May-02-22

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

May 2, 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

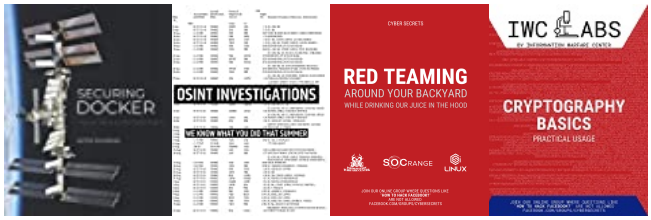
Internet Storm Center Infocon Status

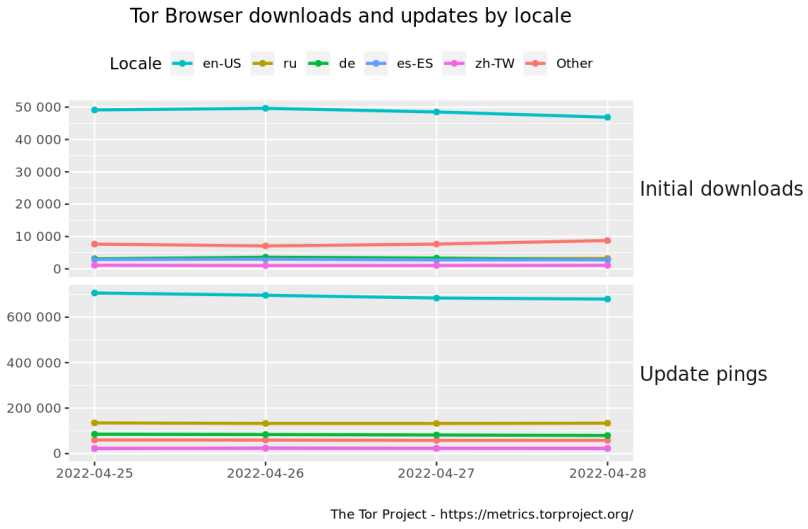
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

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

* Vulnerable Plugins Plague The CMS Website Security Landscape
* Interpol: We Can't Arrest Our Way Out Of Cybercrime
* Powerful DDoS Targets Cryptocurrency Platform
* Private Equity Executive Sought To Undermine NSO Critics
* Malicious Relays And The Health Of The Tor Network
* GitHub Repos Breached Using Stolen OAuth Tokens
* Microsoft Details Rampant Russian Invasion Cyber Warfare
* Microsoft Patches Cross Tenant Bug In Azure PostgreSQL
* Five Eyes Nations Reveal 2021's Fifteen Most Exploited Flaws
* This Two-Inch Diamond Disc Could Hold A Staggering Billion Blu-Ray's Worth Of Data
* Chinese Drone-Maker DJI Suspends Ops In Russia, Ukraine
* Bitcoin Becomes Official Currency In Central African Republic
* Millions Of Java Apps Remain Vulnerable To Log4Shell
* Firms Push For CVE-Like Cloud Bug System
* Nation-State Hackers Target Journalists With Goldbackdoor Malware
* Breach Update Shows 2.6M Individuals Affected By Smile Brands Data Theft
* Microsoft Finds New Elevation Of Privilege Linux Flaw, Nimbuspwn
* Bronze President Spies On Russian Targets As Ukraine Invasion Continues
* Bored Ape Yacht Club Instagram Hacked, NFTs Worth Millions Stolen
* Intuit Sued Over Alleged Crypto Currency Thefts Via Mailchimp Intrusion
* The White House Wants More Powers To Crack Down On Rogue Drones
* The Emotet Botnet Is Back, And It Has Some New Tricks To Spread Malware
* EU Warns Elon Musk Over Twitter Moderation Plans
* FBI Says BlackCat Ransomware Scratched 60+ Orgs
* Hackers Are Exploiting Zero Days More Than Ever

Krebs on Security

* You Can Now Ask Google to Remove Your Phone Number, Email or Address from Search Results
* Fighting Fake EDRs With 'Credit Ratings' for Police
* Leaked Chats Show LAPSUS$ Stole T-Mobile Source Code
* Conti's Ransomware Toll on the Healthcare Industry
* Microsoft Patch Tuesday, April 2022 Edition
* RaidForums Gets Raided, Alleged Admin Arrested
* Double-Your-Crypto Scams Share Crypto Scam Host
* Actions Target Russian Govt. Botnet, Hydra Dark Market
* The Original APT: Advanced Persistent Teenagers
* Fake Emergency Search Warrants Draw Scrutiny from Capitol Hill

Dark Reading

* 2022 Security Priorities: Staffing and Remote Work
* Good News! IAM Is Near-Universal With SaaS
* Critical Vulnerabilities Leave Some Network-Attached Storage Devices Open to Attack
* Cloudflare Flags Largest HTTPS DDoS Attack It's Ever Recorded
* Take a Diversified Approach to Encryption
* Ambient.ai Expands Computer Vision Capabilities for Better Building Security
* Microsoft Patches Pair of Dangerous Vulnerabilities in Azure PostgreSQL
* IT Teams Worry Staff Lack Cloud-Specific Skills
* Capital One Ventures, Snowflake Ventures, Verizon Ventures, and Wipro Ventures Join Securonix $1B+ Gr
* The Ransomware Crisis Deepens, While Data Recovery Stalls
* Bumblebee Malware Buzzes Into Cyberattack Fray
* Microsoft: Russia Using Cyberattacks in Coordination With Military Invasion of Ukraine
* Explainable AI for Fraud Prevention
* A Peek into Visa's AI Tools Against Fraud
* Doppler Takes on Secrets Management
* Chinese APT Bronze President Mounts Spy Campaign on Russian Military
* Synopsys to Acquire WhiteHat Security from NTT
* CISA: Log4Shell Was the Most-Exploited Vulnerability in 2021
* Tenable's Bit Discovery Buy Underscores Demand for Deeper Visibility of IT Assets
* Coca-Cola Investigates Data-Theft Claims After Ransomware Attack

The Hacker News

* Google Releases First Developer Preview of Privacy Sandbox on Android 13
* Here's a New Tool That Scans Open-Source Repositories for Malicious Packages
* Microsoft Documents Over 200 Cyberattacks by Russia Against Ukraine
* Microsoft Azure Vulnerability Exposes PostgreSQL Databases to Other Customers
* Indian Govt Orders Organizations to Report Security Breaches Within 6 Hours to CERT-In
* Experts Detail 3 Hacking Teams Working Under the Umbrella of TA410 Group
* Everything you need to know to create a Vulnerability Assessment Report
* Cybercriminals Using New Malware Loader 'Bumblebee' in the Wild
* Twitter's New Owner Elon Musk Wants DMs to be End-to-End Encrypted like Signal
* New RIG Exploit Kit Campaign Infecting Victims' PCs with RedLine Stealer
* U.S Cybersecurity Agency Lists 2021's Top 15 Most Exploited Software Vulnerabilities
* Cloudflare Thwarts Record DDoS Attack Peaking at 15 Million Requests Per Second
* QNAP Advises to Mitigate Remote Hacking Flaws Until Patches are Available
* [eBook] Your First 90 Days as MSSP: 10 Steps to Success
* Chinese Hackers Targeting Russian Military Personnel with Updated PlugX Malware

Security Week

* 'Right to be Forgotten': Israel Firm Promises to Purge Digital Footprint
* Fleet Raises $20M for Endpoint Visibility Technology
* Sabanci Group Acquires Majority Stake in OT Security Firm Radiflow for $45 Million
* New OpenSSF Project Hunts for Malicious Packages in Open Source Repositories
* Many Internet-Exposed Servers Affected by Exploited Redis Vulnerability
* Synology, QNAP, WD Warn Users About Vulnerabilities Exploited at Hacking Contest
* Google Adds Ways to Keep Personal Info Private in Searches
* Data Security Firm Veza Emerges From Stealth With $110 Million in Funding
* Microsoft Warns of 'Nimbuspwn' Security Flaws Haunting Linux
* 1.2 Million Bad Apps Blocked From Reaching Google Play in 2021
* How Linux Became the New Bullseye for Bad Guys
* Synopsys to Acquire White Hat Security in $330M All-Cash Deal
* Cisco Patches 11 High-Severity Vulnerabilities in Security Products
* Critical Vulnerabilities in Azure PostgreSQL Exposed User Databases
* National Cybersecurity Agencies List Most Exploited Vulnerabilities of 2021
* Cloudflare Customer Targeted in Record HTTPS DDoS Attack
* Overcoming Cybersecurity Recruiting Challenges
* A Chilling Russian Cyber Aim in Ukraine: Digital Dossiers
* IETF Publishes RFC 9116 for 'security.txt' File
* Over 300,000 Internet-Exposed Databases Identified in 2021
* Russia Coordinating Cyberattacks With Military Strikes in Ukraine: Microsoft
* Privacy Enhancing Tech Startup Enveil Bags $25 Million Investment
* Watch: The Four Stages of Zero Trust Maturity
* Risk Intelligence Company Strider Raises $45 Million
* Can Tech Visionary Elon Musk Spur Cybersecurity Innovation at Twitter?
* Internet Outages in French Cities After Cable 'Attacks': Operator

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* 75% of SMBs Would Only Survive Seven Days or less from a Ransomware Attack
* Half of IT Leaders Say their Non-Technical Staff are Unprepared for a Cyber Attack
* [EYE OPENER] The Ransom Payment is Only 15% of The Total Cost of Ransomware Attacks
* Criminal Gang Impersonates Russian Government in Phishing Campaign
* CyberheistNews Vol 12 #17 [EYE OPENER] "Being Annoying" as a Social Engineering Tactic
* How Hackers Get Your Passwords and How To Defend Yourself
* Hacking the Hacker: An Inside Look at the Karakurt Cyber Extortion Group
* Nearly all Data Breaches in Q1 2022 Were the Result of a Cyber Attack
* Cyber Attacks on the Global Supply Chain Have Increased by 51%
* More_eggs Malware Distributed Via Spear Phishing

ISC2.org Blog

* (ISC)² Hellenic Chapter Wins Award for Creating Educational Materials
* CLOUD: A SHAKESPEAREAN DRAMA?
* Quantum Cybersecurity: Addressing the Boogeyman in the Room
* Why Are Ransomware Attacks Increasing and How Can We Prevent Them?
* Celebrating Service and Diversity - Nominate a Colleague Today!

HackRead

* Breast Cancer Charity Exposed Sensitive Images of U.S. Patients
* "Computer malfunction" Caused Death of 27,000 Chickens
* Elon Musk Wants to Make Twitter DMs End-to-End Encrypted
* US and China Exposed Most Databases Among 308,000 Discovered in 2021
* How to detect phishing images in emails
* Explaining Cloud Native Application Security
* Ransomware Attacks: Everything You Need to Know

Koddos

* Breast Cancer Charity Exposed Sensitive Images of U.S. Patients
* "Computer malfunction" Caused Death of 27,000 Chickens
* Elon Musk Wants to Make Twitter DMs End-to-End Encrypted
* US and China Exposed Most Databases Among 308,000 Discovered in 2021
* How to detect phishing images in emails
* Explaining Cloud Native Application Security
* Ransomware Attacks: Everything You Need to Know

Naked Security

* GitHub issues final report on supply-chain source code intrusions
* S3 Ep80: Ransomware news, phishing woes, NAS bugs, and a giant hole in Java [Podcast]
* Ransomware Survey 2022 - like the Curate's Egg, "good in parts"
* Phishing goes KISS: Don't let plain and simple messages catch you out!
* QNAP warns of new bugs in its Network Attached Storage devices
* S3 Ep79: Chrome hole, a bad place for a cybersecurity holiday, and crypto-dodginess [Podcast]
* Critical cryptographic Java security blunder patched - update now!
* Beanstalk cryptocurrency heist: scammer votes himself all the money
* Yet another Chrome zero-day emergency update - patch now!
* S3 Ep78: Darkweb hydra, Ruby, quantum computing, and a robot revolution [Podcast]

Threat Post

* Security Turbulence in the Cloud: Survey Says…
* Cyberespionage APT Now Identified as Three Separate Actors
* Attacker Breach 'Dozens' of GitHub Repos Using Stolen OAuth Tokens
* Cyberattacks Rage in Ukraine, Support Military Operations
* Emotet is Back From 'Spring Break' With New Nasty Tricks
* Millions of Java Apps Remain Vulnerable to Log4Shell
* Firms Push for CVE-Like Cloud Bug System
* Nation-state Hackers Target Journalists with Goldbackdoor Malware
* Lapsus$ Hackers Target T-Mobile
* Zero-Trust For All: A Practical Guide

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

* shinytest2, Rhino R Shiny framework top news at Appsilon conference
* AWS can't help Amazon avoid first loss since 2015
* Why public clouds lead with renewables
* What is a data lake? Massively scalable storage for big data analytics
* Deno 1.21 improves REPL, error handling
* Oracle Java popularity sliding, New Relic reports
* 8 great new JavaScript language features in ES12
* How to work with Azure Functions in C#
* Akamai jumps into DBaaS market with Linode Managed Database
* GraalVM speeds up native image builds

C4ISRNET - Media for the Intelligence Age Military

* Feared Russian cyberattacks against US have yet to materialize
* Army Futures Command learning from Russia's invasion of Ukraine
* The anti-satellite test ban must not undermine deterrence
* US Army wraps review of 'future battlespace' network tools
* DARPA budget request seeks to bolster 'critical' defense technologies
* Biden nominates Haugh as CYBERCOM deputy
* Intelligence agency takes over Project Maven, the Pentagon's signature AI scheme
* Pentagon wants at least $377 million over five years for new rapid experimentation fund
* NORAD's VanHerck says artificial intelligence capabilities lacking
* Pentagon hails Lyft exec Martell for AI post

The Hacker Corner

Conferences

* Zero Trust Cybersecurity Companies
* Types of Major Cybersecurity Threats In 2022
* The Five Biggest Trends In Cybersecurity In 2022
* The Fascinating Ineptitude Of Russian Military Communications
* Cyberwar In The Ukraine Conflict
* Our New Approach To Conference Listings
* Marketing Cybersecurity In 2022
* Cybersecurity Employment Market
* Cybersecurity Marketing Trends In 2021
* Is It Worth Public Speaking?

Google Zero Day Project

* The More You Know, The More You Know You Don't Know
* CVE-2021-1782, an iOS in-the-wild vulnerability in vouchers

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.

* EZ CTF | Beginner Friendly
* San Diego CTF 2022
* m0leCon CTF 2022 Teaser
* TJCTF 2022
* CTF InterIUT 2022
* @HackDay Final 2022
* Challenge the Cyber - Cyber Express
* Cyber Apocalypse CTF 2022: Intergalactic Chase
* VolgaCTF 2022 Qualifier
* 404 CTF

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

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

Tools & Techniques

Packet Storm Security Tools Links

* TOR Virtual Network Tunneling Tool 0.4.7.7
* nfstream 6.5.1
* GNU Privacy Guard 2.2.35
* Mandos Encrypted File System Unattended Reboot Utility 1.8.15
* GNU Privacy Guard 2.3.6
* Zeek 4.2.1
* Suricata IDPE 6.0.5
* XDNR Shellcode Cryptor / Encoder
* AIEngine 2.1.0
* Haveged 1.9.18

Kali Linux Tutorials

* S3Sec : Check AWS S3 Instances For Read/Write/Delete Access
* Nuclei-Burp-Plugin : Nuclei Plugin For BurpSuite
* Ghostbuster : Eliminate Dangling Elastic IPs By Performing Analysis On Your Resources
* Kali Linux - The Best Tool For Penetration Testing?
* Epagneul : Graph Visualization For Windows Event Logs
* S1EM : This Project Is A SIEM With SIRP And Threat Intel, All In One
* Mip22 : An Advanced Phishing Tool
* PurplePanda : Identify Privilege Escalation Paths Within And Across Different Clouds
* RefleXXion : A Utility Designed To Aid In Bypassing User-Mode Hooks Utilised By AV/EPP/EDR Etc
* WMEye : A Post Exploitation Tool That Uses WMI Event Filter And MSBuild Execution For Lateral Movemen

GBHackers Analysis

* Critical RCE Vulnerability in Google's VirusTotal Platform Let Attackers Scans Capabilities
* Critical Android Bug Let Attackers to Access Users' Media and Audio Conversations
* 15-Year-old Security Vulnerability In The PEAR PHP Repository Permits Supply Chain Attack
* Honda Bug Let Attackers Unlock and Start the Car
* Hundreds of HP Printer Models Affected by Critical Remote Code Execution

Weekly Cyber Security Video and Podcasts

SANS DFIR

* SANS Threat Analysis Rundown
* Inside FOR710 Reverse-Engineering Malware: Advanced Code Analysis
* The New GIAC MacOS and iOS Examiner Certification (GIME)
* CTI Summit Wrap Up Panel

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

* Watch Hackers Destroy Industrial Systems With Code - Retia
* WiFi Pineapple Version 2.0 + 5 Ghz Deep Dive and Q&A with Kody Kinzie and Darren Kitchen
* Zero Days Are On The Rise - ThreatWire

The PC Security Channel [TPSC]

* Avast vs Ransomware | Compared with Windows Defender
* Discord Infostealers: How hackers steal your password

Eli the Computer Guy

* Sick Day Project - Javascript and iPhone Accelerometer
* Having COVID SUCKS - my whole body hurts
* Dojo Derby - Race Timer Arduino Project
* I Got COVID - See you next week, unless I don't

Security Now

* The 0-Day Explosion - Lenovo EUFI Firmware, Everscale Blockchain Wallet, Major Java Update
* A Critical Windows RPC RCE - Another Chrome 0-day, MS Patch-Fest, US Nuclear Systems Unhackable?

Troy Hunt

* Weekly Update 293

Intel Techniques: The Privacy, Security, & OSINT Show

* 259-Leaving Kindle
* 258-Introducing UNREDACTED Magazine

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Home Clean Service System 1.0 SQL Injection
* Redis Lua Sandbox Escape
* Zepp 6.1.4-play User Account Enumeration
* Miele Benchmark Programming Tool 1.1.49 / 1.2.71 Privilege Escalation
* Backdoor.Win32.Agent.aegg Hardcoded Credential
* Trojan-Downloader.Win32.Agent Insecure Permissions
* Backdoor.Win32.GF.j Remote Command Execution
* Backdoor.Win32.Cafeini.b Man-In-The-Middle
* Backdoor.Win32.Cafeini.b Hardcoded Credential
* Trojan-Downloader.Win32.Small.ahlq Insecure Permissions
* Virus.Win32.Qvod.b Insecure Permissions
* Email-Worm.Win32.Sidex Remote Command Execution
* Net-Worm.Win32.Kibuv.c Authentication Bypass
* Backdoor.Win32.Jokerdoor Buffer Overflow
* Trojan-Banker.Win32.Banker.heq Insecure Permissions
* Prime95 30.7 Build 9 Buffer Overflow
* WordPress Curtain 1.0.2 Cross Site Scripting
* WordPress Coru LFMember 1.0.2 Cross Site Scripting
* Gitlab 14.9 Cross Site Scripting
* Gitlab 14.9 Authentication Bypass
* WordPress WP-Invoice 4.3.1 Cross Site Scripting
* Joomla Sexy Polling 2.1.7 SQL Injection
* WordPress ScrollReveal.js Effects 1.1.1 Cross Site Scripting
* ManageEngine ADSelfService Plus Custom Script Execution
* Watch Queue Out-Of-Bounds Write

CXSecurity

* Watch Queue Out-Of-Bounds Write
* Easy Appointments 1.4.2 Information Disclosure
* ManageEngine ADSelfService Plus Custom Script Execution
* USR IOT 4G LTE Industrial Cellular VPN Router 1.0.36 Remote Root Backdoor
* ManageEngine ADSelfService Plus 6.1 User Enumeration
* WordPress Elementor 3.6.2 Shell Upload
* Easy!Appointments Information Disclosure

Proof of Concept (PoC) & Exploits

Exploit Database

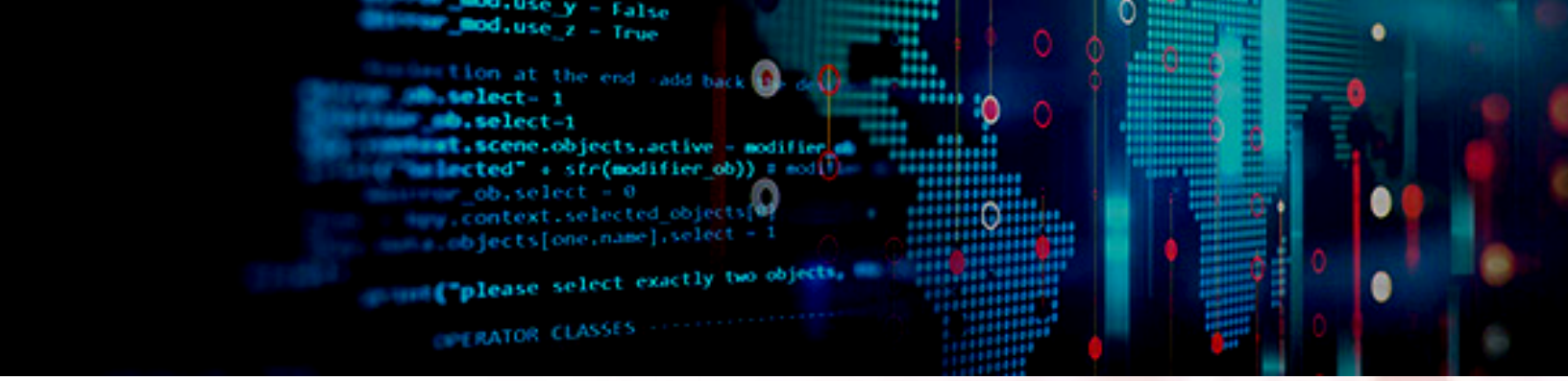
* [webapps] GitLab 14.9 - Stored Cross-Site Scripting (XSS)
* [webapps] Gitlab 14.9 - Authentication Bypass
* [local] EaseUS Data Recovery - 'ensserver.exe' Unquoted Service Path
* [local] PTPublisher v2.3.4 - Unquoted Service Path
* [webapps] Fuel CMS 1.5.0 - Cross-Site Request Forgery (CSRF)
* [webapps] WordPress Plugin Elementor 3.6.2 - Remote Code Execution (RCE) (Authenticated)
* [webapps] PKP Open Journals System 3.3 - Cross-Site Scripting (XSS)
* [remote] Delta Controls enteliTOUCH 3.40.3935 - Cookie User Password Disclosure
* [remote] Delta Controls enteliTOUCH 3.40.3935 - Cross-Site Scripting (XSS)
* [remote] Delta Controls enteliTOUCH 3.40.3935 - Cross-Site Request Forgery (CSRF)
* [webapps] REDCap 11.3.9 - Stored Cross Site Scripting
* [webapps] WordPress Plugin Popup Maker 1.16.5 - Stored Cross-Site Scripting (Authenticated)
* [remote] Verizon 4G LTE Network Extender - Weak Credentials Algorithm
* [webapps] WordPress Plugin Videos sync PDF 1.7.4 - Stored Cross Site Scripting (XSS)
* [remote] ManageEngine ADSelfService Plus 6.1 - User Enumeration
* [webapps] Scriptcase 9.7 - Remote Code Execution (RCE)
* [webapps] Easy Appointments 1.4.2 - Information Disclosure
* [remote] Zyxel NWA-1100-NH - Command Injection
* [webapps] WordPress Plugin Motopress Hotel Booking Lite 4.2.4 - SQL Injection
* [local] Microsoft Exchange Active Directory Topology 15.0.847.40 - 'Service MSExchangeADTopology' Unq
* [local] Microsoft Exchange Mailbox Assistants 15.0.847.40 - 'Service MSExchangeMailboxAssistants' Unq
* [webapps] Razer Sila - Command Injection
* [webapps] Razer Sila - Local File Inclusion (LFI)
* [webapps] Telesquare TLR-2855KS6 - Arbitrary File Deletion
* [webapps] Telesquare TLR-2855KS6 - Arbitrary File Creation

Exploit Database for offline use

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

user@yourlinux:~$ *searchsploit keyword1 keyword2*

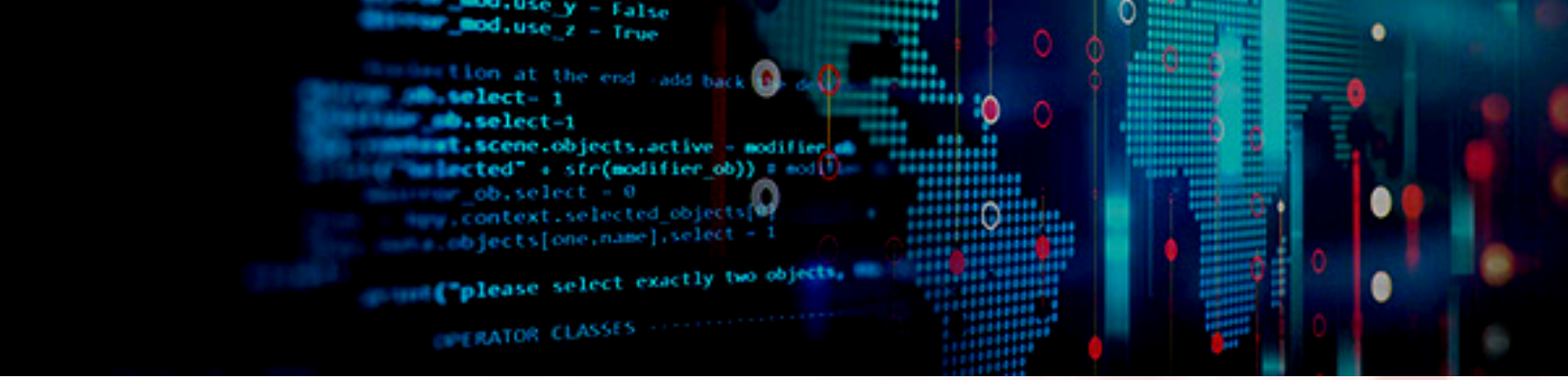
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://www.gid.gov.ly
https://www.gid.gov.ly notified by AnonCoders
https://pemkomedan.go.id/hell.php
https://pemkomedan.go.id/hell.php notified by hell_c0de
http://tapselkab.go.id/galau.html
http://tapselkab.go.id/galau.html notified by Simsimi
http://pn-muarabulian.go.id
http://pn-muarabulian.go.id notified by F4st~03
http://www.diskominfo.palikab.go.id
http://www.diskominfo.palikab.go.id notified by AnonCoders
http://kla.palikab.go.id
http://kla.palikab.go.id notified by AnonCoders
https://www.pnn.gov.co/psy.html
https://www.pnn.gov.co/psy.html notified by psycIllusion
http://palikab.go.id
http://palikab.go.id notified by Matigan1337
http://bappeda.bengkulutengahkab.go.id
http://bappeda.bengkulutengahkab.go.id notified by Matigan1337
https://perpustakaan.pa-ambarawa.go.id/ex.txt
https://perpustakaan.pa-ambarawa.go.id/ex.txt notified by AnonCoders
https://siormas.situbondokab.go.id
https://siormas.situbondokab.go.id notified by F4st~03
http://www.ssk3.go.th/zz.html
http://www.ssk3.go.th/zz.html notified by xNot_RespondinGx
http://pta-palu.go.id/hyme.html
http://pta-palu.go.id/hyme.html notified by Family Attack Cyber
https://pariwisata.tolitolikab.go.id
https://pariwisata.tolitolikab.go.id notified by Cubjrnet7
https://diskominfo.tolitolikab.go.id
https://diskominfo.tolitolikab.go.id notified by Cubjrnet7
http://rsudnyitdah.tabanankab.go.id
http://rsudnyitdah.tabanankab.go.id notified by 1877
http://newdisdukcapil.tabanankab.go.id
http://newdisdukcapil.tabanankab.go.id notified by 1877



Dark Web News

Darknet Live

German Arrested for Selling Marijuana on the Darkweb

Police in Lower Bavaria, Germany, arrested two men suspected of trading in large quantities of drugs through the dark web. According to a press release by police in Lower Bavaria, the first suspect, a 31-year-old man, has been selling marijuana through the darkweb since April 2021. The second suspect, a 25-year-old man, is accused of reselling marijuana purchased on the darkweb. He allegedly resold 10 kilograms of marijuana since February 2021. The investigations that led to the discovery of the suspects' identities were carried out by the Lower Bavaria criminal police inspectorate in conjunction with the Deggendorf and Landshut public prosecutors. On April 27, 2022, the investigators acquired and executed search warrants on the 31-year-old's apartment, workshop, and his girlfriend's apartment. At the same time, the police also searched the 25-year-old's apartment and his mother's apartment. The searches resulted in the seizure of approximately 400 pills containing an undisclosed opioid, anabolic steroids, and small quantities of undisclosed drugs. The investigators also found and seized several thousand euros and electronic devices. The press release also pointed to an increase in the number of drug cases in the region in 2021: After a decrease in registered offenses of 11.6% from 2019 to 2020, the statistics for 2021 show an increase of 225 cases (5.8%) to 4,131 cases (2020: 3,906). This is the second highest value in a ten-year comparison. The increase in illegal trade and smuggling alone is 91 cases to 685 (2020: 594 cases). At 94.4% in 2021 (2020: 95.3%), the clearance rate remained at a very high level. Drug-related crime consists almost exclusively of offenses that are usually only uncovered by police investigations and which express a connection between the statistical number of cases and successful intervention by the police. (via darknetlive.com at https://darknetlive.com/post/german-arrested-for-selling-marijuana-on-the-darkweb/)

Dark.fail's News Site to Launch "This Monday."

Dark.fail has been working on a news website and media organization that will launch "this Monday.” According to Dark.fail on Twitter, the news website has been a year in the making. Other than the fact that the site will require a subscription of some sort, there is very little publicly available information. Dark.fail: "It's my 4th year here, providing original reporting on privacy and cyber matters. Thank you readers. This Monday I launch my independent news website, years in the making. Want a free one year subscription? D.M. or email me your Protonmail within the next 24 hours. Hiring writers.” On April 29, Dark.fail tweeted , "Launching this Monday: my new media organization. (delayed by a bug.).” If the timeline does not shift, the launch will presumably take place on May 1, 2022. Subscriptions Perhaps the subscription model is the way to go here. As someone who is not truly anonymous or someone trying to stay out of the crosshairs of the U.S. government, there are not a ton of options here. There are the occasional emails, such as the one below, that read like bait from law enforcement. Most likely not LE but who knows. Someone could easily make a killing by launching a directory site and soliciting this. They would obviously have to maintain perfect OPSEC or stay out of the reach of the U.S. government. If someone was going to go through that whole routine, they might as well go all in - run phishing sites, exit scams with Eckmar scripts, etc. I do not have accurate traffic figures for this site. Still, I do know that while the total number of

pageviews is relatively high, the number of pageviews for most articles is much lower than the pageviews for practical pages like Dread, Not Evil, the market list, etc. Articles generate more activity than new markets and less popular forums. But as a general rule, over 30 days, the market list, the onion list, Dread, the forum list, a couple of markets, etc., will all generate more pageviews than any article. This is a fairly typical lineup for pageviews over 30 days. Dark.fail generates more pageviews than this site, I suspect. The news organization might be a successful venture financially. I am not trying to sound like I am complaining about anything (Dark.fail potentially finding a way to make running an independent news site financially viable). I did not take this on to make money. (via darknetlive.com at https://darknetlive.com/post/darkfails-news-site-to-launch-this-monday/)

FinCEN: PATRIOT Act Is Not the "Right Size" for Crypto Threats

The acting director of the United States Financial Crimes Enforcement Network, Him Das, laid the groundwork for expanding PATRIOT Act powers to counter the so-called "threats” posed by cryptocurrency. Das' comments were a part of a House Financial Services Committee hearing on "Oversight of the Financial Crimes Enforcement Network.” During the hearing, Kentucky Representative Andy Barr pointed out that the Financial Crimes Enforcement Network (FinCEN) rarely used the "special measures” authorized under Section 311 of the PATRIOT Act. Section 311 is summarized by the Treasury Department as "a range of options that can be adapted to target specific money laundering and terrorist financing risks most effectively.” Acting Director of the United States Financial Crimes Enforcement Network, Him Das Das explained that Section 311 applied primarily to traditional financial systems. "Section 311 was enacted in a time when most financial relationships and transactions were done through the traditional banking system where there are traditional correspondent account relationships,” he said. "Nowadays, cross-border transactions often include money services businesses, payment systems, […] foreign exchange houses as well as cryptocurrency.” Das also hinted at the need to expand FinCEN's powers under Section 311. "Currently, the Section 311 authority is not right-sized for the types of threats that we're seeing through the use of cryptocurrency.” Das also spoke about FinCEN's plans to regulate "unhosted wallets.” The Treasury Department's regulatory plan from January revealed that additional cryptocurrency regulations were under consideration.

"It's not that unhosted wallets are entirely opaque. Unhosted wallets often engage in transactions with cryptocurrency exchanges, which are subject to AML/CFT regulation […] Law enforcement can engage with cryptocurrency exchanges with respect to suspicious activity reporting and other reports that might be applicable to them in terms of getting some degree of understanding in terms of transactions with unhosted wallets as well.” Representatives also asked questions about FinCEN's ability to counter the potential use of cryptocurrency by "Russian oligarchs” to evade sanctions imposed by the United States. Das reiterated FinCEN's position from March when he answered a similar question: "In the face of mounting economic pressure on Russia, it is vitally important for U.S. financial institutions to be vigilant about potential Russian sanctions evasion, including by both state actors and oligarchs. Although we have not seen widespread evasion of our sanctions using methods such as cryptocurrency, prompt reporting of suspicious activity contributes to our national security and our efforts to support Ukraine and its people.” 🪝🪝🪝 At the recent hearing, Das said, "we've not seen large-scale evasion through the use of cryptocurrency, but we're mindful of that and we're working with financial institutions so that they're aware of that potential that we can identify a large-scale evasion using cryptocurrency and act on it as well.” "Oversight of the Financial Crimes Enforcement Network” Memorandum pdf Summary page archive.is, archive.org, financialservices.house.gov YouTube broadcast youtube.com (via darknetlive.com at https://darknetlive.com/post/fincen-patriot-act-powers-are-not-the-right-size-for-crypto-threats/)

US Charges Two Europeans Over DPRK Crypto Conference

The United States has charged two Europeans for allegedly conspiring to bring a cryptocurrency conference to the Democratic People's Republic of Korea. DPRK Alejandro Cao De Benos, 47, a citizen of Spain, and Christopher Emms, 30, a citizen of the United Kingdom, planned and

organized the DPRK Cryptocurrency Conference, according to a superseding indictment unsealed in the Southern District of New York. Christopher Emms and Alejandro Cao De Benos

The United States clarified that it still has the power to decide which nations are allowed to pursue a policy of mutually assured destruction. "The United States will not allow the North Korean regime to use cryptocurrency to evade global sanctions designed to thwart its goals of nuclear proliferation and regional destabilization,” said Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division. "This indictment, along with the successful prosecution of co-conspirator, Virgil Griffith, makes clear that the department will hold anyone, wherever located, accountable for conspiring with North Korea to violate U.S. sanctions.” Cao De Benos and Emms allegedly recruited Griffith, a citizen of the United States who lived in Singapore, to deliver a presentation at the DPRK Cryptocurrency Conference titled "Blockchain and Peace.” Cao De Benos and Emms are co-conspirators identified as "Individual 1” and "Individual 2” in Griffith's court documents. In 2018, Cao De Benos and Emms allegedly planned and organized the DPRK Cryptocurrency Conference. As a part of their alleged conspiracy, they arranged for Griffith's travel to the DPRK in April 2019. Emms told Griffith that DPRK "would not stamp [your] passport.” As the court documents from Griffth's case revealed, DPRK officials never stamped Griffith's passport. Instead, they stamped a separate piece of paper. "As alleged, Alejandro Cao de Benos and Christopher Emms conspired with Virgil Griffith, a cryptocurrency expert convicted of conspiring to violate economic sanctions imposed on North Korea, to teach and advise members of the North Korean government on cutting-edge cryptocurrency and blockchain technology, all for the purpose of evading U.S. sanctions meant to stop North Korea's hostile nuclear ambitions,” said U.S. Attorney Damian Williams for the Southern District of New York. "In his own sales pitch, Emms allegedly advised North Korean officials that cryptocurrency technology made it 'possible to transfer money across any country in the world regardless of what sanctions or any penalties that are put on any country.' The sanctions imposed against North Korea are critical in protecting the security interests of Americans, and we continue to aggressively enforce them with our law enforcement partners both here and abroad.”

I have seen a more recent picture where the Glorious Leader looks more healthy than this but I can't find them. Emms opened the conference by stating that it was a "great honor” to be "leading this delegation” to "explain to you a lot about blockchain… and how you can use this technology here in the DPRK.” At the conference, Emms and Griffith answered questions about cryptocurrency from "individuals whom they understood worked for the North Korean government.” Although feds from the United States presumably attended the conference, the italicized phrase could mean that investigators did not verify if the individuals worked for the Korean government. Emms and Griffith "mapped out cryptocurrency transactions designed to evade and avoid U.S. sanctions” by "diagraming such transactions on a whiteboard.” Cao De Benos and Emms allegedly conspired with Griffith after the conference by trying to introduce conference attendees to cryptocurrency service providers. According to the Department of Justice, they also discussed developing infrastructure related to cryptocurrency within the DPRK. All three defendants also allegedly planned a second DPRK Cryptocurrency Conference for 2020, but Griffith's arrest in November 2019 disrupted their plans.

Their plans for a second cryptocurrency conference in the DPRK were thwarted. The superseding indictment charges Cao De Benos and Emms, each with one count of conspiring to violate and evade U.S. sanctions in violation of IEEPA. The charge carries a maximum statutory penalty of 20 years in federal prison. Cao De Benos and Emms are charged with one count of conspiring to violate and evade U.S. sanctions in violation of IEEPA, which carries a maximum statutory penalty of 20 years in prison. Griffith pleaded guilty to one count of conspiracy to violate the IEEPA. A judge sentenced him to 63 months in federal prison and a fine of $100,000. Two European Citizens Charged for Conspiring with a U.S. Citizen to Assist North Korea in Evading U.S. Sanctions archive.is archive.org justice.gov In an ordinary world, one might assume that Cao De Benos and Emms would have avoided an outcome such as this one by involving speakers without U.S. or U.S.-adjacent citizenships. Of course, feds could have slipped an undercover agent in with other attendees to bring Cao De Benos and Emms into the broad scope of U.S. law enforcement's jurisdiction. I am not sure they would even bother with that technicality

anymore. Every leader without "our values” is a madman On top of all of this, sanctions do not work. At least not in a way that accomplishes the stated purpose of the sanctions. The United States has conducted military drills with the K-Pop Korea, south of the DPRK, sends them military equipment, etc. I feel as if we have seen this situation before. Maybe Cao De Benos and Emms can possibly disappear in Russia, China, or Belarus. I am not sure they could receive asylum in the DPRK. They are not in custody currently, but if they get arrested, they will get extradited to the United States where a prison sentence is a certainty. (via darknetlive.com at https://darknetlive.com/post/us-charges-two-europeans-for-planning-dprk-crypto-conference/)

Dark Web Link

Top Darknet Markets 2022: The Outstanding Performances To Consider Now

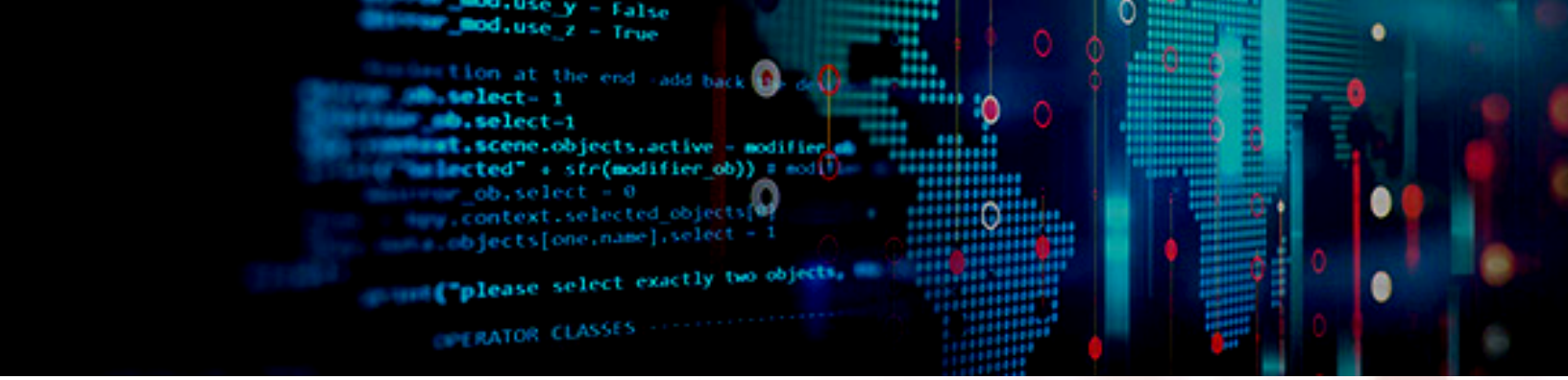
The darknet markets are subject to availability and one of the many factors that contributes to the working of these dark web markets is their performances. The top darknet markets 2022 is the example where each of the marketplaces in the Tor network has proven its performance over and over again. So, 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

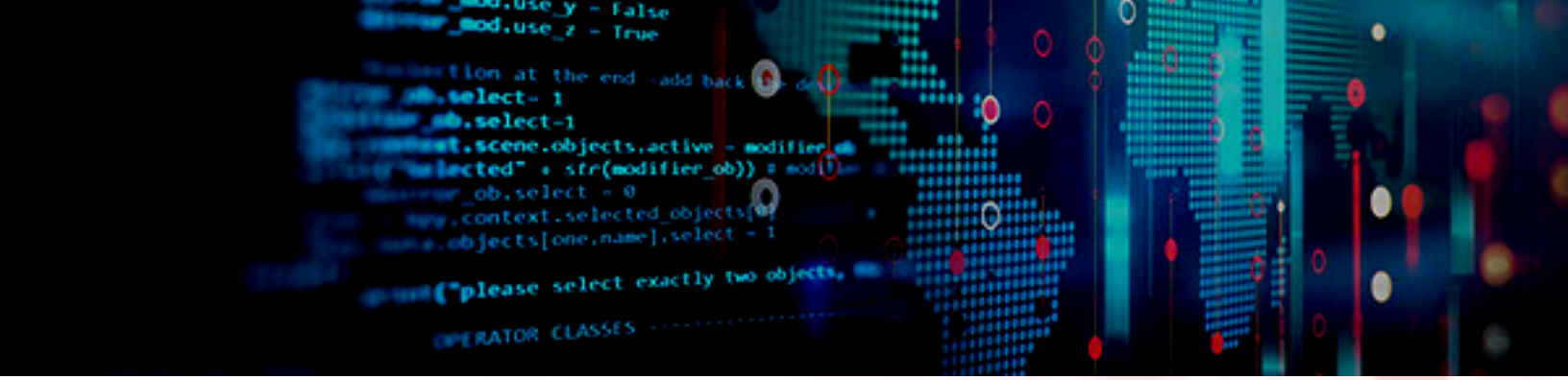
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

* RiskIQ Threat Intelligence Roundup: Trickbot, Magecart, and More Fake Sites Targeting Ukraine
* 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

FireEye

* Metasploit Wrap-Up
* Widespread Exploitation of VMware Workspace ONE Access CVE-2022-22954
* [Security Nation] Whitney Merrill on the Crypto & Privacy Village (and the Latest in Data Privacy)
* How to Strategically Scale Vendor Management and Supply Chain Security
* Velociraptor Version 0.6.4: Dead Disk Forensics and Better Path Handling Let You Dig Deeper
* Opportunistic Exploitation of WSO2 CVE-2022-29464
* Metasploit Weekly Wrap-Up
* Rapid7 Named a Visionary in 2022 Magic Quadrantâ„¢ for Application Security Testing Second Year in a
* 2022 Cloud Misconfigurations Report: A Quick Look at the Latest Cloud Security Breaches and Attack Tr
* What's New in InsightVM and Nexpose: Q1 2022 in Review



Advisories

US-Cert Alerts & bulletins

* Cisco Releases Security Updates for Multiple Products
* Google Releases Security Updates for Chrome
* CISA and FBI Update Advisory on Destructive Malware Targeting Organizations in Ukraine
* 2021 Top Routinely Exploited Vulnerabilities
* CISA Adds Seven Known Exploited Vulnerabilities to Catalog
* FBI Releases IOCs Associated with BlackCat/ALPHV Ransomware
* Drupal Releases Security Updates
* Cisco Releases Security Updates for Multiple Products
* AA22-117A: 2021 Top Routinely Exploited Vulnerabilities
* AA22-110A: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure
* Vulnerability Summary for the Week of April 18, 2022
* Vulnerability Summary for the Week of April 11, 2022

Zero Day Initiative Advisories

Packet Storm Security - Latest Advisories

Red Hat Security Advisory 2022-1644-01

Red Hat Security Advisory 2022-1644-01 - XML-RPC is a remote procedure call protocol that uses XML to encode its calls and HTTP as a transport mechanism. The xmlrpc-c packages provide a network protocol to allow a client program to make a simple RPC over the Internet. It converts an RPC into an XML document, sends it to a remote server using HTTP, and gets back the response in XML. Issues addressed include a code execution vulnerability.

Red Hat Security Advisory 2022-1492-01

Red Hat Security Advisory 2022-1492-01 - The OpenJDK 8 packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Software Development Kit. This release of the Red Hat build of OpenJDK 8 for Windows serves as a replacement for the Red Hat build of OpenJDK 8 and includes security and bug fixes, and enhancements.

Red Hat Security Advisory 2022-1643-01

Red Hat Security Advisory 2022-1643-01 - XML-RPC is a remote procedure call protocol that uses XML to encode its calls and HTTP as a transport mechanism. The xmlrpc-c packages provide a network protocol to allow a client program to make a simple RPC over the Internet. It converts an RPC into an XML document, sends it to a remote server using HTTP, and gets back the response in XML. Issues addressed include a code execution vulnerability.

Red Hat Security Advisory 2022-1436-01

Red Hat Security Advisory 2022-1436-01 - The OpenJDK 17 packages provide the OpenJDK 17 Java Runtime Environment and the OpenJDK 17 Java Software Development Kit. This release of the Red Hat build of OpenJDK 17 for portable Linux serves as a replacement for the Red Hat build of OpenJDK 17 and includes security and bug fixes, and enhancements.

Red Hat Security Advisory 2022-1437-01

Red Hat Security Advisory 2022-1437-01 - The OpenJDK 17 packages provide the OpenJDK 17 Java Runtime Environment and the OpenJDK 17 Java Software Development Kit. This release of the Red Hat build of OpenJDK 17 for portable Linux serves as a replacement for the Red Hat build of OpenJDK 17 and includes security and bug fixes, and enhancements.

Red Hat Security Advisory 2022-1439-01

Red Hat Security Advisory 2022-1439-01 - The OpenJDK 11 packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Software Development Kit. This release of the Red Hat build of OpenJDK 11 for Windows serves as a replacement for the Red Hat build of OpenJDK 11 and includes security and bug fixes, and enhancements.

Red Hat Security Advisory 2022-1438-01

Red Hat Security Advisory 2022-1438-01 - The OpenJDK 8 packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Software Development Kit. This release of the Red Hat build of OpenJDK 8 for portable Linux serves as a replacement for Red Hat build of OpenJDK 8 and includes security and bug fixes as well as enhancements.

Red Hat Security Advisory 2022-1435-01

Red Hat Security Advisory 2022-1435-01 - The OpenJDK 11 packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Software Development Kit. This release of the Red Hat build of OpenJDK 11 for portable Linux serves as a replacement for the Red Hat build of OpenJDK 11 and includes security and bug fixes, and enhancements.

Ubuntu Security Notice USN-5398-1

Ubuntu Security Notice 5398-1 - It was discovered that SDL incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code.

Ubuntu Security Notice USN-5397-1

Ubuntu Security Notice 5397-1 - Patrick Monnerat discovered that curl incorrectly handled certain OAUTH2. An attacker could possibly use this issue to access sensitive information. Harry Sintonen discovered that curl

incorrectly handled certain requests. An attacker could possibly use this issue to expose sensitive information.
Ubuntu Security Notice USN-5396-1
Ubuntu Security Notice 5396-1 - It was discovered that Ghostscript incorrectly handled certain PostScript files. If a user or automated system were tricked into processing a specially crafted file, a remote attacker could possibly use this issue to access arbitrary files, execute arbitrary code, or cause a denial of service.
Ubuntu Security Notice USN-5395-1
Ubuntu Security Notice 5395-1 - It was discovered that networkd-dispatcher incorrectly handled internal scripts. A local attacker could possibly use this issue to cause a race condition, escalate privileges and execute arbitrary code.
Red Hat Security Advisory 2022-1642-01
Red Hat Security Advisory 2022-1642-01 - The zlib packages provide a general-purpose lossless data compression library that is used by many different programs.
Ubuntu Security Notice USN-5392-1
Ubuntu Security Notice 5392-1 - It was discovered that Mutt incorrectly handled certain requests. An attacker could possibly use this issue to expose sensitive information. This issue only affected Ubuntu 20.04 LTS. It was discovered that Mutt incorrectly handled certain input. An attacker could possibly use this issue to cause a crash, or expose sensitive information.
Ubuntu Security Notice USN-5394-1
Ubuntu Security Notice 5394-1 - A large number of security issues were discovered in the WebKitGTK Web and JavaScript engines. If a user were tricked into viewing a malicious website, a remote attacker could exploit a variety of issues related to web browser security, including cross-site scripting attacks, denial of service attacks, and arbitrary code execution.
Ubuntu Security Notice USN-5371-2
Ubuntu Security Notice 5371-2 - USN-5371-1 fixed several vulnerabilities in nginx. This update provides the fix for CVE-2021-3618 for Ubuntu 22.04 LTS. It was discovered that nginx Lua module mishandled certain inputs. An attacker could possibly use this issue to perform an HTTP Request Smuggling attack. This issue only affects Ubuntu 18.04 LTS and Ubuntu 20.04 LTS.
Ubuntu Security Notice USN-5393-1
Ubuntu Security Notice 5393-1 - 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, conduct spoofing attacks, or execute arbitrary code. It was discovered that Thunderbird ignored OpenPGP revocation when importing a revoked key in some circumstances. An attacker could potentially exploit this by tricking the user into trusting the authenticity of a message or tricking them into use a revoked key to send an encrypted message.
Ubuntu Security Notice USN-5391-1
Ubuntu Security Notice 5391-1 - Nicolas Iooss discovered that libsepol incorrectly handled memory when handling policies. An attacker could possibly use this issue to cause a crash, resulting in a denial of service, or possibly execute arbitrary code. It was discovered that libsepol incorrectly handled memory when handling policies. An attacker could possibly use this issue to cause a crash, resulting in a denial of service, or possibly execute arbitrary code.
Red Hat Security Advisory 2022-1628-01
Red Hat Security Advisory 2022-1628-01 - Red Hat Gluster Storage Web Administration includes a fully automated setup based on Ansible and provides deep metrics and insights into active Gluster storage pools by using the Grafana platform. Red Hat Gluster Storage Web Administration provides a dashboard view that allows an administrator to get a view of overall gluster health in terms of hosts, volumes, bricks, and other components of GlusterFS.
Red Hat Security Advisory 2022-1420-01
Red Hat Security Advisory 2022-1420-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory

contains the RPM packages for Red Hat OpenShift Container Platform 3.11.665. Issues addressed include bypass and denial of service vulnerabilities.

[WordPress Booking Calendar 9.1 PHP Object Injection / Insecure Deserialization]

WordPress Booking Calendar plugin versions 9.1 and below suffer from PHP object injection and insecure deserialization vulnerabilities.

[Ubuntu Security Notice USN-5376-3]

Ubuntu Security Notice 5376-3 - USN-5376-1 fixed vulnerabilities in Git, some patches were missing to properly fix the issue. This update fixes the problem. 俞晨东 discovered that Git incorrectly handled certain repository paths in platforms with multiple users support. An attacker could possibly use this issue to run arbitrary commands.

[Red Hat Security Advisory 2022-1626-01]

Red Hat Security Advisory 2022-1626-01 - AMQ Broker is a high-performance messaging implementation based on ActiveMQ Artemis. It uses an asynchronous journal for fast message persistence, and supports multiple languages, protocols, and platforms. This release of Red Hat AMQ Broker 7.8.6 serves as a replacement for Red Hat AMQ Broker 7.8.5, and includes security and bug fixes, and enhancements.

[Red Hat Security Advisory 2022-1627-01]

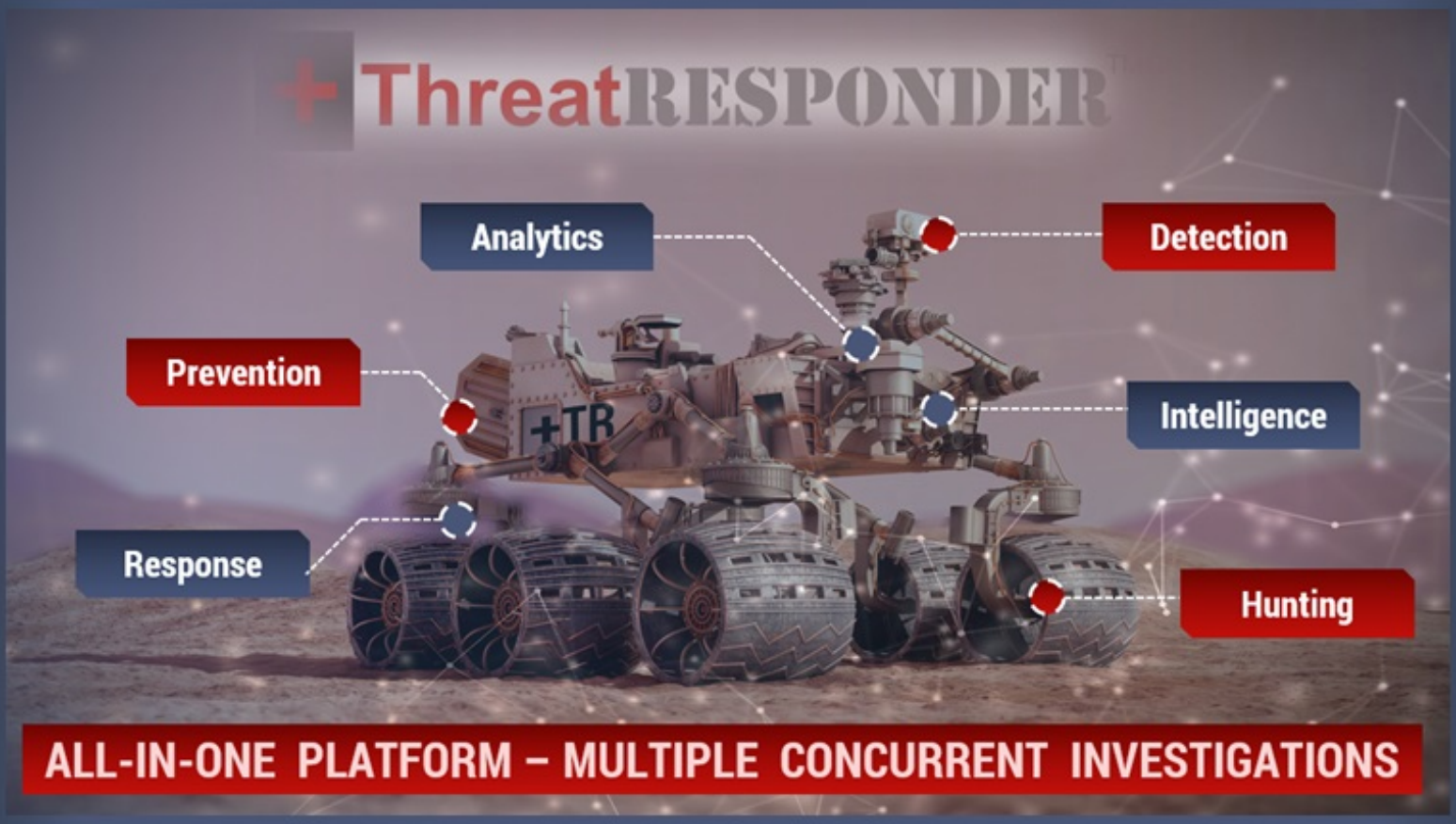
Red Hat Security Advisory 2022-1627-01 - AMQ Broker is a high-performance messaging implementation based on ActiveMQ Artemis. It uses an asynchronous journal for fast message persistence, and supports multiple languages, protocols, and platforms. This release of Red Hat AMQ Broker 7.9.4 serves as a replacement for Red Hat AMQ Broker 7.9.3, and includes security and bug fixes, and enhancements.

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



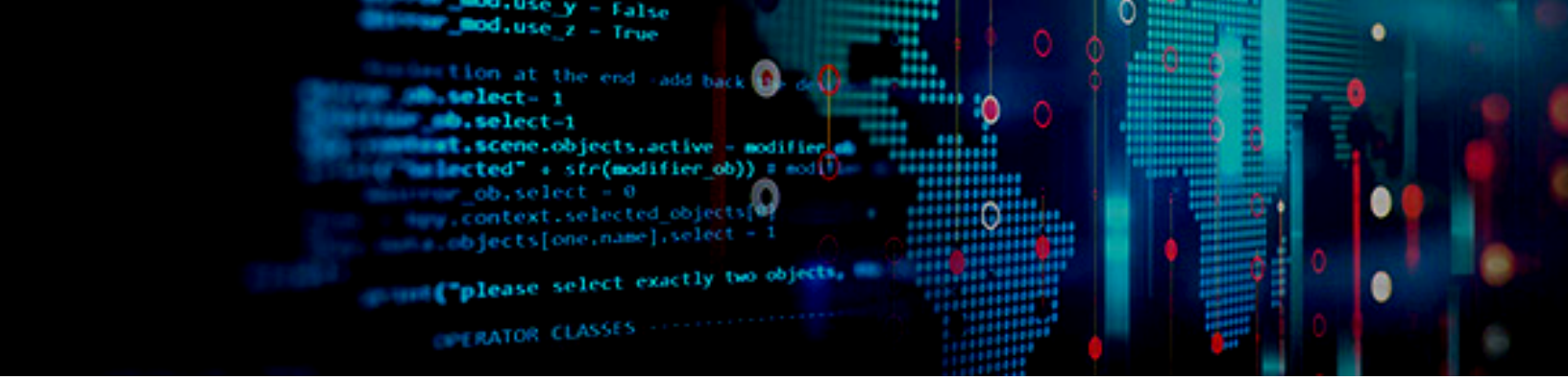
The Solution – ThreatResponder® Platform

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

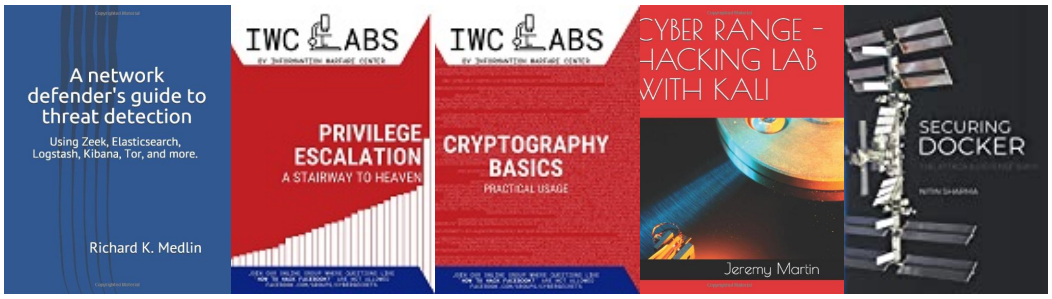


The Cyber Secrets publications on Amazon

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