Feb-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

February 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

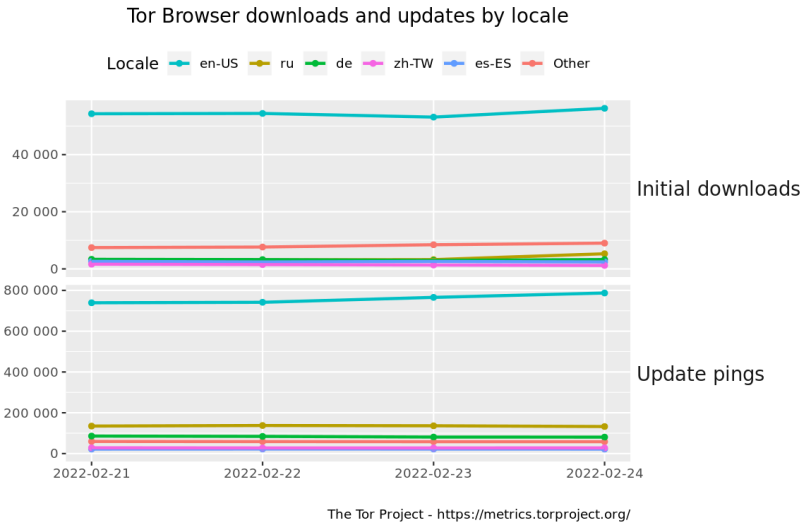
Internet Storm Center Infocon Status

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

* Would Banning Russia From Getting Software Updates Make It Easier To Hack?
* Ukraine Military Calls On Citizens With Hobby Drones To Help Kyiv
* Cyberwarfare Looms As Russia Invades, Shells Ukraine
* White House Denies Mulling Massive Cyberattacks Against Russia
* Russian Forces Are Inching Closer To Kyiv
* Russia Invades Ukraine
* SockDetour Backdoor Used In Attacks On Defense Contractors
* Chinese Company Doxes Apparent NSA Hacking Operation
* Crypto Currencies Fall After Russia Invades Ukraine
* UK Firms Most Likely To Pay Ransomware Hackers
* EU Rules Take Aim At Illegal Data Transfer To Non-EU Governments
* This Is The 'Hacking' Investigation Into Journalist Who Clicked 'View Source' On Government Website
* Malware Authors Target Rivals With Malicious npm Packages
* Samsung Shipped 100 Million Phones With Flawed Encryption
* Airtag Clones Can Sidestep Apple Anti-Stalker Tech
* Payment Card Skimming Reemerges With An Online Twist
* US Financial Industry Uniquely Susceptible To Supply Chain Threats
* Almost 100,000 New Mobiles Banking Trojans Discovered In 2021
* Britain Warns Of Cyber Attacks As Russia Ukraine Crisis Escalates
* Security Spend To Reach $1 Billion In Brazil In 2022
* US To Attack Cyber Criminals First, Ask Questions Later
* Linux Snap Package Tool Fixes Make-Me-Root Bugs
* Hacker Uses Phishing Attack To Steal $1.7 Million In NFTs From OpenSea Users
* WTF Is Our Most Critical Cybersecurity Resource? And How Can We Preserve It?
* Severe WordPress Plug-In UpdraftPlus Bug Threatens Backups

Krebs on Security

* Russia Sanctions May Spark Escalating Cyber Conflict
* IRS: Selfies Now Optional, Biometric Data to Be Deleted
* Report: Missouri Governor's Office Responsible for Teacher Data Leak
* Red Cross Hack Linked to Iranian Influence Operation?
* Wazawaka Goes Waka Waka
* Russian Govt. Continues Carding Shop Crackdown
* Microsoft Patch Tuesday, February 2022 Edition
* IRS To Ditch Biometric Requirement for Online Access
* How Phishers Are Slinking Their Links Into LinkedIn
* Fake Investor John Bernard Sinks Norwegian Green Shipping Dreams

Dark Reading

* 7 Steps to Take Right Now to Prepare for Cyberattacks by Russia
* Ukrainian Troops Targeted in Phishing Attacks by Suspected Belarusian APT
* Top 5 Interview Questions to Ask DevOps Candidates in 2022
* The Future of Cyber Insurance
* Putting the X Factor in XDR
* Fears Rise of Potential Russian Cyberattacks on US, Allies Over Sanctions
* Why Developers Should Care About Log4j
* Trickbot Comes Up With a New Set of Tricks
* Insider Threats Are More Than Just Malicious Employees
* 4 Simple Steps to a Modernized Threat Intelligence Approach
* Businesses Are at Significant Risk of Cybersecurity Breaches Due to Immature Security Hygiene and Pos
* Illusive Launches Identity Risk Management Platform
* JupiterOne Unveils Starbase for Graph-Based Security
* SaaS in the Enterprise: The Good, the Bad, and the Unknown
* New York Opens Joint Security Operations Center in NYC
* Darktrace Acquires Attack Surface Management Company Cybersprint
* Cloud Storage Leaks Grew by 150% in 2021, New CybelAngel Report Reveals
* What Does Least Privilege Access Mean for Cloud Security?
* Automakers Need to Lock Their Doors Against Ransomware
* Cloudflare to Acquire Area 1 Security to Expand Its Zero Trust Platform

The Hacker News

* Experts Create Apple AirTag Clone That Can Bypass Anti-Tracking Measures
* Iranian Hackers Using New Spying Malware That Abuses Telegram Messenger API
* Social Media Hijacking Malware Spreading Through Gaming Apps on Microsoft Store
* Russia-Ukraine War: Phishing, Malware and Hacker Groups Taking Sides
* New "SockDetour" Fileless, Socketless Backdoor Targets U.S. Defense Contractors
* Iran's MuddyWater Hacker Group Using New Malware in Worldwide Cyber Attacks
* Putin Warns Russian Critical Infrastructure to Brace for Potential Cyber Attacks
* Notorious TrickBot Malware Gang Shuts Down its Botnet Infrastructure
* New Flaws Discovered in Cisco's Network Operating System for Switches
* TrickBot Gang Likely Shifting Operations to Switch to New Malware
* From Pet Systems to Cattle Farm - What Happened to the Data Center?
* Warning - Deadbolt Ransomware Targeting ASUSTOR NAS Devices
* CISA Alerts on Actively Exploited Flaws in Zabbix Network Monitoring Platform
* U.S., U.K. Agencies Warn of New Russian Botnet Built from Hacked Firewall Devices
* New Wiper Malware Targeting Ukraine Amid Russia's Military Operation

Security Week

* NSO Sues Israeli Paper After Explosive Articles on Police
* Attacks From Within Seen as a Growing Threat to Elections
* Email Security and Brand Protection Firm Red Sift Raises $54 Million
* US, UK Warn of Iranian Cyberattacks on Government, Commercial Networks
* Ransomware Used as Decoy in Destructive Cyberattacks on Ukraine
* BlueVoyant Raises $250 Million to Boost Technical Capabilities, Global Expansion
* Cyber Attack Risks Poised to Soar as Russia Attacks Ukraine
* GE SCADA Product Vulnerabilities Show Importance of Secure Configurations
* Nigerian Admits in US Court to Hacking Payroll Company
* Cloudflare Plans to Acquire Email Security Startup Area 1
* 3 Steps Security Leaders Can Take Toward Closing the Skills Gap
* NSA Informs Cisco of Vulnerability Exposing Nexus Switches to DoS Attacks
* Deadbolt Ransomware Targeting Asustor NAS Devices
* Russia, Ukraine and the Danger of a Global Cyberwar
* New York Plans Cybersecurity Hub to Coordinate Responses
* Russia, Ukraine and the Danger of a Global Cyberwar
* Belden Sells Tripwire for $350M After Acquiring It for $710M
* anecdotes Raises $25 Million for Its Compliance OS Platform
* Destructive 'HermeticWiper' Malware Targets Computers in Ukraine
* New 'Cyclops Blink' Malware Linked to Russian State Hackers Targets Firewalls
* Salesforce Paid Out $12.2 Million in Bug Bounty Rewards to Date
* Cyberattacks Accompany Russian Military Assault on Ukraine
* Chinese Researchers Detail Linux Backdoor of NSA-Linked Equation Group
* Cyber Intelligence Firm Cyble Bags $10 Million in Series A Funding
* Astrix Security Nabs $15M to Tackle Attack Surface Sprawl

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* [EYES OPEN] The Kremlin Propaganda Machine Now Works Overtime. INFOGRAPHIC
* [Heads Up] The Ukraine War Started A New Wiper Malware Spillover Risk
* When the Phishers Want a Reply, not a Click
* CyberheistNews Vol 12 #08 [Eye Opener] Here Are the 4 Traits of Most Scams
* New Phishing Campaign Angles for Monzo Banking Customers
* 20 Year-Old "Right-to-Left Override" Functionality Used in Attacks to Trick Microsoft 365 Users Out o
* New QBot Attack Only Takes 30 Minutes to Elevate Privileges and Steal Data
* Phishing Campaign Targets NFT Speculators
* [Heads Up] There Is A Whole New Type of Blockchain Scam Called "Ice phishing"
* Conti Ransomware Attacks Reap in $180 Million in 2021 as Average Ransomware Payments Rise by 34%

ISC2.org Blog

* An Entry-Level Cybersecurity Certification: Why Every Employer Should Want Their Staff to Have One
* Igniting Adoption of a Secure Software Development Lifecycle - A Guide for Secure Software Champions
* Catching up with Kaleb Worku, 2020 KnowBe4 Black Americans in Cybersecurity Scholarship Recipient
* (ISC)² PULSE SURVEY: LOG4J REMEDIATION EXPOSES REAL-WORLD TOLL OF THE CYBERSECURITY WORKFORCE GA
* New Report by U.K. NCSC Highlights the Impact of Diversity on the Cybersecurity Workforce

HackRead

* Importance of soft skills in Technology
* Meet SockDetour fileless backdoor targeting U.S. Defense contractors
* Malware families using Pay-Per-Install service to expand targets
* 4 Benefits of Cloud VPN to your Business
* Hacking forum Raidforums.com allegedly seized by authorities
* Official website of Russian Parliament, MoD and Kremlin go offline
* DDoS Attack and Data Wiper Malware hit Computers in Ukraine

Koddos

* Importance of soft skills in Technology
* Meet SockDetour fileless backdoor targeting U.S. Defense contractors
* Malware families using Pay-Per-Install service to expand targets
* 4 Benefits of Cloud VPN to your Business
* Hacking forum Raidforums.com allegedly seized by authorities
* Official website of Russian Parliament, MoD and Kremlin go offline
* DDoS Attack and Data Wiper Malware hit Computers in Ukraine

Naked Security

* Did we learn nothing from Y2K? Why are some coders still stuck on two digit numbers?
* S3 Ep71: VMware escapes, PHP holes, WP plugin woes, and scary scams [Podcast + Transcript]
* Apple AirTag anti-stalking protection bypassed by researchers
* WordPress backup plugin maker Updraft says "You should update"…
* French speakers blasted by sextortion scams with no text or links
* Irony alert! PHP fixes security flaw in input validation code
* S3 Ep70: Bitcoin, billing blunders, and 0-day after 0-day after 0-day [Podcast + Transcript]
* VMware fixes holes that could allow virtual machine escapes
* Google announces zero-day in Chrome browser - update now!
* Adobe fixes zero-day exploit in e-commerce code: update now!

Threat Post

* TrickBot Takes a Break, Leaving Researchers Scratching Their Heads
* Microsoft Exchange Bugs Exploited by 'Cuba' Ransomware Gang
* 6 Cyber-Defense Steps to Take Now to Protect Your Company
* White House Denies Mulling Massive Cyberattacks Against Russia
* The Harsh Truths of Cybersecurity in 2022, Part II
* Zenly Social-Media App Bugs Allow Account Takeover
* Microsoft App Store Sizzling with New 'Electron Bot' Malware
* Web Filtering and Compliances for Wi-Fi Providers
* Cyberattackers Leverage DocuSign to Steal Microsoft Outlook Logins
* The Art of Non-boring Cybersec Training-Podcast

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

* Why SWIFT is the nuclear option of Russian financial sanctions
* GitLab 14.8 adds security approval policies, extends SSH support
* What is Apache Kafka? Scalable event streaming
* Use the cloud to strengthen your supply chain
* What's new in Rust 1.59
* Microsoft unveils C# 11 list patterns, raw string literals
* Implement authorization for Swagger in ASP.NET Core 6
* Understand the RSA encryption algorithm
* Go 1.18 adds much-anticipated generics
* Deno 1.19 extends web streams support

C4ISRNET - Media for the Intelligence Age Military

* Here's what stood out at the UAE's unmanned defense expo
* Pentagon wants to bolster domestic microelectronics base with new innovation network
* Navy remains mum on Project Overmatch details so China won't steal them
* US 'prepared to respond' to Russian cyberattacks, says Biden
* US space officials expect Russia, Ukraine conflict to extend into space
* Ukraine pelted with cyberattacks ahead of Russian assault
* Saab showcases new DeployNet 5G network
* Project Convergence reinforces the need for shared standards across the services
* US Space Force awards contract for deep-space radar
* US Army cyber conference seeks to bolster holistic national cybersecurity

The Hacker Corner

Conferences

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

Google Zero Day Project

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

Capture the Flag (CTF)

CTF Time has links to a lot of current Capture the Flag competitions and information on past events. Below is a list if CTFs they have on thier calendar.

* D^3CTF 2022
* FooBar CTF 2022
* DaVinciCTF 2022
* UTCTF 2022
* picoCTF 2022
* zer0pts CTF 2022
* VishwaCTF 2022
* VolgaCTF 2022 Qualifier
* T3N4CI0US CTF 2022
* Wicked 6: 2022 Women's Global Cyber League

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

* Packet Fence 11.2.0
* OpenSSH 8.9p1
* I2P 1.7.0
* OpenStego Free Steganography Solution 0.8.4
* TestSSL 3.0.7
* Collabfiltrator 2.1
* Wireshark Analyzer 3.6.2
* nfstream 6.4.2
* nfstream 6.4.1
* GNU Privacy Guard 2.2.34

Kali Linux Tutorials

* Log4J-Detect : Script To Detect The "Log4j" Java Library Vulnerability For A List Of URLs With Multit
* Rustpad : Multi-Threaded Padding Oracle Attacks Against Any Service
* SyntheticSun : A Defense-In-Depth Security Automation And Monitoring Framework
* Msmailprobe : Office 365 And Exchange Enumeration
* RPC Firewall : Stopping Lateral Movement via the RPC Firewall
* Lsarelayx : NTLM Relaying For Windows Made Easy
* RiotPot : Resilient IoT And Operational Technology Honeypot
* Skrull : A Malware DRM, That Prevents Automatic Sample Submission By AV/EDR
* PMAT-labs : Labs For Practical Malware Analysis And Triage
* ShonyDanza : A Customizable Tool For Researching, Pen Testing, And Defending With The Power Of Shodan

GBHackers Analysis

* Flaws With Horde Webmail Let Attackers Gain Full Access to the Email Account
* VMware Issues Patches for Shell Injection and Privilege Vulnerability
* Critical Magento 0-Day Let Attackers Execute Arbitrary Code
* ACTINIUM Hackers Group Targeting Government, Military, NGO to Steal Sensitive Data
* ESET Antivirus Flaw Let Attackers to Escalate Privileges & Execute Arbitrary Code

Weekly Cyber Security Video and Podcasts

SANS DFIR

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

Defcon Conference

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

Hak5

* ESP32-S2 Setup in Arduino | HakByte
* Live Hacking Q&A with Kody and Alex
* Hacking Stay-Logged-In Cookies with Owasp Zap | HakByte

The PC Security Channel [TPSC]

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

Eli the Computer Guy

* Amazon Lord of the Rings TV Show Selling Diversity
* Trump's Truth Social Network is a Scam - seems like a CIA honeypot
* Black Lives Matter is a Fraud
* Security System Installed - Cancel YouTube, Subscribe to Life

Security Now

* A BGP Routing Attack - UpdraftPlus, Xenomorph, Ukranian DDoS, The Bobiverse Trilogy
* InControl - PHP Everywhere, Magento Emergency, Project Zero Stats, Goodbye WMIC, SeriousSAM

Troy Hunt

* Weekly Update 284

Intel Techniques: The Privacy, Security, & OSINT Show

* 252-Secure Communications Conversion
* 251-Six Important Show Updates

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Microsoft Exchange Server Remote Code Execution
* Bank Management System 1.0 SQL Injection
* WordPress Photoswipe Masonry Gallery 1.2.14 Cross Site Scripting
* Technitium Installer 4.4 DLL Hijacking
* Dahua ToolBox 1.010.0000000.0 DLL Hijacking
* Simple Mobile Comparison Website 1.0 SQL Injection
* Wondershare MirrorGo 2.0.11.346 Insecure File Permissions
* Backdoor.Win32.FTP.Ics Remote Command Execution
* Microweber CMS 1.2.10 Local File Inclusion
* Backdoor.Win32.FTP.Ics Authentication Bypass / Code Execution
* WebHMI 4.1.1 Remote Code Execution
* WebHMI 4.1 Cross Site Scripting
* Backdoor.Win32.FTP.Ics Man-In-The-Middle
* aaPanel 6.8.21 Directory Traversal
* Adobe ColdFusion 11 Remote Code Execution
* Backdoor.Win32.Acropolis.10 Insecure Permissions
* ICL ScadaFlex II SCADA Controllers SC-1/SC-2 1.03.07 Remote File Modification
* Backdoor.Win32.Dsocks.10 Hardcoded Password
* Agirhnet 1.0 Cross Site Scripting
* Backdoor.Win32.Agent.baol Insecure Permissions
* WordPress 99robots Header Footer Code Manager 1.1.16 Cross Site Scripting
* Air Cargo Management System 1.0 SQL Injection
* Trojan.Win32.Cosmu.abix Insecure Permissions
* Chrome RenderFrameHostImpl Use-After-Free
* Cyclades Serial Console Server 3.3.0 Privilege Escalation

CXSecurity

* ICL ScadaFlex II SCADA Controllers SC-1/SC-2 1.03.07 Remote File Modification
* Servisnet Tessa MQTT Credentials Dump (Unauthenticated) (Metasploit)
* Hotel Druid 3.0.3 Remote Code Execution
* Tiny File Manager 2.4.3 Shell Upload
* Ignition Remote Code Execution
* Nagios XI Autodiscovery Shell Upload
* Grandstream GXV31XX settimezone Unauthenticated Command Execution

Proof of Concept (PoC) & Exploits

Exploit Database

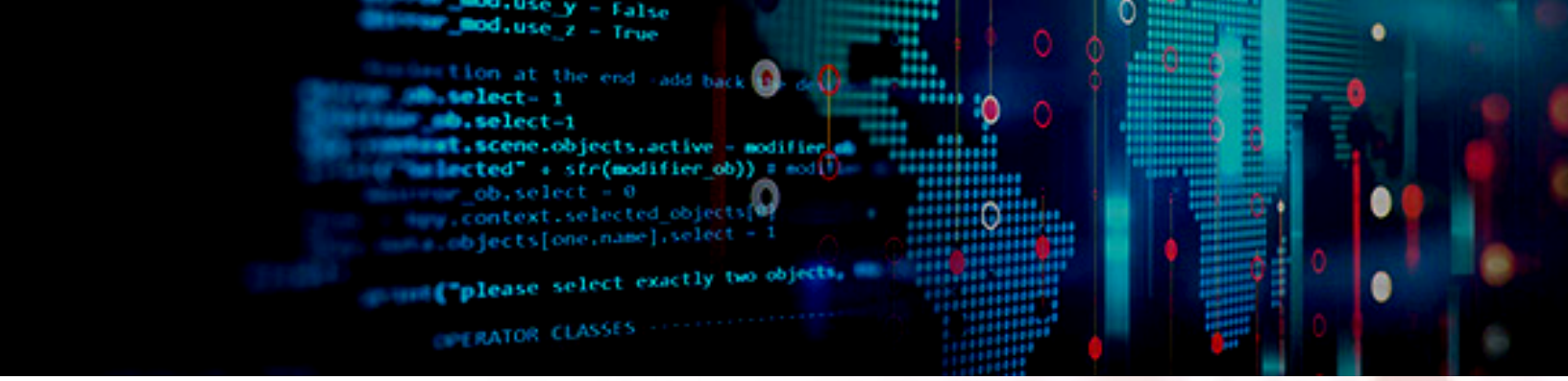
* [remote] WAGO 750-8212 PFC200 G2 2ETH RS - Privilege Escalation
* [webapps] Casdoor 1.13.0 - SQL Injection (Unauthenticated)
* [local] Cobian Backup Gravity 11.2.0.582 - 'CobianBackup11' Unquoted Service Path
* [local] Cobian Backup 11 Gravity 11.2.0.582 - 'Password' Denial of Service (PoC)
* [local] Cobian Reflector 0.9.93 RC1 - 'Password' Denial of Service (PoC)
* [webapps] Cipi Control Panel 3.1.15 - Stored Cross-Site Scripting (XSS) (Authenticated)
* [local] Wondershare MirrorGo 2.0.11.346 - Insecure File Permissions
* [webapps] Microweber CMS 1.2.10 - Local File Inclusion (Authenticated) (Metasploit)
* [webapps] WebHMI 4.1 - Stored Cross Site Scripting (XSS) (Authenticated)
* [webapps] WebHMI 4.1.1 - Remote Code Execution (RCE) (Authenticated)
* [remote] ICL ScadaFlex II SCADA Controllers SC-1/SC-2 1.03.07 - Remote File CRUD
* [webapps] Student Record System 1.0 - 'cid' SQLi (Authenticated)
* [remote] Adobe ColdFusion 11 - LDAP Java Object Deserialization Remode Code Execution (RCE)
* [webapps] aaPanel 6.8.21 - Directory Traversal (Authenticated)
* [webapps] Air Cargo Management System v1.0 - SQLi
* [webapps] Simple Real Estate Portal System 1.0 - 'id' SQLi
* [local] Microsoft Gaming Services 2.52.13001.0 - Unquoted Service Path
* [webapps] Dbltek GoIP - Local File Inclusion
* [webapps] FileCloud 21.2 - Cross-Site Request Forgery (CSRF)
* [local] Cyclades Serial Console Server 3.3.0 - Local Privilege Escalation
* [webapps] WordPress Plugin WP User Frontend 3.5.25 - SQLi (Authenticated)
* [webapps] Thinfinity VirtualUI 2.5.26.2 - Information Disclosure
* [webapps] Thinfinity VirtualUI 2.5.41.0 - IFRAME Injection
* [webapps] Cab Management System 1.0 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Microweber 1.2.11 - Remote Code Execution (RCE) (Authenticated)

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*

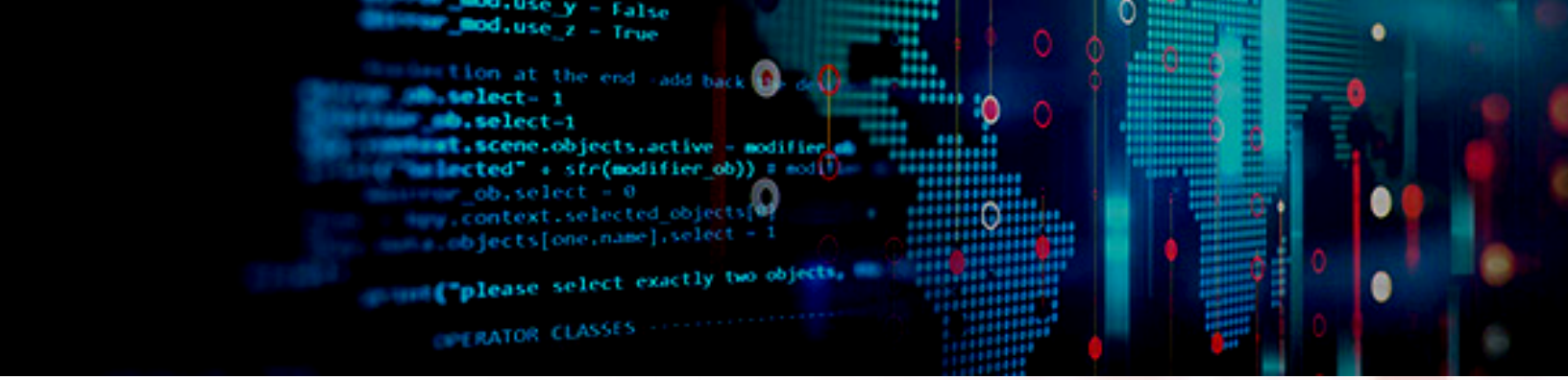
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://bkd.pacitankab.go.id/olala.htm
http://bkd.pacitankab.go.id/olala.htm notified by WE WILL BE BACK SOON WITH THE BIGGEST CYBER ATTACK OF ALL TIME
https://tachiapas.gob.mx/kurd.html
https://tachiapas.gob.mx/kurd.html notified by 0x1998
https://kedahlib.gov.my/kurd.htm
https://kedahlib.gov.my/kurd.htm notified by 0x1998
https://hcdloscocos.gob.ar/kurd.htm
https://hcdloscocos.gob.ar/kurd.htm notified by 0x1998
https://www.corfepalmira.gov.co/kurd.html
https://www.corfepalmira.gov.co/kurd.html notified by 0x1998
http://remigio.pb.leg.br/kurd.html
http://remigio.pb.leg.br/kurd.html notified by 0x1998
https://wra.go.ke/ft.php
https://wra.go.ke/ft.php notified by Black_X12
http://www.ldc.gov.zw/kurd.html
http://www.ldc.gov.zw/kurd.html notified by 0x1998
https://pn-tarakan.go.id
https://pn-tarakan.go.id notified by Mr.spongebob
http://perpus.pn-curup.go.id
http://perpus.pn-curup.go.id notified by Mr.spongebob
https://www.pn-curup.go.id
https://www.pn-curup.go.id notified by Mr.spongebob
http://buritibravo.ma.gov.br/xD.html
http://buritibravo.ma.gov.br/xD.html notified by v3n0m
http://saodomingosdomaranhao.ma.gov.br/xD.html
http://saodomingosdomaranhao.ma.gov.br/xD.html notified by v3n0m
https://kpr.okukab.go.id
https://kpr.okukab.go.id notified by WE WILL BE BACK SOON WITH THE BIGGEST CYBER ATTACK OF ALL TIME
https://disnakertrans.sukabumikab.go.id
https://disnakertrans.sukabumikab.go.id notified by Mr.spongebob
http://www.munivmt.gob.pe/gp.htm
http://www.munivmt.gob.pe/gp.htm notified by WE WILL BE BACK SOON WITH THE BIGGEST CYBER ATTACK OF ALL TIME
http://kejari-prabumulih.go.id



Dark Web News

Darknet Live

Heroin Vendor "CaliClaire" Sentenced to Five Years in Prison

A Maryland man who sold heroin on the darkweb under the name "CaliClaire” was sentenced to five years in federal prison. U.S. District Judge Catherine Blake sentenced Jason Green, of Salisbury, Maryland, to five years in prison. The custodial sentence will be followed by three years of supervised release. Green previously pleaded guilty to one count of possession with intent to distribute a controlled substance (heroin). Green admitted selling heroin through the darkweb under the name "CaliClaire.”

CaliClaire appeared to be a signigicant vendor. From an earlier article on Darknetlive.com about the CaliClaire case: "The investigation that resulted in Green's arrest involved, according to the Department of Justice's press release, traditional surveillance coupled with undercover purchases from Green's vendor accounts. In one example, an undercover investigator purchased one gram of heroin from CaliClaire's vendor site on Dream Market for approximately $200 in bitcoin in 2018. The next day, undercover law enforcement officers watched Green drive his BMW to a Post Office in Ocean City, Maryland. While at the Post Office, Green deposited several packages into a mailbox. After Green had left the Post Office, law enforcement officers retrieved the packages from the mailbox. One package bore the address provided to CaliClaire by the undercover law enforcement officer on Dream Market. After obtaining search warrants, investigators found that the packages contained 3.5 and 4.5 grams of heroin.” CaliClaire sold heroin to customers on Dream Market until the market shut down in 2019. After Dream Market had closed, investigators learned that CaliClaire had continued to sell heroin using encrypted email services and messaging applications. According to court documents, investigators learned this after seizing two packages of heroin and questioning the intended recipients about the source of the product. "In 2019, after Dream Market shut down, law enforcement seized two packages of heroin addressed to recipients in Fairfax County, Virginia, and Washington County, Oregon. Investigators contacted the recipients and learned that both individuals had purchased from CaliClaire on Dream Market. The recipients told investigators that CaliClaire had continued to sell heroin through at least two encrypted email services. On one email service, CaliClaire had retained the CaliClaire username. On the other service, the vendor had switched to 'clairebear2.'” "In late 2019, investigators started conducting undercover purchases from the vendor through his encrypted email accounts. After placing orders for two grams of heroin, undercover investigators would send the vendor $300 in Bitcoin. Later, undercover law enforcement officers would follow Green to Post Offices in Maryland and Delaware. Police would fish the packages out of the mailboxes after Green had left the premises. Investigators seemingly always found a package addressed to the address provided by the undercover LEO.” On October 16, 2019, police raided Green's home and a storage unit used by Green as a part of his drug trafficking operation. During the raids, police recovered 77 grams of heroin; 41 grams of cocaine; five grams of MDA, 33 grams of amphetamine; more than 1.4 kilograms of marijuana; 334 grams of cutting agents; and drug paraphernalia. During a forensic analysis of Green's electronic devices, investigators found evidence linking Green to one of the encrypted email services used by CaliClaire and a Bitcoin wallet. The wallet held 15.97 Bitcoin, which at the time of Green's arrest was worth approximately $130,000. A forensic analysis of the laptop revealed: searches

related to the addresses of customers; the names and addresses of 56 individuals who appeared in either the return or recipient addresses on packages seized by police, including undercover purchases; email addresses used by CaliClaire; a password to one of the email addresses used by CaliClaire; USPS tracking numbers, including for the undercover parcels and; and 44 PDF files containing USPS shipping labels from nearly every heroin package seized during the investigation. The announcement from the United States Attorney's Office states that there has been an increase in "the use of the internet to facilitate the illegal sale and distribution of narcotics and firearms.” They can increase the number of people arrested for buying and selling drugs on the darkweb at any given time since it is clear they can essentially identify and arrest anyone. Traditional investigative methods alone have proven successful in so many cases covered on this site. However, some of the tactics used by law enforcement in recent cases appear much more disruptive. One such example is the bulk analysis of mail pieces searching for patterns indicative of darkweb drug activity. We do not even know the tactics used that law enforcement officers obscured through parallel construction. As for the alleged increase in illegal firearm transactions, well, they will need to start arresting themselves. US Attorney for the District of Maryland Erek Barron announced the sentence The totally real Dark Market and Digital Currency Crimes (DMDCC) Task Force received credit for the successful investigation and conviction of CaliClaire. Guilty plea: pdf USAO Announcement: archive.org (via darknetlive.com at https://darknetlive.com/post/dream-vendor-caliclaire-sentenced-to-prison/)

"Dark0de Reborn" Exit Scammed

Dark0de Reborn exit scammed. According to DarkDotFail, Dark0de Reborn exit scammed. That is largely all there is to it as far as I know. It appears as if the market simply vanished. Which is fairly boring as far as exit scams go. It is worth noting that Dark0de Reborn had no relation to the original Dark0de forum which law enforcement seized in 2015. DarkDotFail speaks Users of the review section on the Darknetlive marketplace page for Dark0de claimed the market exit scammed last week.

Sorry for the delays in approving reviews. Someone on Twitter claimed that their marketplace password changed last week and they had used Dark0de's official link. It is obviously smart to write this kind of stuff on Twitter. If Dark0de had some massive OPSEC failure, I do not think it was public knowledge. So it might have been a general exit scam. It has been a long time since we have had a chaotic and fascinating exit scam such as the Nightmare Market exit scam wherein someone had hacked the market and was toying with users and staff. Someone recently pointed out to me that Dark0de seemed large due to their inflated presence on forums and websites with banner ads but actually had fewer transactions than some of the markets that do not have as much of a presence on the internet. Most markets fake the number of users and listings on their platform. One of the best metrics for comparing marketplace transaction volume is looking at the transaction counts of vendors with profiles on multiple marketplaces. This is a flawed method for obvious reasons but works for my purposes. The website dark0demarketlink[dot]com seemed like one of the many sites set up to either direct users to phishing links or profit off affiliate links. However, all the links on the site appear legitimate and the listed address for Dark0de (which was not a hyperlink) matched the official address. The site's hyperlink to darknetlive.com was apparently still alive in February 2022 but it is now offline. (archive.org) I have no idea if the site is connected to Dark0de at all. It resembles many fraudulent sites but appeared to provide only accurate information. In fairness, from what I have seen, market administrators running clearnet sites make more mistakes when operating unrelated projects from the same server. Or, even when running them from different servers but using the same parts of a stylesheet. Partially custom and partially copied from some random project on Github.

DDF Tweet (nitter): archive.is/onion I really have nothing here. What a boring exit scam. (via darknetlive.com at https://darknetlive.com/post/dark0de-reborn-exit-scammed/)

"SicknessVersion2" Defendant Sentenced to 11 Years in Prison

An Arizona man will be spending more than 11 years in prison for selling heroin on the darkweb under the username "SicknessVersion2.” U.S. District Judge Troy L. Nunley sentenced David Lee White, 52, of Chandler, Arizona, to 11 years and three months in prison. According to court documents, White, alongside two co-defendants, operated the vendor accounts "SicknessVersion2” and "23mightymouse23” on

Dream Market. White distributed heroin, cocaine, methamphetamine, marijuana, and other controlled substances to customers throughout the United States through the vendor accounts. Co-Defendants _ __ Feds identified White on USPS CCTV footage. White's co-defendants, Jason Arnold and Alicia Mccoy, have not been sentenced. Arnold pleaded guilty to count one in the indictment (conspiracy to distribute controlled substances). Since White named both of them in his plea agreement, they had very little room to avoid a conviction. McCoy has not yet entered a guilty plea. Arnold's girlfriend appears regularly in the criminal complaint but remains unindicted. I am leaving her name out of the article. Undercover Purchases _ His customers included federal agents. Federal Bureau of Investigation (FBI) Special Agent Daniel M. Bryant wrote that investigators conducted their first undercover purchase of heroin in May 2018. Between May 2018 and December 2018, federal agents purchased heroin from SicknessVersion2 on Dream Market on at least five occasions. The vendor mailed the packages of heroin to addresses controlled by the United States Postal Inspection Service (USPIS). After delivery of the package, investigators opened it and field-tested its contents. Special Agent Bryant wrote that the vendor had disguised the heroin within bags of Haribo gummy bears. The sender's name often referenced "sweets” or "treats.” __ Feds seized tons of customer records. I blurred the last names for some reason. USPS Records _ Using USPS records, case agents analyzed the United States Postal Service (USPS) tracking numbers on the packages. The feds could have based their entire case on the records associated with just one of the tracking numbers. For example, the tracking number 9405 5016 9932 0155 7645 77 belonged to a prepaid USPS Priority Mail shipping label purchased on May 15, 2018, by the USPS customer "jasoncka23.” On that date, the customer had purchased 100 prepaid USPS labels, including the one referenced above. USPS records identified the user "jasoncka23” as Jason Arnold. Arnold had registered the USPS account using his home address in Chandler, Arizona, and regularly accessed the Postal Service website using the IP address 98.165.31.245. Arnold had also provided USPS with an email address, business address, and phone number. __ More customer records. USPS records showed that Arnold had purchased approximately 1,100 labels using the same "jasoncka23” account between April 9, 2018, and November 2, 2018. About 1,000 packages had entered the mail system. The vendor had sent most of the packages to addresses in the United States. Still, people in France, Canada, New Zealand, Australia, and Bangladesh had received more than 100 packages. Many of the labels had the name of the sender listed as: "Sweets for my Sweet”; "Candy Store”; "Sweet Tooth”; "Sweet Designs”; "Nettles Sweet Emporium”; "Hays Sweetie”; "Haribos Sweets”; "Ware's Sweets Emporium”; and "D&A Sweet Emporium”; Arnold's purchases through his USPS account totaled more than $11,000. USPS Employees/Informants _ In the criminal complaint, Special Agent Bryant described how a regular employee of the Postal Service had regularly provided information about White to federal investigators. Specifically, an employee at the Post Office in Gilbert, Arizona, told investigators that an individual, later identified as White, had purchased $100 worth of Sleeping Bear Dunes Priority Express stamps on December 10, 2018. On the same day, another USPS employee collected mail from the Post Office's mail collection box and found approximately 10 Priority Express packages with the same Sleeping Bear Dunes stamps. The employee reported that the return addresses on every package were listed as "Chris' Candy” or "Chris's Candy's.” __ Even more customer records. I mean... I have never seen so many included in public court documents. Later that day, White returned to the same Post Office and purchased approximately $300 worth of Sleeping Bear Dunes Priority Express stamps. The USPS employee/informant watched White enter a vehicle. Although the employee managed to remember the vehicle's license plate number, their description of the car consisted of "a 2008 Dodge Charger.” This identification seems impressive since the differences between the different sixth-generation Chargers are so subtle. In 2009, Dodge moved the "Charger” emblem from the left side of the decklid to the right side. I am not sure there are any differences between the SE models in 2006, 2007, or 2008. "On or about December 26, 2018, a US Postal employee in Arizona advised case agents that a female customer attempted to purchase 12 Sleeping Bear Dunes Express mail stamps. The employee observed the woman exit a black Dodge Charger and enter the post office. Further, the employee stated that the woman left the post office then returned to the

same black Dodge Charger.” "According to the same employee, after the woman returned to [the Charger], a person matching the description of White exited the driver's side and dropped several items into a blue postal collection box just outside the front lobby door at the Post Office. Within minutes of this drop-off, a US Postal employee pulled the items from the postal collection box and saw several mailings which listed "Chris's Candy's” and "Sweet Tooth” as the sender with the same return address of [an address associated with White].” "In addition, the employee noted that affixed to each of the items were Sleeping Bear Dunes Express stamps. The employee described the female as very short. Maricopa county booking information for Alicia Mccoy listed her height as 5'0.” Further, after reviewing social media pictures of White's girlfriend, Alicia Mccoy, and Maricopa County booking photographs of Alicia Mccoy, the US Postal employee positively identified Alicia Mccoy as the female who purchased postage on or about December 26, 2018.” Feds conducted "open-source analysis” on Arnold's USPS account's email address and phone number. They found social media accounts linked to Arnold that had "references to […] words similar to SicknessVersion2, such as "sikness23”; "Big Sickness”; "sick”; and "2siclunade3.” Additionally, Arnold has the word "sick” tattooed on his neck. Coinbase _ Coinbase provided investigators with information associated with the defendants as well as Arnold's unindicted girlfriend. __ After feds arrested the defendants, they found some verbose notes as well as handwritten account passwords Some of the critical information provided by Coinbase included transaction history, usage patterns, and specific account labels. Arnold, for example, had added his Wells Fargo bank account to his Coinbase account. He had labeled the account "Wells Fargo - Sickness.” Coinbase - Arnold _ Between December 7, 2017, and July 9, 2018, Arnold's Coinbase account received approximately 20 Bitcoin and sold over 20 Bitcoin in exchange for $143,000. Arnold then transferred the money to his Wells Fargo account. Between March 30, 2018, and June 12, 2018, Arnold received at least six Bitcoin transfers from external addresses totaling approximately $9,200. On May 23, 2018, Arnold withdrew $3,187. ("This is around the same date of the first undercover purchase,” Special Agent Bryant wrote.) Coinbase closed Arnold's account on July 9, 2018. Coinbase - Arnold's Girlfriend _ Between July 14, 2018, and October 28, 2018, Arnold's girlfriend received and then sold 19 Bitcoin worth approximately $128,885. On July 25, 2018, she withdrew approximately $8,000 and $2,320 (around the same date as the second undercover purchase). On October 20, 2018, she withdrew approximately $2,636 and $3,551 (this is around the same date of the third undercover purchase, as described above). Coinbase closed the account on October 28, 2018, for suspicious activity. Coinbase - White _ From November 12, 2018, through December 26, 2018, White sold approximately 12.693 Bitcoin in exchange for $54,803. Coinbase also provided information about McCoy's account, but it is essentially a repeat of what I listed for White. Surveillance _ On December 28, 2018, agents conducted surveillance at the Chandler Andersen Springs Post Office. The 2008 Dodge Charger arrived at the post office; McCoy exited the vehicle and went inside. Agents followed her inside. McCoy purchased ten Priority Mail stamps and 20 Priority Mail Express stamps for $561. After buying the stamps, McCoy returned to the Charger and put on blue latex gloves. Agents watched McCoy place items in envelopes while inside the vehicle. After six minutes, McCoy circled the parking lot to the blue collection box drop-off. Police watched her place Express Mail envelopes into the collection box. She had not taken the gloves off, agents noted. A USPS employee pulled the packages out of the collection box after McCoy had left the Post Office. Several Express Mail packages had return names listed as "Sweet Tooth” and "Chris's Candy's.” Agents followed the Charger to The Aloha Motel in Chandler, Arizona. White and McCoy lived at the hotel in room 44. According to White's attorneys, "Arnold paid for a hotel and food, so White and McCoy could live. White never made a penny from his conduct.” The rest of the surveillance described in the criminal complaint is more of the same. In summary, the feds watched Arnold meet White and McCoy at the hotel. They watched White meet Arnold at Arnold's residence. They watched Arnold drive White to the Post Office in one of his many vehicles, including a 2010 Dodge Challenger and a 1957 Chevrolet Bel Air. The 2008 Charger functionally belonged to Arnold; his girlfriend's mother had registered the car. definitely a random encounter with police _ On December 26, 2018, officers with the Mesa Police Department pulled over a 1957 Chevrolet Bel Air. Officers claimed they were responding to a shots fired call near an apartment complex in Mesa, Arizona. According to court documents,

the police saw White in the Bel Air and thought he fit the description of the purported shooter. Police removed the driver, Arnold, and White, the passenger, from the car. During a pat-down, officers found $4,000 and a bag of heroin in White's front pocket. White told the officer that he had earned the cash with Arnold by flipping cars. Police also found $4,134 and a bag of heroin on Arnold. Mesa Police arrested both men. Between the December 26, 2018, arrest and their arrests on February 22, 2019, the Arizona court system released both White and Arnold. Arrests _ In February 2019, the feds arrested Arnold, White, and McCoy for conspiracy to distribute a controlled substance (methamphetamine and heroin) and distribution of a controlled substance (heroin). The indictment included one count of the conspiracy charge and four counts of the distribution charge. During the execution of search warrants, police found logins for vendor profiles and lists of customer names, addresses, and purchases. They also found at least 315 grams of heroin, 45 grams of cocaine, 593 grams of methamphetamine, and 30 grams of marijuana. __ The UFED 4 does not appear to be plugged into a device yet the laptop screen indicates otherwise? Full res UFED 4 available here. After being arrested, it seems as if Arnold attempted to blame McCoy for masterminding the operation. Discovery pages Arnold_002374-75: "Agents told McCoy that Arnold was saying she was the mastermind/computer person and that on her phone showed evidence of her involvement regarding another moniker/vendor, 23mightymouse23. McCoy said it was not their thing but Arnold's. Drugs would come from Arnold. Arnold sent a list of customers to McCoy. McCoy said they (McCoy/White presumably) were mules. There was not a typical payment amount McCoy received. Arnold did not have a partner, McCoy did not know all the details, McCoy was told what to do.” And Discovery page Arnold_02376: "Arnold showed McCoy how to do everything with the computers. White really did not do anything with the computers. McCoy did not see [Arnold's girlfriend] on the computers. As far as she knew, it was just herself and Arnold.” Arnold Talks _ After his arrest, Arnold provided the Department of Homeland Security with the usernames, passwords, and pins to the vendor accounts on Dream Market. He signed a form authorizing the federal government to use his profiles. Arnold interviewed with the government several times to receive a reduced sentence for his cooperation. After his first interview with the government, Arnold was unhappy with his proposed sentencing reduction.

__ Consent to assume online presence At a later debrief, Arnold tried to earn more time off his sentence by informing on someone else. He told the feds that McCoy and White had operated 23mightymouse23. This contradicted a previous claim where Arnold claimed that he managed the SicknessVersion2 and 23mightymouse23 vendor accounts. Not only did Arnold know the pin for 23mightymouse23, but the pin also matched his Arizona Department of Corrections identification number. McCoy stated that she did not know the pin to the 23mightymouse23 account. Arnold pleaded guilty to only one of the five counts in the indictment. White pleaded guilty to two. I suspect whatever he gave the feds proved at least somewhat helpful. And that is on top of the thousands of incriminated customers. As always, this case "was the product of an investigation by the Northern California Illicit Digital Economy (NCIDE) Task Force.” (which is very real and totally not an op.) archive.org, archive.is, onion complaint pdf, html indictment pdf, html (via darknetlive.com at https://darknetlive.com/post/dealer-sentenced-to-11-years-in-prison-in-sicknessversion2-case/)

Fent Vendor "XanaxKing2" Sentenced to 30 Years in Prison

A California man was sentenced to 360 months in prison after he was found guilty of distributing fentanyl analogues through the dark web. US District Judge Michael A. Shipp sentenced 30-year-old Andrew Tablack, of Beverly Hills, California, to 30 years in prison. A jury convicted Tablack of one count of manufacturing, supplying, and possessing with intent to manufacture and distribute cyclopropyl fentanyl pills and one count of conspiracy to Manufacture and Distribute Fentanyl pills. __ This picture, which is is frequently used in other fent-related articles, originally came from a DEA bust in this case IIRC. An investigation led by the Organized Crime Drug Enforcement Task Force (OCDETF) resulted in Tablack's arrest and subsequent imprisonment. The task force's investigation revealed that Tablack and his accomplice Stephan Durham, 43, masterminded a fentanyl pill production operation from California. According to court records, the duo produced and distributed fentanyl-laced pills from at least March 2017 through December 2017. The duo produced and distributed hundreds of thousands of fentanyl analogue pills throughout the

United States using a vendor account on a darkweb marketplace. Investigators identified Tablack as the vendor "XanaxKing2.” A 2017 investigation by the Drug Enforcement Administration (DEA) resulted in the seizure of approximately 300,000 pills containing cyclopropyl fentanyl at a residence in Monmouth County, New Jersey. During the investigation, the DEA found packages of cyclopropyl fentanyl pills at other homes in Monmouth County. Investigators later identified Tablack as the source of the drugs.

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

A press seized by the DEA. During the height of the "XanaxKing2” operation, Tablack distributed approximately 400,000 pills every month. In February 2022, Judge Shipp sentenced Tablack to 30 years in prison and three years of supervised release. The judge also ordered Tablack to forfeit the cryptocurrencies and electronic devices seized by law enforcement. Indictment pdf (via darknetlive.com at https://darknetlive.com/post/xanaxking2-sentenced-to-30-years-in-prison/)

Dark Web Link

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

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

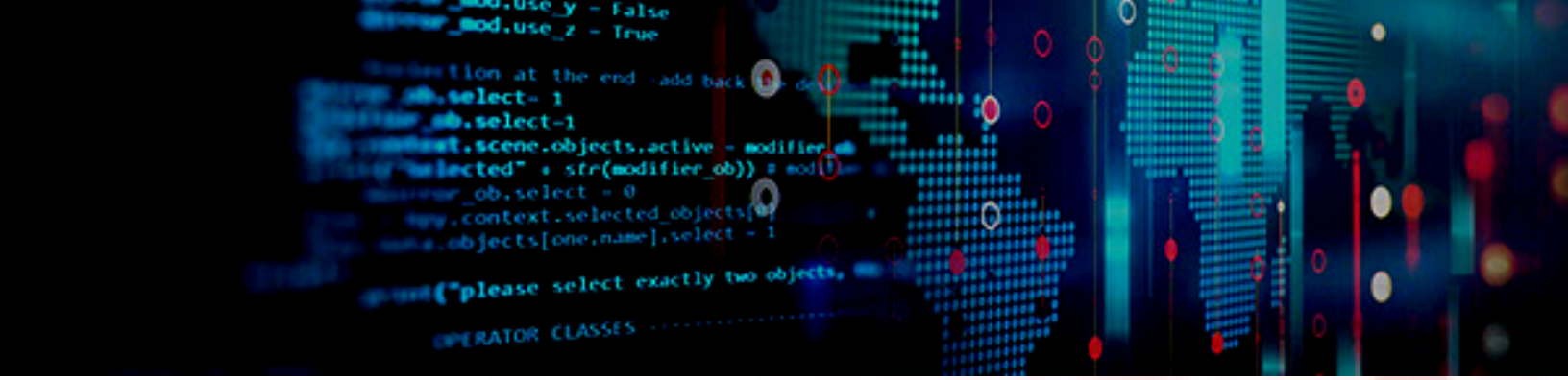
Faucibarriers Against 'Dark Web People' Distressing His Daughters And Wife With Vicious Threats

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

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

Two flaws in a technology used by whistleblowers and the media to securely communicate material have been

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



Trend Micro Anti-Malware Blog

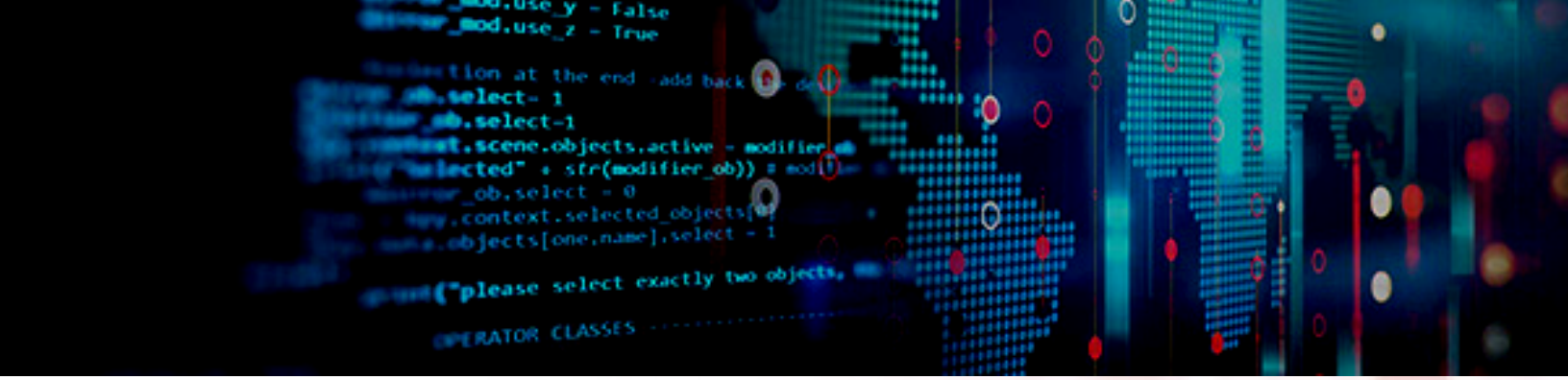
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

* RiskIQ 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
* New Aggah Campaign Hijacks Clipboards to Replace Cryptocurrency Addresses
* The Vagabon Kit Highlights 'Frankenstein' Trend in Phishing

FireEye

* Metasploit Weekly Wrap-Up
* Russia/Ukraine Conflict: What Is Rapid7 Doing to Protect My Organization?
* Staying Secure in a Global Cyber Conflict
* Demystifying XDR: How Curated Detections Filter Out the Noise
* For Health Insurance Companies, Web Apps Can Be an Open Wound
* This CISO Isn't Real, But His Problems Sure Are
* Metasploit Weekly Wrap-Up
* What's New in InsightVM and Nexpose: Q4 2021 in Review
* Log4Shell 2 Months Later: Security Strategies for the Internet's New Normal
* Cloud Security and Compliance: The Ultimate Frenemies of Financial Services



Advisories

US-Cert Alerts & bulletins

* CISA Releases Advisory on Destructive Malware Targeting Organizations in Ukraine
* CISA Adds Four Known Exploited Vulnerabilities to Catalog
* Mozilla Releases Security Update for Mozilla VPN
* Iranian Government-Sponsored MuddyWater Actors Conducting Malicious Cyber Operations
* Cisco Releases Security Updates for Multiple Products
* New Sandworm Malware Cyclops Blink Replaces VPNFilter
* CISA Adds Two Known Exploited Vulnerabilities to Catalog
* CISA Insights: Foreign Influence Operations Targeting Critical Infrastructure
* AA22-057A: Destructive Malware Targeting Organizations in Ukraine
* AA22-055A : Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government an
* Vulnerability Summary for the Week of February 14, 2022
* Vulnerability Summary for the Week of February 7, 2022

Zero Day Initiative Advisories

ZDI-CAN-16708: Adobe
A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-02-25, 3 days ago. The vendor is given until 2022-06-25 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-16549: 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 'Andrea Micalizzi aka rgod (@rgod777)' was reported to the affected vendor on: 2022-02-25, 3 days ago. The vendor is given until 2022-06-25 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-16550: 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 'Andrea Micalizzi aka rgod (@rgod777)' was reported to the affected vendor on: 2022-02-25, 3 days ago. The vendor is given until 2022-06-25 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-16547: 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 'Andrea Micalizzi aka rgod (@rgod777)' was reported to the affected vendor on: 2022-02-25, 3 days ago. The vendor is given until 2022-06-25 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-16546: 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 'Andrea

Micalizzi aka rgod (@rgod777)' was reported to the affected vendor on: 2022-02-25, 3 days ago. The vendor is given until 2022-06-25 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-16707: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-02-25, 3 days ago. The vendor is given until 2022-06-25 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-16548: 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 'Andrea Micalizzi aka rgod (@rgod777)' was reported to the affected vendor on: 2022-02-25, 3 days ago. The vendor is given until 2022-06-25 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-16528: 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 'Andrea Micalizzi aka rgod (@rgod777)' was reported to the affected vendor on: 2022-02-25, 3 days ago. The vendor is given until 2022-06-25 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-16158: Apple

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 'actae0n of Blacksun Hackers Club' was reported to the affected vendor on: 2022-02-25, 3 days ago. The vendor is given until 2022-06-25 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-16552: 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 'Andrea Micalizzi aka rgod (@rgod777)' was reported to the affected vendor on: 2022-02-25, 3 days ago. The vendor is given until 2022-06-25 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-16698: Microsoft

A CVSS score 6.1 (AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-02-25, 3 days ago. The vendor is given until 2022-06-25 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-16316: Trend Micro

A CVSS score 7.3 (AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Xavier Danest - Decathlon' was reported to the affected vendor on: 2022-02-25, 3 days ago. The vendor is given until 2022-06-25 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-16722: FreeBSD

A CVSS score 8.2 (AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-02-25, 3 days ago. The vendor is given until 2022-06-25 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-16531: 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 'Andrea Micalizzi aka rgod (@rgod777)' was reported to the affected vendor on: 2022-02-25, 3 days ago. The vendor is given until 2022-06-25 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-16696: Microsoft

A CVSS score 6.1 (AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-02-25, 3 days ago. The vendor is given until 2022-06-25 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-16723: FreeBSD

A CVSS score 8.2 (AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-02-25, 3 days ago. The vendor is given until 2022-06-25 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-16697: Microsoft

A CVSS score 6.1 (AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H) severity vulnerability discovered by 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-02-25, 3 days ago. The vendor is given until 2022-06-25 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-16530: 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 'Andrea Micalizzi aka rgod (@rgod777)' was reported to the affected vendor on: 2022-02-25, 3 days ago. The vendor is given until 2022-06-25 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-16545: 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 'Andrea Micalizzi aka rgod (@rgod777)' was reported to the affected vendor on: 2022-02-25, 3 days ago. The vendor is given until 2022-06-25 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-16703: Oracle

A CVSS score 6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-02-23, 5 days ago. The vendor is given until 2022-06-23 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-16621: Bentley

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-02-23, 5 days ago. The vendor is given until 2022-06-23 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-16409: Oracle

A CVSS score 6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L) severity vulnerability discovered by 'lc' was reported to the affected vendor on: 2022-02-23, 5 days ago. The vendor is given until 2022-06-23 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-16635: Bentley

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-02-23, 5 days ago. The vendor is given until 2022-06-23 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-16704: Oracle

A CVSS score 6.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L) severity vulnerability discovered by 'Lucas Leong (@_wmliang_) of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-02-23, 5 days ago. The vendor is given until 2022-06-23 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Red Hat Security Advisory 2022-0672-01
Red Hat Security Advisory 2022-0672-01 - Ruby is an extensible, interpreted, object-oriented, scripting language. It has features to process text files and to perform system management tasks. Issues addressed include a code execution vulnerability.
Red Hat Security Advisory 2022-0665-01
Red Hat Security Advisory 2022-0665-01 - The python-pillow packages contain a Python image processing library that provides extensive file format support, an efficient internal representation, and powerful image-processing capabilities. Issues addressed include a buffer over-read vulnerability.
Red Hat Security Advisory 2022-0669-01
Red Hat Security Advisory 2022-0669-01 - The python-pillow packages contain a Python image processing library that provides extensive file format support, an efficient internal representation, and powerful image-processing capabilities. Issues addressed include a buffer over-read vulnerability.
Red Hat Security Advisory 2022-0666-01
Red Hat Security Advisory 2022-0666-01 - The cyrus-sasl packages contain the Cyrus implementation of Simple Authentication and Security Layer. SASL is a method for adding authentication support to connection-based protocols.
Red Hat Security Advisory 2022-0555-01
Red Hat Security Advisory 2022-0555-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. Issues addressed include a cross site request forgery vulnerability.
Red Hat Security Advisory 2022-0668-01
Red Hat Security Advisory 2022-0668-01 - The cyrus-sasl packages contain the Cyrus implementation of Simple Authentication and Security Layer. SASL is a method for adding authentication support to connection-based protocols.
Red Hat Security Advisory 2022-0667-01
Red Hat Security Advisory 2022-0667-01 - The python-pillow packages contain a Python image processing library that provides extensive file format support, an efficient internal representation, and powerful image-processing capabilities. Issues addressed include a buffer over-read vulnerability.
Ubuntu Security Notice USN-5292-4
Ubuntu Security Notice 5292-4 - USN-5292-1 fixed a vulnerability in snapd. Unfortunately that update introduced a regression that could break the fish shell. This update fixes the problem. James Troup discovered that snap did not properly manage the permissions for the snap directories. A local attacker could possibly use this issue to expose sensitive information. Ian Johnson discovered that snapd did not properly validate content interfaces and layout paths. A local attacker could possibly use this issue to inject arbitrary AppArmor policy rules, resulting in a bypass of intended access restrictions. The Qualys Research Team discovered that snapd did not properly validate the location of the snap-confine binary. A local attacker could possibly use this issue to execute other arbitrary binaries and escalate privileges. The Qualys Research Team discovered that a race condition existed in the snapd snap-confine binary when preparing a private mount namespace for a snap. A local attacker could possibly use this issue to escalate privileges and execute arbitrary code.
Red Hat Security Advisory 2022-0663-01
Red Hat Security Advisory 2022-0663-01 - Samba is an open-source implementation of the Server Message Block protocol and the related Common Internet File System protocol, which allow PC-compatible machines to share files, printers, and various information. Issues addressed include a code execution vulnerability.
Red Hat Security Advisory 2022-0664-01
Red Hat Security Advisory 2022-0664-01 - Samba is an open-source implementation of the Server Message Block protocol and the related Common Internet File System protocol, which allow PC-compatible machines to share files, printers, and various information. Issues addressed include a code execution vulnerability.
Red Hat Security Advisory 2022-0561-01

Red Hat Security Advisory 2022-0561-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the container images for Red Hat OpenShift Container Platform 4.9.22.

Red Hat Security Advisory 2022-0557-01

Red Hat Security Advisory 2022-0557-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments.

Red Hat Security Advisory 2022-0658-01

Red Hat Security Advisory 2022-0658-01 - The cyrus-sasl packages contain the Cyrus implementation of Simple Authentication and Security Layer. SASL is a method for adding authentication support to connection-based protocols.

Red Hat Security Advisory 2022-0661-01

Red Hat Security Advisory 2022-0661-01 - This release of Red Hat Fuse 7.10.1 serves as a replacement for Red Hat Fuse 7.10, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include code execution, deserialization, and remote SQL injection vulnerabilities.

VMware Security Advisory 2022-0006

VMware Security Advisory 2022-0006 - VMware Workspace ONE Boxer update addresses a persistent cross site scripting vulnerability.

Ubuntu Security Notice USN-5300-1

Ubuntu Security Notice 5300-1 - It was discovered that PHP incorrectly handled certain scripts. An attacker could possibly use this issue to cause a denial of service. It was discovered that PHP incorrectly handled certain inputs. An attacker could possibly use this issue to cause a denial of service, or possibly obtain sensitive information. It was discovered that PHP incorrectly handled certain scripts with XML parsing functions. An attacker could possibly use this issue to obtain sensitive information.

Red Hat Security Advisory 2022-0609-01

Red Hat Security Advisory 2022-0609-01 - The python-pillow packages contain a Python image processing library that provides extensive file format support, an efficient internal representation, and powerful image-processing capabilities. Issues addressed include a buffer over-read vulnerability.

Red Hat Security Advisory 2022-0620-01

Red Hat Security Advisory 2022-0620-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include double free, out of bounds write, privilege escalation, and use-after-free vulnerabilities.

Ubuntu Security Notice USN-5302-1

Ubuntu Security Notice 5302-1 - Yiqi Sun and Kevin Wang discovered that the cgroups implementation in the Linux kernel did not properly restrict access to the cgroups v1 release_agent feature. A local attacker could use this to gain administrative privileges. Brendan Dolan-Gavitt discovered that the Marvell WiFi-Ex USB device driver in the Linux kernel did not properly handle some error conditions. A physically proximate attacker could use this to cause a denial of service.

Ubuntu Security Notice USN-5301-2

Ubuntu Security Notice 5301-2 - USN-5301-1 fixed a vulnerability in Cyrus. This update provides the corresponding update for Ubuntu 14.04 ESM and Ubuntu 16.04 ESM. It was discovered that the Cyrus SASL SQL plugin incorrectly handled SQL input. A remote attacker could use this issue to execute arbitrary SQL commands.

Ubuntu Security Notice USN-5301-1

Ubuntu Security Notice 5301-1 - It was discovered that the Cyrus SASL SQL plugin incorrectly handled SQL input. A remote attacker could use this issue to execute arbitrary SQL commands.

Red Hat Security Advisory 2022-0621-01

Red Hat Security Advisory 2022-0621-01 - OpenLDAP is an open-source suite of Lightweight Directory Access Protocol applications and development tools. LDAP is a set of protocols used to access and maintain

distributed directory information services over an IP network.

Red Hat Security Advisory 2022-0622-01

Red Hat Security Advisory 2022-0622-01 - The kernel-rt packages provide the Real Time Linux Kernel, which enables fine-tuning for systems with extremely high determinism requirements. Issues addressed include double free, out of bounds write, privilege escalation, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-0629-01

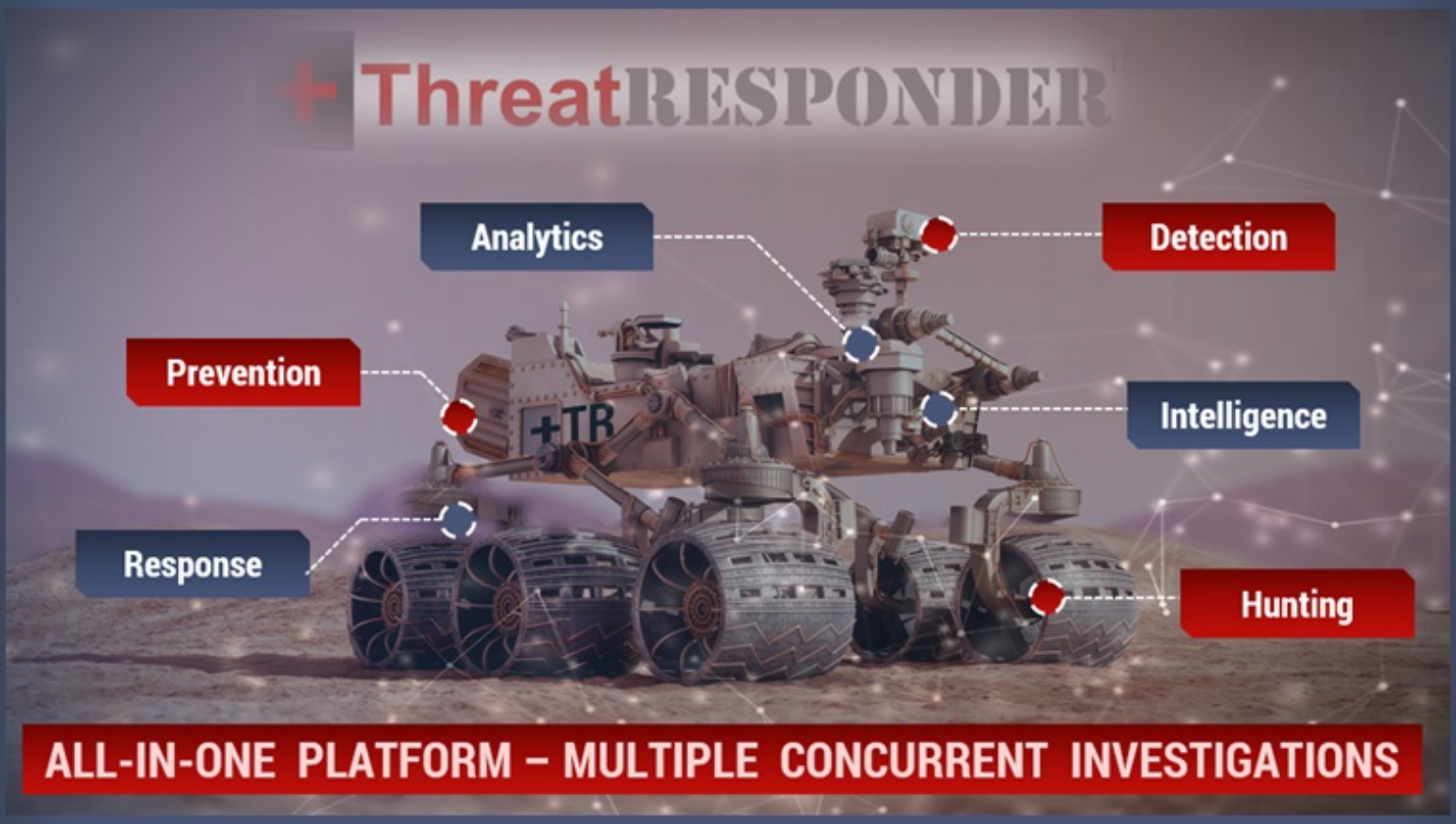
Red Hat Security Advisory 2022-0629-01 - The kernel-rt packages provide the Real Time Linux Kernel, which enables fine-tuning for systems with extremely high determinism requirements. Issues addressed include privilege escalation and use-after-free vulnerabilities.

Are You...

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

Do DFIR Investigations Better

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



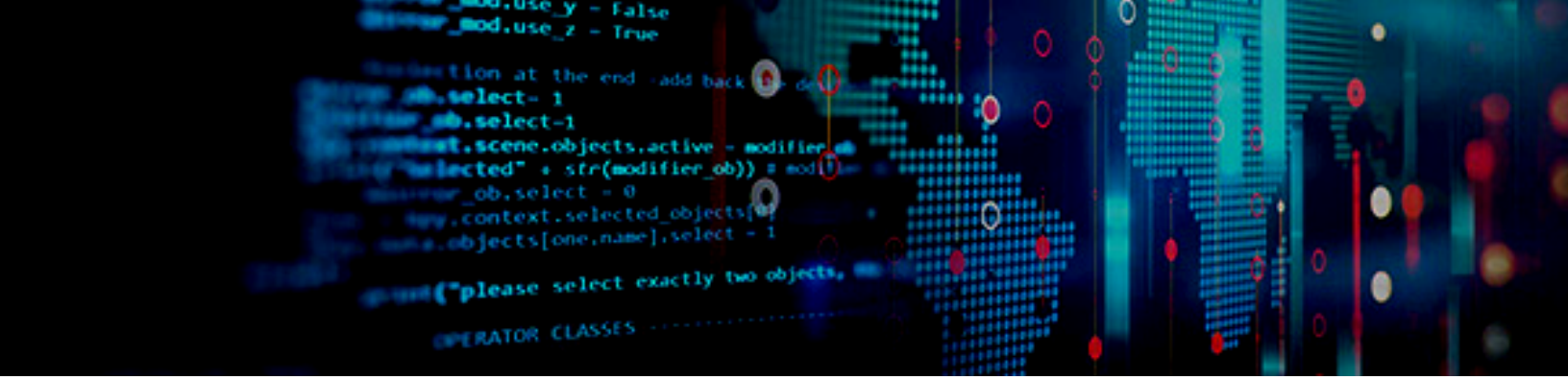
The Solution – ThreatResponder® Platform

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

Get a Trial Copy

Mention **CODE: CIR-0119**

https://netsecurity.com

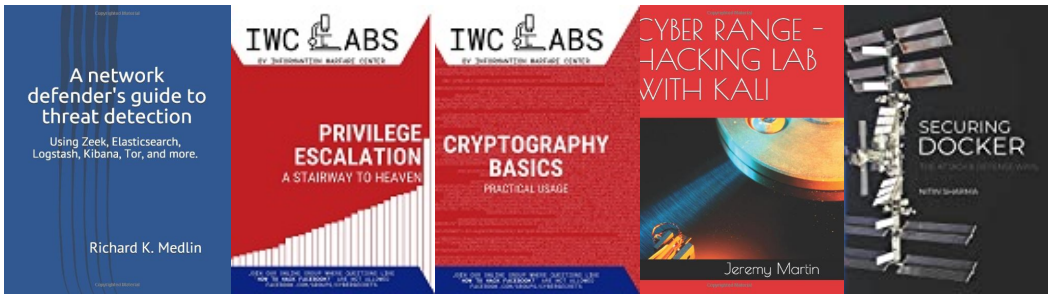


The Cyber Secrets publications on Amazon

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

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

Other Publications from Information Warfare Center



CYBER WEEKLY AWARENESS REPORT

VISIT US AT **INFORMATIONWARFARECENTER.COM**

THE IWC ACADEMY
ACADEMY.INFORMATIONWARFARECENTER.COM

FACEBOOK GROUP
FACEBOOK.COM/GROUPS/CYBERSECRETS

CSI LINUX
CSILINUX.COM

CYBERSECURITY TV
CYBERSEC.TV

ARGOS
APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity

ThreatRESPONDER

Accredited Training Center
EC-Council

CYBERQ GROUP