Feb-02-22

CYBER WEEKLY AWARENESS REPORT

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

ARGOS
APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity

February 2, 2022

The Cyber WAR (Weekly Awareness Report) is an Open Source Intelligence AKA OSINT resource focusing on advanced persistent threats and other digital dangers received by over ten thousand individuals. APTs fit into a cybercrime category directed at both business and political targets. Attack vectors include system compromise, social engineering, and even traditional espionage. Included are clickable links to news stories, vulnerabilities, exploits, & other industry risk.

Summary

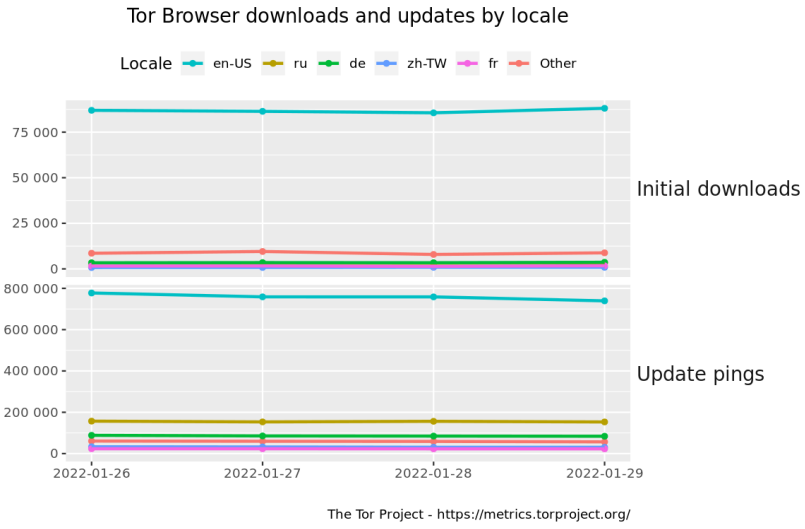
Internet Storm Center Infocon Status

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

Other IWC Publications

Cyber Secrets books and ebook series can be found on Amazon.com at. amzn.to/2UuIG9B

Cyber Secrets was originally a video series and is on both YouTube.



Interesting News

* Free Cyberforensics Training - CSI Linux Basics

Download the distro and take the course to learn what CSI Linux can add to your arsenal. This include a case management solution, document templates (reports and legal docs), and more GUI options for gathering digital evidence while storing it to the ongoing case.
https://training.csilinux.com/course/view.php?id=5

* * Our active Facebook group discusses the gambit of cyber security issues. Join the Cyber Secrets Facebook group here.

Index of Sections

Packet Storm Security

* Cyber Attack Strikes German Fuel Supplies
* Apple Pays $100.5K Bug Bounty For Mac Webcam Hack
* NSO Group Pegasus Spyware Aims At Finnish Diplomats
* FBI Urges Temporary Phones For Olympic Athletes
* Top US Spy Warns Too Many Government Secrets Harms National Security
* Smart-Chain Financial Site Qubit Hacked For $80 Million
* What To Do To Delete The Scary Amount Of Data Google Has On You
* Unsecured AWS Server Exposed 3TB In Airport Employee Records
* Shipment Delivery Scams Become The Favored Way To Spread Malware
* 2FA App With 10,000 Google Play Downloads Loaded Well-Known Banking Trojan
* US Bans Telecom Giant China Unicom Over Spying Concerns
* Intel Fails To Get Spectre, Meltdown Class Action Suits Thrown Out
* Microsoft Fends Off Record Breaking 3.47Tbps DDoS Attack
* Indonesia Bars Financial Institutions From Offering Crypto Services
* Let's Encrypt To Revoke About 2 Million HTTPS Certificates In Two Days
* DeepDotWeb Operator Sentenced To Eight Years Behind Bars
* Apple Fixes 2 Zero-Day Security Bugs, One Exploited In the Wild
* Kentucky Hospital Reports Network Outage, Care Delays Amid Cyberattack
* Chinese Hackers Target German Pharma And Tech Firms
* What Enterprises Should Learn From Merck's $1.4 Billion Insurance Lawsuit
* New York Fines EyeMed $600k After Data Breach Investigation Finds Security Flaws
* Threat Actors Blanket Androids With Flubot, Teabot Campaigns
* A Bug Lurking For 12 Years Gives Attackers Root On Every Major Linux Distro
* Apple Pays Researcher $100k For Safari Vulnerability
* People Are Still Getting Pwned A Week After A Crypto Hack Was Contained

Krebs on Security

* Fake Investor John Bernard Sinks Norwegian Green Shipping Dreams
* Who Wrote the ALPHV/BlackCat Ransomware Strain?
* Scary Fraud Ensues When ID Theft & Usury Collide
* Crime Shop Sells Hacked Logins to Other Crime Shops
* IRS Will Soon Require Selfies for Online Access
* 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

Dark Reading

* Secure Web Browsers Tackle Ransomware, Insider Threat in Enterprises
* ThycoticCentrify Renamed Delinea
* Nucleus Security Forms Strategic Partnership with Mandiant
* Vectra Acquires Siriux Security Technologies to Extend Leadership in Identity and SaaS Threat Managem
* Forescout Acquires CyberMDX to Expand Healthcare Cybersecurity Focus
* Ping Identity Launches PingOne DaVinci
* Digital Shadows Launches New Vulnerability Intelligence Module
* Disclosure, Panic, Patch: Can We Do Better?
* ShiftLeft CORE 'Velocity Update' Streamlines Triage, Automates Build Security Controls
* 7 Red Flags That Can Stop Your Company From Becoming a Unicorn
* Complexity vs. Capability: How to Bridge the Security Effectiveness Gap
* Qualys Adds Advanced Remediation Capabilities to Minimize Vulnerability Risk
* Mastercard Launches Global Cybersecurity Alliance Program to Further Secure The Digital Ecosystem
* Critical Log4j Vulnerabilities Are the Ultimate Gift for Cybercriminals
* NortonLifeLock Introduces Social Media Monitoring
* Coalition Launches Executive Risks Products With Personalized Risk Assessment
* Cymulate Launches Service to Augment In-House Security Teams
* Security Service Edge Boosters Form New Forum to Encourage Adoption
* Mandiant: 1 in 7 Ransomware Extortion Attacks Exposes OT Data
* BlackBerry Agrees to Sell Legacy Patents for $600M

The Hacker News

* Dozens of Security Flaws Discovered in UEFI Firmware Used by Several Vendors
* Hacker Group 'Moses Staff' Using New StrifeWater RAT in Ransomware Attacks
* Critical Bug Found in WordPress Plugin for Elementor with Over a Million Installations
* SolarMarker Malware Uses Novel Techniques to Persist on Hacked Systems
* Iranian Hackers Using New PowerShell Backdoor in Cyber Espionage Attacks
* Ukraine Continues to Face Cyber Espionage Attacks from Russian Hackers
* Reasons Why Every Business is a Target of DDoS Attacks
* Researchers Uncover New Iranian Hacking Campaign Targeting Turkish Users
* New SureMDM Vulnerabilities Could Expose Companies to Supply Chain Attacks
* New Samba Bug Allows Remote Attackers to Execute Arbitrary Code as Root
* Behind The Buzzword: Four Ways to Assess Your Zero Trust Security Posture
* Your Graphics Card Fingerprint Can Be Used to Track Your Activities Across the Web
* German Court Rules Websites Embedding Google Fonts Violates GDPR
* Researchers Use Natural Silk Fibers to Generate Secure Keys for Strong Authentication
* Apple Pays $100,500 Bounty to Hacker Who Found Way to Hack MacBook Webcam

Security Week

* Forescout Acquires Healthcare Cybersecurity Firm CyberMDX
* RIPTA Data Breach Affected About 22,000 People
* Newly Detected "StrifeWater" RAT Linked to Iranian APT
* Think Big, Start Small, Move Fast: Applying Lessons From The Mayo Clinic to Cybersecurity
* Israeli Police: Possible Improper Surveillance by Our Own
* OpenSSF Alpha-Omega Project Tackles Supply Chain Security
* Two Dozen UEFI Vulnerabilities Impact Millions of Devices From Major Vendors
* British Council Student Data Found in Unprotected Database
* Germany: 2 Oil Storage and Supply Firms Hit by Cyberattack
* Iranian Hackers Using New PowerShell Backdoor Linked to Memento Ransomware
* Critical Flaw Impacts WordPress Plugin With 1 Million Installations
* Cybersecurity M&A Roundup: 32 Deals Announced in January 2022
* CISA Adds Recent iOS, SonicWall Vulnerabilities to 'Must Patch' List
* 'White Tur' Hacking Group Borrows Techniques From Multiple APTs
* Cyber Insights 2022: Improving Criminal Sophistication
* OT Data Stolen by Ransomware Gangs Can Facilitate Cyber-Physical Attacks
* Cyberattacks Increasingly Hobble Pandemic-Weary US Schools
* North Korean Hackers Abuse Windows Update Client in Attacks on Defense Industry
* More Russian Attacks Against Ukraine Come to Light
* The Third Building Block for the SOC of the Future: Balanced Automation
* SureMDM Vulnerabilities Exposed Companies to Supply Chain Attacks
* CISA's 'Must Patch' List Puts Spotlight on Vulnerability Management Processes
* Israeli Lawyer, Hungarian Rights Group Target Pegasus Spyware
* Finnish Diplomats Targeted by Pegasus Spyware: Ministry
* Network Security Firm Portnox Raises $22 Million in Series A Funding

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* COVID-19 Test-Related Phishing Scams Jump 521% Into January
* 8 New Malware Payloads Spotted As Part of Attacks Against Ukrainian Targets
* New Phishing Campaign is Impersonating Zoom to Steal Credentials
* CyberheistNews Vol 12 #05 [Heads Up] DHS Sounds Alarm on New Russian Destructive Disk Wiper Attack Po
* Beware of QuickBooks Payment Scams
* Increased "Shipping Delays" Now Served as Phishbait
* KnowBe4 Continues to be One of Okta's Most Popular Apps in the 2021 Businesses at Work Report
* A Data-Driven Approach for Your Third-Party Risk Management Processes
* Microsoft Warns of Latest "Consent Phishing" Attack Intent on Reading Your Email
* Dark Web Service Sells Access to Compromised Accounts and Browser Sessions

ISC2.org Blog

* THE STAKES HAVE NEVER BEEN HIGHER: HOW TO EXPAND THE CYBER WORKFORCE
* HOW TO BECOME AN (ISC)² VOLUNTEER AND MAKE A DIFFERENCE IN THE CYBERSECURITY COMMUNITY
* Why is cybersecurity one of the best fields for young people to enter?
* REGISTER TODAY FOR THE (ISC)² ENTRY-LEVEL CYBERSECURITY CERTIFICATION PILOT EXAM
* TIME TO HIT THE BOOKS! TRAINING COURSE IS AVAILABLE FOR CANDIDATES PREPARING FOR THE NEW (ISC)²

HackRead

* BRATA Android malware factory resets phones after stealing funds
* SaaS Security Guide: How to Protect Your SaaS Business
* Security giant exposed 3TB of sensitive airport & employees data
* Key Features Of Threat Intelligence Platforms
* Microsoft Azure customer hit by largest ever 3.47 Tbps DDoS attack
* What is WooCommerce, and Why You Should Care
* LockBit ransomware hits French Ministry of Justice & European firms

Koddos

* BRATA Android malware factory resets phones after stealing funds
* SaaS Security Guide: How to Protect Your SaaS Business
* Security giant exposed 3TB of sensitive airport & employees data
* Key Features Of Threat Intelligence Platforms
* Microsoft Azure customer hit by largest ever 3.47 Tbps DDoS attack
* What is WooCommerce, and Why You Should Care

* LockBit ransomware hits French Ministry of Justice & European firms

Naked Security

* Linux kernel patches "performance can be harmful" bug in video driver
* Website operator fined for using Google Fonts "the cloudy way"
* Coronavirus SMS scam offers home PCR testing devices - don't fall for it!
* Happy Data Privacy Day - and we really do mean "happy" :-)
* Apple fixes Safari data leak (and patches a zero-day!) - update now
* S3 Ep67: Tax scams, carder busts and crypto capers [Podcast + Transcript]
* "PwnKit" security bug gets you root on most Linux distros - what to do
* Tax scam emails are alive and well as US tax season starts
* Alleged carder gang mastermind and three acolytes under arrest in Russia
* Cryptocoin broker Crypto.com says 2FA bypass led to $35m theft

Threat Post

* FBI: Use a Burner Phone at the Olympics
* Unpatched Security Bugs in Medical Wearables Allow Patient Tracking, Data Theft
* The Account Takeover Cat-and-Mouse Game
* Samba 'Fruit' Bug Allows RCE, Full Root User Access
* Living Off the Land: How to Defend Against Malicious Use of Legitimate Utilities
* Public Exploit Released for Windows 10 Bug
* Apple Pays $100.5K Bug Bounty for Mac Webcam Hack
* NSO Group Pegasus Spyware Aims at Finnish Diplomats
* Lazarus APT Uses Windows Update to Spew Malware
* Zerodium Spikes Payout for Zero-Click Outlook Zero-Days

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

* Go language adds much-anticipated generics
* How SQL can unify access to APIs
* 3 multicloud myths that cloud pros still believe
* Deno 1.18 completes Web Crypto API
* "Do More with R" video tutorials
* Do you need a cloud center of excellence?
* The cloud is too big for one winner
* Google releases differential privacy pipeline for Python
* Roblox's cloud-native catastrophe: A post mortem
* Microsoft .NET Community Toolkit backs .NET 6

C4ISRNET - Media for the Intelligence Age Military

* British military plans to spend big on space, but some wonder if it's enough
* Ukraine seeks closer ties with NATO on cyber defense
* Space weather sensor passes final design review
* NSA's cybersecurity directorate looks to scale up this year
* AT&T sees progress in Navy's 5G smart warehouse experiment
* Here's how intelligence agencies can search foreign documents without learning the language
* DoD must focus on skilled cyber defenders, not just new tech, warns weapons tester
* US Army's tactical network must overcome several challenges, says Pentagon weapons tester
* Empower our Space Force, just as we do for the other armed services
* US Navy adopts new strategy prioritizing 'the building blocks' of unmanned tech

The Hacker Corner

Conferences

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

Google Zero Day Project

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

Capture the Flag (CTF)

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

* DiceCTF 2022
* 24h@CTF
* Cyber Grabs CTF 0x03 Junior
* STAY ~/ CTF 2022
* DefCamp CTF 2122 Online
* 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

* Falco 0.31.0
* OpenStego Free Steganography Solution 0.8.3
* Zeek 4.2.0
* American Fuzzy Lop plus plus 4.00c
* Lynis Auditing Tool 3.0.7
* Logwatch 7.6
* GRAudit Grep Auditing Tool 3.3
* AIDE 0.17.4
* Clam AntiVirus Toolkit 0.104.2
* Proxmark3 4.14831

Kali Linux Tutorials

* STEWS : A Security Tool For Enumerating Web Sockets
* Toutatis : A Tool That Allows You To Extract Information From Instagram Accounts Such As E-Mails, Pho
* Forbidden : Bypass 4Xx HTTP Response Status Codes
* AirStrike : Automatically Grab And Crack WPA-2 Handshakes With Distributed Client-Server Architecture
* IAM Vulnerable : Use Terraform To Create Your Own Vulnerable By Design AWS IAM Privilege Escalation P
* IDA2Obj : Static Binary Instrumentation
* DLLHijackingScanner : This Is A PoC For Bypassing UAC Using DLL Hijacking And Abusing The "Trusted Di
* ClusterFuzzLite : Simple Continuous Fuzzing That Runs In CI
* Crawpy : Yet Another Content Discovery Tool
* Kerberoast : Kerberoast Attack -Pure Python-

GBHackers Analysis

* OpenSubtitles Hacked - Over 7 million Subscribers Email, IP Addresses & Usernames Leaked
* Critical Flaw With Zoho Desktop Central Let Attackers to Bypass Authentication
* Chinese Hackers Exploiting Log4Shell Vulnerability & Attack Internet-Facing Systems
* Bugs With URL Parsing Libraries Could Allow DoS, RCE, Spoofing & More
* 5 Most Fearsome Hacks in 2022

Weekly Cyber Security Video and Podcasts

SANS DFIR

* Network Forensics: Tools of the Trade… At Scale and on a Budget
* SANS Threat Analysis Rundown
* SANS Threat Analysis Rundown
* Inside FOR608: Enterprise-Class Incident Response & Threat Hunting - Course Preview

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

* The Biggest DDoS In History - ThreatWire
* Introducing the OMG Plug
* How Deauth Attacks Jam WiFi Devices | HakByte

The PC Security Channel [TPSC]

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

Eli the Computer Guy

* ELVIRA ATTACKS JOE ROGAN and SPOTIFY - geezers unite!
* LINUS TECH TIPS says ADBLOCK IS PIRACY - after getting paid to do videos on how to use adblock
* NEW COVID VARIANT EVEN MORE INFECTIOUS - 1.5 times gazillion worse
* JOE ROGAN COSTS SPOTIFY $2 BILLION - or spotify is just failing

Security Now

* The "Topics” API - PwnKit Tech Details, DrawnApart, Zerodium Bug Bounties, Log4Shell Hits Ubiquiti
* Inside the NetUSB Hack - Log4J Update, Cyber-Insurance and Ransomware, EU Bug Bounty Programs

Troy Hunt

* Weekly Update 280

Intel Techniques: The Privacy, Security, & OSINT Show

* 248-Privacy vs. COVID
* 247-Weekly Recap

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Packet Storm New Exploits For January, 2022
* Cisco Small Business RV Series Authentication Bypass / Command Injection
* Moxa TN-5900 Post Authentication Command Injection
* Moxa TN-5900 Firmware Upgrade Checksum Validation
* Backdoor.Win32.Tiny.c Code Execution
* HackTool.Win32.Muzzer.a Buffer Overflow
* Fetch Softworks Fetch FTP Client 5.8 Denial Of Service
* WordPress RegistrationMagic V 5.0.1.5 SQL Injection
* WordPress Modern Events Calendar 6.1 SQL Injection
* PolicyKit-1 0.105-31 Privilege Escalation
* Oracle WebLogic Server 14.1.1.0.0 Local File Inclusion
* WordPress Mortgage Calculators WP 1.52 Cross Site Scripting
* Linux Kernel Slab Out-Of-Bounds Write
* Linux Kernel Slab Out-Of-Bounds Write
* Polkit pkexec CVE-2021-4034 Local Root
* Polkit pkexec CVE-2021-4034 Proof Of Concept
* Backdoor.Win32.WinShell.50 Weak Hardcoded Password
* Polkit pkexec CVE-2021-4034 Local Root
* Grandstream UCM62xx IP PBX sendPasswordEmail Remote Code Execution
* Ethercreative Logs 3.0.3 Path Traversal
* CosaNostra Builder WebPanel Cross Site Request Forgery
* uBidAuction 2.0.1 Cross Site Scripting
* FAUST iServer 9.0.018.018.4 Local File Inclusion
* CosaNostra Builder WebPanel Insecure Cryptographic Storage
* Xerox Versalink Denial Of Service

CXSecurity

* Fetch Softworks Fetch FTP Client 5.8 Denial Of Service
* VMware vCenter Server Unauthenticated Log4Shell JNDI Injection Remote Code Execution
* Grandstream GXV3175 Unauthenticated Command Execution
* Worktime 10.20 Build 4967 DLL Hijacking
* SonicWall SMA 100 Series Authenticated Command Injection
* Log4Shell HTTP Header Injection
* Automox Agent 32 Local Privilege Escalation

Proof of Concept (PoC) & Exploits

Exploit Database

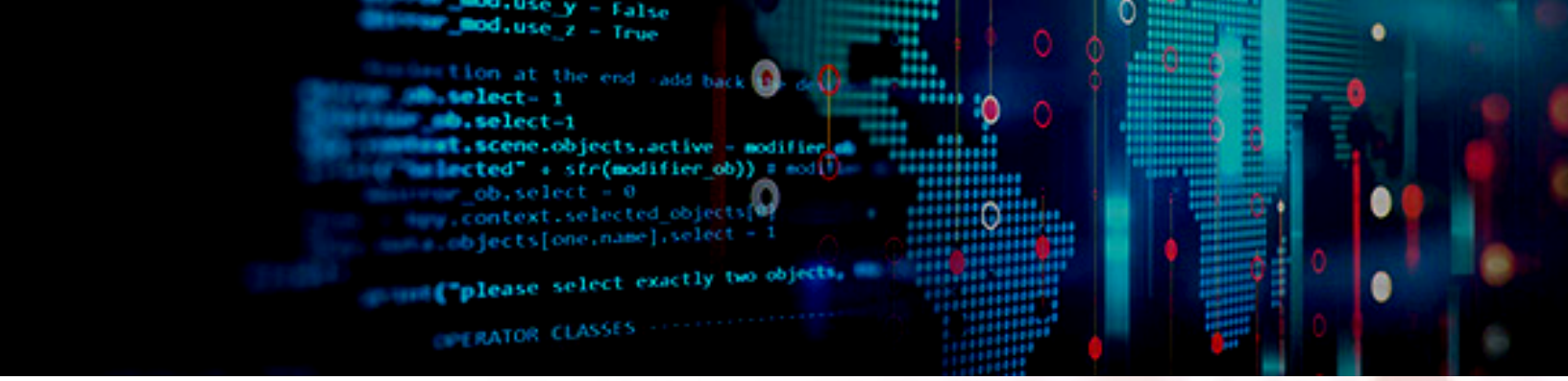
* [webapps] PHP Restaurants 1.0 - SQLi (Unauthenticated)
* [webapps] Wordpress Plugin 404 to 301 2.0.2 - SQL-Injection (Authenticated)
* [webapps] WordPress Plugin Domain Check 1.0.16 - Reflected Cross-Site Scripting (XSS) (Authenticated)
* [local] Fetch Softworks Fetch FTP Client 5.8 - Remote CPU Consumption (Denial of Service)
* [webapps] Wordpress Plugin Download Monitor WordPress V 4.4.4 - SQL Injection (Authenticated)
* [webapps] Chamilo LMS 1.11.14 - Account Takeover
* [webapps] uBidAuction v2.0.1 - 'Multiple' Cross Site Scripting (XSS)
* [webapps] Ametys CMS v4.4.1 - Cross Site Scripting (XSS)
* [local] Mozilla Firefox 67 - Array.pop JIT Type Confusion
* [local] CONTPAQi(R) AdminPAQ 14.0.0 - Unquoted Service Path
* [local] PolicyKit-1 0.105-31 - Privilege Escalation
* [remote] Oracle WebLogic Server 14.1.1.0.0 - Local File Inclusion
* [webapps] WordPress Plugin Modern Events Calendar V 6.1 - SQL Injection (Unauthenticated)
* [webapps] WordPress Plugin RegistrationMagic V 5.0.1.5 - SQL Injection (Authenticated)
* [webapps] WordPress Plugin Mortgage Calculators WP 1.52 - Stored Cross-Site Scripting (XSS) (Authenti
* [webapps] PHPIPAM 1.4.4 - SQLi (Authenticated)
* [webapps] Online Project Time Management System 1.0 - Multiple Stored Cross Site Scripting (XSS) (Aut
* [webapps] Online Project Time Management System 1.0 - SQLi (Authenticated)
* [webapps] Landa Driving School Management System 2.0.1 - Arbitrary File Upload
* [webapps] Affiliate Pro 1.7 - 'Multiple' Cross Site Scripting (XSS)
* [webapps] Rocket LMS 1.1 - Persistent Cross Site Scripting (XSS)
* [webapps] uDoctorAppointment v2.1.1 - 'Multiple' Cross Site Scripting (XSS)
* [webapps] Creston Web Interface 1.0.0.2159 - Credential Disclosure
* [webapps] Nyron 1.0 - SQLi (Unauthenticated)
* [webapps] Simple Chatbot Application 1.0 - 'message' Blind SQLi

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*

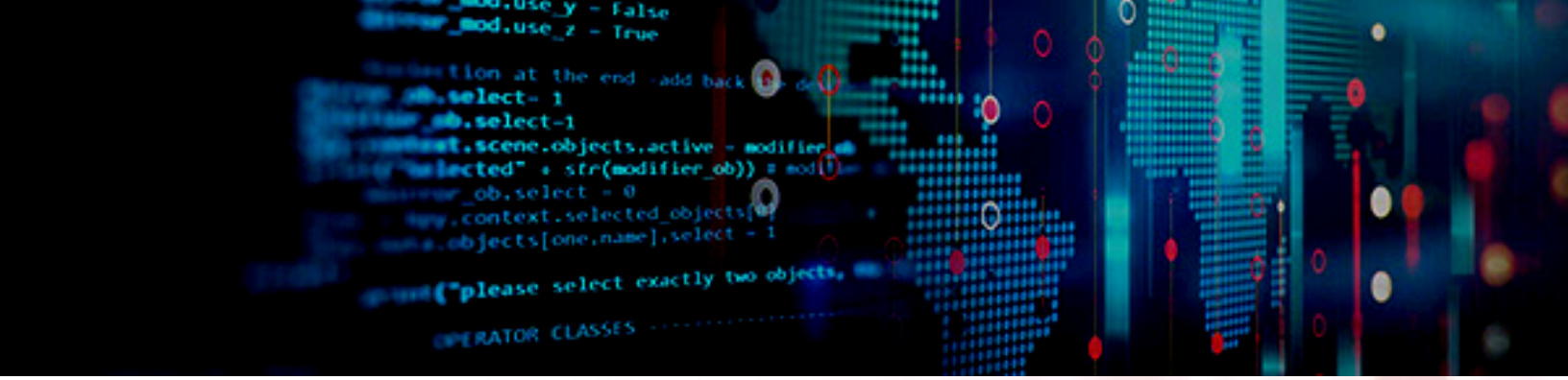
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://merida.gob.ve/b4.html
http://merida.gob.ve/b4.html notified by 0x1998
http://dinkes.pamekasankab.go.id/readme.html
http://dinkes.pamekasankab.go.id/readme.html notified by 0x1998
http://mdfi.gov.ua/b4.html
http://mdfi.gov.ua/b4.html notified by 0x1998
https://hsr.moh.gov.my
https://hsr.moh.gov.my notified by Kareem_Hacker
https://htaiping.moh.gov.my
https://htaiping.moh.gov.my notified by Kareem_Hacker
https://qeh.moh.gov.my
https://qeh.moh.gov.my notified by Kareem_Hacker
https://hsetiu.moh.gov.my
https://hsetiu.moh.gov.my notified by Kareem_Hacker
https://hpontian.moh.gov.my
https://hpontian.moh.gov.my notified by Kareem_Hacker
https://hsip.moh.gov.my
https://hsip.moh.gov.my notified by Kareem_Hacker
https://seguridad.gob.hn
https://seguridad.gob.hn notified by F4k3-ScR!pT (Bangladeshi Hacker)
https://policianacional.gob.hn/fake.php
https://policianacional.gob.hn/fake.php notified by F4k3-ScR!pT (Bangladeshi Hacker)
https://fmckatsina.gov.ng/fake.php
https://fmckatsina.gov.ng/fake.php notified by F4k3-ScR!pT (Bangladeshi Hacker)
http://municanchis.gob.pe/fake.php
http://municanchis.gob.pe/fake.php notified by F4k3-ScR!pT (Bangladeshi Hacker)
http://cdcerrito.gob.ar/kurd.html
http://cdcerrito.gob.ar/kurd.html notified by 0x1998
http://pustaka.pn-calang.go.id/repository/krz.txt
http://pustaka.pn-calang.go.id/repository/krz.txt notified by Mr.Kro0oz.305
http://perpustakaan.pn-amlapura.go.id/repository/krz.txt
http://perpustakaan.pn-amlapura.go.id/repository/krz.txt notified by Mr.Kro0oz.305
http://www.scac.go.ke
http://www.scac.go.ke notified by 1877



Dark Web News

Darknet Live

CipherTrace Uses Honeypots

CipherTrace, a blockchain intelligence company owned by Mastercard, uses "honeypots” to gather information about Bitcoin addresses, according promotional material sent to a government official. A Freedom of Information Act (FOIA) request from CoinDesk asked the Treasury for emails that "included the word 'cryptocurrency' or several synonyms ('virtual currency,' 'digital asset,' etc.) or mentioned prominent companies in the industry like Coinbase or Ripple.” In the trove of documents received nine months later, CoinDesk found an email sent to then-Treasury Secretary Steven Mnuchin by the CEO and co-founder of CipherTrace. FOIAd CipherTrace Slides The slide contained a graphic not found on their public-facing material. The email contained promotional material in the form of slides about the services provided by CipherTrace. Like Chainalysis, CipherTrace advertises "blockchain intelligence” services to the public and private sectors. The slide shared by CoinDesk appears to be part of a set of promotional materials for CipherTrace's "CipherTrace Inspector” suite, which the company describes as: "A suite of powerful and easy-to-use de-anonymization tools for law enforcement. Investigators use this integrated platform to obtain solid evidence on individuals who use Bitcoin to launder money, finance terrorism, or carry out drug dealing, extortion, and other crimes. The intuitive CipherTrace visual environment allows even non-technical agents and analysts to easily identify and trace criminals who attempt to use Bitcoin on the internet to conceal their illicit activities. The platform also supports de-anonymization for more than 800 cryptocurrencies — including Bitcoin Cash, Ethereum, and Litecoin. This de-anonymization capability spans more than 87% of global virtual assets.” A picture of a promotional image from CipherTrace. Unlike the publicly available datasheet and product page for Inspector on the company's website, the slide sent to Mnuchin listed "honeypots” as one of the sources of data used by the company. CipherTrace does not make this information publicly known. As a result, we do not know anything about CipherTrace's honeypots. Chainalysis as a honeypot example However, unrelated slides from a Chainalysis presentation to Italian police revealed the way Chainalysis used a honeypot for years under the radar. CipherTrace's tactics could resemble those employed by the industry leader, Chainalysis. Somebody leaked Chainalysis material intended for Italian police. The slides, which surfaced on Dark Leaks, the "decentralized information black market,” revealed that Chainalysis collected the I.P. addresses of people who used a block explorer secretly controlled by the company. When a user visits the site and looks at a specific transaction or address, Chainalysis associates their I.P. address with the transaction or address. "Confidential” Slides from Chainalysis In machine-translated English, the relevant part of the slide reads: • Capability: Suspects may use walletexplorer[.]com to monitor transactions rather than checking exchanges directly for fear of leaving a "footprint”: The Exchange "scrapes” the suspects' I.P. address. Chainalysis owns walletexplorer[.]com, and as such, we collect this data_._ • Results (empirical): Using this dataset, we provided law enforcement with meaningful leads related to I.P. data associated with a relevant cryptocurrency address. It is also possible to conduct a reverse lookup on any known I.P. address to identify other BTC

addresses. It can also collect the data of an address of a data form that has yet to transit on the Blockchain - that is, 'The BTC address provided as part of an investigation into a kidnapping or a threat to life - if the suspect checks his own address. (I added emphasis where I suspect the automated translation may have failed. I am not entirely sure what the sentence in italics means. The URLs were also broken by me and appeared without the brackets in the slide.) Wallet Explorer _ __ Before The website's only mention of Chainalysis was a footnote that stated, "the author of WalletExplorer[.]com now works [at Chainalysis] as analyst and programmer.” CoinDesk wrote an article about the slide, prompting Chainalysis to add a privacy policy to the site wherein they identified themselves as its owner. __ After The new privacy policy on WalletExplorer WalletExplorer.com Privacy Notice

Last Updated: October 14, 2021 WalletExplorer.com, a Chainalysis website, is a Bitcoin Blockchain explorer designed to provide easy access to Public Blockchain Data (our "Services”) for our website visitors (our "Visitors”). This Privacy Notice explains how we collect, use, disclose, and otherwise process Blockchain Information and Visitor Information in connection with our Services. This Privacy Notice is not a contract and does not create any legal rights or obligations. Our Collection of Blockchain Information and Visitor Information

Blockchain Information

When we use the term "Blockchain Information” in this Privacy Notice, we mean: Public Blockchain Data: Blockchain is a shared, immutable ledger used to record transactions of assets, like Bitcoin. The Bitcoin Blockchain is a public ledger, meaning anyone in the world can view the transactions recorded on the Bitcoin Blockchain. Our Services are designed to pull the latest publicly-recorded transactions from the Bitcoin Blockchain every 1-2 days to provide our visitors an easy platform to review the following Public Blockchain Data:

Bitcoin Wallet Address: The unique Bitcoin Wallet address from which or to which Bitcoin is transferred.

Bitcoin Wallet Balance: The balance associated with the Bitcoin Wallet address.

Bitcoin Transaction Details: The transaction identifier, Bitcoin Blockchain position for the transaction, date and time of the transaction, amount sent or received, fee amount, Bitcoin Wallet Address of the sender and recipient, and storage size of the transaction.

WalletExplorer Blockchain Data: To make it easier for our Visitors to navigate the Bitcoin Blockchain, we supplement the Public Blockchain Data with the following data elements:

Wallet ID: Bitcoin Wallets may have one address or many addresses. To help our Visitors view Public Blockchain Data for a Bitcoin Wallet with multiple addresses, we use a mathematical function (known as "hashing”) to convert each Bitcoin Wallet address into a unique 16-digit alphanumeric identifier (the "Wallet ID”). Where multiple Bitcoin Wallet addresses contribute to the spending of Bitcoin in a transaction or "co-spend” on a transaction, we assume the addresses must belong to the same owner and link later Wallet IDs to the earliest Wallet ID assigned to an address within the Bitcoin Wallet giving each Bitcoin Wallet a single Wallet ID.

Wallet Name: A Bitcoin Wallet is a program for holding and transacting with Bitcoin. There are many companies that offer Bitcoin Wallets to the public so they can easily transact on the Bitcoin Blockchain. These companies collect a fee from users of their services and collect the fees in a company-owned Bitcoin Wallet. We are sometimes able to identify which Bitcoin Wallet Addresses belong to Bitcoin Wallet companies and, where we are able to do so, we assign a name to that group of addresses that replaces the alphanumeric Wallet ID (the "Wallet Name”). This Wallet Name is shown in lieu of a Wallet ID when available.

Visitor Information

When we use the term "Visitor Information” in this Privacy Notice, we mean the standard technical information we receive from Visitors to our Services when their browsers make a request to our website's servers. Our servers automatically log Visitor Information, including the Internet Protocol (IP) address making the request, the website URL requested (which may contain the Wallet Name, Wallet ID, or Bitcoin Wallet Address associated with the page requested), the Visitor's browser type and version, and other technical details used to ensure the website is delivered in the correct format (such as language and operating system

type). Our Use of Blockchain Information and Visitor Information

To Provide Visitors Our Services

We use Blockchain Information to provide our Services by permitting Visitors to review Blockchain Information either on our website, WalletExplorer.com, or via a dedicated Application Programming Interface (API) which allows our more technical Visitors to review the same Blockchain Information through their own computer processing programs. We use Visitor Information to provide our Services by using the Visitor Information to deliver the requested URL to each Visitor. To Otherwise Operate Our Services

We use Blockchain Information and Visitor Information to optimize Visitor experience with our Services, diagnose errors and problems with existing Services, develop and test new Services, and conduct research and analytics on Service usage and trends. To Exercise or Comply with Legal Obligations or Rights

We use Blockchain Information and Visitor Information to exercise or comply with legal obligations and rights, including in connection with lawful criminal investigation requests. Our Disclosure of Blockchain Information and Visitor Information

Our Other Business Lines

We share Blockchain Information and Visitor Information with our other Chainalysis business lines to help us deliver and improve those services. For example, other Chainalysis business lines may be able to use the information we provide to better connect one Bitcoin Wallet Address to another Bitcoin Wallet Address. Our Service Providers

We engage third parties, such as website hosting providers, to perform certain functions on our behalf in connection with the uses of Blockchain Information and Visitor Information described above. Depending on the function the third party serves, the service provider may process Blockchain Information or Visitor Information on our behalf or have access to Blockchain Information or Visitor Information while performing functions on our behalf. Business Transaction or Reorganization

We may take part in or be involved with a corporate business transaction, such as a merger, acquisition, joint venture, or financing or sale of company assets. We may disclose Blockchain Information and Visitor Information to a third party during negotiation of, in connection with or as an asset in such a corporate business transaction. Blockchain Information and Visitor Information may also be disclosed in the event of insolvency, bankruptcy, or receivership. Legal Obligations and Rights

We may disclose Blockchain Information and Visitor Information to third parties, such as legal advisors and law enforcement: in connection with the establishment, exercise, or defense of legal claims;

to comply with laws or to respond to lawful requests and legal process;

to protect the rights and property of us, our agents, Visitors, and others, including to enforce our agreements, policies, and terms of use;

to detect, suppress, or prevent fraud;

to reduce credit risk and collect debts owed to us;

to protect the health and safety of us, our Visitors, or any person; or

as otherwise required by applicable law.

Consent

We may disclose personal information about you to certain other third parties with your consent. Personal Data

Certain information we process in connection with our Services may qualify as "personal data” or "personal information” under the laws of specific jurisdictions. Please visit our Chainalysis Privacy Policy for information relating to our processing of "personal data” and "personal information” and any rights you may have in relation to such data. Children's Information

Our Services are not directed to, and we do not intend to, or knowingly, collect or solicit information from children under the age of 13. If you are under the age of 13, please do not use our Services or otherwise provide us with any information either directly or by other means. If a child under the age of 13 has provided information to us, we encourage the child's parent or guardian to contact us to request that we remove the personal information from our systems. If we learn that any information we collect has been provided by a child under the age of 13, we will promptly delete that information. Third-Party Websites

Our Services may include links to third-party websites, plug-ins and applications. Except where we post, link to or expressly adopt or refer to this Privacy Notice, this Privacy Notice does not apply to, and we are not responsible for, any data practices of third-party websites and online services or the practices of other third parties. To learn about the data practices of third parties, please visit their respective privacy notices. Updates to This Privacy Notice

We will update this Privacy Notice from time to time. When we make changes to this Privacy Notice, we will change the "Last Updated” date at the beginning of this Privacy Notice. If we make material changes to this Privacy Notice, we will notify you by prominent posting on the Services, or through other appropriate communication channels. All changes shall be effective from the date of publication unless otherwise provided.

CoinDesk emailed the company to ask about their use of honeypots. In response, CipherTrace sent, "A 'crypto money pot' or 'honeypot' is a security term referring to a mechanism that creates a virtual trap to lure would-be-attackers.” I do not know what kind of honeypot(s) CipherTrace is using. Another block explorer website? Could they succesfully run a Bitcoin mixer? I expect any honeypot would need to provide as much data or the same type of data as Chainalysis' WalletExplorer. CipherTrace has appeared on Darknetlive in the past, as many will remember. They provided the feds with a set of "Monero tracing” tools ("tracing” seems like a stretch but they used those words). They have two patents for tracing Monero. And they highlighted the movement of 69,370 Bitcoins in 2020 that someone had originally stolen from the Silk Road many years ago. A few days later, the feds announced they had tracked down the hacker, identified in court documents only as "Individual X,” and somehow "convinced” the individual to forfeit the Bitcoin to the U.S. government. Also, CipherTrace is owned by Mastercard now and does business with the largest defense contractor in Europe, BAE Systems. It seems like they were a small-ish startup not long ago. Amazing. They do have a neat Maltego transform though The OP honeypot would be creating a cryptocurrency, encouraging criminal use of your coin, and then charging the federal governnment hundreds of thousands of dollars to trace these transactions. Or do the same thing as the feds… (via darknetlive.com at https://darknetlive.com/post/ciphertrace-uses-honeypots-to-investigate-crypto-wallets/)

Three Sentenced to Prison in "VanillaSurf" Case

Three Manchester men were sentenced to prison for their roles in distributing large quantities of a wide variety of drugs through the darkweb. Drugs seized during execution of a search warrant. The North West Regional Organised Crime Unit (NWROCU) announced that Andrew Moores, Paul Gregory, and Austin "Ozzy” Beckett were sentenced to prison for selling drugs on the darkweb. The defendants pleaded guilty to money laundering and a conspiracy to supply, and export class A and B controlled drugs last year. Through the username "VanillaSurf,” among others, the trio sold cocaine, ecstasy, ketamine, amphetamine, and cannabis. Andrew Moores Investigators with the Metropolitan Police started investigating the vendor account "Vanilla Surf” in November 2019. The Dark Web Operations Team of the NWROCU took control of the investigation after the Encrochat takedown in April 2020. After law enforcement had gained control of the Encrochat network, they learned that three Encrochat users distributed drugs through the Vanilla Surf vendor account as well as "Staxx” and "GovUk.” Austin Beckett The investigators established that Moores had used the EncroChat username "Toxic Jaguar” and was in charge of a drug trafficking operation that distributed drugs through the "Vanilla Surf,” "Staxx,” and "GovUk” vendor accounts. Gregory and Beckett worked for Moores and used the usernames "Matte Soda” and "Real Cake,” respectively, on the Encrochat encrypted network. Beckett was allegedly in charge of the trio's drug distribution center while Gregory handled packaging and shipping. Paul Gregory The execution of search warrants resulted in the seizure of large quantities of drugs, cash, computers, encrypted mobile phones, and cryptocurrency worth approximately Â£30,000. The Manchester Crown Court heard that the investigators found Gregory's DNA on an ecstasy package ordered by law enforcement officers. Drugs seized by police during a search of Beckett's house. The defendants had earned roughly Â£3 million via their drug trafficking operation. They pleaded guilty to conspiracy to supply and export class A and B controlled drugs and money laundering. Judge John Potter sentenced Moore to 16 years and six months in

prison, Gregory to 14 years and four months in prison, and Beckett to 11 years and three months. archiveiya74codqgiixo33q62qlrqtkgmcitqx5u2oeqnmn5bpcbiyd.onion, archive.is, archive.org DNL: Police caught Beckett by coincidence, apparently. They were "going to a house in Hazel Grove to arrest someone unconnected” to these defendants. Police claim that Beckett panicked and moved a suitcase from his house to his neighbor's house. The police, by chance, were interested in Beckett's neighbor and found the suitcase. It contained "a 'large quantity' of drugs including high purity cocaine, as well as scales and other drugs paraphernalia.” (via darknetlive.com at https://darknetlive.com/post/three-sentenced-to-prison-in-vanillasurf-case/)

DeepDotWeb Admin Sentenced to 97 Months in Prison

A federal judge sentenced the administrator of DeepDotWeb.com to 97 months in prison. United States District Court Judge Donetta W. Ambrose sentenced Tal Prihar, 37, to 97 months in federal prison for laundering almost $8.5 million in cryptocurrency. Prihar, in March 2021, pleaded guilty to one count of conspiracy to commit money laundering (18 USC 1956h). In sealed court documents, Prihar admitted to creating the darkweb news site DeepDotWeb.com in 2013. DeepDotWeb (DDW) was the largest darkweb news and general information website between October 2013 and April 2019. In addition to providing news about darkweb markets, DDW published information about darkweb marketplaces and provided users with working links. This is what a millionaire's website looks like. The Department of Justice stated that Prihar was sentenced to prison "for operating DeepDotWeb.” Prihar's attorney pointed out in a sentencing memorandum that the operation of DDW was not inherently criminal. Prihar committed a crime when he attempted to launder cryptocurrency earned through marketplace referral links. The DOJ described the so-called "kickback scheme” in one of their first announcements: "[A] percentage of the profits of all of the activities conducted on the marketplace by any user who made purchases on the marketplace by using DDW's customized referral link. Through the use of the referral links, DDW received kickbacks from Darknet marketplaces every time a purchaser used DDW to buy illegal narcotics or other illegal goods on the marketplace.” The DoJ put a lot of effort into making affiliate links interesting to the general public. In the sentencing memorandum, Prihar's attorney summarized the criminal element succinctly: "Some of these public characterizations of DeepDotWeb and Mr. Prihar's conduct, leaning too far one way or the other, seem to lose sight of the more straightforward and accurate description that is relevant under this [sentencing] factor. Mr. Prihar earned money from customers who followed some of the links on DeepDotWeb to other websites. He pleaded guilty because he knew that some of the links led to darknet marketplaces where those customers could purchase illegal items. He did not operate a darknet marketplace, he did not force website visitors to click links, and he did not know which visitors linked to which marketplace or spent their money on which items. Mr. Prihar did not even set out to operate a referral website for darknet marketplaces. DeepDotWeb began as a news and information resource. It still was at the time of its seizure, and its revenue sources were not solely the referrals or "kickbacks” described by the government, but included other lawful enterprises.” Rabbi Shlomo Goldfarb is one of many who called for Prihar's release. Referral links proved unbelievably profitable for Prihar and his alleged co-conspirator Michael Phan, 34, of Israel. Through referral links, DDW earned more than $15 million in cryptocurrency. Prihar agreed to forfeit his half of the earnings: $8,414,173. The DoJ has accused the duo of splitting the $15+ million. They are seeking the forfeiture of Phan's half of the profits too. Almost all well known markets at the time depended on DDW for link distribution. DDW had a massive audience. When investigators seized the Alphabay and Hansa servers, they analyzed the links associated with every transaction on both marketplaces. Approximately 23 percent of all orders completed on AlphaBay and 47 percent of all orders completed on Hansa were associated with accounts created through DDW referral links. Nearly half of all transactions on Hansa Market generated income for Prihar.

Tal Prihar said someone did an antisemitism to him while he was in jail in France. "When I was arrested, one of the policemen boasted: 'We caught another Jew who took money',” Prihar said in an interview before entering a guilty plea. This obviously happened. In response to a question about the $8 million in Bitcoin he had (allegedly at the time) earned, Prihar said: "What money? The site earned through

different and completely legal marketing channels such as Bitcoin gambling websites, anonymous VPN software, and Bitcoin exchanges. Any legitimate revenue received from this site or from other sites we operated entered the bank. And we paid taxes. Everything else has gone to lawyers. The Americans intend to take what is left of my income” He was certainly correct about the intentions of the US government. Prihar had moved his family to Brasil a little over a year prior to his arrest. He regularly traveled between Israel and Brasil during this period. During one of these trips, the feds executed arrest warrants and raided properties associated with Prihar and Phan. Prihar, on one of his trips between Israel and Brasil, had a layover at the Charles de Gaulle Airport in France. French law enforcement arrested Prihar on May 6, 2019. Both Prihar and Phan were charged via indictment on April 24, 2019. A seizure banner showed up on deepdotweb.com on the same day the arrest warrants were executed. The seizure banner for DeepDotWeb resembled banners used in market seizures. The case against Phan, which is essentially the same case, has not made nearly as much progress as the Prihar case. Prihar initially fought his extradition from France to the United States. Eventually, a court authorized his extradition. He pleaded guilty in March 2021. On May 6, 2019, the Tel Aviv Police arrested two people in connection with this case. Only one of the two, Phan, has been named as a co-conspirator in Prihar's indictment. The Tel Aviv police held both suspects for six days. Phan is still "fighting extradition” in Israel. I think I know how this one unfolds. As a part of the judgment, Prihar must forfeit approximately 8,155 Bitcoins (worth roughly $8.4 million at the time of the transactions), a couple of bank accounts, the Deepdotweb.com domain, a Binance account, a Kraken account, and an iPhone.

Prihar hid cash in printers. Everyone does it. The FBI said some funny things about the site, including that "websites like DeepDotWeb pose global threats” and that "we are coming after the operators of these dangerous websites.” FBI Special Agent in Charge Robert Jones: "Websites like DeepDotWeb pose global threats that require global partnerships. DDW acted as a gateway to the Darknet, allowing for the purchase and exchange of illicit drugs and other illegal items around the world, and the individuals charged today profited from those nefarious transactions. The efforts of federal and international law enforcement should send the message that we are coming after the operators of these dangerous websites .” lol archive.org, archive.is, archiveiya74codqgiixo33q62qlrqtkgmcitqx5u2oeqnmn5bpcbiyd.onion Sentencing memo (pdf) Judgement (pdf) (via darknetlive.com at https://darknetlive.com/post/deepdotweb-admin-sentenced-to-97-months-in-prison/)

Suspected CanadaHQ Admin Arrested in Canada

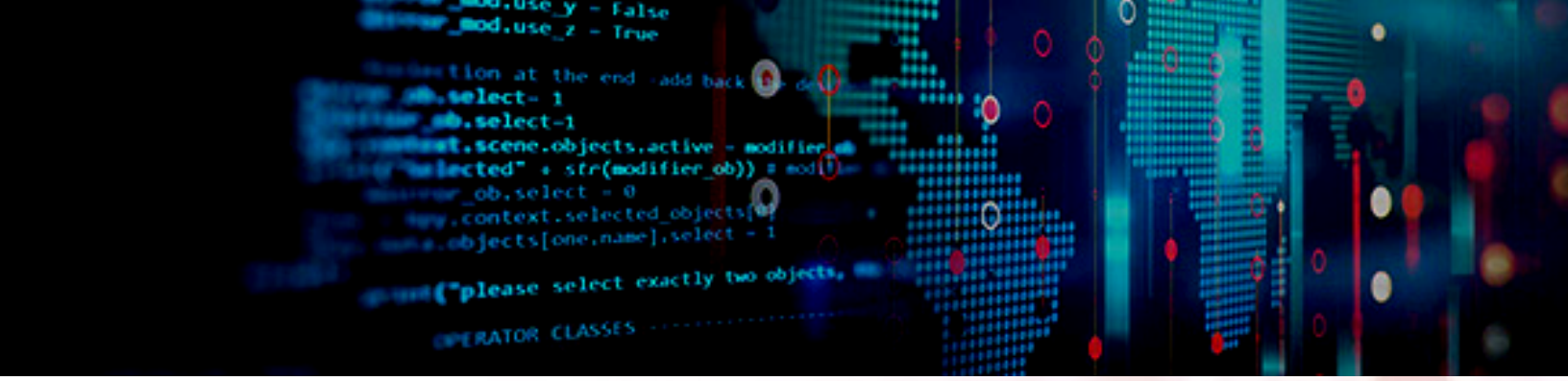
Canadian law enforcement shut down Canadian Headquarters and arrested the marketplace's alleged administrator. Four people, including the alleged creator of Canadian Headquarters (CanadaHQ), received fines for violating Canada's anti-spam legislation, according to the Canadian Radio-television and Telecommunications Commission (CRTC). In an announcement on January 26, 2022, the CRTC revealed that in 2020 and 2021, the regulatory agency had investigated CanadaHQ, its administrator, and three others associated with the market. Following the execution of warrants by CRTC staff in 2021, CanadaHQ disappeared.

CanadaHQ | Source: @darkdotfail In 2021, a former CanadaHQ vendor posted on Dread that the market had exit scammed. The site "deepwebmarketsreview,” which I am sure is a trusted source, published an article about the market's apparent exit scam in July 2021. Someone claiming to be a CanadaHQ administrator or staff member had contacted me in April 2021 about user migration after the Tor Project killed v2 onions. I suspect Canadian LEOs/regulatory agency employees arrested the alleged market administrator between April 25, 2021, and July 1, 2021. The agency focused on four suspects who "allegedly sent emails mimicking well-known brands in order to obtain personal data including credit card numbers, banking credentials, and other sensitive information.” The following defendants received penalties for sending commercial electronic messages without consent in violation of Canada's anti-spam legislation (CASL): Chris Tyrone Dracos (a.k.a. Poseidon); Marc Anthony Younes (a.k.a CASHOUT00 and Masteratm); Souial Amarak (a.k.a Wealtyman and Supreme) and Moustapha Sabir (a.k.a La3sa) According to the CASL, Dracos is the creator and administrator of the marketplace. Dracos received a penalty of $150,000, and the others received penalties of $50,000. His penalty reflects the fact that he allegedly aided in the "commission of numerous violations of CASL by the platform's vendors and customers.” CRTC claimed

that law enforcement has identified "a number of other vendors” and that "actions will be taken against them in the near future.” Unsurprisingly, the CRTC had assistance from the Royal Canadian Mounted Police's National Edition, the Sûreté du Québec, and Flare Systems. Steven Harroun, Chief Compliance and Enforcement Officer, CRTC: "Some Canadians are being drawn into malicious cyber activity, lured by the potential for easy money and social recognition among their peers. This case shows that anonymity is not absolute online, and there are real-world consequences when engaging in these activities. Canadian Headquarters was one of the most complex cases our team has tackled since CASL came into force. I would like to thank the cyber-security firm Flare Systems, the Sûreté du Québec, and the RCMP's National Division for their invaluable assistance. Our team is committed to investigating CASL non-compliance on all fronts.” Flare Systems' "AI-driven technology monitors the dark, deep and clear web,” according to their website. The differences between Flare Systems' solutions and Experian's " FREE Dark Web Triple Scan” are not apparent. I do not know what happened here. Did Canada's version of the FCC randomly investigate some people responsible for sending phishing emails who just happened to run CanadaHQ? archive.is, archive.org, archiveiya74codqgiixo33q62qlrqtkgmcitqx5u2oeqnmn5bpcbiyd.onion (via darknetlive.com at https://darknetlive.com/post/canadian-police-arrested-the-alleged-canadahq-admin/)

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

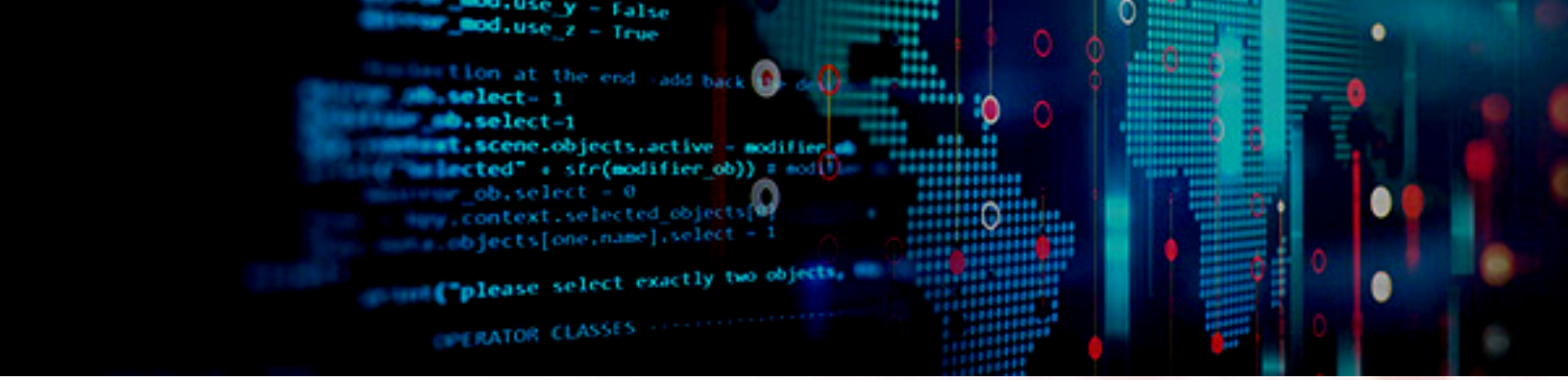
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

* RiskIQ 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
* Watch On-Demand: Five Security Intelligence Must-Haves For Next-Gen Attack Surface Management
* Discord CDN Abuse Found to Deliver 27 Unique Malware Types

FireEye

* 2021 Cybersecurity Superlatives: An InsightIDR Year in Review
* Metasploit Weekly Wrap-Up
* Why Security in Kubernetes Isn't the Same as in Linux: Part 1
* How Ransomware Is Changing US Federal Policy
* The Great Resignation: 4 Ways Cybersecurity Can Win
* Metasploit Weekly Wrap-Up
* Is the Internet of Things the Next Ransomware Target?
* [Security Nation] Mike Hanley of GitHub on the Log4j Vulnerability
* Open-Source Security: Getting to the Root of the Problem
* Active Exploitation of VMware Horizon Servers



Advisories

US-Cert Alerts & bulletins

* FBI Releases PIN on Potential Cyber Activities During the 2022 Beijing Winter Olympics and Paralympic
* Samba Releases Security Updates
* CISA Adds Eight Known Exploited Vulnerabilities to Catalog
* Apple Releases Security Updates for Multiple Products
* FBI Releases PIN on Iranian Cyber Group Emennet Pasargad
* CISA Publishes Infographic on Layering Network Security Through Segmentation
* McAfee Releases Security Update for McAfee Agent for Windows
* CISA Adds Four Known Exploited Vulnerabilities to Catalog
* 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 24, 2022
* Vulnerability Summary for the Week of January 17, 2022

Zero Day Initiative Advisories

ZDI-CAN-16422: Measuresoft
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 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-02-01, 1 days ago. The vendor is given until 2022-06-01 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-16403: Measuresoft
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 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-02-01, 1 days ago. The vendor is given until 2022-06-01 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-16417: Measuresoft
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 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-02-01, 1 days ago. The vendor is given until 2022-06-01 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-16426: Measuresoft
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 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-02-01, 1 days ago. The vendor is given until 2022-06-01 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-16423: Measuresoft
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: 2022-02-01,

1 days ago. The vendor is given until 2022-06-01 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-16433: Measuresoft

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 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-02-01, 1 days ago. The vendor is given until 2022-06-01 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-16434: Measuresoft

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: 2022-02-01, 1 days ago. The vendor is given until 2022-06-01 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-16469: Bentley

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-02-01, 1 days ago. The vendor is given until 2022-06-01 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-16424: Bentley

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-02-01, 1 days ago. The vendor is given until 2022-06-01 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-16368: 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: 2022-01-28, 5 days ago. The vendor is given until 2022-05-28 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-15982: Lexmark

A CVSS score 8.8 (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Christopher Anastasio @mufinnnnnnn and Justin Taft @JustTaft' was reported to the affected vendor on: 2022-01-28, 5 days ago. The vendor is given until 2022-05-28 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-16379: 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: 2022-01-28, 5 days ago. The vendor is given until 2022-05-28 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-16098: Trend Micro

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 'Abdelhamid Naceri' was reported to the affected vendor on: 2022-01-28, 5 days ago. The vendor is given until 2022-05-28 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-16367: 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: 2022-01-28, 5 days ago. The vendor is given until 2022-05-28 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-16369: 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: 2022-01-28, 5 days ago. The vendor is given until 2022-05-28 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-16022: 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: 2022-01-28, 5 days ago. The vendor is given until 2022-05-28 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-16332: 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: 2022-01-28, 5 days ago. The vendor is given until 2022-05-28 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-16249: Microsoft

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 'kdot' was reported to the affected vendor on: 2022-01-26, 7 days ago. The vendor is given until 2022-05-26 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-16187: Foxit

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2022-01-26, 7 days ago. The vendor is given until 2022-05-26 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-16032: Canon

A CVSS score 8.8 (AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Angelboy(@scwuaptx) from DEVCORE Research Team' was reported to the affected vendor on: 2022-01-26, 7 days ago. The vendor is given until 2022-05-26 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-16321: ABB

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 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-01-26, 7 days ago. The vendor is given until 2022-05-26 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-16223: Linux

A CVSS score 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H) severity vulnerability discovered by 'maxpl0it (@maxpl0it)' was reported to the affected vendor on: 2022-01-26, 7 days ago. The vendor is given until 2022-05-26 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-16278: ABB

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 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-01-26, 7 days ago. The vendor is given until 2022-05-26 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-16277: ABB

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 'Michael DePlante (@izobashi) of Trend Micro's Zero Day Initiative' was reported to the affected vendor on: 2022-01-26, 7 days ago. The vendor is given until 2022-05-26 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

Packet Storm Security - Latest Advisories

Ubuntu Security Notice USN-5260-1

Ubuntu Security Notice 5260-1 - Orange Tsai discovered that the Samba vfs_fruit module incorrectly handled certain memory operations. A remote attacker could use this issue to cause Samba to crash, resulting in a denial of service, or possibly execute arbitrary code as root. Michael Hanselmann discovered that Samba incorrectly created directories. In certain configurations, a remote attacker could possibly create a directory on the server outside of the shared directory.

Ubuntu Security Notice USN-5260-2

Ubuntu Security Notice 5260-2 - Orange Tsai discovered that the Samba vfs_fruit module incorrectly handled certain memory operations. A remote attacker could use this issue to cause Samba to crash, resulting in a denial of service, or possibly execute arbitrary code as root.

Red Hat Security Advisory 2022-0335-02

Red Hat Security Advisory 2022-0335-02 - This is a kernel live patch module which is automatically loaded by the RPM post-install script to modify the code of a running kernel.

Gentoo Linux Security Advisory 202202-01

Gentoo Linux Security Advisory 202202-1 - Multiple vulnerabilities have been found in WebkitGTK+, the worst of which could result in the arbitrary execution of code. Versions less than 2.34.4 are affected.

Red Hat Security Advisory 2022-0331-02

Red Hat Security Advisory 2022-0331-02 - 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 2022-0325-02

Red Hat Security Advisory 2022-0325-02 - The Advanced Virtualization module provides the user-space component for running virtual machines that use KVM in environments managed by Red Hat products. Issues addressed include a null pointer vulnerability.

Red Hat Security Advisory 2022-0330-03

Red Hat Security Advisory 2022-0330-03 - 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 2022-0328-03

Red Hat Security Advisory 2022-0328-03 - 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 2022-0329-03

Red Hat Security Advisory 2022-0329-03 - 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 2022-0332-02

Red Hat Security Advisory 2022-0332-02 - 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.

Ubuntu Security Notice USN-5257-1

Ubuntu Security Notice 5257-1 - It was discovered that ldns incorrectly handled certain inputs. An attacker could possibly use this issue to expose sensitive information.

Red Hat Security Advisory 2022-0323-02

Red Hat Security Advisory 2022-0323-02 - nginx is a web and proxy server supporting HTTP and other protocols, with a focus on high concurrency, performance, and low memory usage.

Gentoo Linux Security Advisory 202201-02

Gentoo Linux Security Advisory 202201-2 - Multiple vulnerabilities have been found in Chromium and Google

Chrome, the worst of which could result in the arbitrary execution of code. Versions less than 97.0.4692.99 are affected.

Apple Security Advisory 2022-01-26-7

Apple Security Advisory 2022-01-26-7 - Safari 15.3 addresses code execution and use-after-free vulnerabilities.

Apple Security Advisory 2022-01-26-6

Apple Security Advisory 2022-01-26-6 - watchOS 8.4 addresses buffer overflow, code execution, path sanitization, and use-after-free vulnerabilities.

Apple Security Advisory 2022-01-26-5

Apple Security Advisory 2022-01-26-5 - tvOS 15.3 addresses buffer overflow, code execution, information leakage, path sanitization, and use-after-free vulnerabilities.

Apple Security Advisory 2022-01-26-4

Apple Security Advisory 2022-01-26-4 - Security Update 2022-001 Catalina addresses buffer overflow, bypass, code execution, and information leakage vulnerabilities.

Apple Security Advisory 2022-01-26-3

Apple Security Advisory 2022-01-26-3 - macOS Big Sur 11.6.3 addresses buffer overflow, bypass, code execution, information leakage, and path sanitization vulnerabilities.

Apple Security Advisory 2022-01-26-2

Apple Security Advisory 2022-01-26-2 - macOS Monterey 12.2 addresses buffer overflow, code execution, information leakage, out of bounds write, path sanitization, and use-after-free vulnerabilities.

Apple Security Advisory 2022-01-26-1

Apple Security Advisory 2022-01-26-1 - iOS 15.3 and iPadOS 15.3 addresses buffer overflow, code execution, information leakage, path sanitization, and use-after-free vulnerabilities.

Foxit PhantomPDF Arbitrary File Write

Foxit PhantomPDF versions prior to 10.1.5 suffered from an arbitrary file write vulnerability.

Red Hat Security Advisory 2022-0317-03

Red Hat Security Advisory 2022-0317-03 - The OpenJDK 8 packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Software Development Kit. This release of the Red Hat build of OpenJDK 8 for portable Linux serves as a replacement for Red Hat build of OpenJDK 8 and includes security and bug fixes as well as enhancements. For further information, refer to the release notes linked to in the References section. Issues addressed include deserialization and integer overflow vulnerabilities.

Red Hat Security Advisory 2022-0321-03

Red Hat Security Advisory 2022-0321-03 - The OpenJDK 8 packages provide the OpenJDK 8 Java Runtime Environment and the OpenJDK 8 Java Software Development Kit. This release of the Red Hat build of OpenJDK 8 for Windows serves as a replacement for the Red Hat build of OpenJDK 8 and includes security and bug fixes, and enhancements. For further information, refer to the release notes linked to in the References section. Issues addressed include deserialization and integer overflow vulnerabilities.

Ubuntu Security Notice USN-5064-2

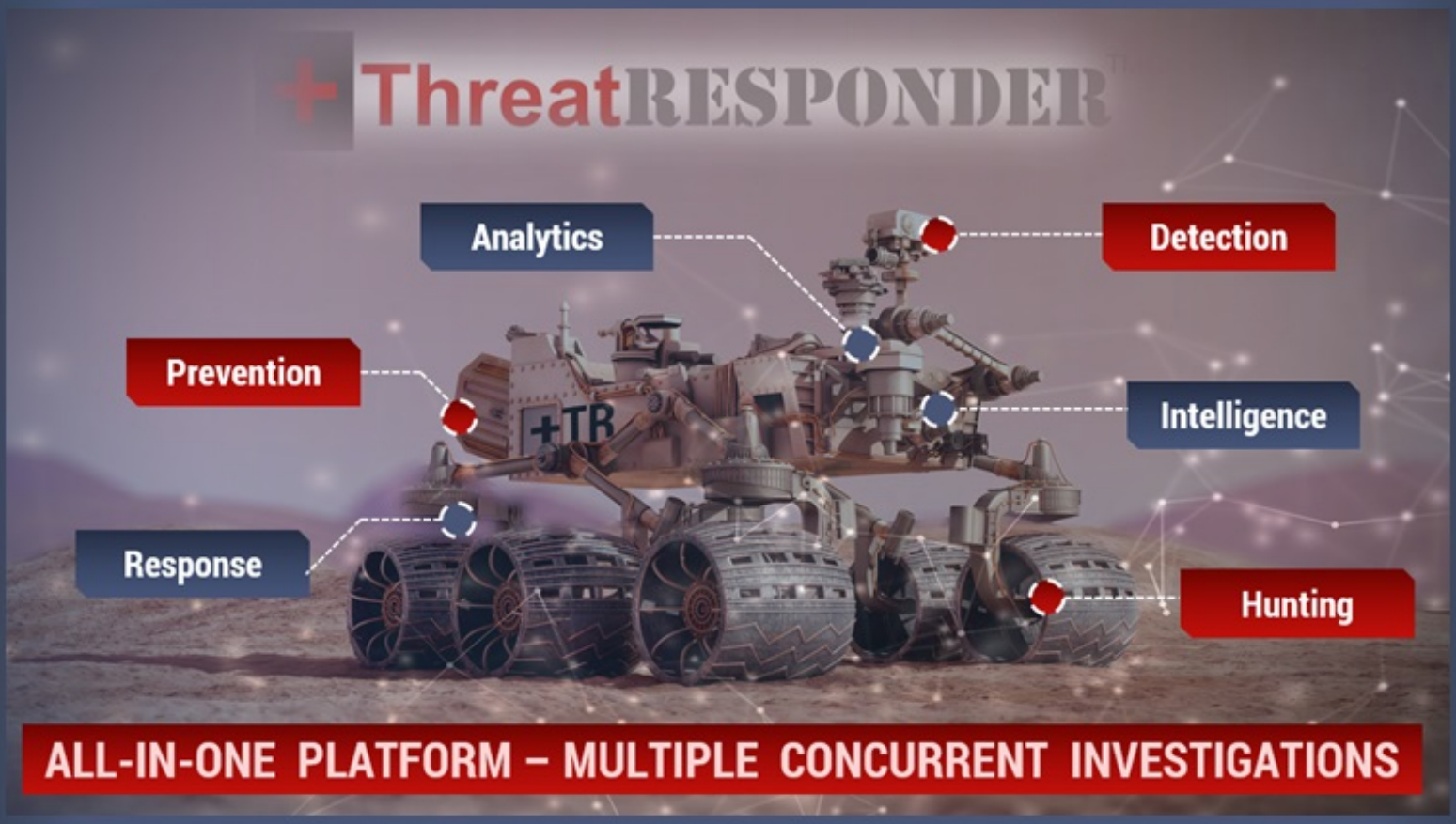
Ubuntu Security Notice 5064-2 - USN-5064-1 fixed vulnerabilities in GNU cpio. This update provides the corresponding updates for Ubuntu 16.04 ESM. Maverick Chung and Qiaoyi Fang discovered that cpio incorrectly handled certain pattern files. A remote attacker could use this issue to cause cpio to crash, resulting in a denial of service, or possibly execute arbitrary code.

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



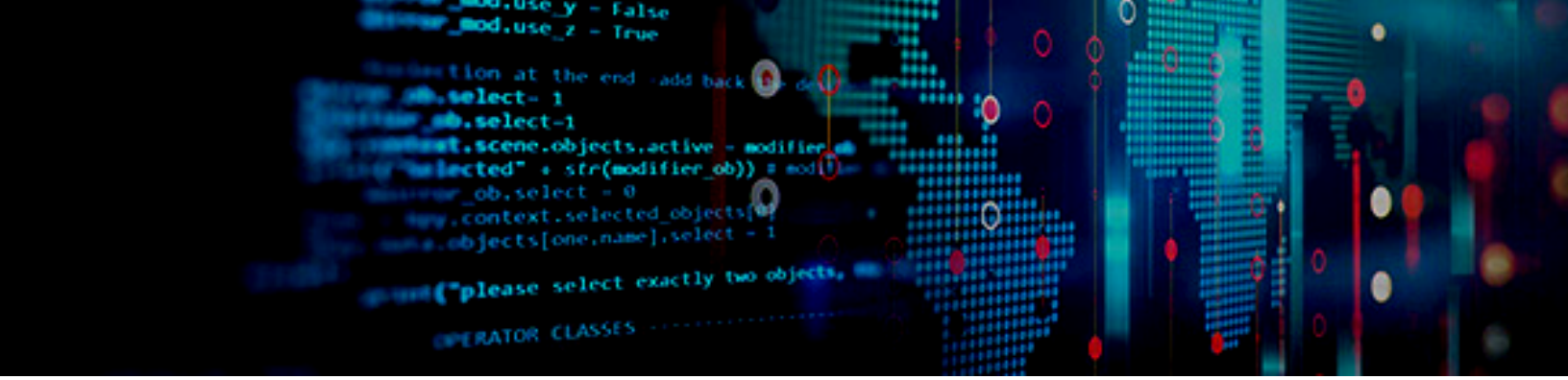
The Solution – ThreatResponder® Platform

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

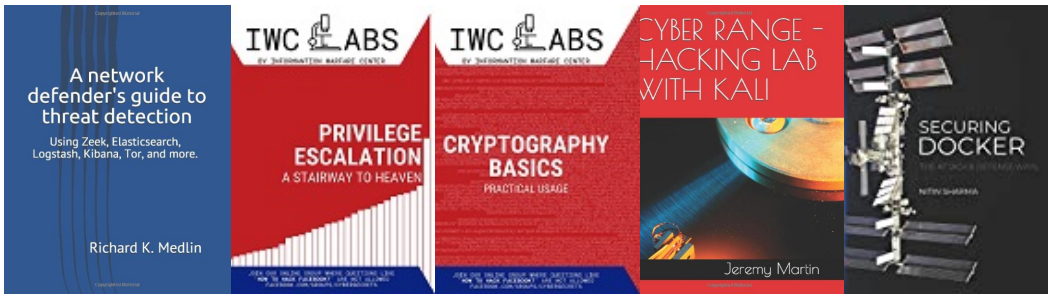


The Cyber Secrets publications on Amazon

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