May-23-22

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

May 23, 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

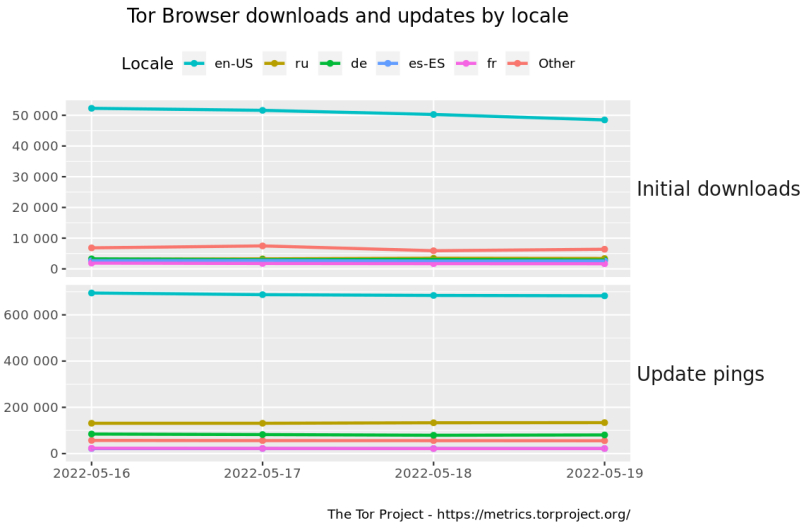
Internet Storm Center Infocon Status

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

Current News
* Packet Storm Security
* Krebs on Security
* Dark Reading
* The Hacker News
* Security Week
* Infosecurity Magazine
* KnowBe4 Security Awareness Training Blog
* ISC2.org Blog
* HackRead
* Koddos
* Naked Security
* Threat Post
* Null-Byte
* IBM Security Intelligence
* Threat Post
* C4ISRNET - Media for the Intelligence Age Military

The Hacker Corner:
* Security Conferences
* Google Zero Day Project

Cyber Range Content
* CTF Times Capture the Flag Event List
* Vulnhub

Tools & Techniques
* Packet Storm Security Latest Published Tools
* Kali Linux Tutorials
* GBHackers Analysis

InfoSec Media for the Week
* Black Hat Conference Videos
* Defcon Conference Videos
* Hak5 Videos
* Eli the Computer Guy Videos
* Security Now Videos
* Troy Hunt Weekly
* Intel Techniques: The Privacy, Security, & OSINT Show

Exploits and Proof of Concepts
* Packet Storm Security Latest Published Exploits
* CXSecurity Latest Published Exploits
* Exploit Database Releases

Cyber Crime & Malware Files/Links Latest Identified
* CyberCrime-Tracker

Advisories
* Hacked Websites
* Dark Web News
* US-Cert (Current Activity-Alerts-Bulletins)
* Zero Day Initiative Advisories
* Packet Storm Security's Latest List

Information Warfare Center Products
* CSI Linux
* Cyber Secrets Videos & Resoures
* Information Warfare Center Print & eBook Publications

Packet Storm Security

* Global Food Supply Chain At Risk From Malicious Hackers
* Strapi Exposed Data, Password Reset To Unprivileged Users
* 380K Kubernetes API Servers Exposed To Public Internet
* DOJ Announces It Won't Prosecute White Hat Security Researchers
* Putin Promises To Bolster Russia's IT Security In Face Of Cyber Attacks
* Homeland Security Pushes Pause On New Disinformation Board
* This Russian Botnet Does Far More Than DDoS Attacks - And On A Massive Scale
* Iran, China-Linked Gangs Join Putin's Disinformation War Online
* Two Military Satellites Just Communicated Using Space Lasers
* Hot Glare Of The Spotlight Doesn't Slow BlackByte Ransomware Gang
* 2 Vulnerabilities With 9.8 Severity Rating Are Under Exploit. A 3rd Looms
* FBI And NSA Say: Stop Doing These 10 Things That Let Hackers In
* Your Data Is Auctioned Off Up To 987 Times A Day, NGO Reports
* Hackers Compromise A String Of Discord Channels
* April VMware Bugs Abused To Deliver Mirai Malware, Exploit Log4Shell
* DOJ Says Doctor Is Malware Mastermind
* President Rodrigo Chaves Says Costa Rica Is At War With Conti Hackers
* New Bluetooth Hack Can Unlock Your Tesla And More
* APTs Overwhelmingly Share Known Vulnerabilities Rather Than Attack 0-Days
* State Of Internet Crime In Q1 2022: Bot Traffic On The Rise, And More
* Wizard Spider Hackers Hire Cold Callers To Scare Ransomware Victims Into Paying Up
* Sysrv-K Botnet Targets Windows, Linux
* FBI: Hackers Used Malicious PHP Code To Grab Credit Card Data
* iPhones Vulnerable To Attack Even When Turned Off
* Don't Accidentally Hire A North Korean Hacker, FBI Warns

Krebs on Security

* Senators Urge FTC to Probe ID.me Over Selfie Data
* When Your Smart ID Card Reader Comes With Malware
* DEA Investigating Breach of Law Enforcement Data Portal
* Microsoft Patch Tuesday, May 2022 Edition
* Your Phone May Soon Replace Many of Your Passwords
* Russia to Rent Tech-Savvy Prisoners to Corporate IT?
* You Can Now Ask Google to Remove Your Phone Number, Email or Address from Search Results
* Fighting Fake EDRs With 'Credit Ratings' for Police
* Leaked Chats Show LAPSUS$ Stole T-Mobile Source Code
* Conti's Ransomware Toll on the Healthcare Industry

Dark Reading

* Chatbot Army Deployed in Latest DHL Shipping Phish
* Partial Patching Still Provides Strong Protection Against APTs
* Quantum Key Distribution for a Post-Quantum World
* Microsoft Rushes a Fix After May Patch Tuesday Breaks Authentication
* Authentication Is Static, Yet Attackers Are Dynamic: Filling the Critical Gap
* New Open Source Project Brings Consistent Identity Access to Multicloud
* More Than 1,000 Cybersecurity Career Pursuers Complete the (ISC)² Entry-Level Cybersecurity Cert
* Deadbolt Ransomware Targeting QNAP NAS Devices
* Pro-Russian Information Operations Escalate in Ukraine War
* DoJ Won't Charge 'Good Faith' Security Researchers
* Majority of Kubernetes API Servers Exposed to the Public Internet
* Dig Exits Stealth With $11M for Cloud Data Detection and Response Solution
* 6 Scary Tactics Used in Mobile App Attacks
* Phishing Attacks for Initial Access Surged 54% in Q1
* MITRE Creates Framework for Supply Chain Security
* CISA to Federal Agencies: Patch VMware Products Now or Take Them Offline
* How Pwn2Own Made Bug Hunting a Real Sport
* Lacework Integrates Kubernetes Features to Enhance Security Across Multi-Cloud Environments
* CISA: Unpatched F5 BIG-IP Devices Under Active Attack
* The Industry Must Better Secure Open Source Code From Threat Actors

The Hacker News

* Chinese "Twisted Panda" Hackers Caught Spying on Russian Defense Institutes
* Researchers Find Backdoor in School Management Plugin for WordPress
* Cisco Issues Patch for New IOS XR Zero-Day Vulnerability Exploited in the Wild
* Microsoft Warns Rise in XorDdos Malware Targeting Linux Devices
* Cytrox's Predator Spyware Targeted Android Users with Zero-Day Exploits
* Researchers Uncover Rust Supply Chain Attack Targeting Cloud CI Pipelines
* Hackers Exploiting VMware Horizon to Target South Korea with NukeSped Backdoor
* Hackers Trick Users with Fake Windows 11 Downloads to Distribute Vidar Malware
* QNAP Urges Users to Update NAS Devices to Prevent Deadbolt Ransomware Attacks
* New Bluetooth Hack Could Let Attackers Remotely Unlock Smart Locks and Cars
* 7 Key Findings from the 2022 SaaS Security Survey Report
* High-Severity Bug Reported in Google's OAuth Client Library for Java
* Web Trackers Caught Intercepting Online Forms Even Before Users Hit Submit
* VMware Releases Patches for New Vulnerabilities Affecting Multiple Products
* How to Protect Your Data When Ransomware Strikes

Security Week

* IBM Dives Into TrickBot Gang's Malware Crypting Operation
* Breach Exposed Data of Half-Million Chicago Students, Staff
* Nikkei Says Customer Data Likely Impacted in Ransomware Attack
* New Brute Force Attacks Against SQL Servers Use PowerShell Wrapper
* DoJ Will No Longer Use CFAA to Charge Ethical Hackers
* Pro-Russian Hackers Spread Hoaxes to Divide Ukraine, Allies
* Researchers Spot Supply Chain Attack Targeting GitLab CI Pipelines
* Phishers Add Chatbot to the Phishing Lure
* QuSecure Lauches Quantum-Resilient Encryption Platform
* Cloud Data Security Firm Dig Emerges From Stealth With $11 Million in Funding
* US Recovers $15 Million From Ad Fraud Group
* Enterprise Data Protection Company Seclore Raises $27 Million
* CISA: Hackers Will Quickly Start Exploiting Newly Patched VMware Vulnerabilities
* Microsoft Teams Exploits Earn Hackers $450,000 at Pwn2Own 2022
* Cornami Raises $68 Million for Quantum Secure Computing on Encrypted Data
* US Government Says North Korean IT Workers Enable DPRK Hacking Operations
* Now Live: SecurityWeek Threat Intelligence Summit Virtual Event
* The Vulnerable Maritime Supply Chain - a Threat to the Global Economy
* National Cybersecurity Agencies Describe Commonly Used Initial Access Techniques
* Over 380,000 Kubernetes API Servers Exposed to Internet: Shadowserver
* Carlyle to Acquire Defense Contractor ManTech in $4.2 Billion Deal
* NVIDIA Patches Code Execution Vulnerabilities in Graphics Driver
* Large-Scale Attack Targeting Tatsu Builder WordPress Plugin
* New Special Interest Group Aims to Enhance ICS/OT Cyber Defenses
* Learn to Use This First: Four Fundamental Tactics to Protect Email Ecosystems
* Access Orchestration Firm Pathlock Announces Several M&As and $200M Funding

Infosecurity Magazine

KnowBe4 Security Awareness Training Blog RSS Feed

* Phishing Attacks Increase by 54% as Initial Attack Vector for Access and Extortion Attacks
* It's More Than Phishing; How to Supercharge Your Security Awareness Training
* Phishing Campaign Impersonates Shipping Giant Maersk
* WSJ: "Cyber Insurance Went Up A Whopping 92% In 2021"
* Spear Phishing a Diplomat
* CyberheistNews Vol 12 #20 [Heads Up] Now You Need to Watch Out for Spoofed Vanity URLs...
* Why People Fall for Scams
* Think BEC Won't Cost You Much? How Does $130 Million Sound?
* Homeland Security: U.S. Ransomware Attacks Have Doubled in the Last Year
* Trezor Crypto Wallet Attacks Results in Class Action Lawsuit Against MailChimp Owner Intuit

ISC2.org Blog

* (ISC)² Entry-Level Cybersecurity Certification Pilot Exam Reaches 1,000 Exam Milestone
* How to Prevent Burnout Among Cybersecurity Professionals Before, During and After a Breach
* (ISC)² Advocates for Membership - Shares Opinions on Proposed UK Standards and Pathway
* Report: Cybersecurity Skills Gap Creates Vulnerabilities
* You Can Join the (ISC)² Board of Directors

HackRead

* 5 Casual Games You Can Play on Your Mobile Browser Now
* A Short Guide to Understanding the Exciting Realm of Fintech
* Avoiding Risks by Using Secure Online Crypto Platform
* Beware of Fake Windows 11 Downloads Distributing Vidar Malware
* Pwn2Own 2022 - Windows 11, MS Teams and Firefox Pwned on Day 1
* New Robo-Dialing Campaign Lets Users Prank Call Russian Bureaucrats
* Attackers Can Unlock Tesla Cars and Smart Devices by Exploiting Bluetooth Flaws

Koddos

* 5 Casual Games You Can Play on Your Mobile Browser Now
* A Short Guide to Understanding the Exciting Realm of Fintech
* Avoiding Risks by Using Secure Online Crypto Platform
* Beware of Fake Windows 11 Downloads Distributing Vidar Malware
* Pwn2Own 2022 - Windows 11, MS Teams and Firefox Pwned on Day 1
* New Robo-Dialing Campaign Lets Users Prank Call Russian Bureaucrats
* Attackers Can Unlock Tesla Cars and Smart Devices by Exploiting Bluetooth Flaws

Naked Security

* Mozilla patches Wednesday's Pwn2Own double-exploit… on Friday!
* Microsoft patches the Patch Tuesday patch that broke authentication
* US Government says: Patch VMware right now, or get off our network
* S3 Ep83: Cracking passwords, patching Firefox, and Apple vulns [Podcast]
* Pwn2Own hacking schedule released - Windows and Linux are top targets
* Apple patches zero-day kernel hole and much more - update now!
* Firefox out-of-band update to 100.0.1 - just in time for Pwn2Own?
* He sold cracked passwords for a living - now he's serving 4 years in prison
* S3 Ep82: Bugs, bugs, bugs (and Colonial Pipeline again) [Podcast]
* Serious Security: Learning from curl's latest bug update

Threat Post

* Closing the Gap Between Application Security and Observability
* 380K Kubernetes API Servers Exposed to Public Internet
* Critical Vulnerability in Premium WordPress Themes Allows for Site Takeover
* DOJ Says Doctor is Malware Mastermind
* APTs Overwhelmingly Share Known Vulnerabilities Rather Than Attack O-Days
* April VMware Bugs Abused to Deliver Mirai Malware, Exploit Log4Shell
* Sysrv-K Botnet Targets Windows, Linux
* iPhones Vulnerable to Attack Even When Turned Off
* Microsoft's May Patch Tuesday Updates Cause Windows AD Authentication Errors
* Threat Actors Use Telegram to Spread 'Eternity' Malware-as-a-Service

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

* What is JPA? Introduction to the Jakarta Persistence API
* Understand the trade-offs with reactive and proactive cloudops
* What's new in Rust 1.61
* OpenFeature feature flag project applies for CNCF sandbox project status
* Java concurrency could be about to get easier
* Developer survey: JavaScript and Python reign, but Rust is rising
* The quantum menace: Quantum computing and cryptography
* Add security to Azure applications with Azure WAF
* The best new features and fixes in Python 3.11
* Bootstrap 5.2.0 bolsters CSS, custom components

C4ISRNET - Media for the Intelligence Age Military

* Military commands spent pandemic money on space analytics, IT upgrades
* Pentagon making progress on cybersecurity amid challenges, watchdog says
* Putin complains about barrage of cyberattacks
* Why Latin American partners need a better way to share intel than WhatsApp
* Pentagon tech chief wants an 'all in one' sensor
* Space Force 'reverse industry day' to address gaps in sensing, tracking
* Ukrainian troops training with US electronic jamming kit
* Pentagon CIO stands ground on December timeline for JEDI follow-up
* Defense Innovation Unit picks designs for space nuclear propulsion demo
* Special ops force calls for 'untethered' tool for recon and resupply

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

* Release of Technical Report into the AMD Security Processor
* The More You Know, The More You Know You Don't Know

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.

* Moroccan Cyber Security Camp 2022
* Hacktrick CTF'22
* BYUCTF 2022
* HeroCTF v4
* DEF CON CTF Qualifier 2022
* HSCTF 9
* SEETF 2022
* BCACTF 3.0
* BSidesSF 2022 CTF
* n00bzCTF

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

* Lynis Auditing Tool 3.0.8
* COOPER Analysis Tool
* Aircrack-ng Wireless Network Tools 1.7
* Samhain File Integrity Checker 4.4.9
* Adversary3 2.0
* Wireshark Analyzer 3.6.5
* Clam AntiVirus Toolkit 0.105.0
* OpenSSL Toolkit 3.0.3
* OpenSSL Toolkit 1.1.1o
* Samhain File Integrity Checker 4.4.8

Kali Linux Tutorials

* Auto-Elevate : Escalate From A Low-Integrity Administrator Account To NT AUTHORITY\SYSTEM
* Subdomains.Sh : A Wrapper Around Tools I Use For Subdomain Enumeration On A Given Domain
* Slyther : AWS Security Tool
* Spring-Spel-0Day-Poc : Spring-Cloud / spring-cloud-function, spring.cloud.function.routing-expression
* Cloak : A Censorship Circumvention Tool To Evade Detection By Authoritarian State Adversaries
* OffensiveNotion : Notion As A Platform For Offensive Operations
* CVE-2022-27254 : PoC For Vulnerability In Honda's Remote Keyless System
* CVE-2022-22963 : PoC Spring Java Framework 0-day Remote Code Execution Vulnerability
* Casper-Fs : A Custom Hidden Linux Kernel Module Generator
* LAZYPARIAH : A Tool For Generating Reverse Shell Payloads On The Fly

GBHackers Analysis

* Ubuntu Desktop & Windows 11 Hacked - Pwn2Own Day 3
* Pwn2Own - Windows 11, Microsoft Teams Hacked & Exploiting 16 Zero-day Bugs
* Hackers Exploiting a Critical Vulnerability in Zyxel Firewall & VPN Devices
* Multiple QNAP Flaws Let attackers to Access and Read Sensitive Data
* Critical Cisco NFVIS Software Flaw Let Attacker Injects Commands at The Root Level

Weekly Cyber Security Video and Podcasts

SANS DFIR

* Learning to Combat Ransomware
* FOR509: Cloud Forensics & Incident Response Course - What to Expect
* Hunting Is Sacred, But We Never Do It for Sport! - SANS THIR Summit 2019
* Did I do that? - Understanding action & artifacts w/ Matthew Seyer & David Cowen - SANS DFIR Summit

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

* Top 5 CTFs to Get Started with Ethical Hacking
* Live Hacking Q&A with Kody Kinzie and Alex Lynd
* Hacking Shut Down iPhones - ThreatWire

The PC Security Channel [TPSC]

* Windows Update Ransomware
* How to tell if your Wifi is hacked?

Eli the Computer Guy

* TESLA is a TOXIC COMPANY - dropped from S&P ESG
* NETFLIX LAYOFFS - Go woke, get fired...
* ELON MUSK HALTS TWITTER DEAL - stupidity makes good clickbait
* WOKE EMPLOYEES FIRED from NETFLIX

Security Now

* The New EU Surveillance State - Eventful Patch Tuesday, Open Source Maintenance Crew, BIG-IP Boxes
* That "Passkeys” Thing - White House and Quantum Computers, Android 0-day, Ransomware snapshot

Troy Hunt

* Weekly Update 296

Intel Techniques: The Privacy, Security, & OSINT Show

* 262-Brief Updates

* 261-A Client Stops By

Proof of Concept (PoC) & Exploits

Packet Storm Security

* Linux USB Use-After-Free
* SAP Application Server ABAP / ABAP Platform Code Injection / SQL Injection / Missing Authorization
* LiquidFiles 3.4.15 Cross Site Scripting
* PHPIPAM 1.4.4 Cross Site Request Forgery / Cross Site Scripting
* Emby Media Server 4.7.0.60 Cross Site Scripting
* Trojan-Ransom.Thanos MVID-2022-0607 Code Execution
* SDT-CW3B1 1.1.0 Command Injection
* Online Discussion Forum Site 1.0 SQL Injection
* Showdoc 2.10.3 Cross Site Scripting
* OpenCart So Listing Tabs 2.2.0 Unsafe Deserialization
* T-Soft E-Commerce 4 SQL Injection
* T-Soft E-Commerce 4 Cross Site Scripting
* Survey Sparrow Enterprise Survey Software 2022 Cross Site Scripting
* SolarView Compact 6.0 Command Injection
* Zyxel Firewall ZTP Unauthenticated Command Injection
* Chrome 100 extensions::ExtensionApiFrameIdMap::GetFrameId Heap Use-After-Free
* IpMatcher 1.0.4.1 Server-Side Request Forgery
* Ransom.Conti MVID-2022-0606 Code Execution
* Zyxel Remote Command Execution
* Ransom.Conti MVID-2022-0605 Code Execution
* WordPress WP Event Manager 3.1.27 Cross Site Scripting
* Ransom.Conti MVID-2022-0604 Code Execution
* HighCMS/HighPortal 12.x SQL Injection
* Ransom.Conti MVID-2022-0603 Code Execution
* Ransom.Conti MVID-2022-0602 Code Execution

CXSecurity

* ExifTool 12.23 Arbitrary Code Execution
* Bitrix24 Remtoe Code Execution
* Ruijie Reyee Mesh Router Remote Code Execution
* Cisco RV340 SSL VPN Unauthenticated Remote Code Execution
* F5 BIG-IP Remote Code Execution
* VMware Workspace ONE Access Template Injection / Command Execution
* Watch Queue Out-Of-Bounds Write

Proof of Concept (PoC) & Exploits

Exploit Database

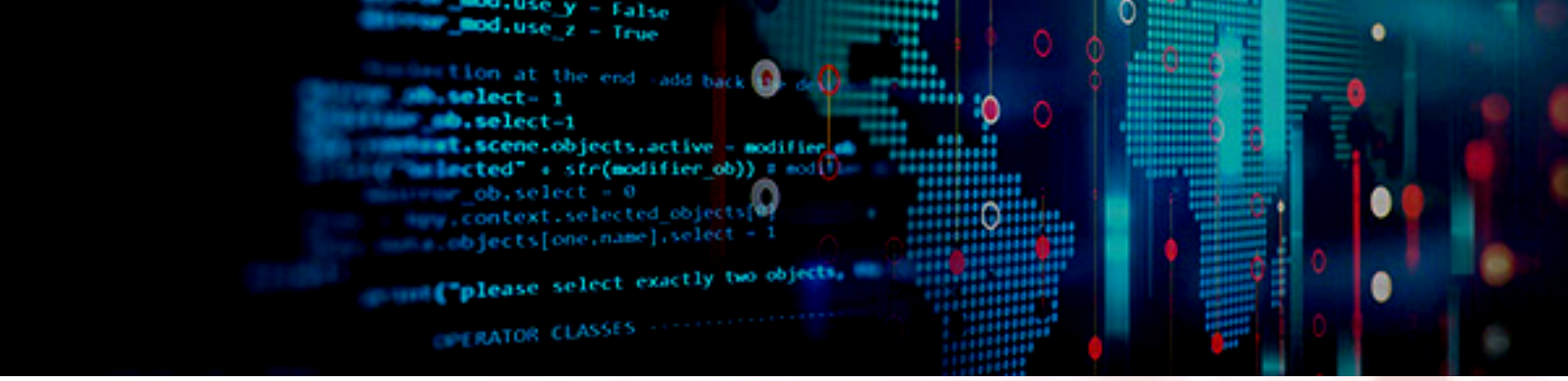
* [webapps] Showdoc 2.10.3 - Stored Cross-Site Scripting (XSS)
* [remote] SolarView Compact 6.0 - OS Command Injection
* [webapps] T-Soft E-Commerce 4 - SQLi (Authenticated)
* [webapps] T-Soft E-Commerce 4 - 'UrunAdi' Stored Cross-Site Scripting (XSS)
* [webapps] Survey Sparrow Enterprise Survey Software 2022 - Stored Cross-Site Scripting (XSS)
* [remote] SDT-CW3B1 1.1.0 - OS Command Injection
* [webapps] TLR-2005KSH - Arbitrary File Delete
* [webapps] Royal Event Management System 1.0 - 'todate' SQL Injection (Authenticated)
* [webapps] College Management System 1.0 - 'course_code' SQL Injection (Authenticated)
* [remote] F5 BIG-IP 16.0.x - Remote Code Execution (RCE)
* [webapps] TLR-2005KSH - Arbitrary File Upload
* [remote] Ruijie Reyee Mesh Router - Remote Code Execution (RCE) (Authenticated)
* [webapps] WordPress Plugin stafflist 3.1.2 - SQLi (Authenticated)
* [webapps] Joomla Plugin SexyPolling 2.1.7 - SQLi
* [webapps] WordPress Plugin Blue Admin 21.06.01 - Cross-Site Request Forgery (CSRF)
* [webapps] MyBB 1.8.29 - MyBB 1.8.29 - Remote Code Execution (RCE) (Authenticated)
* [webapps] Beehive Forum - Account Takeover
* [webapps] PHProjekt PhpSimplyGest v1.3. - Stored Cross-Site Scripting (XSS)
* [webapps] Navigate CMS 2.9.4 - Server-Side Request Forgery (SSRF) (Authenticated)
* [webapps] Explore CMS 1.0 - SQL Injection
* [remote] DLINK DAP-1620 A1 v1.01 - Directory Traversal
* [remote] PyScript - Read Remote Python Source Code
* [remote] Google Chrome 78.0.3904.70 - Remote Code Execution
* [remote] Tenda HG6 v3.3.0 - Remote Command Injection
* [webapps] Anuko Time Tracker - SQLi (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*

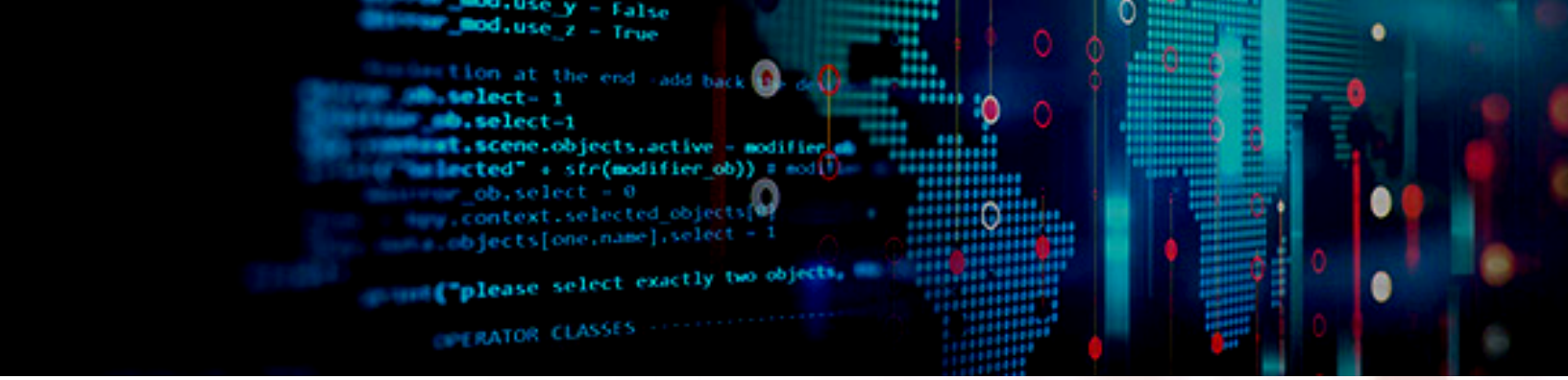
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.



Latest Hacked Websites

Published on Zone-h.org

https://taxeszone6.gov.bd/1975.html
https://taxeszone6.gov.bd/1975.html notified by 1975 Team
http://ngbvd.mglsd.go.ug/dz.php
http://ngbvd.mglsd.go.ug/dz.php notified by djebbaranon
http://sfc.go.ug
http://sfc.go.ug notified by CodeBoy1877
http://user.comune.caprinoveronese.vr.it//allegati/fckeditor/images/97.gif
http://user.comune.caprinoveronese.vr.it//allegati/fckeditor/images/97.gif notified by Ali Duzlawi097
http://www.comune.caprinoveronese.vr.it//allegati/fckeditor/images/97.gif
http://www.comune.caprinoveronese.vr.it//allegati/fckeditor/images/97.gif notified by Ali Duzlawi097
https://satpolppdamkar.purworejokab.go.id/$.php
https://satpolppdamkar.purworejokab.go.id/$.php notified by CytoRizki
http://kesra.mappikab.go.id
http://kesra.mappikab.go.id notified by Hamza Anonime
https://bpkad.mappikab.go.id
https://bpkad.mappikab.go.id notified by Hamza Anonime
https://bpbd.mappikab.go.id
https://bpbd.mappikab.go.id notified by Hamza Anonime
https://kerjasama.perpusnas.go.id/forger.html
https://kerjasama.perpusnas.go.id/forger.html notified by AnonSec Team
https://rb.perpusnas.go.id/forger.html
https://rb.perpusnas.go.id/forger.html notified by AnonSec Team
https://www.tlanalapa.gob.mx
https://www.tlanalapa.gob.mx notified by Hamza Anonime
http://montealto.sp.gov.br/kurdz.txt
http://montealto.sp.gov.br/kurdz.txt notified by 0x1998
https://is-mp.nuvem.gov.br/authenticationendpoint/psy.html
https://is-mp.nuvem.gov.br/authenticationendpoint/psy.html notified by psycIllusion
https://api.prodam.sp.gov.br/authenticationendpoint/psy.html
https://api.prodam.sp.gov.br/authenticationendpoint/psy.html notified by psycIllusion
https://idmtest.secretariajuridica.gov.co//authenticationendpoint/psy.txt
https://idmtest.secretariajuridica.gov.co//authenticationendpoint/psy.txt notified by psycIllusion
https://is-admin-mp.nuvem.gov.br/authenticationendpoint/dock.html
https://is-admin-mp.nuvem.gov.br/authenticationendpoint/dock.html notified by psycIllusion



Dark Web News

Darknet Live

EncroChat: Coke Dealer Sentenced to Almost 13 Years in Prison

A drug dealer in the United Kingdom was sentenced to 12 years in prison for supplying cocaine, heroin, and cannabis, to people "across the country.” Joseph Byrne, 44, of Knowsley, was sentenced to 12 years and nine months in prison after pleading guilty to conspiracy to supply class A and B drugs at Liverpool Crown Court. Joseph Byrne "We will continue to keep this momentum going and pursue offenders who think they can lie undetected by using the darkweb, as we are taking action and bringing them to justice,” Merseyside Police Detective Inspector Chris Lowe said. Merseyside Police arrested Byrne as a part of Operation Venetic; during the investigation into the encrypted communication service Encrochat, investigators identified Byrne as the person operating an Encrochat account under the username "Foxhedge.” Byrne used the account to facilitate the distribution of multiple kilograms of heroin, cocaine, and cannabis to buyers "from Liverpool to Wales.” Drugs and cash seized by police during the investigation into Byrne Police also learned that the dealer had grossed Â£349,000 within three months. "Byrne's guilty plea reinforces the strength of evidence we have in these type cases to convict those attempting to evade detection by utilizing encrypted devices. This latest sentencing, along with the other convictions that we have accomplished, highlights our success in arresting and convicting people,” Detective Inspector Chris Lowe said. (via darknetlive.com at https://darknetlive.com/post/encrochat-drug-dealer-sentenced-to-prison/)

Three Sentenced to Prison for Selling Amphetamines

Three drug dealers were sentenced at the Munich Regional Court to lengthy prison terms after police intercepted a package containing 10 kilograms of amphetamine. In February 2021, the Bavarian State Criminal Police Office (BLKA), in close cooperation with local law enforcement, arrested three drug dealers for "drug trafficking via the dark web.” "This investigative success was preceded by extensive investigations into orders for narcotics on an online trading platform on the darkweb,” according to an announcement from the BLKA. Police arrested three people on February 10, 2021, after one of the defendants had accepted the delivery of a shipment containing ten kilograms of amphetamine. The press release indicates that a supplier on the darkweb had shipped the amphetamine. A separate investigation into two of the drug dealers is underway. Investigators are analyzing so-called "crypto cell phones” for evidence of additional criminal activity. One of the dealers may have dealt up to "90 kilograms of marijuana, 13 kilograms of amphetamine, and one kilogram of cocaine. The court sentenced the defendants to prison terms of 9 years and eight months, seven years, and six years and four months. The defendants were also ordered to pay fines of up to six figures. polizei.bayern.de, archive.is, archive.org (via darknetlive.com at https://darknetlive.com/post/three-bavarian-dealers-sentenced-to-prison/)

Paris: Versus Market Exploit "is Real"

The Versus Market exploit is legitimate, Paris claimed. A user on Dread (/u/threesixty) hacked Versus Market "in a time span of about 2 hours,” according to a post on the Versus subdread. "Please remove security driven from your website title. You are not security driven.”

threesixty generated little traction with his brand new account The user who had discovered the vulnerability, /u/threesixty, contacted DeSnake, the administrator of AlphaBay, about "the security issues on Versus.” According to DeSnake's posts on Dread about the incident, he initially assumed threesixty's post contained FUD. DeSnake and threesixty then worked together "to get even more proof on top of what he had recovered initially.” A "meaningless excerpt from the file,” posted by threesixty as a form of proof for Versus staff. It is not a form of proof for those of us without access to Versus: -- -- Table structure for table `crons` -- DROP TABLE IF EXISTS `crons`; /*!40101 SET @saved_cs_client = @@character_set_client */; /*!40101 SET character_set_client = utf8 */; CREATE TABLE `crons` (`id` int(10) unsigned NOT NULL AUTO_INCREMENT, `created` timestamp NOT NULL DEFAULT current_timestamp(), `last_edit` timestamp NOT NULL DEFAULT current_timestamp() ON UPDATE current_timestamp(), `next_run` timestamp NOT NULL DEFAULT '0000-00-00 00:00:00', `interval` int(10) unsigned NOT NULL, `cron` text NOT NULL, `took` bigint(20) NOT NULL, PRIMARY KEY (`id`)) ENGINE=InnoDB AUTO_INCREMENT=14 DEFAULT CHARSET=utf8mb4; /*!40101 SET character_set_client = @saved_cs_client */; -- -- Dumping data for table `crons` -- LOCK TABLES `crons` WRITE; /*!40000 ALTER TABLE `crons` DISABLE KEYS */; INSERT INTO `crons` VALUES (1,'2019-12-03 09:56:24','2021-10-16 17:24:18','2021-10-16 17:25:18',60,'check_invoices',7238),(2,'2019-12-03 09:56:14','2021-10-16 17:24:03','2021-10-16 17:25:03',60,'get_rates',219)... DeSnake described the impact of their work as a "complete takeover. Database, files, cryptocurrency wallets (of course those that have used multisig are okay either way), real IP exposed etc. Complete pwn.” Versus hacked for 3rd time or why security must be a priority for DNM admins _ The hyperlinks have been removed to prevent you know, the thing. DeSnake: Disclaimer: Before I begin with the post I would like to point out that I do not have anything against /u/WilliamGibson himself. Yes I do not think security (getting hacked 3 times) and stability (offline almost all the time during DDoS) is on point for their status as a marketplace even more so 3 years down the line. Yes their inability to get their Staff issues/communication spills over the business and the posts from customers speaks for that. However at the very least they kept going and were providing a platform for people to trade. I was contacted around a day ago by the hacker /u/threesixty about the security issues on Versus. As with everything I take it with a cup full of salt before I do my own verification. I took a look at his profile and of course it was a new one which led me even further to believe this to be FUD. He had created a post on Versus subdread (dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/e408c16ab482106c4eea)/ which got suprisingly little attention for the details that it was outlining and claiming. I decided to ask him for further details and in an encrypted PGP message he provided an interesting amount of information. Now anyone could have created that information so the only way to verify it was to test myself. I was almost certain it had been patched by Versus… but even after the post threesixty had done the vulnerability was still sitting there plain as day allowing anyone to browse through the system and potentially escalate to full control over the server. Together with the good-willed hacker 360, we were able to get even more proof on top what he had recovered initially that indeed it is the real server of Versus. All proof was provided to Paris right before putting this post up. The Vulnerability _ Testing the vulnerability was straightforward and as threesixty said a textbook one. There was no complexity in it or discovering it. How no one has reported it or fixed in 3 years I or him do not understand. Complete props go to him for finding it. The Impact _ Complete takeover. Database, files, cryptocurrency wallets (of course those that have used multisig are okay either way), real IP exposed etc. Complete pwn. From threesixties (and mine) side nothing has been taken or modified in any shape or form. Only information was downloaded such as databases and files (including system ones to prove the existence) which would allow us to prove the vulnerability exists to other high ranking people like /u/Paris . Cryptocurrency wallets were never touched. Given the issues with security that are now happening for the 3rd time in the markets history, Staff problems also affect Versus. I have no doubt that affects the security and maintenance of the marketplace. Staff are a core part of the marketplace without Staff administrators are nothing and vice versa. So for all of you marketplace admins make sure your Staff are well, financially and in other ways. When you are an employer it is your duty to ensure you create a good environment for individual employees to thrive and grow both professionally and personally. Witchman05 himself said in this thread about Versus vendor

issues, quote dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/e83da76a7c5f41e2f844)/#c-f13009c91041cbb306 I do know that Huxley, Poe, Gibson and Rowling have had some differences in opinion that came to a head about two weeks ago, and they're probably still kind of simmering about that. I won't go into detail, because that's their business, but just saying, you're probably not going to get an instant reply on this thread. There were a lot of factors, a lot of… underlying issues, a lot of kind of hurtful things were said, and it was honestly kind of ugly. I've been talking with all of them, seeing it from all sides, and while I'm honestly kind of hesitant to pick sides on that whole mess, considering I don't have any sort of actual bond to the market itself anymore, I will say some things definitely could stand to have a bit of a shake-up in the process it's been handled with. Of course, I could be wrong. These guys that I've known for almost a decade could have decided to go completely irrational at the drop of a hat, burning not only these names but also their entire reputation for the rest of their careers on the Darknet. My point is, be careful, all. What I am trying to get to here is it all starts within. Bad Staff management leads to poor handling of tickets, lack of care for either customers or vendors, lack of any upkeep on servers and network and so on. As a marketplace putting up a patch is not enough e.g. restarting your services because they went down due to DDoS. Ask yourself why did they go down what is the core issue, it is all in the logs. That is how you solve the core of the problems not treat the aftermath with painkillers figuretively speaking. Not everyone has this way of thinking and that is fine but as a marketplace, a reputable one, it is your duty to have your shit in order. I would also not be surprised that some of the 'phishing' of high ranking vendors that has happened had actually been hacked accounts from the database. Lots of reputable vendors got 'phished' with no clear explanation in sight. I am assuming another hacker has the Versus database as well and knows about this or other vulnerabilities and has abused their access. In spirit of full disclosure currently Versus markets backend seem to be giving a white screen of death which may or not be related to the thinkering myself and /u/threesixty had been doing. That white screen has happened before which would mean we have not caused it or… someone else has had access to files and databases like we did and has abused it to DoS the backend into submission. If it had been a result of our testing we apologize. We hope to have a fruitful conversation about security on marketplaces especially on established ones. Since day one my goal with AlphaBay was security followed by stability and usability and in the era of takedowns, DDoS (which further exposes your infrastructure as a marketplace) and rinse and repeat scams like those of groups like lovelace, administrators can not allow themselves not to test every single user input and sanitize it. Further how an active Web Application Firewall (WAF) is not present on Versus is also beyond me. A lot of features of 'security' seem to be missing by a 'security-driven marketplace' like Versus claims to be. Admins should not be slacking when it comes to the security of their customers who are both buyers and vendors. The results are known what happens when you let go and do not follow the security guideliness. Security is not a product, it is a never-ending process. Both threesixty and myself have the best intentions. That is why we did not leak the database or stole any coins. For me personally, 3 times is too much of anything but as with everything we should at least be grateful for what we have first and then work on improving it second. Thank you. Dread: dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/81fac8c141c9fc519b9f Paris _ Paris, the co-administrator of Dread, responded in the comment section of DeSnake's post, claiming that he had verified the exploit. Paris: /u/DeSnake has provided me the exploit and rational. I have personally verified it. IT IS REAL. The exploit is extremely simple but compromising. It allows for full access to the underlining file system on the server. This include information within the /etc/ directory as well as wallet directories. It is a full information compromise of the system. Everything to the server's IP address, to the backup of the database in the admin home folder, to the wallet files themselves. I am able to traverse nearly the entire file system with web server level access. There is no jail, WAF, and minimal care to limit the information disclosure in the event of a web server compromise. I am able to view the history of IP addresses which have previously accessed the server. This is a major compromise and it is very easy to find and pull off. Even a simple scriptkitty that is running a web server tester will find this exploit. /u/WilliamGibson I will be passing this information over to you. This shouldn't be a problem with even the most basic jailing practices on the web server layer. Until such time

as this is fixed nobody should use Versus. I can't say that enough. This entire server is probably compromised already by law enforcement and being monitored. It is a total compromise and is without a doubt one of the worse outcomes to a simple security exploit I have seen in a very long time. Signed Copy -----BEGIN PGP SIGNED MESSAGE----- Hash: SHA256 /u/DeSnake has provided me the exploit and rational. I have personally verified it. IT IS REAL. The exploit is extremely simple but compromising. It allows for full access to the underlining file system on the server. This include information within the /etc/ directory as well as wallet directories. It is a full information compromise of the system. Everything to the server's IP address, to the backup of the database in the admin home folder, to the wallet files themselves. I am able to traverse nearly the entire file system with web server level access. There is no jail, WAF, and minimal care to limit the information disclosure in the event of a web server compromise. I am able to view the history of IP addresses which have previously accessed the server. This is a major compromise and it is very easy to find and pull off. Even a simple scriptkitty that is running a web server tester will find this exploit. /u/WilliamGibson I will be passing this information over to you. This shouldn't be a problem with even the most basic jailing practices on the web server layer. Until such time as this is fixed nobody should use Versus. I can't say that enough. This entire server is probably compromised already by law enforcement and being monitored. It is a total compromise and is without a doubt one of the worse outcomes to a simple security exploit I have seen in a very long time. -----BEGIN PGP SIGNATURE-----
iQIzBAEBCAAdFiEEbfleES3oPdbct1q5DE1JcU+sN9gFAmKETTgACgkQDE1JcU+s
N9jjpQ//avXy8kS1tMhVK4botRjGhXit+k88pwKwWnizwg+GQTaFCu+XCd3SrDa9
tjZrcgmaVYJYjr+lprKE/aSw9ak1go8D90631N59mTR6DRlBr4Q8c1O0uMKC8cX8
+ONi+JSN5QBiigtp1MC/mVIhQJeLdgx5bDl+MtJe0jXFK+t26WwvKpscbydr22kQ
0enYyhliHDp+ikH12gXVLGn2yLBMCi12UD3xxlCJDBB/nbzH10dY3L8qQmsyf0JV
dRV4YPpxKabui0yYxqrUy2uLGDxuyKx7thBG0zJyOg/Oewss2iRexGkxyomuw9be
82ijGWMHNKorNXwwgj41485cOknSsuPo3JaibQJr5BNESvjxCos2gbhnfJ10xXR+
SkM7hFQAJt28W1dV3/qXl+wV/iL1+VsxNBpjckDK+m+D4UsDwpS8eZkx1+Vq0jOI
qAQBubC/d9vLpQvgSqRUFdyiK+FTY/u6P3eXdTXJCB+AZ5wWfaUAiEKhstSK1Zba
W4Gh2TQSxgTZtmyh2NdahkRFTSe0NaGFx9FsDBA5gzL8PcVg8CqWuZwo4LH3/f8S
F2whSD9AUnPZ4mUpi4JzSVOOWyEL1cGiVni7Y5aKVdwWFEb6vWhEia178EOAjOjK
KlqkptcI1LMuy2DLPBK/c/vCW/NpbADUXj21X4DxRsxRwblyxHY= =zt91 -----END PGP SIGNATURE----- dread:
dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/81fac8c141c9fc519b9f/#c-fa7cd8851e945ec830 "immediately compromised” _ A user in the comments asked Paris why "you and your best friend desnake (the only market operator here that has actually has a market busted by LE) blow it wide open and you even make it an announcement?” Paris responded: You need to understand that the server with a simple exploit like this is immediately compromised. As in it has already been compromised for a long time. Unless law enforcement is sitting on their hands they have already pwned this entire server. Priority for me is community safety. Which means immediate disclosure and warning. You may think that is fucking the community over but it's not. The exploit is ALREADY there and probably has been there for a long time. Easily findable and a simple request crafted in a specific way exploits the file system access to basically whatever. Limiting the damage caused is disclosing this and not having it behind closed doors to be fixed when the admins decide to fix it. They must move servers immediately and patch before bringing it up to the public. Right fucking now. Because right now it's a free season and all the information to be had about versus's server is up for grabs. dread:
dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/post/81fac8c141c9fc519b9f/#c-d447d6525bd3caefd6 Previous Incidents _ I.P. Leak _ In March 2020, Versus paused operations to conduct a security audit after a "a potential IP leak from one of our middleware server[s].” Versus staff posted an explanation: What happened? _ A few days ago a DDOS against Versus started. The application layer of Versus is very strong, so it was tor failing sometimes. The attacker found an application layer vulnerability by requesting non existing captcha images. This lead to a lot of useless file IO and exhausted the main server

resources. Changing the captcha system isn't a quick fix, so we deployed a custom middle-ware on the tor fronted servers to deliver the captchas and filter bad traffic before it even gets to the main server. To further improve the resistance of Versus we did a V3 load balancing test. To not have to apply the middle-ware to all servers for this test, it was moved to a single server in the same DC the tor front-end servers. The plan was to use one middle-ware server for every balanced mirror, not every tor instance. A bad decision lead to an IP leak of the middle-ware server. Versus was down for about 14 hours to move our complete infrastructure to other hosts. From every DC, not just the compromised one. Some additional errors then popped up because bitcoin-core, monero-core and our database got updated to the most recent version. How we fucked up. _ A trace route showed a perfect loop-back on the middle-ware server IP so the request was routed there via IP as nothing would go beyond the first router. THIS WAS A BAD DECISION MADE AFTER NEARLY 3 DAYS WITH NEXT TO NO SLEEP. The middle-ware gets the onion and adds it to a custom header so that we see from which mirror the request is coming from, but instead of extracting the onion, it extracted the IP from the request (it's own) and added it to the header. The main server used this header to generate the 2FA message where the IP was shown. What we did to avoid such stupid mistakes in the future. _ The middle-ware was fixed to extract to correct onion under any circumstances. The display of the hostname gets validated via regex. There is no more routing via IP. The middle-ware will run on every single tor instance. The routing to the back-end server is also over Tor. Additionally we checked the source to look for any other instance where the hostname/custom header might show up. Nothing was found. This multiple layers of security will make sure, that even a bad decisions under sleep deprivation will not lead to such an event again. Bitcoin Theft _ In July 2020, Versus staff announced that someone had hacked the market and had stolen the majority of the Bitcoin held in escrow. This is a post i hoped to never make but the foundation of Versus is honesty and transparency to our members. As of today, July 10th, we were hacked and a majority of bitcoin held in escrow was stolen. We immediately took down the market and confirmed that no sensitive has been compromised. We are committed to identifying the vulnerability that was exploited and will not go back online until this is solved. We know many of you are reading this and worried about your funds. We are going to do our best to make up for it just like we did with the lost XMR, either through refunds , reduced fees, free ads and more. We also want to remind everyone that this is an unfortunate example of why MS is so important , your funds simply cannot be stolen. Multisig payments are NOT affected and can be received with the presigned and timelocked raw transactions we provided vendors with. To be perfectly clear: When we get back we will enforce multisig payments. We know some of you may scream exit scam and we expect that. We aren't going anywhere and will be back stronger and more secure than ever. We live, we learn. The Versus Project is a lot more than just a market and we won't abandon our vision. To our community , thank you for sticking with us. Going Forward _ Markets rarely return after something like this becomes public. However, Versus has experienced this at least twice. The market is more popular now than in 2020 after both incidents described above. (via darknetlive.com at https://darknetlive.com/post/paris-verfied-desnake-versus-hack/)

Australian Police Arrest Two Alleged Darkweb Vendors

Cybercrime investigators dismantled a darkweb drug trafficking operation and arrested two suspects.

Australian police always seem to have suspiciously thin back plates According to a press release from the NSW Police, investigators from the State Crime Command's Cybercrime Squad launched an investigation into darkweb drug trafficking in Australia. Strike Force Glene identified a marketplace where users could exchange cryptocurrency for prohibited drugs and restricted substances. Yesterday, on May 17, police executed three search warrants in Chatswood and Rose Bay. At the Chatswood address, police arrested a 33-year-old man. At the home in Rose Bay, police arrested a 39-year-old man. They also searched a business in Rose Bay.

Three bags of powder seized during the raids "In terms of scale, this operation sits as one of the more sophisticated we've seen with respect to both the quantity of illicit drugs being traded, right through to distribution and packaging,” Det Supt Craft said.

A picture of what appears to be blotter of some sort During the searches, investigators more than 100 grams of cocaine and MDMA, 3kg of unidentified powder, thousands of unidentified pills, and "17kg of confectionery, suspected to be laced with THC.” They additionally seized nearly $60,000 cash,

an engagement ring worth approximately $100,000, mobile phones, computers, electronic storage devices, and cryptocurrency. A ring police believe was purchased with the proceeds of crime The suspects face charges for "supply prohibited drug, participate criminal group contribute criminal activity, supply prohibited drugs on an ongoing basis, and knowingly deal with proceeds of crime.” Since 2015, the suspects allegedly processed more than 30,000 drug transactions worth at least $1.16 million. More powder A bag of pills seized during the raid Powder seized by NSW police The ring police will lose in the near future. Possibly LSD blotter "We will be alleging the profits both these men were reaping as a result of these illicit trades were so vast, attempts were made to launder funds in cryptocurrency and cash using third parties. Those involved with this operation believed the dark web provided with them a cloak of invisibility and anonymity to conduct their illicit sales; their court appearance today says otherwise,” Det Supt Craft said. Sophisticated 'dark web' drug supply syndicate dismantled - Cybercrime Squad - arcive.is, archive.org, police.nsw.gov.au (via darknetlive.com at https://darknetlive.com/post/nsw-police-bust-a-million-dollar-drug-trafficking-ring/)

Dark Web Link

Top Darknet Markets 2022: The Outstanding Performances To Consider Now

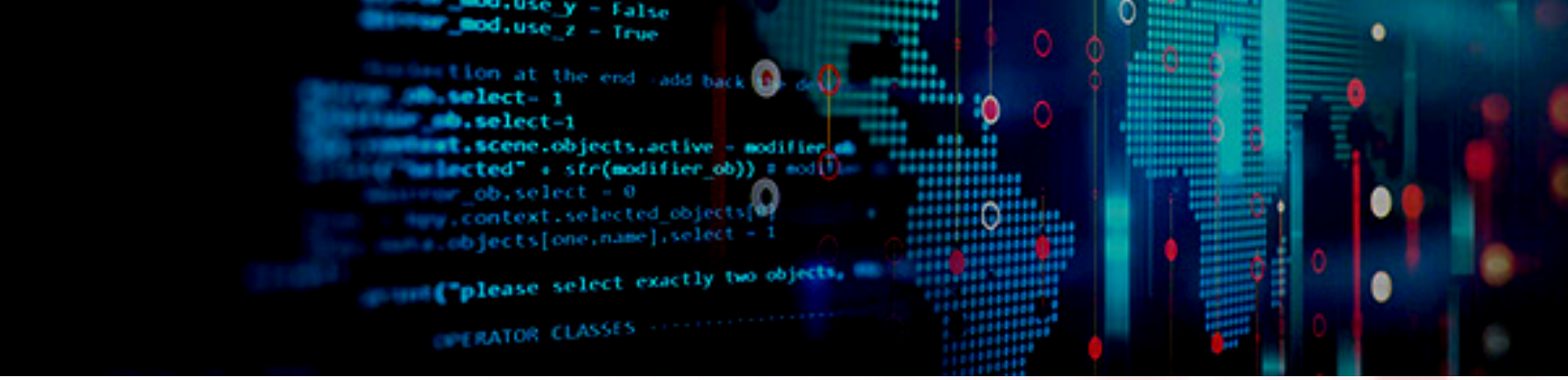
The darknet markets are subject to availability and one of the many factors that contributes to the working of these dark web markets is their performances. The top darknet markets 2022 is the example where each of the marketplaces in the Tor network has proven its performance over and over again. So, 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

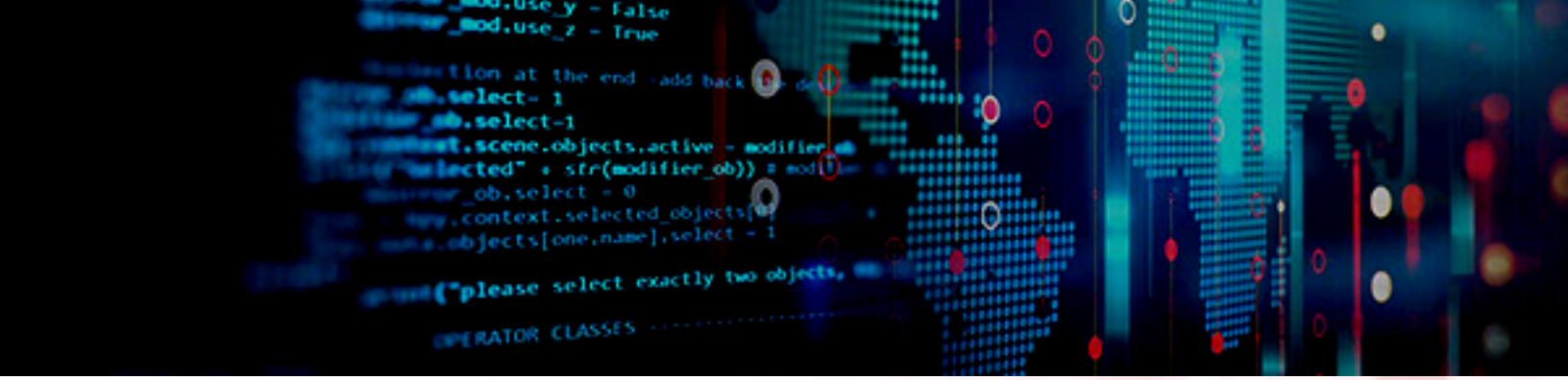
Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.

RiskIQ

* Skimming for Sale: Commodity Skimming and Magecart Trends in Q1 2022
* RiskIQ Threat Intelligence Roundup: Phishing, Botnets, and Hijacked Infrastructure
* 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

FireEye

* Metasploit Weekly Wrap-Up
* Are You in the 2.5% Who Meet This Cybersecurity Job Requirement?
* CVE-2022-22972: Critical Authentication Bypass in VMware Workspace ONE Access, Identity Manager, and
* Find, Fix, and Report OWASP Top 10 Vulnerabilities in InsightAppSec
* Maximize Your VM Investment: Fix Vulnerabilities Faster With Automox + Rapid7
* Metasploit Weekly Wrap-Up
* Update for CIS Google Cloud Platform Foundation Benchmarks - Version 1.3.0
* CVE-2022-30525 (FIXED): Zyxel Firewall Unauthenticated Remote Command Injection
* [Security Nation] Jim O'Gorman and g0tmi1k on Kali Linux
* Patch Tuesday - May 2022



Advisories

US-Cert Alerts & bulletins

* ISC Releases Security Advisory for BIND
* CISA Releases Analysis of FY21 Risk and Vulnerability Assessments
* CISA Issues Emergency Directive and Releases Advisory Related to VMware Vulnerabilities
* Threat Actors Exploiting F5 BIG IP CVE-2022-1388
* Apple Releases Security Updates for Multiple Products
* Weak Security Controls and Practices Routinely Exploited for Initial Access
* CISA Adds Two Known Exploited Vulnerabilities to Catalog
* Apache Releases Security Advisory for Tomcat
* AA22-138B: Threat Actors Chaining Unpatched VMware Vulnerabilities for Full System Control
* AA22-138A: Threat Actors Exploiting F5 BIG-IP CVE-2022-1388
* Vulnerability Summary for the Week of May 9, 2022
* Vulnerability Summary for the Week of May 2, 2022

Zero Day Initiative Advisories

Packet Storm Security - Latest Advisories

Red Hat Security Advisory 2022-4668-01

Red Hat Security Advisory 2022-4668-01 - Red Hat OpenShift Virtualization release 4.10.1 is now available with updates to packages and images that fix several bugs and add enhancements. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-4690-01

Red Hat Security Advisory 2022-4690-01 - Red Hat Openshift GitOps is a declarative way to implement continuous deployment for cloud native applications. Issues addressed include a spoofing vulnerability.

Red Hat Security Advisory 2022-4692-01

Red Hat Security Advisory 2022-4692-01 - Red Hat Openshift GitOps is a declarative way to implement continuous deployment for cloud native applications. Issues addressed include a spoofing vulnerability.

Red Hat Security Advisory 2022-4691-01

Red Hat Security Advisory 2022-4691-01 - Red Hat Openshift GitOps is a declarative way to implement continuous deployment for cloud native applications. Issues addressed include a spoofing vulnerability.

Red Hat Security Advisory 2022-4623-01

Red Hat Security Advisory 2022-4623-01 - This release of Red Hat build of Quarkus 2.7.5 includes security updates, bug fixes, and enhancements. For more information, see the release notes page listed in the References section. Issues addressed include HTTP request smuggling, cross site scripting, denial of service, information leakage, and privilege escalation vulnerabilities.

Red Hat Security Advisory 2022-4644-01

Red Hat Security Advisory 2022-4644-01 - The kernel-rt packages provide the Real Time Linux Kernel, which enables fine-tuning for systems with extremely high determinism requirements. Issues addressed include a privilege escalation vulnerability.

Red Hat Security Advisory 2022-2205-01

Red Hat Security Advisory 2022-2205-01 - 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 4.9.33. Issues addressed include a cross site scripting vulnerability.

Red Hat Security Advisory 2022-4661-01

Red Hat Security Advisory 2022-4661-01 - The pcs packages provide a command-line configuration system for the Pacemaker and Corosync utilities. Issues addressed include a traversal vulnerability.

Red Hat Security Advisory 2022-4655-01

Red Hat Security Advisory 2022-4655-01 - 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 a privilege escalation vulnerability.

Red Hat Security Advisory 2022-4642-01

Red Hat Security Advisory 2022-4642-01 - The kernel packages contain the Linux kernel, the core of any Linux operating system. Issues addressed include null pointer and privilege escalation vulnerabilities.

Red Hat Security Advisory 2022-4667-01

Red Hat Security Advisory 2022-4667-01 - OpenShift Virtualization is Red Hat's virtualization solution designed for Red Hat OpenShift Container Platform. This advisory contains OpenShift Virtualization 4.10.1 RPMs. Issues addressed include a denial of service vulnerability.

Red Hat Security Advisory 2022-4651-01

Red Hat Security Advisory 2022-4651-01 - The container-tools module contains tools for working with containers, notably podman, buildah, skopeo, and runc. Issues addressed include a privilege escalation vulnerability.

Ubuntu Security Notice USN-5429-1

Ubuntu Security Notice 5429-1 - Thomas Amgarten discovered that Bind incorrectly handled certain TLS connections being destroyed. A remote attacker could possibly use this issue to cause Bind to crash, resulting

in a denial of service.

Ubuntu Security Notice USN-5430-1

Ubuntu Security Notice 5430-1 - It was discovered that GNOME Settings incorrectly handled the remote desktop sharing configuration. When turning off desktop sharing, it may be turned on again after rebooting, contrary to expectations.

Ubuntu Security Notice USN-5428-1

Ubuntu Security Notice 5428-1 - Tobias Stoeckmann discovered that libXrandr incorrectly handled certain responses. An attacker could possibly use this issue to cause a denial of service, or possibly execute arbitrary code.

Ubuntu Security Notice USN-5423-2

Ubuntu Security Notice 5423-2 - USN-5423-1 fixed several vulnerabilities in ClamAV. This update provides the corresponding update for Ubuntu 14.04 ESM and 16.04 ESM. Michał Dardas discovered that ClamAV incorrectly handled parsing CHM files. A remote attacker could possibly use this issue to cause ClamAV to stop responding, resulting in a denial of service.

Jupiter / JupiterX Theme Privilege Escalation / LFI / DoS / Access Control Issues

Jupiter Theme versions 6.10.1 and below as well as JupiterX Core plugin versions 2.0.7 and below suffer from privilege escalation and post deletion vulnerabilities. JupiterX Theme versions 2.0.6 and below as well as JupiterX Core versions 2.0.6 and below suffer from plugin deactivation and setting modification flaws. JupiterX Theme versions 2.0.6 and below as well as Jupiter Theme versions 6.10.1 and below suffer from path traversal and local file inclusion vulnerabilities. Jupiter Theme versions 6.10.1 and below suffer from an arbitrary plugin deletion vulnerability. JupiterX Core plugin versions 2.0.6 and below suffer from information disclosure, modification, and denial of service vulnerabilities.

Ubuntu Security Notice USN-5427-1

Ubuntu Security Notice 5427-1 - Muqing Liu and neoni discovered that Apport incorrectly handled detecting if an executable was replaced after a crash. A local attacker could possibly use this issue to execute arbitrary code as the root user. Gerrit Venema discovered that Apport incorrectly handled connections to Apport sockets inside containers. A local attacker could possibly use this issue to connect to arbitrary sockets as the root user.

Ubuntu Security Notice USN-5426-1

Ubuntu Security Notice 5426-1 - Jakub Wilk discovered that needrestart incorrectly used some regular expressions. A local attacker could possibly use this issue to execute arbitrary code.

Ubuntu Security Notice USN-5425-1

Ubuntu Security Notice 5425-1 - Yunho Kim discovered that PCRE incorrectly handled memory when handling certain regular expressions. An attacker could possibly use this issue to cause applications using PCRE to expose sensitive information. This issue only affects Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, Ubuntu 21.10 and Ubuntu 22.04 LTS. It was discovered that PCRE incorrectly handled memory when handling certain regular expressions. An attacker could possibly use this issue to cause applications using PCRE to have unexpected behavior. This issue only affects Ubuntu 14.04 ESM, Ubuntu 16.04 ESM, Ubuntu 18.04 LTS and Ubuntu 20.04 LTS.

Apple Security Advisory 2022-05-16-8

Apple Security Advisory 2022-05-16-8 - Xcode 13.4 addresses a logic issue and a privilege escalation issue.

Ubuntu Security Notice USN-5424-1

Ubuntu Security Notice 5424-1 - It was discovered that OpenLDAP incorrectly handled certain SQL statements within LDAP queries in the experimental back-sql backend. A remote attacker could possibly use this issue to perform an SQL injection attack and alter the database.

Ubuntu Security Notice USN-5423-1

Ubuntu Security Notice 5423-1 - Michał Dardas discovered that ClamAV incorrectly handled parsing CHM files. A remote attacker could possibly use this issue to cause ClamAV to stop responding, resulting in a denial of service. Michał Dardas discovered that ClamAV incorrectly handled parsing TIFF files. A remote attacker could possibly use this issue to cause ClamAV to stop responding, resulting in a denial of

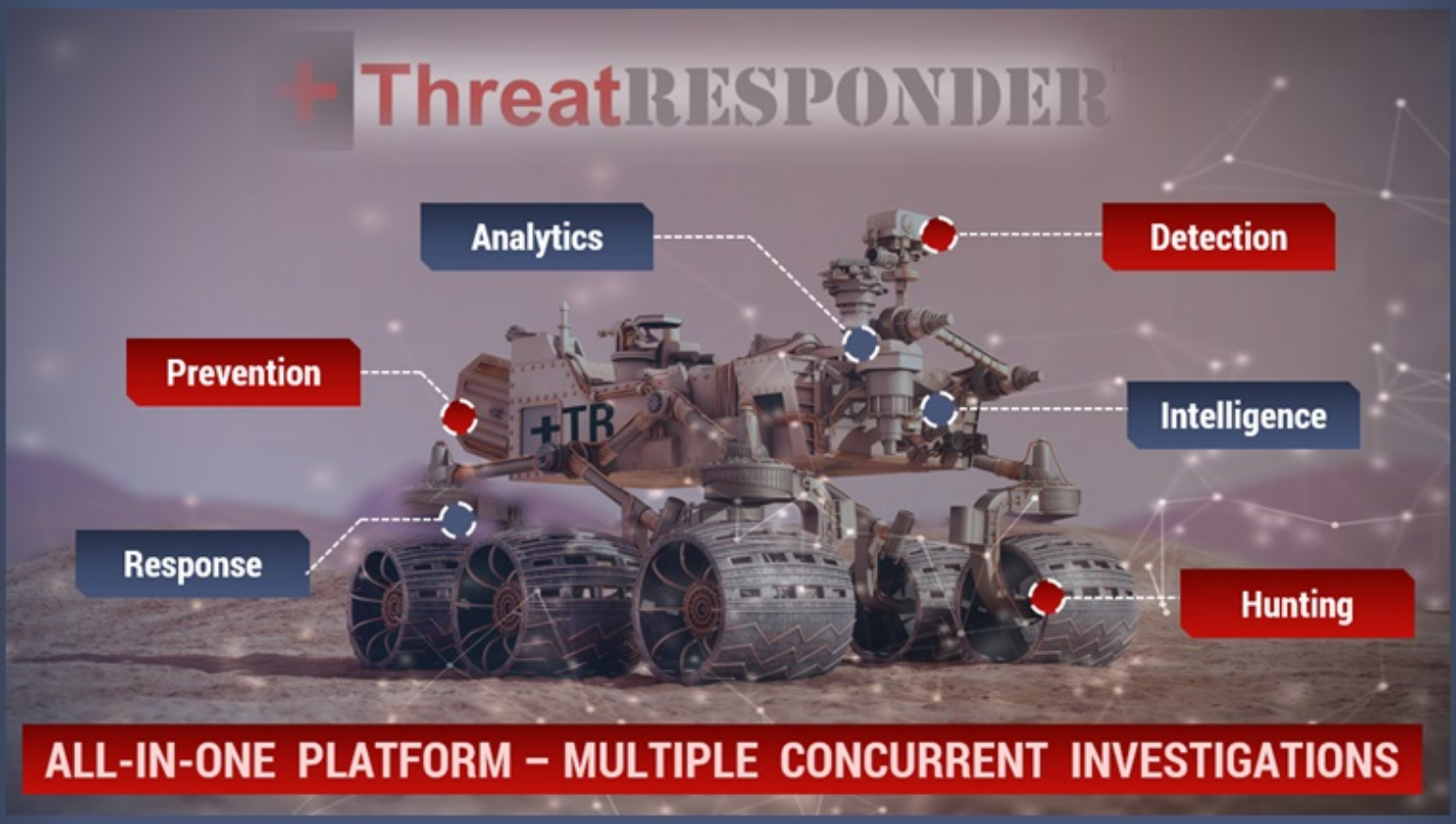
service. Michał Dardas discovered that ClamAV incorrectly handled parsing HTML files. A remote attacker could possibly use this issue to cause ClamAV to consume resources, resulting in a denial of service.
Ubuntu Security Notice USN-5311-2
Ubuntu Security Notice 5311-2 - USN-5311-1 released updates for contained. Unfortunately, a subsequent update reverted the fix for thisCVE by mistake. This update corrects the problem. It was discovered that containerd allows attackers to gain access to read- only copies of arbitrary files and directories on the host via a specially- crafted image configuration. An attacker could possibly use this issue to obtain sensitive information.

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



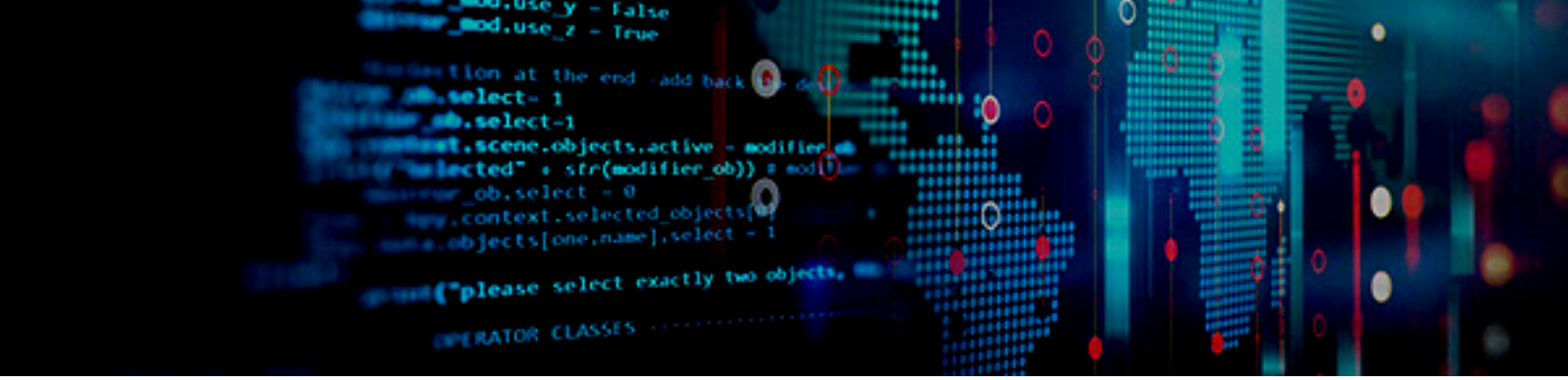
The Solution – ThreatResponder® Platform

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

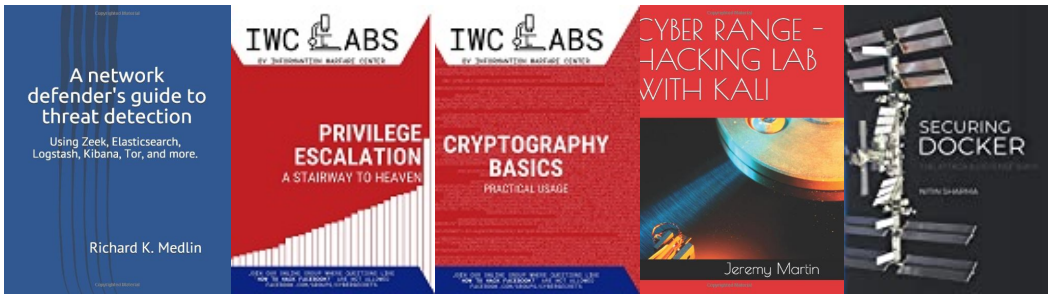


The Cyber Secrets publications on Amazon

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