Jan-17-22

CYBER WEEKLY AWARENESS REPORT

JOIN OUR ONLINE GROUP WHERE QUESTIONS LIKE "**HOW TO HACK FACEBOOK?**" ARE NOT ALLOWED
FACEBOOK.COM/GROUPS/CYBERSECRETS

ARGOS
APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity

January 17, 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

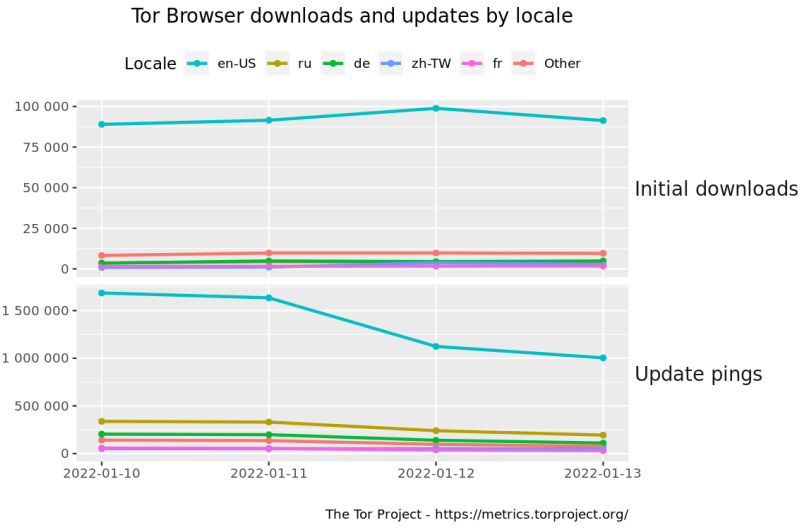
Internet Storm Center Infocon Status

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

* Ukrainian Government Websites Face Attack
* North Korean Hackers Impersonate Crypto Firm To Scam Startups
* BioPlus Faces Class-Action Lawsuit Over Security Measures
* Three Plugins With Same Bug Put 84k WordPress Sites At Risk
* REvil Ransomware Gang Arrested In Russia
* Amazon Fixes Security Flaw In AWS Glue Service
* Dark Web Carding Platform UniCC Shuts Up Shop After Making Millions
* New GootLoader Campaign Targets Accounting, Law Firms
* Adobe Cloud Abused To Steal Office 365, Gmail Credentials
* Ransomware Locks Down Prison, Knocks Systems Offline
* Dozens Of Teslas Hacked Using A Flaw In Third Party App
* Kim Kardashian Sued In Crypto Pump And Dump Case
* Pis Detect Malware By Scanning For Electromagnetic Waves
* FIFA Ultimate Team Account Takeovers Plague EA Gamers
* Moxie Marlinspike Leaves Encrypted Messaging App Signal
* Microsoft Starts 2022 With Big Bundle Fixes For 96 Security Bugs In Its Software
* Costa Rica Hydro Plant Gets New Lease On Life From Crypto Mining
* EU Data Watchdog To Europol: You've Helped Yourself To Too Much Data
* macOS Bug Could Bypass Controls And Access Private User Data
* SysJoker Backdoor Malware Targets Windows, Linux, And macOS
* Millions Of Routers Exposed To RCE By USB Kernel Bug
* Critical SonicWall NAC Vulnerability Stems From Apache Mods
* Developer Sabotages His Own Apps, Then Claims Aaron Swartz Was Murdered
* Indian Patchwork Hacking Group Infects Itself With RAT
* China Puts Walmart In The Naughty Corner Over 19 Vulnerabilities

Krebs on Security

* At Request of U.S., Russia Rounds Up 14 REvil Ransomware Affiliates
* Who is the Network Access Broker 'Wazawaka?'
* 'Wormable' Flaw Leads January 2022 Patch Tuesday
* 500M Avira Antivirus Users Introduced to Cryptomining
* Norton 360 Now Comes With a Cryptominer
* Happy 12th Birthday, KrebsOnSecurity.com!
* NY Man Pleads Guilty in $20 Million SIM Swap Theft
* Microsoft Patch Tuesday, December 2021 Edition
* Inside Ireland's Public Healthcare Ransomware Scare
* Canada Charges Its "Most Prolific Cybercriminal"

Dark Reading

* Russia Takes Down REvil Ransomware Operation, Arrests Key Members
* The Cybersecurity Measures CTOs Are Actually Implementing
* Maryland Dept. of Health Responds to Ransomware Attack
* White House Meets With Software Firms and Open Source Orgs on Security
* What's Next for Patch Management: Automation
* BlueNoroff Threat Group Targets Cryptocurrency Startups
* Fighting Back Against Pegasus, Other Advanced Mobile Malware
* How to Protect Your Phone from Pegasus and Other APTs
* New Vulnerabilities Highlight Risks of Trust in Public Cloud
* How Cybercriminals Are Cashing in on the Culture of 'Yes'
* Redefining the CISO-CIO Relationship
* Microsoft RDP Bug Enables Data Theft, Smart-Card Hijacking
* Check If You Have to Worry About the Latest HTTP Protocol Stack Flaw
* Oxeye Introduce Open Source Payload Deobfuscation Tool
* New Research Reveals Public-Sector IAM Weaknesses and Priorities
* New Cyberattack Campaign Uses Public Cloud Infrastructure to Spread RATs
* Why Is Cyber Assessment So Important in Security?
* Flashpoint Acquires Risk Based Security
* Critical Infrastructure Security and a Case for Optimism in 2022
* Patch Management Today: A Risk-Based Strategy to Defeat Cybercriminals

The Hacker News

* Dark Web's Largest Marketplace for Stolen Credit Cards is Shutting Down
* High-Severity Vulnerability in 3 WordPress Plugins Affected 84,000 Websites
* Ukrainian Government Officially Accuses Russia of Recent Cyberattacks
* New Unpatched Apple Safari Browser Bug Allows Cross-Site User Tracking
* A New Destructive Malware Targeting Ukrainian Government and Business Entities
* Russia Arrests REvil Ransomware Gang Responsible for High-Profile Cyber Attacks
* Get Lifetime Access to Cybersecurity Certification Prep Courses
* Massive Cyber Attack Knocks Down Ukrainian Government Websites
* North Korean Hackers Stole Millions from Cryptocurrency Startups Worldwide
* U.K. Hacker Jailed for Spying on Children and Downloading Indecent Images
* Husband-Wife Arrested in Ukraine for Ransomware Attacks on Foreign Companies
* Cisco Releases Patch for Critical Bug Affecting Unified CCMP and Unified CCDM
* GootLoader Hackers Targeting Employees of Law and Accounting Firms
* Researchers Decrypted Qakbot Banking Trojan's Encrypted Registry Keys
* Iranian Hackers Exploit Log4j Vulnerability to Deploy PowerShell Backdoor

Security Week

* Personal Information Compromised in Goodwill Website Hack
* Microsoft Uncovers Destructive Malware Used in Ukraine Cyberattacks
* Russian Court Remands Hackers in Custody
* Ukraine Says Has 'Evidence' Russia Behind Cyberattack
* Ukraine Hacks Add to Worries of Cyber Conflict With Russia
* Details Published on AWS Flaws Leading to Data Leaks
* Austrian Regulator Says Google Analytics Contravenes GDPR
* North Korean Hackers Stole $400 Million Worth of Cryptocurrency in 2021
* Cyber Attack in Albuquerque Latest to Target Public Schools
* Russia Lays the Smackdown on REvil Ransomware Gang
* Recent GootLoader Campaign Targets Law, Accounting Firms
* Salvadoran Government Denies Using Spyware on Journalists
* U.S. Government, Tech Giants Discuss Open Source Software Security
* Ukraine Reports Massive Cyber Attack on Government Websites
* Maryland Lawmaker: Officials Misled on Ransomware Attack
* Meshed Cybersecurity Platforms Enable Complex Business Environments
* FCC Chair Proposes New Policies for Carrier Data Breach Reporting
* Ransomware Group That Targeted Over 50 Companies Dismantled in Ukraine
* Maryland Confirms Ransomware Attack at Health Agency
* Cisco Patches Critical Vulnerability in Contact Center Products
* ZDI Announces Rules and Prizes for Pwn2Own 2022
* U.S. Cyber Command Officially Links MuddyWater Group to Iranian Intelligence
* Report: Dozens of El Salvador Journalists, Activists Hacked
* Ransomware Attack Locks Down US Prison
* Apple Patches iOS HomeKit Flaw After Researcher Warning

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* Nuclear Ransomware 3.0: We Thought It Was Bad and Then It Got Even Worse
* Fifty FIFA eSports Accounts Were Hacked Via Social Engineering
* FBI: Beware of a New Google Voice Authentication Scam - Even if You Don't Use Google Voice!
* Payment Fraud Moves to the Real World with Fake QR Codes on Parking Meters
* U.S. Government Warns of More Cyberattacks Targeting Critical Infrastructure
* It's a Fact: Cyberattacks Continue Because Your Users Forget
* "Information Disorder": Giving a Name to One of the Most Impactful Parts of Phishing Scams
* Over 200 Ransomware Strains Detected in Last Part of 2021
* KnowBe4 Named a Leader in the Winter 2022 G2 Grid Report for Security Awareness Training
* Business Email Compromise Attack Leads to Millions in Non-Profit Loss

ISC2.org Blog

* A Cybersecurity Role Has Topped List of Best Jobs
* Help Shape The CSSLP Exam
* The Future of Work without Workers
* U.S. Cyber Command Operation Targets 'Real-life Cyber Threats'
* New Opportunity: Join (ISC)² Regional Event Committees

HackRead

* 3 ways to improve your website security
* SnatchCrypto attack hits DeFi and Blockchain Platforms with backdoor
* Largest dark web market for stolen cards UniCC calls it quits
* Russia "neutralizes" REvil ransomware gang, arrests 14
* Husband and wife among ransomware operators arrested in Ukraine
* 3rd-party flaws allowed a teen hacker to track location of Tesla cars
* Hot wallet hack: Hackers steal $18.7m from Animoca's Lympo NTF platform

Koddos

* 3 ways to improve your website security
* SnatchCrypto attack hits DeFi and Blockchain Platforms with backdoor
* Largest dark web market for stolen cards UniCC calls it quits
* Russia "neutralizes" REvil ransomware gang, arrests 14
* Husband and wife among ransomware operators arrested in Ukraine
* 3rd-party flaws allowed a teen hacker to track location of Tesla cars
* Hot wallet hack: Hackers steal $18.7m from Animoca's Lympo NTF platform

Naked Security

* Serious Security: Linux full-disk encryption bug fixed - patch now!
* REvil ransomware crew allegedly busted in Russia, says FSB
* S3 Ep65: Supply chain conniption, NetUSB hole, Honda flashback, FTC muscle [Podcast + Transcript]
* Wormable Windows HTTP hole - what you need to know
* Home routers with NetUSB support could have critical kernel hole
* JavaScript developer destroys own projects in supply chain "lesson"
* Honda cars in flashback to 2002 - "Can't Get You Out Of My Head"
* Log4Shell-like security hole found in popular Java SQL database engine H2
* S3 Ep64: Log4Shell again, scammers keeping busy, and Apple Home bug [Podcast + Transcript]
* FTC threatens "legal action" over unpatched Log4j and other vulns

Threat Post

* Top Illicit Carding Marketplace UniCC Abruptly Shuts Down
* Real Big Phish: Mobile Phishing & Managing User Fallibility
* Critical Cisco Contact Center Bug Threatens Customer-Service Havoc
* 'Be Afraid:' Massive Cyberattack Downs Ukrainian Gov't Sites
* Russian Security Takes Down REvil Ransomware Gang
* Three Plugins with Same Bug Put 84K WordPress Sites at Risk
* Microsoft Yanks Buggy Windows Server Updates
* North Korean APTs Stole ~$400M in Crypto in 2021
* US Military Ties Prolific MuddyWater Cyberespionage APT to Iran
* New GootLoader Campaign Targets Accounting, Law Firms

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

* Small Business Cybersecurity: What Will Be Different in 2022?
* The Great Resignation: How to Acquire and Retain Cybersecurity Talent
* The Best Threat Hunters Are Human
* Digital Transformation: Balancing Speed, Security and Innovation
* Arming CISOs With the Skills to Combat Disinformation
* Cloud Security Trends: What Is Cybersecurity Mesh?
* Small Business Cybersecurity: What to Fix, What to Manage and What to Outsource
* Omnichannel E-commerce Growth Increases API Security Risk
* 5 Things New with Bug Bounty Programs
* The Most Important Security Takeaway from the October Facebook Outage

InfoWorld

* A new kind of old-school testing
* 4 models for escalating access permissions during emergencies
* Parcel CSS parser offered as performance enhancer
* View cloud architecture through a new optimization lens
* IPython REPL update advances code formatting
* Hands-on with GatsbyJS
* Firefox 96 enhances CSS, Canvas support for developers
* What is Web3? A new decentralized web, or the latest marketing buzzword
* Understanding Azure HPC
* Get started with generics in Go

C4ISRNET - Media for the Intelligence Age Military

* Britain to upgrade communications on Cyprus military base
* A yearlong continuing resolution will hinder unmanned systems integration
* Following procurement cut, the Army is looking to add funding back in 2022 for aerial jamming pod
* Pentagon tech chief says new rapid experimentation reserve is moving forward
* US Army plans to make big advances in cloud initiatives this year
* Army readies to deliver first set of Strykers with 50-kilowatt laser weapons
* In change, Army to allow file downloads for Army 365 email on personal devices
* Three ways the Pentagon can create an automation first culture
* Ellen Lord joins GEOST board of directors
* US Space Force considers purchasing weather data as a service

The Hacker Corner

Conferences

* Marketing Cybersecurity In 2021
* Cybersecurity Employment Market
* Cybersecurity Marketing Trends
* Is It Worth Public Speaking?
* Our Guide To Cybersecurity Marketing Campaigns
* How To Choose A Cybersecurity Marketing Agency
* The "New" Conference Concept: The Hybrid
* Best Ways To Market A Conference
* Marketing To Cybersecurity Companies
* Upcoming Black Hat Events (2021)

Google Zero Day Project

* A deep dive into an NSO zero-click iMessage exploit: Remote Code Execution
* This shouldn't have happened: A vulnerability postmortem

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.

* KnightCTF 2022
* Real World CTF 4th
* Insomni'hack teaser 2022
* DiceCTF 2022
* STAY ~/ CTF 2022
* Hayyim CTF 2022
* Decompetition v2.0
* #kksctf open / 5th anniversary edition
* VU CYBERTHON 2022
* CInsects CTF 2022

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

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

Tools & Techniques

Packet Storm Security Tools Links

* Clam AntiVirus Toolkit 0.104.2
* Proxmark3 4.14831
* Faraday 3.19.0
* Haveged 1.9.17
* Haveged 1.9.16
* SQLMAP - Automatic SQL Injection Tool 1.6
* Wireshark Analyzer 3.6.1
* Wapiti Web Application Vulnerability Scanner 3.0.9
* TOR Virtual Network Tunneling Tool 0.4.6.9
* Google OSS Fuzz

Kali Linux Tutorials

* ThreadBoat : Program Uses Thread Execution Hijacking To Inject Native Shell-code Into A Standard Win3
* Stacs : Static Token And Credential Scanner
* SillyRAT : A Cross Platform Multifunctional (Windows/Linux/Mac) RAT
* Registry-Recon : Cobalt Strike Aggressor Script That Performs System/AV/EDR Recon
* pwnSpoof : Generates realistic spoofed log files for common web servers with customisable attack scen
* Nosferatu : Lsass NTLM Authentication Backdoor
* Kubernetes-Goat : Is A "Vulnerable By Design" Kubernetes Cluster
* Facebook Messenger Hack: Which One to Choose and How to Go About It?
* Kube-Applier : Enables Automated Deployment And Declarative Configuration For Your Kubernetes Cluster
* Covery: Online Fraud Detection Software

GBHackers Analysis

* Chinese Hackers Exploiting Log4Shell Vulnerability & Attack Internet-Facing Systems
* Bugs With URL Parsing Libraries Could Allow DoS, RCE, Spoofing & More
* 5 Most Fearsome Hacks in 2022
* Elephant Beetle Hacking Group Attack Organizations To Steal Financial Data
* Chinese Hackers Using Log4Shell Exploit Tools to Perform Post-Exploitation Attacks

Weekly Cyber Security Video and Podcasts

SANS DFIR

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

Defcon Conference

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

Hak5

* OMG Cable - Android Reverse Shell - Payload & Detections
* WarFlying Drone: Hunt Down WiFi Devices from the Air | HakByte
* Moxie Marlinspike Leaving Signal (Stepping Down As CEO!) - ThreatWire

The PC Security Channel [TPSC]

* Norton is now a Crypto Miner
* Best Browser Security: Edge vs Firefox vs Chrome

Eli the Computer Guy

* INFLATION SOARS to HIGHEST IN 40 YEARS - biden's failing economy
* HALF of EUROPE will CATCH OMICRON within WEEKS - riding the party bus to hell
* OSHA COVID VACCINATION MANDATE is UNCONSTITUTIONAL - supreme court says Biden is WRONG
* APPLE ABUSED FACTORY WORKERS in INDIA - indian women eating worms in deplorable conditions

Security Now

* URL Parsing Vulnerabilities - US CISA on Log4J, WordPress Security Update, What Is a Pluton
* December 33rd - Log4j Update, RSA Postponed, Hack the DHS Expanded, Cyber Insurance Cost Rising

Troy Hunt

* Weekly Update 278

Intel Techniques: The Privacy, Security, & OSINT Show

* 246-Android Sanitization
* 245-OSINT 9 & Privacy Updates

Proof of Concept (PoC) & Exploits

Packet Storm Security

* SonicWall SMA 100 Series Authenticated Command Injection
* Chrome IPC::ChannelAssociatedGroupController Memory Corruption
* Microsoft Windows EFSRPC Arbitrary File Upload / Privilege Escalation
* Apple ColorSync Out-Of-Bounds Read
* RLM 14.2 Cross Site Scripting
* Online Diagnostic Lab Management System 1.0 Missing Access Control
* Online Diagnostic Lab Management System 1.0 Cross Site Scripting
* Online Diagnostic Lab Management System 1.0 SQL Injection
* WordPress Core 5.8.2 SQL Injection
* Hospitals Patient Records Management System 1.0 Cross Site Scripting
* SalonERP 3.0.1 SQL Injection
* Log4Shell HTTP Header Injection
* Crestron HD-MD4X2-4K-E 1.0.0.2159 Credential Disclosure
* Libstagefright Heap Out-Of-Bounds Write
* WordPress Frontend Uploader 1.3.2 Cross Site Scripting
* DMCA.com Improper Access Control / Cross Site Scripting
* Backdoor.Win32.Controlit.10 Code Execution
* Microsoft Windows Defender / Detection Bypass
* Microsoft Windows .Reg File Dialog Spoofing / Mitigation Bypass
* Linux Garbage Collection Memory Corruption
* Open-AudIT Community 4.2.0 Cross Site Scripting
* WordPress Contact Form Entries Cross Site Scripting
* HTTP Commander 3.1.9 Cross Site Scripting
* Online Examination System Project 1.0 SQL Injection
* Online Resort Management System 1.0 SQL Injection

CXSecurity

* SonicWall SMA 100 Series Authenticated Command Injection
* Log4Shell HTTP Header Injection
* Automox Agent 32 Local Privilege Escalation
* Siemens S7 Layer 2 Denial of Service (DoS)
* AWebServer GhostBuilding 18 Denial Of Service
* Gerapy 0.9.7 Remote Code Execution
* Vodafone H-500-s 3.5.10 WiFi Password Disclosure

Proof of Concept (PoC) & Exploits

Exploit Database

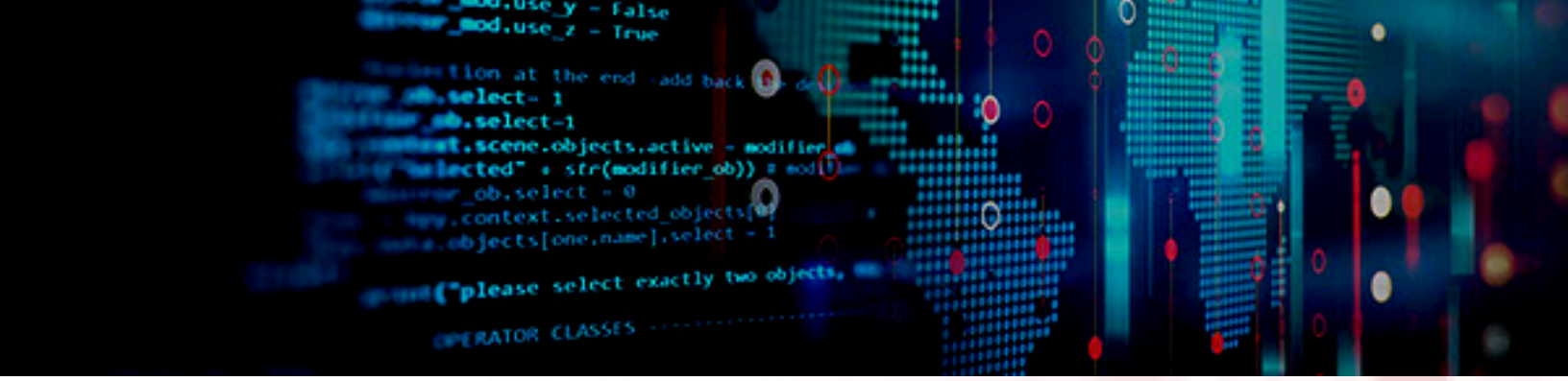
* [webapps] WordPress Core 5.8.2 - 'WP_Query' SQL Injection
* [webapps] Online Diagnostic Lab Management System 1.0 - SQL Injection (Unauthenticated)
* [webapps] Online Diagnostic Lab Management System 1.0 - Stored Cross Site Scripting (XSS)
* [webapps] Online Diagnostic Lab Management System 1.0 - Account Takeover (Unauthenticated)
* [webapps] SalonERP 3.0.1 - 'sql' SQL Injection (Authenticated)
* [webapps] Hospitals Patient Records Management System 1.0 - 'doctors' Stored Cross Site Scripting (XS
* [webapps] Hospitals Patient Records Management System 1.0 - 'room_list' Stored Cross Site Scripting (
* [webapps] Hospitals Patient Records Management System 1.0 - 'room_types' Stored Cross Site Scripting
* [webapps] WordPress Plugin Frontend Uploader 1.3.2 - Stored Cross Site Scripting (XSS) (Unauthenticat
* [local] Microsoft Windows Defender - Detections Bypass
* [local] Microsoft Windows .Reg File - Dialog Spoof / Mitigation Bypass
* [remote] CoreFTP Server build 725 - Directory Traversal (Authenticated)
* [webapps] Open-AudIT Community 4.2.0 - Cross-Site Scripting (XSS) (Authenticated)
* [local] VUPlayer 2.49 - '.wax' Local Buffer Overflow (DEP Bypass)
* [webapps] Online Railway Reservation System 1.0 - 'Multiple' Stored Cross Site Scripting (XSS) (Unaut
* [webapps] Online Railway Reservation System 1.0 - Admin Account Creation (Unauthenticated)
* [webapps] Online Railway Reservation System 1.0 - Remote Code Execution (RCE) (Unauthenticated)
* [webapps] Online Railway Reservation System 1.0 - 'id' SQL Injection (Unauthenticated)
* [webapps] HTTP Commander 3.1.9 - Stored Cross Site Scripting (XSS)
* [webapps] Online Veterinary Appointment System 1.0 - 'Multiple' SQL Injection
* [webapps] WordPress Plugin AAWP 3.16 - 'tab' Reflected Cross Site Scripting (XSS) (Authenticated)
* [local] Automox Agent 32 - Local Privilege Escalation
* [webapps] Projeqtor v9.3.1 - Stored Cross Site Scripting (XSS)
* [remote] Gerapy 0.9.7 - Remote Code Execution (RCE) (Authenticated)
* [remote] Dixell XWEB 500 - Arbitrary File Write

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*

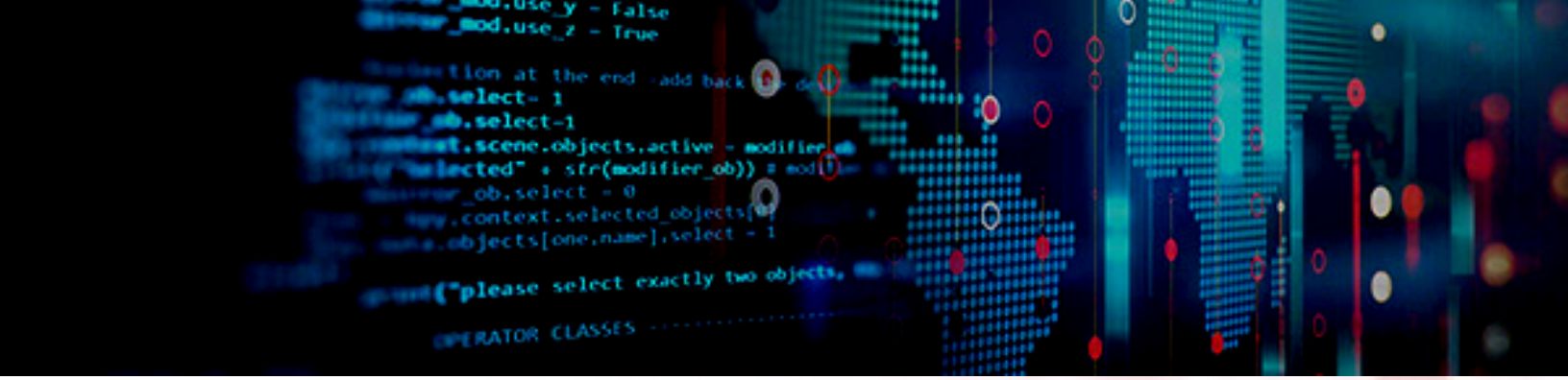
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://www.cepro.pi.gov.br
http://www.cepro.pi.gov.br notified by Paraná Cyber Mafia
http://www.pm.pi.gov.br
http://www.pm.pi.gov.br notified by Paraná Cyber Mafia
https://hpe.gov.vn
https://hpe.gov.vn notified by 0x1998
http://hoaphuong.gov.vn/fck.html
http://hoaphuong.gov.vn/fck.html notified by 0x1998
https://etidi.gov.et/kz.html
https://etidi.gov.et/kz.html notified by Mr.Kro0oz.305
http://pops.int/kurd.html
http://pops.int/kurd.html notified by 0x1998
http://archive.pic.int/kurd.html
http://archive.pic.int/kurd.html notified by 0x1998
http://article15.pops.int/kurd.html
http://article15.pops.int/kurd.html notified by 0x1998
https://toolkit.pops.int/kurd.htm
https://toolkit.pops.int/kurd.htm notified by 0x1998
http://chm.pops.int/kurd.html
http://chm.pops.int/kurd.html notified by 0x1998
http://synergies.pops.int/kurd.html
http://synergies.pops.int/kurd.html notified by 0x1998
http://pic.int/kurd.html
http://pic.int/kurd.html notified by 0x1998
http://www.basel.int/kurd.html
http://www.basel.int/kurd.html notified by 0x1998
https://amc.namem.gov.mn/kz.html
https://amc.namem.gov.mn/kz.html notified by Mr.Kro0oz.305
https://siaya.go.ke/kz.html
https://siaya.go.ke/kz.html notified by Mr.Kro0oz.305
http://saojoaodomanteninha.cam.mg.gov.br/b4.html
http://saojoaodomanteninha.cam.mg.gov.br/b4.html notified by 0x1998
https://tramites.campeche.gob.mx/b4.html
https://tramites.campeche.gob.mx/b4.html notified by 0x1998



Dark Web News

Darknet Live

"Church Leader" to Plead Guilty in Murder-For-Hire Case

The "church leader” accused of trying to hire a hitman on the darkweb is planning to accept a plea agreement, according to court records. DeAnna Marie Stinson, 50, stands accused of soliciting a crime of violence and murder-for-hire. Stinson spent $12,000 in Bitcoin on a darkweb murder-for-hire site, according to the U.S. Attorney's Office for the Middle District of Florida. A federal court status report indicates that Stinson will be accepting a plea agreement. Per WFLA: Stinson's "case will resolve with an open plea to the court… A change of plea hearing is scheduled for Wednesday, January 19, 2022.” Seems like just yesterday that this site published an article about the defendant's arrest, seemingly moving from arrest to conviction in record time. However, the U.S. Marshals Service raided Stinson's home and arrested her on September 24, 2021. Still only months between arrest and conviction but not as drastic as I had remembered.

Ok. Unless the statement of facts contains something surprising, no useful information will come out of this case. This is unfortunate as this case is an atypical "darkweb murder-for-hire ” case; a federal law enforcement officer posed as the hitman (feds possibly ran this murder-for-hire site as well) the defendant had hired. In the usual cases involving the same crime, the defendants attempt to hire a hitman through one of the many murder-for-hire sites operated by "Yura,” such as Besa Mafia, Crimebay, Cosa Nostra International Network, Camorra Hitmen, and the Sicilian Hitmen International Network. I was hoping we would get to see at least some information about fed-run murder-for-hire scams. Perhaps this is one reason Stinson so quickly indicated her willingness to sign a plea deal. This "church leader” is currently being held in Pinellas County Jail. The change of plea hearing is scheduled for 2 p.m. on January 19, 2022. Oh yeah. Here is the church leader bit. Patch.com: Stinson is the director of finance for Bible-Based Fellowship Church at 4811 Erlich Road in Carrollwood.

In addition to her work at the church, Stinson is the founder of Woman of Excellence Consulting in New Tampa.

According to Woman of Excellence website, Stinson founded the organization in 2002 to help small, minority-owned businesses who can't afford administrative, organizational or accounting services. WFLA: "Change of plea hearing set for Tampa woman arrested in murder-for-hire plot” archive.org | archive.is | archive[…].onion Patch.com: (via darknetlive.com at https://darknetlive.com/post/church-leader-to-plead-guilty-in-darkweb-murder-for-hire-case/)

Meth Vendor "IcyDicy" Sentenced to 160 Months in Prison

A federal district judge in Florida sentenced a 26-year-old Arizona man to 160 months in prison for selling drugs on darkweb markets. From 2018 to 2020, Jose Rodolfo Barraza Flores advertised and sold crystal methamphetamine, cocaine, counterfeit Percocet pills, and other drugs on White House Market, Empire Market, and Yellow Brick Market. According to a criminal complaint filed by FBI Special Agent Gregory Hoffman, Flores operated the vendor accounts "GXAW” and "IcyDicy.”

Drugs seized during the execution of a search warrant. During the investigation, feds conducted a substantial number of controlled purchases from Flores' vendor accounts. In one order, an undercover fed

purchased 500 counterfeit oxycodone pills. Below is an example of one of the controlled purchases on Yellow Brick Market: On September 2, 2020, FBI agents purchased four (4) ounces of crystal methamphetamine from GXAW on Yellow Brick Road Market for .157277 Bitcoins. In the description, GXAW advertised the drugs as "4 oz 99% Crystal Meth”. After receiving the package in the Southern District of Florida, agents found a crystalline substance secreted in a wax candle. The substance was sent to the DEA Southeast Laboratory for testing with positive lab results for I12.6g (+- 0.2g) methamphetamine hydrochloride (100% Purity +-6%).

Police found a passport belonging to Flores at a property assosciated with his brother. One Yellow Brick vanished, feds started purchasing from the vendor on Empire Market. And once Empire Market vanished, feds started purchasing from the vendor on White House Market. Example below. Since at least October of 2020, agents identified a narcotics vendor operating on White House Market under the moniker IcyDicy. On several occasions, FBI agents have made undercover online purchases of crystal methamphetamine from IcyDicy on White House Market and received the drugs via U.S. Mail, shipped to undercover mailboxes throughout the Unites States to include Palm Beach County, Florida. For instance:

On December 4, 2020, FBI agents purchased twenty-eight (28) grams of crystal methamphetamine from IcyDicy on White House Market for 3.035592319950 XMR (Monero). In the description, IcyDicy advertised the drugs as "14 grams 99% Crystal Meth”. The package was mailed on December 8, 2020, at the Glendale Post Office, Glendale, AZ. Postal Inspectors recovered the package and upon opening it, agents found a crystalline substance secreted in a wax candle, similar to the crystal methamphetamine received from UXAW and IcyDicy in prior purchases. The substance field-tested positive for methamphetamine and weighed approximately 30.4 grams.

Postal Inspectors obtained the IP address of the defendant or one of his co-conspirators after the party checked the tracking on one of the packages ordered by law enforcement. The IP address was associated with a Cox account and a property that belonged to the defendant's brother. Investigators also checked surveillance footage at the Post Office and identified the party responsible for mailing the packages as a Hispanic male. I suspect that the defendant had used a card to purchase postage on at least one occasion because investigators somehow linked the vendor to a Capital One bank account. Records from Capital One provided investigators with Flores' identity, address, and Gmail email address. Records from Google pertaining to the GMail address revealed that Fores had set "oneoneboy11@gmail.com” as a recovery email address. The criminal complaint reveals that when investigators imported GXAW's PGP key into Kleopatra, they noticed the email address " oneoneboy@outlook.com.” Flores, or a co-conspirator, had apparently used that email address when creating their PGP key.

USPIS identified Flores on USPS security camera footage. Special Agent Hoffman wrote about the similarities between the two email addresses: In your affiant's training and experience, I am aware that regular internet users, and users of the darkweb in particular, often have common personalized naming schemes and themes with which they create email addresses, anonymous internet profiles, and account usernames. Therefore, due to the similarity in naming convention, between oneoneboy11@gmail.com and oneoneboy@outlook.com, your affiant believes it is reasonable to conclude that FLORES was operating the PGP account associated with the GXAW moniker.

They have pages of pictures of Flores at USPS locations. A raid at the address associated with Flores resulted in the discovery of his Mexican passport, pictures of his family, drugs, and equipment used in the distribution of those drugs, including: 4-5 pounds of methamphetamine; an undisclosed quantity of cocaine; a pill press; melted wax in containers; hot plates; melted wax in pots and; candle molds similar to the candles used by the vendor accounts GXAW and IcyDicy.

Defendant kept some records of his drug orders on at least one of his HP Laptops, among other devices he used to conduct his dark web activity. Other information and photographs regarding drugs, darkweb vending, and the use of Cryptocurrency were found on another computer and phones belonging to FLORES which were recovered in the course of this investigation. Defendant only accepted cryptocurrency, in particular, Bitcoin and Monero, as payments for his drug sales and communicated with customers via encrypted messaging through marketplace-provided messaging services. Feds analyzed the review sections of Yellow Brick Market and White House Market to get the total weight of the drugs Flores had distributed. Yellow Brick: Agents were able

to aggregate the weights of drugs sold by GXAW as confirmed through this marketplace review process: 4878g of Meth 99%, 1815 pills of Pere M30s, 98.5g of Coke 96%, and 76g of Coke 77%. White House: Agents were able to aggregate the weights of drugs sold by GXAW as confirmed through this marketplace review process: approximately 4764 grams of methamphetamine and 4482 Perc M30s were sold by IcyDicy between July 19, 2020, and November 2, 2020. Also, the DEA seized $75,000 in cash from Flores at a Greyhound and Amtrack station in Albuquerque, New Mexico. The DEA found the money in an amplifier stored in the luggage storage area of the bus. Flores said that he had brought the amplifier with him but had not known about the money. So the DEA wrote him a receipt for the "abandoned money.” The full text of the report is available below. MY INVOLVEMENT IN THE SEIZURE OF $79,380 DOLLARS OF US CURRENCY. ON SEPTEMBER 9, 2016, DRUG ENFORCEMENT AGENCY (DEA) SPECIAL AGENT (SA) JARRELL PERRY AND I WERE CONDUCTING CONSENSUAL ENCOUNTERS AT THE GREYHOUND AND AMTRACK STATION IN ALBUQUERQUE, NM. WHILE THE GREYHOUND BUS WAS GETTING SERVICED IN THE MAINTENANCE BAY, I OBSERVED A BLACK TRATE" AMPLIFIER IN THE CHECK-IN LUGGAGE STORAGE AREA OF THE BUS THE AMPLIFIER HAD A CHECK-IN TAG THAT STATED THE AMPLIFIER BELONGED TO A JOSE BARRAZA-FLORES. THE CHECK-IN TICKET STATED MR. BARRAZA-FLORES WAS TRAVELING FROM INDIANAPOLIS, INDIANA, AND HIS FINAL DESTINATION WAS PHOENIX, ARIZONA. I FOUND IT STRANGE THERE WAS NO INSTRUMENT IN THE CHECK-IN LUGGAGE STORAGE OF THE BUS AND MR. BARRAZA-FLORES DID NOT HAVE ANY OTHER CHECK-IN-IN LUGGAGE. I RETRIEVED THE AMPLIFIER FROM THE STORAGE AREA, AND I FELT THE AMPLIFIER WAS EXTREMELY HEAVY. I RETRIEVED MY CANINE 'KIMBA' FROM MY PATROL UNIT TO DO AN EXTERIOR SNIFF OF THE AMPLIFIER ALONG WITH OTHER LUGGAGE FROM THE CHECK-IN STORAGE. DURING THE EXTERIOR SNIFF, I OBSERVED ALERT BEHAVIOR FROM CANINE KIMBA WHEN SHE SNIFFED THE EXTERIOR OF THE AMPLIFIER. CANINE KIMBA IS CERTIFIED TO DETECT THE ODORS OF MARIJUANA, COCAINE, HEROIN, METHAMPHETAMINES, AND THEIR DERIVATIVES. CANINE KIMBA IS CERTIFIED BY THE CALIFORNIA NARCOTICS CANINE ASSOCIATION (CNCA), AND BY THE DEPARTMENT OF PUBLIC SAFETY CANINE PROGRAM. CANINE KIMBA AND I ARE A CERTIFIED WORKING TEAM. I INFORMED SA PERRY OF THE ALERT, I (sic?) SEEN FROM CANINE KIMBA THE AMPLIFIER WAS PLACED BACK IN THE STORAGE AREA OF THE BUS. THE BUS LEFT THE MAINTENANCE LOT AND PARKED IN THE PASSENGER BOARDING AREA OF THE GREYHOUND BUS STATION, AND BEGAN TO BOARD PASSENGERS WHO ARE TRAVELING WEST TOWARD PHOENIX, AZ. SA PERRY AND I BOARDED THE BUS AND BEGAN CONSENSUAL ENCOUNTERS WITH THE PASSENGERS. DURING THE ENCOUNTERS SA PERRY TALKED TO MR. BARRAZA-FLORES. SA PERRY INFORMED ME HE HAD GOTTEN VOLUNTARY CONSENT FROM MR. BARRAZA-FLORES TO SEARCH THE AMPLIFIER WHICH WAS IN THE CHECK-IN STORAGE AREA OF THE BUS. DURING SA PERRYS SEARCH HE LOCATED TWO PLASTIC GROCERY BAGS INSIDE OF THE AMPLIFIER, WHICH CONTAINED LARGE AMOUNTS OF US CURRENCY. ALSO IN THE AMPLIFIER, THERE WAS A WHITE BED SHEET AND TWO WHITE BATH TOWELS INSIDE. SA PERRY INFORMED ME MR. BARRAZA-FLORES WAS COMING FROM INDIANAPOLIS, INDIANA, AND WAS ON HIS WAY BACK TO PHOENIX, AZ. SA PERRY TOLD ME MR. BARRAZA-FLORES STATED HE WENT TO VISIT HIS AUNT AND UNCLE. HE STATED HIS AUNT AND UNCLE PLAY IN A BAND, AND THEY HAD ASKED HIM TO BRING AN AMPLIFIER WITH HIM. HE TOLD SA PERRY HE DID HAVE A GUITAR, BUT IT WAS BROKEN, AND THAT IS WHY HE DID NOT BRING IT ON THE TRIP. ACCORDING TO MR. BARRAZA-FLORES HE HAD MADE THE TRIP TO INDIANAPOLIS, INDIAN APPROXIMATELY 4 TIMES, AND HE HAS TAKEN THE AMPLIFIER WITH HIM ON THOSE TRIPS. MR. BARRAZA-FLORES STATED HE DID NOT KNOW THE AMPLIFIER CONTAINED MONEY, AND HE SAID IT DID NOT BELONG TO HIM. SA PERRY SEIZED THE MONEY AND GAVE MR. BARRAZA-FLORES A RECIEPT FOR THE ABANDONED MONEY. MR. BARRAZA-FLORES WAS RELEASED WITHOUT FURTHER INCIDENT. In October 2021, Barraza Flores pleaded guilty to conspiracy to distribute a controlled substance and three counts of distribution of a controlled substance. U.S. District Judge Aileen M. Cannon imposed a sentence of 160 months in prison and a $400 fine. Attached: proffer statement (pdf) Report on cash

seizure (pdf) USAO press release archive.org, archive.is, archive.is .onion (via darknetlive.com at https://darknetlive.com/post/meth-vendor-icydicy-sentenced-to-160-months-in-prison/)

Counterfeit Oxy Vendor "Ghost831" Sentenced to Prison

An Arizona man was sentenced to prison for distributing a wide variety of drugs through the darkweb under the "Ghost831” vendor moniker. According to court records (.org, .onion), 29-year-old Jacob Matthew Medina, of Glendale, Arizona, was imprisoned after he admitted that he had participated in a conspiracy to distribute fentanyl and heroin on the darkweb through a vendor account on Dream Market. The profile on Dream Market had the username "Ghost831.” During execution of a search warrant, feds found 502 grams of counterfeit oxycodon pills. The United States Postal Inspection Service (USPIS) launched an investigation into Medina's drug trafficking operation in November 2018, after investigators discovered the "Ghost831” vendor account on Dream Market. The vendor sold heroin, methamphetamine, and counterfeit oxycodone pills. During the investigations, investigators conducted an undercover purchase of heroin from "Ghost831.” Investigators also intercepted multiple drug packages that had been mailed by the vendor. Further investigations traced the packages back to Medina. Investigators executed a search warrant at Medina's home on March 4, 2019. The search resulted in the seizure of 502 grams of counterfeit oxycodone pills that tested positive for fentanyl, more than 400 grams of heroin, a list of customer mailing addresses, package tracking numbers, $31,000 in cash, and a firearm.

Feds found mailers and the usual vendor equipment during the raid. The investigators established that one of the customers who had purchased drugs from Medina had fatally overdosed. Melisa Llosa, Inspector in Charge of the USPIS, Phoenix Division: "Mr. Medina profited off of numerous individuals addicted to opioids with his fentanyl-laced pills. He utilized the dark web, mistakenly thinking he could outsmart the authorities. The US Postal Inspection Service is committed to investigating and dismantling drug trafficking organizations to keep US Postal Service customers and employees safe from such dangerous drugs.” Medina pleaded guilty to conspiring in the possession of fentanyl and heroin with intent to distribute. On January 4, 2022, U.S. District Judge Douglas L. Rayes sentenced Medina to 13 years and four months in federal prison.

DNL: I want to add a little background to this case as I do not think we have covered it and the sentencing announcement contains very little information. This case is a result of an investigation initiated by the Narcotics and Economic Crime Investigations (NECI) Task Force in Sacramento, CA. Undercover purchases revealed that the vendor operated out of Arizona. Investigators found that Medina and one of his co-conspirators had purchased postage at a USPS self service kiosk (SSK). Surveillance footage revealed that one of the people purchasing postage for packages associated with the vendor account was a "Hispanic male with a bard and goatee” who appeared to be between the ages of 20 and 30. They also matched the postage purchases with a pre-paid Visa card from Bancorp Bank.

A USPIS Activity/Investigation report There is a change.org petition calling for the release of an inmate named Jacob Matthew Medina that has a picture matching the description above. The petition claims that Medina is serving "a mandatory minimum of 10 years in prison for a alleged non violent drug offense” at an institution in Arizona. It provides a Central Arizona Florence Correctional Complex inmate number that matches the profile an inmate also matching the description of Medina with a 1992 DOB. Interestingly, the criminal complaint described the U.S. Postal Inspection Service (USPIS) Cyber Crime Unit's role in the investigation. Postal Inspectors sent a request to the U.S. Postal Inspection Service (USPIS) Cyber Crime Unit for an analysis of "Ghost831.” Historical USPIS information showed a "Ghost831” registered accounts on the Alphabay (AB), Cloud9, Hydra, SilkRoad (SR), and SilkRoad 2.0 (SR2) markets. The following historical information was found for "Ghost831” on SR: Registered: October 17, 2012. Last Seen: September 22, 2013. Private "sent” messages show "Ghost831” was selling Oxycodone. "Ghost 831” identified his location as being in Arizona. On May 22, 2013, "Ghost831” posted "…in AZ theres a lot of BS here…” On June 3, 2013, "Ghost831” identified himself as being 21 years old when he posted, "…I been hustling since I was 15 im 21 on june 3”'…" This would have meant the date of birth for "Ghost83 1” was June 3, ' 1992. User Email: jsquad3@yahoo.com This information alone was enough to identify Medina, according to

the complaint. And not through the use of a court order for subscriber information assosciated with the Yahoo email address. On January 30, 2019, analysts utilized a law enforcement database to search for individuals who were arrested in Arizona with a date of birth of June 3, 1992 and a first initial of "J” based on the email address, jsquad3@yahoo.com, provided by "Ghost831” on SR. The research identified a male individual with the name of JACOB MATTHEW MEDINA (MEDINA). Analysts obtained a booking photo of MEDINA and visually compared the booking photo and his Arizona driver's license photo with the SSK photos obtained of the male mailer on December 4, 2018. The comparison revealed the mailer to be MEDINA. Investigators found Facebook profiles for Medina and the second defendant. They conducted an extensive physical surveillance campaign, following the defendants to Post Offices and grocery stores. And the rest is history. Also, here is an excerpt from the USPIS Activity/Investigation Report filed by Postal Inspector Andrea Brandon As of December 28, 2018, Postal Inspector Brandon still had not received anything. Postal Inspector Brandon logged into NFusion and the Dream Market and sent Ghost831 a message inquiring about the purchase. On the same day, Ghost831 responded and asked when the order was placed and what address it was supposed to go to. Postal Inspector Brandon provided the information and Ghost831 stated, "I believe yours is in route ill check later today? " On December 31, 2018, Postal Inspector Brandon sent Ghost831 another message inquiring about the purchase. Ghost831 replied, We know we checked the tracking and its lost we gave you 3.5 and sent you a new one were sorry or the inconvenience? On January 4, 2019, Postal Inspector Brandon was notified that the SUBJECT PARCEL had arrived at the undercover address.

On January 7, 2019, Postal Inspector Michael Kaminski took custody of the SUBJECT PARCEL and transported it to the U.S. Postal Inspection Service, Phoenix Headquarters, for evidence processing. The SUBJECT PARCEL is described as follows: One USPS First-Class parcel with a return address of "Gift card LLC, 6409 N. Scottsdale Rd., Scottsdale, AZ 85253? It is a manila envelope; measuring approximately 4” X 7”; mailed on 12/31/18 from a SSK at the Cactus Station, located at 2901 E. Greenway Rd., Phoenix, AZ 85032; with $1.00 in postage. On January 11, 2019, Postal Inspectors McClamrock and Postal Inspector Shepard processed the SUBJECT PARCEL and contents, which revealed the following: one manila envelope and one small blue zip lock baggie containing a white crystallized substance. The total weight of the baggie and white crystallized substance was approximately 4.0 grams. Postal Inspector McClamrock conducted a TruNarc drug identification test (scan 329), which resulted in a positive alert for methamphetamine. h/t to the person who pointed out that the archive.is onion does not require a captcha often, if ever. Criminal complaint pdf

Plea agreement pdf (via darknetlive.com at https://darknetlive.com/post/counterfeit-oxy-vendor-ghost831-sentenced-to-13-years-in-prison/)

Reminder: Facebook Helped the FBI Hack a Tor User

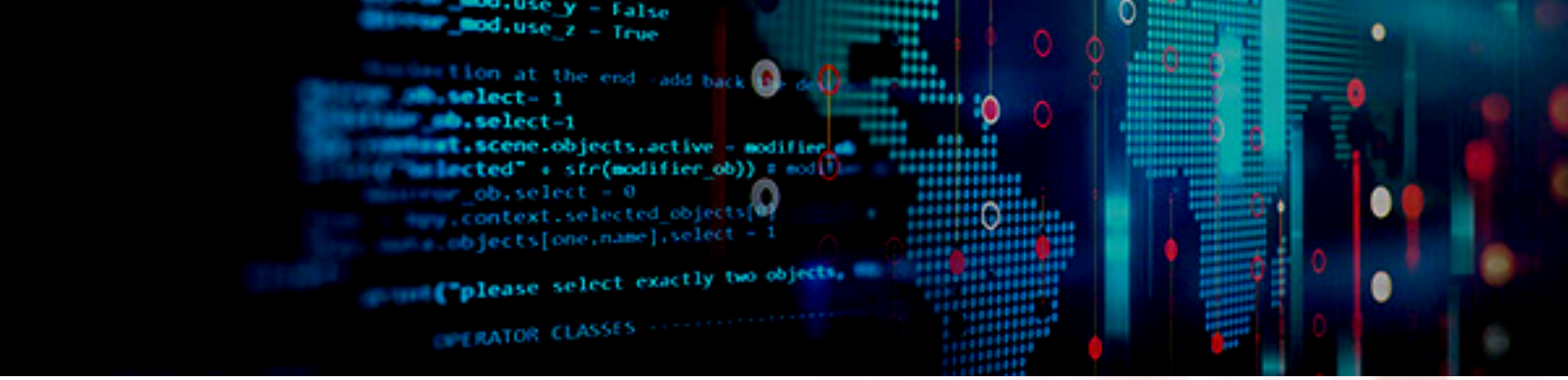
To help the FBI identify a Tor user in 2017, Facebook paid a cybersecurity firm to take advantage of a zero-day exploit in Tails, a privacy-focused operating system. Buster Hernandez, known online as "Brian Kil,” notoriously coerced high school-aged girls to send him "child erotica” or sexually explicit pictures and videos. According to court records, Hernandez coerced these teenagers from about 2015 through mid-2017. However, during the FBI investigation (1:17-cr-00183) that resulted in his arrest, none of the victims were minors. The child pornography charges applied to content received through January 2016, indicating that his victims were perhaps 16 or 17 years old at the time. (Note: some news articles have different timelines than the criminal complaint but it appears as if his victims all stopped being minors long before the police arrested Hernandez. Additionally, he seemingly targeted high school-aged girls in general as some of them were not minors when he contacted them.) Tails Hernandez, through possibly hundreds of Facebook profiles created through Tor, sent messages to three teenage girls who went to a high school in Plainfield, Indiana. The messages generally followed a pattern outlined below: "Brian Kil” contacted random individuals (typically minors) by sending private messages that said, for example, "Hi [Victim Name], I have to ask you something. Kinda important. How many guys have you sent dirty pics to cause I have some of you?” If the teenager responded, Hernandez would demand additional pictures or videos and threaten to distribute the ones in his possession if the girl refused to comply. Brian Kil also

just pretended to have explicit content altogether. Hernandez became something of a problem for Facebook as well as the Plainfield community. Motherboard reported: Hernandez was so notorious within Facebook that employees considered him the worst criminal to ever use the platform, two former employees told Motherboard. According to these sources, Facebook assigned a dedicated employee to track him for around two years and developed a new machine learning system designed to detect users creating new accounts and reaching out to kids in an attempt to exploit them. That system was able to detect Hernandez and tie different pseudonymous accounts and their respective victims to him, two former Facebook employees said. Hernandez taunted Facebook employees, local law enforcement, and the FBI in some of his posts. Investigators never received anything but the I.P. addresses of Tor exit nodes when requesting information on "Brian Kil” from Facebook, email providers, and related services. Brian Kil actually did better than most darkweb vendors as far as OPSEC goes. So Facebook decided to hire a cybersecurity firm to help the FBI identify the user. They paid a cybersecurity consulting firm six figures to create a hacking tool that took advantage of a vulnerability in the video player that shipped with the Tails operating system. The cybersecurity firm's tool, which they worked with a Facebook engineer to create, seemingly created a piece of malware disguised as a video file. When a Tails user attempted to view the video, the malware sent the user's real I.P. address to a server controlled by the cybersecurity firm (or, at the end of the investigation, to a server controlled by alphabet boys). Facebook gave the hacking tool to a third party who then passed it to the FBI. In 2017, the FBI obtained authorization from a judge to deploy the Network Investigative Technique (NIT). The FBI described the file as a real video file with the malware attached to it. Brian Kil seemed to believe the file or the DropBox account lacked content. As outlined in the search warrant application presented to Judge Lynch, the FBI was authorized by the Court to add a small piece of code (NIT) to a normal video file produced by Victim 2, which did not contain any visual depictions of any minor engaged in sexually explicit activity. As authorized, the FBI then uploaded the video file containing the NIT to the Dropbox.com account known only to Kil and Victim 2. When Kil viewed the video containing the NIT on a computer, the NIT would disclose the true IP address associated with the computer used by Kil. After obtaining the IP address, the FBI received authorization to install and use pen registers and tap-and-trace devices on the IP. The FBI, through the use of the wiretap, learned that Hernandez accessed Tor nodes after his significant other left the house. They also identified 4chan threads Hernandez had accessed, among other things. Facebook sources told Motherboard that they justified their involvement in the creation of a hacking tool because of the type of crime Hernandez had committed. The defendant pleaded guilty to 41 charges, including Production of Child Pornography, Coercion and Enticement of a Minor, and Threats to Kill, Kidnap, and Injure. Additionally, Facebook employees said that an upcoming Tails release had removed the vulnerable code from the video player. A Tails spokesperson told Motherboard that, at the time, they "didn't know about the story of Hernandez until now and we are not aware of which vulnerability was used to deanonymize him.” I am sure I will get inaccurately branded by the usual suspect as a defender of pedophiles or something for publishing this article. The fact of the matter is that if these companies are doing this to one person, they are doing it to others. Although Facebook's six-figure Tails hack might be an extreme example, data uncovered in the BlueLeaks hack revealed that companies do this kind of stuff for free: Guardian: A little-known investigative unit inside search giant Google regularly forwarded detailed personal information on the company's users to members of a counter-terrorist fusion center in California's Bay Area, according to leaked documents reviewed by the Guardian. […] Other users are identified by more sophisticated methods, and while some are banned from YouTube, they appear to retain access to other Google services. One user was identified by matching two separate Gmail addresses to a single Android device, which yielded the user's name, age, address, and phone number. That user had posted YouTube comments making anti-Jewish comments, praising white supremacist terrorists, including mass killers, and suggesting he may emulate them. I suppose that as long as you are buying packs of marijuana on darkweb drug markets and not doing a racism, you might be safe for now. The feds openly and almost regularly use NITs during child exploitation investigations. But given their explicit training on parallel construction and limitless resources, I doubt we know about even half of the cases in which an NIT was deployed against Tor users. Criminal Complaint: pdf, html, html2 Also, I guess it

is time for an article on the Rich Uncle Pennybags situation. Also also, I tried to use archive.org instead of archive.is throughout. I personally like .is better as a service but the use of Google captchas is obviously a problem. Plus, have you ever tried logging into Dread? (via darknetlive.com at https://darknetlive.com/post/reminder-facebook-helped-the-fbi-hack-a-tor-user/)

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

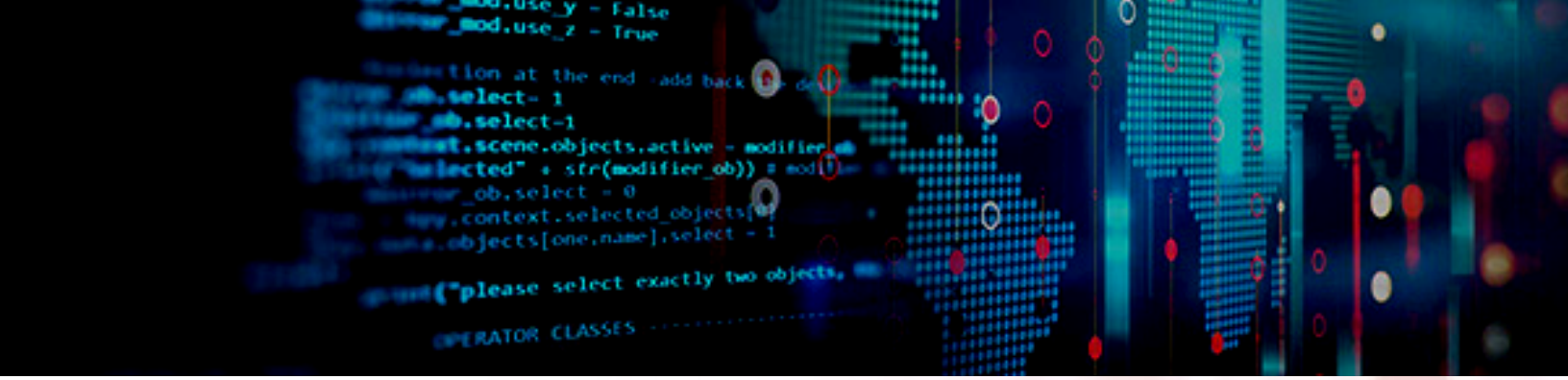
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

* "Offshore" Shinjiru Provides Bulletproof Services to Cyberattackers
* Retailers Using WooCommerce are at Risk of Magecart Attacks
* 5 Tips to Stay on the Offensive and Safeguard Your Attack Surface
* New E-Commerce Cybersecurity Guide Helps Brands be Proactive This Holiday Shopping Season
* New Aggah Campaign Hijacks Clipboards to Replace Cryptocurrency Addresses
* The Vagabon Kit Highlights 'Frankenstein' Trend in Phishing
* Watch On-Demand: Five Security Intelligence Must-Haves For Next-Gen Attack Surface Management
* Discord CDN Abuse Found to Deliver 27 Unique Malware Types
* The Threat Landscape is Dynamic and Ever-Changing - Can You Keep Up?
* Mana Tools: A Malware C2 Panel with a Past

FireEye

* Metasploit Weekly Wrap-Up
* 7Rapid Questions: Stephen Donnelly
* Being Naughty to See Who Was Nice: Machine Learning Attacks on Santa's List
* Evaluating MDR Vendors: A Pocket Buyer's Guide
* A Quick Look at CES 2022
* A December to Remember - Or, How We Improved InsightAppSec in Q4 in the Midst of Log4Shell
* Demystifying XDR: How Humans and Machines Join Forces in Threat Response
* Patch Tuesday - January 2022
* CVE-2021-20038..42: SonicWall SMA 100 Multiple Vulnerabilities (FIXED)
* The 2021 Naughty and Nice Lists: Cybersecurity Edition



Advisories

US-Cert Alerts & bulletins

* Microsoft Warns of Destructive Malware Targeting Ukrainian Organizations
* Ivanti Updates Log4j Advisory with Security Updates for Multiple Products
* Juniper Networks Releases Security Updates for Multiple Products
* Citrix Releases Security Updates for Hypervisor
* Apple Releases Security Updates for iOS and iPadOS
* Cisco Releases Security Updates for Multiple Products
* CNMF Identifies and Discloses Malware used by Iranian APT MuddyWater
* Adobe Releases Security Updates for Multiple Products
* AA22-011A: Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infras
* AA21-356A: Mitigating Log4Shell and Other Log4j-Related Vulnerabilities
* Vulnerability Summary for the Week of January 3, 2022
* Vulnerability Summary for the Week of December 27, 2021

Zero Day Initiative Advisories

ZDI-CAN-16202: Bentley
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-01-14, 3 days ago. The vendor is given until 2022-05-14 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-16172: Bentley
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-01-14, 3 days ago. The vendor is given until 2022-05-14 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-15975: Linux
A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Ayaz Mammadov (McYoloSwagHam)' was reported to the affected vendor on: 2022-01-14, 3 days ago. The vendor is given until 2022-05-14 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-16021: GE
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: 2022-01-14, 3 days ago. The vendor is given until 2022-05-14 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-15721: GE
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: 2022-01-14, 3 days ago. The vendor is given until 2022-05-14 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-16171: Bentley

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-01-14, 3 days ago. The vendor is given until 2022-05-14 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-15739: Trend Micro

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 'Amir Ahmadi (@KingAmir)' was reported to the affected vendor on: 2022-01-14, 3 days ago. The vendor is given until 2022-05-14 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-16020: GE

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: 2022-01-14, 3 days ago. The vendor is given until 2022-05-14 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-16023: GE

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: 2022-01-14, 3 days ago. The vendor is given until 2022-05-14 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-16164: Zoom

A CVSS score 7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by '@Kharosx0' was reported to the affected vendor on: 2022-01-13, 4 days ago. The vendor is given until 2022-05-13 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-15635: Cisco

A CVSS score 4.3 (AV:A/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-01-12, 5 days ago. The vendor is given until 2022-05-12 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-12551: Oracle

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 'Anonymous' was reported to the affected vendor on: 2022-01-12, 5 days ago. The vendor is given until 2022-05-12 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-15634: Cisco

A CVSS score 4.3 (AV:A/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-01-12, 5 days ago. The vendor is given until 2022-05-12 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-15361: Docker

A CVSS score 7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Hashim Jawad (@ihack4falafel)' was reported to the affected vendor on: 2022-01-12, 5 days ago. The vendor is given until 2022-05-12 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-15636: Cisco

A CVSS score 4.3 (AV:A/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L) severity vulnerability discovered by 'Anonymous'

was reported to the affected vendor on: 2022-01-12, 5 days ago. The vendor is given until 2022-05-12 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-15768: GE

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: 2022-01-12, 5 days ago. The vendor is given until 2022-05-12 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-15708: GE

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: 2022-01-12, 5 days ago. The vendor is given until 2022-05-12 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-15766: GE

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: 2022-01-12, 5 days ago. The vendor is given until 2022-05-12 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-15707: GE

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: 2022-01-12, 5 days ago. The vendor is given until 2022-05-12 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-15725: GE

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: 2022-01-12, 5 days ago. The vendor is given until 2022-05-12 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-15720: GE

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: 2022-01-12, 5 days ago. The vendor is given until 2022-05-12 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-15706: GE

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: 2022-01-12, 5 days ago. The vendor is given until 2022-05-12 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-15709: GE

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: 2022-01-12, 5 days ago. The vendor is given until 2022-05-12 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-15767: GE

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: 2022-01-12, 5 days ago. The vendor is given until 2022-05-12 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 2022-0138-06

Red Hat Security Advisory 2022-0138-06 - Red Hat AMQ Streams, based on the Apache Kafka project, offers a distributed backbone that allows microservices and other applications to share data with extremely high throughput and extremely low latency. This release of Red Hat AMQ Streams 2.0.0 serves as a replacement for Red Hat AMQ Streams 1.8.4, and includes security and bug fixes, and enhancements. Issues addressed include bypass and code execution vulnerabilities.

Ubuntu Security Notice USN-5227-1

Ubuntu Security Notice 5227-1 - It was discovered that Pillow incorrectly handled certain image files. If a user or automated system were tricked into opening a specially-crafted file, a remote attacker could cause Pillow to hang, resulting in a denial of service. It was discovered that Pillow incorrectly handled certain image files. If a user or automated system were tricked into opening a specially-crafted file, a remote attacker could cause Pillow to crash, resulting in a denial of service. This issue ony affected Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, and Ubuntu 21.04.

Ubuntu Security Notice USN-5224-2

Ubuntu Security Notice 5224-2 - USN-5224-1 fixed several vulnerabilities in Ghostscript. This update provides the corresponding update for Ubuntu 16.04 ESM. It was discovered that Ghostscript incorrectly handled certain PostScript files. If a user or automated system were tricked into processing a specially crafted file, a remote attacker could possibly use this issue to cause Ghostscript to crash, resulting in a denial of service, or possibly execute arbitrary code.

Ubuntu Security Notice USN-5223-1

Ubuntu Security Notice 5223-1 - It was discovered that Apache Log4j 1.2 was vulnerable to deserialization of untrusted data if the configuration file was editable. An attacker could use this vulnerability to cause a DoS or possibly execute arbitrary code.

Red Hat Security Advisory 2022-0124-04

Red Hat Security Advisory 2022-0124-04 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.5.0 ESR. Issues addressed include buffer overflow, bypass, spoofing, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-0026-06

Red Hat Security Advisory 2022-0026-06 - 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 4.6.53. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-0125-03

Red Hat Security Advisory 2022-0125-03 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.5.0 ESR. Issues addressed include buffer overflow, bypass, spoofing, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-0123-02

Red Hat Security Advisory 2022-0123-02 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.5.0. Issues addressed include buffer overflow, bypass, spoofing, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-0126-03

Red Hat Security Advisory 2022-0126-03 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.5.0 ESR. Issues addressed include buffer overflow, bypass, spoofing, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-0128-02

Red Hat Security Advisory 2022-0128-02 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.5.0. Issues addressed include buffer overflow, bypass, spoofing, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-0130-03

Red Hat Security Advisory 2022-0130-03 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.5.0 ESR. Issues addressed include buffer overflow, bypass, spoofing, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-0129-02

Red Hat Security Advisory 2022-0129-02 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.5.0. Issues addressed include buffer overflow, bypass, spoofing, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-0131-02

Red Hat Security Advisory 2022-0131-02 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.5.0. Issues addressed include buffer overflow, bypass, spoofing, and use-after-free vulnerabilities.

Ubuntu Security Notice USN-5226-1

Ubuntu Security Notice 5226-1 - It was discovered that systemd-tmpfiles employed uncontrolled recursion when removing deeply nested directory hierarchies. A local attacker could exploit this to cause systemd-tmpfiles to crash or have other unspecified impacts.

Ubuntu Security Notice USN-5210-2

Ubuntu Security Notice 5210-2 - USN-5210-1 fixed vulnerabilities in the Linux kernel. Unfortunately, that update introduced a regression that caused failures to boot in environments with AMD Secure Encrypted Virtualization enabled. This update fixes the problem.

Red Hat Security Advisory 2022-0132-03

Red Hat Security Advisory 2022-0132-03 - Mozilla Firefox is an open-source web browser, designed for standards compliance, performance, and portability. This update upgrades Firefox to version 91.5.0 ESR. Issues addressed include buffer overflow, bypass, spoofing, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-0133-04

Red Hat Security Advisory 2022-0133-04 - The redhat-virtualization-host packages provide the Red Hat Virtualization Host. These packages include redhat-release-virtualization-host, ovirt-node, and rhev-hypervisor. Red Hat Virtualization Hosts are installed using a special build of Red Hat Enterprise Linux with only the packages required to host virtual machines. RHVH features a Cockpit user interface for monitoring the host's resources and performing administrative tasks.

Apple Security Advisory 2022-01-12-1

Apple Security Advisory 2022-01-12-1 - iOS 15.2.1 and iPadOS 15.2.1 addresses denial of service and resource exhaustion vulnerabilities.

Red Hat Security Advisory 2022-0127-02

Red Hat Security Advisory 2022-0127-02 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.5.0. Issues addressed include buffer overflow, bypass, spoofing, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-0024-04

Red Hat Security Advisory 2022-0024-04 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.6.53.

Ubuntu Security Notice USN-5225-1

Ubuntu Security Notice 5225-1 - It was discovered that lxml incorrectly handled certain XML and HTML files. An attacker could possibly use this issue to execute arbitrary code.

Ubuntu Security Notice USN-5224-1

Ubuntu Security Notice 5224-1 - It was discovered that Ghostscript incorrectly handled certain PostScript files. If a user or automated system were tricked into processing a specially crafted file, a remote attacker could possibly use this issue to cause Ghostscript to crash, resulting in a denial of service, or possibly execute arbitrary code.

Red Hat Security Advisory 2022-0072-05

Red Hat Security Advisory 2022-0072-05 - The kernel packages contain the Linux kernel, the core of any Linux operating system.

Red Hat Security Advisory 2022-0065-05

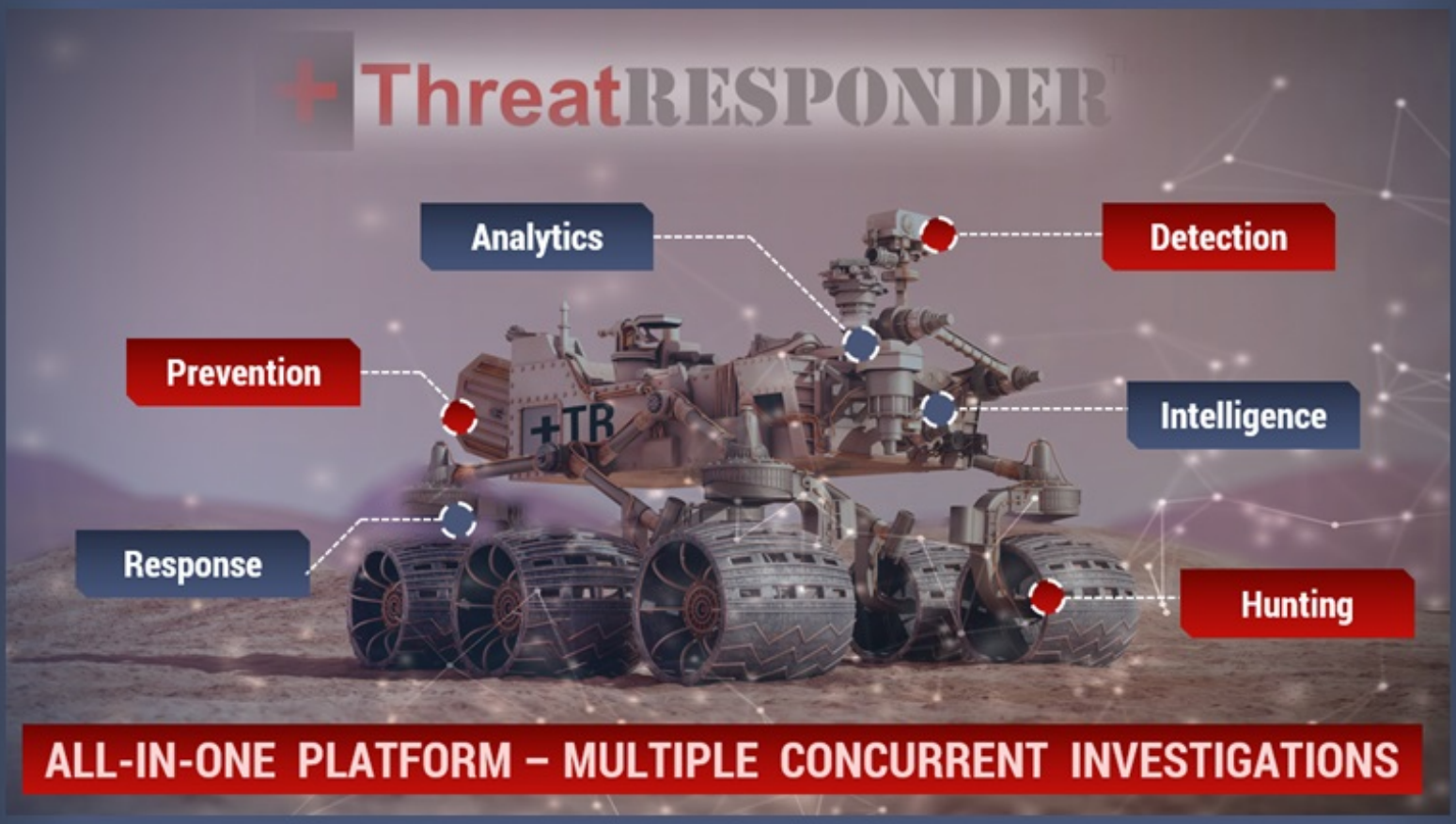
Red Hat Security Advisory 2022-0065-05 - The kernel-rt packages provide the Real Time Linux Kernel, which enables fine-tuning for systems with extremely high determinism requirements. Issues addressed include a buffer overflow vulnerability.

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



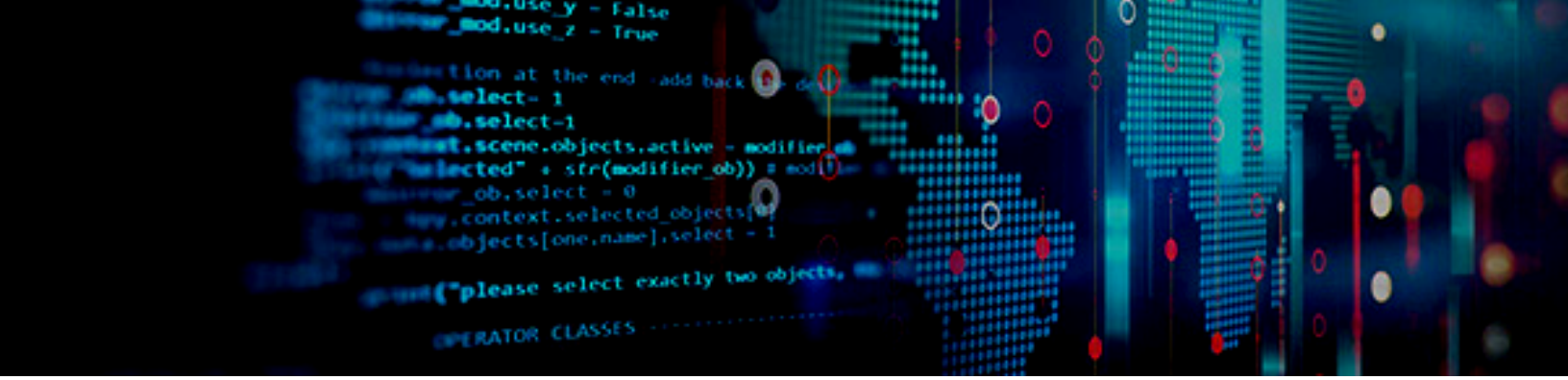
The Solution – ThreatResponder® Platform

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

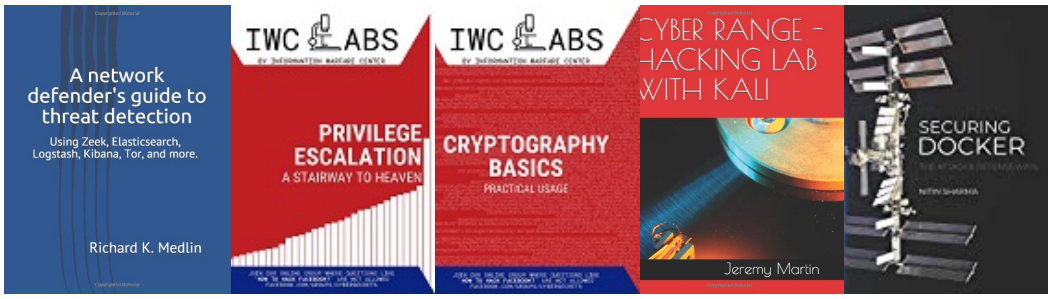


The Cyber Secrets publications on Amazon

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