45b982cb3a9bf6ed93b57971. (archive: 2JJ1K) "[Hernandez] was involved in a highly sophisticated drug-trafficking operation, where he personally took on various roles to

ensure its success: obtaining multiple types of narcotics, selling them directly to customers, and laundering money on the backend in a sophisticated manner,” prosecutors wrote in a sentencing memorandum. Hernandez has been ordered to forfeit a 2010 Mercedes-Benz, approximately $35,000 in cash, and various watches, necklaces, rings, and other jewelry. (via darknetlive.com at https://darknetlive.com/post/ex-pro-skateboarder-sentenced-to-prison-for-selling-meth-to-vendors/)

EU's Proposed DNS Resolver Blocks Illegal URLs (For Free!)

The EU wants to build its own DNS resolver called "DNS4EU.” The European Commission published a call for proposals that included details about the government-run DNS resolver on January 12, 2022. The call for proposals contained more than enough information to predict the direction of this project. But their goals are straightforward enough. The deployment of DNS4EU aims to address such consolidation of DNS resolution in the hands of a few companies, which renders the resolution process itself vulnerable in case of significant events affecting one major provider. They actually published the plans for the DNS resolver in December 2020 as a part of the "EU's Cybersecurity Strategy for the Digital Decade.” The 2020 document contains much of the same language: "[P]eople and organizations in the EU increasingly rely on a few public DNS resolvers operated by non-EU entities. Such consolidation of DNS resolution in the hands of a few companies renders the resolution process itself vulnerable in case of significant events affecting one major provider and makes it more difficult for EU authorities to address possible malicious cyberattacks and major geopolitical and technical incidents.” The call for proposals listed the project requirements. Most of the requirements are standard. The concept of feature parity comes to mind. At the site, the list of requirements includes a short description of the requirement. Since the majority of the features are not interesting to me, I will simply include a concise summary instead of the entire requirement's description. High adoption rate through targetting the entire EU as a customer base; High reliability and uptime, as well as low latency of DNS resolution; Broad accessibility (low barrier of entry); "Widely discoverable” by users and services; Opt-in paid premium services for enhanced security; Opt-in and fully transparent parental control filtering services; To include the "latest DNS security and privacy-enhancing technologies”; GDPR compliant; A federated infrastructure spread throughout the EU "State-of-the-art protection against cybersecurity threats by blocking malware, phishing and other threats”; To include DoT and DoH and be fully IPv6 compliant; No monetization of personal data And you knew it was coming: "Lawful filtering: Filtering of URLs leading to illegal content based on legal requirements applicable in the EU or national jurisdictions (e.g. based on court orders), in full compliance with EU rules.” This seems like a pointless exercise on its own. Perhaps they will introduce legislation that requires people to obtain a license to change their DNS resolver? How silly. TorrentFreak pointed to an oddity. "[I]t will offer better security options for "customers” who pay, which seems strange for a government-backed service.” I can't envision a world where people voluntarily switch to an (openly) state-controlled DNS resolver. The existence of premium options makes me think that individuals might not actually be the targeted userbase here. Would a large corporation pay the government to do the DNS thing? Probably. Very boring: The EU's Cybersecurity Strategy for the Digital Decade (pdf) (via darknetlive.com at https://darknetlive.com/post/the-eu-proposed-dns-resolver-will-filter-illegal-urls/)

Talking to Cops: Austrian Man Admits Darkweb Drug Orders

Police in Upper Austria arrested a man suspected of importing large quantities of drugs purchased through the dark web. The Upper Austria State Police Directorate disclosed in a press release that police officers in Wels received information about the defendant from an undisclosed law enforcement agency. Austrian law enforcement launched an investigation into the 29-year-old man using the received data. The undisclosed law enforcement agency informed police in Wels that the 29-year-old had ordered a total of 1500 grams of amphetamine from a vendor on the darkweb. Police in Wels executed a search warrant at the suspect's residence on January 15, 2022. The search resulted in the seizure of an undisclosed quantity of amphetamine and a handgun. Police officers arrested the 29-year-old at the residence. During an "interview” with police, the defendant allegedly admitted to investigators that he had imported a total of at least four kilograms of amphetamine, approximately 180 grams of cocaine, 48 ecstasy pills, as well as tilidine and Xanax. Authorities transferred The defendant to the Wels Prison pending trial. archive.is archive.org

archiveiya74codqgiixo33q62qlrqtkgmcitqx5u2oeqnmn5bpcbiyd.onion DNL: "Interview,” lol.

Innocence Project seems to be focused on something other than innocence but at least they link to the Nat. Reg. of exonerations (via darknetlive.com at https://darknetlive.com/post/austrian-man-arrested-for-purchasing-drugs-on-the-dark-web/)

Monopoly Market and Cartel Market Are Gone.

Monopoly Market vanished in late December 2021 at roughly the same time the administrator of Cartel Market disappeared. Note about DNS leaks for beginners: Nearly every link in this article is a Dread link. Without a configuration (on your COMPUTER MACHINE) intended to prevent DNS leaks, clicking one (USING YOUR MOUSE CURSOR TO "TOUCH” ONE) in a normal browser (A BROWSER THAT IS NOT THE TOR BROWSER) could result in the request being sent to your DNS resolver (NOT GOOD). If you have configured your DNSPort, TransPort, resolv.conf, etc., then why are you still reading this? You are not a beginner. To start us off, the best Dread comment about the entire ordeal is the following one. HE AINT EXIT HE JUST CLOSE DOWN WITHOUT TELLIN NOBODY - /u/donkeysquadreborn Monopoly Market Users of Monopoly Market last accessed the market in late December 2021. Based on an examination of comments posted on Dread by the /u/MonopolyOfficial account as well as comments posted in the /d/monopoly subdread, it appears as if the market went offline at some point during December 28. The administrator fairly actively responded to comments from genuine users asking questions about the downtime as well as one-day-old accounts attempting to take advantage of the situation by sharing their "insider information.”

Not the official Monopoly Market logo. On December 29, /u/MonopolyOfficial responded to a user's request for an ETA with the following: I cannot give an ETA, and I am not going to sit in public going into details as to why we are down right now. It's not appropriate, some things are not to be discussed in public. The fact I am here doing my best to ease the retards should be enough to tell you that we are not trying to exit scam. What the fuck would be the point? If I was exiting, I would have taken your money and been offline right now. Why would I be here, with an offline market trying to convince people otherwise… We are experiencing downtime during the holiday period, our hands are tied right now unless of course something bad has happened and I am just unaware of it right now which I do not believe to be the case. I am right now looking at the escrow funds, I can assure you if you guys had something to worry about I would too be worrying as the balance would be 0. The error code displayed when visiting Monopoly is "X'F0' Onion Service Descriptor Can Not be Found." According to one Dread user, the market threw a 500 error before finally going offline (with the SOCKS5 error above) on December 28. There is very little information on any public platform about what happened. And as of this article, all that is publicly available seems to be speculation. ShakyBeats, a well-known Dread moderator, locked down Monopoly's subdread in an attempt to limit the brand new accounts from spreading "FUD and crazy theories.” In the post announcing the lockdown, ShakyBeats wrote, "scam? busted? Overdosed? We may never know what happened to /u/MonopolyOfficial.”

lol The fallout on Monopoly's subdread unfolded the way you might expect, given Monopoly's history on Dread. On ShakyBeats' lockdown post, one user wrote, "Any idea why german markets always screw up at the end? It's strange…” In a different thread, the user wrote, "he was from Germany, everybody knows that.” In another, "German markets always screw up at the end. Wonder why?” The same user posted a thread about the estimated value of the escrow wallet for the "german dark market Monopoly.” These people are clearly very familiar with the market.

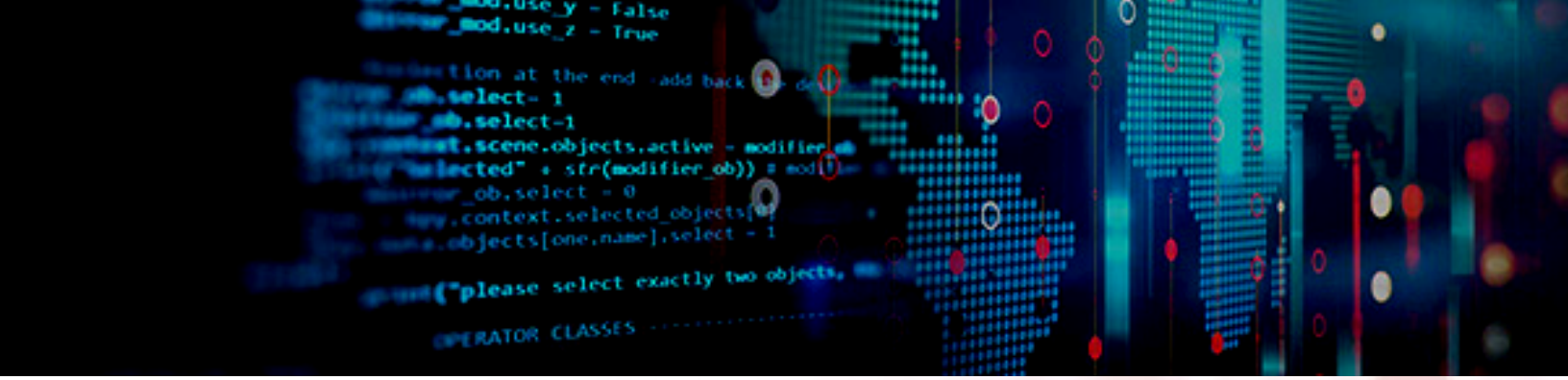
Obviously these are totally organic posts from users who happened to sign up on December 28 In the thread titled "Busted,” a different commenter asked if the "admin who is clearly of British origin” had exited or been arrested. One user had this to add: "well I heard about the drives on his server got seized or something like that…” I have linked a couple of the threads in the paragraph above if the quotes failed to demonstrate the quality of the information available about the purported exit scam. There are essentially three camps on Dread that I have seen: Monopoly exit scammed; Monopoly rage quit after [insert one of many reasons]; Law enforcement action resulted in the market's seizure. "Monopoly went to jail,” a user said in one thread while explaining in another that the value of the stolen escrow wallet was "not enough for the ten years jail he will get when he is convicted.” He may or may not be in jail; I could provide only

speculations of my own. But I think the part of the comment about the relatively small amount of cryptocurrency in escrow had merit. Monopoly had, at the time of the disappearance, less than 200 vendors. Not all of the vendors had finalize early (FE) privileges. One vendor on Dread stated that if Monopoly had waited another day to vanish (in the case of an exit scam), he would have collected his commission from vendors with FE privileges. There seems to be some dispute about the length of the cycle on Monopoly. According to vendors on Dread, the cycle is either 23 days or 30 days(???). The error became sentient and deleted the market. Among the Dread comments with useful information was one by the user /u/ lolwhatsecurity that explained how theft from Monopoly, being a "walletless” market, would work. A walletless market, as demonstrated by Monopoly, is not unable to disappear with user funds. MonopolyOfficial explained this as well back in October 2021. Skip if you know how Monopoly worked. Not all vendors had FE privileges. It was walletless sort of how WHM was walletless. You pay the amount required when placing an order but it could be in escrow for up to 30 days. The difference was if there was a refund or the order wasn't accepted the coins would go back into the wallet you specified when placing the order and not a wallet controlled by the market. An exit scam would be possible. However, the admin always spoke as if a direct deal was the goal for all vendors and it wasn't a big market. It had around 180 vendors. On top of that vendors had a fairly low number of orders that could be open at any one time. A new, non-FE vendor could have 50 (I think) orders open. Lastly, they'd closed applications for new vendors a couple of months ago. It wasn't an ideal setup for an exit scam. Paris, a Dread administrator, wrote "right now we got a couple of theories all of them are not the best outcomes.” Cartel Market The administrator of Cartel Market strangely vanished alongside Monopoly. The last update from the market is from the Cartel Market staffer Ryuu in a post titled "The Situation” which was created on December 29. Below the quote are some hard references to the days mentioned by Ryuu. So everyone knows that we got hit by DDOS on past Friday, /u/6ix said that only on Monday things will probably be back to normal, and that was the last time we spoke, he is offline for 6 days now. I don't have access to the backend and I don't know if something happened with him. But I really believe that some serious shit is going on with him, I hope it's not the case. I talked with dread staff and we are going to wait a couple more days because of the holidays to see if something change. Cartel Market. In an earlier post, Ryuu wrote that the market was undergoing a heavy DDoS attack on December 23, 2021. In the message above, Ryuu is referring to Friday, December 24, 2021. I think that discrepancy is inconsequential. Access to the market was limited starting December 23 or December 24. Ryuu said that the market would be back online on Monday, December 27, 2021. The administrator of Cartel Market had been offline since December 23 (possibly early December 24) when Ryuu posted the status update. Between Ryuu's first announcement concerning site issues on December 23 and December 27, users had limited access to the market and reported seeing a 502 error (which is not really useful information outside of serving as a marker for the market's different stages of "gone”). On December 27, users reported seeing the SOCKS5 error "X'F0' Onion Service Descriptor Can Not be Found." On a post about Cartel Market returning, Paris wrote, "sorry to break it to ya but most signs point to no right now. Same with monopoly.” This means your markets are gone. Ryuu wrote that they thought "something serious [had] happened with [the administrator of Cartel Market].” This sentiment has been repeated to this author by others, including well-known actors in this market sector. It is hard to imagine such a new market having an escrow balance worth stealing in an exit scam. But that is speculation. ShakyBeats, in their comment about locking down the Cartel subdread, wrote, "This is very unlike their admin, but right now it is looking either he exit scammed, or something more serious happened. I'd rather be cautious until we know for sure. /u/6ix if you see this please get in contact with one of the Dread staff so we can sort this out and give you back your sub.” Some odd things are happening right now in this sector, including abnormal behavior from other onion service administrators. However, those oddities are hardly necessary to view the simultaneous disappearances of Monopoly and Cartel as a strange continuation of markets retiring or exit scamming around the same general quarter. In three months, White House Market announced their retirement, Cannazon announced their retirement, ToRReZ announced their retirement, Monopoly vanished, and Cartel vanished. These markets are gone. "I

have no problem giving entitled shits a dose of their own medicine” Also, Monopoly's canary expired before the market vanished. I seem to recall it being nine days old at one point. Did this ever get updated? (via darknetlive.com at https://darknetlive.com/post/monopoly-market-and-cartel-market-are-gone/)

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

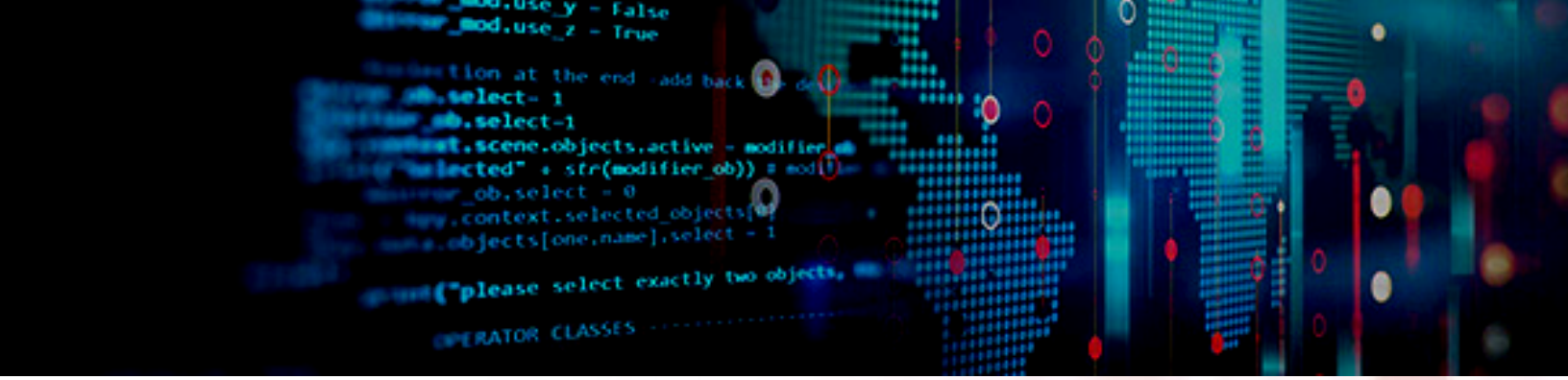
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

* 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
* Discord CDN Abuse Found to Deliver 27 Unique Malware Types
* The Threat Landscape is Dynamic and Ever-Changing - Can You Keep Up?

FireEye

* Metasploit Weekly Wrap-Up
* Is the Internet of Things the Next Ransomware Target?
* [Security Nation] Mike Hanley of GitHub on the Log4j Vulnerability
* Open-Source Security: Getting to the Root of the Problem
* Active Exploitation of VMware Horizon Servers
* 2022 Planning: Metrics That Matter and Curtailing the Cobra Effect
* Metasploit Weekly Wrap-Up
* 7Rapid Questions: Stephen Donnelly
* Being Naughty to See Who Was Nice: Machine Learning Attacks on Santa's List
* Evaluating MDR Vendors: A Pocket Buyer's Guide



Advisories

US-Cert Alerts & bulletins

* McAfee Releases Security Update for McAfee Agent for Windows
* CISA Adds Four Known Exploited Vulnerabilities to Catalog
* F5 Releases January 2022 Quarterly Security Notification
* Drupal Releases Security Updates
* Google Releases Security Updates for Chrome
* Cisco Releases Security Updates for Multiple Products
* CISA Releases Final Version of Guidance: IPv6 Considerations for TIC 3.0
* Zoho Releases Security Advisory for ManageEngine Desktop Central and Desktop Central MSP
* AA22-011A: Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infras
* AA21-356A: Mitigating Log4Shell and Other Log4j-Related Vulnerabilities
* Vulnerability Summary for the Week of January 10, 2022
* Vulnerability Summary for the Week of January 3, 2022

Zero Day Initiative Advisories

ZDI-CAN-16340: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-01-21, 3 days ago. The vendor is given until 2022-05-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-16345: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-01-21, 3 days ago. The vendor is given until 2022-05-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-16344: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-01-21, 3 days ago. The vendor is given until 2022-05-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-16341: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-01-21, 3 days ago. The vendor is given until 2022-05-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-16339: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-01-21, 3 days ago. The vendor is

given until 2022-05-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16343: Bentley

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: 2022-01-21, 3 days ago. The vendor is given until 2022-05-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16310: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-01-21, 3 days ago. The vendor is given until 2022-05-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16342: Bentley

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: 2022-01-21, 3 days ago. The vendor is given until 2022-05-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16306: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-01-21, 3 days ago. The vendor is given until 2022-05-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16280: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-01-21, 3 days ago. The vendor is given until 2022-05-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16308: Bentley

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: 2022-01-21, 3 days ago. The vendor is given until 2022-05-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16282: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-01-21, 3 days ago. The vendor is given until 2022-05-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16168: Microsoft

A CVSS score 9.0 (AV:A/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Oliver Lyak (@ly4k_) of Institut For Cyber Risk' was reported to the affected vendor on: 2022-01-21, 3 days ago. The vendor is given until 2022-05-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16307: Bentley

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: 2022-01-21, 3 days ago. The vendor is given until 2022-05-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-16193: MariaDB

A CVSS score 7.0 (AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous'

was reported to the affected vendor on: 2022-01-20, 4 days ago. The vendor is given until 2022-05-20 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-16191: MariaDB

A CVSS score 7.0 (AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-01-20, 4 days ago. The vendor is given until 2022-05-20 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-16190: MariaDB

A CVSS score 7.0 (AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-01-20, 4 days ago. The vendor is given until 2022-05-20 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-16209: MariaDB

A CVSS score 7.0 (AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-01-20, 4 days ago. The vendor is given until 2022-05-20 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-16208: MariaDB

A CVSS score 7.0 (AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-01-20, 4 days ago. The vendor is given until 2022-05-20 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-16192: MariaDB

A CVSS score 7.0 (AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-01-20, 4 days ago. The vendor is given until 2022-05-20 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-16207: MariaDB

A CVSS score 7.0 (AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-01-20, 4 days ago. The vendor is given until 2022-05-20 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-16174: 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: 2022-01-19, 5 days ago. The vendor is given until 2022-05-19 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-16186: Foxit

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-01-19, 5 days ago. The vendor is given until 2022-05-19 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-16036: ASUS

A CVSS score 6.3 (AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-01-17, 7 days ago. The vendor is given until 2022-05-17 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

Ubuntu Security Notice USN-5246-1

Ubuntu Security Notice 5246-1 - Multiple security issues were discovered in Thunderbird. If a user were tricked into opening a specially crafted website in a browsing context, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information, conduct spoofing attacks, bypass security restrictions, or execute arbitrary code.

Red Hat Security Advisory 2022-0227-04

Red Hat Security Advisory 2022-0227-04 - Openshift Logging Bug Fix Release. Issues addressed include code execution and denial of service vulnerabilities.

Red Hat Security Advisory 2022-0225-02

Red Hat Security Advisory 2022-0225-02 - Openshift Logging Bug Fix Release. Issues addressed include a code execution vulnerability.

Red Hat Security Advisory 2022-0226-04

Red Hat Security Advisory 2022-0226-04 - OpenShift Logging Bug Fix Release. Issues addressed include code execution and denial of service vulnerabilities.

Red Hat Security Advisory 2022-0223-02

Red Hat Security Advisory 2022-0223-02 - A minor version update is now available for Red Hat Camel K that includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include code execution and denial of service vulnerabilities.

Red Hat Security Advisory 2022-0222-02

Red Hat Security Advisory 2022-0222-02 - This update of Red Hat Integration - Camel Extensions for Quarkus serves as a replacement for 2.2 GA. Issues addressed include code execution and denial of service vulnerabilities.

Red Hat Security Advisory 2022-0219-03

Red Hat Security Advisory 2022-0219-03 - Red Hat AMQ Streams, based on the Apache Kafka project, offers a distributed backbone that allows microservices and other applications to share data with extremely high throughput and extremely low latency. This release of Red Hat AMQ Streams 1.6.6 serves as a replacement for Red Hat AMQ Streams 1.6.5, and includes security and bug fixes, and enhancements. For further information, refer to the release notes linked to in the References section. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-0205-02

Red Hat Security Advisory 2022-0205-02 - Red Hat Data Grid is an in-memory, distributed, NoSQL datastore solution. It increases application response times and allows for dramatically improving performance while providing availability, reliability, and elastic scale. Data Grid 8.2.3 replaces Data Grid 8.2.2 and includes bug fixes and enhancements. Issues addressed include code execution and denial of service vulnerabilities.

Kernel Live Patch Security Notice LSN-0084-1

William Liu and Jamie Hill-Daniel discovered that the file system context functionality in the Linux kernel contained an integer underflow vulnerability, leading to an out-of-bounds write. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code.

Red Hat Security Advisory 2022-0083-03

Red Hat Security Advisory 2022-0083-03 - This release of Red Hat build of Eclipse Vert.x 4.1.8 GA includes security updates. For more information, see the release notes listed in the References section. Issues addressed include code execution and denial of service vulnerabilities.

Red Hat Security Advisory 2022-0216-06

Red Hat Security Advisory 2022-0216-06 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This asynchronous patch is a security update for Red Hat JBoss Enterprise Application Platform 7.4. Issues addressed include code execution and denial of service vulnerabilities.

Ubuntu Security Notice USN-5243-1

Ubuntu Security Notice 5243-1 - David Bouman discovered that AIDE incorrectly handled base64 operations. A local attacker could use this issue to cause AIDE to crash, resulting in a denial of service, or possibly execute arbitrary code.

Ubuntu Security Notice USN-5242-1

Ubuntu Security Notice 5242-1 - It was discovered that Open vSwitch incorrectly handled certain fragmented packets. A remote attacker could possibly use this issue to cause Open vSwitch to consume resources, leading to a denial of service.

Ubuntu Security Notice USN-5021-2

Ubuntu Security Notice 5021-2 - USN-5021-1 fixed vulnerabilities in curl. This update provides the corresponding updates for Ubuntu 16.04 ESM. Harry Sintonen and Tomas Hoger discovered that curl incorrectly handled TELNET connections when the -t option was used on the command line. Uninitialized data possibly containing sensitive information could be sent to the remote server, contrary to expectations.

Red Hat Security Advisory 2022-0203-03

Red Hat Security Advisory 2022-0203-03 - The releases of Red Hat Fuse 7.8.2, 7.9.1 and 7.10.1 serve as a patch to Red Hat Fuse on Karaf and Red Hat Fuse on Spring Boot and includes security fixes, which are documented in the Release Notes document linked to in the References. Issues addressed include code execution and denial of service vulnerabilities.

Red Hat Security Advisory 2022-0202-04

Red Hat Security Advisory 2022-0202-04 - The Migration Toolkit for Containers enables you to migrate Kubernetes resources, persistent volume data, and internal container images between OpenShift Container Platform clusters, using the MTC web console or the Kubernetes API.

Red Hat Security Advisory 2022-0191-03

Red Hat Security Advisory 2022-0191-03 - OpenShift Virtualization is Red Hat's virtualization solution designed for Red Hat OpenShift Container Platform. This advisory contains OpenShift Virtualization 4.9.2 images.

Red Hat Security Advisory 2022-0199-02

Red Hat Security Advisory 2022-0199-02 - Libreswan is an implementation of IPsec and IKE for Linux. IPsec is the Internet Protocol Security and uses strong cryptography to provide both authentication and encryption services. These services allow you to build secure tunnels through untrusted networks such as virtual private network.

Ubuntu Security Notice USN-5241-1

Ubuntu Security Notice 5241-1 - It was discovered that QtSvg incorrectly handled certain malformed SVG images. If a user or automated system were tricked into opening a specially crafted image file, a remote attacker could use this issue to cause QtSvg to crash, resulting in a denial of service, or possibly execute arbitrary code.

Ubuntu Security Notice USN-5240-1

Ubuntu Security Notice 5240-1 - William Liu and Jamie Hill-Daniel discovered that the file system context functionality in the Linux kernel contained an integer underflow vulnerability, leading to an out-of-bounds write. A local attacker could use this to cause a denial of service or execute arbitrary code.

Red Hat Security Advisory 2022-0190-04

Red Hat Security Advisory 2022-0190-04 - Red Hat Satellite is a system management solution that allows organizations to configure and maintain their systems without the necessity to provide public Internet access to their servers or other client systems. It performs provisioning and configuration management of predefined standard operating environments. Issues addressed include an information leakage vulnerability.

Red Hat Security Advisory 2022-0188-07

Red Hat Security Advisory 2022-0188-07 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include a heap overflow vulnerability.

Red Hat Security Advisory 2022-0114-04

Red Hat Security Advisory 2022-0114-04 - 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 4.7.41.

Red Hat Security Advisory 2022-0186-07

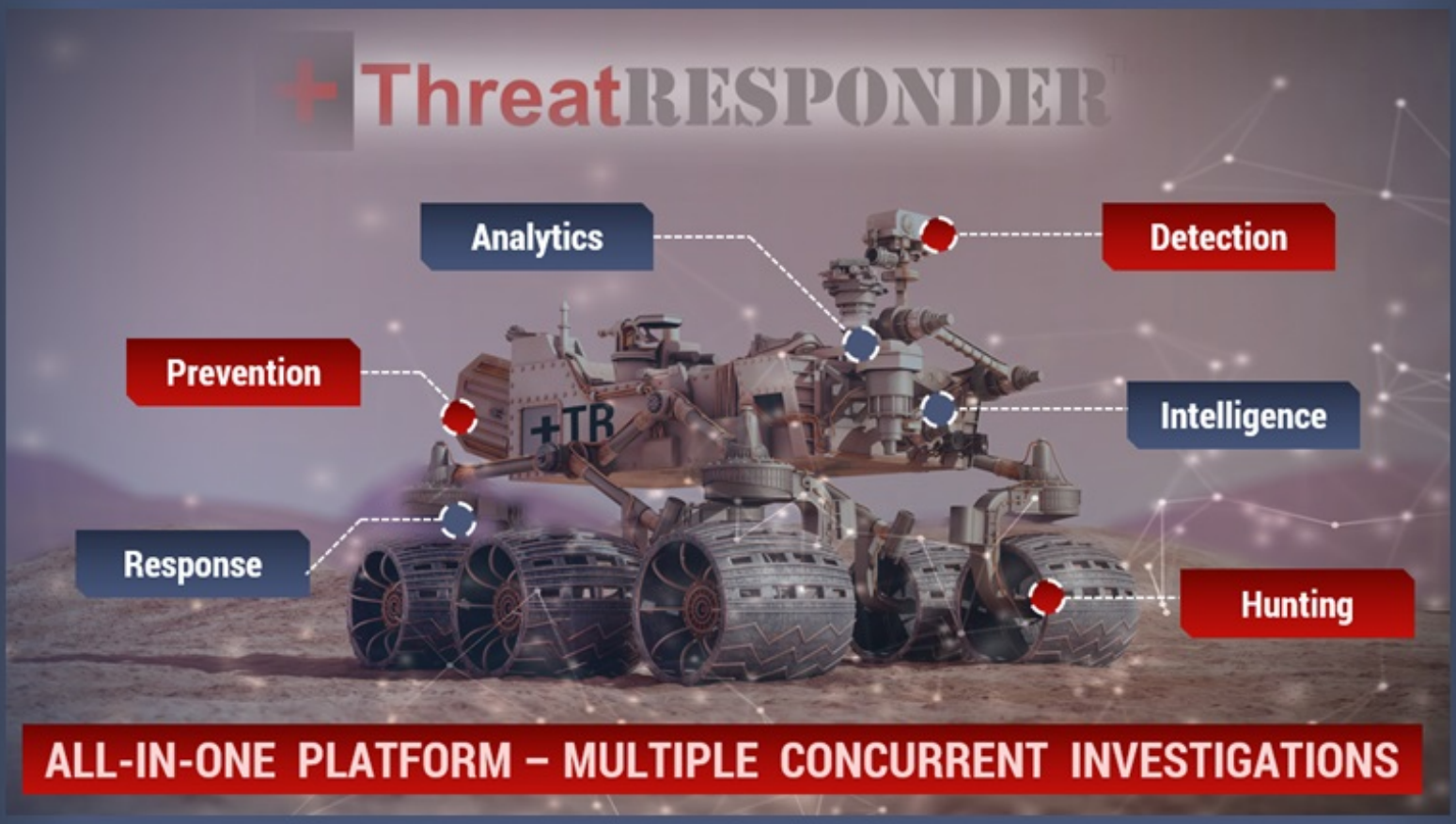
Red Hat Security Advisory 2022-0186-07 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include heap overflow and privilege escalation vulnerabilities.

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



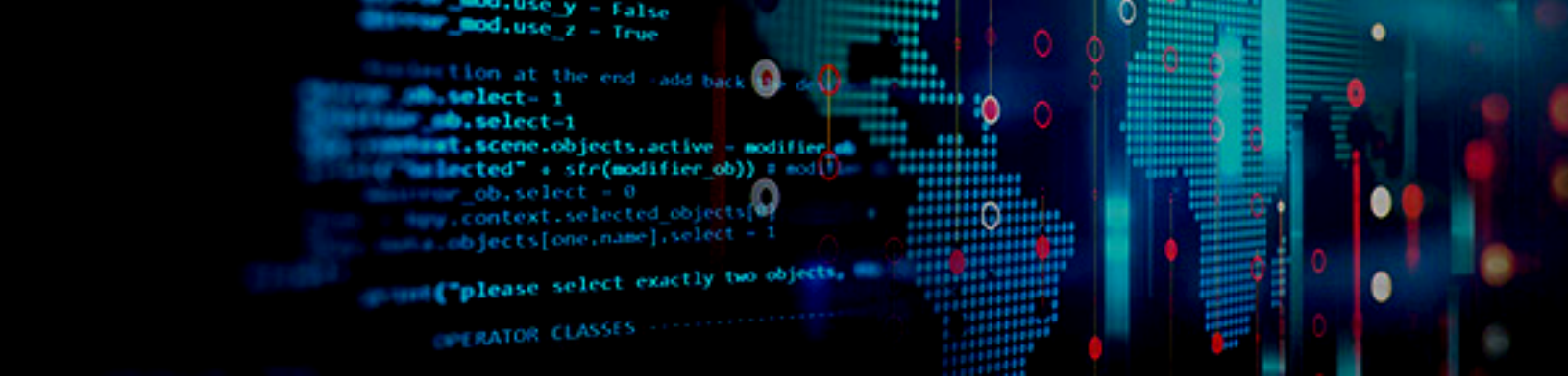
The Solution – ThreatResponder® Platform

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

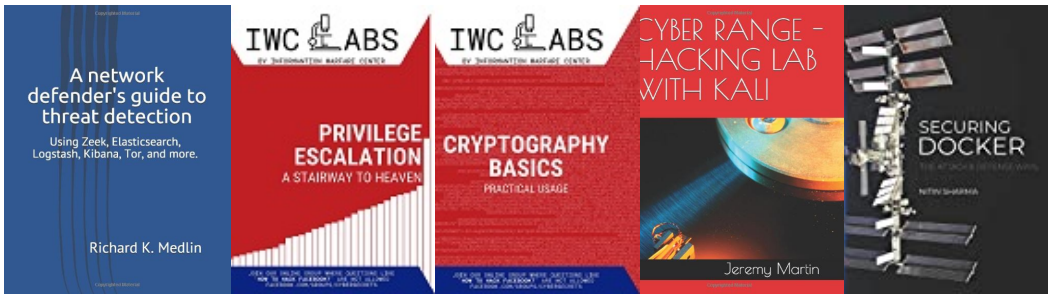


The Cyber Secrets publications on Amazon

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