Apr-18-22

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

April 18, 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

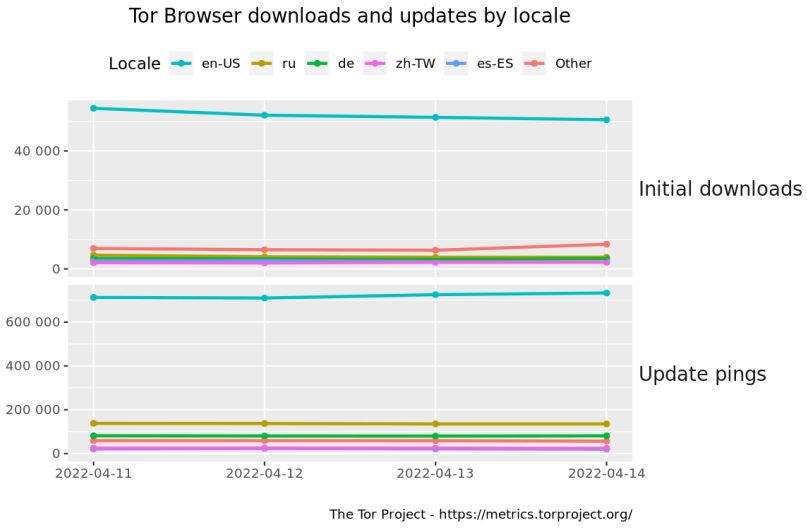
Internet Storm Center Infocon Status

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

* FBI Says North Korea Behind Biggest Crypto Theft In History Against Axie Infinity
* Google Issues Third Emergency Fix For Chrome This Year
* Cisco's WebEx App Phoned Home Audio Telemetry Even When Muted
* North Korea's Lazarus Caught Spying On Chemical Sector Companies
* Preparing For Armageddon: How Ukraine Battles Russian Hackers
* Threat Group Builds Custom Malware To Attack Industrial Systems
* Apache Says Struts 2 Security Bug Wasn't Fully Fixed In 2020
* Microsoft Disrupts Ransomware Spreading Botnet
* Home Office's Visa Service Apologizes For Email Address Data Breach
* How Facial Recognition Is Identifying The Dead In Ukraine
* Sandworm Hackers Attempted A Third Blackout In Ukraine
* Microsoft Zero Days, Wormable Bugs Spark Concern
* Enemybot: A New Mirai, Gafgyt Hybrid Botnet Joins The Scene
* Menswear Brand Zenga Reveals Ransomware Attack
* Cryptocurrency Expert Jailed For Helping North Korea Evade Sanctions
* Account Takeover Poised To Surpass Malware As The No. 1 Security Concern
* T-Mobile Secretly Bought Its Customer Data From Hackers To Stop Leak. It Failed
* U.S. And European Partners Take Down Hacker Website RaidForums
* Critical Bug Allows Attacker To Remote Control Medical Robot
* DuckDuckGo Announces A New Privacy Focused Mac Browser
* Microsoft Takes Down Domains Used In Cyberattack Against Ukraine
* Driverless Car Appears To Flee The Scene After Being Pulled Over By Cops
* How Identity And Access Management Fits Into Zero Trust
* OpenSSH Now Defaults To Protecting Against Quantum Computer Attacks
* Spring4Shell Is Now Being Used To Spread This Botnet Malware

Krebs on Security

* 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
* A Closer Look at the LAPSUS$ Data Extortion Group
* 'Spam Nation' Villain Vrublevsky Charged With Fraud

Dark Reading

* Upgrades for Spring Framework Have Stalled
* Google Emergency Update Fixes Chrome Zero-Day
* Cloud Cost, Reliability Raise IT Concerns
* Lazarus Targets Chemical Sector With 'Dream Jobs,' Then Trojans
* CISA Alert on ICS, SCADA Devices Highlights Growing Enterprise IoT Security Risks
* Cybersecurity Act of 2022: A Step in the Right Direction With a Significant Loophole
* greymatter.io Closes $7.1 Million Series A to Meet Rising Need for Its Enterprise Microservices Platf
* Kaspersky Relocates Cyberthreat-Related Data Processing for Users in Latin America and Middle East to
* New Malware Tools Pose 'Clear and Present Threat' to ICS Environments
* Data Scientists, Watch Out: Attackers Have Your Number
* Inside a Data Center Outage: Lessons About Resilience
* The Misconceptions of 2021's Black Swan Cyber Events
* Secure Systems Need Hardware-Enhanced Tools, Intel Says
* Microsoft Leads Operation to Disrupt Zloader Botnet
* KKR to Acquire Barracuda Networks
* More Than 60% of Organizations Suffered a Breach in the Past 12 Months
* Palo Alto Networks Extends SASE to Protect Home Networks With Okyo Garde Enterprise Edition
* Securing the Stopgap: Controlling Access to SaaS Applications
* Supply and Demand Hits Cybersecurity: Navigating the Skills Shortage
* Identifying a Vulnerability in the SAP Software Supply Chain

The Hacker News

* New Hacking Campaign Targeting Ukrainian Government with IcedID Malware
* Critical RCE Flaw Reported in WordPress Elementor Website Builder Plugin
* Lazarus Group Behind $540 Million Axie Infinity Crypto Hack and Attacks on Chemical Sector
* Get Lifetime Access to This 60-Hour Java Programming Training Bundle @ 97% Discount
* GitHub Says Hackers Breached Dozens of Organizations Using Stolen OAuth Access Tokens
* JekyllBot:5 Flaws Let Attackers Take Control of Aethon TUG Hospital Robots
* Haskers Gang Gives Away ZingoStealer Malware to Other Cybercriminals for Free
* Critical Auth Bypass Bug Reported in Cisco Wireless LAN Controller Software
* As State-Backed Cyber Threats Grow, Here's How the World Is Reacting
* Critical VMware Cloud Director Bug Could Let Hackers Takeover Entire Cloud Infrastructure
* Google Releases Urgent Chrome Update to Patch Actively Exploited Zero-Day Flaw
* Ethereum Developer Jailed 63 Months for Helping North Korea Evade Sanctions
* Rarible NFT Marketplace Flaw Could've Let Attackers Hijack Crypto Wallets
* New EnemyBot DDoS Botnet Borrows Exploit Code from Mirai and Gafgyt
* Microsoft Disrupts ZLoader Cybercrime Botnet in Global Operation

Security Week

* OHSU Apologizes After Phishing Test Draws Complaints
* North Korea APT Lazarus Targeting Chemical Sector
* Juniper Networks Patches Vulnerabilities in Contrail Networking, Junos OS
* House Panels Probe Gov't Use of Facial Recognition Software
* Conti Ransomware Gang Claims Cyberattack on Wind Turbine Giant Nordex
* New 'Enemybot' DDoS Botnet Targets Routers, Web Servers
* Google Patches Third Actively Exploited Chrome Zero-Day of 2022
* U.S. Gov Blames North Korea Hackers for $600M Cryptocurrency Heist
* Critical Code Execution Flaw Haunts VMware Cloud Director
* Cloud Security Startup DoControl Raises $30 Million
* Obsidian Raises $90 Million for SaaS Security Platform
* Critical Vulnerability in Elementor Plugin Impacts Millions of WordPress Sites
* Several Vulnerabilities Allow Disabling of Palo Alto Networks Products
* Cisco Patches Critical Vulnerability in Wireless LAN Controller
* Russia-Linked Pipedream/Incontroller ICS Malware Designed to Target Energy Facilities
* VMware Confirms Workspace One Exploits in the Wild
* U.S. Warns Sophisticated ICS/SCADA Malware Can Damage Critical Infrastructure
* Microsoft Seizes Control of Notorious Zloader Cybercrime Botnet
* Ransomware Claims Trending Downward, Insurance Firm Says
* Wind Turbine Giant Nordex Scrambling to Recover From Cyberattack
* MDR Provider Critical Start Lands $215 Million Growth Investment
* Flaws in ABB Network Interface Modules Expose Industrial Systems to DoS Attacks
* Citrix Patches Vulnerabilities in Several Products
* ICS Patch Tuesday: Siemens, Schneider Fix Several Critical Vulnerabilities
* SAP Releases Patches for Spring4Shell Vulnerability
* Silverfort Banks $65 Million for Identity Threat Protection Platform

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* Q1 2022 Report: Holiday-Themed Phishing Emails Get Employees to Click
* Storytelling to Improve Your Organization's Security Culture [PODCAST]
* Reduce Your Chances of Getting Scammed
* Strategies to Achieve Compliance and Real Risk Reduction at the Same Time
* Small and Medium Businesses Account for Nearly Half of all Ransomware Victim Organizations
* One in Three U.K. Businesses Experience Cyber Attacks Weekly
* Meta Stops Three Cyber Espionage Groups Targeting Critical Industries
* Smishing Scams Abuse Name of Legitimate Ukrainian Charity
* CyberheistNews Vol 12 #15 [Heads Up] Hard-boiled Social Engineering by a Fake "Emergency Data Request
* Business Email Compromise (BEC): the Costliest Cybercrime

ISC2.org Blog

* SECURE London stokes debate on the future of the cybersecurity workforce
* WINNING TACTICS FOR SECURITY AWARENESS INNOVATIONS via EXPERIENCE (2 of 2)
* We Stand with All of You
* What Do You Mean My Email Isn't Free?
* What is Neurodiversity? Understanding Neurodiversity and its Prominence in Cybersecurity

HackRead

* GitHub Blocks Accounts of Two Large Russian Banks Amid US Sanctions
* GitHub: Hackers Stole OAuth Access Tokens to Target Dozens of Firms
* Latest Update for Google Chrome Fixes Actively Exploited 0-day Flaw
* Conti Ransomware Gang Hits German Wind Turbine Giant Nordex
* Rarible NFT Market Vulnerability Authorized Attackers to Transfer Crypto Assets
* Ukraine Thwart Russian Industroyer 2 Malware Attack on Energy Provider
* "Ethical Hacker" Stole Half a Million in Crypto Form Elderly Person

Koddos

* GitHub Blocks Accounts of Two Large Russian Banks Amid US Sanctions
* GitHub: Hackers Stole OAuth Access Tokens to Target Dozens of Firms
* Latest Update for Google Chrome Fixes Actively Exploited 0-day Flaw
* Conti Ransomware Gang Hits German Wind Turbine Giant Nordex
* Rarible NFT Market Vulnerability Authorized Attackers to Transfer Crypto Assets
* Ukraine Thwart Russian Industroyer 2 Malware Attack on Energy Provider
* "Ethical Hacker" Stole Half a Million in Crypto Form Elderly Person

Naked Security

* 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!
* S3 Ep77: Bugs, busts and old-school PDP-11 hacking [Podcast]
* Serious Security: Darkweb drugs market Hydra taken offline by German police
* Firefox 99 is out - no major bugs, but update anyway!
* Google's monthly Android updates patch numerous "get root" holes

Threat Post

* Karakurt Ensnares Conti, Diavol Ransomware Groups in Its Web
* Feds: APTs Have Tools That Can Take Over Critical Infrastructure
* Feds Shut Down RaidForums Hacking Marketplace
* Microsoft Zero-Days, Wormable Bugs Spark Concern
* Menswear Brand Zegna Reveals Ransomware Attack
* Microsoft Takes Down Domains Used in Cyberattack Against Ukraine
* Google Play Bitten by Sharkbot Info-stealer 'AV Solution'
* SSRF Flaw in Fintech Platform Allowed for Compromise of Bank Accounts
* MacOS Malware: Myth vs. Truth - Podcast
* Attackers Spoof WhatsApp Voice-Message Alerts to Steal Info

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

* The steady march of general-purpose databases
* How to minimize new technical debt
* 9 low-rent cloud providers to challenge AWS, Azure, and GCP
* JetBrains IntelliJ IDEA adds dependency analyzer
* Microsoft .NET 7 Preview 3 focuses on speedups
* Approach cloud architecture from the outside in
* What is CI/CD? Continuous integration and continuous delivery explained
* Virtualenv and venv: Python virtual environments explained
* Atlassian unveils Compass collaboration portal for developers
* How to enforce architecture rules in C#

C4ISRNET - Media for the Intelligence Age Military

* US and India launch talks about military AI
* Ukraine conflict heightens US military's data privacy vulnerabilities
* Cyberattacks don't win wars
* Defense Intelligence Agency cites 70% growth in Russia and China's combined space assets since 2019
* Putin is holding GPS hostage - Here's how to get it back
* Space companies investing in small satellite production capacity as customers shift to hybrid archite
* NORTHCOM wants millions more for AI and data handling
* SPACECOM requests more funding for key space domain awareness center
* Cyber Mission Force could continue growing, says commander
* US Space Force to test experimental navigation satellite in upcoming Army exercise

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

* CVE-2021-1782, an iOS in-the-wild vulnerability in vouchers
* CVE-2021-30737, @xerub's 2021 iOS ASN.1 Vulnerability

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.

* b01lers CTF
* CUCTF 1.0
* Incognito 3.0
* MidnightFlag - INFEKTION 2022
* RuCTF 2022
* Simulations Arcade Hack CTF
* NahamCon CTF 2022
* PatriotCTF
* Digital Overdose Conference 2022 CTF
* ångstromCTF 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

* Haveged 1.9.18
* OpenSSH 9.0p1
* Wireshark Analyzer 3.6.3
* Adversary3 1.0
* nfstream 6.4.3
* OpenSSL Toolkit 3.0.2
* OpenSSL Toolkit 1.1.1n
* Falco 0.31.1
* UFONet 1.8
* Samhain File Integrity Checker 4.4.7

Kali Linux Tutorials

* Codecat v0.56 : An Open-Source Tool To Help You Find/Track User Input Sinks And Security Bugs
* Nivistealer : Steal Victim Images Exact Location Device Info And Much More
* ASSAMEE : Free Advance Encryptor For Anon Cloud
* WSVuls : Website Vulnerability Scanner Detect Issues
* Scanmycode-Ce : Code Scanning/SAST/Static Analysis/Linting Using Many tools/Scanners
* Master_Librarian : A Tool To Audit Unix/*BSD/Linux System Libraries To Find Public Security Vulnerabi
* GONET-Scanner : Golang Network Scanner With Arp Discovery And Own Parser
* Geowifi : Search WiFi Geolocation Data By BSSID And SSID On Different Public Databases
* GraphQL Cop : Security Auditor Utility For GraphQL APIs
* Fastfuz-Chrome-Ext : Site Fast Fuzzing With Chorme Extension

GBHackers Analysis

* 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
* FBI Warns that Hackers Gain Network Access by Exploiting MFA and "PrintNightmare" Vulnerability

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

* Live Hacking Q&A with Kody Kinzie: Security Ethics, ESP32 - C3 Released, and More
* Spring4Shell Patches Released; Hydra Is Beheaded - ThreatWire
* Modding DJI FPV Goggles with Analog Input w/Glytch

The PC Security Channel [TPSC]

* Discord Infostealers: How hackers steal your password
* Free Security Tools Everyone Should Use

Eli the Computer Guy

* Elon Musk ISN'T BUYING TWITTER
* Mark Zuckerberg DESTROYING REALITY with AR in 2024
* Elon Musk Offers to BUY TWITTER
* CNN+ is DEAD

Security Now

* Spring4Shell - Patch Tuesday, Microsoft's Autopatch System, NGINX 0-Day
* Port Knocking - Wyze Gets Spanked, FinFisher Bites the Dust, Spring4Shell, LAPSUS$ Update

Troy Hunt

* Breach Disclosure Blow-by-Blow: Here's Why It's so Hard

Intel Techniques: The Privacy, Security, & OSINT Show

* 257-Early Warning
* 256-Extreme Privacy Fatigue

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Siemens A8000 CP-8050/CP-8031 SICAM WEB Missing File Download / Missing Authentication
* Backdoor.Win32.NetSpy.10 Remote Command Execution
* Backdoor.Win32.NetCat32.10 Remote Command Execution
* Backdoor.Win32.NinjaSpy.c Authentication Bypass
* Email-Worm.Win32.Pluto.b Insecure Permissions
* Backdoor.Win32.Kilo.016 Denial Of Service
* HackTool.Win32.IpcScan.c Buffer Overflow
* Backdoor.Win32.Psychward.03.a Weak Hardcoded Password
* Backdoor.Win32.Prorat.cwx Insecure Permissions
* Backdoor.Win32.MotivFTP.12 Authentication Bypass
* Microsoft HTTP Protocol Stack Denial Of Service
* Delta Controls enteliTOUCH 3.40.3935 Cookie User Password Disclosure
* Delta Controls enteliTOUCH 3.40.3935 Cross Site Scripting
* Delta Controls enteliTOUCH 3.40.3935 Cross Site Request Forgery
* Online Car Wash Booking System 1.0 Blind SQL Injection
* Online Car Wash Booking System 1.0 SQL Injection
* REDCap Cross Site Scripting
* Spring4Shell Code Execution
* Verizon 4G LTE Network Extender 0.4.038.2131 Weak Credential Algorithm
* Easy!Appointments Information Disclosure
* Explore CMS 1.0 SQL Injection
* Razer Sila 2.0.418 Command Injection
* Razer Sila 2.0.418 Local File Inclusion
* WordPress Anti-Malware Security And Brute-Force Firewall Cross Site Scripting
* WordPress LayerSlider Cross Site Scripting

CXSecurity

* Easy!Appointments Information Disclosure
* Small HTTP Server 3.06 Remote Buffer Overflow
* Zenario CMS 9.0.54156 Remote Code Execution
* ALLMediaServer 1.6 Buffer Overflow
* Atom CMS 1.0.2 Shell Upload
* PostgreSQL 11.7 Remote Code Execution
* Trend Micro Virtual Mobile Infrastructure 6.0.1278 Denial Of Service

Proof of Concept (PoC) & Exploits

Exploit Database

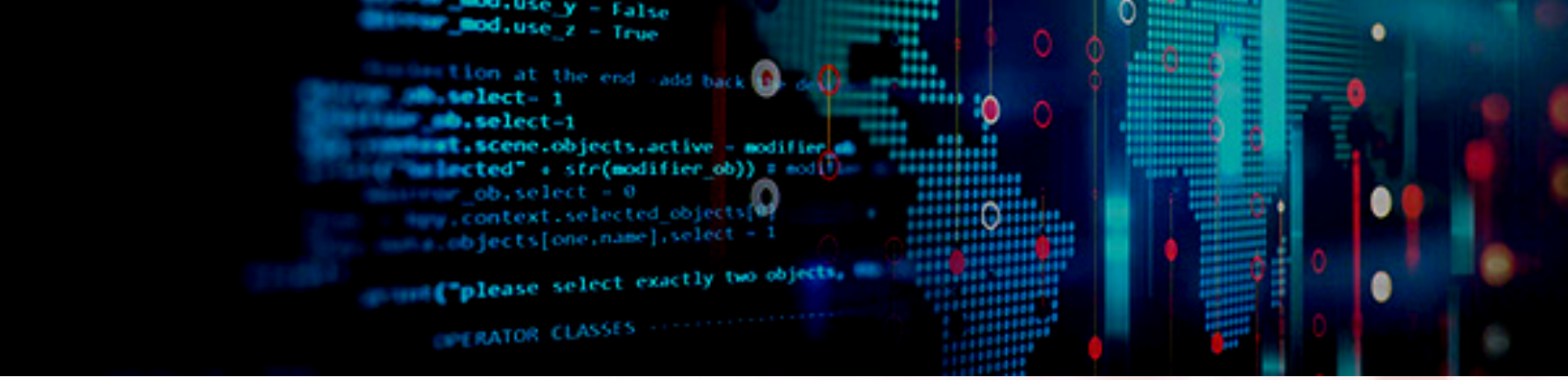
* [webapps] Razer Sila - Command Injection
* [webapps] Razer Sila - Local File Inclusion (LFI)
* [webapps] Telesquare TLR-2855KS6 - Arbitrary File Deletion
* [webapps] Telesquare TLR-2855KS6 - Arbitrary File Creation
* [remote] Franklin Fueling Systems Colibri Controller Module 1.8.19.8580 - Local File Inclusion (LFI)
* [webapps] SAM SUNNY TRIPOWER 5.0 - Insecure Direct Object Reference (IDOR)
* [local] MiniTool Partition Wizard - Unquoted Service Path
* [local] binutils 2.37 - Objdump Segmentation Fault
* [remote] Opmon 9.11 - Cross-site Scripting
* [remote] Kramer VIAware - Remote Code Execution (RCE) (Root)
* [webapps] ICEHRM 31.0.0.0S - Cross-site Request Forgery (CSRF) to Account Deletion
* [webapps] qdPM 9.2 - Cross-site Request Forgery (CSRF)
* [webapps] minewebcms 1.15.2 - Cross-site Scripting (XSS)
* [local] Sherpa Connector Service v2020.2.20328.2050 - Unquoted Service Path
* [webapps] KLiK Social Media Website 1.0 - 'Multiple' SQLi
* [webapps] Zenario CMS 9.0.54156 - Remote Code Execution (RCE) (Authenticated)
* [webapps] WordPress Plugin Easy Cookie Policy 1.6.2 - Broken Access Control to Stored XSS
* [remote] Kramer VIAware 2.5.0719.1034 - Remote Code Execution (RCE)
* [remote] PostgreSQL 9.3-11.7 - Remote Code Execution (RCE) (Authenticated)
* [webapps] CSZ CMS 1.2.9 - 'Multiple' Blind SQLi(Authenticated)
* [webapps] WordPress Plugin admin-word-count-column 2.2 - Local File Read
* [webapps] WordPress Plugin video-synchro-pdf 1.7.4 - Local File Inclusion
* [webapps] WordPress Plugin cab-fare-calculator 1.0.3 - Local File Inclusion
* [webapps] WordPress Plugin Curtain 1.0.2 - Cross-site Request Forgery (CSRF)
* [webapps] Drupal avatar_uploader v7.x-1.0-beta8 - Cross Site Scripting (XSS)

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*

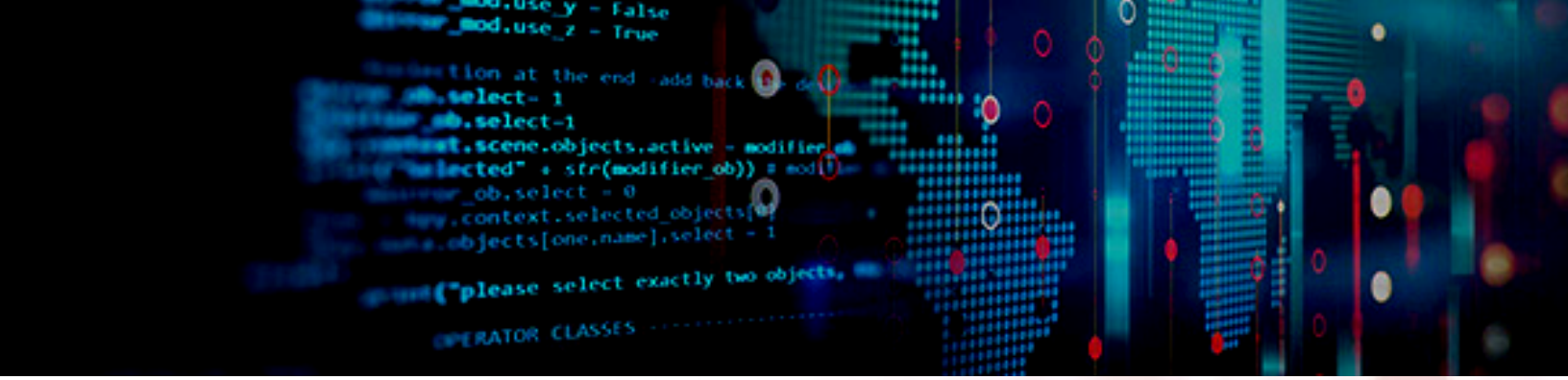
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

http://sikhoraphumcity.go.th/zz.html
http://sikhoraphumcity.go.th/zz.html notified by xNot_RespondinGx
https://www.ugelchincha.gob.pe/index.php
https://www.ugelchincha.gob.pe/index.php notified by ZoRRoKiN
https://office.yst1.go.th/1975.html
https://office.yst1.go.th/1975.html notified by 1975 Team
https://news.banggailautkab.go.id/readme.html
https://news.banggailautkab.go.id/readme.html notified by AnonCoders
https://satpolpp.banggailautkab.go.id/readme.html
https://satpolpp.banggailautkab.go.id/readme.html notified by AnonCoders
http://southcorfu.gov.gr/o.htm
http://southcorfu.gov.gr/o.htm notified by chinafans
https://banggailautkab.go.id/readme.html
https://banggailautkab.go.id/readme.html notified by Mr.Z
https://portal.dint.pm.es.gov.br/index.html
https://portal.dint.pm.es.gov.br/index.html notified by psycIllusion
https://sipom.pm.es.gov.br/index.html
https://sipom.pm.es.gov.br/index.html notified by psycIllusion
https://dint.pm.es.gov.br/index.html
https://dint.pm.es.gov.br/index.html notified by psycIllusion
https://rlw.gov.ru/2020120201.php
https://rlw.gov.ru/2020120201.php notified by AnonSec Team
https://jateng.litbang.pertanian.go.id
https://jateng.litbang.pertanian.go.id notified by AnonSec Team
https://www.komnasperempuan.go.id/readme.php
https://www.komnasperempuan.go.id/readme.php notified by AnonSec Team
http://www.chon3.go.th/1975.html
http://www.chon3.go.th/1975.html notified by 1975 Team
https://nb2.go.th/1975.html
https://nb2.go.th/1975.html notified by 1975 Team
https://www.nsw2.go.th/1975.html
https://www.nsw2.go.th/1975.html notified by 1975 Team
https://pangkepkab.go.id/anjay.html
https://pangkepkab.go.id/anjay.html notified by Mr.spongebob



Dark Web News

Darknet Live

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” 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.” 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.” 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.” 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,” "Rf.ws,” and "Raid.lol.” "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.” 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” 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.” 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” but received nothing in return. "On or about December 16, 2018, COELHO, who was using the moniker "Downloading,” 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.” "On or about March 4, 2019, in the Eastern District of Virginia and elsewhere, COELHO, who was using the moniker "Downloading,” 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” 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.” "On or about March 5, 2019, in the Eastern District of Virginia and elsewhere, Coelho, who was using the monikers "Downloading,” "Omnipotent,” and "Shiza,” 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.” In a different undercover transaction described in the indictment, the RaidForums user "SubVirt” 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.” 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,” transferred the false registration of the domain "Raidforums.com” to a U.S.-based domain registrar based in Phoenix, Arizona using the alias "Kevin Maradona.” Coelho falsely registered the domain name knowing that it was used to support the RaidForums website in furtherance of the conspiracy.” 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,” 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.” 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/)

Maryland Inmate Sentenced for Mail and Wire Fraud

A Maryland man was sentenced to five years in prison for funding inmate accounts with stolen credit cards purchased on the darkweb. U.S. District Judge George J. Hazel sentenced Abraham Oliver, age 26, to 61 months in federal prison and three years of supervised release. Oliver previously pleaded guilty to conspiracy to commit mail and wire fraud and aggravated identity theft. When Oliver was an inmate at the Montgomery County Department of Correction and Rehabilitation (DOCR), he directed Octavia Ikea Terry, age 25, of Maxton, North Carolina, to purchase Bitcoin and then use the Bitcoin to buy stolen credit and debit cards on the darkweb. "Oliver further instructed Terry to identify available credit and debit counts available for sale that were from Maryland, then use the debit and credit card numbers to make deposits into Oliver's inmate escrow account and other inmates' escrow accounts.” Oliver also instructed Terry to set up a Post Office box in North Carolina where other inmates could send checks from their inmate escrow accounts. Using the stolen credit and debit cards, Terry deposited $31,252.35 into the accounts of at least 12 different inmates. She deposited $5,579.10 into Oliver's inmate account. Oliver and two other inmates mailed checks to Terry's Post Office box totaling $9,325. Judge Hazel ordered Oliver to forfeit $12,166.93 and pay restitution of $31,252.35. Terry pleaded guilty to her role in the conspiracy but has not yet been sentenced. archive.org (via darknetlive.com at https://darknetlive.com/post/maryland-inmate-sentenced-for-mail-and-wire-fraud/)

US Treasury Sanctioned Hydra Market

The U.S. Treasury Department sanctioned Hydra, the world's largest darkweb marketplace. The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned Hydra and the virtual currency exchange Garantex. "The global threat of cybercrime and ransomware that originates in Russia, and the ability of criminal leaders to operate there with impunity, is deeply concerning to the United States,” said Secretary of the Treasury Janet L. Yellen. "Our actions send a message today to criminals that you cannot hide on the darknet or their forums, and you cannot hide in Russia or anywhere else in the world. In coordination with allies and partners, like Germany and Estonia, we will continue to disrupt these networks.” The banner uploaded by German police after the seizure of Hydra's servers in Germany. Alongside the sanctions, the Department of Justice indicted Dmitry Olegovich Pavlov for conspiracy to distribute narcotics and conspiracy to launder money "in connection with his operation and administration of the servers used to run Hydra.” According to the U.S. government, Pavlov is living in Russia, where he is safe from Yellen and the demands of the U.S. government. If he is living in the Ukraine, like the alleged administrators of Hydra, Yellen could be correct about his inability to hide. "Starting in or about November 2015, Pavlov is alleged to have operated a company, Promservice Ltd., also known as All Wheel Drive and 4x4host.ru, that administered Hydra's servers (Promservice). During that time, Pavlov, through his company Promservice, administered Hydra's servers, which allowed the market to operate as a platform used by thousands of drug dealers and other unlawful vendors to distribute large quantities of illegal drugs and other illicit goods and services to thousands of buyers, and to launder billions of dollars derived from these unlawful transactions.” "As an active administrator in hosting Hydra's servers, Pavlov allegedly conspired with the other operators of Hydra to further the site's success by providing the critical infrastructure that allowed Hydra to operate and thrive in a competitive darknet market environment. In doing so, Pavlov is alleged to have facilitated Hydra's activities and allowed Hydra to reap commissions worth millions of dollars generated from the illicit sales conducted through the site.” On Rutor, someone claiming to be Hellgirl is giving the usual "we will return” message. The message is signed but I do not have Hellgirl's original PGP key saved. I am skeptical that it is the real Hellgirl. However, feds seized Hydra once before in 2014… Some Russian vendors were directing customers to new storefronts on Mega. Mega has been intermittently online while apparently struggling to deal with the massive influx of users. Legal has been under a denial of service attack for several days. There is also a push to move customers to Telegram where many vendors have bots.

SPECIALLY DESIGNATED NATIONALS LIST UPDATE GARANTEX EUROPE OU (Latin: GARANTEX EUROPE OÜ), Harju maakond, Kesklinna linnaosa, J., Poska tn 51a/1-3, Tallinn 10150,

Estonia; Harju maakond, Lasnamae linnaosa, Peterburi tee 47, Tallinn 11415, Estonia; Moscow, Russia; St. Petersburg, Russia; Website garantex.io; Digital Currency Address - XBT 3Lpoy53K625zVeE47ZasiG5jGkAxJ27kh1; Digital Currency Address - ETH 0x7FF9cFad3877F21d41Da833E2F775dB0569eE3D9; Digital Currency Address - USDT 3E6ZCKRrsdPc35chA9Eftp1h3DLW18NFNV; Business Registration Number 14850239 (Estonia) issued 18 Nov 2019 [RUSSIA-EO14024]. HYDRA MARKET (a.k.a. HYDRA MARKETPLACE; a.k.a. "HYDRA”), Russia; Commonwealth of Independent States; Website http://hydram6esdjf6otepmr5c3vjyndsoddz22afphbbjznwb5ln2c6op7ad.onion/; alt. Website http://hydraclubbioknikokex7njhwuahc2l67lfiz7z36md2jvopda7nchid.onion/; Digital Currency Address - XBT 3K4rjdh8A5yi6LWvft2rbmyZvqEbPSSSX4; alt. Digital Currency Address - XBT 17mhyeBX617ABZ1ffThhUTJkHUcMvCkfd5; alt. Digital Currency Address - XBT 35qwVtMEohWDdBWRiCSR7azoP5cbY8SG1Q; alt. Digital Currency Address - XBT 35KAdTa2vqnJzitF2xiUzZn1Gmcas2Y465; alt. Digital Currency Address - XBT 35LScRJ8hzDvvWh9t9UA8bHGnGNVz3YEfa; alt. Digital Currency Address - XBT 1PJp8diNa89cVHpiT1VPu7EQ8LxYM5HX6v; alt. Digital Currency Address - XBT 17V7THwHMiDJmDwZK4unhE5HgKFJKx7VCe; alt. Digital Currency Address - XBT 3PiCnZrBvGfWAKQ9hr4cCpfaDjy64yNSpE; alt. Digital Currency Address - XBT 14gM1HuLVDELNHaFU22qpabjtiWek4HhV1; alt. Digital Currency Address - XBT 1GYuu9d5HPikafbys3k5Q3DRJq6debGsoB; alt. Digital Currency Address - XBT 3GXdtA6kbb4M5aqzZm5qqxcFDFRMW8LqdJ; alt. Digital Currency Address - XBT 1B11Ezqg3AXjFhMdRq5UpPDpNyriYNVtkn; alt. Digital Currency Address - XBT 16SPDQFFzgsoNSPiFFTfS8Dw8LLXqia4oc; alt. Digital Currency Address - XBT 19pPbUDvoSBZafkUCYkD2Z9AkuqqV6sWm7; alt. Digital Currency Address - XBT 3BQACtiMXYB9JpUMpkEWt9m8BzswpGHq4X; alt. Digital Currency Address - XBT 1DGsY4ww3BJnWXTsnmTgWa6UWdoRXgA1pX; alt. Digital Currency Address - XBT 1GcKLUUXodTQcLcPD7VLMgvCc4hs5Q775; alt. Digital Currency Address - XBT 1EvhBad5wCZYhBoAsGaciV6AvmZ1osLpeJ; alt. Digital Currency Address - XBT bc1qsmv6lkrw65l30yazdqpdjjtwzpvk9f8gfh0cy7; alt. Digital Currency Address - XBT bc1qs9u6j78e3utj08mwvqkkmqm9de5xk3g4yh8qtq; alt. Digital Currency Address - XBT 12VrYZgS1nmf9KHHped24xBb1aLLRpV2cT; alt. Digital Currency Address - XBT bc1q202ajnhxgg9d9jjczmg0g4usp6haqldyy2eakl; alt. Digital Currency Address - XBT 1NbGwQwt4uEhg2srAKppLf8QaF6fbp3PZG; alt. Digital Currency Address - XBT 13LQJQ1oJ9K7PsqsGfjNhoVv6UeU6hgzQz; alt. Digital Currency Address - XBT 1CG1aSCxUnbmv9G34ofxTQoHtuVnMLJtQV; alt. Digital Currency Address - XBT 3Kp8Qc5z7yevDeoQxhS5RSSKnEi5x7AQ43; alt. Digital Currency Address - XBT 331TS6DyASY7iU5CRA8UryBnkPS78fP2B1; alt. Digital Currency Address - XBT 1NvJm3jfZxENNyqws5BKQvhkLxg9chLJdo; alt. Digital Currency Address - XBT 1LicqjCa74n8pmNaoARXLLqcTUTHFpxbXH; alt. Digital Currency Address - XBT 175BUqf8JCU1uoG1iTRKTacDa4uvJDUCw2; alt. Digital Currency Address - XBT 1ANpca7g93BwptUJg1zV116v49zn9gjDi3; alt. Digital Currency Address - XBT 1BCWMwpR4M1nYUuuYe2bmzrNuwGoF9ZAbA; alt. Digital Currency Address - XBT 18cFGAdYcvNHkuhXLBE7izQKCyUW8TzCJE; alt. Digital Currency Address - XBT 1QHxyuLGRMHfbNPJikV4Dwhfx45HWfUMWB; alt. Digital Currency Address - XBT 1GnFTy5F9qi5MfaRZfgdg2jkyT5xtAHvd8; alt. Digital Currency Address - XBT bc1quyc6j8ca84q9gjej5jjd2n8hra0vfu0j60fefs57p6e5rerkq07q0l5u3w; alt. Digital Currency Address - XBT 16p2UWTZwXRyK5bTHNVjdDyy1D3EQGsZf2; alt. Digital Currency Address - XBT 1CddRqw7oSPrT4tt5oXKyx2LiHJDPszy7y; alt. Digital Currency Address - XBT 1Hhe61Bwxs8Hd2WxzWY9FQyZicBiZGeSNW; alt. Digital Currency Address - XBT 1D3GuaS9eqKw8dWj9JFQtNufdRtysjSLxZ; alt. Digital Currency Address - XBT

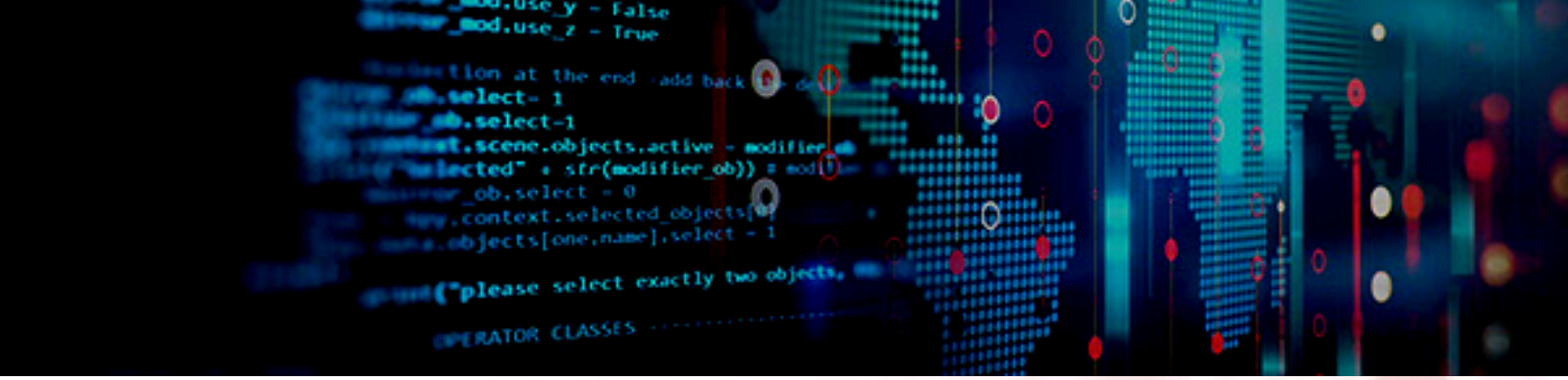
1PWRKxkR5AU7Tc9zPqjdhtu1eGW1QZzs4y; alt. Digital Currency Address - XBT
1D1ej7zQzywWBDNXKNYpmH7Hso2U9koDG4; alt. Digital Currency Address - XBT
3KGQ3hX6eFYtBjTBFSdvdkzHmwZyYWLRQh; alt. Digital Currency Address - XBT
1LKE3XA9bf5JFqtGtCHzWj5QGxKGwMfXZw; alt. Digital Currency Address - XBT
1MtsQsw6n2jvJCWhpCw7jifTfD9Q3rBBVg; alt. Digital Currency Address - XBT
1KkaKujnqwJf7Cbm7JKAZGF3X9d4685m8n; alt. Digital Currency Address - XBT
1Ge8JodC2HiBiEuT7D3MoH6Fak6XrcT9Kf; alt. Digital Currency Address - XBT
bc1qsmqpalp3gtgkltag4x3ygevmhh9y2hzk73t2ug; alt. Digital Currency Address - XBT
1E9uUnLbyfToazo95vmM3ysYnzgkrL7GeC; alt. Digital Currency Address - XBT
1HH8eiuaTMucTNyvGCUmAvmCZCtdMi8SqK; alt. Digital Currency Address - XBT
19FQzHibWDhSP8pKmJS3uagFYoisXtehzw; alt. Digital Currency Address - XBT
3DLGfN7hgsWXXSp9euXcnmWXLpFQuswW2t; alt. Digital Currency Address - XBT
1PXxwPVtYxZiCRp9LKq7aKMDFrhAQztvUE; alt. Digital Currency Address - XBT
1Q4tJjH2aBr3AJrzxqa4Z3jPpf5SDgF4jK; alt. Digital Currency Address - XBT
1PYtgFS2t6i57WdDvbRa7kPcsagGMBxzfg; alt. Digital Currency Address - XBT
16ZSAEfYpPCj3D94fsNt2okYj9Ue8mxy6T; alt. Digital Currency Address - XBT
bc1qvlzfn6kmezv44d8kw0p5jsmxe6wchv3zc7gsxs; alt. Digital Currency Address - XBT
3QVyoH4u3qT88uChAeJVhfB3r6maZt431y; alt. Digital Currency Address - XBT
1FFS6pX1TCKTNy668Mbk2Lyoem1qB48kYX; alt. Digital Currency Address - XBT
1Dpddb1TMjvmNQeYDqgyd1ww6cmwPJRdSk; alt. Digital Currency Address - XBT
3AjiWiUdKB5mcGUSS9mBeoHCeYJw3Zo8r6; alt. Digital Currency Address - XBT
1EtMuBPQnPCa3cecerdSH1SzydxnhbTmw; alt. Digital Currency Address - XBT
3CCmt5LjQ5yKkaFY1DWC2SbERVEtWRnSRD; alt. Digital Currency Address - XBT
1MQBDeRWsiJBf7K1VGjJ7PWEL6GJXMfmLg; alt. Digital Currency Address - XBT
1MbtT2ZsTtLp7EKZUV9r74cTyqvsMtTP2M; alt. Digital Currency Address - XBT
36yS87PLuW7sErLg1TY26WzaVarTim7AcC; alt. Digital Currency Address - XBT
3AYU365Tcjef7j9pdKF9Xe8rWpEpsH196t; alt. Digital Currency Address - XBT
148LKmyZT3FGE4x1GjsFN6RsAwcjzk5iuE; alt. Digital Currency Address - XBT
16EKTes8ahD8xvwisqjc2xSNLiG3fDHatW; alt. Digital Currency Address - XBT
3GuQjr7kkrR5EjpanMgyAuxuLgrjEUwe21; alt. Digital Currency Address - XBT
35eanEz5iYg2eYaxCtMrR4SCoypFqrBWUH; alt. Digital Currency Address - XBT
3QWUdP5taP4GrRuueVDud1eWetb7hc3wDH; alt. Digital Currency Address - XBT
3Czhm6xqn8odwz6jgTcjRrUjog28v6aVS8; alt. Digital Currency Address - XBT
1F7UL41qYm6TvnExZzPHBCyeENvX3XDEMS; alt. Digital Currency Address - XBT
123WBUDmSJv4GctdVEz6Qq6z8nXSKrJ4KX; alt. Digital Currency Address - XBT
3BCN3WgMRJwULTz1vsEQ7NZrBjwaUBf5Ca; alt. Digital Currency Address - XBT
35SwVFxosV3AsvnrBfzdXarqavRbvDyyxv; alt. Digital Currency Address - XBT
32pCmCWEjwhkLwh5BgLNAeBQFp5Gi1hv81; alt. Digital Currency Address - XBT
1G64TFMFVJTjhJXra6x74BBhsfSyiWaFtT; alt. Digital Currency Address - XBT
1A3iYY4c3dkgNYGewzYzr7EsqfBuWXibGo; alt. Digital Currency Address - XBT
3GAUBtrTtWp1D9yeXgr3wMg8B599QHa5m5; alt. Digital Currency Address - XBT
3HJN4jRa4mdfkey9JR9jUhr86yPwL86A3C; alt. Digital Currency Address - XBT
1EuUMPBCZtSd5pVVFEqmRqUSfU1qy6ASuL; alt. Digital Currency Address - XBT
1Pu1nAW7kCoSMThMs8QcpM8JxuByQDZgH; alt. Digital Currency Address - XBT
3QnWE5GVfQu3wVav91RuFkqip4Ti4NWqAY; alt. Digital Currency Address - XBT
1CNbhgxGRZvsWnEHotfXge7k2E1UPzBDC7; alt. Digital Currency Address - XBT
3HSZc4BLnQBznjSq7JvXgqNCZUUs3M9fZz; alt. Digital Currency Address - XBT
37dDBCexFPraKW4jGSqkE3NyG52YeZQbJx; alt. Digital Currency Address - XBT
1H8sDTTgJPBKw83EBZDLhXvetCbxZUMMZM; alt. Digital Currency Address - XBT

1BvJRBRp9ZZ6zLyuZaZsV7g3xP6JokdZQW; alt. Digital Currency Address - XBT
bc1q237mvl0heyw0r38wd3xz8h5mar96rrwpams8pp; alt. Digital Currency Address - XBT
34dxZvijpBM1YkPybczbQ7DuGuKAnULdfS; alt. Digital Currency Address - XBT
1GkLN7DbA9mAtHNzQWNPANcdWbefaz4Gzm; alt. Digital Currency Address - XBT
13hfsQm6oCaDZehfYBSMFiJVAi1jsL6sQd; alt. Digital Currency Address - XBT
1Sf6e4xQv8muMZqYPTdRFf3e5o5eWcg9F; alt. Digital Currency Address - XBT
bc1qj6j6p0jdefl6pvdzx3kx8245yy5mz6q4luhzes; alt. Digital Currency Address - XBT
1B3u21itzjgKtm7QsNQNCBpSkwzzeDHqrW; alt. Digital Currency Address - XBT
3JhPsVV3KnL9dBYGSZALS9EbrLr97R865a; alt. Digital Currency Address - XBT
bc1qqf8kcc9m57xjqcvsvuf989nnl48ve6d2s24cx3; alt. Digital Currency Address - XBT
1HuYfoEwsfHgZiRhbhJrCd5ST3iksa8KEx; alt. Digital Currency Address - XBT
1J9wJH2bamZVxscXAvoDH4jvtGKb7sYFDm; alt. Digital Currency Address - XBT
34WWXwFKAsXL9zYxbeNPaPV6vDamkjQLUo; alt. Digital Currency Address - XBT
3PDmRwotTkRAFRLGTUrucCERp2JdM1q4ar; alt. Digital Currency Address - XBT
3AFcE2mbSSndcpYFgHoExSmjUc26ef2gQh; alt. Digital Currency Address - XBT
3P6PzdfETr4275Gn3veLkCyDxA1jV8fHKm; alt. Digital Currency Address - XBT
3HRExd8GKFskZC5inmVcpiyy9UWG7FVa6o; alt. Digital Currency Address - XBT
3MP7yBGSW2gkXVRE8S84T2j4KVgPh3rEzv; alt. Digital Currency Address - XBT
1K2fmE9hfhbRNSZoBvCBWZAvsS5idTUxBG; alt. Digital Currency Address - XBT
3ES6pqCueDPCnC4hCqhhYuey6gyiRJZw6E; alt. Digital Currency Address - XBT
3KvBX3jo69Qn8jHy44M33RYoeYcf8DdRBD; alt. Digital Currency Address - XBT
3K26aMKmnrv97Pj6YiFcqiXk2LxeHfhnG3; alt. Digital Currency Address - XBT
3BWP6ZQAhc4j5wR1b95zJAthJEFvhdees7; alt. Digital Currency Address - XBT
3JuSgFrwnrNfuhvR4GpWAPmeJVot4xrEae; alt. Digital Currency Address - XBT
1DKGRGJXGNLAtTeFb9SNPNHtrkZ87q7qKi; alt. Digital Currency Address - XBT
361AkMKNNWYwZRsCE8pPNmoh5aQf4V7g4p; alt. Digital Currency Address - XBT
33fWcMdmsB2Ey4CEbVWbjGFkuevBSyP9nG; alt. Digital Currency Address - XBT
35aTjkBh4yeTypJsi9nuTdoMKHTsawKVgX; Organization Established Date 2015 [CYBER2]. archive.org indictment Feds are acting as if they have won some victory over Hydra's administrators. I do not see this being true if the administrators are Russians in Russia. I am skeptical about the authenticity of the dox placing them in the Ukraine (which ordinarily would not be a problem for the United States government but the ongoing border skirmish might have changed things). (via darknetlive.com at https://darknetlive.com/post/us-treasury-sanctioned-hydra-market/)

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

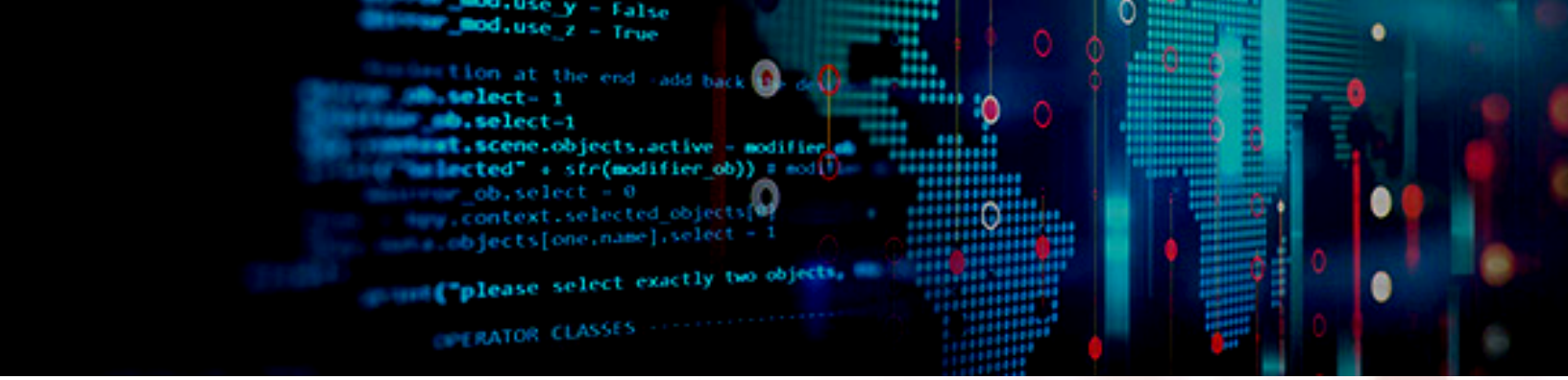
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

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
* 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

* 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
* Patch Tuesday - April 2022
* CVE-2022-24527: Microsoft Connected Cache Local Privilege Escalation (Fixed)
* 3 Ways InsightIDR Users Are Achieving XDR Outcomes
* Metasploit Wrap-Up
* 7 Rapid Questions: Meet Adrian Stewart, Aspiring Pilot Turned Product Manager



Advisories

US-Cert Alerts & bulletins

* Google Releases Security Updates for Chrome
* VMware Releases Security Updates for Cloud Director
* CISA Adds Nine Known Exploited Vulnerabilities to Catalog
* Juniper Networks Releases Security Updates for Multiple Products
* Cisco Releases Security Updates for Multiple Products
* CISA Adds One Known Exploited Vulnerability to Catalog
* Microsoft Releases Advisory to Address Critical Remote Code Execution Vulnerability (CVE-2022-26809)
* APT Actors Target ICS/SCADA Devices
* AA22-103A: APT Cyber Tools Targeting ICS/SCADA Devices
* AA22-083A: Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targe
* Vulnerability Summary for the Week of April 4, 2022
* Vulnerability Summary for the Week of March 28, 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, 3 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, 3 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, 3 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, 4 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, 5 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, 5 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, 5 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, 5 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, 5 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, 5 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, 5 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, 5 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, 5 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, 5 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, 5 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, 5 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, 5 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, 5 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, 5 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, 12 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, 12 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, 12 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, 12 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, 12 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

Asterisk Project Security Advisory - AST-2022-002

Asterisk suffers from a server-side request forgery vulnerability. When using STIR/SHAKEN, it is possible to send arbitrary requests like GET to interfaces such as localhost using the Identity header. Asterisk Open Source versions 16.15.0 up to but not including 16.25.2, 18.x up to but not including 18.11.2, and 19.x up to but not including 19.3.2 are affected.

Asterisk Project Security Advisory - AST-2022-001

When using STIR/SHAKEN in Asterisk, it is possible to download files that are not certificates. These files could be much larger than what you would expect to download. Asterisk Open Source versions 16.15.0 up to but not including 16.25.2, 18.x up to but not including 18.11.2, and 19.x up to but not including 19.3.2 are affected.

Red Hat Security Advisory 2022-1379-01

Red Hat Security Advisory 2022-1379-01 - Red Hat Decision Manager is an open source decision management platform that combines business rules management, complex event processing, Decision Model & Notation execution, and business optimization for solving planning problems. It automates business decisions and makes that logic available to the entire business. This asynchronous security patch is an update to Red Hat Decision Manager 7. Issues addressed include a code execution vulnerability.

Red Hat Security Advisory 2022-1378-01

Red Hat Security Advisory 2022-1378-01 - Red Hat Process Automation Manager is an open source business process management suite that combines process management and decision service management and enables business and IT users to create, manage, validate, and deploy process applications and decision services. This asynchronous security patch is an update to Red Hat Process Automation Manager 7. Issues addressed include a code execution vulnerability.

Red Hat Security Advisory 2022-1372-01

Red Hat Security Advisory 2022-1372-01 - Red Hat OpenShift Data Foundation is software-defined storage integrated with and optimized for the Red Hat OpenShift Container Platform. Red Hat OpenShift Data Foundation is a highly scalable, production-grade persistent storage for stateful applications running in the Red Hat OpenShift Container Platform.

WordPress Elementor 3.6.2 Remote Code Execution

WordPress Elementor versions 3.6.0 through 3.6.2 suffer from a remote code execution vulnerability.

Red Hat Security Advisory 2022-1373-01

Red Hat Security Advisory 2022-1373-01 - 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 privilege escalation and use-after-free vulnerabilities.

Ubuntu Security Notice USN-5378-4

Ubuntu Security Notice 5378-4 - USN-5378-1 fixed a vulnerability in Gzip. This update provides the corresponding update for Ubuntu 14.04 ESM and 16.04 ESM. Cleemy Desu Wayo discovered that Gzip incorrectly handled certain filenames. If a user or automated system were tricked into performing zgrep operations with specially crafted filenames, a remote attacker could overwrite arbitrary files.

Ubuntu Security Notice USN-5378-3

Ubuntu Security Notice 5378-3 - USN-5378-2 fixed a vulnerability in XZ Utils. This update provides the corresponding update for Ubuntu 14.04 ESM and 16.04 ESM. Cleemy Desu Wayo discovered that Gzip incorrectly handled certain filenames. If a user or automated system were tricked into performing zgrep operations with specially crafted filenames, a remote attacker could overwrite arbitrary files.

Red Hat Security Advisory 2022-1361-01

Red Hat Security Advisory 2022-1361-01 - Red Hat OpenShift Data Foundation is software-defined storage integrated with and optimized for the Red Hat OpenShift Container Platform. Red Hat OpenShift Data Foundation is a highly scalable, production-grade persistent storage for stateful applications running in the Red Hat OpenShift Container Platform.

Red Hat Security Advisory 2022-1345-01

Red Hat Security Advisory 2022-1345-01 - Red Hat AMQ Streams, based on the Apache Kafka project, offers a distributed backbone that allows microservices and other applications to share data with extremely high throughput and extremely low latency. This release of Red Hat AMQ Streams 2.1.0 serves as a replacement for Red Hat AMQ Streams 2.0.1, and includes security and bug fixes, and enhancements. Issues addressed include HTTP request smuggling and integer overflow vulnerabilities.

Red Hat Security Advisory 2022-1248-01

Red Hat Security Advisory 2022-1248-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.7.48. Issues addressed include a bypass vulnerability.

Red Hat Security Advisory 2022-1360-01

Red Hat Security Advisory 2022-1360-01 - This release of Red Hat Fuse 7.10.2 serves as a replacement for Red Hat Fuse 7.10.1, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References.

Red Hat Security Advisory 2022-1354-01

Red Hat Security Advisory 2022-1354-01 - .NET Core is a managed-software framework. It implements a subset of the .NET framework APIs and several new APIs, and it includes a CLR implementation.

Ubuntu Security Notice USN-5378-1

Ubuntu Security Notice 5378-1 - Cleemy Desu Wayo discovered that Gzip incorrectly handled certain filenames. If a user or automated system were tricked into performing zgrep operations with specially crafted filenames, a remote attacker could overwrite arbitrary files.

Ubuntu Security Notice USN-5378-2

Ubuntu Security Notice 5378-2 - Cleemy Desu Wayo discovered that XZ Utils incorrectly handled certain filenames. If a user or automated system were tricked into performing xzgrep operations with specially crafted filenames, a remote attacker could overwrite arbitrary files.

Ubuntu Security Notice USN-5371-1

Ubuntu Security Notice 5371-1 - It was discovered that nginx Lua module mishandled certain inputs. An attacker could possibly use this issue to perform an HTTP Request Smuggling attack. This issue only affects Ubuntu 18.04 LTS and Ubuntu 20.04 LTS. It was discovered that nginx Lua module mishandled certain inputs. An attacker could possibly use this issue to disclose sensitive information. This issue only affects Ubuntu 18.04 LTS and Ubuntu 20.04 LTS.

Ubuntu Security Notice USN-5377-1

Ubuntu Security Notice 5377-1 - It was discovered that the network traffic control implementation in the Linux kernel contained a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. Yiqi Sun and Kevin Wang discovered that the cgroups implementation in the Linux kernel did not properly restrict access to the cgroups v1 release_agent feature. A local attacker could use this to gain administrative privileges.

Red Hat Security Advisory 2022-1179-01

Red Hat Security Advisory 2022-1179-01 - Red Hat support for Spring Boot provides an application platform that reduces the complexity of developing and operating applications for OpenShift as a containerized platform. This release of Red Hat support for Spring Boot 2.5.10 serves as a replacement for Red Hat support for Spring Boot 2.4.9, and includes bug fixes and enhancements. For more information, see the release notes listed in the References section. Issues addressed include HTTP request smuggling and denial of service vulnerabilities.

Red Hat Security Advisory 2022-1333-01

Red Hat Security Advisory 2022-1333-01 - A micro version update is now available for Red Hat Camel K that includes CVE fixes in the base images, which are documented in the Release Notes document linked in the References section.

Ubuntu Security Notice USN-5376-1

Ubuntu Security Notice 5376-1 - 俞晨东 discovered that Git incorrectly handled certain repository paths in platforms with multiple users support. An attacker could possibly use this issue to run arbitrary commands.

Ubuntu Security Notice USN-5372-1

Ubuntu Security Notice 5372-1 - Evgeny Kotkov discovered that Subversion servers did not properly follow path-based authorization rules in certain cases. An attacker could potentially use this issue to retrieve information about private paths. Thomas Wei

Red Hat Security Advisory 2022-1309-01

Red Hat Security Advisory 2022-1309-01 - Expat is a C library for parsing XML documents. Issues addressed include code execution and integer overflow vulnerabilities.

Red Hat Security Advisory 2022-1326-01

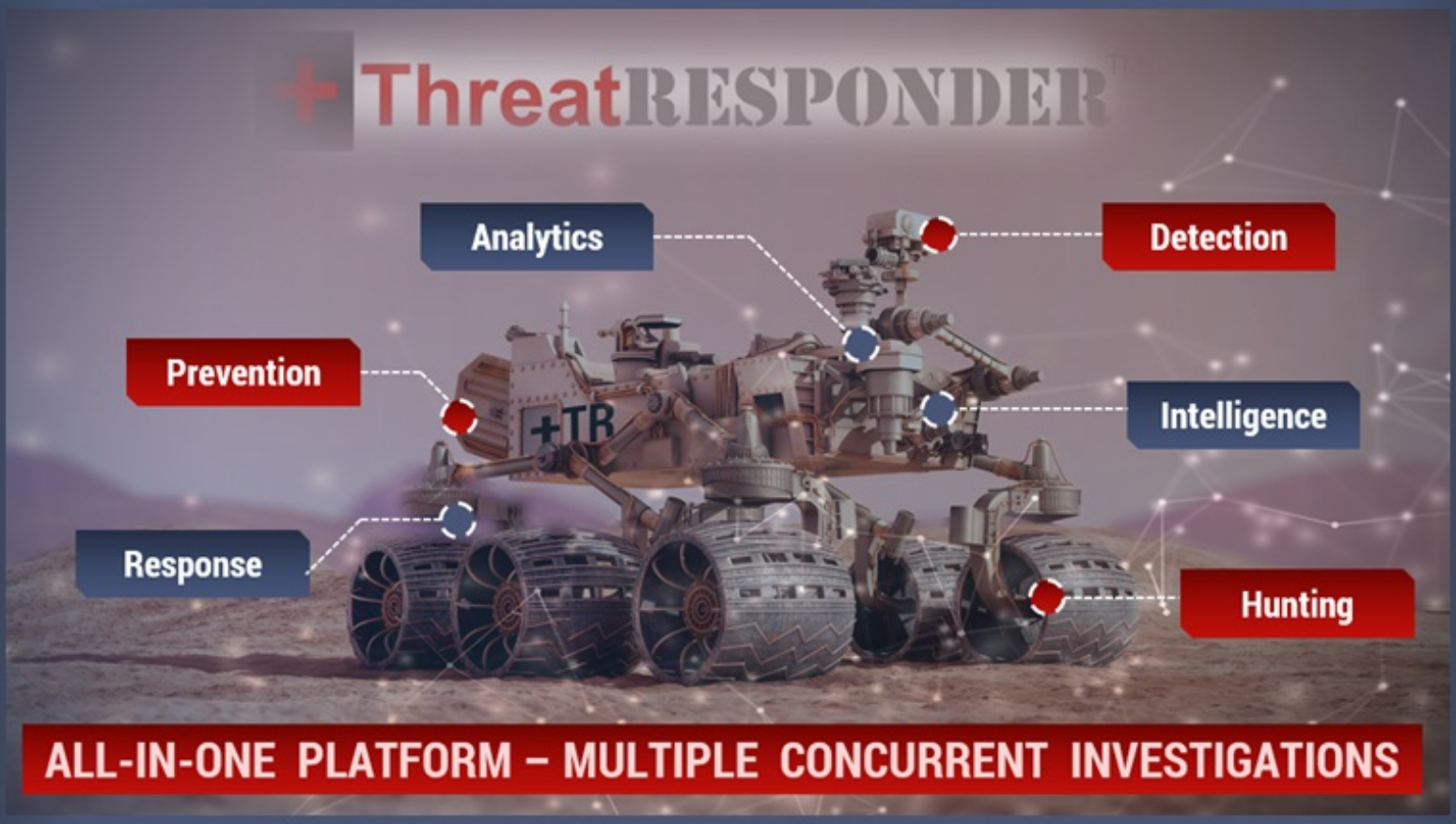
Red Hat Security Advisory 2022-1326-01 - Mozilla Thunderbird is a standalone mail and newsgroup client. This update upgrades Thunderbird to version 91.8.0. Issues addressed include denial of service, out of bounds write, and use-after-free vulnerabilities.

Are You...

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

Do DFIR Investigations Better

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



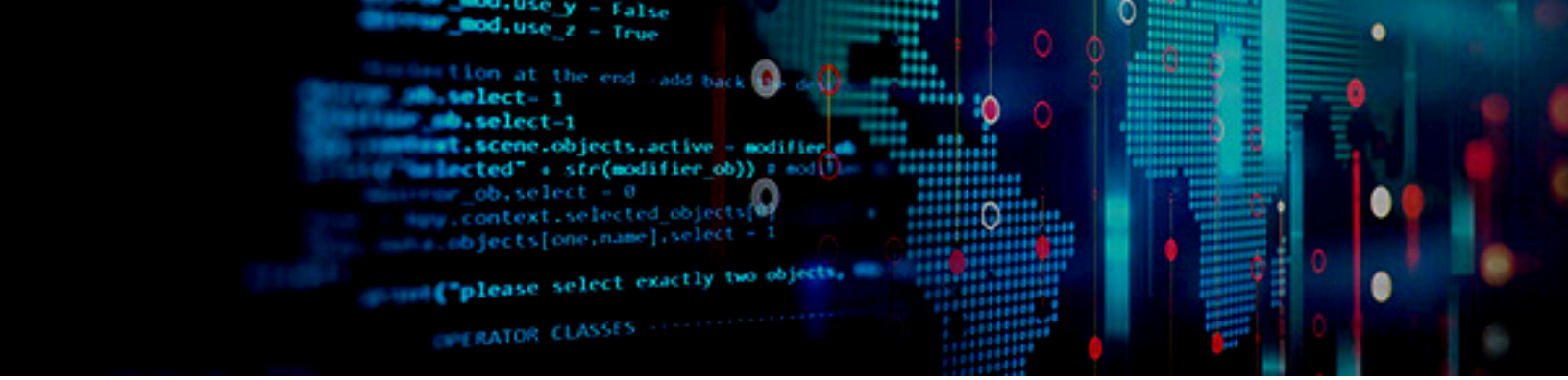
The Solution – ThreatResponder® Platform

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

Get a Trial Copy

Mention **CODE: CIR-0119**

https://netsecurity.com

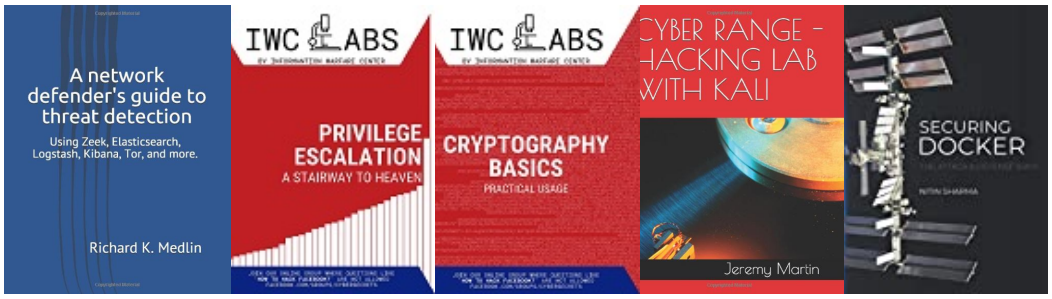


The Cyber Secrets publications on Amazon

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

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

Other Publications from Information Warfare Center



CYBER WEEKLY AWARENESS REPORT

VISIT US AT **INFORMATIONWARFARECENTER.COM**

THE IWC ACADEMY
ACADEMY.INFORMATIONWARFARECENTER.COM

FACEBOOK GROUP
FACEBOOK.COM/GROUPS/CYBERSECRETS

CSI LINUX
CSILINUX.COM

CYBERSECURITY TV
CYBERSEC.TV

ARGOS
APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity

ThreatRESPONDER

Accredited Training Center
EC-Council

CYBERQ GROUP