Apr-25-22

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®

CYBER WEEKLY AWARENESS REPORT

April 25, 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

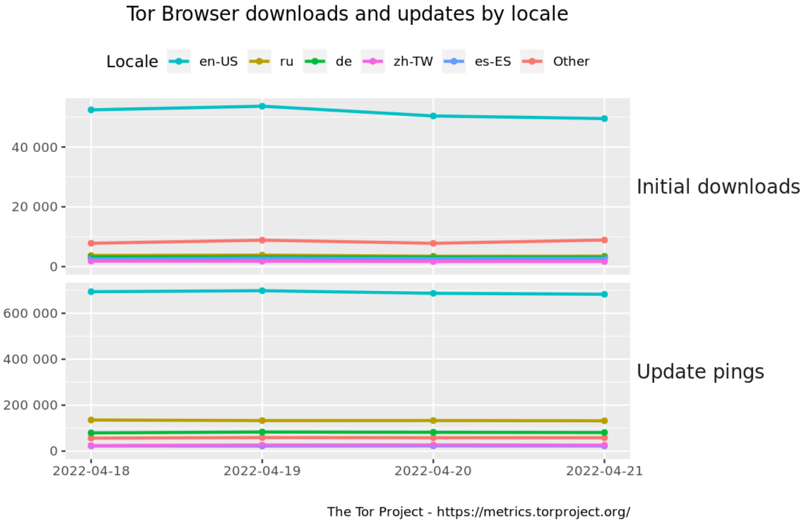
INTERNET STORM CENTER infocon:GREEN http://isc.sans.edu

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

Current News

The Hacker Corner:

Cyber Range Content

Tools & Techniques

InfoSec Media for the Week

Exploits and Proof of Concepts

Cyber Crime & Malware Files/Links Latest Identified

Advisories

Information Warfare Center Products

LATEST NEWS

Packet Storm Security

* Zero-Trust For All: A Practical Guide
* Flaw Could Have Let Hackers Commandeer Millions Of Android Devices
* Bluetooth Vulnerability In Smart COVID Test Patched
* ISPs Can't Find Any Judges Who Will Block California Net Neutrality Law
* It's Pretty Easy To Hack The Program That Runs Our Power Grids, It Turns Out
* LemonDuck Botnet Plunders Docker Cloud Instances In Cryptocurrency Crime Wave
* Major Cryptography Blunder In Java Enables Psychic Paper Forgeries
* AWS's Log4j Patches Blew Holes In Its Own Security
* Emotet Reestablishes Itself At The Top Of The Malware World
* Most Email Security Approaches Fail To Block Common Threats
* Beanstalk DeFi Project Robbed Of $182 Million In Flash Loan Attack
* REvil Appears To Return After 14 Of Its Members Were Arrested In January
* Hackers Can Infect Over 100 Lenovo Models With Unremovable Malware. Are You Patched?
* Catalan President Calls For NSO Spyware Investigation
* Google: 2021 Was A Banner Year For Exploited 0-Day Bugs
* Oracle's Critical Patch Update Arrives With 520 Fixes
* Criminals Adopting New Methods To Bypass Improved Defenses, Says Zscaler
* Your iOS App May Still Be Covertly Tracking You
* NATO Plays Cyberwar To Prep For A Real Russian Attack
* Funky Pigeon Pauses All Orders After Security Incident
* Court Rules Data Scraping Is Legal In LinkedIn Appeal
* Report: NSO Spyware Hit Boris Johnson's Office, Dozens More European Leaders
* Microsoft Raises Bug Bounties For Some High Impact Security Flaws
* Russian Court Says Google, Wikipedia Face Fines Over Fake Content
* Crypto Stablecoin Collapses After $182M Hack

Krebs on Security

* Leaked Chats Show LAPSUS$ Stole T-Mobile Source Code
* Conti's Ransomware Toll on the Healthcare Industry
* Microsoft Patch Tuesday, April 2022 Edition
* RaidForums Gets Raided, Alleged Admin Arrested
* Double-Your-Crypto Scams Share Crypto Scam Host
* Actions Target Russian Govt. Botnet, Hydra Dark Market
* The Original APT: Advanced Persistent Teenagers
* Fake Emergency Search Warrants Draw Scrutiny from Capitol Hill
* Hackers Gaining Power of Subpoena Via Fake "Emergency Data Requests"
* Estonian Tied to 13 Ransomware Attacks Gets 66 Months in Prison

LATEST NEWS

Dark Reading

* Many Medical Device Makers Skimp on Security Practices
* Sophos Buys Alert-Monitoring Automation Vendor
* Neustar Security Services' UltraDNS Integrates Terraform for Streamlined, Automated DNS Management
* FBI Warns Ransomware Attacks on Agriculture Co-ops Could Upend Food Supply Chain
* Early Discovery of Pipedream Malware a Success Story for Industrial Security
* Bitdefender Enhances Premium VPN Service With New Privacy Protection Technologies
* Contrast Security Introduces Cloud-Native Automation
* Forescout Enhances Continuum Platform With New OT Capabilities
* PerimeterX Code Defender Extends Capability To Stop Supply Chain Attacks
* CyberUSA, and Superus Careers Launch Cyber Career Exchange Platform
* Fortress Information Security Receives $125M Strategic Investment from Goldman Sachs Asset Managemen
* Comcast Business 2021 DDoS Threat Report: DDoS Becomes a Bigger Priority as Multivector Attacks are
* Creating Cyberattack Resilience in Modern Education Environments
* Zero-Day Exploit Use Exploded in 2021
* What Steps Do I Take to Shift Left in Security?
* Devo Acquires Threat Hunting Company Kognos
* Exploring Biometrics and Trust at the Corporate Level
* New Zscaler Research Shows Over 400% Increase in Phishing Attacks With Retail and Wholesale Industrie
* Cybereason Launches Digital Forensics Incident Response
* Alert Logic Releases MDR Incident Response Capability for Addressing a Breach

The Hacker News

* New BotenaGo Malware Variant Targeting Lilin Security Camera DVR Devices
* FBI Warns of BlackCat Ransomware That Breached Over 60 Organisations Worldwide
* T-Mobile Admits Lapsus$ Hackers Gained Access to its Internal Tools and Source Code
* Atlassian Drops Patches for Critical Jira Authentication Bypass Vulnerability
* Researcher Releases PoC for Recent Java Cryptographic Vulnerability
* Watch Out! Cryptocurrency Miners Targeting Dockers, AWS and Alibaba Cloud
* QNAP Advises Users to Update NAS Firmware to Patch Apache HTTP Vulnerabilities
* Cisco Releases Security Patches for TelePresence, RoomOS and Umbrella VA
* Hackers Sneak 'More_Eggs' Malware Into Resumes Sent to Corporate Hiring Managers
* Amazon's Hotpatch for Log4j Flaw Found Vulnerable to Privilege Escalation Bug
* Unpatched Bug in RainLoop Webmail Could Give Hackers Access to all Emails
* Critical Chipset Bugs Open Millions of Android Devices to Remote Spying
* New Incident Report Reveals How Hive Ransomware Targets Organizations
* Five Eyes Nations Warn of Russian Cyber Attacks Against Critical Infrastructure
* Google Project Zero Detects a Record Number of Zero-Day Exploits in 2021

LATEST NEWS

Security Week

* Spain Vows to be Transparent in Probe of Pegasus Spyware Use
* Cyberattack Causes Chaos in Costa Rica Government Systems
* Strike Security Scores Funding for 'Perpetual Pentesting' for SMBs
* When Attacks Surge, Turn to Data to Strengthen Detection and Response
* Motorola Launches Cyber Threat Information Sharing Hub for Public Safety
* Several Critical Vulnerabilities Affect SmartPTT, SmartICS Industrial Products
* Unpatched Vulnerability Allows Hackers to Steal Emails of RainLoop Users
* VMware's Head of Cybersecurity Strategy Discusses Modern Bank Heists
* Audio Codec Made by Apple Introduced Serious Vulnerabilities in Millions of Android Phones
* Catalan Chief Accuses Spain's Intelligence Agency of Hacking
* Google, Mandiant Share Data on Record Pace of Zero-Day Discoveries
* Meta Offers Rewards for Flaws Allowing Attackers to Bypass Integrity Checks
* ICS Exploits Earn Hackers $400,000 at Pwn2Own Miami 2022
* Today's Network Is Different, Not Dead - Here's How You Secure It
* Access Bypass, Data Overwrite Vulnerabilities Patched in Drupal
* Cisco Patches Virtual Conference Software Vulnerability Reported by NSA
* Many Industrial Firms Say Cybersecurity Systems Cause Problems to Operations
* FBI Shares Information on BlackCat Ransomware Attacks
* New BotenaGo Variant Infects Lilin Security Cameras With Mirai
* US, Allies Say New Intel Suggests Coming Russian Cyberattack
* ThreatLocker Raises $100 Million for Zero Trust Endpoint Security Solution
* When Is It Right to Stay Silent?
* FBI Warns of Ransomware Attacks on Farming Co-ops During Planting, Harvest Seasons
* Organizations Warned of Attacks Exploiting Recently Patched Windows Vulnerability
* Serious Vulnerabilities Found in AWS's Log4Shell Hot Patches
* Judge Sends Assange Extradition Decision to UK Government

Infosecurity Magazine

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* If You Got a "Your Bill Is Paid For" Text, You're Part of a Massive T-Mobile Texting Scam
* LinkedIn is the Most Impersonated Brand in Phishing Attacks
* New Phishing Attack Targets MetaMask Users for their Crypto Wallet Private Keys
* UK Information Commissioner: Many Cybersecurity Incidents are "Preventable"
* Critical: CISA Warns of Potential Attacks on Infrastructure by Russian State-Sponsored and Criminal C
* TraderTraitor: When States do Social Engineering
* Ransomware Attacks Show Temporary Slowing but are Expected to Increase in 2022 [Graphs]
* Only Half of All Organizations Have Refreshed Their Security Strategy Based on the Pandemic
* FBI Warns of Bank Fraud Smishing Campaign
* CyberheistNews Vol 12 #16 [Eye Opener] The Costliest Cybercrime: Business Email Compromise (BEC)

ISC2.org Blog

* Quantum Cybersecurity: Addressing the Boogeyman in the Room
* Why Are Ransomware Attacks Increasing and How Can We Prevent Them?
* Celebrating Service and Diversity - Nominate a Colleague Today!
* What Does Volunteering at (ISC)&sup2; Mean? Hear From Volunteer Lisa Vaughan
* SECURE London stokes debate on the future of the cybersecurity workforce

HackRead

* Sensitive Data: Securing Your Most Important Asset
* LemonDuck Cryptomining Botnet Hunting for Misconfigured Docker APIs
* What is a VPN and what does data logging by a VPN means?
* Why Uploading Your Personal Data on Social Media is a Bad Idea
* Beware of Fake Windows 11 Update Delivering Malware
* How to Choose the Right Web Development Firm for Your Startup?
* LAZARUS APT Using TraderTraitor Malware to Target Blockchain Orgs, Users

Koddos

* Sensitive Data: Securing Your Most Important Asset
* LemonDuck Cryptomining Botnet Hunting for Misconfigured Docker APIs
* What is a VPN and what does data logging by a VPN means?
* Why Uploading Your Personal Data on Social Media is a Bad Idea
* Beware of Fake Windows 11 Update Delivering Malware
* How to Choose the Right Web Development Firm for Your Startup?
* LAZARUS APT Using TraderTraitor Malware to Target Blockchain Orgs, Users

LATEST NEWS

Naked Security

* QNAP warns of new bugs in its Network Attached Storage devices
* S3 Ep79: Chrome hole, a bad place for a cybersecurity holiday, and crypto-dodginess [Podcast]
* Critical cryptographic Java security blunder patched - update now!
* Beanstalk cryptocurrency heist: scammer votes himself all the money
* Yet another Chrome zero-day emergency update - patch now!
* S3 Ep78: Darkweb hydra, Ruby, quantum computing, and a robot revolution [Podcast]
* US cryptocurrency coder gets 5 years for North Korea sanctions busting
* Hospital robot system gets five critical security holes patched
* OpenSSH goes Post-Quantum, switches to qubit-busting crypto by default
* Popular Ruby Asciidoc toolkit patched against critical vuln - get the update now!

Threat Post

* Zero-Trust For All: A Practical Guide
* Skeletons in the Closet: Security 101 Takes a Backseat to 0-days
* Most Email Security Approaches Fail to Block Common Threats
* Google: 2021 was a Banner Year for Exploited 0-Day Bugs
* Rethinking Cyber-Defense Strategies in the Public-Cloud Age
* 'CatalanGate' Spyware Infections Tied to NSO Group
* Protect Your Executives' Cybersecurity Amidst Global Cyberwar
* Cyberattackers Put the Pedal to the Medal: Podcast
* Karakurt Ensnares Conti, Diavol Ransomware Groups in Its Web
* Feds: APTs Have Tools That Can Take Over Critical Infrastructure

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

LATEST NEWS

IBM Security Intelligence

Unfortunately, at the time of this report, the IBM Security Intelligence Blog resource was not availible.

InfoWorld

* JDK 19: The features targeted for Java 19
* Devs For Ukraine to raise money for charities, NGOs operating in warzone
* AWS Amplify adds visual development tool
* Why we multicloud
* The new Elastic CEO puts cloud front and center
* AWS unveils ML-powered devops for AWS Lambda
* AWS launches $30M Impact Accelerator for minority-led startups
* C# 11 previews raw string literals, dumps parameter null checking
* Go serverless with Vercel, SvelteKit, and MongoDB
* Microsoft unifies large-scale data management under Purview framework

C4ISRNET - Media for the Intelligence Age Military

* Space Fence now has a direct link to key Space Force data hub
* Finland wins NATO cyber defense competition
* DARPA seeks proposals on improving satellite imagery technology
* What war in Ukraine reveals about information age conflict
* US to encourage other nations to join ban on anti-satellite weapons testing
* Goodbye hoarding? Official sees increased data sharing at Pentagon
* US Space Force developing plans for tactically responsive capabilities
* US Space Force space defense squadron tasked to focus on deep space
* SpaceX shut down a Russian electromagnetic warfare attack in Ukraine last month - and the Pentagon is
* Pentagon seeks reauthorization, expansion of small business funding

The Hacker Corner

Conferences

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

Google Zero Day Project

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

Capture the Flag (CTF)

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

* NahamCon CTF 2022
* PatriotCTF
* Digital Overdose Conference 2022 CTF
* &aring;ngstromCTF 2022
* RPCA CTF 2022
* San Diego CTF 2022
* m0leCon CTF 2022 Teaser
* TJCTF 2022
* @HackDay Final 2022
* VolgaCTF 2022 Qualifier

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

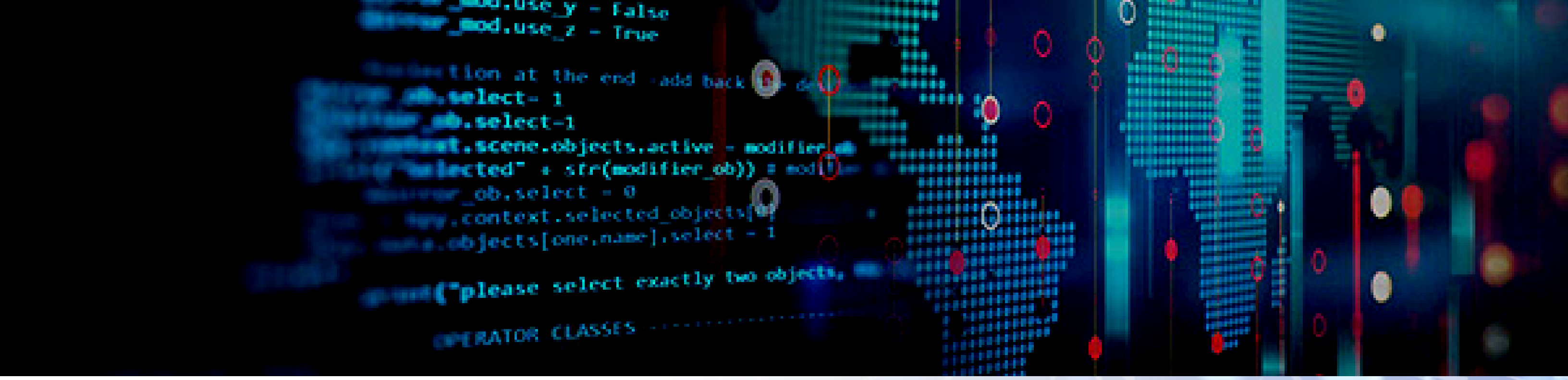
* Zeek 4.2.1
* Suricata IDPE 6.0.5
* XDNR Shellcode Cryptor / Encoder
* AIEngine 2.1.0
* Haveged 1.9.18
* OpenSSH 9.0p1
* Wireshark Analyzer 3.6.3
* Adversary3 1.0
* nfstream 6.4.3
* OpenSSL Toolkit 3.0.2

Kali Linux Tutorials

* Mip22 : An Advanced Phishing Tool
* PurplePanda : Identify Privilege Escalation Paths Within And Across Different Clouds
* RefleXXion : A Utility Designed To Aid In Bypassing User-Mode Hooks Utilised By AV/EPP/EDR Etc
* WMEye : A Post Exploitation Tool That Uses WMI Event Filter And MSBuild Execution For Lateral Movemen
* Lnkbomb : Malicious Shortcut Generator For Collecting NTLM Hashes From Insecure File Shares
* Patching : An Interactive Binary Patching Plugin For IDA Pro
* Code Analysis : Static Code Analysis
* GoodHound : Uses Sharphound, Bloodhound And Neo4j To Produce An Actionable List Of Attack Paths
* Domain Alerting : Daily Alert When A New Domain Name Is Registered And Contains Your Keywords
* Dome : Fast And Reliable Python Script That Makes Active And/Or Passive Scan To Obtain Subdomains

GBHackers Analysis

* Critical Android Bug Let Attackers to Access Users' Media and Audio Conversations
* 15-Year-old Security Vulnerability In The PEAR PHP Repository Permits Supply Chain Attack
* Honda Bug Let Attackers Unlock and Start the Car
* Hundreds of HP Printer Models Affected by Critical Remote Code Execution
* CISA Has Added 15 New Flaws to the List of Actively Exploited Vulnerabilities



Weekly Cyber Security Video and Podcasts

SANS DFIR

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

Defcon Conference

* DEF CON 29 Ham Radio Village - Kurtis Kopf - An Introduction to RF Test Equipment
* DEF CON 29 Ham Radio Village - Tyler Gardner - Amateur Radio Mesh Networking
* DEF CON 29 Ham Radio Village - Bryan Fields - Spectrum Coordination for Amateur Radio
* DEF CON 29 Ham Radio Village - Eric Escobar - Getting started with low power/long distance Comms

Hak5

* How Hackers Phish Windows Users for Cheap with SSDP
* Live Hacking Q&A with Kody and Alex
* Infrastructure Attacks Target Ukraine & US - ThreatWire

The PC Security Channel [TPSC]

* Windows Defender vs Avast: Do you need Free Antivirus?
* Discord Infostealers: How hackers steal your password

Eli the Computer Guy

* CNN+ SHUTDOWN
* CHINA ATTACKS TAIWAN says TV NEWS by ACCIDENT
* TWITTER CANCELLED by CNN CEO
* Netflix is DEAD

Security Now

* A Critical Windows RPC RCE - Another Chrome 0-day, MS Patch-Fest, US Nuclear Systems Unhackable?
* Spring4Shell - Patch Tuesday, Microsoft's Autopatch System, NGINX 0-Day

Troy Hunt

* Weekly Update 292

Intel Techniques: The Privacy, Security, & OSINT Show

* 258-Introducing UNREDACTED Magazine
* 257-Early Warning

Proof of Concept (PoC) & Exploits

Packet Storm Security

* ManageEngine ADSelfService Plus Custom Script Execution
* Watch Queue Out-Of-Bounds Write
* USR IOT 4G LTE Industrial Cellular VPN Router 1.0.36 Remote Root Backdoor
* Pharmacy Management System 1.0 SQL Injection
* Pharmacy Management System 1.0 Shell Upload
* Online Restaurant Table Reservation System 1.0 SQL Injection
* 7-Zip 16 DLL Hijacking
* Jenkins Remote Code Execution
* BlueZ Key Theft / bluetoothd Double-Free
* Backdoor.Win32.GateHell.21 Authentication Bypass
* Backdoor.Win32.Delf.zn Insecure Credential Storage
* Linux FUSE Use-After-Free
* WordPress Motopress Hotel Booking Lite 4.2.4 SQL Injection
* Linux watch_queue Filter Out-Of-Bounds Write
* Backdoor.Win32.GateHell.21 Man-In-The-Middle
* WordPress Popup Maker 1.16.5 Cross Site Scripting
* Responsive Online Blog 1.0 SQL Injection
* Backdoor.Win32.Psychward.03.a Weak Hardcoded Password
* ManageEngine ADSelfService Plus 6.1 User Enumeration
* PKP Open Journals System 3.3 Cross Site Scripting
* Backdoor.Win32.Hupigon.haqj Unquoted Service Path
* Trojan.Win32.TScash.c Insecure Permissions
* WordPress Videos Sync PDF 1.7.4 Cross Site Scripting
* Backdoor.Win32.Loselove Denial Of Service
* WordPress Elementor 3.6.2 Shell Upload

CXSecurity

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

Proof of Concept (PoC) & Exploits

Exploit Database

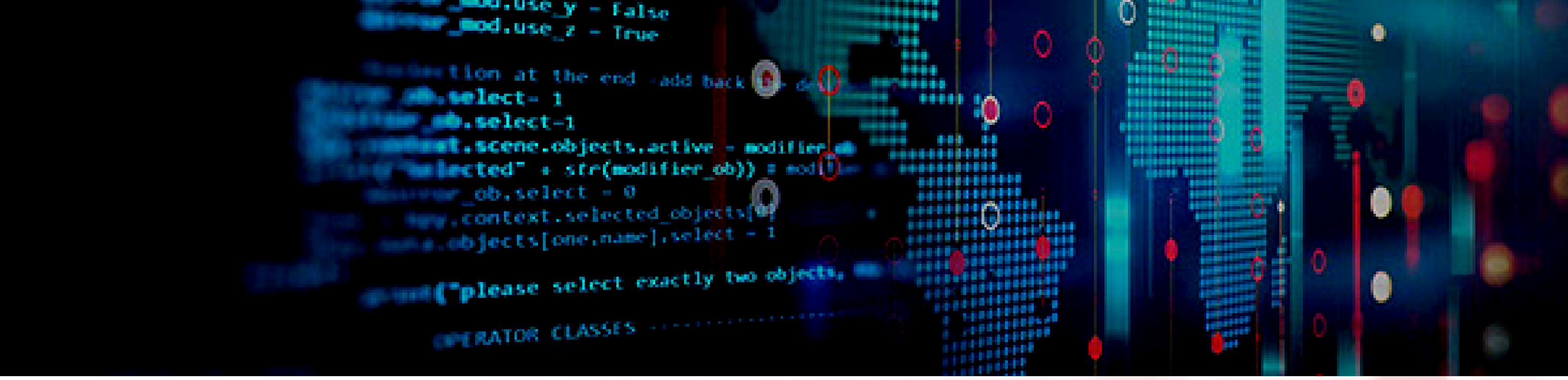
* [local] EaseUS Data Recovery - 'ensserver.exe' Unquoted Service Path
* [local] PTPublisher v2.3.4 - Unquoted Service Path
* [webapps] Fuel CMS 1.5.0 - Cross-Site Request Forgery (CSRF)
* [local] 7-zip - Code Execution / Local Privilege Escalation
* [webapps] WordPress Plugin Elementor 3.6.2 - Remote Code Execution (RCE) (Authenticated)
* [webapps] PKP Open Journals System 3.3 - Cross-Site Scripting (XSS)
* [remote] Delta Controls enteliTOUCH 3.40.3935 - Cookie User Password Disclosure
* [remote] Delta Controls enteliTOUCH 3.40.3935 - Cross-Site Scripting (XSS)
* [remote] Delta Controls enteliTOUCH 3.40.3935 - Cross-Site Request Forgery (CSRF)
* [webapps] REDCap 11.3.9 - Stored Cross Site Scripting
* [webapps] WordPress Plugin Popup Maker 1.16.5 - Stored Cross-Site Scripting (Authenticated)
* [remote] Verizon 4G LTE Network Extender - Weak Credentials Algorithm
* [webapps] WordPress Plugin Videos sync PDF 1.7.4 - Stored Cross Site Scripting (XSS)
* [remote] ManageEngine ADSelfService Plus 6.1 - User Enumeration
* [webapps] Scriptcase 9.7 - Remote Code Execution (RCE)
* [webapps] Easy Appointments 1.4.2 - Information Disclosure
* [remote] Zyxel NWA-1100-NH - Command Injection
* [webapps] WordPress Plugin Motopress Hotel Booking Lite 4.2.4 - SQL Injection
* [local] Microsoft Exchange Active Directory Topology 15.0.847.40 - 'Service MSExchangeADTopology' Unq
* [local] Microsoft Exchange Mailbox Assistants 15.0.847.40 - 'Service MSExchangeMailboxAssistants' Unq
* [webapps] Razer Sila - Command Injection
* [webapps] Razer Sila - Local File Inclusion (LFI)
* [webapps] Telesquare TLR-2855KS6 - Arbitrary File Deletion
* [webapps] Telesquare TLR-2855KS6 - Arbitrary File Creation
* [remote] Franklin Fueling Systems Colibri Controller Module 1.8.19.8580 - Local File Inclusion (LFI)

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.


mod.use_y = False
mod.use_z = True
tion at the end -add back
ob.select= 1
ob.select=1
.scene.objects.active = modifier
"selected" + str(modifier_ob)) # modi
_ob.select = 0
.context.selected_objects[0]
.objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES

Latest Hacked Websites

Published on Zone-h.org

https://www.nfra.go.tz/abcd.html

https://www.nfra.go.tz/abcd.html notified by ./KeyzNet

https://www.nirc.go.tz/abcd.html

https://www.nirc.go.tz/abcd.html notified by ./KeyzNet

https://www.nhbra.go.tz/abcd.html

https://www.nhbra.go.tz/abcd.html notified by ./KeyzNet

https://www.ndctz.go.tz/abcd.html

https://www.ndctz.go.tz/abcd.html notified by ./KeyzNet

https://www.ncc.go.tz/abcd.html

https://www.ncc.go.tz/abcd.html notified by ./KeyzNet

https://www.modans.go.tz/abcd.html

https://www.modans.go.tz/abcd.html notified by ./KeyzNet

https://www.mifugouvuvi.go.tz/abcd.html

https://www.mifugouvuvi.go.tz/abcd.html notified by ./KeyzNet

https://www.mawasiliano.go.tz/abcd.html

https://www.mawasiliano.go.tz/abcd.html notified by ./KeyzNet

https://www.maji.go.tz/abcd.html

https://www.maji.go.tz/abcd.html notified by ./KeyzNet

https://www.lita.go.tz/abcd.html

https://www.lita.go.tz/abcd.html notified by ./KeyzNet

https://www.gpsa.go.tz/abcd.html

https://www.gpsa.go.tz/abcd.html notified by ./KeyzNet

https://www.ethicssecretariat.go.tz/abcd.html

https://www.ethicssecretariat.go.tz/abcd.html notified by ./KeyzNet

https://www.dcea.go.tz/abcd.html

https://www.dcea.go.tz/abcd.html notified by ./KeyzNet

https://www.dart.go.tz/abcd.html

https://www.dart.go.tz/abcd.html notified by ./KeyzNet

https://www.cma.go.tz/abcd.html

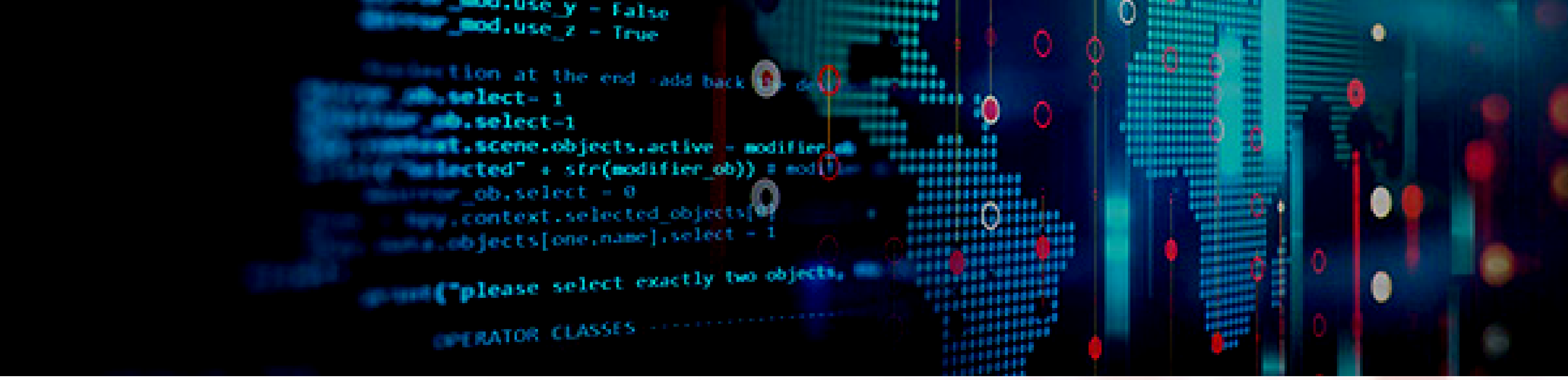
https://www.cma.go.tz/abcd.html notified by ./KeyzNet

https://www.agitf.go.tz/abcd.html

https://www.agitf.go.tz/abcd.html notified by ./KeyzNet

https://emoldovata.gov.md/storage/598/hacked.htm

https://emoldovata.gov.md/storage/598/hacked.htm notified by HAMMAML1F



Dark Web News

Darknet Live

AUSTRAC Releases Guide on Profiling Crypto Transactions

Australian Transaction Reports and Analysis Centre (AUSTRAC) released a guide on "preventing the criminal abuse of digital currencies.&rdquo; Digital currency exchanges can use the lists of indicators in the guide to profile their customers. The guide "provides financial indicators to help businesses, including digital currency exchange providers, recognize and report criminal activity through digital currencies,&rdquo; according to the AUSTRAC website. The guide lists money laundering, the purchase and sale of illicit products via darknet marketplaces, terrorism financing, scams, tax evasion, and ransomware as serious crimes enabled by cryptocurrency. In the money laundering section of the guide, AUSTRAC noted that criminals use mixing services and privacy coins to launder money. "Although conversion services and privacy coins operate outside of the traditional banking sector, blockchain analysis tools can be used to identify digital currency addresses connected to conversion services, creating an opportunity for financial service providers to identify transactions coming from or going to these services.&rdquo; __ The report suggests that businesses avoid "de-banking&rdquo; suspicious customers. The most interesting part of the guide is the section on behavioral and financial indicators. Each listed indicator should trigger enhanced customer due diligence. If the digital currency exchange suspects a customer or transaction is linked to criminal activity, they must submit a Suspicious Matter Report to AUSTRAC. General Indicators _ Identification, verification, and profile information _ Behavioral Indicators _ Customer is reluctant or declines to provide identification or personal information. Customer attempts to provide as little identity information as possible, including incomplete or insufficient identification information. Customer provides stolen, forged or fake documentation. Customer verification information is a photograph of data on a computer screen rather than the original document. Company beneficial ownership is difficult to establish. Customer provides documentation with identifiable alterations or of a low quality during on-boarding or when conducting ECDD. Customer on-boarding documentation is unable to be verified or does not match the details of the account. Customer acts on behalf of someone else (without disclosing the fact) or impersonates someone else. Customer appears to be using a virtual private network (VPN) or encrypted email in an attempt to hide their identity. Customer is known to law enforcement, via publicly available information. Customer frequently changes their identification information, including email addresses, internet protocol (IP) addresses, or financial information. Customer is difficult to contact, responds only via email or web chat, and at unusual hours. Customer uses a mail account provider known for high privacy features. Law enforcement or regulator interaction indicates that a customer is linked to illicit activity. Customer has adverse media or open source reports. Source of funds and wealth _ Financial indicators _ Customer has unexplained wealth or the source of their funds does not match their profile. Customer purchases large amounts of digital currency not substantiated by available wealth or consistent with their profile. Structuring (or perceived structuring) of government issued currency deposits or digital currency withdrawals via cryptocurrency ATMs or retail locations. Behavioral Indicators _ Customer provides inconsistent explanations as to the source of funds or source of wealth that are used for the purchase of digital currencies. Customer provides documents that appear to have been altered or of low quality during on-boarding or when conducting ECDD processes. Customer requests higher limits inconsistent with their occupation or profile. Customer is reluctant or declines to provide source of funds or wealth. Account activity _ Financial indicators _ Use of chain-hopping in an apparent attempt to obfuscate source or destination of funds. Multiple customers send funds to the same external wallet address (that is not a service). Publicly available information such as sanctions lists or analytical tools indicate a customer's wallets, or wallets the customer is transacting with, are associated or linked to illicit activity. Unusual transactions such as customer moving earnings through mixers, multiple conversions or layering through multiple exchanges prior to cashing out. Customers that regularly make significant profits or losses by transacting with the same subset of wallet addresses. Behavioral Indicators _ Multiple customer accounts are opened with either the same email address, phone number, IP address, residential address, postal address or on-boarding documents. Customer accesses their accounts from a high number of different electronic devices or IP addresses. Customer lacks knowledge or provides inaccurate information about the transaction, the source of funds, or the wallet address where they want to send the digital currency. Customer seems anxious or impatient with the time taken to make a large transaction. Customer is evasive as to the reason for the transfer. Customer wants to increase transaction limits shortly after opening an account. Customer creates or attempts to create separate accounts under different names to circumvent restrictions on trading or withdrawal limits imposed. Customer attempts to coerce or persuade staff to ignore reporting obligations or break normal protocol to conduct a transaction. Customer consistently conducts transactions under actual or perceived reporting thresholds. Customer gambles with digital currency or has transactions to/from gambling websites. Customer uses privacy enhanced digital currencies which do not appear to be used for investment purposes. Customer IP addresses do not match the state or country the customer resides in. Crime-Specific Indicators _ Illicit Darknet Market Activity Indicators _ Financial indicators _ Blockchain analysis tools link a customer's transactions to darknet clusters, child exploitation clusters, mixers or high risk exchanges. Customer's wallet addresses show exposure to high-risk conversion services or darknet marketplaces. Use of, or donations to darknet explorers, including a platform enabling anonymised internet access indicating access to, and possible illicit purchases on the darknet marketplaces. Terrorism Financing (totally real) _ Financial indicators _ Public information or blockchain analysis tools indicate a customer has transacted with websites or wallet addresses considered to be high risk for terrorism activities or proliferation financing. Transactions with sanctioned wallet addresses or people of interest listed on government websites, such as the Office of Foreign Assets Control (OFAC) or the Department of Foreign Affairs and Trade (DFAT). Transactions to crowdfunding or online fundraising campaigns linked to ideologically or religiously motivated violent extremism focused forums. Transfers to/from international exchanges with less stringent 'know your customer' processes, including those owned or hosted in high risk jurisdictions. Customer account receives multiple small deposits, which are immediately transferred to private wallets. Behavioral Indicators _ Social media (or online profiles/handles) indicate the customer holds ideologically or religiously motivated violent extremism ideologies or sympathies. Tax Evasion _ Financial indicators _ Use of services that do not make commercial or economic sense. For example, a business moving earnings through mixers or an individual converting a digital currency multiple times prior to cashing out, incurring additional conversion fees. Behavioral Indicators _ Customer makes enquires about avoiding tax reporting obligations. Customer asks if personal or transaction information will be shared with the Australian Taxation Office. Customer requests to hide or delete transaction activity held. Customer sends or receives government issued currency to a wide range of related personal or business accounts at different institutions. Preventing the Criminal Abuse of Digital Currencies Financial Crime Guide (via darknetlive.com at https://darknetlive.com/post/austrac-releases-guide-on-profiling-crypto-transactions/)

Dread Now Has an i2p Mirror (DDoS Update)

Dread is now accessible over i2p. After a period of downtime, Paris&mdash;one of the administrators of Dread&mdash;published the hostname of Dread's i2p mirror. In the announcement post for the March 2022 Dread update (Dread V3), Paris promised an i2p mirror for Dread. The eepsite launch was apparently delayed due to stability issues: "A new i2p endpoint is online and flood-filling but it hasn't been as stable as I need it to be. I'll be holding off posting the address till such time (probably within a couple of days). I can get it more stable for an average user to visit if you want to both prepare and help this process along install i2pd and running it. This network needs to 2X its size with a shit ton more nodes which have ipv6. I'm doing what I can to get it up, but the reach-ability of the address is poor, and connections are unstable. It is better than when I have tried before but more work needs to be done on this. It is far more resistant against DDOS attacks though, and with enough noise Sybil attacks become basically impossible to conduct on anything other than an extremely targeted attack.&rdquo; Paris wrote that "someone doesn't want [Dread] online&rdquo; on April 12, 2022. The post referenced a distributed denial-of-service attack that rendered Dread inaccessible. As one of the largest and most well-known onion services with a western userbase, the downtime did not go unnoticed. Infosec Twitter users suggested that law enforcement had sponsored the attacks (the FBI once paid CMU to conduct a traffic confirmation attack and a Sybil attack during an investigation into marketplaces). Darknetlive's peanut gallery claimed that "asap siezed [sic], dread siezed [sic], abacus siezed [sic]&rdquo; or, "Dread, cryptostamps, and ASAP were all seized.&rdquo; Dread, cryptostamps, ASAP, and Abacus are online without apparent seizure signs. Dread's onion service is only intermittently working though. The commenters apparently have access to secret evidence. Paris, "Someone doesn't want us up. April 11 DDOS attack. I2P mirror online? &rdquo; (signed copy below this post). And here I was going to just relax a bit, work on the recon update, and not worry too much. BUT NO. We can't have nice things.   I have been delaying the i2p endpoint announcement simply because my reliability with the i2p network has been&hellip; terrible is one word I'll use. It might because how I'm personally connecting into the i2p network or because of how the i2p network system is designed for dread (layers of i2p nodes to the core). I was figuring it out and also gathering information about how the i2p network handles different things. There is a chicken and an egg problem here with i2p. They need more people using their network. It is, from what I got from the IPs and bandwidth statistics on the distributed floodfill nodes, far smaller and far less resistant to Sybil attacks. They don't try to hide that fact (in their fantastic documentation) but it is still a problem. With scale there is a lot of promise here with the proper supports. Dread will NEVER use any addressbook which can transparently MiTM attack you. It is very important to only visit using the base32 hostname. With that being said I'm going forward with the announcement to provide a hopefully more stable as time goes on i2p mirror.   This is Paris from Dread. As promised we now have an i2p mirror: http://dreadtoobigdsrxg4yfspcyjr3k6675vftyco5pyb7wg4pr4dwjq.b32.i2p   It is the biggest dicked i2p website yet. Guaranteed. There are people who leave helpful comments on Darknetlive articles, though. One user posted a reminder that HugBunter has been missing for two months. HugBunter's last comment on Dread was on February 20, 2022&mdash;54 days from the time of writing. Additionally, HugBunter's warrant canary is out of date by 15 days at the time of writing (the canary update was "scheduled for Thursday, March 31, 2022&rdquo;). This is not the first time HugBunter has let a canary expire. Paris has a current canary as of April 15, 2022. The canary is due for an update by today (April 15, 2022), but Paris and HugBunter often operate on Dread time (Gregorian date &plusmn; three days). Busy onion service operators regularly miss their self-imposed deadline by a day or two.   A sign in a library in Craftsbury, Vermont in 2005 | Jessamyn West   There are certainly some weird things happening behind the scenes.   Paris: i2p mirror   -----BEGIN PGP SIGNED MESSAGE-----   Hash: SHA256   And here I was going to just relax a bit, work on the recon update, and not worry too much. BUT NO. We can't have nice things.   I have been delaying the i2p endpoint announcement simply because my reliability with the i2p network has been... terrible is one word I'll use. It might because how I'm personally connecting into the i2p network or because of how the i2p network system is designed for dread (layers of i2p nodes to the core). I was figuring it out and also gathering information about how the i2p network handles different things. There is a chicken and an egg problem here with i2p. They need more people using their network. It is, from what I got from the IPs and bandwidth statistics on the distributed floodfill nodes, far smaller and far less resistant to Sybil attacks. They don't try to hide that fact (in their fantastic documentation) but it is still a problem. With scale there is a lot of promise here with the proper supports.   Dread will NEVER use any addressbook which can transparently MiTM attack you. It is very important to only visit using the base32 hostname. With that being said I'm going forward with the announcement to provide a hopefully more stable as time goes on i2p mirror.   This is Paris from Dread. As promised we now have an i2p mirror:

http://dreadtoobigdsrxg4yfspcyjr3k6675vftyco5pyb7wg4pr4dwjq.b32.i2p It is the biggest dicked i2p website yet. Guaranteed. -----BEGIN PGP SIGNATURE-----
iQIzBAEBCAAdFiEEbfleES3oPdbct1q5DE1JcU+sN9gFAmJU3NQACgkQDE1JcU+s
N9iFcw//R+h7ppmmvpjLh90qOdRmzTxC4x5SjXSThBN3Am/+AWY8XJX+tJ1wSlMj
KxzsOWyfZ/Tr4sOBvvSNK975oMvN4WlxEmYg0cd5Nvz1z/Q0sS3uYQrwociuS4Vk
LspqyL3N+wiTwySwGci2JxzQexPbt9sEIDo9haIFbsVHXsVMD4ZpsvmgGddl07UJ
QxF7YmVshnImNcw4eYVUNtCim+586ldJPYyGdciBUgRRbGLZE0JTTQ3LcGZ3Wk2w
YDXcQ1D6DaYmRHFnntxS2G3Q4TSG+KuJwak7ZAbC31fU2QrG+EmT3KRjhw7jpPDR
Hieyib/2tjwNcpfnigvWdJIN3AW4JMtW9Q/DKtZt3oBeZtBdirInUZadRpsMitCy
dpsYoftAnDW96UC13uTH+RQWVUAtJcuByuCOaJWRrxeD/cQdbYwAf7EtGEVED6HR
vnkicwaJCWGtd5fN8jYUhIA0a93qEcujJnQcvYlJjvXUvdeKNO4BXnOlsqg20WSd
iBVdFQfdVr3lX/+UjkmS9/ZmsDELiNDg/iCGGg4SWgWQC+dNcldRqSp3fZw4R6v5
yk3hfdBMRCNcyPsUVYflSt+aBD+46G6nN5FRfi8Lw/CTdmVgveR+lk+gSdJ5P1+k
OlgM3ppCwjA7wp9vsfam5jgnUz7b6mhtPhnp0kQ+zyC7R3QdKDg= =FxQf -----END PGP SIGNATURE-----
Canary: Paris -----BEGIN PGP SIGNED MESSAGE----- Hash: SHA256 I, Paris am alive and free as of April 1st 2022 and in full control of Dread, Recon and all other services related to our network. Next canary update is scheduled for April 15th 2022 Hug is alive. Two new platforms coming soon. Main Dread URL: http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion Main Recon URL: http://recon222tttn4ob7ujdhbn3s4gjre7netv14zybuvbq2bcqwltkiqinhad.onion/ Bitcoin Height:
000000000000000000077d011569f26c0ebb6deaad63a7fbbbf256badc61bbf6 -----BEGIN PGP SIGNATURE----- iQIzBAEBCAAdFiEEbfleES3oPdbct1q5DE1JcU+sN9gFAmJHSJgACgkQDE1JcU+s
N9gUoBAA4amh+dk7tcLyFNxXNvFduluhR2mJWH/HVLFBXOziq+2CmY19kjuZVU4d
3UmOlDa5C9/XwKKF2dH+yrMPINhpXozL4HTsm9Lqan8LF0ATGScCuqpwAUUx+bww
btPBwyRLRsFSt97XCBMLgeiL9Q+TMAzoNjohM1hVD/fYQeQP2EuCpClA/tSqtN0T
7DQxJFb6GbYToK08trv7nu3TvQX6GwiZTSc9vHNZxSghKtm6/Y63AoCdsdc2BjrP
BWZOwkLPxoU3924O6GzWJZhEO3xXmOuRCfppAuvi5fq4kxJeXd/V7ahWa67nQMOP
Kom8IjxK99a1QeIkHBsUMKWt9vs0ryXBaD5+IT9OExUyd30xkhM+rFO8TbH4K+kR
Jn4BnFfmssNE+n1ZlzAc9ALtEcNjOxG1S7PFdUgEqzJdTBiZ9WbrVdZB5iY6Xs7u
Ewr4A+kHtDze3OuRVyA8FIM1IM9k9O3fesYUL9llUicMMZfuf6WFo5gqh+uA16MH
XL4c0JWQygqt7s0YhAI8UHEBqDxvFvvHUnrBLj4h66HCtvioWU0gmI0/EWHJGbGg
xB4+UAdkT1Q+0UhMoVOKjiAkrSmhWEgol2QDWERZDG2iOclnp2V4POXWSgPoUESj
HHL5erO8kXiJCs8QGMK1yDwnf23I6InP09SC0C4N1V/Injn32Hc= =gk3y -----END PGP SIGNATURE-----
Canary: HugBunter -----BEGIN PGP SIGNED MESSAGE----- Hash: SHA256 I, HugBunter am alive and free as of Tuesday, March 22nd 2022 and in full control of Dread, Recon and all other services related to our network. Next canary update is scheduled for Thursday, March 31st 2022
0000000000000000000561de6ffa1624cabb82d101c8cea16ffb0079496b8fe8 -----BEGIN PGP SIGNATURE-----
iQIzBAEBCAAdFiEEYTOs4fS4fFHb8/6l6GEFEPmm6SIFAmI5rIkACgkQ6GEFEPmm
6SLORRAAg130ufd3X1//RUGK+v9m/kxUieaLCSE5A6xjcuapWsfhOJVKH5AOH03q
VZCf4e79i8U4WphpfHMdM81x+zvtxZh0Q+OgumEC9rQXmHeRUZI/mIsdo3Yq3cHE
H9ljQLKlam+WVadW4mbSWLb0Bu7KJhtnt0530zClzgPQPpOo9wNmT1rSYGXHTySn
55WCmzsEWL4CSGKhqclDnIAaK8mvKEgs0rRK/XauiBBrn9PfzJU8Ldxne01tpLMa
NNyWiTV6WG9rNHNkqeM18cFQF4mCApYEQCY9C7qh59EgkWt2dTtlZZmmzNcYXPwH
UskEog5/NAhFUuOhO+r2rOOqGi7zp+tJ+TAPG0H9uPJwr8ZcArBAJ1wZV/ub7v08
jTCgMi5wSGy2gJjzvhk437JdD1WfNHLkA0SJPxs8VtyUVifR0lwqn4uCMrusY8fi
XTtkaa3lcd3zMaDfj0CSBHSs9MAnB2JKMGYw0lVrWIriI/xFf/SPnP1LMalkWKZu
NzGkHz/BWprCgk3VHkox8XhCou/gXK7AlAQNNmYS5qS0OGwFqWN04e7Gyen5yz/R
s5NsCI5KGgDCkxTFjEuvGS/ZH5IxoIpM2Oa7mv3eHp1jkFjcbEQU921lh/ZDmhs7
7imrhZYV5HfBqeVol4EgiHaSUFpT+DO195sm+h3ndf+rP1+eeDw= =fs3t -----END PGP SIGNATURE-----
CannaHome next? (via darknetlive.com at

https://darknetlive.com/post/dread-now-has-an-i2p-mirror-ddos-update/)

Australian Trio Arrested for Selling Drugs on the Darkweb

Australian Trio Arrested for Selling Drugs on the Dark Web In New South Wales, Australia, authorities arrested and charged three people suspected of distributing illicit drugs through the darkweb. According to a press release by the NSW Police, the defendants-two men aged 47 and 30 and a 42-year-old woman-made approximately $1.185 million from the sale of large quantities of drugs, including E-cigarettes containing THC and synthetic cannabinoids on the darkweb. __ Are they missing their back plates? The State Crime Command's Cybercrime Squad's "Strike Force Alaine&rdquo; started investigating darkweb drug vendors in the Lake Macquarie area in May 2021. During the investigation, law enforcement officers learned that the defendants had cashed out cryptocurrency worth $1.185 million through their bank accounts. __ On April 12, 2022, the investigators executed search warrants on two properties allegedly linked to the defendants. The searches resulted in the seizure of more than 100 liters of THC analogs, 15 kilograms of lollipops laced with illegal drugs, and electronic devices. Officers arrested all three defendants after searching their properties. __ The 47-year-old man and 42-year-old woman were arrested befoe the third suspect. Cybercrime Squad Commander, Detective Acting Superintendent Gordon Arbinja: "These arrests should serve as a warning to those using the internet to conceal criminal activity, your anonymity is not guaranteed, and you aren't outside the reach of law enforcement.&rdquo; The 47-year-old man and a 42-year-old woman were charged with three counts of supplying a psychoactive substance for human consumption, eight counts of supplying a prohibited drug, knowingly dealing with the proceeds of crime, knowingly directing a criminal group to assist crime, and participating in a criminal group contributing to criminal activity. __ The duo was denied bail and is set to appear before the Belmont Local Court on April 13, 2022. The 30-year-old man was charged with three counts of knowingly supplying a psychoactive substance for human consumption, eight counts of supplying a prohibited drug, and participating in a criminal group. __ Police seized "seized more than 100 litres of THC-based chemicals and 15kg of lollipops ... laced with a prohibited drug.&rdquo; He was granted bail and will appear before the Belmont Local Court on April 20, 2022. archive.org (via darknetlive.com at https://darknetlive.com/post/australian-trio-arrested-for-selling-drugs-on-the-darkweb/)

Feds Seized RaidForums

The United States Department of Justice announced the seizure of RaidForums, "a popular marketplace for cybercriminals to buy and sell hacked data.&rdquo; An ongoing investigation led by the FBI's Washington Field Office and the U.S. Secret Service resulted in the seizure of the popular cybercrime forum RaidForums and the arrest of the alleged creator of the site, Diogo Santos Coelho. Police in the United Kingdom arrested Coelho on January 31, 2022. A recently unsealed six-count indictment charged Coelho with conspiracy, access device fraud, and aggravated identify theft. The indictment accuses Coelho of creating and operating RaidForums from January 1, 2015, to January 31, 2022. On April 11, 2022, the Department of Justice announced the seizure of "Raidforums.com,&rdquo; "Rf.ws,&rdquo; and "Raid.lol.&rdquo; "RaidForums served as a major online marketplace for individuals to buy and sell hacked or stolen databases containing the sensitive personal and financial information of victims in the United States and elsewhere, including stolen bank routing and account numbers, credit card information, login credentials, and social security numbers. Before its seizure, RaidForums members used the platform to offer for sale hundreds of databases of stolen data containing more than 10 billion unique records for individuals residing in the United States and internationally.&rdquo; __ The seizure banner visible at RaidForums.com In addition to creating and administrating the site, Coelho allegedly sold hacked or stolen information to RaidForums users and operated a fee-based "Official Middleman&rdquo; service. According to the indictment, "Coelho offered to accept cryptocurrency from the purchaser and files, including stolen access devices and means of identification, from the seller.&rdquo; Coelho then ensured the buyer and seller were satisfied with the transaction and released the funds to the seller and the files or data to the customer. During the investigation, law enforcement officers operating in an undercover capacity purchased social security numbers, email addresses, passwords, and bank routing and account numbers from sellers on RaidForums. Coelho interacted with undercover law enforcement officers on several occasions, including his alleged role as a middleman and seller. In one interaction described in the indictment, feds spent $4,000 in Bitcoin on 1.1 million "payment card account numbers, names, addresses, and phone numbers associated with the payment card account numbers&rdquo; but received nothing in return. "On or about December 16, 2018, COELHO, who was using the moniker "Downloading,&rdquo; made a posting on the RaidForums website, which offered for sale 2.3 million payment card account numbers, including the names, addresses, and phone numbers associated with the payment card account numbers, which were purportedly obtained from a breach of records belonging to United States hotels.&rdquo;   "On or about March 4, 2019, in the Eastern District of Virginia and elsewhere, COELHO, who was using the moniker "Downloading,&rdquo; provided an undercover law enforcement officer with three stolen access devices, to wit, payment card account numbers, card verification values, expiration dates, and the names associated with the payment cards. COELHO agreed to this exchange to convince the undercover law enforcement officer that "Downloading&rdquo; could be trusted to sell approximately 1.1 million stolen access devices in exchange for a Bitcoin amount that was equivalent to approximately $4,000 at the time.&rdquo;   "On or about March 5, 2019, in the Eastern District of Virginia and elsewhere, Coelho, who was using the monikers "Downloading,&rdquo; "Omnipotent,&rdquo; and "Shiza,&rdquo; arranged to both sell and serve as the middleman in the transaction to sell approximately 1.1 million stolen access devices to the undercover law enforcement officer. Coelho received a Bitcoin amount that was then equivalent to approximately $4,000; however, he did not provide the stolen access devices.&rdquo; In a different undercover transaction described in the indictment, the RaidForums user "SubVirt&rdquo; listed 30 million records stolen from a major telecommunications company and wireless network operator. The records included "customer names, social security numbers, dates of birth, driver's license numbers, phone numbers, billing account numbers, customer relationship manager information. Mobile Station Integrated Services Digital Network (MSISDN) information. International Mobile Subscriber Identity (IMSI) numbers, and International Mobile Equipment Identity (IMEI) numbers.&rdquo; A third-party operating on behalf of the hacked telecom company then purchased the data, using Coelho's middleman service. RaidForums before the raid.   The indictment also accuses Coelho of falsely registering a domain name. "On or about June 6, 2018, Coelho, using the moniker "Omnipotent,&rdquo; transferred the false registration of the domain "Raidforums.com&rdquo; to a U.S.-based domain registrar based in Phoenix, Arizona using the alias "Kevin Maradona.&rdquo; Coelho falsely registered the domain name knowing that it was used to support the RaidForums website in furtherance of the conspiracy.&rdquo; Several law enforcement agencies assisted the FBI and USSS in the investigation, including the Joint Cybercrime Action Taskforce (Europol), National Crime Agency, Swedish Police Authority, Romanian National Police, Judicial Police, Internal Revenue Service Criminal Investigation, and the Federal Criminal Police Office. "Our interagency efforts to dismantle this sophisticated online platform - which facilitated a wide range of criminal activity - should come as a relief to the millions victimized by it, and as a warning to those cybercriminals who participated in these types of nefarious activities,&rdquo; said Jessica D. Aber, U.S. Attorney for the Eastern District of Virginia. "Online anonymity was not able to protect the defendant in this case from prosecution, and it will not protect other online criminals either.&rdquo; Coelho is in custody in the U.K. pending the results of an extradition hearing. archive.is/ archive.org indictment (via darknetlive.com at https://darknetlive.com/post/feds-seized-raidforum/)

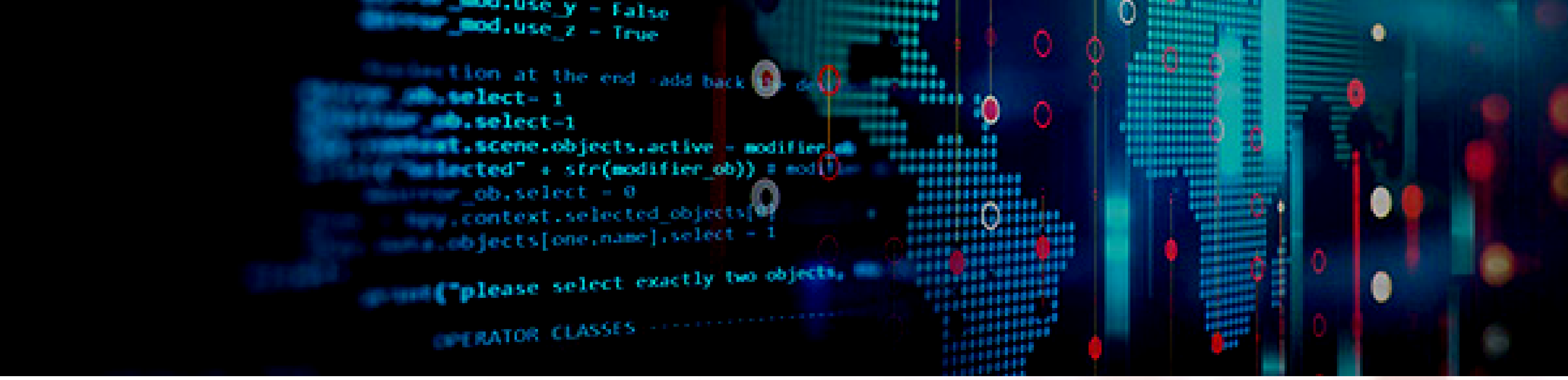
Dark Web Link

Top Darknet Markets 2022: The Outstanding Performances To Consider Now
The darknet markets are subject to availability and one of the many factors that contributes to the working of these dark web markets is their performances. The top darknet markets 2022 is the example where each of the marketplaces in the Tor network has proven its performance over and over again. So, in this article [...] The post Top Darknet Markets 2022: The Outstanding Performances To Consider Now appeared first on Dark Web Link | Deep web Onion Links | Darknet News.
Breaking Bad Forum On The Darknet Is Revolutionary

The Breaking Bad Forum housed by the Tor network is a revolutionary darknet site indeed! So many forums exist on the dark web. But nothing could match the vibe of something like Breaking Bad. In this article, we will take you through the various aspects of the new forum. Breaking Bad Forum: A Gist Breaking [...] The post Breaking Bad Forum On The Darknet Is Revolutionary appeared first on Dark Web Link | Deep web Onion Links | Darknet News.

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

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



Trend Micro Anti-Malware Blog

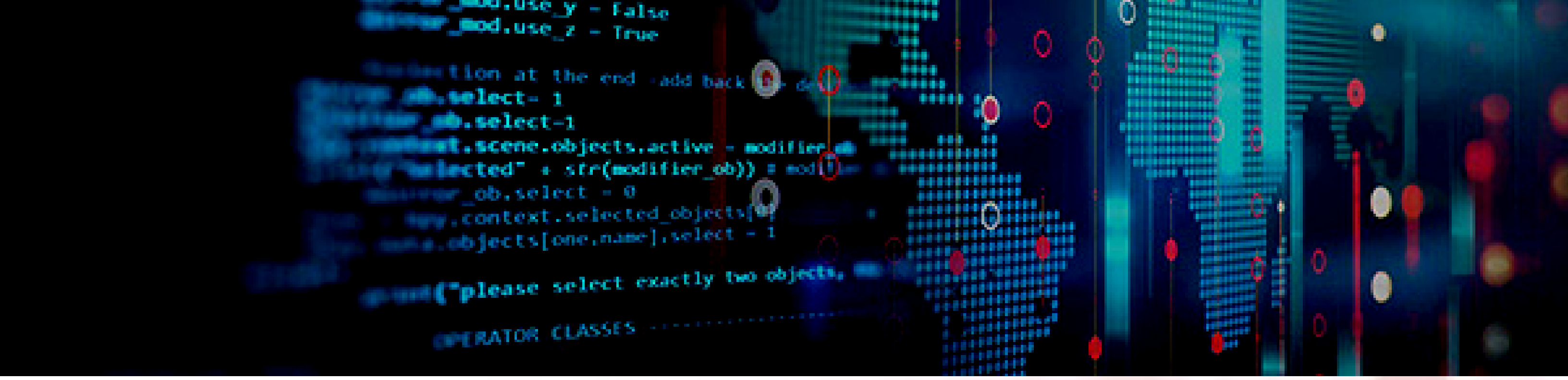
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

* RiskIQ Threat Intelligence Roundup: Trickbot, Magecart, and More Fake Sites Targeting Ukraine
* RiskIQ Threat Intelligence Roundup: Campaigns Targeting Ukraine and Global Malware Infrastructure
* RiskIQ Threat Intelligence Supercharges Microsoft Threat Detection and Response
* RiskIQ Intelligence Roundup: Spoofed Sites and Surprising Infrastructure Connections
* RiskIQ Threat Intelligence Roundup: QBot, Magecart, Agent Tesla Headline Hijacked Infrastructure&nbsp
* RiskIQ Threat Intelligence Roundup: C2 and Nation-State Threat Infrastructure
* Jupyter Notebooks Make RiskIQ Data a Digital 'Mech Suit' for Threat Intelligence Analysts
* "Offshore" Shinjiru Provides Bulletproof Services to Cyberattackers
* Retailers Using WooCommerce are at Risk of Magecart Attacks
* 5 Tips to Stay on the Offensive and Safeguard Your Attack Surface

FireEye

* Opportunistic Exploitation of WSO2 CVE-2022-29464
* Metasploit Weekly Wrap-Up
* Rapid7 Named a Visionary in 2022 Magic Quadrantâ„¢ for Application Security Testing Second Year in a
* 2022 Cloud Misconfigurations Report: A Quick Look at the Latest Cloud Security Breaches and Attack Tr
* What's New in InsightVM and Nexpose: Q1 2022 in Review
* Metasploit Weekly Wrap-Up
* Let's Dance: InsightAppSec and tCell Bring New DevSecOps Improvements in Q1
* InsightCloudSec Supports the Recently Updated NSA/CISA Kubernetes Hardening Guide
* CVE-2022-28810: ManageEngine ADSelfService Plus Authenticated Command Execution (Fixed)
* [Security Nation] Kate Stewart on Open-Source Projects at the Linux Foundation



Advisories

US-Cert Alerts & bulletins

* FBI Releases IOCs Associated with BlackCat/ALPHV Ransomware
* Drupal Releases Security Updates
* Cisco Releases Security Updates for Multiple Products
* Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure
* Oracle Releases April 2022 Critical Patch Update
* CISA Adds Three Known Exploited Vulnerabilities to Catalog
* CISA Releases Secure Cloud Business Applications (SCuBA) Guidance Documents for Public Comment
* North Korean State-Sponsored APT Targets Blockchain Companies
* AA22-110A: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure
* AA22-108A: TraderTraitor: North Korean State-Sponsored APT Targets Blockchain Companies
* Vulnerability Summary for the Week of April 11, 2022
* Vulnerability Summary for the Week of April 4, 2022

Zero Day Initiative Advisories

ZDI-CAN-17057: Softing
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 'Flashback Team: Pedro Ribeiro (@pedrib1337) && Radek Domanski (@RabbitPro)' was reported to the affected vendor on: 2022-04-15, 10 days ago. The vendor is given until 2022-08-13 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-17060: Softing
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 'Flashback Team: Pedro Ribeiro (@pedrib1337) && Radek Domanski (@RabbitPro)' was reported to the affected vendor on: 2022-04-15, 10 days ago. The vendor is given until 2022-08-13 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-17059: Softing
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 'Flashback Team: Pedro Ribeiro (@pedrib1337) && Radek Domanski (@RabbitPro)' was reported to the affected vendor on: 2022-04-15, 10 days ago. The vendor is given until 2022-08-13 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-16253: ICONICS
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 'Alex Birnberg of Zymo Security' was reported to the affected vendor on: 2022-04-14, 11 days ago. The vendor is given until 2022-08-12 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-17125: Adobe
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-04-13, 12 days ago. The vendor

is given until 2022-08-11 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-15984: Cisco

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 'Q. Kaiser from IoT Inspector Research Lab' was reported to the affected vendor on: 2022-04-13, 12 days ago. The vendor is given until 2022-08-11 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-17077: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-04-13, 12 days ago. The vendor is given until 2022-08-11 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-17072: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-04-13, 12 days ago. The vendor is given until 2022-08-11 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-16955: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'kdot' was reported to the affected vendor on: 2022-04-13, 12 days ago. The vendor is given until 2022-08-11 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-17128: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-04-13, 12 days ago. The vendor is given until 2022-08-11 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-17074: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-04-13, 12 days ago. The vendor is given until 2022-08-11 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-17126: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-04-13, 12 days ago. The vendor is given until 2022-08-11 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-17075: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-04-13, 12 days ago. The vendor is given until 2022-08-11 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-17127: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-04-13, 12 days ago. The vendor is given until 2022-08-11 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-17076: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of

Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-04-13, 12 days ago. The vendor is given until 2022-08-11 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-17073: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-04-13, 12 days ago. The vendor is given until 2022-08-11 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-15905: D-Link

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 'Anonymous' was reported to the affected vendor on: 2022-04-13, 12 days ago. The vendor is given until 2022-08-11 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-15906: D-Link

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 'Anonymous' was reported to the affected vendor on: 2022-04-13, 12 days ago. The vendor is given until 2022-08-11 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-16525: Trend Micro

A CVSS score 5.5 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N) severity vulnerability discovered by 'Abdelhamid Naceri' was reported to the affected vendor on: 2022-04-13, 12 days ago. The vendor is given until 2022-08-11 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-17084: 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 'Simon Zuckerbraun - Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-04-06, 19 days ago. The vendor is given until 2022-08-04 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-17083: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-04-06, 19 days ago. The vendor is given until 2022-08-04 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-17079: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-04-06, 19 days ago. The vendor is given until 2022-08-04 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-17082: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-04-06, 19 days ago. The vendor is given until 2022-08-04 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-17078: Adobe

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2022-04-06, 19 days ago. The vendor is given until 2022-08-04 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 2022-1461-01]
Red Hat Security Advisory 2022-1461-01 - Updates have been made to Logging Subsystem 5.4 - Red Hat OpenShift. Issues addressed include denial of service and man-in-the-middle vulnerabilities.
[Red Hat Security Advisory 2022-1476-01]
Red Hat Security Advisory 2022-1476-01 - Red Hat Advanced Cluster Management for Kubernetes 2.4.3 images Red Hat Advanced Cluster Management for Kubernetes provides the capabilities to address common challenges that administrators and site reliability engineers face as they work across a range of public and private cloud environments. Clusters and applications are all visible and managed from a single console&mdash;with security policy built in. This advisory contains the container images for Red Hat Advanced Cluster Management for Kubernetes, which provide some security fixes and bug fixes. Issues addressed include an information leakage vulnerability.
[Red Hat Security Advisory 2022-1363-01]
Red Hat Security Advisory 2022-1363-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the container images for Red Hat OpenShift Container Platform 4.9.29.
[Ubuntu Security Notice USN-5385-1]
Ubuntu Security Notice 5385-1 - Brendan Dolan-Gavitt discovered that the aQuantia AQtion Ethernet device driver in the Linux kernel did not properly validate meta-data coming from the device. A local attacker who can control an emulated device can use this to cause a denial of service or possibly execute arbitrary code. It was discovered that the UDF file system implementation in the Linux kernel could attempt to dereference a null pointer in some situations. An attacker could use this to construct a malicious UDF image that, when mounted and operated on, could cause a denial of service.
[Ubuntu Security Notice USN-5384-1]
Ubuntu Security Notice 5384-1 - It was discovered that the UDF file system implementation in the Linux kernel could attempt to dereference a null pointer in some situations. An attacker could use this to construct a malicious UDF image that, when mounted and operated on, could cause a denial of service. Lyu Tao discovered that the NFS implementation in the Linux kernel did not properly handle requests to open a directory on a regular file. A local attacker could use this to expose sensitive information.
[Ubuntu Security Notice USN-5383-1]
Ubuntu Security Notice 5383-1 - David Bouman discovered that the netfilter subsystem in the Linux kernel did not properly validate passed user register indices. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. Brendan Dolan-Gavitt discovered that the Marvell WiFi-Ex USB device driver in the Linux kernel did not properly handle some error conditions. A physically proximate attacker could use this to cause a denial of service.
[Ubuntu Security Notice USN-5381-1]
Ubuntu Security Notice 5381-1 - David Bouman discovered that the netfilter subsystem in the Linux kernel did not properly validate passed user register indices. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. It was discovered that the block layer subsystem in the Linux kernel did not properly initialize memory in some situations. A privileged local attacker could use this to expose sensitive information.
[Ubuntu Security Notice USN-5382-1]
Ubuntu Security Notice 5382-1 - Albin Eldst&aring;l-Ahrens and Lukas Lamster discovered libinput did not properly handle input devices with specially crafted names. A local attacker with physical access could use this to cause libinput to crash or expose sensitive information.
[Red Hat Security Advisory 2022-1389-01]
Red Hat Security Advisory 2022-1389-01 - This release adds the new Apache HTTP Server 2.4.37 Service Pack 11 packages that are part of the JBoss Core Services offering. This release serves as a replacement for Red Hat JBoss Core Services Apache HTTP Server 2.4.37 Service Pack 10 and includes bug fixes and

enhancements. Issues addressed include HTTP request smuggling, buffer overflow, bypass, null pointer, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-1443-01

Red Hat Security Advisory 2022-1443-01 - The java-11-openjdk packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Software Development Kit.

Red Hat Security Advisory 2022-1390-01

Red Hat Security Advisory 2022-1390-01 - Red Hat JBoss Core Services is a set of supplementary software for Red Hat JBoss middleware products. This software, such as Apache HTTP Server, is common to multiple JBoss middleware products, and is packaged under Red Hat JBoss Core Services to allow for faster distribution of updates, and for a more consistent update experience. This release adds the new Apache HTTP Server 2.4.37 Service Pack 11 packages that are part of the JBoss Core Services offering. This release serves as a replacement for Red Hat JBoss Core Services Apache HTTP Server 2.4.37 Service Pack 10 and includes bug fixes and enhancements. Issues addressed include HTTP request smuggling, buffer overflow, bypass, null pointer, and use-after-free vulnerabilities.

Red Hat Security Advisory 2022-1478-01

Red Hat Security Advisory 2022-1478-01 - Red Hat Satellite is a system management solution that allows organizations to configure and maintain their systems without the necessity to provide public Internet access to their servers or other client systems. It performs provisioning and configuration management of predefined standard operating environments.

Red Hat Security Advisory 2022-1455-01

Red Hat Security Advisory 2022-1455-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include out of bounds write and privilege escalation vulnerabilities.

Red Hat Security Advisory 2022-1444-01

Red Hat Security Advisory 2022-1444-01 - The java-11-openjdk packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Software Development Kit.

Red Hat Security Advisory 2022-1441-01

Red Hat Security Advisory 2022-1441-01 - The java-11-openjdk packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Software Development Kit.

Red Hat Security Advisory 2022-1469-01

Red Hat Security Advisory 2022-1469-01 - Red Hat Single Sign-On 7.5 is a standalone server, based on the Keycloak project, that provides authentication and standards-based single sign-on capabilities for web and mobile applications. This release of Red Hat Single Sign-On 7.5.2 serves as a replacement for Red Hat Single Sign-On 7.5.1, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-1463-01

Red Hat Security Advisory 2022-1463-01 - Red Hat Single Sign-On 7.5 is a standalone server, based on the Keycloak project, that provides authentication and standards-based single sign-on capabilities for web and mobile applications. This release of Red Hat Single Sign-On 7.5.2 on RHEL 8 serves as a replacement for Red Hat Single Sign-On 7.5.1, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-1445-01

Red Hat Security Advisory 2022-1445-01 - The java-17-openjdk packages provide the OpenJDK 17 Java Runtime Environment and the OpenJDK 17 Java Software Development Kit.

Red Hat Security Advisory 2022-1336-01

Red Hat Security Advisory 2022-1336-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-1440-01

Red Hat Security Advisory 2022-1440-01 - The java-11-openjdk packages provide the OpenJDK 11 Java

Runtime Environment and the OpenJDK 11 Java Software Development Kit.

Red Hat Security Advisory 2022-1462-01

Red Hat Security Advisory 2022-1462-01 - Red Hat Single Sign-On 7.5 is a standalone server, based on the Keycloak project, that provides authentication and standards-based single sign-on capabilities for web and mobile applications. This release of Red Hat Single Sign-On 7.5.2 on RHEL 7 serves as a replacement for Red Hat Single Sign-On 7.5.1, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-1442-01

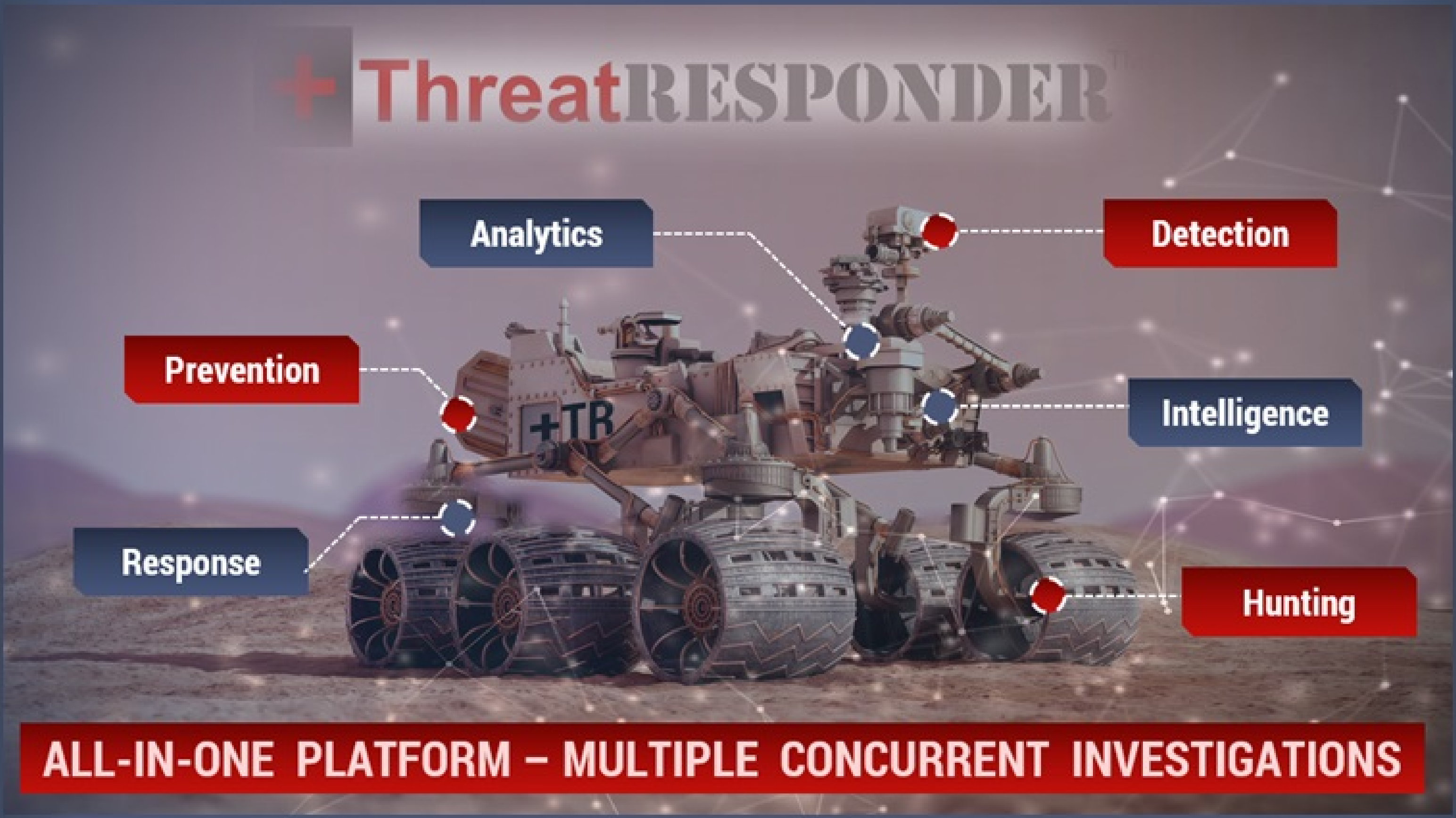
Red Hat Security Advisory 2022-1442-01 - The java-11-openjdk packages provide the OpenJDK 11 Java Runtime Environment and the OpenJDK 11 Java Software Development Kit.

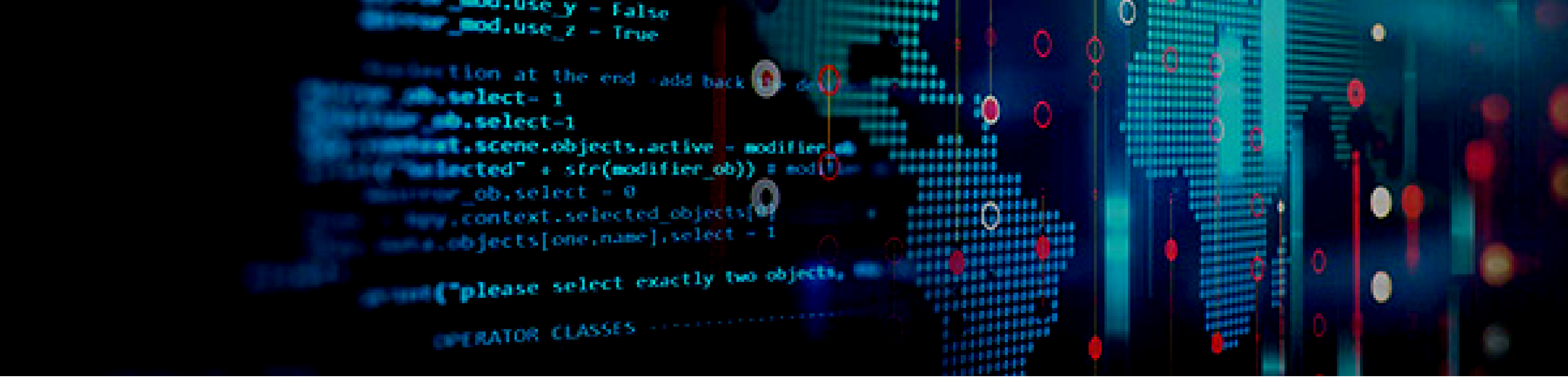
Ubuntu Security Notice USN-5380-1

Ubuntu Security Notice 5380-1 - It was discovered that Bash did not properly drop privileges when the binary had the setuid bit enabled. An attacker could possibly use this issue to escalate privileges.

Red Hat Security Advisory 2022-1418-01

Red Hat Security Advisory 2022-1418-01 - 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. Issues addressed include out of bounds write and privilege escalation vulnerabilities.


ThreatRESPONDER
Analytics
Detection
Prevention
+TR
Intelligence
Response
Hunting
ALL-IN-ONE PLATFORM – MULTIPLE CONCURRENT INVESTIGATIONS



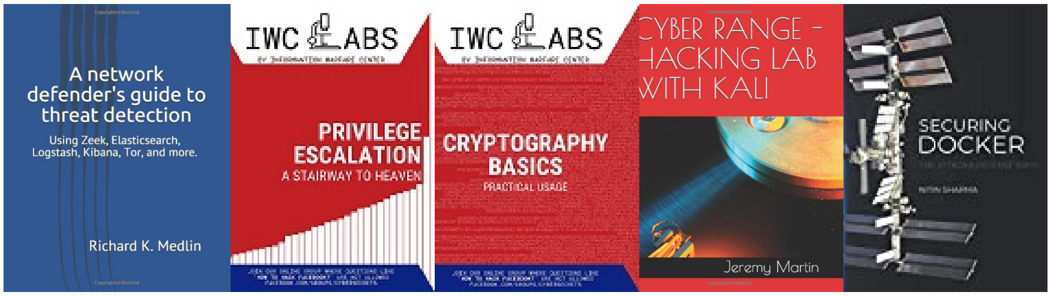
The Cyber Secrets publications on Amazon

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.

CYBER Secrets
Information Warfare Center
What's Inside?
Threat Intelligence & Training
Visit our YouTube Channel
CYBER SECRETS
DIVE INTO THE 5TH DOMAIN THREAT INTELLIGENCE
CYBER SECRETS
RED TEAMING AROUND YOUR BACKYARD
WHILE DRINKING OUR JUICE IN THE HOOD
CYBER SECRETS
THE 8 LAYERS OF THE OSI CAKE
A FORENSIC TASTE OF EACH LAYER
CYBER SECRETS
LAUNCHING EXPLOITS
ONE SMALL VULNERABILITY FOR A COMPANY, ONE GIANT HEAP FOR PORT BIND.
INCIDENT RESPONSE DO NOT CROSS
CYBER SECRETS
INCIDENT RESPONSE
EVIDENCE PRESERVATION AND COLLECTION

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