Mar-28-22

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

March 28, 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

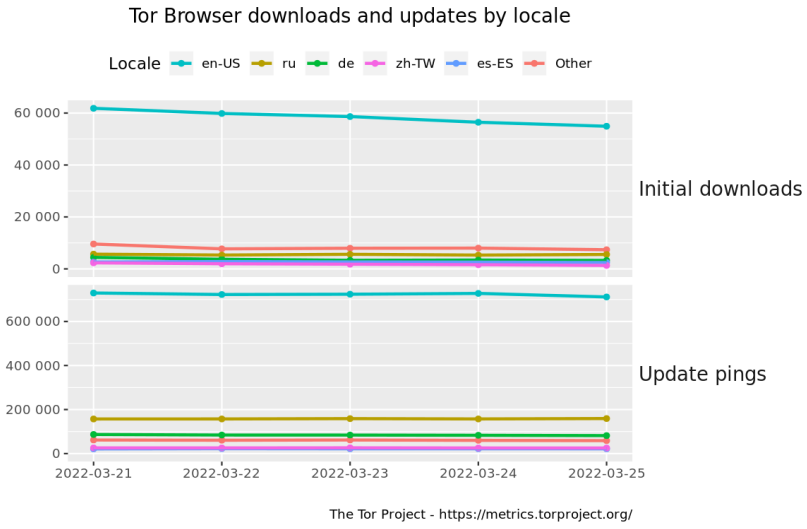
Internet Storm Center Infocon Status

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

* Morgan Stanley Wealth Management Accounts Breached In Vishing Attack
* Hundreds More Packages Found In Malicious npm Factory
* FCC Puts Kaspersky On Security Threat List
* Sophos Patches Critical Remote Code Execution Vulnerability In Firewall
* Feds Allege Destructive Russian Hackers Targeted US Oil Refineries
* Frosties NFT Operators Arrested Over $1.1 Million Rug Pull Scam
* Russia Hacked Ukrainian Satellite Comms, Officials Believe
* US Charges 4 Russian Hackers Over Attacks On Energy Sector
* UK Cops Collar 7 Suspected Lapsus$ Gang Members
* North Korean Hackers Unleashed Chrome 0-Day Exploit On Hundreds Of US Targets
* North Korea TV Airs Action Movie-Style Footage Of Newest Nuclear Missile
* Grimes Said She Orchestrated Cyber Attack That Shut Down Hipster Runoff
* Microsoft Help Files Disguise Vidar Malware
* The Three Russian Cyber Attacks The West Most Fears
* Malicious npm Packages Target Azure Devs To Steal Personal Data
* Nestle: Anonymous Can't Hack Us, We Leaked Our Own Data
* UK Ministry Of Defence Takes Recruitment System Offline, Confirms Data Leak
* ImpressCMS: From Unauthenticated SQL Injection To RCE
* Someone Hacked The Spelling Bee
* Hackers Are Targeting European Refugee Charities
* Lockbit Wins Ransomware Speed Test, Encrypts 25,000 Files Per Minute
* This Is How Much The Average Conti Hacking Group Member Earns A Month
* Serpent Backdoor Uses Chocolatey Installer
* Biden: Russia Exploring US Cyber Attacks
* Okta Breached Through Customer Support

Krebs on Security

* Estonian Tied to 13 Ransomware Attacks Gets 66 Months in Prison
* A Closer Look at the LAPSUS$ Data Extortion Group
* 'Spam Nation' Villain Vrublevsky Charged With Fraud
* Pro-Ukraine 'Protestware' Pushes Antiwar Ads, Geo-Targeted Malware
* Lawmakers Probe Early Release of Top RU Cybercrook
* Report: Recent 10x Increase in Cyberattacks on Ukraine
* Microsoft Patch Tuesday, March 2022 Edition
* Internet Backbone Giant Lumen Shuns .RU
* Conti Ransomware Group Diaries, Part IV: Cryptocrime
* Conti Ransomware Group Diaries, Part III: Weaponry

Dark Reading

* Zero-Day Surge Led to More Rapid Exploitation of Bugs in 2021
* Triton Malware Still Targeting Energy Firms
* Vodafone Portugal: The Attack on Brand Reputations and Public Confidence Through Cybercrime
* Security's Life Cycle Isn't the Developers' Life Cycle
* Indictment of Russian National Offers Glimpse Into Methodical Targeting of Energy Firm
* How Do I Demonstrate the ROI of My Security Program?
* WiCyS Members Now Have Access to Cyber Defense Challenge Through Target
* Here's How Fast Ransomware Encrypts Files
* HR Alone Can't Solve the Great Resignation
* Russian Nationals Indicted for Epic Triton/Trisis and Dragonfly Cyberattacks on Energy Firms
* Downloaders Currently the Most Prevalent Android Malware
* How Casinos Can Prevent Loyalty Incentive and Account Takeover Fraud
* Ransomware Payments, Demands Rose Dramatically in 2021
* Pandemic Leaves Firms Scrambling for Cybersecurity Specialists
* For MSPs, Next-Gen Email Security Is a Must
* APIs & the Software Supply Chain - Evolving Security for Today's Digital Ecosystem
* What the Conti Ransomware Group Data Leak Tells Us
* FBI: Cybercrime Victims Suffered Losses of Over $6.9B in 2021
* Okta Says 366 Customers Impacted via Third-Party Breach
* Could Gaming Close the Cyberskills Gap?

The Hacker News

* Hackers Hijack Email Reply Chains on Unpatched Exchange Servers to Spread Malware
* Of Cybercriminals and IP Addresses
* 'Purple Fox' Hackers Spotted Using New Variant of FatalRAT in Recent Malware Attacks
* Muhstik Botnet Targeting Redis Servers Using Recently Disclosed Vulnerability
* FCC Adds Kaspersky and Chinese Telecom Firms to National Security Threat List
* Another Chinese Hacking Group Spotted Targeting Ukraine Amid Russia Invasion
* Google Issues Urgent Chrome Update to Patch Actively Exploited Zero-Day Vulnerability
* U.S. Charges 4 Russian Govt. Employees Over Hacking Critical Infrastructure Worldwide
* 7 Suspected Members of LAPSUS$ Hacker Gang, Aged 16 to 21, Arrested in U.K.
* Experts Uncover Campaign Stealing Cryptocurrency from Android and iPhone Users
* North Korean Hackers Exploited Chrome Zero-Day to Target Fintech, IT, and Media Firms
* 23-Year-Old Russian Hacker Wanted by FBI for Running Marketplace of Stolen Logins
* Chinese APT Hackers Targeting Betting Companies in Southeast Asia
* How to Build a Custom Malware Analysis Sandbox
* Researchers Trace LAPSUS$ Cyber Attacks to 16-Year-Old Hacker from England

Security Week

* Researchers Hack Remote Keyless System of Honda Vehicles
* Checkmarx Finds Threat Actor 'Fully Automating' NPM Supply Chain Attacks
* Estonian Ransomware Operator Sentenced to Prison in US
* German Authorities Seize Spyware Firm FinFisher's Accounts
* Critical Remote Code Execution Vulnerability in Sophos Firewall
* CISA Adds 66 Vulnerabilities to 'Must Patch' List
* Google Issues Emergency Fix for Chrome Zero-Day
* US, EU Sign Data Transfer Deal to Ease Privacy Concerns
* Chinese Hackers Seen Targeting Ukraine Post-Invasion
* MixMode Banks $45 Million in Series B Funding
* The Elusive Goal of Network Security
* FBI: 649 Ransomware Attacks Reported on Critical Infrastructure Organizations in 2021
* How European Rulings Imperil Flagship Google Product
* US Charges Russian Hackers Over Infamous Triton, Havex Cyberattacks on Energy Sector
* North Korea Gov Hackers Caught Sharing Chrome Zero-Day
* The Chaos (and Cost) of the Lapsus$ Hacking Carnage
* New Vidar Infostealer Campaign Hidden in Help File
* Over 100 Building Controllers in Russia Vulnerable to Remote Hacker Attacks
* Enterprise Browser Startup Island Snags Massive Funding Round
* Russian Operator of Cybercrime Marketplace Indicted in US
* Many Critical Flaws Patched in Delta Electronics Energy Management System
* VMware Patches Critical Vulnerabilities in Carbon Black App Control
* Achieving Positive Outcomes With Multi-Domain Cyber and Open Source Intelligence
* Serious Vulnerability Exploited at Hacking Contest Impacts Over 200 HP Printers
* Theta Lake Raises $50 Million in Series B Funding Round
* Ransomware, Malware-as-a-Service Dominate Threat Landscape

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* KnowBe4 and Okta Update
* Making Better Push-Based MFA
* Buy Now, Pay Later Scams
* WIRED: "A Mysterious Satellite Hack Has Victims Far Beyond Ukraine"
* Fidelity: "Why cybersecurity is material to all industries"
* Repertoire of Ukraine Charity Phishing Scams
* Initial Access Broker Group Relies on Social Engineering
* Try the New Compliance Audit Readiness Assessment Today for the SSAE18 Framework
* Number of Phishing Attacks Hits an All-Time High in 2021, Tripling That of Early 2020
* Phishing Attack-Turned-Wire Fraud Case Sees a Win for the Policyholder

ISC2.org Blog

* HOW CAN YOU WIN BIG IN VEGAS? - Global Achievement Awards Nominations Open Now
* Tips from a CISO: How to Create a Security Program
* GOING FOR (ISC)² CERTIFICATION? GET THE FACTS BEFORE YOU CHOOSE A TRAINING PROVIDER
* What Concerns Cyber Pros Most About the Invasion of Ukraine
* Meet the Young Women Tackling Gender Bias in Cybersecurity

HackRead

* Anonymous Hacks 2 Russian Industrial Firms, Leak 112GB of Data for Ukraine
* Update Chrome Browser Now - Google Releases Emergency Security Update
* RAV Antivirus: How to Protect Your Data in 2022
* US Adds Kaspersky to List of Firms Posing Threat to National Security
* Confirmed: Anonymous Hacks Central Bank of Russia; Leaks 28GB of Data
* 100s of Russian Building Controllers Can be Remotely Hacked
* Modern Gaming Sucks Because of Abundance Fatigue

Koddos

* Anonymous Hacks 2 Russian Industrial Firms, Leak 112GB of Data for Ukraine
* Update Chrome Browser Now - Google Releases Emergency Security Update
* RAV Antivirus: How to Protect Your Data in 2022
* US Adds Kaspersky to List of Firms Posing Threat to National Security
* Confirmed: Anonymous Hacks Central Bank of Russia; Leaks 28GB of Data
* 100s of Russian Building Controllers Can be Remotely Hacked
* Modern Gaming Sucks Because of Abundance Fatigue

Naked Security

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

Threat Post

* Okta Says It Goofed in Handling the Lapsus$ Attack
* Critical Sophos Security Bug Allows RCE on Firewalls
* DOJ Indicts Russian Gov't Employees Over Targeting Power Sector
* Google Chrome Zero-Day Bugs Exploited Weeks Ahead of Patch
* UK Cops Collar 7 Suspected Lapsus$ Gang Members
* Microsoft Azure Developers Awash in PII-Stealing npm Packages
* Just-Released Dark Souls Game, Elden Ring, Includes Killer Bug
* HubSpot Data Breach Ripples Through Crytocurrency Industry
* Chinese APT Combines Fresh Hodur RAT with Complex Anti-Detection
* Microsoft Help Files Disguise Vidar Malware

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

* Beyond SQL: 8 new languages for data querying
* If you build it, it will run
* Managing the complexity of cloud strategies
* Microsoft ends support for .NET 5.0
* PlanetScale introduces Rewind feature to 'undo' bad schema migrations
* Redis Stack outfits Redis for real-time apps
* Why governance is critical to cloud success
* DataStax adds real-time data streaming to managed AstraDB service
* ECMAScript 2022 endorses class fields, top-level await
* Intro to Lit: A JavaScript framework

C4ISRNET - Media for the Intelligence Age Military

* Navy dramatically increases funding for secretive Project Overmatch
* Pentagon seeks $11.2 billion for cyber in FY23 budget request
* Space Force wants 40% budget increase as it looks to bolster space-based missile warning
* Cuts to Army's IVAS were 'good oversight' by Congress, says acquisitions boss
* Webcast: Army Spring Update 2022
* US Air Force establishes new information warfare detachment
* Following cyberattack, communication satellite operators want more guidance on reporting
* Lockheed eyes Project Convergence after successful 5G expedition
* NATO wants a say in 5G standardization talks
* DoD acquisition nominee pledges to push advanced tech, small business opportunities

The Hacker Corner

Conferences

* 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
* Is It Worth Public Speaking?
* Our Guide To Cybersecurity Marketing Campaigns
* How To Choose A Cybersecurity Marketing Agency
* The Hybrid Conference Model

Google Zero Day Project

* Racing against the clock -- hitting a tiny kernel race window
* A walk through Project Zero metrics

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.

* Space Heroes CTF
* RITSEC CTF 2022
* UMassCTF 2022
* Midnight Sun CTF 2022 Quals
* Imperial CTF 22
* nullcon HackIM 2022
* @HackDay Qualification 2022
* PlaidCTF 2022
* Winja CTF | Nullcon Berlin 2022
* JerseyCTF II

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

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

Tools & Techniques

Packet Storm Security Tools Links

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

Kali Linux Tutorials

* Chain-Reactor : An Open Source Framework For Composing Executables
* Voltron : A Hacky Debugger UI For Hackers
* SSR Fire : An Automated SSRF Finder. Just Give The Domain Name And Your Server
* Hybrid Test Framework : End To End Testing Of Web, API And Security
* Talisman : By Hooking Talisman Validates The Outgoing Changeset For Things That Look Suspicious
* Sharp Cookie Monster : Extracts Cookies From Chrome
* Njsscan : A Semantic Aware SAST Tool That Can Find Insecure Code Patterns In Node.js Applications
* Snaffler : A Tool For Pentesters To Help Find Delicious Candy
* Macrome : Excel Macro Document Reader/Writer For Red Teamers And Analysts
* FakeLogonScreen : Fake Windows Logon Screen To Steal Passwords

GBHackers Analysis

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

Weekly Cyber Security Video and Podcasts

SANS DFIR

* I Award You No Points, and May God have Mercy Upon your Soul: Feedback in CTI
* Applied Forecasting: Using Forecasting Techniques to Anticipate Cyber Threats
* La Evolución del Ransomware: Previsión de Escenarios Posibles para 2022
* Clip Addiction: A Threat Intelligence Approach to Video-Based Chinese InfoOps

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

* Live Hacking Q&A with Kody and Alex
* Zap Crypto Scammers with the Bee Movie
* Global coverage with OMG keymaps

The PC Security Channel [TPSC]

* Is Kaspersky safe to use?
* Hermetic Wiper: Ukraine Cyberattack Analysis

Eli the Computer Guy

* Trump's Truth Social FAILED - Even Trump doesn't use it
* ELON MUSK FIGHTS RUSSIA - Starlink used to attack Russian soldiers
* IT ARMY of UKRAINE - Twitter Supports Cyberwar Against Russia
* Buzzfeed NEWS Layoffs - Loses $10 MILLION a YEAR

Security Now

* Use After Free - OpenSSL Bug, Cybercrime Reporting Law, Node.js Supply Chain Compromise
* QWACs on? or QWACs off? - Patch Tuesday Recap, NVIDIA Hacked, EUFI Firmware Flaw, ProtonMail

Troy Hunt

* Weekly Update 288

Intel Techniques: The Privacy, Security, & OSINT Show

* 255-Dedicated VPN IP Addresses
* 254-OSINT+Fugitives=Rewards

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Razer Synapse 3.6.x DLL Hijacking
* Backdoor.Win32.Cafeini.b Hardcoded Credential
* Covid-19 Directory On Vaccination System 1.0 SQL Injection
* Covid-19 Directory On Vaccination System 1.0 SQL Injection
* PDF Generator Web Application 1.0 SQL Injection
* Royale Event Management System 1.0 Cross Site Scripting
* Royale Event Management System 1.0 Privilege Escalation
* Backdoor.Win32.Avstral.e Remote Command Execution
* WordPress Admin Word Count Column 2.2 Local File Inclusion
* Online Banking System 1.0 SQL Injection
* Backdoor.Win32.Chubo.c Cross Site Scripting
* Backdoor.Win32.Chubo.c Remote Command Execution
* Microfinance Management System 1.0 Cross Site Scripting
* PDF Generator Web App Using TCPDF 1.0 Local File Inclusion
* Backdoor.Win32.Cafeini.b Denial Of Service
* Pay Slip PDF Generator System 1.0 Shell Upload
* Pay Slip PDF Generator System 1.0 SQL Injection
* Backdoor.Win32.Cyn.20 Insecure Permissions
* ALLMediaServer 1.6 Remote Buffer Overflow
* FruityWifi Remote Code Execution
* One Church Management System 1.0 SQL Injection
* Microfinance Management System 1.0 SQL Injection
* One Church Management System 1.0 Cross Site Scripting
* RTLO Injection URI Spoofing
* Event Management System 1.0 Shell Upload

CXSecurity

* Trend Micro Virtual Mobile Infrastructure 6.0.1278 Denial Of Service
* Xlight FTP 3.9.3.2 Buffer Overflow
* Amazing CD Ripper 1.2 Buffer Overflow
* Moodle 3.11.5 SQL Injection
* Dirty Pipe Local Privilege Escalation
* Zabbix 5.0.17 Remote Code Execution
* Audio Conversion Wizard 2.01 Buffer Overflow

Proof of Concept (PoC) & Exploits

Exploit Database

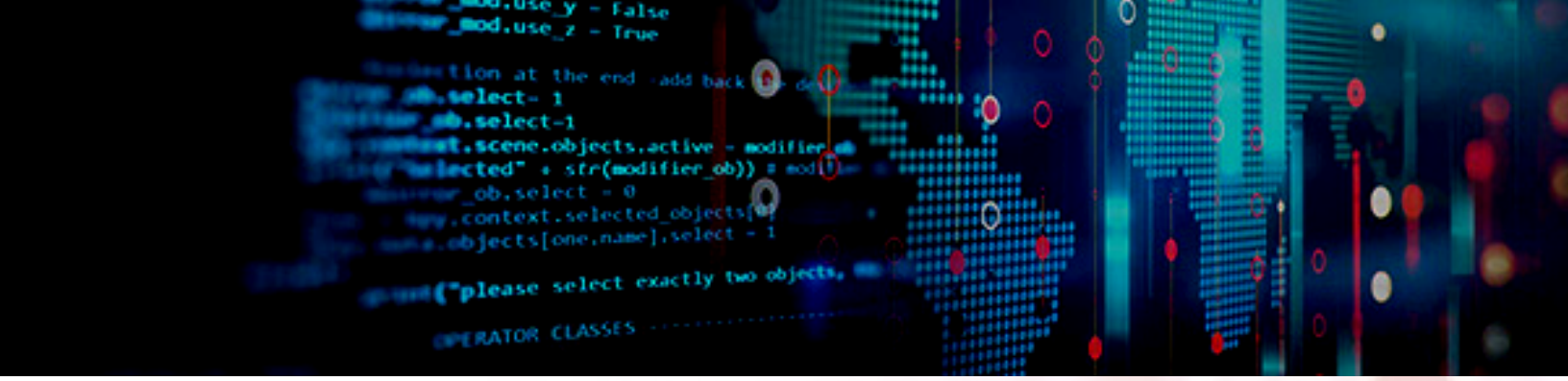
* [webapps] WordPress Plugin amministrazione-aperta 3.7.3 - Local File Read - Unauthenticated
* [local] ProtonVPN 1.26.0 - Unquoted Service Path
* [remote] ICT Protege GX/WX 2.08 - Client-Side SHA1 Password Hash Disclosure
* [remote] ICT Protege GX/WX 2.08 - Stored Cross-Site Scripting (XSS)
* [local] Sysax FTP Automation 6.9.0 - Privilege Escalation
* [remote] Ivanti Endpoint Manager 4.6 - Remote Code Execution (RCE)
* [remote] iRZ Mobile Router - CSRF to RCE
* [webapps] ICEHRM 31.0.0.0S - Cross-site Request Forgery (CSRF) to Account Takeover
* [webapps] Wordpress Plugin iQ Block Country 1.2.13 - Arbitrary File Deletion via Zip Slip (Authentica
* [remote] Apache APISIX 2.12.1 - Remote Code Execution (RCE)
* [webapps] Tiny File Manager 2.4.6 - Remote Code Execution (RCE)
* [webapps] Pluck CMS 4.7.16 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Moodle 3.11.5 - SQLi (Authenticated)
* [local] VIVE Runtime Service - 'ViveAgentService' Unquoted Service Path
* [webapps] Baixar GLPI Project 9.4.6 - SQLi
* [remote] Tdarr 2.00.15 - Command Injection
* [remote] Seowon SLR-120 Router - Remote Code Execution (Unauthenticated)
* [local] Sandboxie-Plus 5.50.2 - 'Service SbieSvc' Unquoted Service Path
* [local] WOW21 5.0.1.9 - 'Service WOW21_Service' Unquoted Service Path
* [local] Sony playmemories home - 'PMBDeviceInfoProvider' Unquoted Service Path
* [webapps] Zabbix 5.0.17 - Remote Code Execution (RCE) (Authenticated)
* [local] BattlEye 0.9 - 'BEService' Unquoted Service Path
* [local] McAfee(R) Safe Connect VPN - Unquoted Service Path Elevation Of Privilege
* [local] Wondershare Dr.Fone 12.0.18 - 'Wondershare InstallAssist' Unquoted Service Path
* [local] Printix Client 1.3.1106.0 - Privilege Escalation

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*

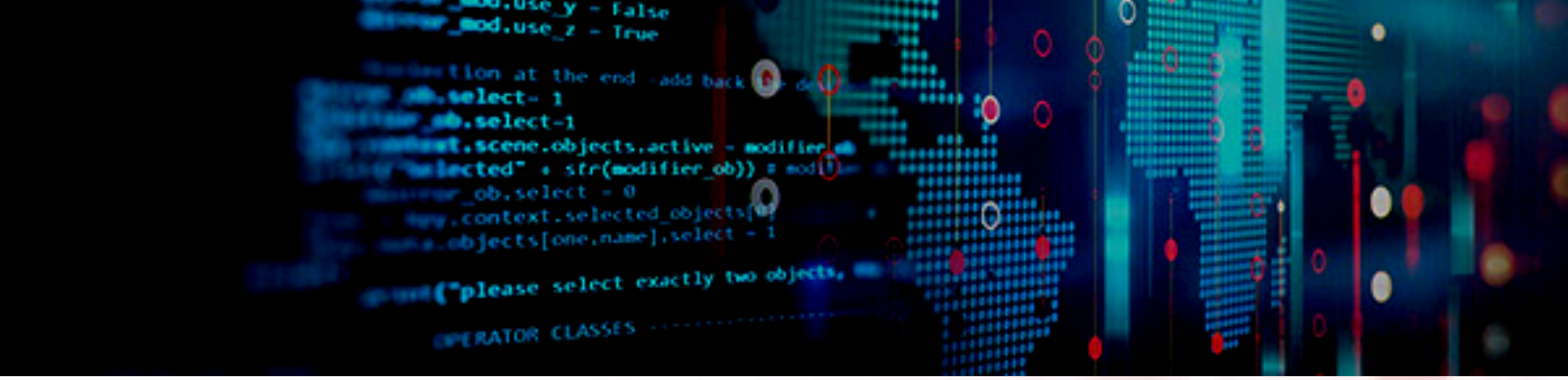
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://www.mofa.gov.ps/hack/
http://www.mofa.gov.ps/hack/ notified by Clash Hackers
http://www.environment.gov.ps/hack/
http://www.environment.gov.ps/hack/ notified by Clash Hackers
http://invest.telangana.gov.in/cl.html
http://invest.telangana.gov.in/cl.html notified by Clash Hackers
http://eod-prett.senescyt.gob.ec/cl.html
http://eod-prett.senescyt.gob.ec/cl.html notified by Clash Hackers
https://exames.emec.gov.pt/cl.html
https://exames.emec.gov.pt/cl.html notified by Clash Hackers
https://dra.gov.bt/?p=7
https://dra.gov.bt/?p=7 notified by Clash Hackers
http://dinkes.madina.go.id/cl.html
http://dinkes.madina.go.id/cl.html notified by Clash Hackers
http://sds.cbj.gov.bd/cl.html
http://sds.cbj.gov.bd/cl.html notified by Clash Hackers
http://pos.cbj.gov.bd/cl.html
http://pos.cbj.gov.bd/cl.html notified by Clash Hackers
http://www.townofgoldenmeadow-la.gov//wp-includes/cl.html
http://www.townofgoldenmeadow-la.gov//wp-includes/cl.html notified by Clash Hackers
http://investincolima.col.gob.mx/cl.html
http://investincolima.col.gob.mx/cl.html notified by Clash Hackers
http://sisat.mazamitla.gob.mx/cl.html
http://sisat.mazamitla.gob.mx/cl.html notified by Clash Hackers
http://bricks.cbj.gov.bd/cl.html
http://bricks.cbj.gov.bd/cl.html notified by Clash Hackers
http://firmacontrattitest.regione.marche.it/cl.html
http://firmacontrattitest.regione.marche.it/cl.html notified by Clash Hackers
http://plangranvision2040.col.gob.mx/cl.html
http://plangranvision2040.col.gob.mx/cl.html notified by Clash Hackers
http://simplemente.mazamitla.gob.mx/cl.html
http://simplemente.mazamitla.gob.mx/cl.html notified by Clash Hackers
http://cohesion.regione.marche.it/cl.html
http://cohesion.regione.marche.it/cl.html notified by Clash Hackers



Dark Web News

Darknet Live

Counterfeit Oxy Dealer Sentenced to Prison in Ohio

A man from Akron, Ohio, was sentenced to 62 months in prison for attempting to possess and distribute counterfeit oxycodone pills. Acting U.S. Attorney Michelle M. Baeppler announced that Thomas Anthony Walker, Jr., 36, of Akron, Ohio, will be spending 62 months in prison for attempted possession with intent to distribute fentanyl. Walker pleaded guilty to the charge in November 2021. The case is almost entirely unremarkable. The investigation into Walker resembled any other "drugs in the mail” topic covered by this site. However, court documents included a detailed look at what appears to be an atypical controlled delivery. Investigation _ Postal Inspector Marc Kudley, while working at the USPS Processing & Distribution Center in Akron, Ohio, identified a USPS Priority Mail Express package as "a suspect drug parcel based on several characteristics, including but not limited to the type of mail, origin, destination, and size.” The Postal Inspector described the package as "a brown USPS Ready Post Mailing Carton with "Seal It. Sent It.” tape over the top and bottom seams.” The package measured 15” X 12” X 10”, weighed about five pounds, and bore $111.40 in U.S. Postage. Inspector Kudley searched CLEAR for information about the person who had mailed the package and the intended recipient. The return address did not exist. The recipient's name, "T. Lewis,” was also fake. CLEAR reported that Walker, who had a previous conviction for heroin possession, lived at the address listed on the package.

CLEAR is an investigation tool from Thomson Reuters. On April 15, 2021, investigators placed the package in a line-up with "blank packages,” which emanated no narcotics odor. A so-called "narcotic detection canine” allegedly alerted on the suspicious package. On the same day, someone signed up for text message alerts regarding the package's delivery status from the USPS. CLEAR records identified Walker as the subscriber of the phone number provided to the USPS. On April 16, 2021, Inspector Kudley obtained a search warrant for the package. The execution of the search warrant resulted in: "the seizure of approximately 70 grams of round blue pills marked as "M” on one side and "30” on the other side, wrapped in clear cellophane in a clear zip-lock bag. The pills were concealed in a package of rolled up tee shirts. The markings on the pills correspond to Oxycodone Hydrochloride 30 milligram pills. Based on my experience with the seizure of pills of similar shape, color, and markings, I suspected the pills were intentionally disguised as Oxycodone Hydrochloride but contained fentanyl.” USPS records revealed that Walker had a USPS account associated with his phone number. "From April 17, 2021, through April 19, 2021, the USPS online account in WALKER's name was logged into by several Internet Protocol (IP) addresses associated with Charter Communications. Furthermore, according to USPS business records, the same IP addresses associated with Charter Communications that were used for logging into the USPS account were also used to track the delivery status of the Subject Parcel using USPS.com or the USPS smartphone application. In other words, the USPS online account in WALKER's name was used to track the delivery status of the Subject Parcel several times between April 17, 2021, and April 19, 2021. Based on the foregoing, I believe WALKER was the intended recipient of the Fentanyl pills mailed inside the Subject Parcel to 559 East Avenue in Akron, Ohio. The address of 559 East Avenue in Akron, Ohio was also listed as WALKER's

residence on his Ohio Driver's License.” Controlled Delivery _ On April 19, USPIS, Drug Enforcement Administration (DEA), Summit County Drug Unit (SCDU), and Akron Police Department (APD) conducted a controlled delivery of the package. Officers conducted surveillance at Walker's house while an undercover postal inspector acting as a USPS carrier delivered the package. The postal inspector left the package on the porch after receiving no response when knocking on the door. __ Walker's house. About 25 minutes later, "an African-American male wearing a white shirt and black pants opened the front door and kicked the Subject Parcel. The individual left the Subject Parcel on the front porch and went back inside the residence.” Roughly an hour later, "an individual wearing a purple or blue jacket, later identified as Walker, opened the front door and retrieved mail from the mailbox that was mounted on the porch next to the front door. Walker left the Subject Parcel on the porch and went back inside the residence.” Minutes after Walker returned to his house, a black Chevrolet SUV pulled into the driveway, obstructing the view of investigators. Police identified the vehicle as a Chevrolet Trax registered to Lakeyda Gardner. Gardner then pulled out of the driveway and left. Police saw an "unknown passenger” in the vehicle. The package was still sitting on the front porch of Walker's house. One minute after Gardner pulled out of the driveway, a Green Infinity sedan pulled up to the house. The passenger, identified only as "individual 2,” retrieved the package and placed it in the sedan. Individual 2 got back in the vehicle and the driver, "Individual 1,” pulled out. APD officers followed the vehicle for several minutes before pulling it over. They could not find the package inside the vehicle. Inspector Kudley eventually found the unopened box near an intersection between Walker's house and the APD traffic stop. Inspector Kudley questioned Individual 1. "Individual 1 said he was hanging out with Individual 2 when Individual 2 received a call from an unknown person. Individual 1 said the caller asked Individual 2 to retrieve a package. Individual 1 said Individual 2 asked for a ride to 559 East Avenue. Individual 1 said he drove Individual 2 to 559 East Avenue, where Individual 2 retrieved a package from the porch and placed it in the back of the Infinity sedan. Individual 1 said they drove away from the residence and identified the police were following them. Individual 1 said Individual 2 threw the package out of the passenger side window before being stopped by the police.” Police found Individual 2's phone on the floor of the car. The phone was on and "showed the contact for "Flaps(2)” with the phone number of 234-237-9484.” Investigators identified the number as Walker's phone number. The postal inspector questioned Individual 2. Individual 2 said Walker had called him and asked him to pick up a package from Walker's front porch. Walker told Individual 2 that he could not pick up the box because his girlfriend had picked him up. "Individual 2 stated he retrieved the Subject Parcel as a favor for WALKER and did not know what the box contained. Individual 2 stated he threw the Subject Parcel out of the Infinity window when he saw the police were following them. Individual 2 said he figured something was wrong with the box.” Walker called Individual 2. With police listening to the call, Individual 2 answered the call. He told Walker that he had picked up the package but threw it out the window when he saw police tailing the car. Walker stated, "If they was on you, they wouldn't have let you get away.” Individual 2 told Walker that he would try to find the package and then ended the call. After the call, the police released Individual 1 on the street where Individual 2 had ditched the package. Individual 2 then called Walker and told him that he had looked for the package but could not find it. Walker responded, "come on. You can't be serious. They would have never let you throw that box out of the car. They gonna pull you all over, man. So now you telling me the box is gone? That big ass box just disappeared?” Inspector Kudley wrote that he heard a turn signal in the background, indicating that Walker was driving around, searching for the package. Moments later, Walker asked Individual 2 why Individual 1 was walking down the road. "It was apparent that Individual 1 entered WALKER's vehicle. The conversation between WALKER and Individual 1 could be overheard through the cellular phone. WALKER asked Individual 1 what happened. Individual 1 stated, 'They caught us' and explained how they were stopped by the police, and the police recovered the box.” Police later located the Chevrolet Trax and arrested Walker. Unlike most defendants covered in articles on this site, Walker did not tell the police about every crime he had ever committed: "Walker stated he had no knowledge or ownership interest in the Subject Parcel. WALKER said he opened the front door at 559 East Avenue and saw the box sitting on the porch when he retrieved his mail. WALKER said he kicked the box since it did not belong to him. WALKER said he was later picked up by his

girlfriend "Keyda” Gardner in the black Chevrolet SUV. WALKER stated he went to eat at the Sonic in Massillon, Ohio and had nothing to do with the box delivered to his residence. The interview was terminated.” just… lol. archive.is/archive.org complaint: pdf CLEAR User Manual (for those interested): pdf (via darknetlive.com at https://darknetlive.com/post/counterfeit-oxy-dealer-sentenced-to-prison-in-ohio/)

Nevada Woman Tried to Hire a Hitman on the Darkweb

A Nevada woman admitted to paying a darkweb hitman site to murder her ex-husband. Kristy Lynn Felkins, 37, of Fallon, Nevada, pleaded guilty to one count of the use of interstate commerce facilities in the commission of murder-for-hire. Felkins admitted sending the administrator of Besa Mafia, a fraudulent murder-for-hire site, 12 Bitcoin to murder her ex-husband. Per the Stipulation to Factual Basis for Guilty Plea: Between approximately March 6, 2016, and March 9, 2016, Felkins sent Besa Mafia just over twelve Bitcoin, the value of which was roughly $5,000 at the time, for a hitman to kill her ex-husband and make it look like an accident. Felkins provided the home address of her ex-husband and other information, such as the time he left for work, vehicle information, and locations at which he could be located. After receiving Bitcoin from Felkins, a Besa Admin acknowledged receipt of the payment and told Felkins that a nearby hitman would be assigned to the job. Felkins has been described in the news as a "stay at home mom.” In the weeks following the payment to Besa Mafia, Felkins regularly communicated with the Besa Mafia administrator. In one communication, Felkins asked the Besa administrator if it was "possible to make it seem like it was a mugging gone wrong? Maybe they take his wallet? I understand if that means it might not happen on Monday am, but it may take an extra day or so to plan. If this isn't possible, I understand.” Felkins explained that she wanted her ex-husband to die so that she could have custody of their children. "I ran, and then he took my children away from me.” Huh. She also said that she was likely to receive her ex-husband's large life insurance payout, retirement, and house. Felkins told the Besa administrator that she did not care if the hitman harmed her ex-husband's girlfriend. Felkins told the site administrator that her ex-husband would be traveling to North Carolina. She asked if the hitman could kill him during his trip. Yura, the administrator of Besa Mafia, described a ludicrous plan: I don't think the sniper hitman will be able to get ready and go there so fast; however, if the current sniper won't be able to do it; he will follow them to the airport and will bribe someone to find out where he is going; eventually he will buy a last-minute flight with the same plane to the same location to stay with him. He will leave his gun in the car, though, as no guns can pass through the airport gate. He will fly towards the same location, and when landed, he will steal a car. He is good at it. He will steal a truck or some solid jeep and will run him over by a car, making it look like an accident. The Besa Mafia administrator repeatedly provided excuses for why the hitman had not yet murdered the Felkins' target. Felkins eventually caught on to the scam and stopped communicating with the fake hitman. Besa Mafia is one of the many murder-for-hire scams operated by a single fraudster. In 2019, an informant provided law enforcement with "scraped” messages from Besa Mafia's servers and the Bitcoin addresses associated with the site's customers: In or about January 2019, an individual not acting on behalf of the government (referred to herein as the "CS-1”) provided information to federal law enforcement agents pertaining to a murder-for-hire website that operated on the dark web (referred to herein as "WEBSITE-1”). Between August 2018 and October 2018, CS-1 used a program to scrape from WEBSITE-1 messages between the site's administrator ("ADMIN”) and its users. CS-1 was also able to identify the Bitcoin addresses associated with the payments made for acts of violence. In early 2019, CS-1 provided law enforcement with the contents of these scrapes of WEBSITE-1 and continues to provide information about WEBSITE-1. CS-1 provided this information to law enforcement without any promise of pecuniary gain or judicial consideration for any pending criminal case in the United States. Law enforcement has found the information provided by CS-1 to be reliable and has corroborated this information. Investigators identified a LocalBitcoins account as the source of the Bitcoin Felkins had sent to Besa Mafia. Felkins had created a LocalBitcoins account under the username "kl85coins.” The account name includes the letters "k” and "l,” which are the first and middle initials of Felkins' name. Felkins was born in March 1985. "Thus, the 'k' and' l' combined with '85' correspond to Felkins' personal identifiers,”

SA Mann wrote. The name listed on the LocalBitcoins account was "Kristy L Felkins.” Felkins is scheduled to be sentenced by U.S. District Judge Troy L. Nunley on June 16, 2022. Felkins faces a maximum statutory penalty of 10 years in prison. The Northern California Illicit Digital Economy Task Force is credited with the investigation that resulted in Felkins' conviction. archive.is/archive.org Criminal Complaint (pdf) Stipulation to Factual Basis for Guilty Plea (pdf) (via darknetlive.com at https://darknetlive.com/post/nevada-woman-tried-to-hire-a-hitman-on-the-darkweb/)

UK: Darkweb Drug Trafficker Sentenced to Prison

A member of a "global darkweb organized crime group” has been sentenced to nine years in prison for shipping kilograms of drugs to buyers around the globe. Mubinar Rahman, 26, mailed more than 104 packages of MDMA to global destinations as a part of an organized darkweb drug trafficking operation, according to the National Crime Agency (NCA). The defendant pleaded guilty at Newcastle Crown Court in October 2020 to trafficking drugs and possession of Class A drugs with intent to supply.

Mubinar Rahman is an "accountancy student” living in South Shields. Between June 29, 2020, and July 27, 2020, the NCA and Border Force intercepted 39 packages shipped by Rahman. Rahman had addressed the packages to buyers in the UK, United States, Israel, Norway, Thailand, Hong Kong, and elsewhere. The investigation resulted in seizures of 90 kilograms of MDMA, 134 kilograms of amphetamine, and more than 6,000 Valium and Xanax pills. In total, the value of the drugs shipped by Rahman was $1,036,025 (or 6,590,367 CNY/59,694,066 INR). The investigation involved cooperation with the United States Homeland Security Investigations (HSI). On 28 July 2020, NCA officers watched Rahman park his 2010 BMW outside a house associated with the drug trafficking operation. Officers arrested Rahman after he had returned to his car. During a search of the BMW, officers found ten packages addressed to international customers. A subsequent search of the house resulted in the discovery of 25 kilograms of MDMA, 134 kilograms of amphetamine sulfate, packaging equipment, and other materials often used by drug traffickers.

The court called Rahman the "warehouse and distribution hub manager.” Rahman refused to answer questions asked by NCA officers. However, according to the NCA, messages shared on EncroChat, the encrypted communications network hacked by law enforcement during Operation Venetic "helped officers identify other suspects involved in the darkweb drugs network.” Law enforcement arrested two additional suspects in April 2021 on suspicion of importing and supplying Class A, B, and C drugs. Investigators identified two more suspects who are allegedly on the run at the time of publication. NCA Branch Commander Martin Clarke: "Rahman was working for a well-established criminal network which exploited the fast parcel system to move illegal drugs. Working with key partners at home such as Border Force and abroad with HSI, we have removed a significant amount of Class A from circulation and denied Rahman's organized crime group the chance to plough profits from those drugs into more criminality. We are determined to do all we can to disrupt all drugs supply routes in and out of the UK.” Tim Hemker, attache at the US Homeland Security Investigations: "Homeland Security Investigations is proud of our strong partnership with the National Crime Agency. "Today's sentencing is the result of our agencies' exemplary collaboration to hold criminals on the dark web accountable for illegally selling and shipping narcotics overseas and putting countless individuals in danger. "We will continue to work together to keep drugs off our streets and our communities safe.” archive.is/archive.org If this guy is a part of a large-scale DTO that operated on markets with the kind of weight described in the article, I think somebody will know the vendor username. (via darknetlive.com at https://darknetlive.com/post/uk-darkweb-drug-trafficker-sentenced-to-prison/)

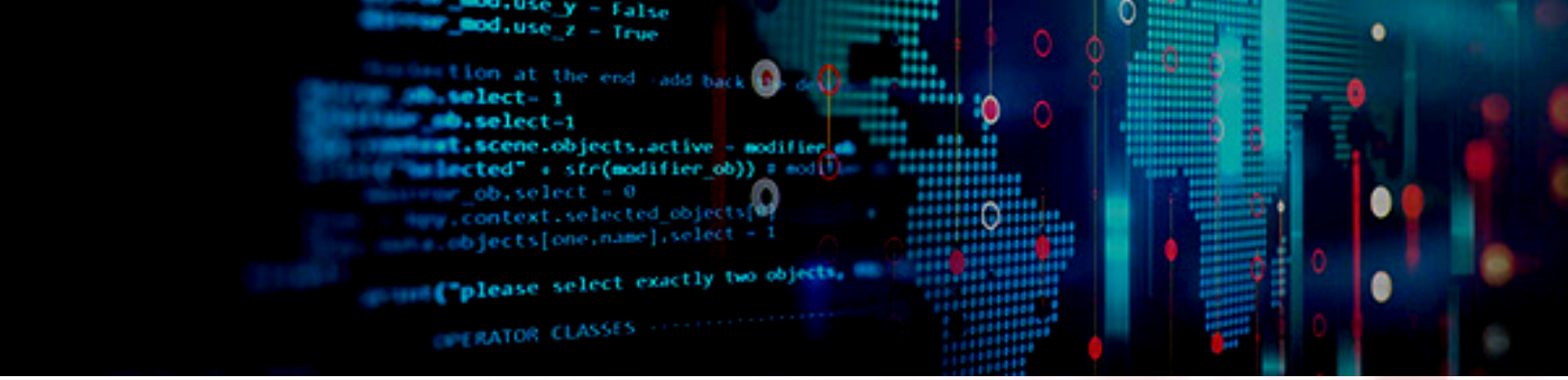
Three Arrested in Austria for Selling Ecstasy and Marijuana

Police in Braunau arrested three people for allegedly buying drugs on the darkweb and reselling them to local customers. Police in Braunau arrested a 29-year-old Romanian, a 40-year-old Croatian citizen, and a 35-year-old Hungarian citizen for selling drugs to people in Braunau. The suspects allegedly distributed "almost 1,000 ecstasy tablets, 700 grams of marijuana in the last six months.” Investigators believe that the 29-year-old has been ordering drugs from vendors on the darkweb since the summer of 2021. In two instances that the police are aware of, the suspect imported 1.5 kilograms of cocaine from a supplier in Germany. The 29-year-old, using a fake identity, worked as a waiter in Braunau. The suspects allegedly sold drugs to people

around a "trendy bar” in the area. polizei.gv.at: He is also accused of selling a large part of the drugs to mentally disabled, underage buyers and of having received sexual favors in return. Those allegations seem like quite the jackpot for a prosecutor. Are they saying that mentally disabled 15-year-olds, possibly at a bar, had sex with one or more defendants? Is there a concentration of underage drug buyers with mental disabilities in the area? Surely the crime would be the "sexual relations with a minor” part. Otherwise, wouldn't the customer be just as guilty of exchanging sex for drugs? What is the implication here? The State Criminal Police Office of Upper Austria, the police in Vöcklabruck, and the police in Steyr arrested the defendants after the trio had received a shipment of amphetamines. During the execution of search warrants, the police found drugs intended for sale. All three suspects made full confessions. Police are now investigating the trio's customers. archive.is/archive.org (via darknetlive.com at https://darknetlive.com/post/three-arrested-in-austria-for-selling-ecstasy-and-marijuana/)

Dark Web Link

Top Darknet Markets 2022: The Outstanding Performances To Consider Now
The darknet markets are subject to availability and one of the many factors that contributes to the working of these dark web markets is their performances. The top darknet markets 2022 is the example where each of the marketplaces in the Tor network has proven its performance over and over again. So, in this article [...] The post Top Darknet Markets 2022: The Outstanding Performances To Consider Now appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Breaking Bad Forum On The Darknet Is Revolutionary
The Breaking Bad Forum housed by the Tor network is a revolutionary darknet site indeed! So many forums exist on the dark web. But nothing could match the vibe of something like Breaking Bad. In this article, we will take you through the various aspects of the new forum. Breaking Bad Forum: A Gist Breaking [...] The post Breaking Bad Forum On The Darknet Is Revolutionary appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
White House Market Plans Retirement: What Important Things You Missed?
One of the latest darknet markets that accepted monero (XMR) as their payment modes have announced their retirement. The dark web market is none other than White House Market (WHM). As soon as the White House Market plans retirement and the news went live, there has been chaos all over the darknet sphere and there [...] The post White House Market Plans Retirement: What Important Things You Missed? appeared first on Dark Web Link | Deep web Onion Links | Darknet News.



Trend Micro Anti-Malware Blog

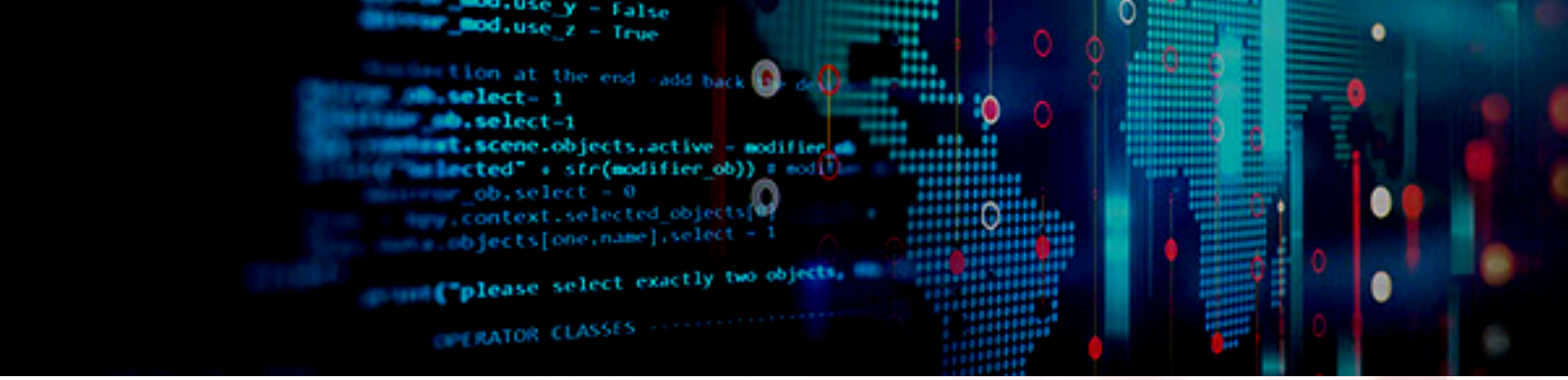
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

* RiskIQ Threat Intelligence Roundup: Campaigns Targeting Ukraine and Global Malware Infrastructure
* RiskIQ Threat Intelligence Supercharges Microsoft Threat Detection and Response
* RiskIQ Intelligence Roundup: Spoofed Sites and Surprising Infrastructure Connections
* RiskIQ Threat Intelligence Roundup: QBot, Magecart, Agent Tesla Headline Hijacked Infrastructure
* RiskIQ Threat Intelligence Roundup: C2 and Nation-State Threat Infrastructure
* Jupyter Notebooks Make RiskIQ Data a Digital 'Mech Suit' for Threat Intelligence Analysts
* "Offshore" Shinjiru Provides Bulletproof Services to Cyberattackers
* Retailers Using WooCommerce are at Risk of Magecart Attacks
* 5 Tips to Stay on the Offensive and Safeguard Your Attack Surface
* New E-Commerce Cybersecurity Guide Helps Brands be Proactive This Holiday Shopping Season

FireEye

* Rapid7 Announces Partner of the Year Awards 2022 Winners
* Analyzing the Attack Landscape: Rapid7's 2021 Vulnerability Intelligence Report
* Metasploit Weekly Wrap-Up
* The Digital Citizen's Guide to Navigating Cyber Conflict
* 4 Fallacies That Keep SMBs Vulnerable to Ransomware, Pt. 1
* Reflecting on Women's History Month at Rapid7
* SIEM and XDR: What's Converging, What's Not
* Rapid7 Recognized as Top Ranked in Current Offering Category in Forrester Waveâ„¢ for Cloud Workload
* 8 Tips for Securing Networks When Time Is Scarce
* Cloud Pentesting, Pt. 1: Breaking Down the Basics



Advisories

US-Cert Alerts & bulletins

* CISA Adds 32 Known Exploited Vulnerabilities to Catalog
* Google Releases Security Updates for Chrome
* CISA Adds 66 Known Exploited Vulnerabilities to Catalog
* State-Sponsored Russian Cyber Actors Targeted Energy Sector from 2011 to 2018
* VMware Releases Security Updates
* FBI and FinCEN Release Advisory on AvosLocker Ransomware
* Drupal Releases Security Updates
* CRI-O Security Update for Kubernetes
* AA22-083A: Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targe
* AA22-076A: Strengthening Cybersecurity of SATCOM Network Providers and Customers
* Vulnerability Summary for the Week of March 21, 2022
* Vulnerability Summary for the Week of March 14, 2022

Zero Day Initiative Advisories

ZDI-CAN-16709: BMC
A CVSS score 7.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Markus Wulftange (@mwulftange)' was reported to the affected vendor on: 2022-03-25, 3 days ago. The vendor is given until 2022-07-23 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-16779: Fuji Electric
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 'kimiya' was reported to the affected vendor on: 2022-03-25, 3 days ago. The vendor is given until 2022-07-23 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-16600: Fuji Electric
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 'kimiya' was reported to the affected vendor on: 2022-03-25, 3 days ago. The vendor is given until 2022-07-23 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-16781: Fuji Electric
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 'kimiya' was reported to the affected vendor on: 2022-03-25, 3 days ago. The vendor is given until 2022-07-23 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-16717: Fuji Electric
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 'kimiya' was reported to the affected vendor on: 2022-03-25, 3 days ago. The vendor is given until 2022-07-23 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-16733: 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 'DoHyun Lee(@l33d0hyun)' was reported to the affected vendor on: 2022-03-25, 3 days ago. The vendor is given until 2022-07-23 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-16976: 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 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-03-25, 3 days ago. The vendor is given until 2022-07-23 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-16867: 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 'DoHyun Lee(@l33d0hyun) of DNSLab, Korea University' was reported to the affected vendor on: 2022-03-25, 3 days ago. The vendor is given until 2022-07-23 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-16751: Advantech

A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by '@rgod777' was reported to the affected vendor on: 2022-03-23, 5 days ago. The vendor is given until 2022-07-21 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-16748: Advantech

A CVSS score 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by '@rgod777' was reported to the affected vendor on: 2022-03-23, 5 days ago. The vendor is given until 2022-07-21 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-16750: Advantech

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by '@rgod777' was reported to the affected vendor on: 2022-03-23, 5 days ago. The vendor is given until 2022-07-21 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-16746: Advantech

A CVSS score 4.9 (AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by '@rgod777' was reported to the affected vendor on: 2022-03-23, 5 days ago. The vendor is given until 2022-07-21 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-16773: Advantech

A CVSS score 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2022-03-23, 5 days ago. The vendor is given until 2022-07-21 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-16771: Advantech

A CVSS score 6.5 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2022-03-23, 5 days ago. The vendor is given until 2022-07-21 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-16775: Advantech

A CVSS score 6.5 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'rgod' was

reported to the affected vendor on: 2022-03-23, 5 days ago. The vendor is given until 2022-07-21 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-16744: Advantech

A CVSS score 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by '@rgod777' was reported to the affected vendor on: 2022-03-23, 5 days ago. The vendor is given until 2022-07-21 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-16752: Advantech

A CVSS score 8.8 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by '@rgod777' was reported to the affected vendor on: 2022-03-23, 5 days ago. The vendor is given until 2022-07-21 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-16731: Advantech

A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by '@rgod777' was reported to the affected vendor on: 2022-03-23, 5 days ago. The vendor is given until 2022-07-21 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-16745: Advantech

A CVSS score 4.9 (AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by '@rgod777' was reported to the affected vendor on: 2022-03-23, 5 days ago. The vendor is given until 2022-07-21 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-16772: Advantech

A CVSS score 6.5 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2022-03-23, 5 days ago. The vendor is given until 2022-07-21 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-16782: Advantech

A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2022-03-23, 5 days ago. The vendor is given until 2022-07-21 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-16776: Advantech

A CVSS score 8.2 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2022-03-23, 5 days ago. The vendor is given until 2022-07-21 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-16783: Advantech

A CVSS score 6.5 (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'rgod' was reported to the affected vendor on: 2022-03-23, 5 days ago. The vendor is given until 2022-07-21 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-16825: Foxit

A CVSS score 2.5 (AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-03-23, 5 days ago. The vendor is given until 2022-07-21 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Red Hat Security Advisory 2022-1082-01
Red Hat Security Advisory 2022-1082-01 - OpenSSL is a toolkit that implements the Secure Sockets Layer and Transport Layer Security protocols, as well as a full-strength general-purpose cryptography library.
Red Hat Security Advisory 2022-1073-01
Red Hat Security Advisory 2022-1073-01 - OpenSSL is a toolkit that implements the Secure Sockets Layer and Transport Layer Security protocols, as well as a full-strength general-purpose cryptography library.
Red Hat Security Advisory 2022-1078-01
Red Hat Security Advisory 2022-1078-01 - OpenSSL is a toolkit that implements the Secure Sockets Layer and Transport Layer Security protocols, as well as a full-strength general-purpose cryptography library.
Red Hat Security Advisory 2022-1075-01
Red Hat Security Advisory 2022-1075-01 - The httpd packages provide the Apache HTTP Server, a powerful, efficient, and extensible web server. Issues addressed include a HTTP request smuggling vulnerability.
Red Hat Security Advisory 2022-1068-01
Red Hat Security Advisory 2022-1068-01 - Expat is a C library for parsing XML documents. Issues addressed include code execution and integer overflow vulnerabilities.
Red Hat Security Advisory 2022-1025-01
Red Hat Security Advisory 2022-1025-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.10.6. Issues addressed include a bypass vulnerability.
Red Hat Security Advisory 2022-1071-01
Red Hat Security Advisory 2022-1071-01 - OpenSSL is a toolkit that implements the Secure Sockets Layer and Transport Layer Security protocols, as well as a full-strength general-purpose cryptography library.
Red Hat Security Advisory 2022-1076-01
Red Hat Security Advisory 2022-1076-01 - OpenSSL is a toolkit that implements the Secure Sockets Layer and Transport Layer Security protocols, as well as a full-strength general-purpose cryptography library.
Red Hat Security Advisory 2022-1069-01
Red Hat Security Advisory 2022-1069-01 - Expat is a C library for parsing XML documents. Issues addressed include code execution and integer overflow vulnerabilities.
Red Hat Security Advisory 2022-1077-01
Red Hat Security Advisory 2022-1077-01 - OpenSSL is a toolkit that implements the Secure Sockets Layer and Transport Layer Security protocols, as well as a full-strength general-purpose cryptography library.
Red Hat Security Advisory 2022-1066-01
Red Hat Security Advisory 2022-1066-01 - OpenSSL is a toolkit that implements the Secure Sockets Layer and Transport Layer Security protocols, as well as a full-strength general-purpose cryptography library.
Red Hat Security Advisory 2022-0577-01
Red Hat Security Advisory 2022-0577-01 - Windows Container Support for Red Hat OpenShift allows you to deploy Windows container workloads running on Windows Server containers.
Red Hat Security Advisory 2022-1080-01
Red Hat Security Advisory 2022-1080-01 - The httpd packages provide the Apache HTTP Server, a powerful, efficient, and extensible web server. Issues addressed include a HTTP request smuggling vulnerability.
Red Hat Security Advisory 2022-1065-01
Red Hat Security Advisory 2022-1065-01 - OpenSSL is a toolkit that implements the Secure Sockets Layer and Transport Layer Security protocols, as well as a full-strength general-purpose cryptography library.
Red Hat Security Advisory 2022-1074-01
Red Hat Security Advisory 2022-1074-01 - The screen utility allows users to have multiple logins on a single terminal.
Red Hat Security Advisory 2022-1081-01

Red Hat Security Advisory 2022-1081-01 - Gatekeeper Operator v0.2 Gatekeeper is an open source project that applies the OPA Constraint Framework to enforce policies on your Kubernetes clusters. This advisory contains the container images for Gatekeeper that include security updates, and container upgrades. Red Hat Product Security has rated this update as having a security impact of Moderate. A Common Vulnerability Scoring System base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link in the References section.

Red Hat Security Advisory 2022-1072-01

Red Hat Security Advisory 2022-1072-01 - The httpd packages provide the Apache HTTP Server, a powerful, efficient, and extensible web server. Issues addressed include a HTTP request smuggling vulnerability.

Ubuntu Security Notice USN-5349-1

Ubuntu Security Notice 5349-1 - It was discovered that GNU binutils gold incorrectly handled certain files. An attacker could possibly use this issue to cause a denial of service.

Ubuntu Security Notice USN-5348-1

Ubuntu Security Notice 5348-1 - David Gnedt and Thomas Konrad discovered that Smarty was incorrectly sanitizing the paths present in the templates. An attacker could possibly use this use to read arbitrary files when controlling the executed template. It was discovered that Smarty was incorrectly sanitizing the paths present in the templates. An attacker could possibly use this use to read arbitrary files when controlling the executed template.

Ubuntu Security Notice USN-5342-1

Ubuntu Security Notice 5342-1 - David Schwoerer discovered that Python incorrectly handled certain inputs. An attacker could possibly use this issue to expose sensitive information. This issue only affected Ubuntu 18.04 LTS. It was discovered that Python incorrectly handled certain FTP requests. An attacker could possibly use this issue to expose sensitive information. This issue only affected Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, and Ubuntu 18.04 LTS.

Red Hat Security Advisory 2022-1056-01

Red Hat Security Advisory 2022-1056-01 - Red Hat OpenShift Serverless Client kn 1.21.0 provides a CLI to interact with Red Hat OpenShift Serverless 1.21.0. The kn CLI is delivered as an RPM package for installation on RHEL platforms, and as binaries for non-Linux platforms.

Red Hat Security Advisory 2022-1051-01

Red Hat Security Advisory 2022-1051-01 - This version of the OpenShift Serverless Operator is supported on Red Hat OpenShift Container Platform versions 4.6, 4.7, 4.8, 4.9, and 4.10, includes security and bug fixes and enhancements. For more information, see the documentation listed in the References section.

Ubuntu Security Notice USN-5321-3

Ubuntu Security Notice 5321-3 - USN-5321-1 fixed vulnerabilities in Firefox. The update introduced several minor regressions. This update fixes the problem. Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, spoof the browser UI, bypass security restrictions, obtain sensitive information, or execute arbitrary code. A TOCTOU bug was discovered when verifying addon signatures during install. A local attacker could potentially exploit this to trick a user into installing an addon with an invalid signature.

Red Hat Security Advisory 2022-1045-01

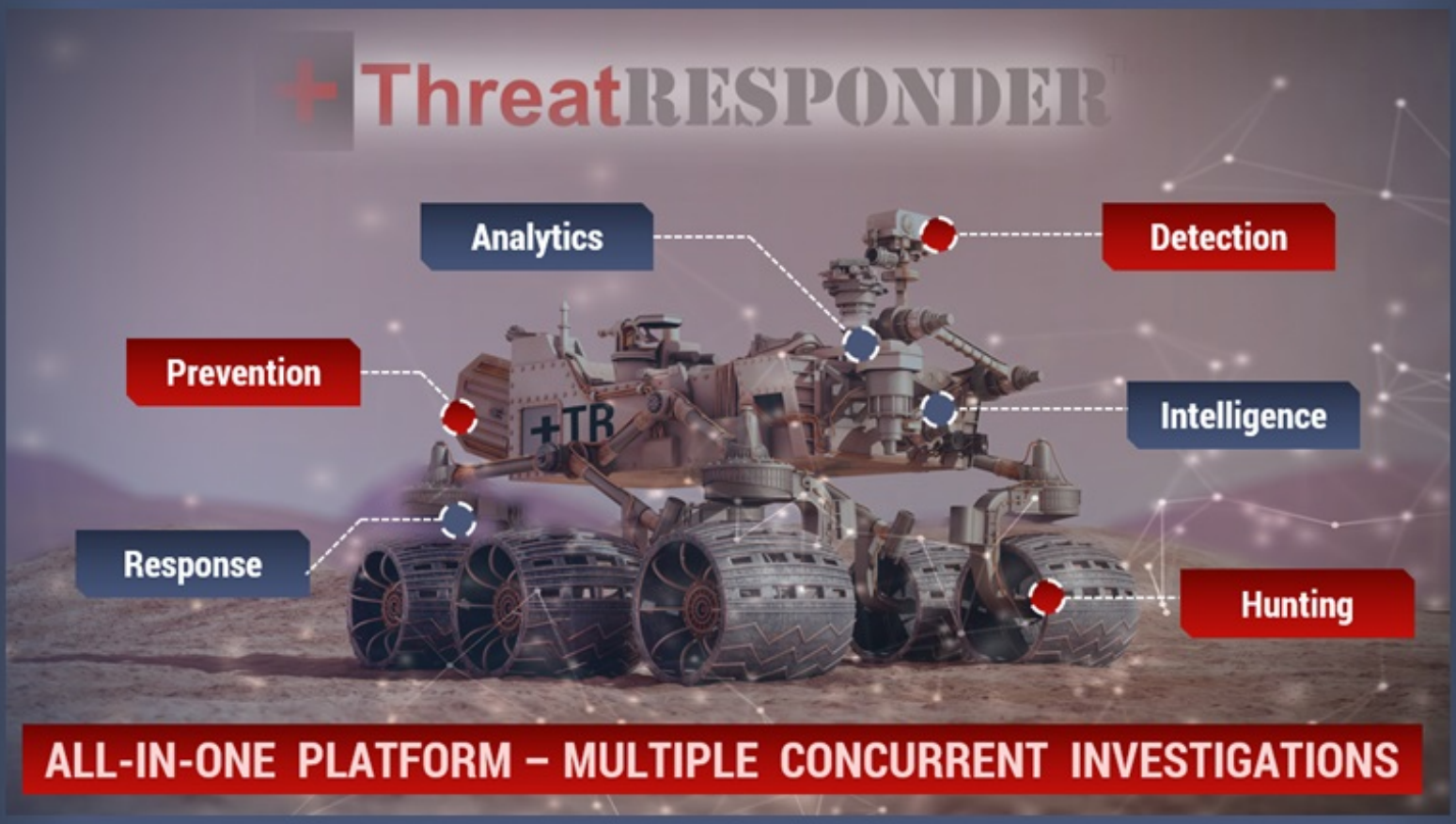
Red Hat Security Advisory 2022-1045-01 - The httpd packages provide the Apache HTTP Server, a powerful, efficient, and extensible web server. Issues addressed include a HTTP request smuggling vulnerability.

Are You...

- Spending several hours, days, or weeks conducting forensic investigations?
- Using different and unnecessary tools that pose correlation challenges?
- Wasting money on needless travels?
- Overworked, understaffed, and facing a backlog of cases?
- Uploading potentially sensitive files to VirusTotal or third-party sites?

Do DFIR Investigations Better

- Conduct DFIR investigations on any remote endpoint regardless of its geolocation – all on a single-pane of glass
- Perform in-depth forensics investigation dating back to the first day the target endpoint was installed
- Conduct full dynamic and static malware analyses with just a click of a mouse
- Conduct legally-defensible multiple DFIR cases simultaneously



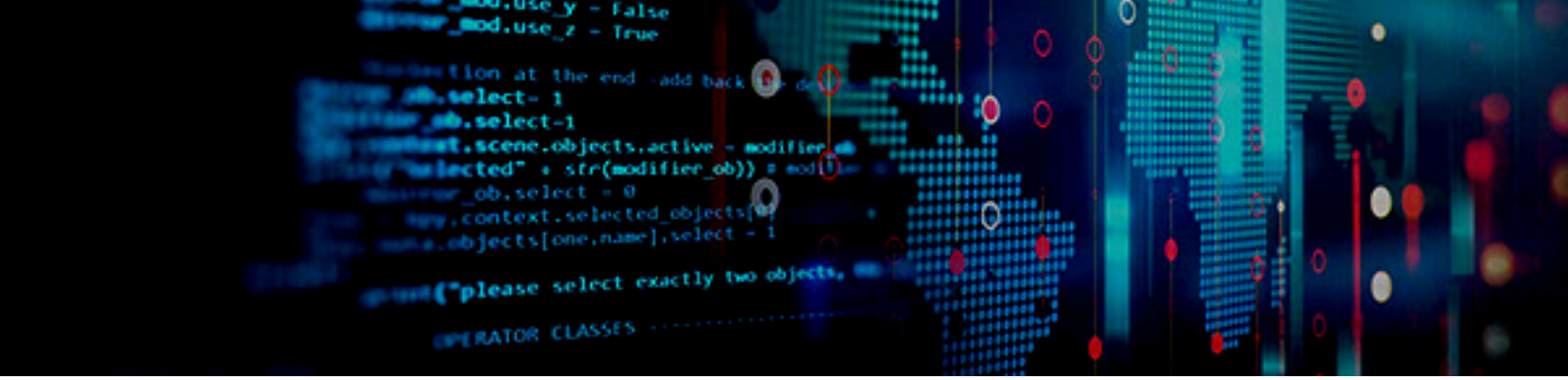
The Solution – ThreatResponder® Platform

ThreatResponder® Platform is an all-in-one cloud-native endpoint threat **detection**, **prevention**, **response**, **analytics**, **intelligence**, **investigation**, and **hunting** product

Get a Trial Copy

Mention **CODE: CIR-0119**

https://netsecurity.com

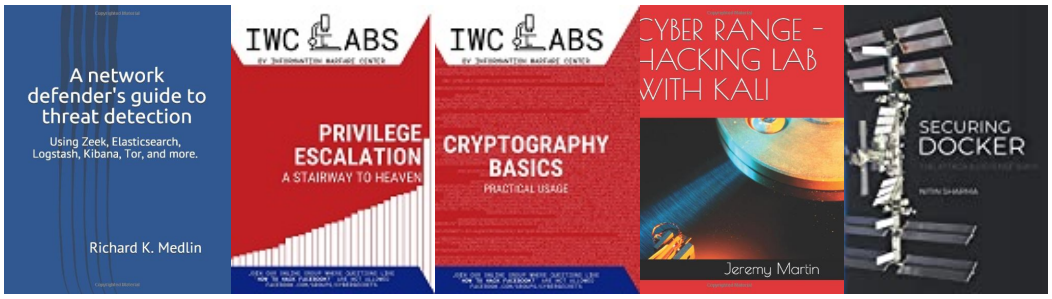


The Cyber Secrets publications on Amazon

The Cyber Weekl Awareness Report (WAR) is an Open Source Intelligence (AKA OSINT) resource centering around an array of subjects ranging from Exploits, Advanced Persistent Threat, National Infrastructure, Dark Web, Digital Forensics & Incident Response (DIFR), and the gambit of digital dangers.

Items that focus on cyber defense and DFIR usually spotlight capabilities in the CSI Linux environment. If interested in helping evolve, please let us know. The Cyber Secrets publications rotates between odd quarters issues focusing on Blue Team and the even issues on Red Team.

Other Publications from Information Warfare Center



CYBER WEEKLY AWARENESS REPORT

VISIT US AT **INFORMATIONWARFARECENTER.COM**

THE IWC ACADEMY
ACADEMY.INFORMATIONWARFARECENTER.COM

FACEBOOK GROUP
FACEBOOK.COM/GROUPS/CYBERSECRETS

CSI LINUX
CSILINUX.COM

CYBERSECURITY TV
CYBERSEC.TV

ARGOS
APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity

ThreatRESPONDER

Accredited Training Center
EC-Council

CYBERQ GROUP