Oct-10-22

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

October 10, 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

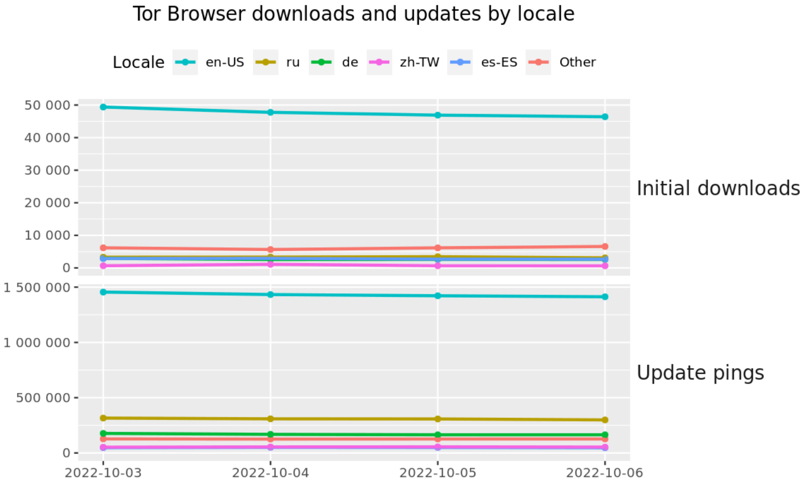
Internet Storm Center Infocon Status

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.



The Tor Project - https://metrics.torproject.org/

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

* Biden Signs Order For EU - U.S. Data Privacy Framework
* 2K Warns Users Their Info Was Stolen Due To A Help Desk Breach
* Binance Says $100 Million Of Crypto Produced Out Of Thin Air By Hackers
* Feds Ink $26 Million Contract For Deception Platform For Defense
* NetWalker Ransomware Scumbag Jailed For 20 Years
* Zelle Fraud Is On The Rise And Many Victims Are Denied Refunds
* No Fix In Sight For Loophole Plaguing a Key Windows Defense
* Uber's Former Security Chief Convicted Of Covering Up 2016 Data Breach
* Modified Version Of Tor Browser Spies On Chinese Users
* DOJ Not Happy With Probation Sentence For Capital One Hacker
* No Shangri-La For You: Top Hotel Chain Confirms Data Leak
* Russian Hacker Arrested In India For Helping Students Cheat In Exam
* Black Holes Can't Trash Info About What They Swallow
* Japanese Sushi Chain Boss Resigns Amid Accusation Of Improper Data Access
* Cybercriminals Leak LA School Data After It Refuses To Ransom
* Singapore Firms See 54 Cybersecurity Incidents Daily
* White House Guidelines For AI Aim To Mitigate Harm
* Kim Kardashian Pays $1.26m Over Crypto Pump And Dump
* How Ransomware Is Causing Chaos In American Schools
* Supreme Court To Scrutinize U.S. Protections For Social Media
* Steganography Alert: Backdoor Spyware Stashed In Microsoft Logo
* Microsoft Says Fix For Two Exchange Zero Days On Accelerated Timeline
* Rights Groups Say Pentagon Is Buying Its Way Around The 4th Amendment
* This Is The GrayKey 2.0, The Tool Cops Use To Hack Phones
* Gone In A Day: Ethical Hackers Say It Would Take Mere Hours To Empty Your Network

Krebs on Security

* Report: Big U.S. Banks Are Stiffing Account Takeover Victims
* Glut of Fake LinkedIn Profiles Pits HR Against the Bots
* Microsoft: Two New 0-Day Flaws in Exchange Server
* Fake CISO Profiles on LinkedIn Target Fortune 500s
* Accused Russian RSOCKS Botmaster Arrested, Requests Extradition to U.S.
* SIM Swapper Abducted, Beaten, Held for $200k Ransom
* Botched Crypto Mugging Lands Three U.K. Men in Jail
* Say Hello to Crazy Thin 'Deep Insert' ATM Skimmers
* Wormable Flaw, 0days Lead Sept. 2022 Patch Tuesday
* Transacting in Person with Strangers from the Internet

LATEST NEWS

Dark Reading

* Email Defenses Under Siege: Phishing Attacks Dramatically Improve
* Credential Harvesting Is Retail Industry's Top Threat
* Cybersecurity Will Account for Nearly One-Quarter of AI Software Market Through 2025
* Meta Flags Malicious Android, iOS Apps Affecting 1M Facebook Users
* State Bar of Georgia Notifies Members and Employees of Cybersecurity Incident
* Patch Now: Fortinet FortiGate & FortiProxy Contain Critical Vuln
* LofyGang Uses 100s of Malicious NPM Packages to Poison Open Source Software
* We Can Save Security Teams From Crushing Workloads. Will We?
* CyberRatings.org Invites Industry Participation in Forthcoming Enterprise Firewall and Data Center Fi
* Sharing Knowledge at 44CON
* macOS Archive Utility Bug Lets Malicious Apps Bypass Security Checks
* Russian Hackers Shut Down US State Government Websites
* US Consumers Are Finally Becoming More Security & Privacy Conscious
* Hackers Have It Out for Microsoft Email Defenses
* Russia-Linked Cybercrime Group Hawks Combo of Malicious Services With LilithBot
* School Is in Session: 5 Lessons for Future Cybersecurity Pros
* 7 IoT Devices That Make Security Pros Cringe
* New SonicWall Survey Data Reveals 91% of Organizations Fear Ransomware Attacks in 2022
* Research Reveals Microsoft Teams Security and Backup Flaws, With Over Half of Users Sharing Business-
* Contrast Security Launches Expanded Security Testing Tools for JavaScript and Popular Angular, React,

The Hacker News

* Hackers Exploiting Unpatched RCE Flaw in Zimbra Collaboration Suite
* Microsoft Issues Improved Mitigations for Unpatched Exchange Server Vulnerabilities
* Fortinet Warns of New Auth Bypass Flaw Affecting FortiGate and FortiProxy
* Facebook Detects 400 Android and iOS Apps Stealing Users Log-in Credentials
* The essentials of GRC and cybersecurity - How they empower each other
* LofyGang Distributed ~200 Malicious NPM Packages to Steal Credit Card Data
* Hackers Can Use 'App Mode' in Chromium Browsers' for Stealth Phishing Attacks
* BlackByte Ransomware Abuses Vulnerable Windows Driver to Disable Security Solutions
* Eternity Group Hackers Offering New LilithBot Malware-as-a-Service to Cybercriminals
* Details Released for Recently Patched new macOS Archive Utility Vulnerability
* The Ultimate SaaS Security Posture Management Checklist, 2023 Edition
* 19-Year-Old Teen Arrested for Using Leaked Optus Breach Data in SMS Scam
* Former Uber Security Chief Found Guilty of Data Breach Coverup
* Experts Warn of New RatMilad Android Spyware Targeting Enterprise Devices
* Telstra Telecom Suffers Data Breach Potentially Exposing Employee Information

LATEST NEWS

Security Week

* Iran State TV Hacked With Image of Supreme Leader in Crosshairs
* Biden Signs Executive Order on US-EU Personal Data Privacy
* VMware Patches Code Execution Vulnerability in vCenter Server
* Cyberinsurance Startup Elpha Secure Raises $20 Million
* Meta Warns of Password Stealing Phone Apps
* Industry Reactions to Conviction of Former Uber CSO Joe Sullivan: Feedback Friday
* Binance Bridge Hit by $560 Million Hack
* Organizations Urged to Patch Vulnerabilities Commonly Targeted by Chinese Cyberspies
* CrowdSec Raises $14 Million for Crowdsourced Threat Intelligence Solution
* Australian Police Make First Arrest in Optus Hack Probe
* The Zero Day Dilemma
* BlackByte Ransomware Abuses Legitimate Driver to Disable Security Protections
* New 'Maggie' Backdoor Targeting Microsoft SQL Servers
* Insurance Giant Lloyd's of London Investigating Cybersecurity Incident
* Cisco Patches High-Severity Vulnerabilities in Communications, Networking Products
* Personal Information of 123K Individuals Exposed in City of Tucson Data Breach
* Hospital Chain Says 'IT Security Issue' Disrupts Operations
* Quantum-Safe Communications Startup Qunnect Raises $8 Million
* FBI, CISA Say Malicious Cyber Activity Unlikely to Disrupt Election
* Former Uber CISO Joe Sullivan Found Guilty Over Breach Cover-Up
* KKR Boosts NetSPI Stake with $410 Million Investment
* SCADA Systems Involved in Many Breaches Suffered by US Ports, Terminals
* SecurityWeek to Host 2022 ICS Cybersecurity Conference October 24-27 in Atlanta
* Iranian Hackers Target Enterprise Android Users With New RatMilad Spyware
* RealDefense Raises $30 Million to Acquire More Privacy, Cybersecurity Firms
* Canadian NetWalker Ransomware Affiliate Gets 20-Year Prison Sentence in US

Infosecurity Magazine

LATEST NEWS

KnowBe4 Security Awareness Training Blog RSS Feed

* [Heads Up] Almost 19 percent of phishing emails bypass Microsoft Defender
* [Head Scratcher] The cyber insurance market is badly broken. But why exactly?
* KnowBe4 Celebrates Winning a Tech Cares Award From TrustRadius 2022
* Cybercriminal Gets 25 Years Prison Time Over Romance Scams and Business Email Compromise Attacks
* Top 5 Phishing Do's & Don'ts
* IRS Warns of A Spike in Smishing Attacks
* FCC Warns of Post-Hurricane Scams
* KnowBe4 Named a Leader in the Fall 2022 G2 Grid Report for Security Awareness Training
* KnowBe4 Named a Leader in the Fall 2022 G2 Grid Report for Security Orchestration, Automation, and Re
* CyberheistNews Vol 12 #40 [Eye Opener] The FBI Warns Against a New Cyber Attack Vector Called Busines

ISC2.org Blog

* Latest Cyberthreats and Advisories - October 7, 2022
* Proposed Amendments to (ISC)&sup2; Bylaws - Member Vote Opens Soon
* Hiring Inexperienced Cybersecurity Practitioners: What's Not to Like?
* October is #CybersecurityAwarenessMonth
* Latest Cyberthreats and Advisories - September 30, 2022

HackRead

* Apple Safari Safest, Google Chrome Riskiest Browser of 2022- Study
* Binance-Linked Network Hacked, Over $570 Million in Losses Recorded
* World's Leading Blockchain DeFiChain Announces Adding Four New dTokens
* Cake DeFi Added Ethereum Staking Service to Allow Unstaking Anytime
* Iranian Hackers Spreading RatMilad Android Spyware Disguised as VPN App
* OnionPoison - Fake Tor Browser Installer Spreading Malware Via YouTube
* Importance of Tax Automation in Digital Business

Koddos

* Apple Safari Safest, Google Chrome Riskiest Browser of 2022- Study
* Binance-Linked Network Hacked, Over $570 Million in Losses Recorded
* World's Leading Blockchain DeFiChain Announces Adding Four New dTokens
* Cake DeFi Added Ethereum Staking Service to Allow Unstaking Anytime
* Iranian Hackers Spreading RatMilad Android Spyware Disguised as VPN App
* OnionPoison - Fake Tor Browser Installer Spreading Malware Via YouTube
* Importance of Tax Automation in Digital Business

LATEST NEWS

Naked Security

* WhatsApp goes after Chinese password scammers via US court
* S3 Ep103: Scammers in the Slammer (and other stories) [Audio + Text]
* Former Uber CSO convicted of covering up megabreach back in 2016
* NetWalker ransomware affiliate sentenced to 20 years by Florida court
* BEC fraudster and romance scammer sent to prison for 25 years
* Scammers and rogue callers - can anything ever stop them?
* S3 Ep102.5: "ProxyNotShell" Exchange bugs - an expert speaks [Audio + Text]
* URGENT! Microsoft Exchange double zero-day - "like ProxyShell, only different"
* S3 Ep102: How to avoid a data breach [Audio + Transcript]
* Optus breach - Aussie telco told it will have to pay to replace IDs

Threat Post

* Student Loan Breach Exposes 2.5M Records
* Watering Hole Attacks Push ScanBox Keylogger
* Tentacles of '0ktapus' Threat Group Victimize 130 Firms
* Ransomware Attacks are on the Rise
* Cybercriminals Are Selling Access to Chinese Surveillance Cameras
* Twitter Whistleblower Complaint: The TL;DR Version
* Firewall Bug Under Active Attack Triggers CISA Warning
* Fake Reservation Links Prey on Weary Travelers
* iPhone Users Urged to Update to Patch 2 Zero-Days
* Google Patches Chrome's Fifth Zero-Day of the Year

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

* VS Code 1.72 enhances Git source control
* Companies are still waiting for their cloud ROI
* Canonical expands application security coverage
* How to merge data in R using R merge, dplyr, or data.table
* Data visualization with Observable JavaScript
* Learn Observable JavaScript with Observable notebooks
* A beginner's guide to using Observable JavaScript, R, and Python with Quarto
* Apollo GraphQL debuts GraphOS platform for building 'supergraphs'
* Hands-on with MongoDB queryable encryption and Node.js
* How to use cancellation tokens in ASP.NET Core 7

C4ISRNET - Media for the Intelligence Age Military

* Unmanned program could suffer if Congress blocks F-22 retirements, Hunter says
* UK to test Sierra Nevada's high-flying spy balloons
* Babcock inks deals to pitch Israeli tech for British radar, air defense programs
* This infantry squad vehicle is getting a laser to destroy drones
* As Ukraine highlights value of killer drones, Marine Corps wants more
* Army Space, Cyber and Special Operations commands form 'triad' to strike anywhere, anytime
* Shell companies purchase radioactive materials, prompting push for nuclear licensing reform
* Marine regiment shows off capabilities at RIMPAC ahead of fall experimentation blitz
* Maxar to aid L3Harris in tracking missiles from space
* US Army's 'Lethality Task Force' looks to save lives with AI

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 quantum state of Linux kernel garbage collection CVE-2021-0920 (Part I)
* 2022 0-day In-the-Wild Exploitation&hellip;so far

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.

* THS CTF 2022
* ASIS CTF Quals 2022
* DEADFACE CTF
* Reply Cyber Security Challenge 2022
* 3rd stage MetaRed CTF Mexico|Anuies-TIC 2022
* Jade CTF
* EyesOpen CTF
* bi0sCTF 2022
* TsukuCTF 2022
* Phoenix CTF

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

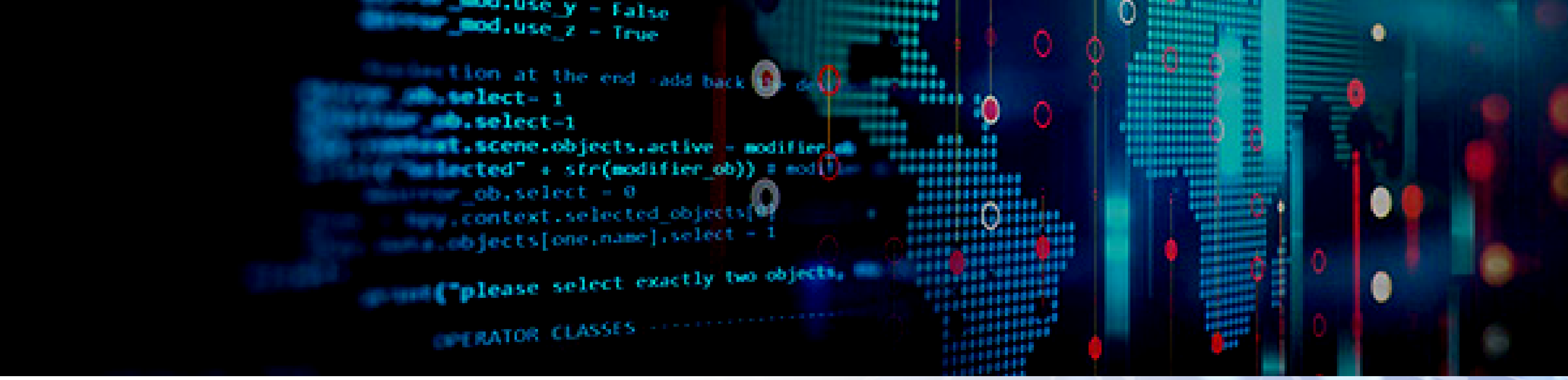
* Wireshark Analyzer 4.0.0
* OpenSSH 9.1p1
* TestSSL 3.0.8
* SIPPTS 3.2
* monomorph MD5-Monomorphic Shellcode Packer
* Suricata IDPE 6.0.8
* nfstream 6.5.2
* Suricata IDPE 6.0.7
* OpenStego Free Steganography Solution 0.8.5
* GNUnet P2P Framework 0.17.6

Kali Linux Tutorials

* Bayanay - Python Wardriving Tool
* Deadfinder - Find Dead-Links (Broken Links)
* Pmanager - Store And Retrieve Your Passwords From A Secure Offline Database
* TestSSL.SH : Testing TLS/SSL Encryption Anywhere On Any Port
* Lunar : UNIX Security Auditing Tool
* Psudohash : Password List Generator That Focuses On Keywords Mutated By Commonly Used Password Creati
* How Does A VPN Work, Is It Safe?
* pyFlipper : Unoffical Flipper Zero Cli Wrapper Written In Python
* bloodyAD : Active Directory Privilege Escalation Framework
* Slicer : Automate The Boring Process Of APK Recon

GBHackers Analysis

* State-Sponsored Hackers Used MS Exchange 0-Day Bugs to Attack At least 10 Orgs
* BIND DNS Software High-Severity Flaws Let Hackers Remotely Trigger the Attack
* RCE Bug in ZOHO Products Let Hackers Execute Arbitrary Code Remotely
* Critical Magento Vulnerability Let Unauthenticated Attackers to Execute Code
* 15-Year-Old Python Bug Let Hacker Execute Code in 350k Python Projects



Weekly Cyber Security Video and Podcasts

SANS DFIR

* SANS Threat Analysis Rundown
* SANS Threat Analysis Rundown
* SANS Threat Analysis Rundown
* The Godfather of Forensics: How to Leverage Your "Year One" to Get an Offer You Cannot Refuse

Defcon Conference

* DEF CON 30 - Sick Codes - Hacking the Farm = Breaking Badly into Agricultural Devices
* DEF CON 30 - RedAlert ICS CTF
* DEF CON 30 - Blue Team Village
* DEF CON 30 - Scavenger Hunt - Flamethrower

Hak5

* Live Hacking Q&A with Kody and Michael
* Chaos Malware Targets Windows and Linux + Giveaway Winner Announcement! - ThreatWire
* Live Hacking Q&A with Kody Kinzie and Alex Lynd

The PC Security Channel [TPSC]

* Most Secure Browser? Chrome vs Firefox vs Edge
* Windows 11 Superlite: No Bloatware and Telemetry

Eli the Computer Guy

* I'm not here... Don't mind me... just testing...
* SUPPLY CHAIN DELAYS - Dojo Diaries
* eBeggar Wednesday - BIDEN DESTROYING JOBS
* COVID is OVER - Dojo Diaries

Security Now

* Poisoning Akamai - Turnstile vs CAPTCHA, Microsoft Teams Under Attack
* DarkNet Politics - EU and Google Analytics, Rockstar hacker busted, Mozilla says no fair

Troy Hunt

* Weekly Update 316

Intel Techniques: The Privacy, Security, & OSINT Show

* 281-The Obsession Of Extreme Privacy
* 280-The Future Of Extreme Privacy

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Joomla Vik Booking 1.15.0 Cross Site Scripting
* WordPress Zephyr Project Manager 3.2.42 SQL Injection
* Joomla KSAdvertiser 2.5.37 Cross Site Scripting
* Linux 3.19 anon_vma Use-After-Free
* Joomla JoomBri Careers 3.3.0 Cross Site Scripting
* Joomla JoomBri Freelance 4.5.0 Cross Site Scripting
* Remote Mouse 4.110 Remote Code Execution
* Ubuntu 22.04.1 X64 Desktop Enlightenment 0.25.3-1 Privilege Escalation
* Canteen Management 1.0-2022 Cross Site Scripting
* WordPress WPvivid Backup Path Traversal
* WordPress Elementor 3.6.2 Shell Upload
* Joomla RAXO All-Mode PRO 2.01 Cross Site Scripting
* Canteen Management 1.0-2022 SQL Injection
* Joomla Solidres 2.12.9 Cross Site Scripting
* Backdoor.Win32.Delf.eg MVID-2022-0647 Remote Command Execution
* Joomla Rentalot Plus 19.05 Cross Site Scripting
* Backdoor.Win32.NTRC MVID-2022-0646 Hardcoded Credential
* Password Manager For IIS 2.0 Cross Site Scripting
* Joomla MarvikShop ShoppingCart 3.4 Cross Site Scripting
* Joomla MarvikShop ShoppingCart 3.4 SQL Injection
* Google Chrome 103.0.5060.53 network::URLLoader::NotifyCompleted Heap Use-After-Free
* Google Chrome 103.0.5060.53 Autofill Assistant Universal Cross Site Scripting
* Joomla JKassa ShoppingCart 2.0.0 SQL Injection
* Joomla Easy Shop 1.4.1 Cross Site Scripting
* Joomla JUX Charity Hub 1.0.4 SQL Injection

CXSecurity

* Ubuntu 22.04.1 X64 Desktop Enlightenment 0.25.3-1 Privilege Escalation
* Remote Mouse 4.110 Remote Code Execution
* qdPM 9.1 Authenticated Shell Upload
* Veritas Backup Exec Agent Remote Code Execution
* Netfilter nft_set_elem_init Heap Overflow Privilege Escalation
* Food Ordering Management System 1.0 SQL Injection
* Bitbucket Git Command Injection

Proof of Concept (PoC) & Exploits

Exploit Database

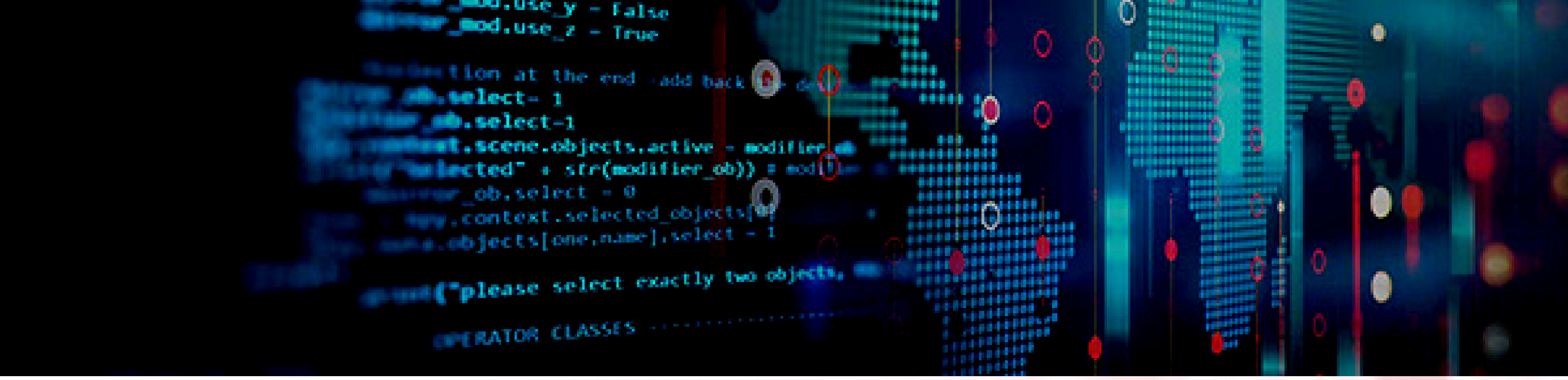
* [webapps] Wordpress Plugin Zephyr Project Manager 3.2.42 - Multiple SQLi
* [webapps] Testa 3.5.1 Online Test Management System - Reflected Cross-Site Scripting (XSS)
* [webapps] Aero CMS v0.0.1 - SQLi
* [webapps] Wordpress Plugin 3dady real-time web stats 1.0 - Stored Cross Site Scripting (XSS)
* [webapps] Wordpress Plugin WP-UserOnline 2.88.0 - Stored Cross Site Scripting (XSS)
* [remote] Teleport v10.1.1 - Remote Code Execution (RCE)
* [webapps] Feehi CMS 2.1.1 - Remote Code Execution (RCE) (Authenticated)
* [webapps] TP-Link Tapo c200 1.1.15 - Remote Code Execution (RCE)
* [remote] WiFiMouse 1.8.3.4 - Remote Code Execution (RCE)
* [remote] Wifi HD Wireless Disk Drive 11 - Local File Inclusion
* [local] Blink1Control2 2.2.7 - Weak Password Encryption
* [webapps] Bookwyrm v0.4.3 - Authentication Bypass
* [webapps] Buffalo TeraStation Network Attached Storage (NAS) 1.66 - Authentication Bypass
* [remote] Airspan AirSpot 5410 version 0.3.4.1 - Remote Code Execution (RCE)
* [remote] Mobile Mouse 3.6.0.4 - Remote Code Execution (RCE)
* [webapps] Gitea 1.16.6 - Remote Code Execution (RCE) (Metasploit)
* [webapps] WordPress Plugin Netroics Blog Posts Grid 1.0 - Stored Cross-Site Scripting (XSS)
* [webapps] WordPress Plugin Testimonial Slider and Showcase 2.2.6 - Stored Cross-Site Scripting (XSS)
* [webapps] Sophos XG115w Firewall 17.0.10 MR-10 - Authentication Bypass
* [remote] PAN-OS 10.0 - Remote Code Execution (RCE) (Authenticated)
* [webapps] ThingsBoard 3.3.1 'description' - Stored Cross-Site Scripting (XSS)
* [webapps] ThingsBoard 3.3.1 'name' - Stored Cross-Site Scripting (XSS)
* [webapps] Feehi CMS 2.1.1 - Stored Cross-Site Scripting (XSS)
* [webapps] Prestashop blockwishlist module 2.1.0 - SQLi
* [remote] uftpd 2.10 - Directory Traversal (Authenticated)

Exploit Database for offline use

Kali has the Exploit-DB preinstalled and updates the database on a monthly basis. The tool that they have added is called "SearchSploit". This can be installed on Linux, Mac, and Windows. Using the tool is also quite simple. In the command line, type:

```
user@yourlinux:~$ searchsploit keyword1 keyword2
```

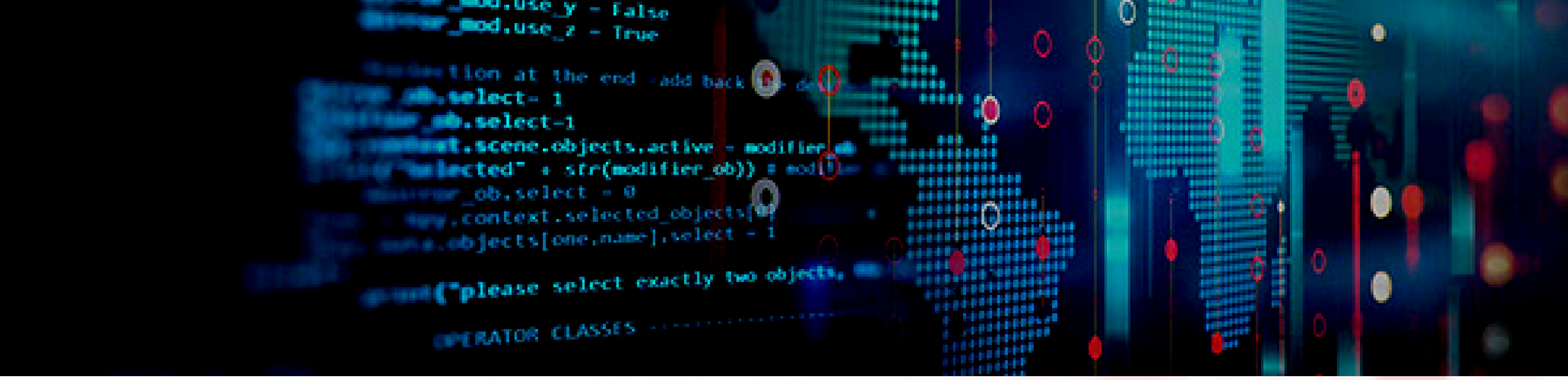
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://sipp.pa-sintang.go.id/babymetal.php
https://sipp.pa-sintang.go.id/babymetal.php notified by KosameAmegai
http://www.pa-sintang.go.id/babymetal.php
http://www.pa-sintang.go.id/babymetal.php notified by KosameAmegai
https://mophrh.gov.mz/bdkr.html
https://mophrh.gov.mz/bdkr.html notified by Mr. BDKR28
https://kpai.go.id
https://kpai.go.id notified by Black_X12
https://www.nicvd.gov.bd/kr.txt
https://www.nicvd.gov.bd/kr.txt notified by Krypton-X
https://alumrania.gov.sd
https://alumrania.gov.sd notified by -1
https://www.crefsp.gov.br/xstro0.html
https://www.crefsp.gov.br/xstro0.html notified by https://www.crefsp.gov.br/xstro0.html
https://rionegro.gov.co/vz.txt
https://rionegro.gov.co/vz.txt notified by aDriv4
https://camaraitapevi.sp.gov.br/vz.txt
https://camaraitapevi.sp.gov.br/vz.txt notified by aDriv4
https://www.lripeo.go.th/robots.txt
https://www.lripeo.go.th/robots.txt notified by ByME
http://ped.go.th
http://ped.go.th notified by ByME
https://bpbd.sukabumikab.go.id/bdkr.html
https://bpbd.sukabumikab.go.id/bdkr.html notified by Mr. BDKR28
http://vms-kominfo.kalbarprov.go.id/666.html
http://vms-kominfo.kalbarprov.go.id/666.html notified by ./s3nt1n3L
http://terbit.dishub.kalbarprov.go.id/666.html
http://terbit.dishub.kalbarprov.go.id/666.html notified by ./s3nt1n3L
http://sippda-disnakertrans.kalbarprov.go.id/666.html
http://sippda-disnakertrans.kalbarprov.go.id/666.html notified by ./s3nt1n3L
http://sipp.dpmptsp.kalbarprov.go.id/666.html
http://sipp.dpmptsp.kalbarprov.go.id/666.html notified by ./s3nt1n3L
http://simrs-rsjd.kalbarprov.go.id/666.html
http://simrs-rsjd.kalbarprov.go.id/666.html notified by ./s3nt1n3L



Dark Web News

Darknet Live

Florida Man Convicted of Using Crypto Mixers to Evade Taxes

A Florida man admitted using "sophisticated online techniques&rdquo; to conceal more than $1 million in cryptocurrency from the IRS. Ethan Thomas Trainor pleaded guilty to attempted tax evasion. According to information revealed in court and a proffer statement, Trainor sold hacked online accounts on darkweb markets in exchange for cryptocurrency. He used mixers in an attempt to obscure the source of the funds. Trainor then underreported his earnings to the IRS by filing tax returns that underrepresented his earnings. For example, according to a criminal information, Trainor filed a tax return in 2015 that was short by $181,933. As a result, the filing resulted in a "loss&rdquo; to the federal government of $40,846. The underreported amounts Trainor admitted that he filed similar tax returns multiple times, resulting in a total "loss&rdquo; to the federal government of $238,894. From the proffer statement: "Ethan TRAINOR bought and sold hacked online account login (usemames and passwonis) for movie streaming websites such as Netflix, pornography websites, Spotify, Major Sports websites, laming websites, and Uber accounts through various dark net markets. TRAINOR illegally obtained these usemames and passwords using various methods, from hacking the accounts himself to buying the hacked usernames and passwords. These darknet markets that TRAINOR operated on are specifically designed to facilitate illegal commerce and provide anonymity through user concealment and by employing numerous financial obfuscation techniques. Agents were able to successfully trace the virtual flow of cryptocurrency proceeds from TRAINOR's sales on various blockchains to numerous mixing and cash-out services.&rdquo; Very serious IRS-CI agents in training There is virtually no information on how investigators tracked Trainor's activities. Perhaps they flagged him for tax evasion and worked backward from there. He faces up to five years in prison and is scheduled to be sentenced in December. Non-Payment of Federal Income Tax on Cryptocurrency Earnings Leads to Conviction for South Florida Resident | www.justice.gov, archive.is, archive.org Statement The last thing you see (via darknetlive.com at https://darknetlive.com/post/florida-man-convicted-of-attempted-tax-evasion/)

US Government Calls for More Cryptocurrency Regulation

Once again, the federal government is calling for more cryptocurrency rules and regulations. The Financial Stability Oversight Council released a report on Digital Asset Financial Stability Risks and Regulation. The report is a response to Section 6 of President Biden's Executive Order 14067 on "Ensuring Responsible Development of Digital Assets.&rdquo; The Council is one of many government bodies with reports calling for the same thing: regulation directed at cryptocurrency. Financial stability risks Crypto-asset activities could pose risks to the stability of the U.S. financial system if their interconnections with the traditional financial system or their overall scale were to grow without adherence to or being paired with appropriate regulation, including enforcement of the existing regulatory structure. The scale of crypto-asset activities has increased significantly in recent years. Although interconnections with the traditional financial system are currently relatively limited, they could potentially increase rapidly. Participants in the crypto-asset ecosystem and the traditional financial system have explored or created a variety of interconnections. Notable sources of potential interconnections include traditional assets held as part of stablecoin activities. Cryptoasset trading platforms may also have the potential for greater interconnections by providing a wide variety of services, including leveraged trading and asset custody, to a range of retail investors and traditional financial institutions. Consumers can also increasingly access cryptoasset activities, including through certain traditional money services businesses. Some characteristics of crypto-asset activities have acutely amplified instability within the crypto-asset ecosystem.   Many crypto-asset activities lack basic risk controls to protect against run risk or to help ensure that leverage is not excessive. Crypto-asset prices appear to be primarily driven by speculation rather than grounded in current fundamental economic use cases, and prices have repeatedly recorded significant and broad declines. Many crypto-asset firms or activities have sizable interconnections with crypto-asset entities that have risky business profiles and opaque capital and liquidity positions. In addition, despite the distributed nature of crypto-asset systems, operational risks may arise from the concentration of key services or from vulnerabilities related to distributed ledger technology.   These vulnerabilities are partly attributable to the choices made by market participants, including crypto-asset issuers and platforms, to not implement or refuse to implement appropriate risk controls, arrange for effective governance, or take other available steps that would address the financial stability risks of their activities. __ Correlations between Bitcoin Prices and Equity Prices   Enforcement of the existing regulatory structure _ Many nonbank firms in the crypto-asset ecosystem have advertised themselves as regulated. Firms often emphasize money services business regulation, though such regulation is largely focused on anti-money laundering controls or consumer protection requirements and does not provide a comprehensive framework for mitigating financial stability vulnerabilities arising from other activities that may be undertaken, for example, by a trading platform or stablecoin issuer. While some firms in the crypto-asset ecosystem have attempted to avoid the existing regulatory system, other firms have engaged with the existing regulatory system by obtaining trust charters or special state-level crypto-asset-specific charters or licenses.   Compliance with and enforcement of the existing regulatory structure is a key step in addressing financial stability risks. For example, certain crypto-asset platforms may be listing securities but are not in compliance with exchange or broker-dealer registration requirements. In addition, certain crypto-asset issuers have offered and sold crypto-assets in violation of federal and state securities laws, because the offering and sale were not registered or conducted pursuant to an available exemption. Regulators have taken enforcement actions over the past several years to address many additional instances of non-compliance with existing rules and regulations, including illegally offered crypto-asset derivatives products, false statements about stablecoin assets, and many episodes of fraud and market manipulation. In addition, false and misleading statements, made directly or by implication, concerning availability of federal deposit insurance for a given product, are violations of the law, and have given customers the impression that they are protected by the government safety net when they are not. Further, misrepresentations by crypto-asset firms about how they are regulated have also confused consumers and investors regarding whether a given crypto-asset product is regulated to the same extent as other financial products.   Regulatory Gaps _ Though the existing regulatory system covers large parts of the crypto-asset ecosystem, this report identifies three gaps in the regulation of crypto-asset activities in the United States. First, the spot markets for crypto-assets that are not securities are subject to limited direct federal regulation. As a result, those markets may not feature robust rules and regulations designed to ensure orderly and transparent trading, prevent conflicts of interest and market manipulation, and protect investors and the economy more broadly. Second, crypto-asset businesses do not have a consistent or comprehensive regulatory framework and can engage in regulatory arbitrage. Some crypto-asset businesses may have affiliates or subsidiaries operating under different regulatory frameworks, and no single regulator may have visibility into the risks across the entire business. Third, a number of crypto-asset trading platforms have proposed offering retail customers direct access to markets by vertically integrating the services provided by intermediaries such as broker-dealers or futures commission merchants. Financial stability and investor protection implications may arise from retail investors' exposure to certain practices commonly proposed by vertically integrated trading platforms, such as automated liquidation.   Recommendations _ The Council notes that large parts of the crypto-asset ecosystem are covered by the existing regulatory structure. In applying these existing authorities, the Council recommends that its members take into consideration a set of principles and emphasizes the importance of continued enforcement of existing rules and regulations.   To address regulatory gaps, the Council recommends: the passage of legislation providing for rulemaking authority for federal financial regulators over the spot market for crypto-assets that are not securities; steps to address regulatory arbitrage including coordination, legislation regarding risks posed by stablecoins, legislation relating to regulators' authorities to have visibility into, and otherwise supervise, the activities of all of the affiliates and subsidiaries of cryptoasset entities, and appropriate service provider regulation; and study of potential vertical integration by crypto-asset firms.   Finally, the Council recommends bolstering its members' capacities related to data and to the analysis, monitoring, supervision, and regulation of crypto-asset activities. The Council appears to be targeting legitimate concerns, such as companies committing securities fraud. Of course, securities fraud is already illegal. The full report can be viewed here. (via darknetlive.com at https://darknetlive.com/post/government-calls-for-more-cryptocurrency-regulation/)

Binance Announces Law Enforcement Training Program

The cryptocurrency exchange Binance announced the launch of a law enforcement training program. Binance, like most other cryptocurrency exchanges and blockchain analytics companies, employs former federal law enforcement officers. These former feds work closely with current feds in many ways, including information sharing and "training programs.&rdquo; The press release: Over the past year, the Binance Investigations team has conducted and participated in more than 30 workshops on countering cyber and financial crime, engaging law enforcement officers in Argentina, Brazil, Canada, France, Germany, Israel, Netherlands, Philippines, Sweden, South Korea, and the UK, among others.   "As more regulators, public law enforcement agencies, and private sector stakeholders look closely at crypto, we are seeing an increased demand for training to help educate on and combat crypto crimes,&rdquo; said Tigran Gambaryan, Global Head of Intelligence and Investigations at Binance. "To meet that demand, we have bolstered our team to conduct more training and work hand-in-hand with regulators across the globe.&rdquo; _

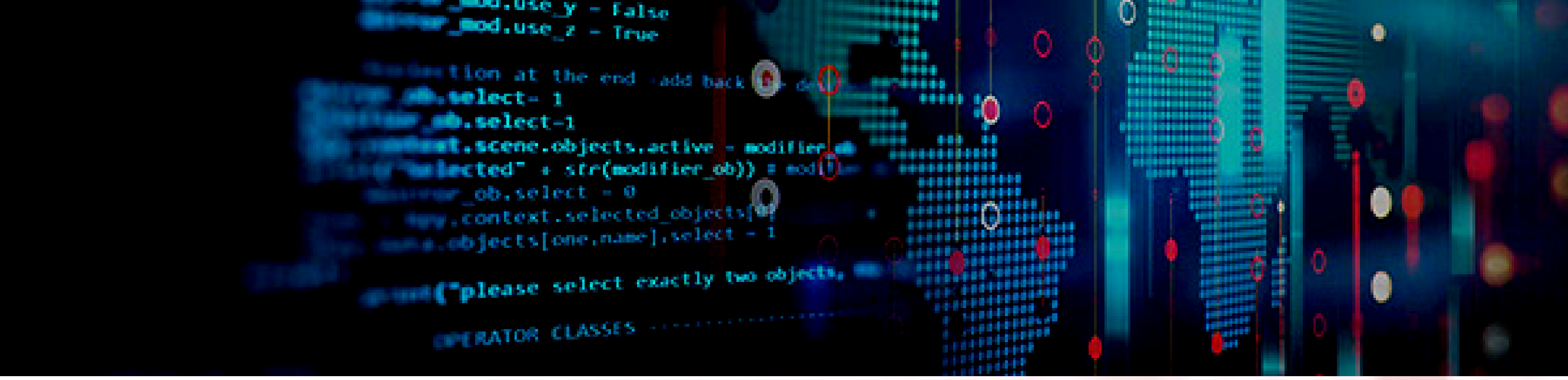
Binance   The training program is led by world-class practitioners from the Binance Investigations team, which employs security experts and former law enforcement agents, including analysts and operatives who had helped take down some of the world's largest criminal platforms, such as Silk Road and Hydra.   The standard one-day training program includes in-person workshops on the fundamental concepts of blockchain and crypto assets, as well as insight into the evolving legal and regulatory environment they operate in. Binance's anti-money laundering (AML) policies and the investigative methods developed by the company to detect and prevent criminal behavior are also discussed in detail.   As a result of deploying robust compliance and AML programs, Binance has recently secured approvals and registrations in France, Italy, and Spain, among others, making the exchange one of the few crypto companies to accomplish this within G7 countries. "Protecting users is our number one priority at Binance. We work hand-in-hand with law enforcement to track and trace suspected accounts and fraudulent activities, contributing to the fight against terrorism financing, ransomware, human trafficking, child pornography, and financial crimes," said Gambaryan, a former special agent of the Internal Revenue Service&mdash;Criminal Investigation (IRS-CI) Cyber Crimes Unit.   Since November 2021, the Binance Investigations team has responded to more than 27,000 law enforcement requests with an average of three days response time, which is faster than any traditional financial institution. "Binance is known among law enforcement to have a fast response system, unmatched by any traditional financial institution,&rdquo; said Gambaryan.   Amid Growing Demand, Binance Boosts its Global Law Enforcement Training Program | www.binance.com, archive.is, archive.org (via darknetlive.com at https://darknetlive.com/post/binance-announces-new-law-enforcement-training-program/)

US Government Working on AI-Powered Stylometry Technology

The Intelligence Advanced Research Projects Activity (IARPA) is working on a program that will use "artificial intelligence technologies capable of attributing authorship.&rdquo; Put another way: the government is creating a program that uses artificial intelligence to identify or fingerprint anonymous authors. IARPA is the research and development arm of the Office of the Director of National Intelligence (ODNI).

_   Office of the Director of National Intelligence   "Each of the selected performers brings a unique, novel, and compelling approach to the HIATUS challenge,&rdquo; said program manager Dr. Tim McKinnon. "We have a strong chance of meeting our goals, delivering much-needed capabilities to the Intelligence Community, and substantially expanding our understanding of variation in human language using the latest advances in computational linguistics and deep learning.&rdquo; The DNI press release: "WASHINGTON, D.C. - The Intelligence Advanced Research Projects Activity (IARPA), the research and development arm of the Office of the Director of National Intelligence, today announced the launch of a program that seeks to engineer novel artificial intelligence technologies capable of attributing authorship and protecting authors' privacy.&rdquo;   "The Human Interpretable Attribution of Text Using Underlying Structure (HIATUS) program represents the Intelligence Community's latest research effort to advance human language technology. The resulting innovations could have far-reaching impacts, with the potential to counter foreign malign influence activities; identify counterintelligence risks; and help safeguard authors who could be endangered if their writing is connected to them.&rdquo;   The program's goals are to create technologies that: Perform multilingual authorship attribution by identifying stylistic features &mdash; such as word choice, sentence phrasing, organization of information &mdash; that help determine who authored a given text. Protect the author's privacy by modifying linguistic patterns that indicate the author's identity. Implement explainable AI techniques that provide novice users an understanding, trust, and verification as to why a particular text is attributable to a specific author or why a particular revision will preserve an author's privacy.   "Through a competitive Broad Agency Announcement, IARPA awarded HIATUS research contracts to the following lead organizations, which together bring more than 20 academic institutions, non-profits, and businesses into the program: Charles River Analytics, Inc. Leidos, Inc. Raytheon BBN SRI International University of Pennsylvania University of Southern California   "The HIATUS test and evaluation team consists of Lawrence Livermore National Labs, Pacific Northwest National Labs, and the University of Maryland Applied Research Laboratory for Intelligence and Security.&rdquo;   \   IARPA Kicks off Research Into Linguistic Fingerprint Technology | www.dni.gov, archive.is, archive.org (via darknetlive.com at https://darknetlive.com/post/dni-funding-stylometry-project/)

Dark Web Link



Trend Micro Anti-Malware Blog

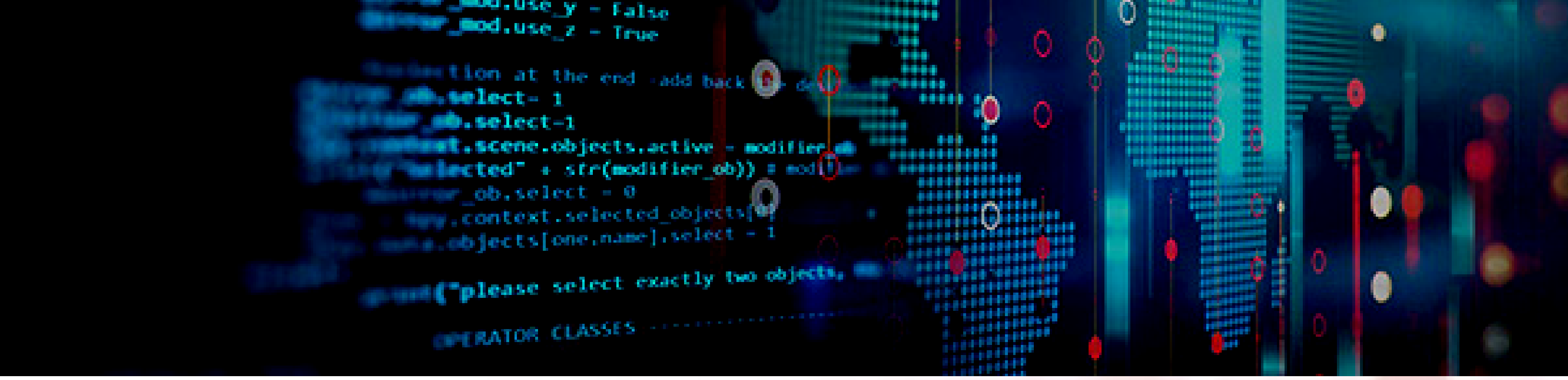
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

Unfortunately, at the time of this report, the RiskIQ resource was not availible.

FireEye

* Metasploit Weekly Wrap-Up
* CVE-2022-40684: Remote Authentication Bypass Vulnerability in Fortinet Firewalls, Web Proxies
* Exploitation of Unpatched Zero-Day Remote Code Execution Vulnerability in Zimbra Collaboration Suite
* What's New in InsightIDR: Q3 2022 in Review
* Velociraptor Version 0.6.6: Multi-Tenant Mode and More Let You Dig Deeper at Scale Like Never Before
* Metasploit Weekly Wrap-Up
* CVE-2022-41040 and CVE-2022-41082: Unpatched Zero-Day Vulnerabilities in Microsoft Exchange Server
* [The Lost Bots] S02E04: Cyber's Most Dangerous Game - Threat Hunting
* The Empty SOC Shop: Where Has All the Talent Gone?
* [Security Nation] Taki Uchiyama of Panasonic on Product Security and Incident Response



Advisories

US-Cert Alerts & bulletins

* FBI and CISA Publish a PSA on Information Manipulation Tactics for 2022 Midterm Elections
* Top CVEs Actively Exploited by People's Republic of China State-Sponsored Cyber Actors
* Cisco Releases Security Updates for Multiple Products
* CISA Releases Two Industrial Control Systems Advisories
* FBI and CISA Publish a PSA on Malicious Cyber Activity Against Election Infrastructure
* Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organ
* CISA Releases Five Industrial Control Systems Advisories
* CISA Issues Binding Operational Directive 23-01: Improving Asset Visibility and Vulnerability Detecti
* AA22-279A: Top CVEs Actively Exploited By People's Republic of China State-Sponsored Cyber Actors
* AA22-277A: Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial
* Vulnerability Summary for the Week of September 26, 2022
* Vulnerability Summary for the Week of September 19, 2022

Zero Day Initiative Advisories

Packet Storm Security - Latest Advisories

Red Hat Security Advisory 2022-6839-01

Red Hat Security Advisory 2022-6839-01 - Squid is a high-performance proxy caching server for web clients, supporting FTP, Gopher, and HTTP data objects.

Red Hat Security Advisory 2022-6850-01

Red Hat Security Advisory 2022-6850-01 - Open vSwitch provides standard network bridging functions and support for the OpenFlow protocol for remote per-flow control of traffic. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-6831-01

Red Hat Security Advisory 2022-6831-01 - Expat is a C library for parsing XML documents. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2022-6832-01

Red Hat Security Advisory 2022-6832-01 - Expat is a C library for parsing XML documents. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2022-6834-01

Red Hat Security Advisory 2022-6834-01 - Expat is a C library for parsing XML documents. Issues addressed include a use-after-free vulnerability.

Red Hat Security Advisory 2022-6835-01

Red Hat Security Advisory 2022-6835-01 - This release of Red Hat Integration - Service registry 2.3.0.GA serves as a replacement for 2.0.3.GA, and includes the below security fixes. Issues addressed include code execution, cross site scripting, denial of service, deserialization, and privilege escalation vulnerabilities.

Red Hat Security Advisory 2022-6833-01

Red Hat Security Advisory 2022-6833-01 - Expat is a C library for parsing XML documents. Issues addressed include a use-after-free vulnerability.

Ubuntu Security Notice USN-5661-1

Ubuntu Security Notice 5661-1 - It was discovered that LibreOffice incorrectly validated macro signatures. If a user were tricked into opening a specially crafted document, a remote attacker could possibly use this issue to execute arbitrary macros. It was discovered that Libreoffice incorrectly handled encrypting the master key provided by the user for storing passwords for web connections. A local attacker could possibly use this issue to obtain access to passwords stored in the user's configuration data.

Hashicorp Boundary Clickjacking

Hashicorp Boundary versions prior to 0.9.1 suffer from a clickjacking vulnerability.

Red Hat Security Advisory 2022-6820-01

Red Hat Security Advisory 2022-6820-01 - Prometheus JMX Exporter is a JMX to Prometheus exporter: a collector that can be configured to scrape and expose MBeans of a JMX target. Issues addressed include a denial of service vulnerability.

Ubuntu Security Notice USN-5659-1

Ubuntu Security Notice 5659-1 - Stephane Chauveau discovered that kitty incorrectly handled image filenames with special characters in error messages. A remote attacker could possibly use this to execute arbitrary commands. This issue only affected Ubuntu 20.04 LTS. Carter Sande discovered that kitty incorrectly handled escape sequences in desktop notifications. A remote attacker could possibly use this to execute arbitrary commands. This issue only affected Ubuntu 22.04 LTS.

Ubuntu Security Notice USN-5660-1

Ubuntu Security Notice 5660-1 - It was discovered that the framebuffer driver on the Linux kernel did not verify size limits when changing font or screen size, leading to an out-of- bounds write. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. Moshe Kol, Amit Klein and Yossi Gilad discovered that the IP implementation in the Linux kernel did not provide sufficient randomization when calculating port offsets. An attacker could possibly use this to expose sensitive information.

Red Hat Security Advisory 2022-6757-01

Red Hat Security Advisory 2022-6757-01 - This release of Red Hat build of Eclipse Vert.x 4.3.3 GA includes security updates. For more information, see the release notes listed in the References section. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-6819-01

Red Hat Security Advisory 2022-6819-01 - 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 2.2.0 serves as a replacement for Red Hat AMQ Streams 2.1.0, and includes security and bug fixes, and enhancements. Issues addressed include denial of service and deserialization vulnerabilities.

Ubuntu Security Notice USN-5658-1

Ubuntu Security Notice 5658-1 - It was discovered that DHCP incorrectly handled option reference counting. A remote attacker could possibly use this issue to cause DHCP servers to crash, resulting in a denial of service. It was discovered that DHCP incorrectly handled certain memory operations. A remote attacker could possibly use this issue to cause DHCP clients and servers to consume resources, leading to a denial of service.

Red Hat Security Advisory 2022-6821-01

Red Hat Security Advisory 2022-6821-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This release of Red Hat JBoss Enterprise Application Platform 7.4.7 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.4.6, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.4.7 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-6823-01

Red Hat Security Advisory 2022-6823-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This release of Red Hat JBoss Enterprise Application Platform 7.4.7 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.4.6, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.4.7 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-6822-01

Red Hat Security Advisory 2022-6822-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This release of Red Hat JBoss Enterprise Application Platform 7.4.7 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.4.6, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.4.7 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-6825-01

Red Hat Security Advisory 2022-6825-01 - Red Hat JBoss Enterprise Application Platform 7 is a platform for Java applications based on the WildFly application runtime. This release of Red Hat JBoss Enterprise Application Platform 7.4.7 serves as a replacement for Red Hat JBoss Enterprise Application Platform 7.4.6, and includes bug fixes and enhancements. See the Red Hat JBoss Enterprise Application Platform 7.4.7 Release Notes for information about the most significant bug fixes and enhancements included in this release. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-6813-01

Red Hat Security Advisory 2022-6813-01 - 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 XML injection, bypass, denial of service, and traversal vulnerabilities.

Red Hat Security Advisory 2022-6815-01

Red Hat Security Advisory 2022-6815-01 - Squid is a high-performance proxy caching server for web clients, supporting FTP, Gopher, and HTTP data objects.

Ubuntu Security Notice USN-5656-1

Ubuntu Security Notice 5656-1 - Joseph Yasi discovered that JACK incorrectly handled the closing of a socket in certain conditions. An attacker could potentially use this issue to cause a crash.

Red Hat Security Advisory 2022-6782-01

Red Hat Security Advisory 2022-6782-01 - 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 7.5.3 on RHEL 7 serves as a replacement for Red Hat Single Sign-On 7.5.2, and includes bug fixes and enhancements, which are documented in the Release Notes document linked to in the References. Issues addressed include HTTP request smuggling, code execution, cross site scripting, and denial of service vulnerabilities.

Red Hat Security Advisory 2022-6777-01

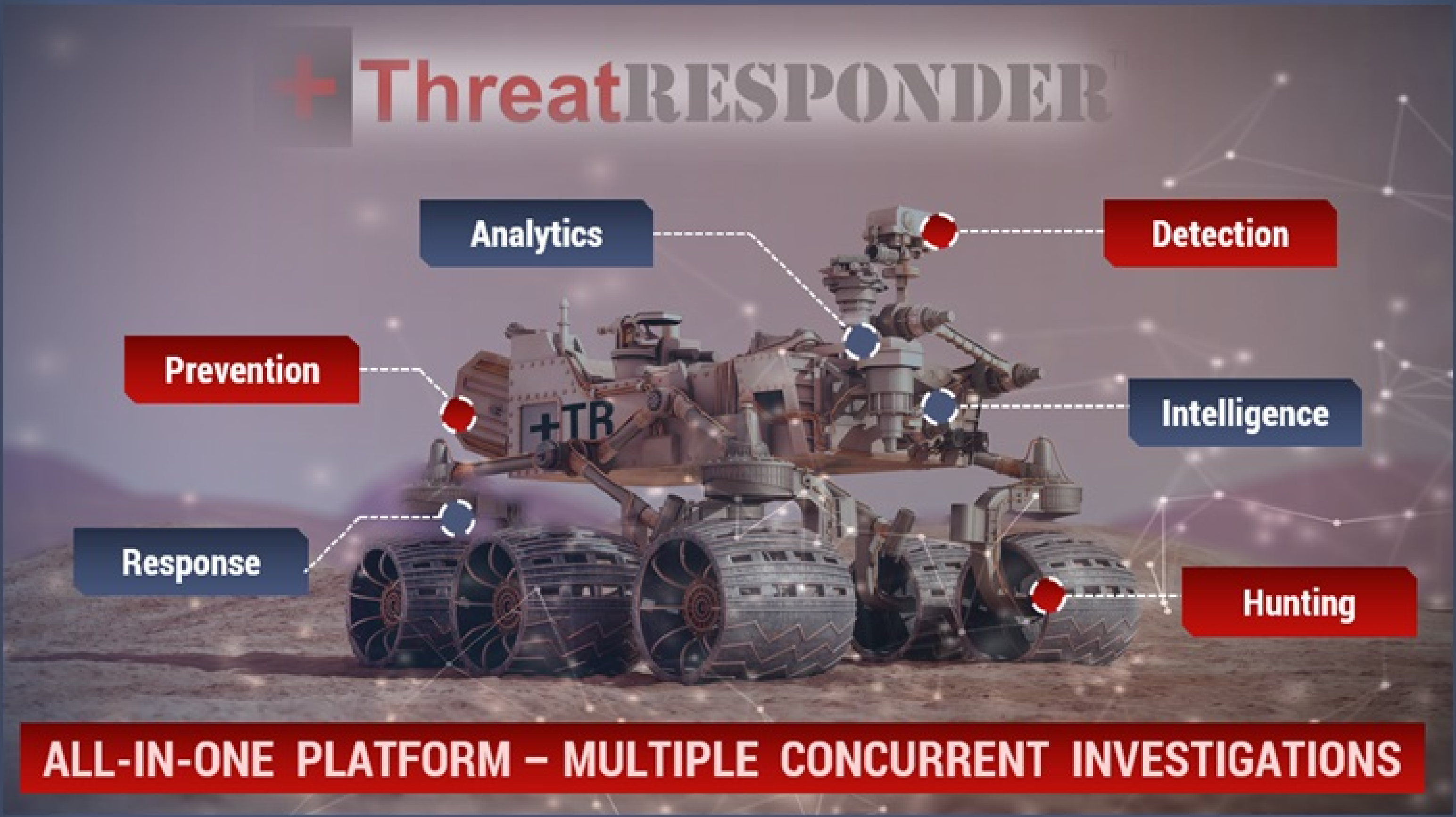
Red Hat Security Advisory 2022-6777-01 - Squid is a high-performance proxy caching server for web clients, supporting FTP, Gopher, and HTTP data objects.

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



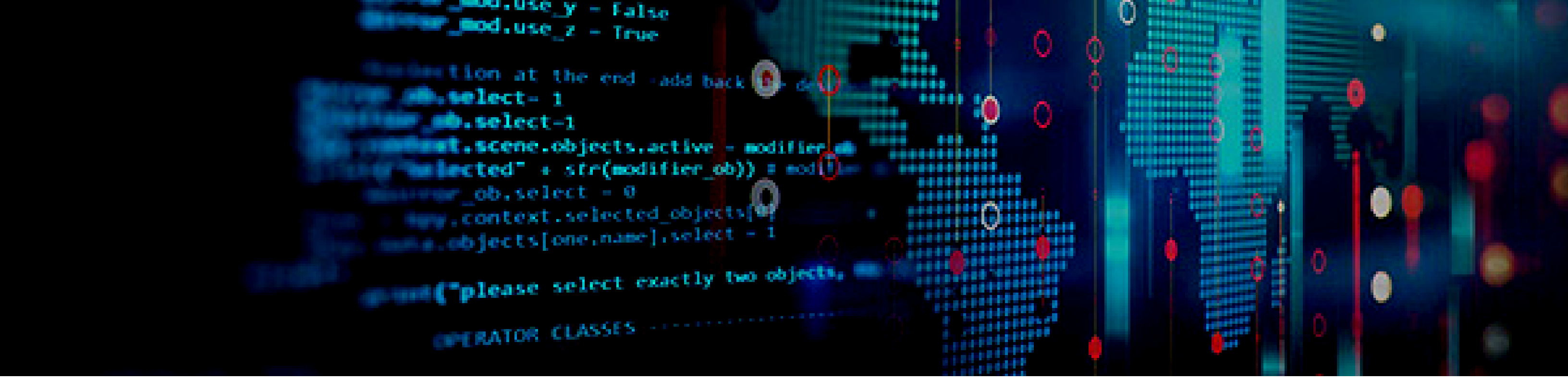
The Solution – ThreatResponder® Platform

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



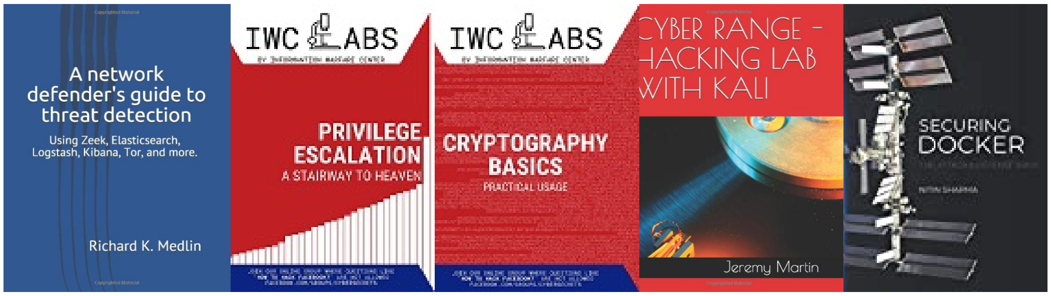
The Cyber Secrets publications on Amazon

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.

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

Other Publications from Information Warfare Center


A network defender's guide to threat detection
Using Zeek, Elasticsearch, Logstash, Kibana, Tor, and more.
Richard K. Medlin
IWC LABS
PRIVILEGE ESCALATION
A STAIRWAY TO HEAVEN
IWC LABS
CRYPTOGRAPHY BASICS
PRACTICAL USAGE
CYBER RANGE - HACKING LAB WITH KALI
Jeremy Martin
SECURING DOCKER

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

Si LINUX

netSecurity®

ThreatRESPONDER

Accredited Training Center EC-Council

CYBERQ GROUP